CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Zlonamjerni programi u službi država

NCERT-PUBDOC-2012-10-338

Nacionalni CERT

Sadržaj

1 Uvod

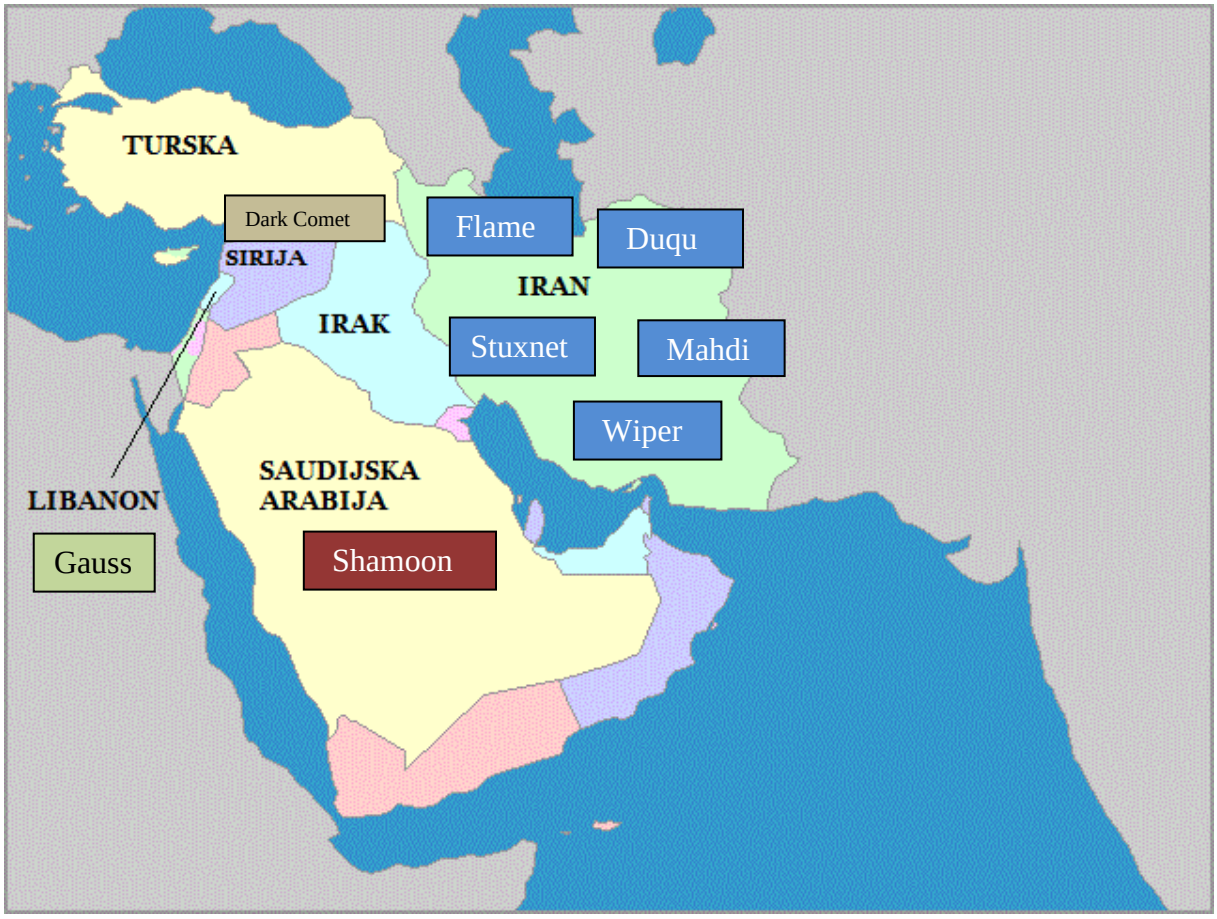
Tijekom 2007. i 2008. korisnici Interneta iz Rusije izveli su napade uskraćivanjem usluge (DoS) na estonske i gruzijske poslovne i državne informacijske sustave. Bio je to prvi slučaj napada na infrastrukturu jedne cijele države te je podigao veliku medijsku prašinu.

Računalni crv Stuxnet je otkriven 2010., a namjena mu je bila remećenje rada elektromotora centrifuga za obogaćivanje urana u Iranu. Taj zlonamjerni program je prvi potegao pitanje zaštite kritične infrastrukture. Kasnije je otkriven cijeli niz špijunskih (i ostalih zlonamjernih) programa od koji su neki povezani sa Stuxnetom, dok su drugi korišteni u drugim zemljama i to u drugačiju svrhu. Tako su primjerice u Siriji korišteni programi za špijunažu oporbe i političkih aktivista. Ovaj dokument daje pregled zlonamjernih programa i njihovih glavnih tehničkih karakteristika, meta, vjerojatnih autora te načina na koji su korišteni.

Stručnjaci se slažu kako je potrebno preispitati pojam „cyber“ rata u kontekstu zaštite informacijskih sustava kritične infrastrukture. Ima li taj pojam uopće smisla ili je preuveličan? Koja je razlika između „cyber rata“ i „cyber“ špijunaže? Je li današnja politika sigurnosti informacijsko-komunikacijskih sustava unutar energetskih i drugih primarnih sustava neke zemlje zadovoljavajuća? Koju ulogu treba država preuzeti i mijenja li se ona? Postoji li opasnost da će kriminalne skupine iskoristiti dostupnost sofisticiranih zlonamjernih programa u svoje svrhe? Koja je uloga komercijalnog sektora proizvođača sigurnosnih rješenja? Da bi mogli dati odgovore na sva ova pitanja, potrebno je dobro razumjeti današnji kontekst informacijske sigurnosti, u čemu će ovaj dokument nastojati pomoći.

2 Pregled zlonamjernih programa prema metama

Pregled zlonamjernih programa započinje sa **Stuxnetom**, **Duquom** i **Flameom**. Izgledno je kako je meta sva tri programa bio Iran. Stuxnet [1], koji je odmah nakon otkrića u lipnju 2010. bio prozvan prvim „cyber" oružjem, ciljao je iranske nuklearne elektrane. Čini se kako je u tome Stuxnet bio vrlo uspješan. Duqu i Flame nisu imali zadatak nanositi štetu, nego špijunirati. Što se Flamea tiče, stručnjaci za računalnu sigurnost navode kako je to najsloženiji zlonamjerni program dosad. Njegova tehnička izvedba ocijenjena je čak 20 puta kompleksnija nego Stuxnetova. Impresivno, s obzirom da je Stuxnet u trenutku otkrića ocijenjen sličnim epitetima uz procjenu da je samo za izradu njegovog programskog koda potrebno 10 čovjek-godina. Zlonamjerni programi **Mahdi** i **Wiper** su također pogodili većinom računala u Iranu. Mahdi je ima ulogu špijunaže, za razliku od Wipera čija je zadaća bila čišćenje tvrdih diskova i uklanjanje tragova kojeg su ostavljali Stuxnet i Duqu.



Slika 2.1: zlonamjerni programi po napadnutim državama

Špijunski program **„Gauss"** je većinom zarazio računala u Libanonu. Nagađa se kako su SAD i Izrael putem tog programa pratili bankovne transakcije organizacije „Hezbollah". Utvrđeno je kako je razvijen na istoj platformi kao i Flame. **„Shammon"** je špijunsko-destruktivni program koji je pogodio „Saudi Aramco", naftnu tvrtku iz Saudijske Arabije. Čini se kako je taj zlonamjerni program odgovor Irana na „cyber" oružja i naftni embargo.

