CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

APT napadi

NCERT-PUBDOC-2012-12-333

Nacionalni CERT

Sadržaj

1 Uvod

U posljednje vrijeme, a posebno nakon pojave zloglasnog crva Stuxneta [5] koji je napravio štetu iranskom nuklearnom programu, vidljivo je kako pojam sigurnosne prijetnje predstavlja mnogo više nego nekad. Napadači mjesecima, pa čak i godinama „pripremaju teren" skupljajući maksimalno širok spektar informacija o specifičnoj meti, testiraju svoj maliciozni softver u simuliranim uvjetima, pokušavaju pridobiti na svoju stranu osoblje blisko meti ili pak treniraju svoje vlastite špijune koji im mogu pomoći u svojem naumu.

Zadnjih desetak godina, mogu se vidjeti različiti primjeri napada koji su nagovijestili pojavu sofisticiranih sigurnosnih prijetnji. Primjerice, u veljači 1998. maliciozni kod je napao [1] računala zračnih snaga i mornarice SAD-a. Kasnije, iste godine, napadači su koristili poseban maliciozni kod za upad u web poslužitelje Američkog ministarstva obrane i NASA-e. Ukraden je velik broj klasificiranih dokumenata. Mnogi su za taj napad okrivili Rusiju, međutim, ruska vlada očekivano nije priznala umješanost. Navodni kineski hakeri su 2004. stajali iza napada na velikog američkog dobavljača oružja Lockheed Martin-a i opet NASA-e. Dvije godine kasnije, izvršni direktor konzultantske kuće Booz Allen Hamilton[1] je primio e-mail od Pentagona s listom oružja koju Indija želi kupiti. Međutim, ispod opisa zrakoplova i motora, nalazio se javno dostupni trojanski konj „Poison Ivy", a poruku uopće nije poslao Pentagon [2]. Srećom za Amerikance, direktor nije otvorio privitak. Kina je 2007. ponovno optužena za izvođenje vrlo sofisticiranog napada na opremu koju je Boeing prodao američkom ministarstvu vanjskih poslova [2]. U lipnju 2010. je otkriven spomenuti zloglasni crv Stuxnet [5]. Riječ je o vjerojatno najsloženijem malveru ikad te je procijenjeno kako su za njegovu izradu i testiranje u industrijskom okruženju trebale godine rada i deseci stručnjaka iz različitih područja. Zbog toga što je koristio izrazito sofisticirane metode prikrivanja, nije otkriven najmanje godinu dana. U veljači 2011. McAffe je otkrio kako je od studenog 2010. trajala koordinirana operacija prozvana „Night Dragoon" [7] koja je uključivala niz napada na razne naftne i petrokemijske tvrtke. Hakeri su oteli povjerljive dokumente o njihovom poslovanju. U ožujku 2011., poznati proizvođač sigurnosnih rješenja (posebno u području kriptografije), RSA je objavio kako je pretrpio napad na svoju infrastrukturu [3]. Istaknuto je kako je bilo riječ o napadu koji je uspio samo djelomično kompromitirati njihov sustav. Konkretno, pod napadom je bio naveliko korišteni sustav dvostruke autentikacije SecureID kojeg koristi 20 tisuća tvrtki i banki diljem svijeta. Sustav radi tako da svaki korisnik dobije svoj token, pseudoslučajni broj koji se mijenja svakih 30 ili 60 sekundi. Sam algoritam za generiranje tokena nije bio ugrožen napadom, ali je RSA morao postupno promijeniti preko 40 milijuna SecureID tokena [4]. Iz ovoga je jasno kako je napad na RSA lančano ugrozio sigurnost milijuna ljudi diljem svijeta. Tijekom 2011. izvedeni su i slični napadi na kanadsku i australsku vladu te Internacionalni monetarni fond (IMF) [8], ali i brojni drugi. U travnju 2011. izvršen je napad na Sony-jev mrežni servis za online igranje, PlayStation Network, u kojem su napadači oteli povjerljive podatke od čak 77 milijuna korisničkih računa.

Spomenute vrste napada zahtijevaju izrazito velike ljudske i novčane resurse, stoga takvu vrstu napada može provesti jedino vlade neke zemlje ili neka velika (bilo ona državna, privatna, teroristička ili kriminalna) organizacija. Naravno, nužan uvjet je da i meta,

[1] koja za američku vladu, između ostalih, obavlja poslove vezane uz strateško planiranje i komunikaciju

odnosno resursi (podaci) koji se namjeravaju ukrasti ili uništiti također budi vrijedni. Advanced Persistent Threat (APT)[2] je termin koji predstavlja upravo takvu vrstu prijetnje.

2 APT i njegove karakteristike

2.1 Značajke APT napada

APT napad je prvenstveno politički ili poslovno motiviran. Prema tome, mete su mu državne institucije i velike korporacije ili u principu bilo koja organizacija koja posjeduje nešto vrijedno. Primjerice, mete APT napada mogu biti: intelektualno vlasništvo (npr. izvorni programski kod, algoritam kriptiranja itd.), strategije pregovaranja ili pak podaci o zatajenim političkim aferama i sl. Što vrijednije podatke određene tvrtka čuva, veća je mogućnost da bude meta APT napada. Moguće je i da je cilj napada bude nanošenje štete specifičnom sustavu (kao u slučaju Stuxneta i iranskih nuklearnih elektrana). Dakle, za razliku od klasičnog malvera koji ne bira svoju metu, nego mu je cilj jednostavno zaraziti što veći broj računala, kod APT napada je meta vrlo specifična. Ranije je spomenuto kako su za provedbu ovakve vrste napada potrebni veliki resursi kakvima obično raspolaže samo neka vlada (odnosno određena vladina organizacija) ili velika organizacija. Međutim, trend se mijenja jer kriminalne skupine koje se bave računalnim kriminalom postaju sve bogatije, a i tehnologija je sve moćnija i (javno) dostupnija.

