Convergența securității digitale

Lect. univ. dr. Cătălin VRABIE

SNSPA, Facultatea de Administrație Publică
vcatalin@snspa.ro

Rezumat. *În fiecare zi, canalele de ştiri sunt inundate cu imagini venite din zonele de conflict din lumea întreagă. Pentru prima dată în istoria lumii, prin intermediul sateliților de comunicare şi grație rețelelor de socializare şi canalelor de ştiri, precum Youtube, Facebook sau Yahoo, avem loc în primul rând în sala de spectacole în care s-a transformat Internetul. Ceea ce camerele nu văd este că mai există o zonă de conflict în culise, în ceea ce astăzi se numește „lumea electronică". Aici luptele nu se dau cu rachete, bombe și gloanțe, ci cu biți și bytes. Convergența digitală, termen cu care literatura de specialitate ne-a obișnuit, se regăsește într-o formă similară și în domeniul securității digitale și al spionajului cibernetic. Acest articol va prezenta perspectiva pe care autorul o are asupra viitorului securității digitale privită prin intermediul istoriei acesteia.*

Cuvinte cheie:protecția datelor, intimitate, securitate digitală.

Introducere

În domeniul cercetării IT&C, securitatea ocupă un segment îngust (Gartner, 2015; Cybersecurity Ventures, 2015). Cu toate acestea, ea cuprinde câteva concepte foarte des întâlnite astăzi în mass media, precum: atacuri cibernetice asupra informațiilor sau asupra canalelor de comunicare, furturi de identitate etc. (Cisco, 2015).

Dacă suntem siguri de ceva în acest domeniu, acesta este faptul că ceea ce se întâmplă astăzi în lumea electronică și, mai cu seama, în securitatea digitală, va avea un impact profund asupra vieții noastre (Verizon, 2015), lucru de care s-ar putea ca noi nici măcar să nu fim conștienți. Un argument care fundamentează ipoteza este că o mare parte din tehnologia pe care o folosim uzual astăzi a fost descoperită în urma cercetărilor finanțate de guvernele lumii în dezvoltarea de noi tehnologii militare (FPRY, 2010).

Generațiile trecute au creat tehnologii precum calculatorul – în cel de-Al Doilea Război Mondial (Zimmermann, 2015), comunicații prin satelit și chiar Internetul – în timpul Războiului Rece (Lainer et al., 2012). Acestea sunt atât de folosite în viața de zi cu zi încât am ajuns în situația în care nu ne putem imagina viața fără ele. Putem vedea ce se întâmplă în cealaltă parte a lumii într-o clipă, precum, de asemenea, putem naviga folosind *Google street view* pe străduțele din cartierul nostru. Dacă tehnologiile create ieri au un asemenea impact asupra vieții noastre astăzi, atunci ce impact au tehnologiile create astăzi asupra zilei de mâine?

Vă vom prezenta câteva studii de caz din lumea securității digitale pentru ca, la final, să prezentăm tehnologia.

Spionajul cibernetic

Există, peste tot în jurul nostru, războaie cibernetice despre care nu avem nici cea mai mică idee (Symantec, 2015, 1). În spațiul cibernetic s-a ajuns deja într-un punct de confluență între om și mașină. Aceste două entități, odată complet separate, astăzi, cu greu mai pot fi distinse independent una față de cealaltă (Symantec, 2015, 2). Aceasta este era spionajului cibernetic.

Când ne gândim la spionaj, ne gândim la James Bond – eroul hollywoodian care se furișa, mai mult sau mai puțin în liniște, în sediile celor mai de temut organizații militare, pentru a proteja lumea de eventuale atacuri nucleare. Câteodată, Hollywood-ul merge prea departe! În acest caz, însă, el nu merge suficient de departe. Astăzi, serviciile de informații nu ar trimite o persoană într-o asemenea locație secretă – ea n-ar putea intra. Spionii de azi sunt spioni cibernetici. În filme, James Bond folosea tehnologia; astăzi, James Bond este tehnologie.

***

Vreau să vă conduc într-o călătorie în viitor. Dar înainte de a merge acolo, trebuie să facem câțiva pași în istorie pentru a înțelege mai bine ceea ce urmează să se întâmple. Ne vom întoarce, astfel, la momentul în care a fost creat primul virus de calculator – practic, momentul de început al acestei călătorii.

Nivelul I de convergență a securității

Primul virus a fost scris într-un joc video, pe o disketă care a fost inserată într-un Macintosh (Associated Press, 2007; Symantec, 2010), în anul 1981. De atunci, însă, lumea s-a schimbat. Acele tipuri de viruși se numeau *sneakerware* (Microsoft, 2013) pentru că cel care voia să infesteze un computer trebuia să meargă literalmente la acesta pentru a-l instala. Acesta a fost primul nivel de convergență, acolo unde omul era complet separat de mașini, interacțiunea dintre aceștia făcându-se punctiform și doar la inițiativa utilizatorului de PC.

