Centar Informacijske Sigurnosti

Advanced Persistent Threat napadi

studeni
2011.

CIS-DOC-2011-11-031

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Tijekom prošle godine ozloglašeni napadi zlonamjernih skupina koje se nazivaju naprednim ustrajnim prijetnjama (eng. *Advanced Persistent Threat*, APT) su postali posebno poznati zbog medijski dobro popraćenih napada na organizacije javnog i privatnog sektora, primjerice napada na Google (napad na uslugu GMail 2010. godine) i nacionalni laboratorij Oak Ridge (pokušaj napada na računalne sustave na kojima su pohranjeni podaci o nuklearnim istraživanjima). Na nesreću, APT napadi nisu ograničeni na vojne, obavještajne i tehnološke mete, već se pojavljuju kod gotovo svake industrije. Prema nekim izvještajima, 59% ispitanih su sigurni ili prilično sigurni da su njihove organizacije bile meta APT napada. Nadalje, 72% organizacija vjeruje da je vrlo vjerojatno da će u budućnosti postati mete APT napada. Istraživanja pokazuju kako većina organizacija nije dovoljno dobro zaštićena od budućih napada, a čak jedna trećina vjeruje kako su njihove organizacije prilično ranjive. Još jedan važan podatak je da 46% velikih organizacija koje su kategorizirane kao one s najboljom informacijskom sigurnosću vjeruje kako su nedovoljno pripremljene za buduće sofisticirane napade.[1]

Ovaj dokument daje detaljniji uvid u APT napade. U poglavlju "Što je Advanced Persistan Threat?" dana je okvirna definicija pojma, opis pojava koje se s njim povezuju i kratak opis načina rada APT skupina. Poglavlje "Povijest APT napada" donosi pregled značajnijih zabilježenih APT napada unatrag deset godina i kratak opis korištenih tehnika. U poglavlju "Anatomija napada, tehnike i metode" detaljno je prikazana anatomija APT napada, navedene su razlike u odnosu na obične hakerske napade te je dan detaljniji pregled najčešće korištenih alata i metoda napada. Poglavlje "Rizici i metode zaštite" daje pregled posebno ranjivih područja i predlaže mjere zaštite od APT napada. U poglavlju "Analiza napada na SK Communications" dana je detaljna analiza napada na tvrtku SK Communications koji se dogodio u srpnju 2011. godine.

[1] Istraživanja je proveo Enterprise Strategy Group; rezultati istraživanja dostupni su na web stranici http://www.enterprisestrategygroup.com/.

2. Što je Advanced Persistent Threat?

Izraz *Advanced Persistent Threat* se obično odnosi na organiziranu skupinu ljudi (primjerice na vladu neke države) koja ima namjeru i sposobnosti za ustrajan i djelotvoran napad na određeni subjekt. Izraz se najčešće koristi u kontekstu računalnih, posebice mrežnih, napada, međutim može se odnositi i na tradicionalne oblike špijunaže i napada. Ostale važnije metode napada uključuju zaražene medije i socijalni inženjering. Izraz APT se ne odnosi na zlonamjerne pojedince (hakere) pošto oni najčešće nemaju dovoljno resursa da bi postali takva vrsta prijetnje. Osim toga, "obični" hakeri svoje napade usmjeravaju prema računalima sa slabom zaštitom, dok APT cilja na točno određene računalne sustave i izvodi ustrajne napade na njih.

Unutar računalne zajednice izraz APT se gotovo uvijek koristi za opisivanje sofisticiranih napada koji traju dulje vremensko razdoblje, a usmjereni su protiv vlada, kompanija i političkih aktivista. Česta je zabluda da APT napadi ciljaju samo vlade zapadnih zemalja. Iako su primjeri APT napada na zapadne zemlje poznatiji i dostupniji, napadači iz mnogih zemalja koriste APT kao sredstvo sakupljanja informacija o pojedincima ili skupinama od interesa. Često se događa da su APT skupine pod državnim nadzorom.

Točne definicije APT-a variraju. Iz izravnog prijevoda izraza APT može se zaključiti sljedeće:

- *Advanced* (napredan) - ljudi koji upravljaju samom prijetnjom koriste cijeli niz tehnika za sakupljanje podataka. One mogu uključivati tehnologije i tehnike koje se koriste za upade u računalne sustave, no uključuju i uobičajene načine skupljanja podataka (primjerice presretanje telefonskih poziva i satelitske snimke). Iako se pojedine komponente napada ne bi mogle nazvati posebno naprednima (primjerice zlonamjerni programi konstruirani uz pomoć jednostavnih i široko dostupnih "uradi sam" alata), napadači po potrebi mogu razviti i naprednije alate. Oni često kombiniraju više metoda, alata i tehnika napada da bi došli do žrtve, ugrozili je i dobili pristup osjetljivim podacima.
- *Persistent* (ustrajan) - napadači posebnu pažnju posvećuju specifičnom zadatku. Oni ne traže informacije oportunistički u svrhu financijske ili neke druge dobiti. Ta osobina nameće zaključak da napadače nadzire neki vanjski subjekt. Napad se odvija uz stalni nadzor. Pritajeni i polagani napadi pokazali su se uspješnijima od stalnih velikih napada. Kad napadači izgube kontakt sa žrtvom obično će ga pokušati ponovno uspostaviti, najčešće uspješno. Jedan od glavnih napadačevih ciljeva je održavanje dugotrajnog pristupa resursima žrtve.
- *Threat* (prijetnja) - APT-ovi predstavljaju prijetnju jer posjeduju i sposobnosti i namjeru za napad. APT napade izvode ljudi, koordinirano, za razliku od uobičajenih napada koji se temelje na automatiziranim dijelovima koda. Napadači imaju specifičan zadatak te posjeduju odgovarajuće vještine, motivirani su, organizirani i odgovarajuće financirani.

Metode i sofisticiranost APT napada variraju ovsino o ciljevima, alatima i tehnikama kojima se napadači koriste. Također, one ovise o sposobnostima otkrivanja, identificiranja i obrane od strane žrtve. Osim toga, napadači moraju paziti da ne budu otkriveni.

APT napadi često koriste dotad nepoznate propuste u računalnim sustavima, programima ili operacijskim sustavima (eng. *zero-day exploits* [2]). Upotreba *zero-day exploit* programa svojstvena je za APT napade pošto je razvoj takvih programa skup, složen i dugotrajan, a rijetki imaju dovoljno resursa za razvoj.

Pojam *Advanced Persistent Threat* skovan je u američkom odjelu za obranu (eng. *Department of Defense,* DoD) za opis prikrivenih računalnih napada s ciljem špijunaže i sakupljanja informacija. Industrija računalne sigurnosti u posljednjih nekoliko mjeseci sve više upozorava na opasnosti APT-a, posebice nakon što je tvrtka Google objavila da je bila žrtva mrežnog napada s izvorištem u Kini, a s ciljem krađe informacija. Također, neki stručnjaci s područja informacijske sigurnosti ističu ulogu kineske vlade u sponzoriranju, ograniziranju i izvođenju takvih napada.

[2] Zlonamjerni programi koji iskorištavaju tek otkrivene i javnosti nepoznate propuste u programskim proizvodima.

3. Povijest APT napada

Prvi javni zapisi o APT napadima datiraju još iz davne 1998. godine kada su Pentagon, NASA, istraživački laboratoriji, privatna sveučilišta te odjel za energetiku Sjedinjenih Država postali žrtvama napada. Tijekom godina većina kompanija koje su priznale da su bile žrtve napada nisu bile voljne dati informacije i detalje o tim događajima. To je vjerojatno zbog toga što ne žele dati povratnu informaciju napadačima ili narušiti ugled.

Značajniji napadi koji se povezuju s APT-om u posljednjih desetak godina su:

- **Moonlight Maze napad** (ožujak 1998.-2000.)

  Računalnim napadima nazvanima Moonlight Maze napadnuta su računala u Penagonu i NASA-i, računala Američkog odjela za energetiku, računala istraživačkih laboratorija i privatnih sveučilišta. Napadači su uspješno dobili pristup desecima tisuća dokumenata.

- **Uredi američkih kongresmena** (kolovoz 2006.-2007.)

  Računalne mreže ureda dvaju kongresmena bile su napadnute, a ukradene su informacije o Pekinškom režimu.

- **Nacionalni laboratorij Oak Ridge** (29. listopad 2007.)

  Nacionalni laboratorij Oak Ridge napadnut je porukama elektroničke pošte koje su izgledale kao legitimne službene poruke. Napadači su dobili pristup računalima i bazi podataka o posjetiteljima laboratorija.

- **Nacionalni laboratorij Los Alamos** (9. studeni 2007.)

  Nacionalni laboratorij Los Alamos objavio je da je iz računalne mreže Yellow ukradena značajna količina podataka. Vjeruje se da je napad bio dio većeg, koordiniranog napada usmjerenog na američke laboratorije i druge važne institucije.

- **Ministarstvo obrane SAD-a** (početak 2008.)

  Ministarstvo obrane SAD-a pretrpjelo je napad na računalne mreže nakon što je strana obavještajna agencija u njihov sustav ubacila zlonamjerni program na vanjskoj memorijskoj jedinici spojenoj na univerzalnu serijsku sabirnicu (eng. *Universal Serial Bus,* USB) . Zaraženo je računalo američke vojske, nakon čega se program proširio kroz njihovu mrežu i zarazio ostala računala.

- **Ured Dalaj Lame** (rujan 2008.)

  Napadači su u rujnu 2008. presreli poruku elektroničke pošte poslanu uredu Dalaj Lame te legitimni privitak zamjenili dokumentom koji je sadržavao zlonamjeran sadržaj. Napadači su uspjeli ukrasti lozinke te ih kasnije koristili za konstantan pristup poslužitelju elektroničke pošte ureda Dalaj Lame.

- **GhostNet** (29. ožujak 2009.)

  Objavljeno je istraživanje o pojedinostima operacija računalne špijunaže nazvane GhostNet. Zaraženo je najmanje 1295 računala u više od 100 zemalja, uključujući i ona koja pripadaju veleposlanstvima, južnokorejskoj vladi te uredu Dalaj Lame.

- **Stuxnet** (lipanj 2009.)

  Prvi poznati ciljani napad na neimenovanu organizaciju dogodio se uporabom crva Stuxnet. Organizacija je bila ponovo pogođena istim crvom u ožujku i travnju 2011. godine. Mnogobrojne druge organizacije, prvenstveno one iz Irana također su bile napadnute. Izgleda da je crv dio koordiniranih napora da se reprogramiraju specifični industrijski upravljački sustavi.

- **Night Dragon** (studeni 2009.)