Kako bi APT napad bio uspješan potrebno je da kroz duže vrijeme bude neotkriven. Sukladno tome, ciljevi napada nisu što brža financijska dobit (krađa), a napadnuti sustavi nakon napada funkcioniraju sasvim normalno. APT se može definirati prema onome što predstavljaju pojmovi u njegovom akronimu [6] [8]:

- **Napredno** (**Advanced**) – napadači koriste široki spektar tehnologija, tehnika i metodologija upada u računalne sustave. Iako pojedinačno korištene tehnike, kao npr. malver, ne moraju biti napredne, sinergijski učinak većeg broja tehnika APT napada zahtjeva primjenu složenijih sustava i strategija obrane. Također, napadači su u stanju prilagoditi se promjeni stanja sustava i nadograditi ili popraviti korištene metode.
- **Perzistentno** (**Persistent**) – napadači daju prioritet specifičnom cilju, a APT napad se provodi neprestanim praćenjem i interakcijom s metom (kompromitiranim sustavom). Jednom kad uspiju upasti u sustav, napadače je jako teško zaustaviti.
- **Prijetnja** (**Threat**) – prijetnja podrazumijeva činjenicu da iza napada stoji koordinirana skupina ljudi, a ne automatizirani programski kod. Riječ je o timu motiviranih i obično dobro plaćenih eksperata.

2.2 Tehnike napada

APT napad, prema svojoj definiciji, koristi različite tehničke i netehničke metode upada u računalni sustav neke organizacije.

[2] termin su 2006. skovale Američke zračne snage (US Air Force) kako bi olakšale komunikaciju s medijima u slučaju napada kojeg nisu smjele klasificirati [9]. Kasnije je preuzet od strane stručnjaka za računalnu sigurnost.

Što se tiče tehničke strane, napad mora biti u stanju zaobići prvi stupanj obrane računalnih resursa, a to su obično mrežni uređaje kao što su vatrozidovi i sl. Dakle, napad se provodi putem uobičajenih mrežnih protokola kao što su HTTP, HTTPS, SMTP (e-mail) i dr. Također, napadači mogu koristiti i posebno izrađen model kriptiranja ili tuneliranje podataka (drugim protokolom) u svrhu prikrivanja mrežnog prometa. Pošto je obično na svakoj radnoj stanici instaliran određeni antivirusni alat, malver mora biti posebno prilagođen meti i kodiran na taj način da ga ti antivirusni alati ne mogu otkriti, odnosno u vrijeme napada ne postoji definicija malvera među proizvođačima antivirusnih rješenja. Više o značajkama malvera navedeno je u potpoglavlju 2.3. U nekoliko APT napada dosad, zabilježeno je korištenje ukradenih digitalnih certifikata (npr. slučaj Stuxneta), a spomenuti napad na RSA je, između ostalog, služio i za krađu mnogobrojnih digitalnih certifikata koji se onda mogu koristiti u sljedećim napadima (iako su certifikati povučeni i dalje napadačima mogu donijeti barem određen stupanj kredibiliteta).

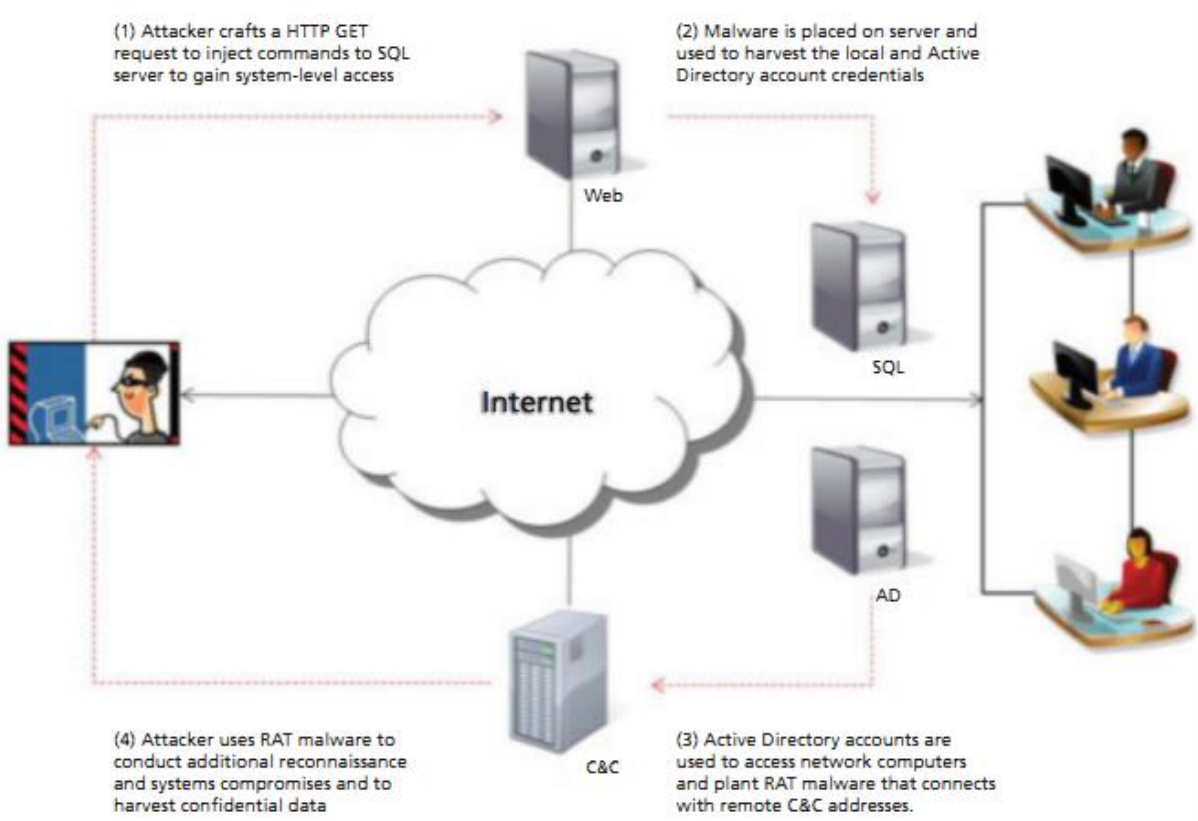
Netehničke metode napada podrazumijevaju korištenje različitih oblika socijalnog inženjeringa [11]. Upravo takve metode inicijalno omogućuju izvođenje daljneg tijeka napada. Radi se o slučajevima u kojima napadač uspijeva žrtvu nagovoriti na pokretanje zaraženog programa. Tehnike nagovaranja mogu biti različite, od lažnih e-mail poruka, telefonskih poziva, nagovaranja žrtve da posjeti zlonamjerne web stranice (phishing) itd. Ono što je zajedničko distribuciji malvera putem socijalnog inženjerigna je interakcija s žrtvom. Također treba imati na umu da će napadač koji provodi socijalni inženjering znati mnogo o funkcioniranju organizacije koja mu je meta. Time su njegove „priče“ uvjerljivije, odnosno napadač dobiva određeni kredibilitet. Napad je ispočetka usmjeren na najslabiju kariku, obično nekog zaposlenika kojeg će napadač (prevarant) moći lako kontaktirati, a potom metodama socijalnog inženjeringa uvjeriti da poduzme akciju koja će napadaču osigurati pristup unutar računalnog sustava organizacije-mete.