Preostala tri špijunska programa su primjeri u kojima države koriste softver, odnosno računalne napade za nadzor svojih građana. U slučaju Sirije i Tibeta (odnosno Kine), špijunirani su aktivisti (oporba i pobunjenici), dok su njemačke državne agencije (i policija) koristile špijunski program u istragama kriminalnih slučajeva. Budući da je izvedba tog softvera u suprotnosti s njemačkim ustavom, to je izazvalo veliku osudu u javnosti.

Slika 2.2: kronologija događaja vezanih uz zlonamjerne programe

2.1 Iran

2.1.1 Stuxnet

Stuxnetove glavne mete bili su sustavi za kontrolu rada koji koriste upravljačke sklopove utemeljene na PLC-u (engl. *Programmable Logic Controller*). Takvi sklopovi se unutar elektrana i sličnih velikih industrijskih postrojenja, nalaze unutar **SCADA** („Supervisory Control and Data Acquisition“) računalnih sustava za nadzor i upravljanje. Konkretno su ciljani PLC uređaji tvrtke Siemens (modeli „Simatic“), s takvim postavkama koje se koriste isključivo u iranskim nuklearnim elektranama. Stoga je jedna od glavnih komponenti koje je crv koristio prvi PLC **„rootkit“** u povijesti, program koji prikriva svoje aktivnosti (izmjene koda) unutar samog PLC-a. Pristup podacima koje je koristio PLC, crvu je omogućio sigurnosni propust u Siemensovom softveru za upravljanje PLC-om („WinCC“), instaliranom na računalima koja su izravno spojena na PLC-e. Naime, korisnička imena i lozinke za pristup bazi podataka bila su ručno upisana u programskom kodu i crv ih je jednostavno pročitao. Stuxnet je za svoje uspješno širenje i stjecanje potrebnih privilegija na operacijskim sustavima Windows iskoristio ukupno pet ranjivosti (od toga su čak četiri tzv. „**zero-day**“ ranjivosti, odnosno dotad nisu bile javno poznate!) različitih inačica Windowsa. Najpoznatija od njih je ranjivost LNK ikona koja se iskorištavala za širenje putem USB memorijskih „stickova“. Uz USB „stickove“, crv se širio i putem lokalne mreže, a imao je i mogućnost dobivanja nadogradnji putem komandnih poslužitelja preko Interneta. Crv je za preuzimanje kontrole nad računalima koje je zarazio koristio i dva ukradena certifikata poznatih računalnih tvrtki s Tajvana. Statistička raspodjela zaraženih računala pokazala je kako se više od polovice zaraženih računala nalazilo u Iranu. Nagađa se kako iza napada stoje SAD i Izrael.

Slika 2.3: računalo spojeno na Siemensov PLC - meta Stuxneta

2.1.2 Duqu

Duqu je zlonamjerni program koji usko povezan sa Stuxnetom. Ime je dobio po tome što izrađuje datoteke s nastavkom „~DQ“. Poznati proizvođač sigurnosnih rješenja Symantec je Duqu nazvao „gotovo potpuno identičnim Stuxnetom, ali s drugačijom svrhom“. Duqu je naime dizajniran kako bi potajno prikupljao povjerljive informacije, odnosno špijunirao mete koje sadrže informacije o nuklearnom programu u Iranu. Za razliku od Stuxneta, nije se bavio PLC sustavima. Ono što mu je zajedničko sa Stuxnetom je korištenje iste programske platforme koju su stručnjaci nazvali „Tilded“. Uz to, kao i Stuxnet koristi ukradeni digitalni certifikat te iskorištava „zero-day“ ranjivost jezgre Windowsa. Ranjivost koju Duqu koristi je vezana uz sustav za obradu „Win32 True Type“ fonta, a iskorištava se putem zlonamjernog Word dokumenta. Upravo su Word dokumenti korišteni u **ciljanom napadu** [2] putem elektroničke pošte preko kojeg se crv proširio. Duqu se sastoji od „**keylogger**“ programa koji snima pritisnute tipke i prikuplja sve sistemske informacije koje mogu imati veze sa sustavima za kontrolu određenih industrijskih postrojenja. Prikupljene podatke, crv sprema u kriptiranu JPEG datoteku (sliku), a stručnjacima nije poznato koje točno informacije prikuplja. Nagađa se kako su prikupljeni podaci mogli poslužiti Stuxnetu za daljnji tijek operacije.

Slika 2.4: lokacije kontrolnih poslužitelja koje je koristio Duqu i žrtvi koje su se spajale na njih [izvor: Securelist]

Stručnjaci su analizirali nekoliko kontrolnih poslužitelja koje je Duqu koristio (slika gore). Nalazili su se u Njemačkoj, Belgiji, Vijetnamu i Kini [3]. Analiza je pokazala kako su se poslužitelji koristili najranije od studenog 2009. te da su kompromitirani putem „brute-force“ napada na „root“ lozinku. Također, 20. listopada 2011. su napadači obrisali gotovo svaki trag o korištenju poslužitelja, tako da zapravo nije izvučena nijedna bitna informacija o operaciji. Crv je od kontrolnih poslužitelja vjerojatno dobivao naredbe za širenje putem lokalne mreže.

2.1.3 Flame

Flame (poznat i kao Skywiper) je otkriven u svibnju 2012., dakle nakon Stuxneta i Duqua. Kao i u slučaju ostala dva zlonamjerna programa, većina zaraženih računala se nalazila u Iranu. Namjena mu je, kao i Duquu, špijunaža. No, Flame je najsofisticiraniji od svih te je vjerojatno najduže ostao neotkriven. Flame je, što je vrlo neobično za zlonamjerne programe, veličine čak 20 megabajta. S obzirom na svoju specifičnu tehničku izvedbu, stručnjaci se slažu kako je riječ o najsloženijem zlonamjernom programu dosad. Tvrtka Kaspersky tvrdi kako je za njegovu cjelovitu analizu potrebno čak deset godina. Kasnija analiza od strane Kasperskog, Symanteca i organizacija IMPACT te CERT Bund-a je pokazala kako je Flame razvijan od strane najmanje četvero razvojnih programera najkasnije od prosinca 2006 [8].