  Koordinirani, tajni i ciljani napadi bili su usmjereni na globalne naftne i petrokemijske kompanije. Napadači su se koristili *phishingom* i ranjivostima operacijskog sustava Microsoft Windows kako bi pridobili pristup računalima. Nakon što su dobili pristup sustavu, napadači su došli do informacija o operativnim i financijskim planovima naftnih i pektrokemijskih kompanija.

- **Operacija Aurora** (sredina prosinca 2009.)

Tvrtka Google je otkrila ciljani napad na svoju infrastrukturu koji je rezultirao krađom intelektualnog vlasništva. Vjeruje se da je ovaj napad bio dio drugog, većeg i koordiniranog napada kojim su napadači pokušali ukrasti izvorne kodove u vlasništvu raznih kompanija.

- **Francuska vlada** (prosinac 2010.-ožujak 2011.)

  Francuska je vlada napadnuta je *phishingom*. Napadači su zarazili više od 150 računala i nadzirali ih više od tri mjeseca. Ukradeni su dokumenti vezani uz Francusko predsjedanje G20 i međunarodne ekonomske afere.

- **Kanadska vlada** (siječanj 2011.)

  Uredi kanadske vlade napadnuti su *phishingom*. Poruke su sadržavale zlćudne privitke koji su zarazili računala kanadske vlade i rezultirali krađom povjerljivih informacija.

- **Comodo Affiliated Root Authority** (15. ožujak 2011.)

  CARA je također bio meta napadača, što je rezultiralo zlćudnim certifikatima sigurnosnog sloja utikača (eng. *Secure Sockets Layer*, SSL) za mnoge popularne domene poput „mail.google.com“, „www.google.com“, „login.yahoo.com“ i „login.live.com“.

- **RSA** (17. ožujak 2011.)

  RSA objavljuje da je bila žrtva napada *phishing* porukama s privitcima zlćudnog sadržaja. Napadači su dobili pristup njihovoj mreži te izvukli informacije vezane za RSA SecurID proizvode. Ukradene informacije kasnije su iskorištene za napade na klijente.

- **Nacionalni laboratorij Oak Ridge** (sredina travnja 2011.)

  Nacionalni laboratorij Oak Ridge *phishing* porukama, koje su sadržavale poveznicu na program koji je iskorištavao dotad nepoznati propust u pregledniku Internet Explorer.

- **L-3 Communications** (6. travanj 2011.)

  Krađa informacija tvrtke RSA rezultirala je redovnim napadima na kompaniju L-3 Communications.

- **Lockheed Martin** (21. svibanj 2011.)

  Tvrtka Lockheed Martin otkrila je napade na svoju računalnu mrežu. Tim zadužen za informacijsku sigurnost poduzeo je brojne akcije kako bi zaštitio sustav. Nije poznato jesu li neki podaci ukradeni. Napad je izveden uz pomoć informacija dobivenih od RSA.

- **Northrop Grumman** (26. svibanj 2011.)

  Informacije ukradene od RSA pomogle su napadu na Northrop Grumman. Tvrtka je ugasila sve pristupe svojoj mreži bez ikakvog upozorenja, što je rezultiralo *resetom* svih lozinki.

- **Interantional Monetary Fund** (svibanj 2011.-lipanj 2011.)

  Napadnuto je najmanje jedno računalo Internacionalnog Monetarnog Fonda. Napad je uključivao i poseban program napravljen isključivo za napad na IMF. Napadnuto računalo korišteno je za pristup internoj mreži IMF-a. Napad bi omogućio pristup osjetljivim ekonomskim i političkim informacijama.

APT-ovi su diljem svijeta napadali vlade, naftne, energetske i petrokemijske kompanije, rudarski sektor, financijske institucije, vojne institucije, sektor tehnologije i znanosti, infrastrukturu i mnoge druge sektore (slika 1). Izvedeni su i napadi na tehnološke kompanije u potrazi za informacijama koje bi olakšale daljnje napade. Operacija Aurora, napad na CARA-u i RSA predstavljaju presedan takvog načina napadanja.

Slika 1. Položaj i broj žrtava APT napada u posljednjih 5 godina
Izvor: mcafee.com

4. Anatomija napada, tehnike i metode

Potpisivanje sadržaja, cerifikati, crne liste i druga sigurnosna rješenja koja zahtijevaju određenu razinu znanja o mogućim prijetnjama ne funkcioniraju u borbi protiv prilagodljivih napadača. Uobičajene metode zaštite ne uspijevaju spriječiti krađu podataka. Napredni napadači iskorištavaju takve sigurnosne propuste.

Današnji APT napadi imaju sljedeća obilježja:

- upotreba zlonamjernih programa (eng. *malware*) za ustrajne napade,
- napadi su motivirani politički ili financijski,
- napadi uključuju stvarne osobe ili skupinu ljudi koja napada određenu organizaciju,
- napadačima je cilj krađa podataka iz računalne mreže organizacije,
- ti se napadi veoma razlikuju od običnih masovnih zaraza crvima ili trojanskim konjima.

Napadači koriste sve alate koje imaju na raspolaganju u svoju korist. To uključuje izradu novih zlonamjernih programa uz pomoć posebnih alata. Takvi programi mogu izbjeći otkrivanje uobičajenim antivirusnim alatima. Osim toga, napadači često iskorištavaju propuste u korisničkim programima (primjerice PDF čitači, Flash, *phishing* na društvenim mrežama).

Kod ciljanog napada, pojedinac ili skupina pokušavaju dobiti pristup točno određenoj, jedinstvenoj mreži. Dakle, napad se mora prilagoditi specifičnom okruženju. Čest je slučaj da se zaposlenike organizacije napada posebno prilagođenim oblikom *phishing* napada. Sve zlonamjerne programe koji se koriste izradila je ta skupina ljudi, posebno za napad na određenu mrežu te oni ne postoje ni u jednoj bazi podataka antivirusnih programa. Stoga tradicionalni antivirusni programi nisu pogodni za zaštitu od takvih napada.

U skoro svim slučajevima napadač želi zadržati vezu s mrežom kojoj je dobio pristup kroz dulje vremensko razdoblje. To je ujedno i njegova glavna slabost. Što dulje napadač ostane u mreži, veća je vjerojatnost da će biti otkriven. Ključni element obrane je, dakle, rano otkrivanje.

Što dulje napad ostane neotkriven veća je vjerojatnost da će važni podaci biti ukradeni ili izgubljeni. Mnogi napadači kradu podatke kroz dulje vremensko razdoblje. Rano otkrivanje pomoći će ublažiti štetu.

4.1. Kada je napad APT?

Ovo je vrlo važno pitanje. Ciljani napadi zahtijevaju više resursa za istraživanje od običnih zaraza zlonamjernim programima ili *botnet* mreža. Većina sigurnosnih timova različitih organizacija su premali da bi istražili svaku sumnjivu aktivnost na mreži. Osim toga, sigurnosni timovi često provode više vremena rješavajući probleme običnih zaraza zlonamjernim programima tako da ciljani napadi izmiču otkrivanju. Otkrivanje je li neki napad ciljan ne postaje kritična točka u sprječavanju APT napada. Jednom kad su otkriveni ciljani napadi, resursi sigurnosnih timova usmjeravaju se na njih.

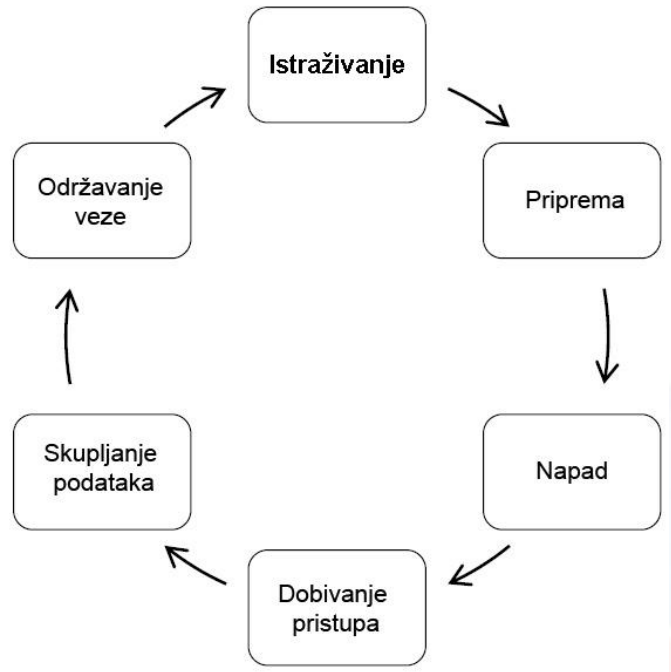
Otkrivanje ciljanih napada ne mora biti složeno. Ne postoje neka posebna pravila za ciljane napade osim prisutnosti stvarne osobe koja obavlja interakciju s mrežom napadnute organizacije. Različiti stručnjaci s područja informacijske sigurnosti imaju različite kriterije prema kojima određuju je li neki napad APT ili ne, no jedan od boljih pristupa je: ako je napad ciljan, može ga se tretirati kao APT. Za većinu organizacija ovo je dovoljan kriterij.

Važno je zapamtiti da APT napadi nisu trivijalni. Na drugom kraju mreže nalazi se osoba koja može svoje metode prilagoditi svakoj protumjeri koju neki sigurnosni tim poduzme. Te metode uključuju ispitivanje vatrozida, ručno inficiranje računala, krađu lozinki, skrivanje komunikacije, zaobilaženje otkrivanja antivirusnim alatima i korištenje antiforenzičkih tehnika.

4.2. Anatomija APT napada

U tablici 1 vidi se da je najčešće upotrebljavani vektor napada socijalni inženjering, odnosno *phishing*, često kombiniran s *zero-day exploit* programima. APT napad tipično napreduje kroz nekoliko faza. Iako nisu čvrsto pravilo te se faze mogu očekivati kod većine napada jer su dio

procesa iskorištavanja propusta. Važno je primijetiti da nakon faze napada još nije došlo do gubitka podataka iako je napadač dobio pristup mreži. Nakon napada i dobivanja pristupa mreži, napadač je izložen i ranjiv. To je moguće iskoristiti za otkrivanje napadača. U nastavku je prikazana anatomija APT napada (slike 2 i 3) sličnog napadu izvedenom na kompaniju EMC. Pojedine faze napada vidljive su na slici 2. Napad se odvijao početkom 2011. godine.