Nivelul al II-lea de convergență a securității

În martie 1999 a fost lansat virusul Melissa – numit astfel de dezvoltatorul acestuia, David L. Smith, după numele dansatoarei lui favorite din Miami. A fost primul virus de tip vierme din lume. Era inserat în attachment-ul unui e-mail care avea subiectul <<Important Message From [numele utilizatorului infectat]>> (F-Secure, 2015). Odată ce attachment-ul era deschis, procesul se repeta și, în trei luni, sistemele de e-mail ale lumii au fost date peste cap. Companii ca Microsoft și Intel au raportat infestări – Microsoft, spre exemplu, și-a închis serverele de e-mail pentru a preveni răspândirea virusului (CNET, 2002). Totodată, acesta a fost și primul SPAM. Acest eveniment, urmat la un an mai târziu de apariția virusului ILOVEYOU (Symantec, 2002), marchează debutul nivelului al doilea al convergenței securității digitale. Aici, omul împuternicește tehnologia pentru a lucra în locul său.

Nivelul al III-lea de convergență a securității

Încă un an mai târziu, lumea securității digitale a fost din nou provocată – și nu vorbim aici de 11 septembrie 2001, ci de 15 iulie. Atunci a fost lansat Code Red. El nu a fost un virus, un vierme sau un troian, ci toate acestea la un loc. A reprezentat cea mai complexă amenințare cibernetică a lumii de până atunci (SANS Institute, 2001, 1), făcând ocolul lumii în trei zile. La 14 ore după lansare erau deja 359.000 de sisteme infestate. În fiecare minut, alte două mii de computere erau virusate. În total, au fost infestate aproximativ 6 milioane de sisteme (SANS Institute, 2001, 2; Greene, 2004), al căror cost de repunere în funcțiune s-a ridicat la 2.75 miliarde dolari, transformându-l, astfel, în cel mai costisitor malware (Greene, 2004). Guvernele lumii au înțeles ce se întâmplă și au realizat, totodată, că se pot folosi de această tehnologie pentru a trece la un nivel superior (Kearns, 2002) – acela de a face treaba pe care un spion uman nu ar reuși să o facă. Aceasta a fost intrarea în a treia fază de dezvoltare a convergenței, aceea în care tehnologia înlocuiește omul. Evenimentul a fost cu adevărat începutul erei spionajului cibernetic.

***

Vom continua prin a explica cum funcționează spionajul cibernetic. Vă vom conduce într-o misiune din viața reală, care a avut loc chiar la începutul decadei acesteia, departe, în Orientul Mijlociu. Deja probabil ați înțeles intenția – aceea de a ne furișa într-o instalație nucleară cu scopul de proteja lumea de o eventuală amenințare militară bazată pe armament atomic.

Imaginea următoare reprezintă baza nucleară Natanz, o instalație de îmbogățire a uraniului din Iran.

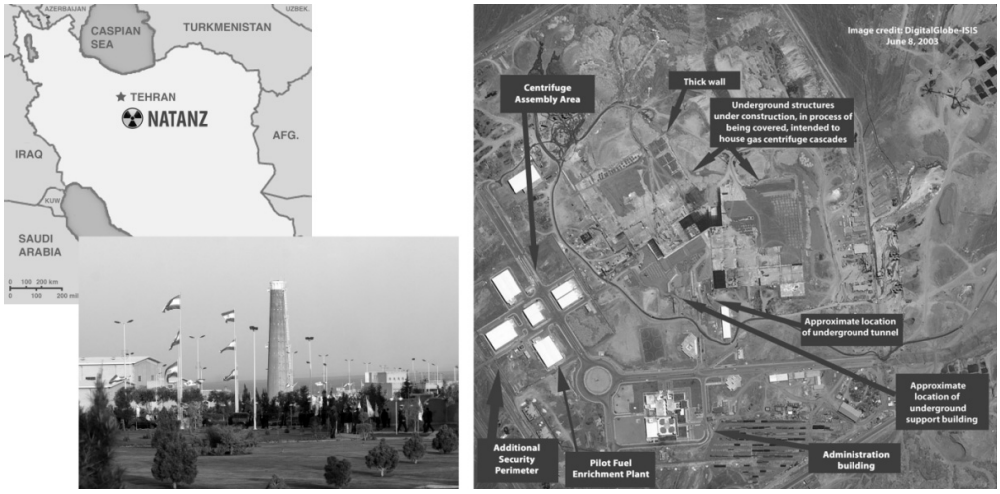

Figura 1. Baza nucleară iraniană Natanz
(1) poziția bazei pe harta Iranului, (2) imagine exterioară, (3) vedere din spațiu
Surse: *(1) nucleargamble.org, (2) usnews.com, (3) DigitalGlobe*

Forțele aliate erau îngrijorate că președintele Mahmoud Ahmadinejad (Figura 2) folosea instalațiile centrifuge din această bază pentru a crea mai mult combustibil nuclear decât avea nevoie în scopul producerii de energie electrică. Și aveau dreptate. El folosea acele centrifuge pentru a crea combustibil nuclear pentru arme atomice (Zetter, 2014).