Lista njegovih mogućnosti je impresivna. Širi se putem USB memorijskih „stickova" i putem lokalne mreže. Može snimati audio zapise, raditi „screenshot" slike, bilježiti pritisnute tipke i snimati mrežni promet. Što se tiče audio zapisa, može snimati Skype razgovore, a zanimljivo sadrži i Bluetooth modul putem kojeg može bežično preuzimati sadržaj s okolnih uređaja (mobitela i sl.). Flame koristi čak 5 različitih metoda za kriptiranje. Prikupljene podatke, program naravno šalje svojim kontrolnim poslužiteljima, od kojih i prima naredbe. Jedna od takvih naredbi je „kill" koja briše sve tragove zlonamjernog programa sa zaraženog računala. Napadači su pokrenuli upravu tu naredbu nakon što je otkriće Flamea javno objavljeno. Za inficiranje računala, Flame koristi dvije iste ranjivosti kao i Stuxnet. Tehnički, najzanimljivije je da je Flame koristio **krivotvoreni** Microsoftov **digitalni certifikat** kako bi „glumio" posredničkog („proxy") poslužitelja zaduženog za instalaciju nadogradnji putem sustava „Windows Update". Te nadogradnje nisu bile ništa drugo nego zlonamjerni kod i zapravo način na koji se Flame dalje širio unutar interne mreže neke organizacije. Krivotvoreni certifikat je dobiven izrazito složenom tehnikom kolizicije MD5 sažetaka [4], odnosno izvršen je napad na ranjivi kriptografski algoritam MD5. Prema procjenama, samo za uspješnu primjenu te tehnike potrebno je korištenje superračunala, odnosno računalne opreme u vrijednosti od 200 tisuća američkih dolara. Što je još impresivnije, kako bi postupak uspio, unutar samog procesa izrade krivotvorenog certifikata (metodom kolizije sažetaka) bilo je potrebno da certifikat bude izrađen u točnoj određenoj milisekundi. Razlog leži u tome što se serijski broj certifikata temelji na točnom vremenu u trenutku izrade, stoga su napadači to vrijeme trebali pogoditi „unaprijed" [4]. Tvrtka Kaspersky je demonstrirala kako je Flame najviše tražio AutoCAD nacrte, PDF i ostale tekstualne dokumente.

Analiza dvaju kontrolnih poslužitelja koje su upravljali Flameom [8] pokazala je da su naredbe za upravljanje nisu slane izravno nego unutar tar.gz datoteka koje bi zlonamjerni program obradio lokalno. Jedan od kontrolnih poslužitelja je služio za prikupljanje podataka, dok je drugi služio za davanje naredbi. Web sučelje tog drugog kontrolnog poslužitelja izgledalo je kako je prikazano na sljedećoj slici:

Slika 2.5: Web sučelje kontrolnog poslužitelja za Flame

Analiza protokola za upravljanje je otkrila kako osim Flamea postoje još tri inačice zlonamjernih programa kojima se upravljalo putem tog kontrolnog poslužitelja. Korišteni su kodovi FL, SP, SPE i IP za razlikovanje klijenata, a FL se odnosilo na Flame.

2.1.4 Mahdi

Mahdi (nazvan prema datotekama koje referiraju muslimanskog mesiju) je još jedan od špijunskih programa koji su pogodili računala u Iranu. Osim Irana, pogođeni su i Izrael, Afganistan, Ujedinjeni Arapski Emirati i Saudijska Arabija. Međutim, većina se ipak nalazila u Iranu. Symantec je naveo kako su žrtve bile organizacije povezane s kritičnom infrastrukturom, veleposlanstva i banke. Zlonamjerni program je snimao pritisnute tipke, uzimao „screenshotove" s računala, špijunirao audio razgovore te presnimavao tekstualne datoteke, kao i slike. Stručnjaci ne mogu sa sigurnošću utvrditi je li neka država stoji iza napada ovim zlonamjernim programom. Napad je izvršen putem zaraženih privitaka u porukama elektroničke pošte u tipičnoj kombinaciji sa socijalnim inženjeringom. Točnije, bilo je riječ o Word dokumentu s naslovom „Israel's Secret Iran Attack Plan: Electronic Warfare" („Izraelski tajni plan napada na Iran": Elektroničko ratovanje") i zlonamjernoj PowerPoint prezentaciji. Otkriveno je pet kontrolnih poslužitelja Mahdija, smještenih u Kanadi. Stručnjaci su nakon javnog objavljivanja informacija o Mahdiju, otkrili kako su napadači u nekoliko navrata vršili nadogradnju programa, kako bi izbjegao detekciju antivirusnim alatima. Neke od meta novih inačica špijunskog programa nalazile su se u SAD-u i Njemačkoj. Vjeruje se kako je riječ o tvrtkama povezanim s Bliskim Istokom.

2.1.5 Wiper

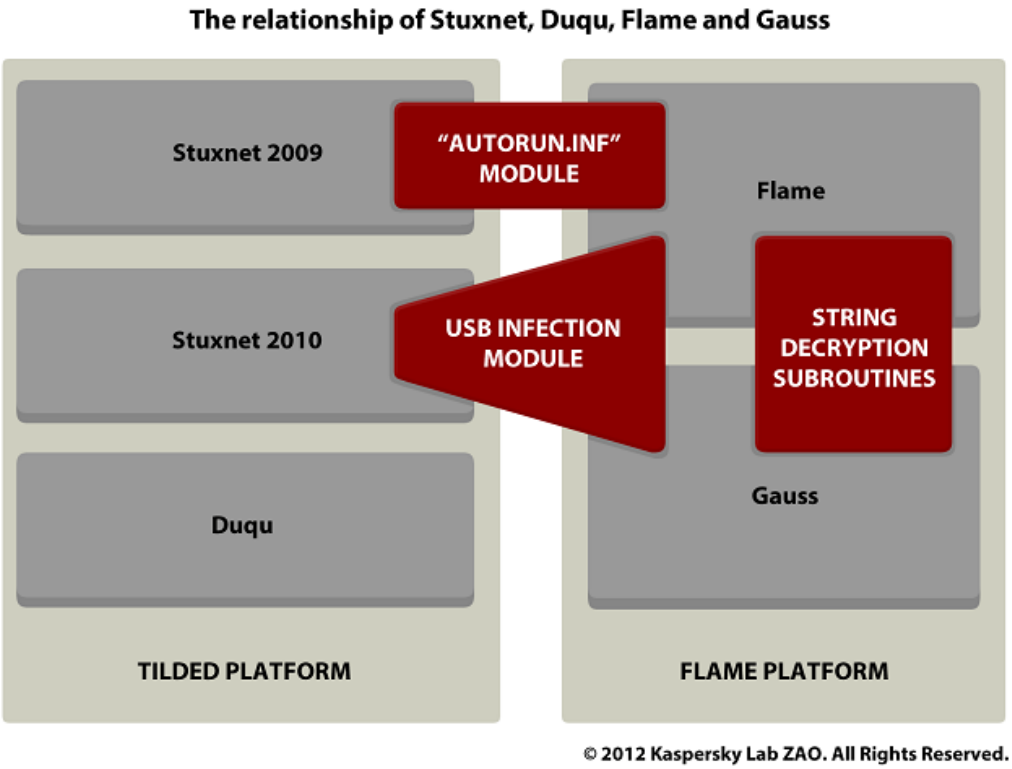
U travnju 2012., u javnost su izašle informacije kako se pojavio misteriozni virus koji gasi računalne sustave u Iranu. Nekoliko članaka je spomenulo zlonamjerni program, nazvan „**Wiper"**. No, nikakvi uzorci programskog koda nisu bili dostupni, pa su mnogi sumnjali u

