Hakovanje - večita igra nadmudrivanja

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Nikola Dimić, Đorđe Pantelić, Nikola Živković,
Mladen Canović
dimic.nikola@gmail.com, pantelicdjole94@gmail.com,
nmzivkovic@gmail.com, mladen.canovic@gmail.com

6. april 2019

Sažetak

Ovaj rad ima za cilj da upozna čitaoca sa konceptima obmane, hakovanja i zlonamernim softverom. Kroz tehničke detalje, primere i savete o bezbednosti, otvoriće diskusiju o značaju sigurnosti na internetu. Kroz izučavanje tehnika i tehnologija koje predstavljaju jednu od najvećih opasnosti današnjice, cilj je napraviti kritički osvrt na bezbednost softvera i skrenuti pažnju na odgovornost, koja je postavljena pred moderno društvo.

Sadržaj

1 Uvod

U originalnom značenju reč haker (eng. *hacker*) je predstavljala osobu koja je, na kreativan način, pokušavala da modifikuje sistem tako da on radi nešto inovativno. Hakerska kultura nastala je na univerzitetu MIT (eng. *Massachusetts Institute of Technology*) tokom pedesetih godina prošlog veka. Za njih *hack* nije predstavljao samo unapređenje funkcionalnosti uređaja, već i prikaz njihove virtuoznosti. Nazvati nekoga hakerom, bio je izraz poštovanja [13].

U ovom radu biće reči o pojmu hakovanja kao i konkretnim primerima kroz koje ćemo se bolje upoznati sa konceptima upada i obmane 2. U nastavku rada, biće reči o tipovima zlonamernog softvera uz detaljnu analizu i primere. Za kraj, obratićemo pažnju na načine zaštite od ovog tipa softvera 3.

2 Hakovanje

Hakovanje (eng. *Hacking*) predstavlja iskorišćavanje nedostataka sistema, računara ili računarskih mreža. Najčešća meta jesu ljudi koji rade na tom sistemu i ova vrsta napada predstavlja društveni inženjering (eng. *social engineering*).

Pored zlonamernih napadača (eng. *Black hat*), postoje hakeri koji uz dozvolu administratora upadaju u sisteme u cilju testiranja njihove sigurnosti. Oni predstavljaju etičke hakere (eng. *White hat*). Hakeri iz sive zone (eng. *Gray hat*), zarad dokazivanja svojih veština, vrše napade bez dozvole ali ne u nameri da nanesu značajnu štetu. Pored njih postoje hakeri koji se žalažu za određenu ideju ili cilj (eng. *Hacktivists*), čiji su najpoznatiji predstavnici grupa Anonimusi (eng. *Anonymous*) [8].

2.1 Umetnost upada

Sa razvojem informacionih tehnologija i računarstva rasla je i pretnja od njihove zloupotrebe.

Za hakovanje su interesovanje prvobitno pokazale mlade osobe, koje su se time bavile zbog ličnog uzbuđenja A.1 ili grupe profesionalaca koje bi koristile svoju ekspertizu zarad materijalne dobiti 2.1.1.

Danas države ulažu ogromna sredstva kako u bezbednost, tako i u regrutovanje talentovanih pojedinaca u političke svrhe i napade na vojne ciljeve 2.1.2 [11].

2.1.1 Milionska prevara kazina

Ranih devedesetih godina, Aleks Mejfild je sa tri prijatelja prezentovao softversko rešenje na konferenciji u Las Vegasu. Nakon posete kockarnici, došli su na ideju hakovanja poker aparata. Poker aparati su imali određene hardverske propuste - postojala je mogućnost zamene originalnog čipa. Zarad testiranja svojih programerskih sposobnosti oni su hakovali aparat na drugačiji način.

Napadači su kupili stariji aparat, jer ranije bezbednosti nije poklanjana velika pažnja, kako bi analizirali njegov algoritam. Koristeći disambler, koji su sami razvili, preveli su izvršni kod u izvorni. Analizom ključnih sekcija pronašli su generator nasumičnih brojeva iz šezdesetih godina, koji je predstavljao listu od oko četiri milijarde uskladištenih brojeva kroz koju se iteriralo na svaki deseti deo sekunde.

Po izvlačenju pet karata izvlačilo se još pet, koje bi bile rezerve u slučaju da igrač želi da zameni neke od prvobitno izvučenih. Tih deset karata predstavlja deset uzastopnih brojeva iz generatora. Pametnim rasporedom brojeva u početnoj listi, aparat kontroliše koja je tačno verovatnoća da igrač pobedi.