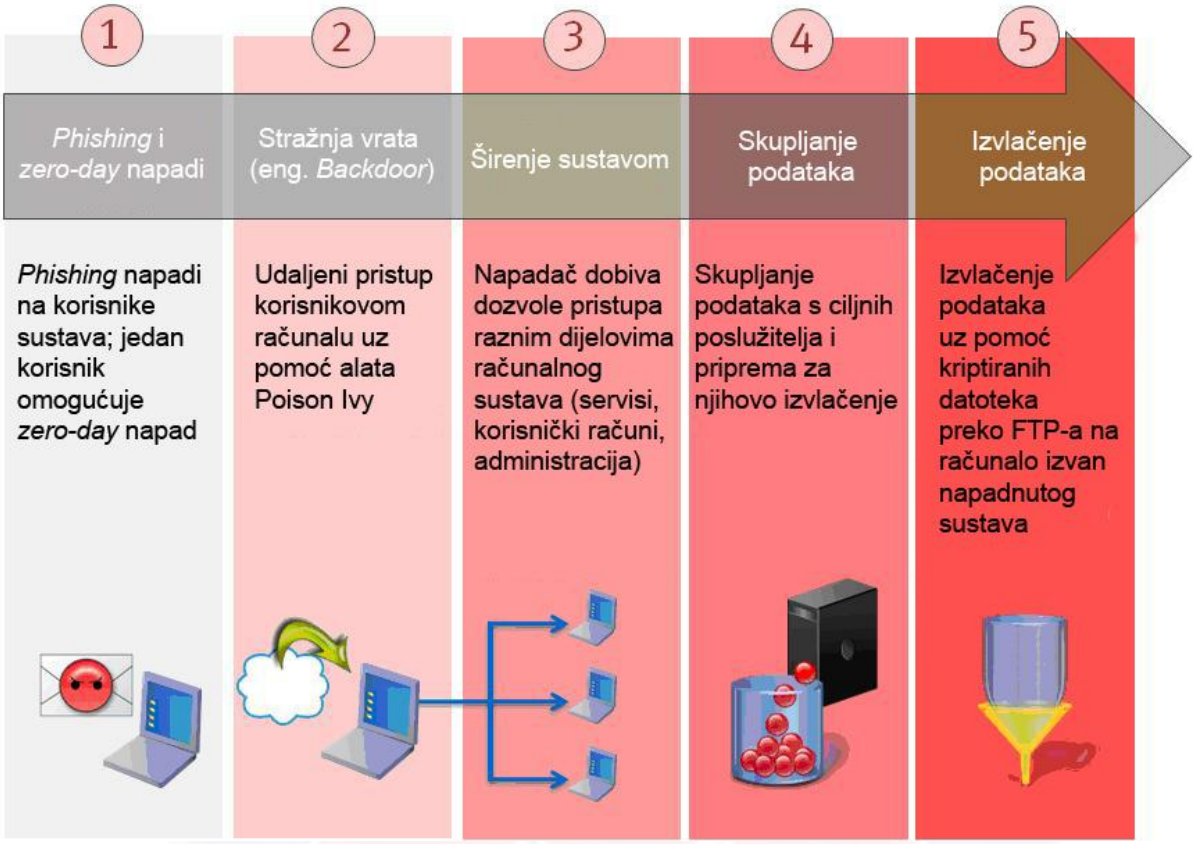


Slika 2. Faze APT napada
Izvor: rsa.com

1. **Istraživanje** - Napadač pasivno sakuplja informacije o žrtvi s ciljem određivanja najbolje metode napada. To može obuhvaćati istraživanje smještaja ureda i računala, društvene mreže (jedan od najvažnijih izvora informacija), web stranice kompanije, tehnologije koje organizacija koristi, načine i sredstva komunikacije (između ureda, s klijentima, nabavom i dioničarima), hijerarhijsku strukturu kompanije, zaposlenike i njihove osobne informacije, kontakte itd.
2. **Priprema** - U ovoj fazi napadač se priprema za napad. On razvija i ispituje prikladne alate i metode za ciljani napad na žrtvu. To može uključivati skeniranje mreže u cilju prepoznavanja slabosti i propusta, pisanje i pribavljanje zlonamjernog koda, izradu zlonamjernih poruka elektroničke pošte (lakovjerni korisnici mogu odabrati poveznicu ili otvoriti dokument koji im šalje kontakt s društvene mreže), odabir adrese elektroničke pošte za slanje zlonamjernih poruka, pribavljanje potrebnih uređaja (primjerice vanjskih memorijskih jedinica), odabir infrastrukture za upravljanje napadom (poslužitelji pod napadačevim nadzorom, skripte za nadziranje, domene registrirane pod lažnim imenom), postavljanje potrebnih korisničkih računa (primjerice za poruke elektroničke pošte, registraciju domena i web prostora) i ispitivanje. Kod naprednijih napada koristi se čitav niz tehnika koje uključuju trojanske konje, *backdoor* servise, posebno oblikovane dokumente koji sadrže zlonamjerni kod, čak i ubacivanje špijuna u organizaciju. U ovoj fazi otkrivanje napadača je vrlo malo vjerojatno.
3. **Napad** - Napadač pokreće napad i traži znakove uspješnog proboja ili neuspjeha. Napad se obično izvodi uz pomoć dokumenta-zamke (dokument s ugrađenim zlonamjernim kodom koji se pokreće kad korisnik otvori dokument) koji se korisniku dostavlja kao privitak *phishing* poruke elektroničke pošte. Osim toga, *phishing* poruke mogu sadržavati i URL poveznice na zlonamjeran sadržaj koji uzrokuje iskorištavanje web preglednika. Zaraziti se može uz pomoć vanjskih uređaja (memorijski štapići, kamere) koji sadrže zlonamjeran kod koji se pokreće kod priključivanja uređaja na računalo. U najgorem slučaju, *backdoor* servisi mogli bi biti instalirani na računala koja organizacija naručuje za svoje potrebe (iako se to čini malo vjerojatno, postoje dokazi o prodaji unaprijed

zaraženih uređaja od proizvođača iz Kine). Mobilni uređaji postaju kritična točka za infekcije. Tim je uređajima često dopušteno da se prijavljuju i odjavljuju s mreže po volji vlasnika. Dok su izvan mreže, te je uređaje moguće zaraziti i upotrijebiti ih za pokretanje *backdoor* servisa jednom kad se ponovno prijave u mrežu organizacije. Kako se na mobilnim uređajima sve češće koriste aplikacije za pristup društvenim mrežama, mobilni uređaji postaju posebno ranjiva točka organizacije. Akcije ove faze napada uključuju: udaljeno spajanje na poslužitelj u vlasništvu organizacije s ciljem iskorištavanja propusta, podmetanje zaraženih medija, slanje *phishing* poruka (ako je moguće s povratnom informacijom), nadziranje infrastrukture za upravljanje napadom u potrazi za odgovorima od žrtve, pokušaje spajanja na potencijalno zaraženo računalo i čekanje odgovora. Općenito, ova je faza napada većinom uspješna zbog nedostatka sigurnosnih mehanizama na strani organizacije. Kao što je već spomenuto, antivirusni alati ne mogu zaustaviti APT napade. Iako postoje i druge mogućnosti, mnoge su preskupe, teško izvedive ili stvaraju previše upozorenja. Za većinu organizacija je čak i upravljanje nadogradnjama programske podrške prevelik izazov.

4. **Dobivanje pristupa** - Jednom kad je napadač uspješno uspostavio vezu s računalnom mrežom organizacije, on pokušava ustanoviti gdje se nalazi u mreži. Napadač najčešće upravlja zaraženim računalom kroz naredbeni redak. Tada se napadač kreće kroz mrežu u potrazi za podacima od interesa, a usput instalira dodatne *backdoor* servise i alate za udaljeno upravljanje (eng. *Remote Administration Tool,* RAT). Obično se koriste različiti oblici *backdoor* programa. Time se osigurava teško uklanjanje iz sustava. Ovo najčešće zahtijeva povratak na korake 2 (priprema) i 3 (napad), prijenos alata i zlonamjernog programskog koda na računalo u mreži, dobivanje većih privilegija, raspoznavanje mreže, identifikaciju ranjivih računala u mreži (na njih se instaliraju *backdoor* servisi). Također, to može obuhvaćati dobivanje pristupa kontroleru domene u potrazi za lozinkama, prikrivanje tragova promjenom dnevnika i zapisa i pristup poslužiteljima datoteka i poruka elektroničke pošte kao pripremu za sakupljanje podataka. Napadač je u ovoj fazi najranjiviji.
5. **Skupljanje podataka** - Jednom kad napadač identificira podatke od interesa, on pokušava skupiti (iz baza podataka, repozitorija, poruka elektroničke pošte ili datoteka) te podatke na jedno računalo i izvući ih iz mreže. To se može učiniti na dva načina: "razbij i zgrabi" (eng. *smash and grab*) - brzo izvlačenje većih količina podataka prije nego je napadač otkriven, ili "polako i prikriveno" - izvlačenje manjih količina podataka kroz dulje vremensko razdoblje.
6. **Održavanje veze** - Nakon što je napadač uspješno uspostavio vezu s mrežom u svrhu skupljanja podataka, on će najčešće pokušati održati pristup mreži kroz dulje vremensko razdoblje. To može uključivati minimizaciju količine zlonamjernih aktivnosti na mreži da bi izbjegao otkrivanje, periodička komunikacija s *backdoor* servisima da osigura njihov ispravan rad i stvaranje promjena po potrebi. Ako upotrebljava automatizirane alate za sakupljanje podataka to može uključivati promjenu parametara pretraživanja, puta za izvlačenje podataka, količine i frekvencije izvlačenja podataka. Održavanje veze uključuje i održavanje posredničke infrastrukture i *callback* domena. Ako napadač ipak izgubi vezu, on se vraća na korake 1 (prepoznavanje) i 2 (priprema) u pokušaju da ponovno dobije pristup.



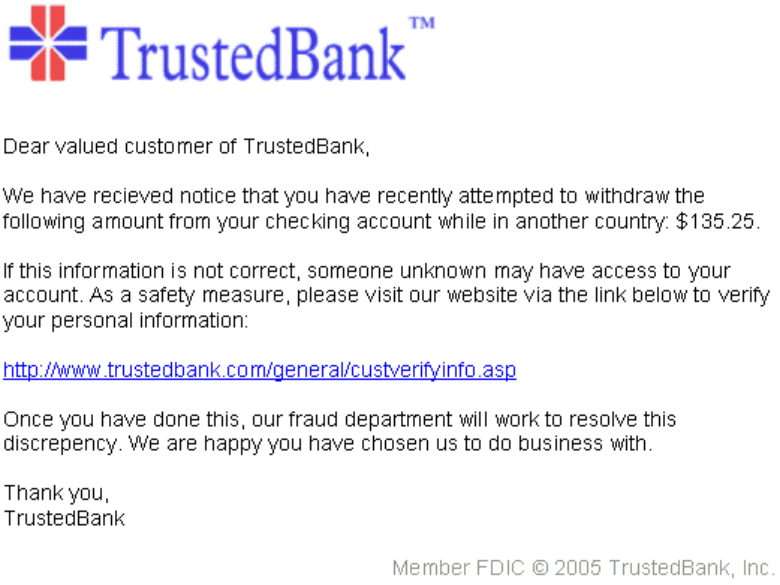
Slika 3. APT napad na tvrtku EMC
Izvor: rsa.com

4.3. Metode i alati

Pri izvođenju napada i za vrijeme interakcije s napadnutom mrežom napadač koristi određen skup metoda i alata za upravljanje zaraženim računalima, pregled mreže te identifikaciju podataka od interesa. Također, on koristi i popratnu infrastrukturu za pristup mreži organizacije koju napada. U sljedećim potpoglavljima slijedi detaljniji pregled nekih metoda i alate koje napadači koriste.