točnost tih informacija. Internacionalna telekomunikacijska unija (ITU) i tvrtka Kaspersky su krenule u istragu koja je kasnije dovela do otkrića zlonamjernih programa Flamea i Gaussa. Također je potvrđeno kako je Wiper kao zasebni zlonamjerni program zaista postojao.
Wiper je, za razliku od ostalih navedenih zlonamjernih programa koji su pogodili Iran, imao zadaću potpuno brisanje sadržaja tvrdih diskova zaraženih računala. Prioritet za brisanje imale su datoteke s .pnf nastavkom, upravo one koje koriste Stuxnet i Duqu. Stručnjaci nisu uspjeli doći do primjerka programa kako bi ga analizirali jer je izrađen tako da uklanja i tragove koje ostavlja iza sebe. Wiper je toliko kvalitetno izrađen da je u potpunosti očistio podatke („wipe“) s tvrdih diskova. Međutim, stručnjaci su analizirali (preostali) sadržaj kopija tvrdih diskova te otkrili imena određenih obrisanih datoteka kojima su kasnije došli do otkrića Flamea i Gaussa. Također je otkrivena datoteka s nastavkom .tip koja sadrži iste bajtove kao datoteke kod Stuxneta i Duqua. To može biti indikator da je riječ o datoteci iz programske platforme „Tilded“, na kojoj se temelje Stuxnet i Duqu. Međutim, nije logično da Wiper dijeli i iste autore. Teško je vjerovati da bi ugrozili skupe operacije samo kako bi očistili tvrde diskove. Obzirom na spomenute sličnosti u programskom kodu, to se ipak ne može isključiti, istaknuli su iz tvrtke Kaspersky[5].

2.2 Libanon

U lipnju 2012. istraživači za računalnu sigurnost, otkrili su zlonamjerni program koji je služio za krađu lozinki iz web preglednika, korisničkih računa (bankovnih i onih namijenjenih društvenim mrežama), „cookie“ i konfiguracijskih datoteka. Zlonamjerni program je nazvan „**Gauss**“, prema svojem glavnom modulu (svi moduli programa nazvani su prema poznatim matematičarima). Kaspersky, tvrtka koja stoji iza otkrića Gaussa, je utvrdila kako dolazi od istih autora kao Stuxnet, Duqu i Flame. Štoviše, čini se kako je izrađen na istoj platformi kao i Flame. Međutim, za razliku od tih zlonamjernih programa, Gauss je većinom zarazio računala u Libanonu. Sumnja se kako je namjena programa praćenje financijskih transakcija u Libanonu. Otkriveno je kako specifično krade korisničke podatke od svih većih libanonskih banaka. Nagađa se kako su SAD i Izrael putem Gaussa pratili bankovne transakcije iz razloga što su otkrili kako libanonske banke služe Hezbollahu za pranje novca [6]. Hezbollah je islamska militantna i politička skupina koju SAD i Izrael smatraju terorističkom.

Tehnički gledano, najzanimljiviji dio Gaussa je njegov modul za zarazu putem USB-a čija je izvršna datoteka kriptirana i do pisanja ovog dokumenta nije odgonetnuto što ta komponenta točno radi. Tvrtka Kaspersky je pozvala stručnjake za kriptoanalizu kako bi pomogli dešifrirati sadržaj datoteke, no stručnjacima to zasad ne polazi za rukom jer se kriptografski ključ generira (i komponenta aktivira) prilikom priključivanja USB memorije na računalo sa specifičnom (nepoznatom) konfiguracijom. Dakle, ključ ovisi o računalu na koje se USB memorija priključuje. Stručnjacima još nije poznata točna metoda širenja zlonamjernog programa, osim putem USB memorija. Što se tiče ranjivosti, Gauss koristi istu LNK ranjivost kod širenja USB medijima, kao i Stuxnet, no na nešto napredniji način. Nepoznato je koristi li neku „zero-day“ ranjivost. Gaussom je upravljalo pet kontrolnih poslužitelja, a zanimljivo je da je korištena redundantna DNS arhitektura („round robin“), što može upućivati na to da je program obrađivao i slao veliku količinu podataka. Kontrolni poslužitelji su srušeni prije nego što su stručnjaci stigli analizirati koje je točno podatke Gauss otimao sa zaraženih računala.



Slika 2.6: Zlonamjerni programi prema platformama

2.3 Saudijska Arabija

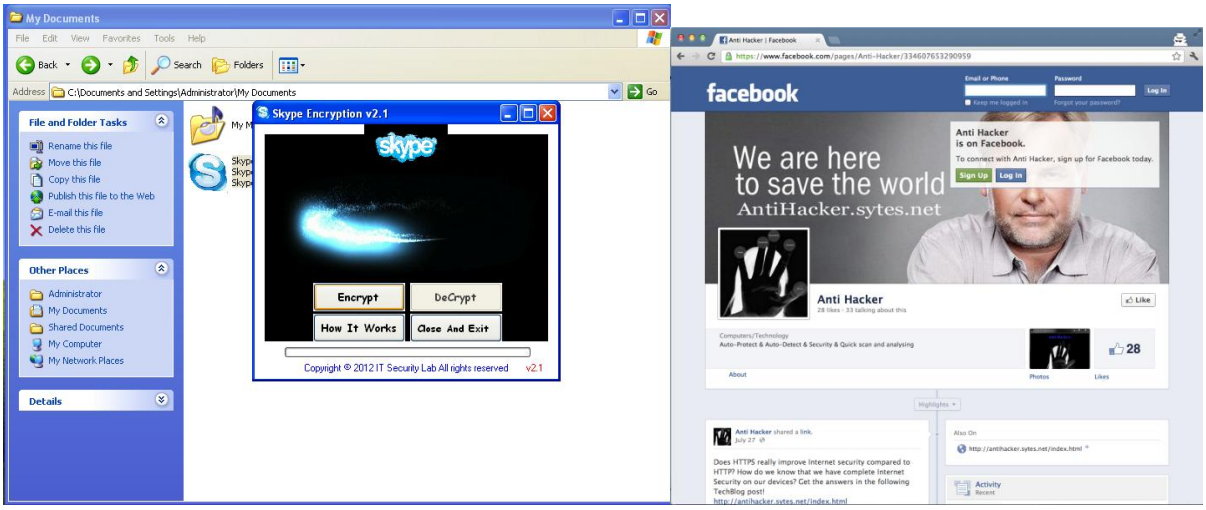
U kolovozu 2012. je otkriveno kako je „Saudi Aramco", naftna tvrtka iz Saudijske Arabije žrtva napada dotad nepoznatim zlonamjernim programom. Program je otkriven nakon što je u navedenoj tvrtki uočen veliki broj onesposobljenih računala kojima su tvrdi diskovi očišćeni (program je brisao tzv. „master boot record" zapise na tvrdim diskovima). Zlonamjerni program je nazvan „Shamoon", a pokazalo se kako je zarazio čak 30 tisuća računala tvrtke „Saudi Aramco". Napadnute su sve inačice operativnog sustava Windows (od inačice 95 nadalje). Analiza je pokazala kako se zlonamjerni program, nakon što zarazi računalo, javlja svojem kontrolnom poslužitelju, a nakon toga otima povjerljive podatke iz različitih predefiniranih Windows direktorija. Uz to se pokušava proširiti internom mrežom, a na kraju izvršava programski kod koji čisti tvrde diskove. Shamoon sadrži i 900 kB kriptiranih programskih modula, a za pristup tvrdom disku koristi digitalni potpis tvrtke „EldoS". Stručnjaci ističu kako nije uobičajeno da zlonamjerni programi korišteni u ovakvim napadima imaju destruktivan karakter, kao što je to slučaj kod Shamoona.