Napadači su uz pomoć štoperice i programa, koji su razvili, znali tačno kada će aparat izbaciti dobitnu kombinaciju. Program je na osnovu prvobitno izvučenih karata mogao da odredi trenutno stanje generatora. Nakon što se njihovo rešenje pokazalo kao uspešno, kupili su moderniji aparat kako bi povećali broj mesta na kojima mogu primeniti svoj metod. Ovaj aparat je imao dva generatora nasumičnih brojeva. Umesto da se svaka izvučena karta određuje na osnovu zbira generatora, iz istog razloga kao u prethodnom slučaju, za sve karte iz jednog izvlačenja korišćena je konstatna vrednost iz drugog generatora. Problem je ovim sveden na problem kriptografije gde su vrednosti prvog generatora pomerene za određeni korak koji se u svakom izvlačenju menja.

Za dve godine oštetili su kazino za preko milion dolara. Vremenom su napadači postali sve manje oprezni što je dovelo do otkrivanja njihove prevare. U zamenu za informacije o bezbednosnim propustima nisu procesuirani [11].

2.1.2 Informatičko ratovanje

Informatičko ratovanje (eng. *Cyberwarfare*) predstavlja način na koje države, bez stavljanja ljudskih života u opasnost, ostvaruju svoje ciljeve.

Stuxnet je zlonamerni program otkriven 2010. godine koji je naneo ogromnu štetu Iranskim nuklearnim elektranama. Pretpostavlja se da je delo Američkih i Izraelskih bezbednosnih agencija. Dizajniran je za napad na programabilne logičke kontrolere koji omogućavaju automatizaciju elektromehaničkih procesa, kao što je kontrola centrifugalnih mašina koje odvajajaju nuklearni materijal.

Koristeći četiri *zero-day*[1] propusta u operativnom sistemu *Microsoft Windows*, virus je bio u mogućnosti da sebe iskopira na sve računare u lokalnoj mreži potpuno neprimetno. Kada se bi se našao na nekom od računara *Stuxnet* je menjao kôd *Step7* alata kompanije *Siemens* za upravljanje kontrolerima i ubrzavao rad centrifugalnih mašina kako bi vremenom došlo do njihovog kvara. Korisnicima bi bili prikazani lažni podaci na osnovu kojih se ne bi moglo zaključiti da nešto nije u redu. *Stuxnet* se sastoji od tri modula od kojih jedan izvodi glavni deo napada, drugi prebacuje virus na ostale računare, a treći sakriva sve zlonamerne procese i datoteke kako bi onemogućio otkrivanje. U sistem je ubačen preko zaraženog *USB* uređaja.

Na samitu o računarskoj bezbednosti u Meksiko Sitiju 2015. godine laboratorija Kasperski (rus. *Лаборатория Касперского*) je objavila otkriće postojanja *Equation* grupe, koja je dobila ime zbog izuzetno sofisticiranog algoritma za šifrovanje koji je razvila. Izveštaji navode da grupa postoji od 2001. godine. Zbog veoma naprednih tehnika i visokog nivoa prikrivenosti, grupa se povezuje sa nacionalnom bezbednosnom agencijom (eng. *National Security Agency, NSA*) Sjedinjenih Američkih Država. Otkriveno je da su pre ili u isto vreme koristili iste *zero-day* napade koji su korišćeni i u virusu *Stuxnet* te se pretpostavljalo da su oni bili odgovorni za razvoj ovog virusa. Laboratorija Kasperski je grupu opisala kao daleko najsofisticiraniju koja je ikada otkrivena.

[1] Zero-day propusti predstavljaju ranjivosti sistema za koje zna samo napadač.

Pored virusa *Stuxnet* povezuju se i sa zlonamernim programom *Flame* otkrivenim 2012. godine koji predstavlja najkompleksniji virus ikada napravljen [3]. Sastoji se od deset grupa modula koji su prikazani u tabeli 1.