Figura 2. Președintele Iranului, Mahmoud Ahmadinejad, în timpul unei vizite la Natanz în 2008
Sursa: *Biroul prezidențial al Republicii Islamice Iran*

Era nevoie ca aceste centrifuge să fie distruse. Dar cum puteau să facă asta? Nu puteau trimite soldați – baza era situată în mijlocul deșertului, așadar era imposibil să nu fie detectați. S-au gândit chiar să trimită avioane de vânătoare pentru a lansa rachete și a arunca în aer totul (Khan, 2010). Acțiunea asta ar fi fost cam gălăgioasă și destul de murdară. Nu era chiar o bună campanie de PR – să ne imaginăm urmările!

Astfel, în loc să lanseze o bombă sau să trimită agenți, au lansat un vierme informatic. Foarte curat. Au numit-o operațiunea *Jocurile Olimpice* [Operation Olympic Games] (New York Times, 2012; Poroshyn, 2014). Un nume minunat pentru o operațiune

atât de curată! Tot ce le rămânea de făcut era să plaseze viermele în interior. Aveau la dispoziție destul de multe căi pentru a face asta, dar din păcate, nu le putem elabora aici pe toate. Există, totuși, una care a fost și cea mai mediatizată; pe aceasta o vom descrie în continuare.

Mai întâi a fost introdus un virus de calculator în stick-uri de memorie pentru USB. Apoi, acestea au fost plasate în jurul bazei, folosindu-se de orașele învecinate – printre care și Teheran, unde se presupunea că o parte din funcționari își petrec viața. Câțiva dintre ei au reușit să intre în posesia stick-urilor și să le insereze în calculatoarele personale – laptop-uri sau PC-uri (Khan, 2010). Era nevoie de o astfel de metodă, deoarece baza nucleară de la Natanz nu era conectată la Internet (Reuters, 2015). Înainte să judecăm greșeala, răspundeți la întrebarea: „Ce ați face voi dacă ați găsi un memory stick?". Gândiți-vă la asta data viitoare când mergeți la un eveniment și primiți de la organizatori un stick de memorie care conține diferite studii și lucrările științifice ce urmează a fi prezentate în plen. În această manieră, agenții electronici au intrat înăuntru și au făcut ceea ce toți agenții buni trebuie să facă: au început munca de recunoaștere, au început să-și facă loc în rețea, „să meargă pe coridoare" cum s-ar zice, căutându-și țintele. Iar aceste ținte erau cutii SIEMENS înțesate cu controlere pentru centrifuge. Odată găsite, a fost lansat un *rootkit* împreună cu un întreg arsenal necesar atacului digital care urma să înceapă. În acest mod, au fost alterați parametrii de lucru ai controlerelor – de fapt, ai aplicațiilor pe care le manageriau (Langner, 2013). Apoi, agenții „au sunat" acasă – în mai multe feluri, și au predat comanda asupra controlerelor Americii și Israelului, care au ordonat acelor centrifuge să se rotească la un asemenea nivel încât acestea au fost scoase din funcțiune luni întregi – fără să fie nevoie ca un agent uman să pună măcar piciorul în incinta instalațiilor iraniene (Poroshyn, 2014). Programul a fost un succes – a încetinit planurile de dezvoltare nucleară a Iranului, trimițându-le înapoi în timp cu câțiva ani (ForeignPolicy, 2013).

A apărut, totuși, o problemă. Aliații au folosit atât de mult timp pentru face acest agent electronic să intre înăuntru încât nu s-au gândit deloc la ce s-ar putea întâmpla dacă acesta iese afară. În continuare, asta s-a și întâmplat: aplicația și-a făcut treaba mai departe. A început să caute alte ținte, alte controlere SIEMENS (Shakarian et al., 2013). Mai întâi în Iran, apoi în Orientul Mijlociu pentru ca, mai apoi, să ajungă în Europa și, de aici, s-a îndreptat spre restul lumii, căutând instalații nucleare. Înainte totuși să ne agităm, trebuie menționat că acest spion își știa foarte bine sarcina. Căuta anumite controlere – cele care purtau semnătura unică a celor din Natanz (Shakarian et al., 2013). În orice caz, apărarea lui a fost distrusă. Industria de securitate, mai exact Kaspersky Lab, l-a descoperit. Ceea ce a fost odată o operațiune de preluare a controlului pentru a proteja lumea de o amenințare nucleară, a devenit *Stuxnet* – cea mai avansată amenințare software elaborată vreodată (Kaspersky Lab, 2010; Langner, 2013).