2.3 Malver

Malver igra središnju ulogu u gotovo svakom APT napadu. On je zapravo sredstvo izvršenja napada – omogućuje upravljanje kompromitiranim računalima, izvlačenje informacija i skrivanje prisutnosti. Malveru možemo dodijeliti slovo P u akronimu APT. On predstavlja perzistentnu komponentu napada. Malver koji je jednom zarazio ciljani računalni sustav može se na njemu dugo zadržati i napadaču osigurati neometanu kontrolu.

Svaka analiza poznatih APT napada uvijek uključuje i malver koji je napadač distribuirao te zarazio ciljani računalni sustav. Za primjer je moguće izdvojiti slijed događaja u NightDragoon napadu opisanom u dokumentu [7]. Iz slike 2.1 je vidljivo da je napadač kompromitirao web poslužitelj i potom iskoristio malver kako bi prikupio podatke o dostupnim korisničkim računima i druge povjerljive podatke.

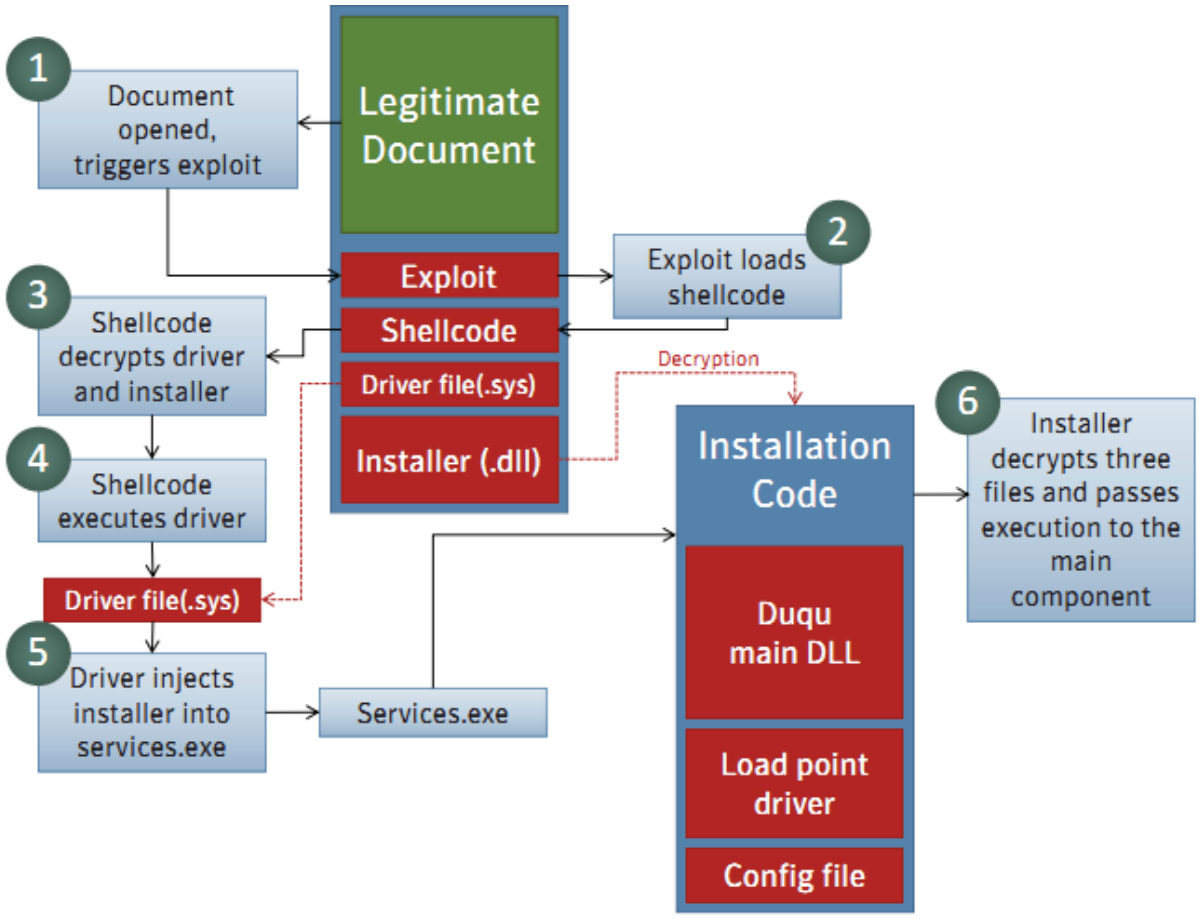
Kako je već ranije spomenuto, malver se u APT napadima širi najčešće putem socijalnog inženjeringa. Važno je još napomenuti da se malver obično distribuira putem PDF, DOCX i sličnih formata datoteka.