Ime grupe	**Namena**
Flame	Moduli zaduženi za upad u sistem
Boost	Moduli zaduženi za prikupljanje informacija
Flask	Tip modula za napad
Jimmy	Tip modula za napad
Munch	Moduli za instalaciju i dalje širenje
Snack	Moduli za lokalno širenje virusa
Spotter	Moduli zaduženi za skeniranje sistema
Transport	Moduli zaduženi za umnožavanje
Euphoria	Slanje podataka ka ciljnim serverima
Headache	Parametri i ostale karakteristike napada

Tabela 1: Moduli zlonamernog programa Flame i njihova moguća namena

Ovaj virus se koristio za špijunažu u zemljama bliskog istoka, pretežno Iranu. Program je mogao da se širi preko lokalnih mreža, kao i preko uređaja koji poseduju *Bluetooth*. Mogao je nezapaženo da snima zvuk i ekran, da registruje unos sa tastature i svu komunikaciju preko mreže. Informacije je slao serverima, koji su korišćeni za upravljanje i čekao dalja uputstva od njih. Posedovao je i *kill* komandu koja je brisala sve tragove postojanja virusa na računaru, a koja je poslata odmah pošto je virus prvi put otkriven. U izveštaju laboratorije Kasperski se navodi da je *Equation* grupa ta koja je pomogla napadačima, dok je *CrySyS Lab*[2] kao odgovorne za razvoj virusa *Flame* označio bezbednosnu agenciju zemlje sa 'značajnim budžetom i kapacitetima' [3].

2.2 Umetnost obmane

Sa razvojem bezbednosnih tehnologija, postaje sve teže iskoristiti tehničke nedostatke sistema. Posledica toga je sve veće iskorišćavanje ljudskog faktora, što je često veoma lako. Vrsta napada, koji se svodi na prevaru žrtve da oda poverljive informacije ili napravi izmene u sistemu na kojem radi, a koje nisu u njenom interesu, naziva se društveni inženjering (eng. *social engineering*) [10].

Osobe koje koriste nedostatke u ljudskoj prirodi, zarad ostvarenja svog cilja, nazivaju se društveni inženjeri (eng. *social engineers*). Napadi društvenih inženjera uspevaju kada ljudi nisu dovoljno upoznati sa dobrom praksom u bezbednosti. Uprkos tome što kompanija ili pojedinac, zarad svoje bezbednosti, kupi sve moguće alate i obuči svoje zaposlene o merama predostrožnosti, ona je i dalje ranjiva jer je ljudski faktor najslabija karika bezbednosnog sistema.

Društveni inženjeri umeju sa ljudima, šarmantni su i harizmatični - osobine koje omogućavaju pridobijanje poverenja i prisnosti sa žrtvom. Iskusni društveni inženjer, koristeći svoje umeće obmane, je u stanju da izvuče željenu informaciju ili inicira određenu radnju žrtve. Strategije za

[2] Laboratorija za kriptografiju i bezbednost sistema, Univerzitet tehnologije i ekonomije u Budimpešti.

napad, koje oni koriste, sačinjene su od više različitih pristupa. Navedeni su neki od njih [10].

Elementi strategija društvenih inženjera

- **Skrivena vrednost informacija**

  Društveni inženjeri često koriste informacije o firmi, koje su naizgled neinteresantne, a mogu biti od velikog značaja za ostvarenje cilja. Poznavanje osnovnih pravila, načina ponašanja i izražavanja, procedura, često korišćenih termina i skraćenica unutar firme ili unutar određenog odeljenja firme, mogu biti presudan faktor napada 2.2.1.

- **Zloupotreba poverenja**

  Poverenje je ključ prevare. Društveni inženjeri planiraju svoj napad vrlo temeljno, pokušavajući da predvide pitanja koja bi žrtva mogla postaviti. Vode razgovor koji, za žrtvu, ne izlazi van okvira uobičajenog. Kada žrtve nemaju razloga za sumnju, napadačima je lako da pridobiju njihovo poverenje i, koristeći svoje veštine, ostvare svoje namere.

- **Pomoć neprijatelja**

  Kada su ljudi uplašeni ili pod određenim pritiskom zbog nekog problema, skloni su da prihvate savete od osoba, koje ostavljaju utisak poverenja, a koje nikada nisu sreli. Napadač kroz pružanje pomoći žrtvi ostvaruje svoje ciljeve. On navodi žrtvu da instalira zlonamerni softver ili otkrije poverljive informacije, koje žrtva prepušta u nadi da će dovesti do rešenja problema. Početni problem može biti prouzrokovan od strane napadača 2.2.2.

- **Iskorišćavanje osećanja**

  Iskusni društveni inženjeri su vešti u manipulisanju osećanjima žrtve. To čine koristeći psihološke okidače (eng. *psychological triggers*)[3], koji dovode do površnog pristupa žrtve problemu bez temeljne analize dostupnih informacija. Napadač izaziva saosećajnost žrtve izmišljajući problem, koji je žrtva prethodno i sama iskusila. Pored ovog pristupa, napadač može izazvati osećaj krivice kod žrtve ili koristiti zastrašivanje kao oružje.