Astăzi, astfel de războaie se desfășoară în întreaga lume, poate chiar în casele noastre – evident, cu altă miză – iar noi nici măcar nu ne dăm seama. Chinezii sunt deosebit de buni la asta (NORSE, 2015). Ceea ce v-am descris mai sus e doar marketing. Nu vedem ce altceva se desfășoară. Să explicăm, deci, puțin.

În 2012, chinezii au intrat, cu succes, în sistemul de securitate al RSA (companie americană de top, specializată în dezvoltarea de soluții de criptare și securitate digitală), prin departamentul de HR (Human Resources). Ca și în cazul Stuxnet, ei au început să caute informațiile pentru care au intrat în sistem. Au găsit date confidențiale ale clienților companiei, precum parolele pe care aceștia le aveau la token-urile SecureID (RSA, 2011).

Figura 3. Diferite modele de token SecurID dezvoltate de RSA
Sursa:*http://www.emc.com/security/rsa-securid/index.htm*

Ce fac aceste token-uri? Permit accesul în rețele – precum cele ale contractorilor militari. Lockheed Martin – constructor aerospațial de prim rang, specializat în domeniul militar, al securității și al tehnologiilor avansate, L-3 Communications – companie care furnizează sisteme de comandă și control necesare aeronavelor, vapoarelor și submarinelor, și alți contractori militari au fost țintele vizate de hackeri (NBS NEWS, 2015). O parte dintre aceste companii erau clienți ai EMC Corporation – companie multinațională specializată în stocare de date, cloud computing etc. (RSA este divizia de securitate a EMC). Având în vedere, de exemplu, că Lockheed Martin produce avioane de vânătoare, ne putem imagina de ce această companie a fost o țintă bună. Documentele puse la dispoziție lumii întregi de către Edward Snowden în 2013 relevă faptul că atacurile hackerilor chinezi au avut succes (Daily News, 2015).

Totuși, pe lângă raționamentele legate de spionajul militar și industrial, mai sunt și altele, orientate spre afaceri. Operațiunea Aurora, dezvoltată tot de hackerii chinezi, a reușit să penetreze rețelele celor de la Google în ianuarie 2010 (Shakarian et al., 2013). Aceasta a avut ca ținte mai mult de 20 de companii, printre care Intel, Cisco, Adobe Systems, Yahoo, Symantec și Morgan Stanley (PCWorld, 2014). Ceea ce puțini înțeleg este că, astăzi, niciuna dintre aceste companii nu mai este imună. Chinezii au acces la nivel de CEO la informații confidențiale și documente cu și despre clienții acestora de mai bine de trei ani. Pentru cei care sunt implicați în exploatări petroliere, de exemplu – în special în concurență cu China – care nu are deloc petrol în subsolurile proprii (Roberts, 2008), fiind astfel bine motivată în acest sens – un wake-up-call ar fi Operațiunea Night Dragon – o serie de atacuri care țintesc (încă o fac, de aceea folosim timpul prezent) companii energetice din întreaga lume și care au fost descoperite de McAfee, divizia de securitate a Intel Corporation (McAfee, 2014; PCWorld, 2015).

Cercetătorii de la Kaspersky Lab, care au descoperit Stuxnet, elaborează trimestrial rapoarte privind securitatea IT în întreaga lume. Studiindu-le, putem vedea că numărul de penetrări a sistemelor din întreaga lume într-un singur an a crescut vertiginos de la 1.1 miliarde (Kaspersky Lab, 2014) – care este deja un număr foarte mare, la 2.2 miliarde (Kaspersky Lab, 2015). Ce se întâmplă? Care sunt implicațiile pentru noi toți, pe plan național sau chiar personal?