Slika 2.1: slijed događaja u "NightDragoon" napadu [izvor: McAfee, 7]

Riječi su slučajevi napada u kojim se malver distribuira bez interakcije s žrtvom. jer za ovakav način distribucije napadač mora iskoristiti ranjivost servisa žrtve, te njenim iskorištavanjem napadač može automatski pokrenuti malver bez interakcije s čovjekom. Ovakve ranjivosti često nisu javno poznate i u sigurnosnoj zajednici se nazivaju „zero-day“ ranjivosti. Na crnom tržištu se informacije o takvim ranjivostima prodaju za tisuće pa čak i stotine tisuća američkih dolara. Iako su riječi, ovakvi slučajevi se ipak događaju i ne smije ih se zanemariti.

Postoji mnoštvo različitih vrsta malvera koji su korišteni u APT napadima u zadnjih nekolilko godina. Zbog opsega dokumenata ukratko ćemo opisati samo jedan – Duqu. Duqu je napredni malver otkriven u jesen 2011. godine za kojega se sumnja da je korišten u nizu APT napada na različite poslovne organizacije diljem Europe. Malver su otrkili stručnjaci iz labaratorija za kriptografiju i sigurne sustave (CrySyS) u Budimpešti, a detaljnu analizu provela je tvrtka Symantec [10].



Slika 2.2: proces instalacije Duqu malvera [izvor: Symantec, 10]

Duqua karakterizira složeni proces instalacije koji iskorištava ranjivosti unutar jezgre Windows operacijskog sustava, a smatra se da je autor malvera imao na raspolaganju kod Stuxneta, budući da ima određenih sličnosti između ova dva malvera. Duqu uspijeva zaraziti sustav iskorištavajući do tada nepoznatu ranjivost unutar jezgre Windows operacijskog sustava. Ovo nije karakteristika standardnog malvera budući da su takve ranjivosti rijetke i njihovo otkrivanje iziskuje mnogo truda i znanja. No, ipak, Duqu zahtjeva i interakciju s žrtvom kako bi zarazio računalo. Naime, dolazi u obliku Word dokumenta koji žrtva mora otvoriti kako bi pokrenila malver. Proces instalacije Duqua prikazan je na slici 2.2.

U prvom koraku, nakon otvaranja dokumenata, aktivira se exploit koji iskorištava ranjivost unutar jezgre operacijskog sustava. Exploit potom učitava shellcode koji u jezgru operacijskog sustava umeće upravljački program. On u petom koraku pokreće glavni proces i time je sustav zaražen. Važno je napomenuti da upravljački program također osigurava da malvare ostane skriven na sustavu i da se pokrene sa svakim pokretanjem operacijskog sustava.

Što se tiče samog funkcioniranja malvera, on djeluje kao alat za udaljeno upravljanje i prikupljanje podataka. Duqu komunicira s kontrolnim poslužiteljem putem kojeg prima zadatke koje treba izvršiti i programe koje treba pokrenuti. Također, kontrolnim poslužiteljima šalje prikupljene podatke s zaraženog sustava.

Duqu prikuplja gotovo sve podatke na koje može naići. Neki od njih su:

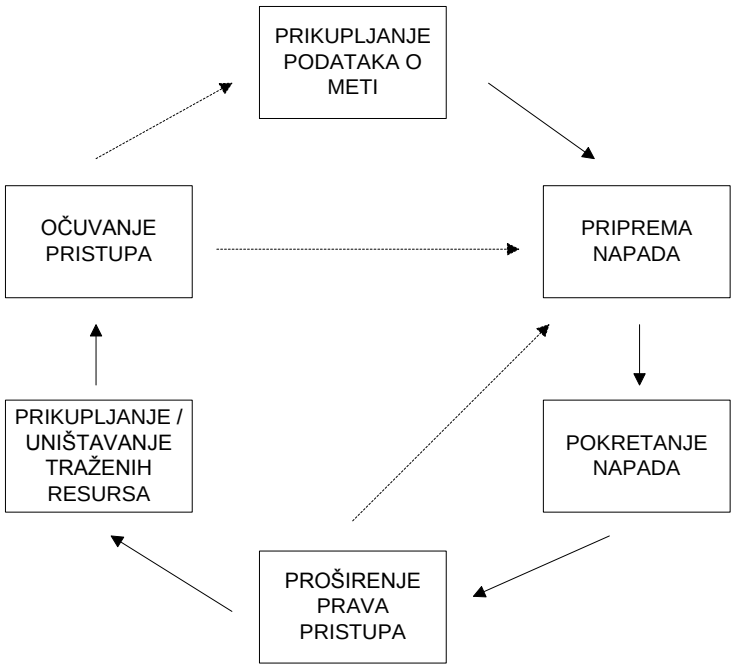
- podaci o aktivnim procesima
- podaci o korisnicima računala
- datoteke i podaci o datotekama
- slike zaslona
- digitalne certifikate prisutne na računalu

Također, Duqu na zaraženo računalo postavlja keylogger koji bilježi sve pritisnute tipke i time prikuplja podatke o lozinkama za druge servise na internoj mreži organizacije. Koristeći te lozinke, Duqu se širi i na druga računala – jednostavno se na računalo prijavi s lozinkom i pokrene svoju kopiju.