Jeffrey Carr [9] je istaknuo kako Iran vrlo vjerojatno stoji iza ovog napada. Navodno je Iran povezan s Hezbolahom (kojeg financira) koji u svojim redovima navodno ima hakerske grupe koje bi mogle stajati iza ovog napada. S obzirom da je upravo Hezbolah bio vjerojatna žrtva napada Wiperom, moguće je kako je Shamoon ustvari kopija Wipera, dobivena metodom reverznog inženjeringa. No, valja istaknuti kako je Shamoon izrađen manje profesionalno od Wipera jer su pronađene određene greške i nelogičnosti u programskom kodu [10]. Postoji i drugi motiv upotrebe ovog zlonamjernog programa, a to

je spor Irana i Saudijske Arabije u vezi embarga na uvoz nafte iz Irana koji je stupio na snagu 1. srpnja 2012. (nametnut od strane EU i SAD-a). Razlog je sumnja da Iran razvija nuklearno oružje i činjenica da nije spreman za prave pregovore, kako je istaknuo saudijski ministar vanjskih poslova [11]. Iran je pogođen činjenicom da su neki od kupaca nadomjestili iransku naftu onom iz Saudijske Arabije, odnosno Saudi Aramca. Iako je nekoliko hakerskih, odnosno haktivističkih skupina preuzelo odgovornost za napad, analitičar za računalnu sigurnost Jeffrey Carr je istaknuo kako se čini kako Iran stoji iza napada, namjerno urađenog da izgleda kao haktivistički. Određen broj zaposlenika Saudi Aramca je navodno pod istragom u vezi sudjelovanja u napadu [12]. Sumnja se kako je netko s potrebnim znanjem o internim sustavima i dovoljnim ovlastima, pomogao u napadu zlonamjernim programom. Zanimljivo je kako Saudi Aramco proizvodi čak desetinu svjetske nafte.

2.4 Sirija

U veljači 2012., poznati proizvođač sigurnosnih rješenja TrendMicro, je otkrio kako je sirijski režim koristio zlonamjerni program „**Dark Comet**“ za špijunažu nad protivnicima režima [13]. Riječ je o tzv. „remote access trojan“ (**RAT**) programu koji služi za udaljeno nadgledanje i upravljanje zaraženih računalom. Program je inače javno poznat i može se nabaviti na Internetu od 2008 te je korišten u mnogim napadima kriminalnih skupina. Trojanski konj je zlonamjerni program koji dolazi skriven zajedno s nekim drugim programom. U ovom slučaju bilo je riječ o nekoliko lažnih programa. Tijekom prvih zabilježenih napada u studenom 2011. [14] to je bio lažni alat za kriptiranje Skype razgovora, „Skype Encryption“ (prikazan na slici dolje), kasnije je korišten „AntiHacker“ koji je u predstavljen kao program namijenjen zaštiti od virusa i hakera [15]. Neki primjeri širili su se i pod lažnim nazivom „MAC Address Changer“ i sirijskim aktivistima su predstavljani kao programi koji omogućuju anonimnost na Internetu.



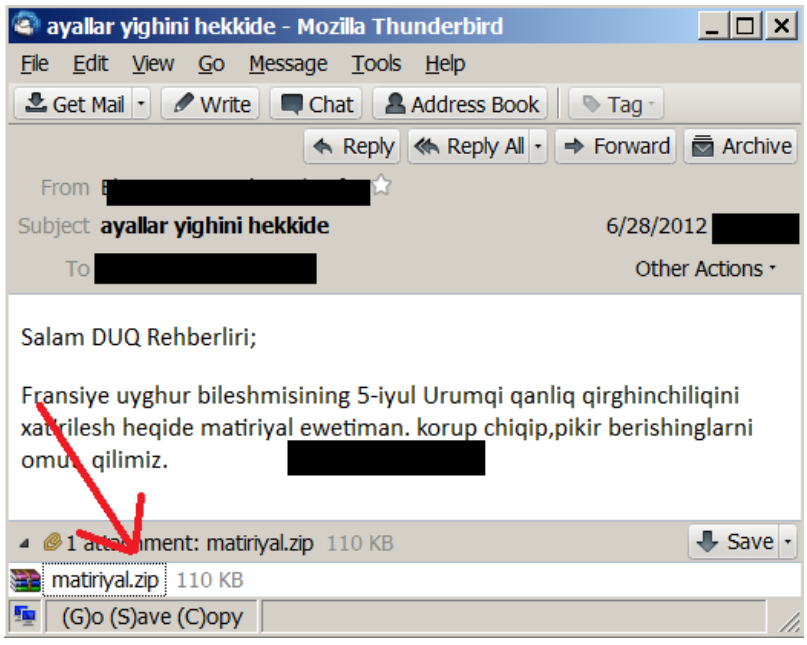
Slika 2.7: trojanski konj u obliku lažnog alata za Skype (lijevo); lažna Facebook grupa (desno)

Zlonamjerni program se širio i putem Skype chat poruka i putem Facebooka (Facebook grupa prikazana je na slici gore). Dark Comet napadačima nudi klasične mogućnosti - uvid

u pritisnute tipke („keylogger“ funkcionalnost), nadzor web kamere, isključivanje antivirusnih programa, krađu povjerljivih podataka, brisanje podataka itd. Nakon instalacije na računalo, zlonamjerni program se spajao na IP adresu koja pripada Sirijskom telekomu. Zanimljivo je kako je autor programa „Dark Comet“, poznat jedino pod nadimkom „DarkCoderSC“ izrazio žaljenje zbog toga što njegov program koristi sirijski režim te je izjavio kako će svejedno nastaviti razvijati program, ali i izdati poseban program za otkrivanje DarkCometa, posebno za sirijske korisnike Interneta.

2.5 Tibet (Kina)

Tvrtka AlienVault je u ožujku 2012. objavila otkriće o napadu na više tibetanskih aktivističkih organizacija. Tvrtka sumnja kako je napad izvršila ista kineska skupina koja se krije iza tzv. „Nitro“ napada koji je 2011. ciljao američke tvrtke koje se bave kemijskom proizvodnjom, uključujući proizvode koje se koriste u vojnim vozilima. Napad se izvodio putem elektroničke pošte i ciljanog „**phishinga**“. U privitcima poruka elektroničke pošte nalazili su se zlonamjerni Office dokumenti koji su koristili od ranije poznatu ranjivost (CVE-2010-3333). Poruke su primatelje pozivale na tibetanski religiozni obred. Analiza je pokazala da je ustvari bilo riječ o zlonamjernom programu „**Gh0st RAT**“ koji spada u istu skupinu kao i program koji je korišten u napadu na sirijsku oporbu. Također ima i sličan skup mogućnosti kao što su krađa dokumenata, špijuniranje putem web kamere, ali i mogućnost prisluškivanja putem mikrofona. Zlonamjerni dokument je koristio klasičnu metodu obfuskacije programskog koda koristeći 256-bitni XOR ključ. Time se izbjegavalo otkrivanje antivirusnim programima ili IDS uređajima. Program je također bio i digitalno potpisan radi dodatne uvjerljivosti. Koristio je tri komandna poslužitelja koji su svi smješteni u Kini.