Național, putem înțelege de ce guvernele sunt atât de îngrijorate. Nu este vorba doar de spionaj, este vorba și despre infrastructura pe care acestea o pun la dispoziție cetățenilor. Dacă se poate prelua controlul unei instalații nucleare în Iran, ce-i oprește pe

hackerii iranieni să răspundă similar – ca un cyber-bumerang? Dacă cineva vrea să atace o națiune, trebuie mai întâi să închidă rețeaua de comunicare și, apoi, pe cele de infrastructură – cum ar fi sistemul bancar. Dacă la acest nivel al convergenței securității informatice vorbim de tehnologia care înlocuiește oamenii, atunci se ridică următoarele întrebări: „Cine pilotează avioanele comerciale astăzi – piloții sau aplicațiile software?", „Dacă acum 10-15 ani câțiva oameni se puteau furișa la bordul unui avion și puteau prelua conducerea acestuia, ce oprește o aplicație software să controleze un pilot-automat sau sistemul software din turnurile de control al traficului aerian?". Secretarul de stat american Leon Panetta, responsabil de problematica apărării naționale a Statelor Unite, a recunoscut public pe 11 octombrie 2012, cu ocazia întâlnirii forumului format din *Business Executives for National Security* din New York, că „the collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life" (Council of Foreign Relations, 2012). Asta ne arată că există, în viitor, o probabilitate foarte mare de a apărea un cyber atac de proporții, cu „distrugeri materiale imense și pierderi de vieți omenești".

Implicațiile la nivel personal sunt de altă natură. Există o mulțime de hackeri care pot executa operații de tip reverse-engineering a acestor instrumente, pentru a le folosi în scopuri personale. Spre exemplu, tot în 2011, peste 100 milioane de conturi ale utilizatorilor aplicațiilor Sony PlayStation au fost furate (BBC NEWS, 2014; Huffington Post, 2015). Ceea ce este interesant este faptul că aceste atacuri s-au desfășurat de-a lungul unor perioade de câteva luni, fiind, de fapt, mai multe atacuri individuale. Iar Sony nici măcar nu și-a dat seama.

Nivelul al IV-lea de convergență a securității – cel de mâine

Pe măsură ce devenim din ce în ce mai dependenți de Internet și aplicațiile acestuia, ne întrebăm ce urmează. Dacă ne gândim la acele centrifuge în Iran, cărora li s-a comandat să se rotească până ce au pierdut controlul, care sunt dispozitivele pe care ne putem baza astăzi, sub prezumția unei conectivități wireless perfect securizate?

Să ne aducem aminte de promisiunea făcută la începutul articolului. Tehnologiile de care am vorbit au fost inventate acum mai bine de un deceniu sau în decursul ultimului. Am spus că vă vom prezenta o viziune asupra spionajului cibernetic din viitor, cu tehnologii care sunt inventate astăzi. Vom păși împreună într-o gaură de vierme digitală, o gaură de vierme în care intenționăm să îi trimitem pe acei atacatori. Dacă vrem să ne apărăm în fața tehnologiei care înlocuiește omul, atunci pasul următor al convergenței este să creăm tehnologie care se comporta ca oamenii – în mediul digital nu se va putea face diferența.

Astăzi este posibilă crearea unor rețele virtuale atât de vaste și aparent reale încât nu vor putea fi diferențiate de cele care sunt efectiv reale (PaloAlto, 2015). În acest fel, când atacatorii vor dori să intre într-o organizație militară sau un departament de HR, în loc să găsească adevărata rețea, ei o vor găsi pe cea virtuală. În aceasta se vor mișca în voie – exact ca Stuxnet sau precum chinezii, căutând sisteme pe care să le infecteze. Dar în loc să le afle pe cele reale, ei le vor găsi pe cele virtuale. Sistemele „din umbră", așa cum sunt ele denumite astăzi, arată și se comportă exact ca angajații reali (Shadow Networks, 2015), verificându-și conturile de e-mail sau stând prea mult timp pe Facebook (Figura 4).

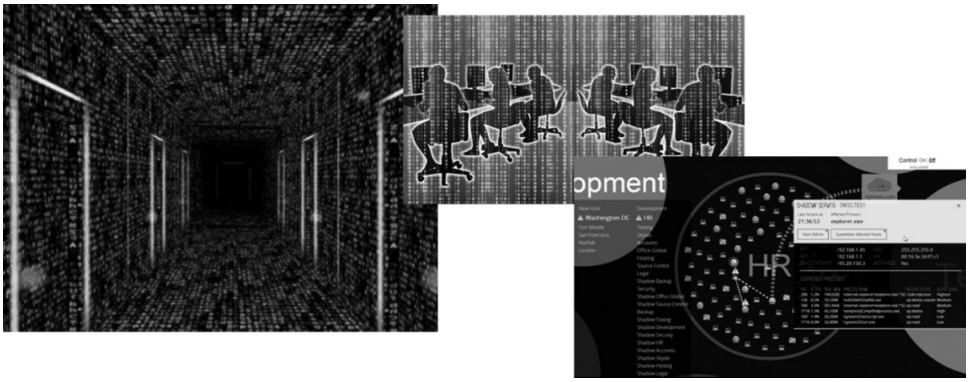

Figura 4. Reprezentarea grafică a unei rețele de tip „shadow”

Iată ce se întâmplă mai departe: dacă unul dintre acei atacatori trimite sistemului un e-mail, eventual cu attachment, și-l roagă să-l deschidă, acesta o va face necondiționat. Dacă va cere date confidențiale, sistemul i le va furniza, sperând că atacatorul „va suna” acasă. Rețelele „din umbră” vor supraveghea și vor înregistra fiecare mișcare a atacatorului.