Duqu je tipičan primjerak malvera koji se koristi u APT napadima. Karakterizira ga prikrivenost i sposobnost krađe velikih količina različitih informacija. To je cilj svakog APT malvera. Računalo koje je njime zaraženo radi sasvim normalno i ne otkriva nikakve tragove infekcije, dok nije prekasno.

3 Tijek APT napada

Kao što je poznato, APT napad je složen i sastoji se od nekoliko faza koje se mogu ugrubo definirati. Faze su prikazane na slici 3.1.



Slika 3.1: osnovna metodologija APT napada

3.1 Prikupljanje podataka i priprema napada

Napad počinje prikupljanjem što veće količine podataka o meti (engl. „*reconnaissance*“) koji se koriste u svim preostalim fazama napada. Ova faza napada je izrazito bitna jer ljudi, a time i tvrtke često nisu ni svijesni koje su sve informacije o njima javno dostupne na Internetu. Napadači obično traže informacije o ključnim ljudima u organizaciji, IT administratorima te ranjivim računalima. Prikupljanje informacija o meti se može izvoditi pasivno i aktivno. Kod pasivnog prikupljanja, napadač nema ama baš nikakve interakcije s metom, nego putem javno dostupnih servisa prikuplja podatke. Postoji i nekoliko automatiziranih alata za tu namjenu.

Kod aktivnog prikupljanja informacija o meti, napadač koristi skeniranje mete, odnosno tehnike kojima šalje određene upite (IP pakete) prema meti i kojima može otkriti informacije o vrsti softvera koji se instaliran na poslužitelju, ranjivosti, IP adresama unutar mreže, domenama itd. Aktivno prikupljanje informacije se više može svrstati u drugu fazu APT napada, odnosno pripremu napada. Ta faza uključuje još i razvoj ili nabavu malicioznog koda, odnosno malvera koji će se koristiti u napadu, izradu phishing poruka, korisničkih računa (npr. za elektroničku poštu) i identiteta (npr. zaposlenik banke), nabavu potrebnog hardvera (poput USB stickova) te definiranje infrastrukture koja će se koristiti (kontrolni poslužitelji itd.).

3.2 Pokretanje napada

U većini slučajeva ova faza podrazumijeva upotrebu malvera u kombinaciji sa socijalnim inženjeringom. Dakle, ovdje napadači putem elektroničke pošte, telefonom ili nekim drugim medijem pokušavaju žrtve nagovoriti na akciju koja će im onda omogućiti upad u računalni sustav mete. Međutim, napadači se mogu pokušati i udaljeno spojiti na ranjivi poslužitelj, prokrijumčariti ili podvaliti zaraženi USB stick. U svakom slučaju, napadači aktivno prate stanje na svojim kontrolnim poslužiteljima za znakovima odgovora, odnosno mrežnog prometa od mete, što znači da je ona uspješno kompromitirana.

3.3 Proširenje prava pristupa

Jednom kada je napadač dobio pristup računalnoj mreži, on će istražiti gdje se točno u mreži nalazi, otkriti druga računala unutar mreže i proširiti svoja prava pristupa na njih. Time ima pristup većoj količini podataka, a ujedno se i osigurava ukoliko iz nekog razloga izgubi kontrolu nad inicijalno kompromitiranim računalom (početnom metom). Napadač traži ranjiva računala, a često kompromitira i domenski kontroler kako bi imao pristup lozinkama računa svih korisnika mreže. Na samom početku napada su pod udarom i certifikacijska tijela, odnosno PKI poslužitelji digitalnih certifikata. Napadači također kompromitiraju mail poslužitelje i poslužitelje koji čuvaju podatke kako bi u sljedećoj fazi prikupili nove informacije. Sve ovo znači da ova faza često podrazumijeva i ponavljanje 1. i 2. faze što se tiče pripreme i pokretanja napada, međutim one u tom slučaju traju mnogo kraće nego te iste faze prije provođenja prvotnog napada. Još jedan važan dio ove faze je i prikrivanje tragova napadačeve aktivnosti , međutim to zapravo vrijedi za cijeli tijek napada.

3.4 Perzistentno izvlačenje informacija

Nakon što je napadač odredio koji ga podaci zanimaju, od onih kojima ima pristup, započinje proces izvlačenja tih podataka. Ovdje može odabrati princip da prvo te podatke filtrira prije nego što ih prenese na svoj sustav ili da tu obradu napravi kasnije. Naravno, to ovisi o količini i vrsti podataka, a napadaču je uvijek u interesu ne pobuditi sumnju, tako da podatke obično izvlači postepeno, tijekom dužeg vremenskog perioda.

3.5 Očuvanje pristupa

Napadač, osim što mora proširiti svoja prava pristupa (4. faza), mora i osigurati očuvanje svojeg pristupa. Navedene dvije faze se često podudaraju. Napadač osigurava svoj pristup traženim resursima periodičnom komunikacijom s rezervnim putevima komunikacije (npr. „backdoor" malver instaliran na drugim radnim stanicama) koje je postavio u 4. fazi APT napada. Da bi napadač što duže ostao neotkriven, također mora paziti da minimizira količinu svoje aktivnosti. Ako ipak izgubi pristup računalom sustavu, napadač može probati napad ispočetka, odnosno vratiti se u 1. fazu (početak) ili pak 2. fazu (priprema) APT napada.