4.3.1. Phishing

Phishing je način dobivanja informacija (primjerice korisničkih imena, lozinki, brojeva kreditnih kartica itd.) oponašanjem subjekata od povjerenja u elektroničkim komunikacijama (slika 4). Obično se izvodi maskiranjem poruka elektroničke pošte i često usmjerava korisnike na lažne web stranice. Takve web stranice izgledaju gotovo identično web stranicama koje žrtva svakodnevno koristi i traže od nje da unese svoje podatke. *Phishing* je tehnika socijalnog inženjeringa koja iskorištava lakovjernost korisnika.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Slika 4. Primjer phishing poruke
Izvor: Wikipedia

4.3.2. Drive-by download

Pojam *drive-by download* ima tri značenja, a sva se odnose na oblik neželjenog preuzimanja podataka s Interneta.

- Preuzimanja koja je žrtva dozvolila, no bez razumijevanja posljedica (preuzimanja koja instaliraju nepoznati ili zlonamjeran program, Java aplet ili ActiveX komponentu).
- Svako preuzimanje koje se odvija bez znanja osobe koja upravlja računalom.
- Preuzimanje bilo koje vrste zlonamjernog programa koje se odvija bez znanja osobe koja upravlja računalom.

Drive-by preuzimanja mogu se dogoditi pri posjetu web stranici, pregledavanju poruke elektroničke pošte ili odabiranju *pop-up* prozora. *Drive-by* instalacija je sličan događaj. Odnosi se na instalaciju (najčešće zlonamjernog) programa bez znanja korisnika.

4.3.3. Backdoor

*S*tražnja vrata (eng. *backdoor*) u računalnom sustavu je metoda zaobilaženja normalne autentifikacije i omogućavanja udaljenog pristupa računalu dok napadač u isto vrijeme pokušava ostati neprimijećen. *Backdoor* dolazi u obliku instaliranog programa ili promjena funkcija operacijskog sustava kao *rootkit*.

4.3.4. Pritajeni *backdoor*

Neki RAT alati se postavljaju kao pritajeni *backdoor*. Tako ostaju u sustavu u neaktivnom stanju tjednima ili mjesecima prije nego pokušaju uspostaviti odlaznu vezu. Takvi "spavajući agenti" služe kao osiguranje u slučaju da je napad otkriven.

4.3.5. RAT alati

RAT (eng. *Remote Administration Tool*) alati su programi koji daju udaljenom "operatoru" nadzor nad sustavom, kao kad ima fizički pristup. Dok se dijeljenje radne površine i

udaljena administracija sustava upotrebljavaju često i legalno, RAT alati se obično povezuju s zlonamjernim i kriminalnim aktivnostima. Zlonamjerni RAT alati obično se instaliraju bez žrtvinog znanja i pokušavaju sakriti svoje djelovanje od korisnika i operacijskog sustava.

Operator upravlja RAT alatom kroz mrežnu vezu. RAT alati omogućuju napadaču sljedeće:

- pregled sadržaja radne površine,
- prijenos uživo ako je računalo opermljeno web kamerom,
- upravljanje naredbenim retkom,
- upravljanje *registryjem,*
- paljenje/gašenje računala,
- prijava/odjava korisnika,
- pregled datoteka,
- i ostale funkcije ovisne o konkretnom alatu.

Glavna im je funkcija davanje pristupa udaljenom računalu. Jedno računalo pokreće "klijentski" program, dok drugo računalo igra ulogu domaćina.

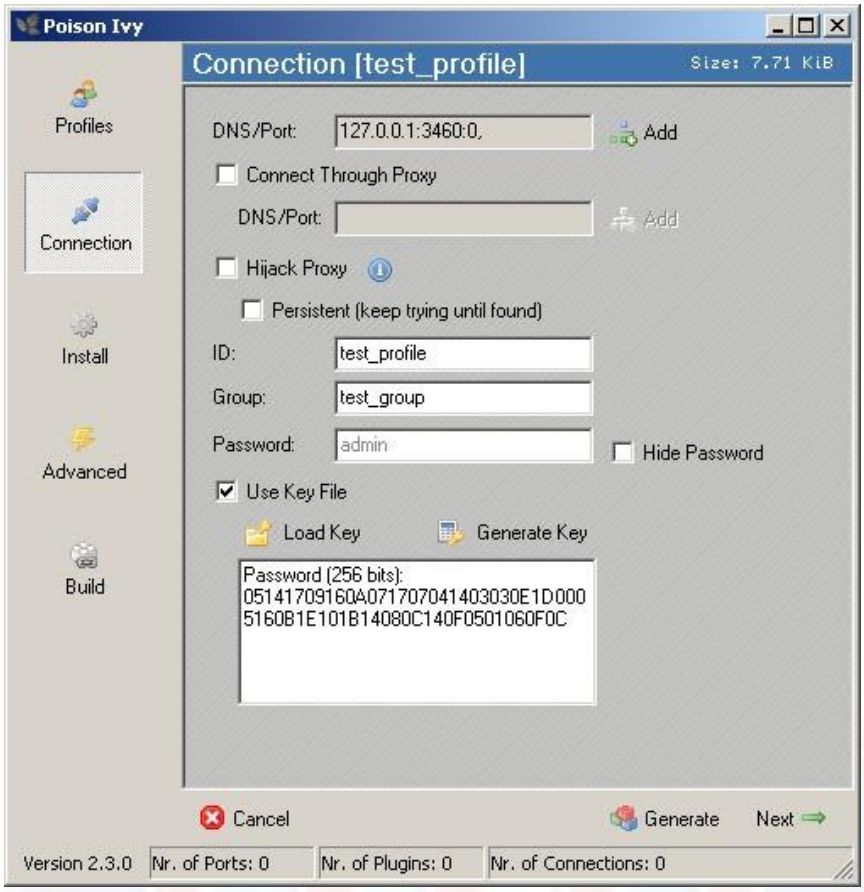
Postoje dvije vrste veza koje uspostavljaju RAT alati između napadača i žrtve: izravna veza i obrnuta veza.

- Izravna veza - Ovaj tip veze moguće je ostvariti jedino ako napadač zna IP adresu računala kojim želi upravljati. Većina vatrozida obično blokira ovaj tip programa. Ipak, iskusni programeri razvili su sofisticirane programe koji zaobilaze često korištene vatrozide.
- Obrnuta veza - Kod ovog oblika veze udaljeno računalo se ponaša kao domaćin za RAT program. RAT-ovi koji koriste ovu metodu uspostavljanja veze imaju sljedeće prednosti:
    - na odlazne se veze obično gleda kao na manje opasne za udaljenog korisnika (žrtvu) jer je žrtva ta koja pokreće postupak preuzimanja RAT programa. Na taj način se izbjegavaju blokade vatrozidima koji se koriste u usmjerivačima.
    - Pošto se udaljeni "domaćin" sam spaja na "administratorovo" računalo, administrator ne mora znati točnu IP adresu domaćina.

Mnogi *backdoor* programi i trojanski konji imaju ugrađene RAT mogućnosti. Često je potrebno na žrtvinom računalu pokrenuti datoteku pod nazivom "server" da bi napadač dobio pristup. Oni se obično šire porukama elektroničke pošte, programima za razmjenu datoteka (eng. *peer-to-peer*, P2P[3]) i preuzimanjima s Interneta i izgledaju kao legitimna datoteka.

Često korišteni RAT alati su: Back Orifice, Bifrost, Bandook RAT, Blackshades Remote Controller, Cerberus RAT, Cybergate, Paradox Remote Administration Tool, Poison Ivy (slika 5), Darkcomet-RAT, Sub Seven, TeamViewer, NetCAR, Netop Remote Control, NetopOnDemand, Netop Mobile & Embedded, Y3k RAT, Optix Pro, LANfiltrator.

[3] Model distribuirane računalne arhitekture u kojem su radni zadaci podijeljeni između više sudionika (svi sa jednakim privilegijama).



Slika 5. Stvaranje veze u RAT alatu Poison Ivy
Izvor: poisonivy-rat.com

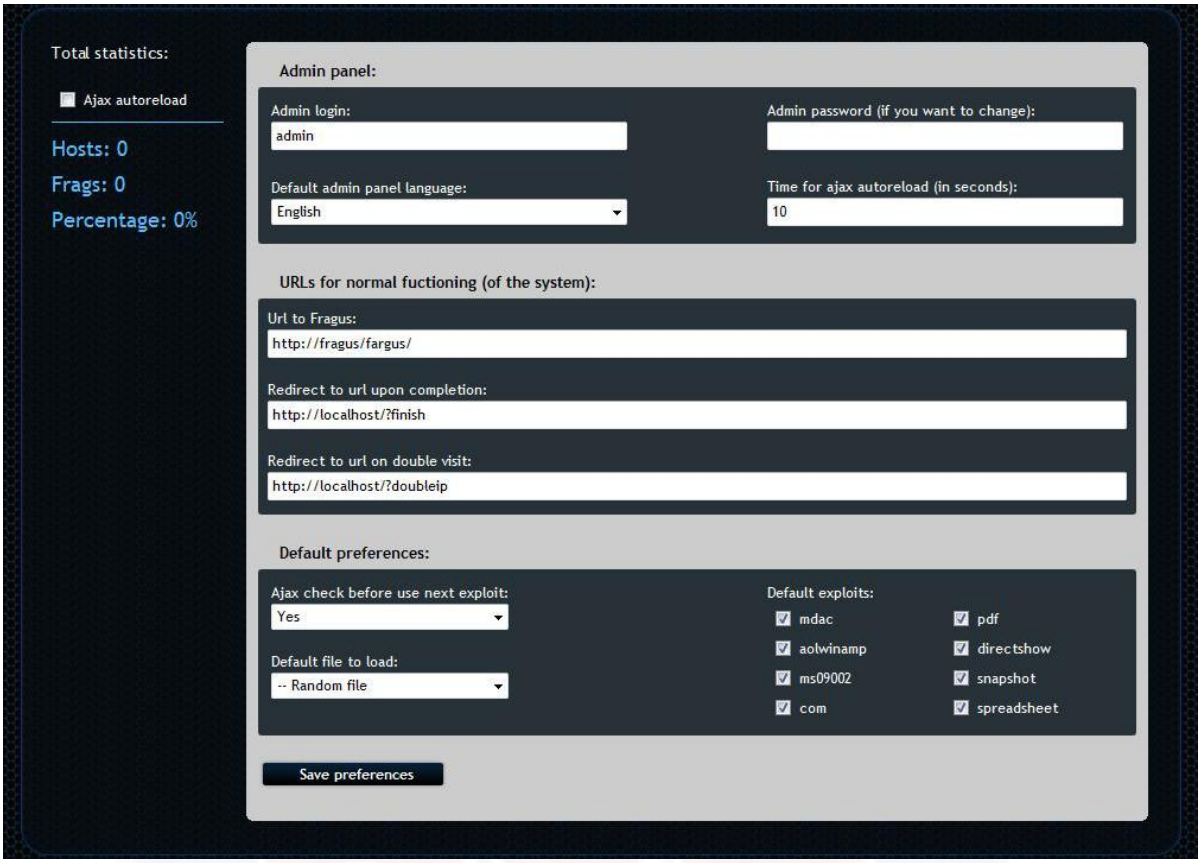
4.3.6. Alati za izradu zlonamjernih programa