Vom prezenta în continuare mecanismele unei astfel de rețele. Trebuie menționat, înainte de a porni în dezvoltarea ideii, că totalitatea proceselor care se desfășoară într-o astfel de rețea sunt cu mult mai bogate, complexe și complicate decât ceea ce va fi descris în rândurile următoare. Dar chiar și așa, vă veți forma o idee despre această a patra fază a convergenței de care vă vorbeam încă de la început.

O aplicație software atacă, spre exemplu, un sistem dintr-un departament de HR al unei instituții din București. Cum e posibil acest lucru? Fie un individ trimite un e-mail unui funcționar public din instituție, cu rugămintea să deschidă fișierele scanate – care pot fi o „banală” scrisoare de intenție însoțită de un CV, fie același individ, când se apropie de birou, inserează în portul USB, fără știrea funcționarului, un stick de memorie care-și va începe treaba – îl va extrage un minut mai târziu, după ce aplicația s-a instalat. Ba chiar se poate întâmpla ca individul să spună funcționarului că documentele pe care acesta le-a solicitat le are pe un memory stick și, dacă este de acord, le poate copia chiar atunci, pe loc, înmânându-i acestuia memory stick-ul intenționat infestat. Există un număr infinit de metode prin care se poate plasa o aplicație *malware* într-un sistem. Odată plasat, agentul software începe să se furișeze prin rețea, căutându-și ținta pentru care a fost creat.

Care va fi reacția rețelei „din umbră”? Ei bine, aceasta va intercepta intruder-ul, dar nu-l va elimina – dacă ar acționa astfel, ea nu ar face altceva decât să provoace ambiția hacker-ului de a-și îmbunătăți tehnica. Nu! Ceea ce aceasta va face este să devieze viermele informatic spre informații a căror valoare este bine cunoscută și care nu reprezintă un pericol în cazul în care sunt copiate, mutate sau corupte. Intenția este de a încerca să vadă cui le trimite, cu cine ia legătura, pe cine „sună”.

Bineînțeles, se poate întâmpla că rețeaua să nu intercepteze intruder-ul. Chiar și în această situație, atâta timp cât aceasta lucrează simulând procese reale – precum angajați care trimit e-mail-uri, care navighează pe Internet sau, așa cum am mai zis, stau pe Facebook – intruder-ul este păcălit. El „va suna” acasă când va găsi ceea ce caută. Acesta este trigger-ul care va declanșa sistemul de securitate. Rețeaua *shadow* nu se poate uita în calculatorul atacatorului care a dezvoltat aplicația *malware*, dar poate vedea ce procese folosește aceasta în rețeaua proprie, reușind astfel să înțeleagă ce caută și, mai presus de

orice, să vadă cu cine „vorbeşte”. Va simula procese precum cele pe care le lansează intruder-ul, îi va oferi fişiere precum cele pe care acesta le caută şi aşa mai departe. Practic, din acel moment, apărătorii sunt cei care vorbesc cu atacatorii, ei reuşind, astfel, să ofere acestora informaţii irelevante – de această dată, fără ca cei din urmă să ştie. Îi va plasa pe aceştia într-o reţea virtuală, falsă, care simulează perfect una reală, de unde intruder-ul poate lua orice doreşte pentru că apărătorii ştiu exact unde vor merge acele informaţii.

***

Am ajuns, astfel, la capătul călătoriei noastre, călătorie în care am explicat cum omul şi maşina au ajuns să lucreze împreună în domeniul securităţii digitale şi a spionajului cibernetic – convergenţa dintre aceştia. Am ajuns la confluenţa dintre două entităţi care au decis să lucreze împreună pentru a face lucrurile mai puternice. Am văzut cum tehnologia a migrat dintr-o zonă complet separată de cea a omului, la situaţia de a se comporta ca un om. Ne întrebăm ce urmează. Ei bine, dacă istoria ne este de vreun folos, atunci nu trebuie să ne întrebăm dacă, într-o bună zi, tehnologia ne va afecta profund viaţile, ci ar trebui să ne întrebăm dacă vom fi în stare să realizăm acest lucru.

Glosar

Atac cibernetic – orice formă ofensivă executată de un individ sau de o organizaţie cu scopul de a controla sau scoate din funcţiune sisteme informatice, reţele de calculatoare sau diferite device-uri personale, precum smart-phone-uri sau laptop-uri.