3.6 Korištenje izvučenih resursa

Nakon što su uspješno izveli APT napad, napadači još moraju izvući (ili uništiti) resurse, odnosno obaviti glavni cilj napada. Ukoliko napadače zanimaju nove informacije koje neprestano pristižu u kompromitirani sustav (npr. podaci o novim korisnicima ili novi poslovni planovi), ovaj proces može trajati jedno duže vrijeme. Na posljetku, napad će završiti jer će ga napadači prekinuti nakon što su postigli svoj cilj ili će žrtva primijetiti napad i zaustaviti ga. Nakon toga, napadači mogu pristupiti [12]:

- **ucjeni (traženju otkupnine)** – ovo je čest način na koji kriminalci unovčuju otete podatke. Žrtvama se prijeti da će se oteti podaci objaviti javno, a organizacija im plaća ukoliko smatra da će time izbjeći štetu zbog rušenja ugleda, kazni regulatora, gubitka korisnika itd.
- **prodaji ili dijeljenju metoda napada** – ako je napad ostao neotkriven, napadači mogu prodati ili podijeliti korištene metode napada s drugim napadačima kojih ih onda mogu iskorisiti za provođenje napada na istu ili sličnu metu
- **prodaji otetih informacija** – ako su ukradeni takvi povjerljivi podaci kao što su brojevi kreditnih kartica, napadači ih mogu prodati drugim kriminalnim skupinama, na crnom tržištu
- **javnoj objavi –** napadači mogu javno objaviti informacije o uspješnom napadu i prije nego što je pogođena organizacija svijesna da je bila napadnuta. Također, njihov cilj može biti jedino javno sramoćenje napadnute organizacije, odnosno ljudi koji stoje iza nje (ukoliko se promiču određene političke ideje, tada je riječ o haktivizmu).

4 Analiza uspješno izvedenog APT napada

Ovo poglavlje je posvećeno napadu na južnokorejsku tvrtku SK Communications, vlasnika i operatora najpopularnije južnokorejske društvene mreže CyWorld i web portala Nate. Napad se dogodio u srpnju 2011. godine, a rezultirao je krađom povjerljivih podataka 35 milijuna ljudi [13]. Ovaj konkretni slučaj iznosi vrijedne tehničke i netehničke detalje o napadu, što može biti od velike koristi ljudima zaduženim za sigurnost mrežnih sustava.

Slika 4.1: web portal Nate

4.1 Izvedba napada

Između 18. i 25. srpnja 2011. napadači su zarazili preko 60 računala SK Communications. To su uspjeli jer su prethodno, koristeći kineske IP adrese, kompromitirali[3] ALZip poslužitelj tvrtke ESTsoft. ESTsoft je velika južnokorejska softverska kuća koja je bila zadužena za redovitu instalaciju sigurnosnih nadogradnji na računala SK Communications. Naime, njihov skup alata ALTools, u koji spada i alat za kompresiju podataka ALZip, ima kao svrhu instalaciju redovitih nadogradnji. Napadači su na ALZip poslužitelj postavili program koji je jedino računalima iz SK servirao nadogradnje zaražene trojanskim konjem. Pritom je za postavljanje trojanskog konja bila iskorištena ranjivost ALTools paketa koja je omogućavala učitavanje maliciozne umjesto legitimne DLL datoteke. Nakon što su računala učitala malicioznu nadogradnju, zarazila su se malverom koji su proizvođači

[3] vjerojatno koristeći (softversku) ranjivost Microsoft ISS poslužitelja

antivirusnih alata imenovali Backdoor.Agent.HZA. Malver bi nakon infekcije, prvo provjerio ima li pristup na Internetu, a nakon toga pokrenuo TCP vezu na svoj kontrolni poslužitelj koji se krio iza jedne južnokorejske IP adrese. Napadači su koristili malicioznu izvršnu datoteku x.exe za prikupljanje informacija o mreži i korisničkim računima (imena i lozinke) unutar nje. Također je instalirana maliciozna datoteka nateon.exe[4] koja predstavlja RAT (Remote Administration Tool) malver koji napadačima omogućuje udaljenu kontrolu zaraženih računala. Malver je na zaraženom računalu RAT instalirao kao Windows servis koji se pokretao zajedno sa svakim pokretanjem operacijskom sustava. RAT se spajao na ranije registriranu domenu iza koje je stajao jedan od kontrolnih poslužitelja. Malver je imao višestruke mogućnosti, a mogao je zaraziti bilo koju inačicu Windowsa. Napadači su ga koristili za uspostavu mrežnih konekcija, modificiranje registra Windowsa, kontrolu procesa i servisa, preuzimanje i izradu datoteka te gašenje i restartanje računala. Malver je koristio tehnike prikrivanja programskog koda (obfuskaciju), a služio je i kao „sniffer" Internet paketa jer bio instaliran na lokalno mrežno sučelje koje je pratilo sav mrežni promet te je radi toga mogao primati naredbe preko bilo kojeg porta i bilo kakvim protokolom.

Nakon pripreme za glavni dio napada, napadači su 26. srpnja RAT malveru izdali naredbe za pristup bazama podataka servisa Nate i Cyworld. Jedan od modula malvera je bio zadužen za pokretanje niza SQL funkcija kojima su napadači došli do povjerljivih korisničkih podataka. IP adresa na koju su napadači poslali otete podatke pripada kineskom IP adresnom prostoru.

4.2 Vremenski tijek napada

Kako bi se dobio uvid u vremenski period tijekom kojeg su trajale različite faze APT napada, više iz perspektive napadača, na slici 4.2 prikazan je kronološki tijek napada [13]:
Vidljivo je kako je dio napada koji se može rekonstruirati trajao čak 10 mjeseci, ne računajući pritom veći dio faze prikupljanja podataka o meti koji je vjerojatno trajao nekoliko mjeseci prije 24. rujna 2010. To je najbolji pokazatelj koliko je truda i znanja potrebno uložiti u izvođenje jednog APT napada.