Alati za izradu zlonamjernih programa (eng. *malware*) sadrže skripte koje pojednostavljuju i automatiziraju proces zaraze računala. Najčešće dolaze u obliku web aplikacija (slika 6) i koriste web tehnologije kao što su PHP: hipertekstni procesor (eng. *PHP: Hypertext Preprocessor*) i MySQL. Omogućavaju napadačima iskorištavanje propusta u popularnim programima (primjerice Internet Explorer, Adobe Acrobat, Flash). Alati se instaliraju na web poslužitelj i povezuju s bazom podataka gdje spremaju zabilješke i izvještaje. Za njihovo korištenje je obično potreban minimum tehničkog znanja. Zaraza i korištenje zlonamjernih programa proizvedenih takvim alatima obično se odvija u nekoliko faza:

- stvaranje zlonamjerne web stranice automatiziranim alatima,
- masovno slanje poruka elektroničke pošte (*spam*, *phishing*) u svrhu sakupljanja posjetitelja zlonamjernih web stranica,
- zaraza računala posjetitelja trojanskim konjima koji iskorištavaju brojne propuste,
- korištenje trojanskih konja za dobivanje pristupa zaraženim računalima.

Alati za izradi zlonamjernih programa se redovito nadograđuju i dobivaju nove mogućnosti iskorištavanja propusta, jeftini su ili besplatni i anonimni i široko dostupni.

Neki često korišteni alati su: WebAttacker, MPack, Fiesta, Eleonore, Siberia, Fragus, CrimePack, Neosploit, LuckySploit, Yes Toolkit.



Slika 6. Administracijska ploča alata Fragus
Izvor: securitybananas.com

4.3.7. Skeniranje mreže

Skeniranje mreže obično počinje otkrivanjem raspona IP adresa i pojedinih sustava unutar tih raspona. Jednom kad otkrije aktivne sustave, napadač ih skenira u potrazi za otvorenim priključnicama (eng. *port*) i pokušava otkriti servise koji slušaju pojedinu priključnicu. Nakon što stvori mapu mreže, napadač pokušava otkriti propuste u sigurnosnoj zaštiti koje bi mogao iskoristiti za napad.

- Rasponi IP adresa organizacije - dobivaju se jednostavnim istraživanjem, krađom informacija sustava imena domena (eng. *Domain Name System*, DNS[4]) ili skeniranjem širih raspona IP adresa. Alati za praćenje puta podataka također mogu biti korisni za stvaranje mape mreže.
- Pronalaženje sustava - nakon što su otkriveni rasponi adresa potrebno je pronaći sustave unutar mreže koji odgovaraju na upite izvana. Ovdje se koriste alati poput *pinga*.
- Priključnice i servisi - sustavima koji odgovaraju na upite skeniraju se priključnice i identificiraju servisi koji slušaju na njima. Ovdje je obavezno odrediti vrstu protokola i tip servisa koji se koristi na određenoj priključnici.
- Inačice servisa - veze sa servisima obično nose oznake koje sadrže informacije o vrsti i inačici servisa. Kad su te informacije dostupne, napadač može iskoristiti točno određene sigurnosne propuste svojstvene pojedinim servisima.
- Određivanje operacijskog sustava - slanjem posebno oblikovanih paketa za ispitivanje protokola i servisa moguće je identificirati operacijski sustav koji pokreće računalo unutar ciljne mreže.

[4] Sustav imenovanja izgrađen na distribuiranim bazama podataka za bilo koji resurs spojen na Internet ili privatnu mrežu.

- Skeniranje u potrazi za propustima - nakon što je dobavio sve informacije o sustavu, napadač skenira sustav u potrazi za jedinstvenim propustima koje bi kasnije mogao iskoristiti.

4.3.8. Napadi na bežičnu mrežu

Zbog brzog razvoja tehnologije na tom području, tehnike napada na bežične mreže mijenjaju se vrlo brzo. Slijedi pregled nekih područja koja su izravno uključena u tehnike napada:

- Istraživanje - većina napada na bežične mreže započinje nekom vrstom istraživanja. Obično se radi o hvatanju paketa podataka.
- WEP (eng. *Wired Equivalent Privacy*) - ovaj sigurnosni protokol više nije siguran ni u kojem obliku. Kod neki starijih inačica moguće je probiti zaštitu sa samo dva paketa. Novije inačice zahtijevaju ubacivanje paketa s ciljem probijanja zaštite. U svakom slučaju postupak je toliko ubrzan da ne traje dulje od desetak minuta.
- WPA (eng. *Wi-Fi Protected Access*) - skupina protokola koji nude viskou razinu zaštite bežičnih mreža. Međutim, mogu biti ranjivi na neke vrste napada riječnicima.
- Bluetooth - ovaj oblik bežičnih komunikacija često se oslanja na kratke udaljenosti kao sigurnosnu zaštitu. Međutim, to je pogrešno razmišljanje. Bluetooth signal moguće je presresti na udaljenosti od preko jednog kilometra. U trenutnom obliku Bluetooth je vrlo nesiguran oblik bežičnih komunikacija.

4.3.9. Napadi putem korisničkih programa

Napadi putem korisničkih programa usmjereni su na sigurnosne propuste u programima koje zaposlenici neke organizacije svakodnevno koriste. Ovo je područje od velike važnosti za napadače jer pokriva velik broj programskih alata i protokola koje oni koriste, a koji imaju neotkrivene propuste. Primjerice:

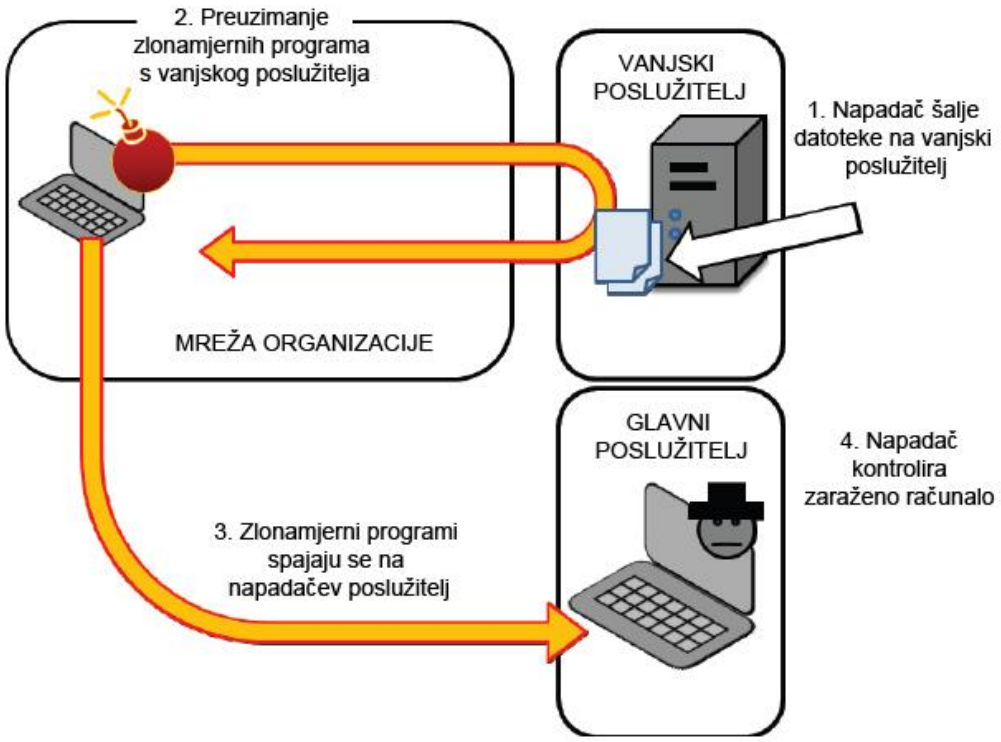
- ubacivanje SQL (eng. *Structured Query Language*) koda - omogućuje pregled i mijenjanje podataka koji se nalaze u bazama podataka, a nisu javno dostupni. Napadači najčešće koriste polja za unos podataka koja nemaju odgovarajuću provjeru unesenih podataka.
- PHP - ovaj često upotrebljavani jezik za izradu web aplikacija ima mnogobrojne propuste. Posebno su opasni propusti u skriptama koje korisnicima omogućuju izravan unos koda.
- XSS (eng. *Cross-site Scripting*) - ubacivanje izvršivog (najčešće JavaScript) koda u kod web stranice koja prikazuje podatke koje unose korisnici.
- VoIP (eng. *Voice over IP*) - VoIP programi često sadrže mnogo propusta koji omogućuju presretanje i ubacivanje paketa sa zlonamjernim sadržajem.
- Ranjivosti raznih protokola kojima se koriste klijentski programi (*File Transfer Protocol*, *Secure Shell*, *Domain Name System*, *Simple Mail Transfer Protocol* itd.).

4.3.10. Nadzor i upravljanje

Da bi omogućili ustrajan pristup, napadačevi RAT programi, koji se nalaze na računalima organizacije, će se periodički spajati na vanjski udaljeni poslužitelj za upravljanje i nadzor (eng. *Command and Control* - C&C). Taj C&C poslužitelj je pod napadačevim nadzorom. Odatle, napadač može slati naredbe i uspostaviti pristup mreži kroz naredbeni redak. Također, može se koristiti udaljeni pristup radnoj površini (terminal).