Slika 2.8: poruka elektroničke pošte sa zlonamjernim privitkom

U lipnju 2012. Kaspersky je otkrio novu varijantu zlonamjernog programa koja se koristila protiv tibetanskih aktivista. Taj zlonamjerni program je ciljao isključivo Appleov operativni

sustav **Mac OS X** [16]. Napad je izveden putem elektroničke pošte, koristeći lažne političke poruke sa zlonamjernim privitkom u kojem se nalazila datoteka „matiriyal.zip“ (slika 2.8). Navedena datoteka je sadržavala sliku i zlonamjernu izvršnu datoteku, skrivenu u obliku tekstualne datoteke.

Slika 2.9: Dalaj Lama u društvu Appleovih proizvoda

Nakon što bi zlonamjerni program zarazio računalo, kontaktirao bi svoj kontrolni poslužitelj koji se nalazi unutar kineskog IP adresnog prostora. Program je iskorištavao ranjivost programskog paketa Java, istu onu koje je koristio „**Flashback**“, prvi zlonamjerni program koji je masovno napao Mac OS X (u rujnu 2011). Zanimljivo je kako je Dalai Lama poznati korisnik Appleovog operativnog sustava, što se može i vidjeti na slici niže, tako da ovaj ciljani napad na korisnike tog operativnog sustava nije nikakvo iznenađenje.

2.6 Njemačka

U listopadu 2011. je „Chaos Computer Club“ (CCC), najveći i najpoznatiji europski hakerski klub, objavio [17] kako je izvršio analizu programa („legalnog presretača prometa“) kojeg koristi njemačka policija. Program je anonimno dostavljen CCC-u nakon što je pronađen „u divljini“, odnosno negdje na Internetu. Njemački ustavni sud je 27. veljače 2008. zabranio korištenje zlonamjernih programa za manipuliranje računalima građana, stoga je njemačka vlada razvila program „**Quellen-TKÜ**“ (ime dolazi od riječi „prisluškivanje izvora“) koji je trebao raditi isključivo na presretanju, odnosno prisluškivanju Internet prometa. Međutim, CCC je otkrio ugrađene funkcionalnosti u programu koje omogućuju mnogo više od toga. Naime, program može udaljeno preuzimati proizvoljne datoteke i udaljeno ih izvršavati. To znači da autori programa nisu ni pokušali implementirati tehničke mjere koje bi omogućavale samo presretanje prometa, nego su ugradili funkcionalnosti koje očito krše

njemačke zakone. Štoviše, te funkcionalnosti su dostupne svima, a ne samo vladinim agencijama, tako da ga mogu koristiti i kriminalci za uhođenje ili pak krivotvorenje dokaza protiv nekog. CCC je razvio svoj softver za nadzor vladinog programa i pokazalo se kako je program u stanju u potpunosti nadzirati rad na računalu, čitati e-mail poruke i tekst u svim oblicima web servisa. Analiza programa je također pokazala nekoliko sigurnosnih propusta. Loša implementacije enkripcije ili nedostatak iste omogućuju trećim stranama preuzimanje kontrole nad programom, slanje lažnih podataka prema državnim agencijama te vjerojatno čak i kompromitiranje mrežne infrastrukture tih agencija. Kako bi se prikrila lokacija komadnog poslužitelja, agencije podatke dobivaju putem poslužitelja smještenog u SAD-u, što je moguće kršenje nacionalne suverenosti, kako navodi CCC. Iako su državni službenici još 2008. obećali CCC-u kako će se za svaki slučaj koristiti posebno izrađena inačica programa, analiza je pokazala kako to nije slučaj. CCC je analizirao nekoliko inačica programa i kod svih je pronađen isti kriptografski ključ, a same inačice ne izgledaju posebno pripremljene. Još jedno obećanje je bilo kako će kvaliteta programa biti podložna strogoj kontroli, kako se ne bi mogao kršiti ustav, međutim, obzirom na ranije navedeno, niti to nije ostvareno.

F-Secure Detection	Backdoor:W32/R2D2.A **(F-Secure Hydra PC)**
Threat	category: **Heuristic** platform: **W32** type: **Block**
Exclusions	Hydra not excluded HIPS not excluded
Confidential	No
Last scan	2011-10-11 09:59:21
First seen	2010-12-09 13:57:04
Last seen	2011-10-11 09:59:16
File Size	643072
File Type	PE32_GUI
Signer	
Sign level	NO SIGNER
SHA-1	a6a0f45180f5b3390ee2ef21fe4b89813ed641f4
MD5	309ede406988486bf81e603c514b4b82

Slika 2.10: Tehnički opis "Bundestrojanera" tvrtke F-Secure

Opisani program je poznat i pod imenima „Bundestrojaner“, „0zapftis“ i „R2D2“ (prema znakovima pronađenim unutar programskog koda). Policija iz pet njemačkih pokrajina je priznala korištenje špijunskog programa i to tijekom razdoblja od dvije godine [19]. Korišten je u različitim kriminalnim slučajevima koji su uključivali i trgovinu drogom. Navodno je primjerak špijunskog programa kojeg je analizirao CCC presnimljen (od strane službenika) na prijenosno računalo sumnjivca dok je on prolazio kroz carinu u munchenskoj zračnoj luci. Taj čovjek je nakon toga angažirao odvjetnika i dao dopuštenje CCC-u da obavi forenziku nad njegovim računalom. Što se tiče autora „Bundestrojaner“

programa, čini se kako je to njemačka softverska tvrtka „DigiTask“ od koje je njemačka carinska služba kupila 2 milijuna eura vrijednu opremu za nadzor [18]. Štoviše, proizvođač sigurnosnih rješenja F-Secure je na svojem blogu objavio [20] kako je u posjedu instalacijske datoteke špijunskog programa. Riječ je o datoteci „scuinst.exe“, što je skraćeno od „Skype Capture Unit“, a to je komercijalni trojanski konj kojeg je razvila upravo tvrtka „DigiTask“. Slika prikazuje informacije F-Securea o navedenom zlonamjernom programu.

Zanimljivo je kako su instalacijsku datoteku dobili preko besplatnog web servisa „VirusTotal“ kojem je anonimni izvor predao tu datoteku na provjeru. VirusTotal sve datoteke dijeli s antivirusnim tvrtkama (čiji proizvodi provode skeniranje), stoga je neobično da su autori programa poslali instalacijsku datoteku na taj servis.

3 Učinak zlonamjernih programa

3.1 Nužnost tehničke zaštite i edukacije

Najveći učinak koji su imali zlonamjerni programi poput Stuxneta, Flamea i ostalih je u tome što su podigli računalnu svijest. Zahvaljujući velikoj medijskoj prašini i količini informacija o zlonamjernim programima te činjenici da su eksperti za računalnu sigurnost analizirali programski kod, organizacije iz različitih sektora su dobile bolji uvid u to kako pravilno zaštititi svoje informacijske sustave. Primjetno je kako je nedostatak osnovnih sigurnosnih principa veliki razlog što su zlonamjerni programi toliko uspješni. Bitno je naglasiti kako se za obranu od ove vrste zlonamjernih programa trebaju koristiti jednake mjere i procedure, kao i protiv klasičnih zlonamjernih programa i sličnih prijetnji.