4.3 Što se može naučiti iz ovog napada

Ovaj napad, pokazuje neke od metoda koje napadači koriste u APT napadima te se iz toga može dosta naučiti. Konkretno, riječ je o:

- napadu na drugu organizaciju kako bi se pomoću nje osigurao pristup pravoj meti-organizaciji
- napadu na specifična računala (u ovom slučaju isključivo računala SK Com., od svih onih koje je ESTSoft posluživao)
- korištenju istih (lažnih) podataka kod registracije domena koje se kasnije koriste u napadu
- registraciji domena sličnog imena, kako bi se dobili na vjerodostojnosti

[4] ime aludira na NateOn kako se zove najpopularniji „instant-messaging" klijent u Južnoj Koreji, kojem je također vlasnik SK Communications. Zapravo, legitimni klijent, NateOn, koristi izvršnu datoteku istog imena.

- ponovnom korištenju iste infrastrukture (u ovom slučaju napadači su koristili više domena na pristup istoj IP adresi unutar dužeg vremenskog perioda)
- TTL polje u konfiguraciji DNS servisa se postavlja na vrlo niske vrijednosti (poput 30 minuta), što napadačima omogućuje brzu promjenu kontrolnih poslužitelja, odnosno bezbrižan pristup meti, u slučaju blokade dijela infrastrukture

Slika 4.2: kronološki slijed događaja vezanih uz napada na SK Com.

5 Mjere obrane od APT napada

APT napad je po prirodi takav da je nemoguće strogo definirati učinkovitu strategiju, odnosno sigurnosnu politiku koja bi štitila od njega. Napad je osmišljen za specifičnu metu, tako da je obrana od njega jedan dugotrajni proces u kojem ključnu ulogu zapravo ima osviještenost i stručnost zaposlenika organizacije. Uz to, potrebno je osigurati nužne preduvjete za učinkovitu obranu od takvog napada, bez kojih cijela sigurnosna politika nema svoj smisao.

5.1 Nužni preduvjeti za obranu

5.1.1 Uvid u slabosti mrežnih uređaja

Tradicionalni mrežni sigurnosni uređaji poput različitih vatrozidova i IDS/IPS uređaja, ne mogu se nositi s ovom vrstom prijetnje. Takvi uređaji su prvenstveno namijenjeni blokiranju poznatih metoda (vektora) napada. Teško je nadzirati cijeli web i e-mail promet u potrezi za malicioznim aktivnostima. Najnovija generacija vatrozidova ima potpunu kontrolu nad svih sedam slojeva i donosi značajan pomak u smislu praćenja mrežnog prometa, no ti uređaji i dalje ovise o definiranim sigurnosnim politikama, odnosno načinu na koji su ti uređaji konfigurirani. Važno je koristiti i uređaje s mogućnošću provjere sadržaja poruka elektroničke pošte, filtiranja URL-ova i blokiranja malicioznog JavaScript koda. Također, uređaj bi morao imati i mogućnost dekriptiranja SSL prometa kako bi se taj promet mogao provjeriti u potrazi za malverom ili povjerljivim podacima.

5.1.2 Praćenje indikatora rizika i njegovog konteksta

Kako bi uspjeli identificirati malicioznu aktivnost, potrebno je poznavati kontekst unutar kojih se aktivnosti događaju. To je nužno jer, kako je poznato, za malver koji se koristi u APT napadima ne postoje antivirusne definicije i on se ne može otkriti. Noviji uređaji za nadzor mreže imaju mogućnost automatskog definiranja „normalne“ aktivnosti kroz aktivno praćenje i „samo-učenje“ o aktivnostima u mreži te stoga predstavljaju dobru osnovu za praćenje sumnjivih aktivnosti u mreži. Takvi uređaji mogu sumnjive događaju rangirati prema interno ugrađenom faktoru rizika, što također može biti od velike pomoći. Potrebno je i da mrežni administratori budu upoznati s lokacijom svih računala, mrežnih uređaja i opreme unutar mreže kako bi bili u stanju aktivno nadzirati stanje.

5.1.3 Osviještenost o lokaciji najosjetljivijih podataka

Ukoliko se primijenjuju vatrozidovi nove generacije koji su konfigurirani na taj način da znaju lokaciju i nadziru prijenos osjetljivih podataka, tada se krađa podataka može lako spriječiti. Dakle, umjesto da se pokušava spriječiti bilo kakav upad u računalni sustav, važnije je odrediti koji resursi, odnosno podaci su najvrijedniji te njih onda osigurati. Tim najvažnijim podacima je potrebno osigurati nekoliko slojeva obrane, a ako je nužno potpuno ih izolirati od mreže. Podatke je potrebno ukloniti s nesigurnih lokacija i lokacija na kojima uopće ne bi trebali ni biti. Korištenje posebno pripremljenog (engl. *custom*) algoritma za kriptiranje, također značajno pomaže u zaštiti najvrijednijih podataka.