Vanjski poslužitelji za upravljanje su često lakovjerne žrtve (zaraženi web poslužitelj - slika 7). Zaraženi poslužitelj se tada koristi za podmetanje zlonamjernih datoteka i slanje naredbi sa zlonamjernim programima instaliranim na računalima organizacije. Ti programi stvaraju više odlaznih veza. Mnogo se puta radi o HTTPS (eng. *Hypertext Transfer Protocol Secure*)

vezama. Tada je teško blokirati promet vatrozidom ili ga proučiti IDS (eng. *Intrusion Detection System*) opremom. Mnogi *backdoor* servisi konfigurirani su da uspostavljaju veze s više C&C poslužitelja. Napadači obično koriste više DNS adresa što im omogućuje lakše zaobilaženje filtriranja ako budu otkriveni.



Slika 7. Tipični C&C scenarij
Izvor: McAfee

4.3.11. Promjerna podataka i konfiguracija

Jedan način koji bi napadač mogao iskoristiti za ometanje rada organizacije i otežavanje otkrivanja napada je promjena podataka. Ovisno o namjeri podaci se mogu mijenjati otvoreno (prisiljava sigurnosne timove na reakciju, koristi se za diskreditaciju podataka ili organizacije) ili prikriveno (ometanje uobičajenih poslova napadnute organizacije).

Napadač također može promijeniti postavke sustava i uređaja. Obično se to radi s ciljem:

- onemogućavanja rada sustava stvaranjem niza problema koje sigurnosni timovi moraju rješavati,
- stvaranja ozbiljnih problema u sustavu velikim promjenama konfiguracija,
- potpunog preuzimanja sustava i ukidanja pristupa sustavu svim korisnicima.

4.3.12. Napadi uskraćivanjem usluge

Napadi uskraćivanjem usluge (eng. *Denial of Service*, DoS) su napadi dizajnirani za onemogućavanje korištenja određenih informacijskih resursa. Oni obuhvaćaju zagušenje mreže prometom, gašenje nekih mrežnih uređaja (računala, usmjerivača, mostova), promjene mrežnih postavki i drugo. Iako postoje brojne mogućnosti, većina DoS napada koristi poplavljivanje uređaja mrežnim prometom. DoS napadi mogu nanijeti veliku štetu organizaciji. Borba protiv takvih napada uglavnom znači pronalaženje izvora napada i njegovo gašenje.

Distribuirani DoS napadi (DDoS) su DoS napadi s više izvorišnih točaka. Kod takvih je napada teško otkriti izvore i zaustaviti ih. DoS i DDoS napadi pokrenuti iz unutrašnjosti organizacije su još razorniji.

4.3.13. Tajnost i praćenje događaja

Tehnike skrivanja mogu napadaču pomoći da prikrije:

- svoju prisutnost u sustavu,
- kanale za nadzor i upravljanje,
- sakupljanje informacija,
- izvlačenje podataka.

Tehnike skrivanja dijele se u dvije glavne kategorije:

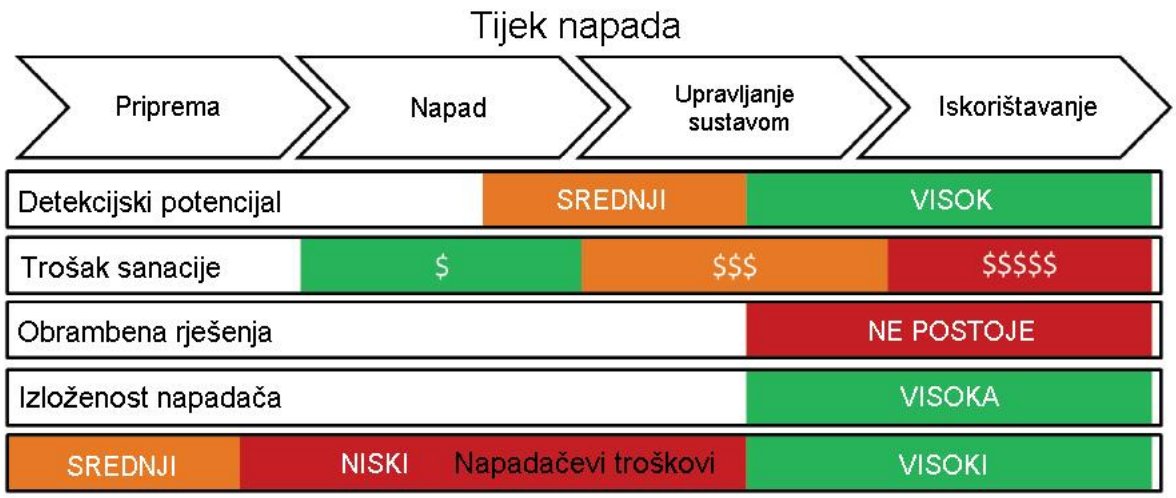
- korištenje *rootkita* za skrivanje datoteka, direktorija i procesa (ubacivanjem zlonamjernog koda u legitimne procese),
- skrivanje komunikacijskih kanala ubacivanjem informacija u protokolne jedinice podataka na mjesta gdje se ne upisuju podaci uz korištenje kriptiranja.

Praćenje događaja uključuje znanje o tome gdje se napadač nalazi i što se oko njega događa što može biti vrlo teško otkriti. U takvim se situacijama koriste analize protokola, metoda obrane od napada, virutalnih računala i otkrivanje zamki koje se koriste u svrhu otkrivanja neovlaštenog pristupa.

5. Rizici i metode zaštite

Postoji nekoliko posebno opasnih područja na kojima su interne mreže različitih organizacija posebno ranjive i koje napadači redovito iskorištavaju u svoju prednost (slika 8).

- Male mogućnosti otkrivanja: Detekcijski potencijal odnosi se na količinu vidljivosti napadačevog djelovanja. U prvoj fazi napada (sakupljanje informacija) napadač ima vrlo nisku razinu izloženosti. Za vrijeme skeniranja mreže izloženost je veća, no i dalje nedovoljna za otkrivanje napada. Skeniranje mreže je postalo vrlo uobičajeno i često, tako da se najčešće zanemaruje. Međutim, u kasnijim fazama napada, mogućnosti otkrivanja napadača su mnogo veće.
- Rast troškova saniranja štete: Što je napadač dulje u sustavu, veća je vjerojatnost da će se dogoditi značajniji gubici podataka. To najčešće znači ogromne štete za organizaciju kojoj su podaci ukradeni. Također, što je napadač dulje u sustavu, zarazit će više računala i nanijeti više štete samom sustavu. To će rezultirati većim troškovima popravka sustava. Konačno, gubitak povjerenja klijenata može biti najveća nanesena šteta.
- Nedostatak sredstva obrane: Ne postoji mnogo komercijalnih proizvoda za otkrivanje napada nakon što je napadač već dobio pristup mreži. Sigurnosni timovi, ako postoje, služe se alatima vlastite izrade koji se teško prilagođavaju različitim platformama i nemaju odgovarajuću podršku.
- Prilagodljivost i niski troškovi napadača: Većina komecijalno dostupnih rješenja fokusiraju se na otkrivanje napada u fazi infekcije. Problem kod takvog pristupa je u tome što napadač ima vrlo velik broj mogućnosti zaobilaženja takvog oblika zaštite. Također, napadač je u prednosti jer može isti propust iskoristiti na više načina i na različitim žrtvama. U praksi, područje koje je "najzaštićenije" je ono na kojem napadač ima najveću prednost.



Slika 8. Razine troškova, izloženosti i detekcijskog potencijala kroz pojedine faze napada Izvor: HBGary

Povećanje sigurnosti, razine otpornosti i sprječavanje APT napada moguće je izvesti pridržavajući se nekih osnovnih sigurnosnih mjera:

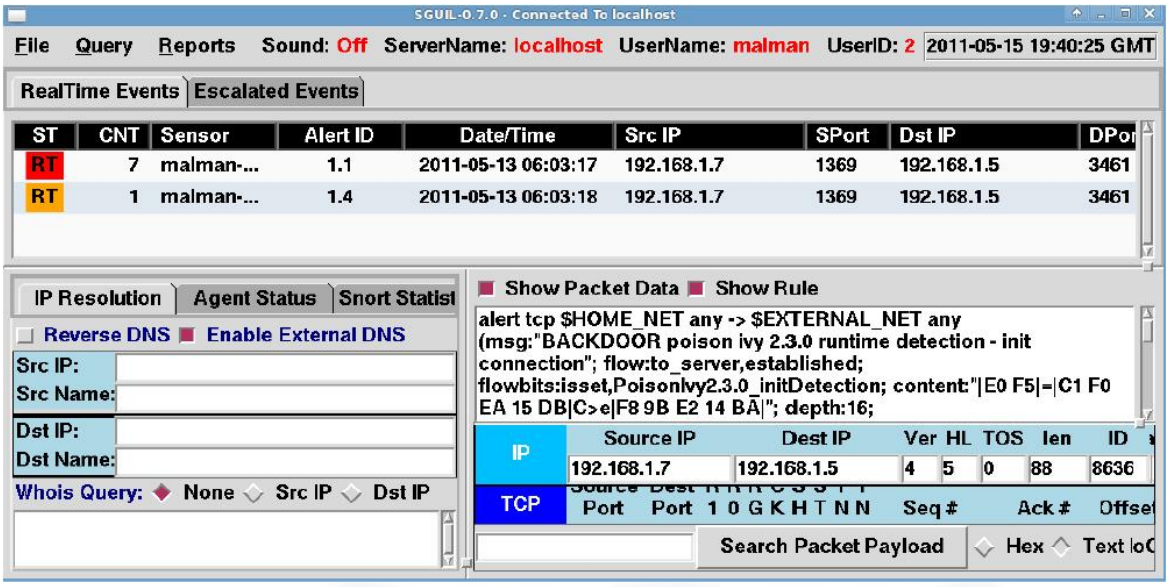
- sigurnosni sustavi orijentirani na informacije - uvođenje sigurnosnih sustava koji posebnu pažnju pridaju zaštiti informacija; takva se zaštita izvodi na nekoliko slojeva, a posebno osjetljivi podaci spremaju se na računala bez pristupa mreži ili unutar posebno odvojene mreže,
- ispravljanje propusta - redovita instalacija zakrpi za propuste otkrivene u programskoj podršci koja se koristi (posebno za operacijske sustave, web preglednike i preglednike dokumenata),
- ograničenje korištenja - uvođenje strogih ograničenja korištenja sustava (ograničenja pristupa, pisanja i izvođenja programskog koda),

- edukacija korisnika - edukacija korisnika o opasnostima socijalnog inženjeringa i *phishing* poruka elektroničke pošte, poticanje korisnika na redovito izvještavanje o takvim porukama,
- ograničenje pristupa mreži - ograničiti žičani, bežični i udaljeni pristup mreži na točno određena računala,
- edukacija mrežnih administratora - osigurati da mrežni administratori imaju potpuna znanja o topologiji mreže, smještaju svih računala, računalne i mrežne opreme u svrhu uvođenja potpunije zaštite,
- nadzor vanjskih memorijskih jedinica - uvesti strogi nadzor vanjskih memorijskih jedinica (npr. USB *flash* memorija) koje se koriste na računalima organizacije; uvesti obavezno kriptiranje podataka,
- analiza proboja zaštite - provoditi analizu proboja zaštite mreže u svrhu otkrivanja zlonamjernih aktivnosti,
- nadzor pristupa - uvesti TFA (eng. *two-factor authentication*) gdje je god moguće (posebno kod VPN pristupa); ograničiti korisnički pristup; poticati upotrebu dobrih lozinki; nadzirati zapise o pristupu; dodijeliti dozvole pristupa,
- SPF (eng. *Sender Policy Framework*) - koristiti SPF kao pomoć u otkrivanju zlonamjernih poruka elektroničke pošte.