Centrifugă [nucleară] – dispozitiv folosit în instalaţiile nucleare pentru a izola izotopul de uraniu U-235 de restul regăsiţi, în mod natural, în acesta (deşi termenul de centrifugă are o definiţie mult mai largă, am folosit-o pe cea care explică cel mai bine sensul cu care el se regăseşte în acest articol).

Cloud computing – o formă de partajare şi sincronizare, în servere situate în diferite locaţii pe glob, a unor elemente software (diferite tipuri de fişiere, între mai multe device-uri aparţinând, de regulă, aceluiaşi proprietar/user).

Controler – un tip de computer folosit pentru automatizarea unor procese tehnologice executate de regulă de instalaţii industriale, precum: linii de asamblare, instalaţii de lumini şi, bineînţeles, centrale electrice de toate tipurile.

Convergenţă – termen împrumutat din optică, ce explică modul în care sunt adunate, într-un singur focar, razele luminoase. În contextul Tehnologiei Informaţiei, acest termen se referă la folosirea diferitor tipuri de echipamente pentru a colecta informaţia într-un singur dispozitiv. Pentru prezentul articol, termenul este folosit cu scopul explicării interacţiunii dintre om şi computere.

Criptare – metode şi tehnici folosite pentru securizarea informaţiilor şi a comunicării într-o reţea în scopul protejării.

Furt de identitate – folosirea, în mod deliberat, a unor elemente de identitate străine celui care le utilizează, cu scopul furtului de bani sau pentru obţinerea de alte avantaje.

Malware – din englezescul *mal*icious soft*ware,* care face referire la o suită de aplicaţii proiectate în mod intenţionat fie pentru a deteriora un sistem sau o reţea de calculatoare, fie pentru a se infiltra în acestea cu scopul de a se prelua conducerea lor fără consimţământul proprietarilor.

Proces – secvenţă de lucru a unei aplicaţii software care se execută într-un anumit moment dat de către un computer.

Rootkit – o colecţie de aplicaţii software cu caracter maliţios, programate pentru a oferi acces unui utilizator neautorizat aflat, de regulă, la distanţă şi care îşi maschează existenţa în spatele unor aplicaţii legitime. Termenul este obţinut prin concatenarea cuvântului *root* – administratorul unui sistem Unix, şi *kit* – componente software care ajută la instalarea aplicaţiei.

Token – un dispozitiv electronic care generează un cod unic, temporar, folosit pentru a accesa o reţea de calculatoare aflată, de regulă, sub condiţii de utilizare foarte stricte, precum accesul la un serviciu de Internet banking.

Troian – termen derivat din legenda Calului Troian şi care are scopul de a introduce, într-un sistem,

aplicații software cu caracter malițios (viruși, viermi informatici, aplicații spion etc.).

Vierme informatic – aplicație software care are implementate instrucțiuni de autoreproducere în scopul infestării și altor sisteme. Acesta se propagă, de regulă, prin intermediul rețelelor de calculatoare.

Virus informatic – similar viermilor informatici, și virușii au capacitatea de a se autoreproduce, dar spre deosebire de primii, aceștia sunt atașați fișierelor care, odată deschise sau executate, lansează în execuție și virusul.

Wireless (en. „fără fir") – rețele de dispozitive conectate între ele prin unde radio, infraroșu sau alte metode care nu implică existența cablurilor.

Bibliografie

BBC NEWS (2014), *Sony's PlayStation hit by hack attack*, http://www.bbc.com/news/technology-30373686

Cisco (2015), *Midyear Security Report*, http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html

CNET (2002), *Melissa virus spreads în Internet time*, http://www.cnet.com/news/melissa-virus-spreads-in-internet-time/

Council of Foreign Relations (2012), Secretary of Defense Leon Panetta discusses the global threat of cybersecurity attacks at the Business Executives for National Security în New York City, October 11, 2012.

CTV News (2007), *Prank starts 25 years of computer security woes*, http://www.ctvnews.ca/prank-starts-25-years-of-computer-security-woes-1.254640

Cybersecurity Ventures (2015), *Cybersecurity Market Report*, http://cybersecurityventures. com/cybersecurity-market-report/

Daily News (2015), *Chinese hackers stole F-35 fighter jet blueprints în Pentagon hack*, http://www.nydailynews. com/news/national/snowden-chinese-hackers-stole-f-35-fighter-jet-blueprints-article-1.2084888

Foreign Policy Research Institute (2010), *The Military's Role în Stimulating Science and Technology: The Turning Point*, http://www.fpri.org/articles/2010/05/militarys-role-stimulating-science-and-technology-turning-point

Foreignpolicy (2013), *The real program to sabotage Iran's nuclear facilities was far more sophisticated than anyone realized*, http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

F-Secure (2015), *Threat description, virus: W32/Melissa*, https://www.f-secure.com/v-descs/melissa.shtml

Gartner (2015), *Forecast Alert: IT Spending, Worldwide, 3Q15 Update*, https://www.gartner.com/doc/3142129

Greene, T.C. (2004), *Computer Security for the Home and Small Office*, Chapter 7 – Trust Nothing, Fear Nothing, Apress, ISBN 1-59059-316-2, pp. 219-279.