Negativna posljedica javne objave programskog koda je mogućnost da će isti iskoristiti kriminalne skupine. No, mnogi stručnjaci često ističu kako je upravo javna objava najveći neprijatelj zlonamjernih programa. U globalnoj mreži danas je najvažnije dijeliti informacije i dobiti ih na vrijeme. Jednom pravovremenom nadogradnjom antivirusnih definicija na mrežnim uređajima, moguće je spriječiti velik broj zlonamjernih programa da napadnu mrežu. Konkretno, što se tiče Stuxneta, jedinstveno je to što je zarazio veliki broj računala kako bi uz pomoć njih došao do svoje krajnje mete – računala spojenih na točno određene PLC sustave. Iskoristio je činjenicu da takva računala koriste zastarjele inačice operativnog sustava Windows koja su ranjiva na već odavno otklonjene ranjivosti iz razloga što nisu spojena na Internet i ne primaju redovite nadogradnje. Međutim, podaci moraju na neki način stići do njih, a za to su korištene USB memorije. Time se pokazalo kako praksa zaštite potpunim isključivanjem sustava od Interneta nije najbolje rješenje. Pokazalo se koliko je bitno redovito vršiti nadogradnju softvera. Sama LNK ranjivost je pokazala kakav učinak može imati pravovremeno ne otklanjanje ranjivosti softvera. S obzirom kako se Stuxnet širio putem USB memorija, pokazalo se i koliko veliki problem može postati ne postojanje posebne sigurnosne politike za sve vanjske uređaje koji se priključuju na računala unutar interne mreže.

3.2 Postoji li „cyber rat“ i kako ga definirati

Od pojave termina „cyber rat“, odnosno još od 1996. godine (objavom SF romana Winna Schwartaua, „Informacijsko ratovanje“), taj termin se često koristio kod pojave novih prijetnji sigurnosti informacijskim sustavima [21]. Termin se često bezrazložno upotrjebljavao za različite ugroze. Ratovanje podrazumijeva dugotrajnu akciju tijekom koje napadač nanosi štetu svojem neprijatelju, što mu dugoročno donosi određenu prednost. U svijetu informacijskih sustava, to bi značilo da napadač mora ostati duže vrijeme neotkriven, inače bi njegova akcija bila financijski potpuno neisplativa i zapravo bi on bio u gubitku. Cijela akcija bi podrazumijevala pripremu, provedbu i remećenje rada vojnih sustava kao i civilne kritične infrastrukture (energetsku mrežu, vodovod, kontrolu prometa itd.). Dakle, „cyber rat“ je potpuno drugačiji termin od „cyber kriminala“ kojeg poznajemo već godinama i mnogo opširniji od tzv. „cyber špijunaže“ ili „cyber terorizma“.

Ranum [21] ističe kako upotreba „cyber“ oružja ima jedino smisla ukoliko država posjeduje ostala strateška sredstva (poput vojske) kojima može osigurati korist od cijelog napada. Dakle, korištenje jedino „cyber“ napada, ne može osigurati strateške ciljeve neke države. Isto vrijedi i za „cyber“ špijunažu. Ukoliko napadač ne posjeduje potrebne resurse da iskoristi prikupljene informacije, one su mu beskorisne. Također je očigledno da u slučaju da neko „cyber“ oružje zaista i nanese veliku i prije svega primjetnu štetu kritičnom sustavu neke države, da će vrlo brzo biti otkriveno. Nadalje, Ranum ističe da će „cyber rat“ s vremenom postati samo jedna vrsta operacija tijekom ratovanja te će pojam kao samostalni termin nestati. U tome ide i prilog činjenica kako se globalna zajednica računalnih tvrtki - proizvođača sigurnosnih rješenja i stručnjaka temelji na brzoj razmjeni informacija o prijetnjama. Nakon što netko iz zajednice otkrije zlonamjerni program (i njegovu funkcionalnost putem reverznog inženjeringa), to se otkriće javno objavljuje te proizvođači kreću u izradu potpisa za otkrivanje zlonamjernih programa. Komercijalni sektor sigurnosnih računalnih proizvoda je naviknut na brze reaktivne mjere svaki put kad „cyber“ kriminalci počnu koristiti neku novu tehniku. Nakon toga, upotreba tog „cyber“ oružja postaje, u principu, beznačajna. Ovo se najbolje vidjelo kod slučaja Stuxneta budući da su, prema neki izvorima[], napadači planirali da će program ostati (neotkriven) unutar kompleksa s centrifugama. Međutim, Stuxnet je „pobjegao“ na isti način i na koji je došao unutar kompleksa, putem vanjskih uređaja poput USB memorijskih diskova.

3.3 Nova uloga država u „cyber“ utrci

Za sve navedene zlonamjerne programe je zajedničko da su za inficiranje računala koristili ili socijalni inženjering ili su bili podmetnuti od strane zaposlenika. Za svoje širenje na druga računala, stjecanje potrebnih ovlasti na sustavima i dohvaćanje podataka koristili su ranjivosti u operativnim sustavima ili drugom softveru. U principu, to je klasičan način na koji zlonamjerni programi rade. Ta činjenica još jednom naglašava važnost pravilne implementacije tehničkih mjera zaštite, ali i edukacije korisnika. Međutim, ono što su zlonamjerni programi poput Stuxneta, Flamea i Gaussa donijeli, to je njihova nova uloga. Ta uloga je toliko specifična, a uz to je vrlo važno da napad ostane što duže neotkriven, tako da su programi morali biti mnogo sofisticiraniji nego klasični. Takva složena tehnička izvedba je tražila mnogo vremena, ljudi, opreme i financijskih sredstava. To je ono po čemu se zlonamjerni, odnosno špijunski programi koje financiraju države razlikuju od ostalih.

Vidljivo je kako su Sirija i Kina koristili javno dostupne zlonamjerne programe (tzv. RAT programe za udaljeni nadzor), umjesto da su koristili softver kojeg su sami razvili (poput Duqua i Gaussa npr.). Obzirom da je riječ o državama, cijena razvoja ne bi trebala imati utjecaj na izbor programa za špijunažu. Jedan od logičnih razloga može biti vremenski faktor jer razvoj posebnog softvera traje određeno vrijeme. U nekim slučajevima razlog može biti skrivanje onog koji stoji iza napada (u slučajevima Siriji i Kine to je ipak očigledno). Treći razlog može biti prebacivanje pozornosti s drugih sustava (softvera) za nadzor kako bi oni ostali neotkriveni.

Ne smije se zaboraviti specifičnost područja računalne sigurnosti. Razvoj rješenja se u tom području postiže testiranjem na stvarnim sustavima (Internetu) tijekom dužeg razdoblja, stoga tržište u punom smislu određuje smjer razvoja. To se najbolje vidi na primjeru razvoja kriptografskih algoritama, koji se godinama (i desetljećima) pomno ispituju, prije

nego što budu proglašeni standardom. Komercijalni sektor područja je vrlo specifičan i podložan brzim promjenama, pri kojim je dovoljno da jedan čimbenik (novo rješenje nekog proizvođača, otkriće itd.) bitno promijeni situaciju na tržištu. Neka država, iako posjeduje velike financijske resurse, može samo unajmiti ili kupiti gotova, prokušana rješenja koja imaju određen, nepredvidljiv vijek trajanja. Dobar primjer za to su „zero-day" ranjivosti. Uloga država se mijenja i one moraju aktivno sudjelovati u izboru ne samo resursa, već i rješenja koja će se koristiti za zaštitu njihovih informacijskih sustava ili praćenje meta.