Pošto se APT napadi oslanjaju na udaljeni pristup i upravljanje, ponekad je moguće otkriti mrežne aktivnosti povezane s udaljenim upravljanjem, te ih analizom odlaznog prometa omesti ili onemogućiti. Za te namjene upotrebljavaju se neka programska rješenja otvorenog koda.

- Snort - sustav za otkrivanje i sprječavanje upada u mrežu (eng. *Intrusion Detection System* - IDS). Koristi vlastiti protokol i potpisivanje, kao i mogućnost otkrivanja anomalija.
- Scapy - program za upravljanje paketima podataka. Može stvarati pakete za različite vrste protokola, upravljati njima i uspostaviti mrežnu komunikaciju. Korisiti se u svrhu otkrivanja napada.
- Sustav otvorenog koda za otkrivanje upada (eng. *Open Source Host-based Intrusion Detection System*, OSSEC) - IDS otvorenog koda. Posjeduje alate za analizu zapisa, provjeru datoteka, nadzor *registryja*, otkrivanje *rookita*, te napredne mogućnosti upozoravanja korisnika. Kompatibilan je s mnogim operacijskim sustavima.
- Splunk - alat za pretraživanje, nadzor i obavještavanje s mogućnostima analize zapisa s različitih mrežnih uređaja.
- Sguil (slika 9) - alat za nadzor u stvarnom vremenu, pregled podataka o sjednicama i hvatanje paketa podataka.
- ModSecurity - vatrozid za web aplikacije.

Ovi se alati mogu koristiti za neke oblike otkrivanja APT napada nadzorom mrežnog prometa.



Slika 9. Upozorenje o mogućem napadu u alatu SGUIL
Izvor: SANS

6. Analiza napada na SK Communications

Krajem srpnja 2011. godine kompanija SK Communications (slika 10) objavila je kako je bila metom napada koji je rezultirao krađom osobnih podataka više od 35 milijuna njihovih korisnika. Otuđeni podaci uključivali su one o CyWorld i Nate korisnicima koji su bili pohranjeni u bazama podataka kompanije SK Communications. CyWorld je najveća društvena mreža Sjeverne Koreje, a Nate popularni web portal. Najvjerojatnije su oboje bili napadnuti APT napadom.

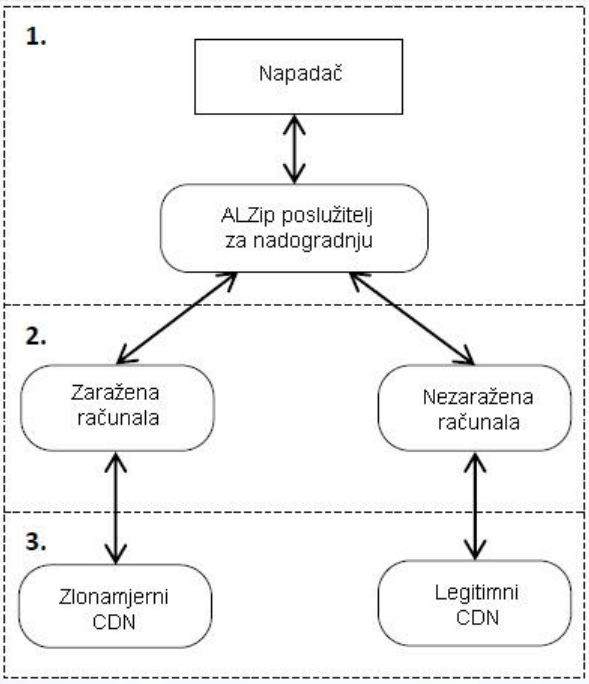
Slika 10. Logo tvrtke SK Communications
Izvor: SK

Napadači su prvo napali poslužitelj koji se koristio za nadogradnju programske podrške kompanije SK Communications. Napadači su prilagodili poslužitelj tako da su računala kompanije SK Communications preuzela datoteku za nadogradnju zaraženu trojanskim konjem. Između 18. i 25. srpnja napadači su postavili C&C poslužitelje, te kroz njih upravljali i nadzirali zaražena računala. To je uključivalo i prijenos alata koje su pohranjivali na web stranicama jedne tajvanske izdavačke kuće čije su poslužitelje već prije napali.

Ukradeni podaci uključivali su imena, brojeve telefona, kućne adrese, adrese elektroničke pošte, datume rođenja, podatke o spolu, korisnička imena i lozinke.

6.1. Program za nadogradnju

Poslužitelj za nadogradnju kojeg su napadači koristili kao početnu točku za svoje napade usmjerene protiv SK Communications bili su poslužitelji ESTsoft ALZip. Napadači su, koristeći IP adrese iz Kine, dobili pristup poslužitelju ALZip i na njega prenijeli zlonamjerni kod (slika 11). Kad su računala SK Communications zatražila nadogradnju zlonamjerni je kod usmjerio računala na nadogradnju zaraženu trojanskim konjem koja se nalazila na CDN (eng. *Content Delivery Network*) mreži napadača. Trojanski konj iskorištava propust programa ALCMUpdate.exe koji se upotrebljava za pronalaženje nadogradnji. Taj je propust dopustio učitavanje zloćudne DLL (eng. Dynamic Link Library) datoteke. To je dovelo do instalacije zlonamjernih programa na računalo koje je zatražilo nadogradnju. Zaraženo je više od 60 računala.



Slika 11. Prvi dio napada na SK Communications
Izvor: Command Five

6.2. Zaražena računala

Nakon što je ALZip program za nadogradnju (ALCMUpdate.exe) preuzeo zaraženu nadogradnju, ona je zarazila računala zloćudnim programom Backdoor.Agent.Hza. *Backdoor* je napadaču omogućio spajanje na zaražena računala. Zaražena su računala komunicirala sa C&C poslužiteljem na IP adresi 116.127.121.41, smještenim u Sjevernoj Koreji, na TCP (eng. *Transmission Control Protocol*) priključnici 8080.

Datoteke preuzete na zaražena računala nalazile su se na adresi www.cph.com.tw/act (web stranica pripada tajvanskoj izdavačkoj kući). Najvjerojatnije je da su web poslužitelji izdavačke kuće bili napadnuti bez znanja vlasnika, te su napadačima koristili kao spremište alata koje su preuzimala zaražena računala.

6.3. Pristup bazi podataka

Nakon tjedan dana sakupljanja podataka, napadači su bili spremni za pristup bazama podataka. Dana 26. srpnja 2011. godine, koristeći informacije koje su pribavili, zajedno sa zlonamjernim programom nateon.exe, dobili su pristup bazama podataka Natea i CyWorlda. Krađa informacija se nastavila i sljedeći dan.

6.4. RAT

Nateon.exe instalira RAT (eng. *Remote Administration Tool*) nazvan winsvcfs.dll. On prilagođava legitimni proces svchost.exe da pokreće RAT svaki put kad se računalo pokrene. Jednom kada je winsvcfs.dll instaliran, nateon.exe se uklanja. Prema informacijama sadržanim u nateon.exe, zloćudni program korišten na računalima kompanije SK Communications konstruiran je 27. rujna 2010. godine u 01:17:04 - više od 6 mjeseci prije samog napada.

RAT ne samo da može ući u bazu podataka i slati upite, već može i pristupiti mrežama na koje su zaražena računala spojena, podešavati i stvarati nove mrežne veze, mijenjati *registry*, onemogućiti radnu površinu računala, upravljati procesima i uslugama, preuzimati datoteke,

stvarati nove datoteke, stvarati slike ekrana, gasiti i ponovo pokretati računalo, odjaviti korisnika itd.

6.5. Infrastruktura

Nazivi domena prevode se u IP adrese korištenjem protokola DNS. On prevodi pojedinu domenu u jedinstvenu IP adresu koju zaražena računala mogu koristiti za pronalaženje i komunikaciju s C&C poslužiteljem. C&C poslužitelji su obično zahtjevniji za postavljanje i održavanje nego domene koje se koriste za uspostavljanje komunikacije s njima. Nije neobično da više domena označava isti C&C poslužitelj.

U vrijeme napada domena nateon.duamlive.com pokazivala je na adresu 121.78.237.135, no kasnije je promijenjena da pokazuje na lokalnu *loopback* adresu (127.0.0.1). Napadači preusmjeravaju domene na *loopback* adresu kad ne žele slati naredbe zaraženim računalima koja koriste te domene. Domena ro.diggfunny.com pokazivala je na sjevernokorejsku IP adresu 116.127.121.109. Ta je adresa u istom rasponu kao i adresa koja je bila korištena za ATLools C&C poslužitelj (116.127.121.0/24). Navedeni raspon adresa u nadležnosti je sjevernokorejskog ISP-a (eng. *Internet Service Provider*) Hanaro Telecom. Također je moguće da su napadači kupili web prostor za postavljanje C&C poslužitelja umjesto napadanja legitimnih poslužitelja. Druge adrese u tom rasponu (116.127.121.0/24) također su povezane sa zlonamjernim aktivnostima.