Huffington Post (2015), *Sony Playstation Hack,*http://www.huffingtonpost.com/news/sony-playstation-hack/

Kaspersky Lab (2010), *Stuxnet Worm: Insight from Kaspersky Lab. Experts believe that Stuxnet manifests the beginning of the new age of cyber-warfare*, http://www.kaspersky.com/about/news/virus/2010/Stuxnet_Worm_Insight_from_Kaspersky_Lab

Kaspersky Lab (2014), *IT Threat Evolution Q1 2014*, https://securelist.com/files/2014/07/q1-it-threats-en.pdf

Kaspersky Lab (2015), *IT Threat Evolution în Q1 2015*, https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/

Kearns, I. (2002), Code Red: Progressive Politics în the Digital Age, Chapter About Digital Society, EMPHASIS, ISBN 1-86030-188-6, pp. 1-5.

Khan, S. (2010), Iran and Nuclear Weapons: Protracted Conflict and Proliferation. Part II and III, Proliferation activity and hostile US policy since 2000 – Case study: Iran, Routledge, ISBN 0-203-86942-7, pp. 25-110.

Langner, R. (2013) To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve, The Langner Group, Arlington, Hamburg, Munich.

Barry, L.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G., Wolff, S, *Brief History of the Internet*, http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf

LiveScience (2015), *History of Computers: A Brief Timeline*, http://www.livescience.com/20718-computer-history.html

McAfee (2014), *Night Dragon – Overview*, http://www.mcafee.com/sg/about/night-dragon.aspx
Microsoft (2013), *Security Intelligence Report*, http://www.microsoft.com/security/sir/default.aspx
NBS NEWS (2015), *Secret NSA Map Shows China Cyber Attacks on U.S. Targets,* http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211
New York Times (2012), *Obama Order Sped Up Wave of Cyberattacks Against Iran*, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=1
Norse corporation (2015), http://www.norse-corp.com/
PaloAlto Networks (2015), *Getting started with Next-Generation Firewall*, http://connect.paloaltonetworks.com/ngfw-ondemand-demo-2
PCWorld (2014), *Security vendors claim progress against Chinese group that hacked Google,* http://www.pcworld.com/article/2833992/security-vendors-claim-progress-against-chinese-group-that-hacked-google.html
PCWorld (2015), 'Night Dragon' Attacks From China Strike Energy Companies, *http://www.pcworld.com/article/219251/article.html*
Poroshyn, R. (2014), *Stuxnet: The True Story of Hunt and Evolution*, Createspace Independent Pub., ISBN 1499709226.
Reuters (2015), *U.S. tried Stuxnet-style campaign against North Korea but failed*, http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529#xFvTEjwuodtsPqyC.97
Roberts, P. (2008), *Sfarsitul petrolului. În pragul unui dezastru*, Ed. Litera, ISBN 978-973-67-5435-7.
RSA (2011), *Anatomy of an Attack,* http://blogs.rsa.com/anatomy-of-an-attack/
SANS Institute (2001) (1), *Code Red: The One to Not "Dew"*, SANS Institute InfoSec Reading Room,https://www.sans.org/reading-room/whitepapers/malicious/code-red-dew-66
SANS Institute (2001) (2), *The Mechanisms and Effects of the Code Red Worm,* SANS Institute InfoSec Reading Room, https://www.sans.org/reading-room/whitepapers/malicious/mechanisms-effects-code-red-worm-87
Shadow Networks (2015), *Advanced Threat Deception*, http://www.shadownetworks.com/wp-content/uploads/Shadow-Networks_Bro_Final.pdf
Shakarian, P., Shakarian, J., Ruef, A. (2013), *Introduction to Cyber-Warfare: A Multidisciplinary Approach,* Capitolul 13:Attacking Iranian Nuclear Facilities: Stuxnet*,* Elsevier 2013, pp. 224-240.
Symantec (2010),*A History of Viruses,*http://www.symantec.com/connect/articles/history-viruses
Symantec (2002), http://www.symantec.com/security_response/writeup.jsp?docid=2000-121815-2258-99
Symantec (2015) (1), *Regin: Top-tier espionage tool enables stealthy surveillance*, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf
Symantec (2015) (2), *Internet Security Threat Report*,Volume 20, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf
Zetter, K. (2014), Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Crown Publishers, ISBN 978-0-7704-3617-9.