3.4 Tržište „zero-day" ranjivosti

Popularizacija špijunskih (zlonamjernih) programa ima utjecaj i na komercijalni sektor sigurnosnih proizvoda. Pronalaženje dotad nepoznatih metoda za zaobilaženje sigurnosnih mjera nekog softvera (ili hardvera), odnosno „rupa" poznatih kao „zero-day" ranjivosti, postao je veliki biznis. Nekad su se takve informacije dijelile jedino među hakerima u „undergroundu", dok danas tvrtke poput Googlea, Applea i Facebooka bogato nagrađuju sigurnosne stručnjake koji im ustupe „zero-day" ranjivosti. Postoje i posebne organizacije poput „HP Zero Day Initiative" koje su specijalizirane za otkup novootkrivenih ranjivosti, odnosno „exploitova" – programskog koda koji iskorištava ranjivosti. Međutim, budući da je riječ o toliko vrijednim otkrićima koja bi mogla poslužiti vladinim organizacijama za špijunažu, neki stručnjaci proizvođačima ne žele otkriti ranjivosti. Najpoznatija tvrtka koja se specijalizirala za pronalazak ranjivosti i prodaju istih trećim stranama je francuski „Vupen" [22].

Slika 3.1: tim tvrtke Vupen [izvor: Forbes]

Na hakerskom natjecanju u Kanadi, kojeg je u ožujku 2012. organizirao Google, cilj je bio pronaći ranjivosti najnovije inačice Chromea, Googlevog web preglednika. Dvojici stručnjaka je to uspjelo i Google im je isplatio nagradu od 60 tisuća američkih dolara u zamjenu da otkriju sve tehničke detalje o tome kako su to uspjeli. Međutim, Vupen nije sudjelovao u tom natjecanju jer nije želio otkriti Googleu otkriti detalje o „exploitovima"

koje posjeduje. Izvršni direktor Vupena, Chaouki Bekrar je izjavio kako te informacije ne bi otkrili ni za milijuna dolara i da ih čuvaju za svoje klijente. Ti klijenti uključuju vladine organizacije koje koriste „zero-day" exploitove za špijuniranje kriminalnih osumnjičenika, ali i drugih meta (vjerojatno iz drugih zemalja) koji posjeduju vrijedne informacije. Kako bi došao do velike zarade, Vupen navodno koristi činjenicu da različite agencije žele imati prevlast u špijunskom „ratu". Bekrar je izjavio kako je politika tvrtke prodaja isključivo NATO-u i njegovim partnerima. Vupen nije jedina tvrtka koja se bavi ovim poslom, postoje i tzv. „exploit brokeri" koji su posrednici u kupoprodaji između vladinih agencija i hakera koji žele ostati anonimni. Oni s jedne strane osiguravaju da haker zaista posjeduje valjani „exploit", dok s druge strane jamče da haker neće prodati informacije nekom četvrtom. Jedan od brokera je za Forbes [23] iznio grubu računicu o tome koliko vrijede exploitovi za pojedini softver. Njegov udio u zaradi iznosi 15%.

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Slika 3.2: procjena cijena "zero-day exploitova" prema softveru

„Zero day exploitovi" koji se ovog trena prodaju na prilično sivom tržištu, mogli bi se naći u narednim špijunskim programima koji će tek biti otkriveni.

4 Literatura

[1] Stuxnet - malver za cyber rat, Nacionalni CERT, dokument, http://www.cert.hr/node/16280 , ožujak 2011.

[2] APT napadi, Nacionalni CERT, dokument, http://www.cert.hr/node/17917 , prosinac 2011.

[3] The Mystery of Duqu: Part Six (The Command and Control servers), Securelist, Kaspersky Lab, https://www.securelist.com/en/blog/625/The_Mystery_of_Duqu_Part_Six_The_Command_and_Control_servers , 30.11.2012.

[4] Analyzing the MD5 collision in Flame, Alex Sotirov, Trail Of Bits, prezentacija, lipanj 2012.

[5] What was that Wiper thing?, https://www.securelist.com/en/blog/208193808/What_was_that_Wiper_thing, Kaspersky lab, 29.8.2012.

[6] Was Flame's Gauss Malware Used To Uncover Hezbollah Money Laundering via Lebanese Banks? http://jeffreycarr.blogspot.com/2012/08/was-flames-gauss-malware-used-to.html, Jeffrey Carr, 9.8.2012.

[7] Kaspersky reports 3 more Flame-related malware variants http://news.cnet.com/8301-1009_3-57514377-83/kaspersky-reports-3-more-flame-related-malware-variants/ , 17.9.2012.

[8] Full Analysis of Flame's Command & Control servers https://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_Command_Control_servers , 17.9.2012.

[9] Who's Responsible for the Saudi Aramco Network Attack?, http://www.infosecisland.com/blogview/22290-Whos-Responsible-for-the-Saudi-Aramco-Network-Attack.html
29.8.2012.

[10] Flaws in Shamoon Malware Reinforce Theory It's Not A Wiper Variant https://threatpost.com/en_us/blogs/flaws-shamoon-malware-reinforce-theory-its-not-wiper-variant-082212 , 22.8.2012.

[11] Saudi Arabia says Iran talks waste of time; EU to enforce oil embargo on July 1st, Al Arabia News, http://www.alarabiya.net/articles/2012/06/26/222774.html , 26.6.2012.

[12] Insiders suspected in Saudi cyber attack, Reuters, http://www.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idUSBRE8860CR20120907 , 7.9.2012.

[13] DarkComet Surfaced in the Targeted Attacks in Syrian Conflict, TrendMicro TrendLabs Malware blog, http://blog.trendmicro.com/darkcomet-surfaced-in-the-targeted-attacks-in-syrian-conflict/ , 23.2.2012.

[14] Fake Skype Encryption Tool Targeted at Syrian Activists Promises Security, Delivers Spyware, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2012/05/fake-skype-encryption-tool-targeted-syrian-activists-promises-security-delivers , 2.5.2012.

[15] Pro-Syrian Government Hackers Target Activists With Fake Anti-Hacking Tool, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2012/08/syrian-malware-post , 15.8.2012.

[16] Dalai Lama + Mac OS X = APT with Tibet malware http://securityaffairs.co/wordpress/6892/intelligence/dalai-lama-mac-os-x-apt-with-tibet-malware.html ,
30.6.2012.

[17] Chaos Computer Club analyzes government malware http://www.ccc.de/en/updates/2011/staatstrojaner , 8.10.2011.

[18] German 'Government' R2D2 Trojan FAQ
http://nakedsecurity.sophos.com/2011/10/10/german-government-r2d2-trojan-faq/ , 10.10.2011.

[19] Several German states admit to use of controversial spy software, Deutsche Welle,
http://www.dw.de/dw/article/0,,15449054,00.html , 11.10.2011.

[20] More Info on German State Backdoor: Case R2D2, F-Secure, https://www.f-secure.com/weblog/archives/00002250.html , 11.10.2011.

[21] Parsing Cyberwar – Part 1: The Battlefield, Marcus J. Ranum,
http://fabiusmaximus.com/2012/08/09/41557/ , 9.8.2012.

[22] Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees), Andy Greenberg, Forbes, http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/ , 21.3.2012.

[23] Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits, Andy Greenberg, Forbes, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/ , 23.3.2012.