7. Budućnost

S obzirom na rastuće trendove napada na velike kompanije i rastuću popularnost virtualizacije, vrlo je vjerojatno da će u budućnosti i kompanije poput VMware Inc., Oracle i ostalih postati žrtvama APT napada. Ako se, primjerice, otkriju novi propusti u programskoj podršci VMwarea, posljedice napada koji bi ih iskorištavali s velikom će vjerojatnošću utjecati i na mnoge druge kompanije. U obzir treba uzeti i rastuću popularnost tzv. računarstva u oblaku (oblik računarstva kod kojeg su svi resursi dijeljeni, a usluge se dostavljaju putem mreže, najčešće Interneta) koje često koristi virtualizaciju za odjeljivanje podataka koji pripadaju različitim korisnicima. Novootkriveni propusti omogućili bi zlonamjerim programima bježanje iz virtualnog okruženja i zarazu cjelokupnih sustava, a napadačima pristup svim podacima pohranjenima na takvom sustavu.

Iako detaljni podaci o APT napadima nisu lako dostupni kroz medije, oni koji su dostupni su dovoljno informativni. Prvo, važno je uvidjeti da su ljudi (korisnici) često najslabija karika u informacijskoj sigurnosti, te da je dobra edukacija korisnika jedan od preduvjeta u smanjivanju rizika od napada. Lažne poruke elektroničke pošte koje se oslanjaju na lakovjernost korisnika jedna su od najčešćih tehnika koje napadači upotrebljavaju. Drugo, važno je uvesti bolje pripreme i metode obrane u računalne i mrežne sustave tehnoloških kompanija koje posjeduju informacije koje bi napadači mogli upotrijebiti za zaoilaženje sigurnosnih mjera njihovih klijenata.

8. Zaključak

APT napadi postaju rastući problem današnjih država, vlada i kompanija javnog i privatnog sektora. Gubici informacija koje APT napadi prouzrokuju mogu u potpunosti uništiti poslovanje napadnute organizacije te čak ugroziti i državnu sigurnost. APT napade posebno opasnima čine sposobnost prilagodbe napadača i ustrajnost u napadu na specifičnu metu.

Tehnike i alati kojima se napadači koriste najčešće nisu posebno napredni, no napadači prema potrebi mogu sami proizvesti vrlo učinkovite alate da bi došli do željenih informacija. Pošto se u početnim stadijima napada napadači vrlo često oslanjaju na socijalni inženjering, vrlo važnu ulogu u sprječavanju gubitka informacija ima edukacija svih korisnika, poticanje istih na oprez, uvođenje posebnih ograničenja i održavanje stalne komunikacije u svrhu dobivanja povratnih informacija od korisnika sustava.

U središtu svakog APT napada nalazi se mogućnost udaljenog upravljanja. Napadači se oslanjaju na te mogućnosti u svrhu pronalaženja specifičnih računala unutar ciljne organizacije, iskorištavanja propusta, upravljanja sustavima i dobivanja stalnog pristupa osjetljivim informacijama. Jednom kad je ta veza onemogućena i napad može biti prekinut. Iako zlonamjerni programi mogu ostati prikriveni, mrežni je promet povezan s napadačima mnogo lakše otkriti specijaliziranim alatima. Unatoč tome, APT skupine uspijevaju pronaći nove metode dobivanja pristupa računalnim i mrežnim sustavima. Ovo područje ostaje stalno bojno polje sigurnosnih timova organizacija pod napadom i APT skupina. Budućnost će, naravno, donijeti nove mogućnosti napada i otkrivanja informacija, ali i nove metode zaštite sustava. Važno je poduzeti sve moguće osnovne mjere zaštite u svrhu sprječavanja takve vrste napada.

9. Leksikon pojmova

Crv
Računalni crv je samoreplicirajući zloćudni program koji koristi mrežu računala kako bi poslao vlastite kopije na druge čvorove mreže bez pomoći korisnika. Ovakvo širenje računalnom mrežom je obično posljedica ranjivosti računala.
http://virusall.com/computer%20worms/worms.php
DNS (eng. *Domain Name System*)
DNS je hijerarhijski sustav imenovanja izgrađen na distribuiranim bazama podataka za računala, usluge ili bilo koji resurs spojen na Internet ili privatnu mrežu.
http://www.kb.iu.edu/data/adns.html
DNS lažiranje
Lažiranje DNS priručne memorije. Kod napada lažiranjem DNS priručne memorije, napadač šalje posebno oblikovani DNS odgovor DNS poslužitelju s namjerom da lažna informacija u DNS odgovoru bude pohranjena u priručnu memoriju DNS poslužitelja. Ovisno o informaciji u lažnom DNS odgovoru, moguć je DoS (eng. *Denial of Service*) ili MITM (eng. *man-in-the-middle*) napad.
http://www.networkworld.com/news/tech/2008/102008-tech-update.html
DOS napad
Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad.
http://searchsoftwarequality.techtarget.com/definition/denial-of-service
Elektronička pošta
Predstavlja način prijenosa tekstualnih poruka putem komunikacijskih mreža, najčešće Interneta. Usluga omogućava umetanje dodatnih datoteka kao privitke (engl. *attachment*). Elektronička pošta je postala standard za poslovnu komunikaciju, te je zamijenilo standardne dopise (dopisi se i dalje šalju ali putem elektroničke pošte). Nedugo nakon popularizacije elektronička pošta je postala medij za prijenos raznih zlonamjernih, štetnih programa kao što su crvi i virusi.
http://www.webopedia.com/TERM/E/e_mail.html
Exploit
Zloćudna informacija ili odsječak koda. Predstavlja odsječak programskog koda ili dio podataka koji iskorištava neispravnost ili aktivnu ranjivost određenog sustava kako bi se nanijela šteta, izazvalo neočekivano ponašanje ili omogućio neovlašten pristup.
http://searchsecurity.techtarget.com/definition/exploit
IP (eng. *Internet Protocol*)
IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanje paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.
http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm
PHP (eng. *PHP: Hypertext Preprocessor*)
Objektno-orijentiran programski jezik namijenjen prvenstveno za izradu dinamičnih web sjedišta. PHP je besplatan proizvod, objavljen pod PHP License licencom. Sintaksom je vrlo sličan popularnim jezicima poput C/C++, Java i Perl, a u potpunosti je implementiran u programskom jeziku C.
http://www.techrepublic.com/article/what-is-php/5074693
Phishing
Napad na računalni sustav. *Phishing* je način prikupljanja nekih osjetljivih informacija, kao što su korisnička imena, lozinke i detalji kreditnih kartica, maskiranjem u pouzdan entitet elektroničkih komunikacija.
http://www.webopedia.com/TERM/P/phishing.html
Rootkit
Oblik zloćudnog programa. *Rootkitovi* su zlonamjerni programi koji su napravljeni da bi preuzeli nadzor nad operacijskim sustavom tako da nadomjeste sustavske procese i podatke bez dopuštenja korisnika.
http://os2.zemris.fer.hr/ns/2008_Mackovic/rootkit.htm
SQL (eng. *Structured Query Language*)
SQL je programski jezik za pohranu, upravljanje i dohvat podataka pohranjenih u relacijskoj bazi podataka. SQL je najraširenij programskih jezik za upravljanje bazama podataka.
http://www.1keydata.com/sql/sql.html
SQL injection napad

Napad ubacivanjem SQL naredbe - napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web aplikacije bazi podataka. Na taj način moguće je ugroziti sigurnost web aplikacije koja konstruira SQL upite iz podataka unesenih od strane korisnika.
https://www.owasp.org/index.php/SQL_Injection

TCP (eng. *Transmission Control Protocol*)
Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela.
http://www.webopedia.com/TERM/T/TCP.html

Trojanski konj
Zlođudni program koji izgleda kao legitimna aplikacija. U početku se pretvara da obavlja korisnu funkcionalnost za korisnika, no u pozadini izvodi štetne radnje (na primjer, krađa informacija). Za razliku od crva, ovaj oblik zlođudnih programa se ne širi samostalno.
http://www.webopedia.com/TERM/T/Trojan_horse.html

URL (eng. *Uniform Resource Locator*)
URL predstavlja adresu određenog resursa na Internetu. Resurs na koji pokazuje URL adresa može biti HTML dokument, slika, datoteka ili bilo koja datoteka koja se nalazi na određenom web poslužitelju.
http://searchnetworking.techtarget.com/definition/URL

VoIP (eng. *Voice over IP*)
VoIP je skup internetskih tehnologija, komunikacijskih protokola i tehnologija prijenosa kako bi se ostvario prijenos govora preko IP mreže. VoIP koristi protokole za podršku sjednice poput SIP-a i SAP-a za uspostavljanje i raskid sjednica, tj. poziva.
http://voip.about.com/od/voipbasics/a/whatisvoip.htm

Wi-Fi
Wi-Fi je naziv za skup standarda IEEE 802.11. Ovaj standard je najčešće korišteni standard za WLAN mreže koje se koriste za bežični pristup Internetu.
http://www.gsmarena.com/glossary.php3?term=wi-fi

WWW (eng. *World Wide Web*)
WWW je jedna od najkorištenijih usluga Interneta koja omogućava dohvaćanje dokumenata. Dokumenti mogu sadržavati tekst, slike i multimedijalne sadržaje, a međusobno su povezani poveznicama (eng. *hyperlink*).
http://www.webopedia.com/TERM/W/World_Wide_Web.html

XSS napad
Cross-site scripting napad - napadačka tehnika koja prisiljava web aplikaciju da korisniku proslijedi zlonamjerni izvršni kod, koji se zatim učitava i izvodi u korisnikovom web pregledniku.
https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

10. Reference

[1] Advanced Persistent Threat - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Advanced_persistent_threat, studeni 2011.

[2] Remote Administration Tool - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Remote_Administration_Tool, studeni 2011.

[3] Trojan horse (computing) - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Trojan_horse_(computing), studeni 2011.

[4] Binde B. E., McRee R., O'Connor T. J.; Assessing Outbound Traffic to Uncover Advanced Persistent Threat; http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf, svibanj 2011.

[5] Li, F.; A Detailed Analysis of an Advanced Persistent Threat Malware; http://www.sans.org/reading_room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware_33814, listopad 2011.

[6] Hoglund G.; Advanced Persistent Threat - What APT Means To Your Enterprise; http://www.issa-sac.org/info_resources/ISSA_20100219_HBGary_Advanced_Persistent_Threat.pdf, studeni 2011.

[7] HackingTheUniverse - Advanced Persistent Threat, http://www.hackingtheuniverse.com/infosec/isnews/advanced-persistent-threat, srpanj 2011.

[8] What is an Advanced Persistent Threat, anyway?, http://www.networkworld.com/news/2011/020111-advanced-persistent-threat.html, veljača 2011.

[9] Advanced Persistent Threats (APT), http://www.damballa.com/knowledge/advanced-persistent-threats.php, studeni 2011.

[10] A Perspective on Advanced Persistent Threat, https://www.infosecisland.com/blogview/17645-A-Perspective-on-Advanced-Persistent-Threat.html, listopad 2011.