5.2 Zaštita od malvera

Obično se krajnjim korisnicima ističe kako je obvezno imati instaliran jedan antivirusni alat za zaštitu od malvera. To je prvi i najvažniji savjet. No, kada su u pitanju APT napadi na organizaciju, ovaj savjet mogao bi zauzimati najniže mjesto po prioritetu. Antivirusni alat mora biti instaliran na sve radne stanice unutar organizacije, ali tek kao usputna mjera povećanja sigurnosti.
Kao što je prethodno rečeno, APT malver pokušava što dulje ostati neprimijećen. U velikoj većini APT napada koristi se posebno dizajniran malver koji nije javno poznat niti je ikada bio analizran. Antivirusni alati ne mogu takav malver prepoznati i nude slabu zaštitu od njega.
Zaštiti od malvera treba pristupiti slojevito. Potrebno je implementirati različite mjere zaštite i usuglasiti ih s mjerama zaštite na ostalim područjima (zaštita mreže, fizička zaštita, sigurnosna politika...). Nekoliko osnovnih savjeta za učinkovitiju zaštitu od malvera:

- pravilna raspodjela **privilegija** između zaposlenika i korisničkih računa – svaki zaposlenik mora imati svoj korisnički račun samo s onim privilegijama koje su mu nužne za rad. Administratorskim korisničkim računom smiju se koristiti samo administratori i IT stručnjaci. Čak ni krovni menadžeri i direktori ne smiju imati administratorske ovlasti. Malver koji se pokrene pod ovlastima običnog korisničkog računa predstavljati će manju opasnost za širenje i bit će ga lakše ukloniti.
- ograničavanje **prava pristupa** dokumentima i datotekama – slično kao i s privilegijama korisničkih računa, svaki dokument mora se čuvati u skladu s značenjem koje ima za organizaciju. Potrebno je oganičiti pristup neovlaštenim osobama. Posebno je važno čuvati kriptografske ključeve i certifikate.
- **informiranost** – IT stručnjaci unutar organizacije moraju biti informirani o najnovijim prijetnjama, opasnostima i vrstama napada. Na taj način mogu reagirati na vrijeme i zaštitit organizaciju
- **edukacija** – svi zaposlenici moraju biti educirani o mogućim opasnostima koje im prijete. Posebno se to odnosi na edukaciju o phishing napadima. Važno im je napomenuti da ne smiju otvarati sumnjive daoteke. To se više ne odnosi samo na .exe datoteke već i na Word i PDF dokumente, video i audio zapise ili neke druge dokumente. Važno je zaposlenike educirati i o opasnostima posjećivanja nepoznatih ili sumnjivih web mjesta.
- **antivirusni alati** – mogu pomoći u sprečavanju zaraze s nekim poznatim malverom.
- korištenje **dvostruke autentikacije** – gdje god je moguće implementirati dvostruku autentikaciju (engl. *two factor authentication*), a posebno na VPN mrežama.

6 Zaključak

S obzirom na veliki broj APT napada koji se dogodio nekoliko posljednih godina, a posebno tijekom 2010. i 2011., vidljivo je kako su oni postali trend. Naravno, s vremenom je porasla i njihova sofisticiranost, ali nažalost i šira dostupnost. Sve veći broj kriminalnih, špijunskih i političkih organizacija u svojim aktivnostima koristi APT napade. S obzirom na javnu ili gotovo javnu dostupnost velike količine podataka na globalnoj mreži, to je zapravo i očekivano. Nažalost, u vremenu ekonomske krize, tvrtke će vjerojatno zanemarivati informacijsko-sigurnosni aspekt svojeg poslovanja te će tako postatit lak plijen spomenutih kriminalnih organizacija.

Glavna protumjera APT napadima, kao i općenito u području računalne sigurnosti, je edukacija svakog zaposlenika, odnosno korisnika mrežne infrastrukture. Međutim, riječ je o zahtjevnoj i sporoj mjeri te dok se globalna svijest o sigurnosti informacija znatno ne popravi, izvodit će se veliki broj (uspješnih) APT napada. Osim toga, takvi napadi su po svojoj prirodi namijenjeni zavaravanju i nadmudrivanju čak i stručnih osoba jer ljudski faktor pogreške se nikad ne može zanemariti. Tvrtkama, državnim i drugim organizacijama ostaje što striktnija primjena sigurnosnih standarda, odnosno provođenje novih i strožih sigurnosnih politika. Važno je zapamtiti kako APT napadi koriste „najslabije karike“ u sustavu, te stoga današnje organizacije moraju kontinuirano educirati, nadzirati i provjeravati rad svojih odjela i zaposlenika.

7 Literatura

1. An Evolving Crisis, http://www.businessweek.com/magazine/content/08_16/b4080032220668.htm, 10. travnja 2008.
2. The New E-spionage Threat, http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm, 10. travnja 2008.
3. RSA warns customers of sophisticated security breach, http://www.v3.co.uk/v3-uk/news/2035153/rsa-warns-customers-sophisticated-security-breach, 18. ožujka 2011.
4. RSA finally comes clean: SecurID is compromised, http://arstechnica.com/security/news/2011/06/rsa-finally-comes-clean-securid-is-compromised.ars, 6. lipnja 2011.
5. Stuxnet - malver za cyber rat, Nacionalni CERT, tehnički dokument, http://www.cert.hr/node/16280, ožujak 2011.
6. Advanced Persistent Threats (APT), http://www.damballa.com/knowledge/advanced-persistent-threats.php, Damballa
7. Global Energy Cyberattacks: „Night Dragoon“, tehnički dokument, McAffe, 10. veljače 2011.
8. Advanced Persistent Threats: A Decade in Review, Command Five Pty Ltd, tehnički dokument, lipanj 2011.
9. J. Tabeling: APT - Advanced Persistent Threat - What is it?, http://idpnow.blogspot.com/2011/06/apt-advanced-persistent-threat-what-is.html, 14. lipnja 2011.
10. W32.Duqu – The precursor to the next Stuxnet, Symantec, tehnički dokument, verzija 1.4, 23. studenog 2011.
11. O socijalnom inženjeringu, Nacionalni CERT, http://www.cert.hr/socijalni_inzenjering
12. Advanced Persistent Threats and Other Advanced Attaks, Websense, tehnički dokument, rev. 2, 2011.
13. SK Hack by an Advanced Persistent Threat, Command Five Pty Ltd, tehnički dokument, rujan 2011.