2.2.1 Najveća računarska prevara u istoriji

Stenli Rifkin je, 1978. godine, radio za kompaniju zaduženu za razvoj sistema za bezbednost jedne od najvećih banaka u Los Anđelesu, pa je imao pristup poverljivim informacijama te banke. Radeći na odeljenju za prenos novca na daljinu (eng. *wire room*), upoznao se sa procedurom transakcija. Službenici koji su imali ovlašćenje da nalože transfer, svakog jutra su dobijali kôd koji su u toku tog dana koristili u procesu autorizacije. Službenici bi najčešće napisali tu šifru na parčetu papira i ostavili je na sebi vidno mesto.

Izvršavajući svoja zaduženja na odeljenju, uspeo je da pročita aktuelni kôd sa parčeta papira jednog od službenika i da ga zapamti. Otišao je do govornice, odakle je pozvao jednog od zaposlenih u odeljenju za prenos novca i predstavio se kao član međunarodnog odeljenja banke. Posle uspešne autorizacije kôdom službenika, naložio je prenos deset miliona dolara na račun u Švajcarskoj, koji je prethodno otvorio. Postojao je deo

[3] Automatski mehanizmi ljudske psihologije koji ih čine podložnim sugestiji.

koji je napadač propustio prilikom upoznavanja sa samom procedurom. Bio mu je potreban i broj međupartijskog poravnanja (eng. *interoffice settlement number*). Nazvao je drugo odeljenje u banci, predstavio se kao zaposleni sa kojim je upravo razgovarao i tražio broj koji mu je nedostajao, uz obrazloženje da ga je zaboravio. Kada je saznao broj, ponovo je pozvao sobu za transfer novca na daljinu i uspešno završio transakciju. U Švajcarskoj je podigao novac kojim je kupio dijamante, koje je kasnije u kaišu prošvercovao nazad.

Iako za ovaj poduhvat nije koristio računar, njegova prevara ušla je u Ginisovu knjigu rekorda u kategoriji 'najveća računarska prevara' [10].

2.2.2 Zloupotreba poverenja

Napadač Bobi Volas je nazvao zaposlenog u kompaniji *Starboard shipbuilding*, čije tajne podatke je želeo da sazna i predstavio se kao tehnička podrška. Obavestio ga je da su u narednom periodu mogući problemi na mreži i da u slučaju nekog kvara pozove prvo njega. Posle nekoliko dana je pozvao mrežni operativni centar kompanije i predstavio se kao zaposleni u kompaniji, koristeći podatke radnika, kojeg je prvobitno nazvao. Od operatera je tražio da isključe mrežu u njegovoj kancelariji, kako bi otklonio kvar. Sada je mreža, u kancelariji žrtve napada, bila isključena, pa nije mogao da preuzme potrebne datoteke sa servera, razmenjuje informacije sa kolegama, proveri elektronsku poštu ili koristi štampač.

Zaposleni je, upozoren da do ovoga može doći, pozvao broj koji je nekoliko dana pre toga dobio od napadača. Napadač se trudio da zvuči željno da pomogne kolegi u nevolji, ali i da ga ubedi da mu pružanjem te pomoći čini veliku uslugu. Nakon nekog vremena pozvao je mrežni operativni centar i zatražio uključenje mreže. Posle toga je ponovo pozvao zaposlenog i koristeći osećaj zahvalnosti koji je otklanjanjem problema izazvao, lako ga ubedio da instalira aplikaciju, koju mu je predstavio kao zaštitu od budućih problema sa mrežom. U pitanju je bio računarski virus - trojanski konj 3.3, koji je napadaču omogućio potpunu kontrolu nad žrtvinim računarom [10].

3 Zlonamerni softver

Zlonamerni softver (eng. *Malware*) predstavlja softver koji je dizajniran tako da nanese štetu ciljnom korisniku. U zavisnosti od namene, funkcije i opasnosti postoji više vrsta zlonamernog softvera. Manje opasni programi mogu samo zauzeti procesorsko vreme ili mesto u memoriji i na taj način usporiti rad računara, dok opasniji mogu uništiti podatke na računaru, pa čak i preuzeti potpunu kontrolu nad njim. Na taj način računar postaje alat koji se može upotrebljavati za razne ilegalne aktivnosti, poput krađe kreditnih kartica ili napada na druge računare u mreži [13].

3.1 Virusi

Računarski virus je program koji se ugrađuje u izvršni kôd drugih programa. Namena računarskog virusa je da zarazi sistem, koristeći loše obezbeđene delove, preuzme kontrolu ili ukrade poverljive podatke. Načini na koje se virus širi su otvaranje dodatka (eng. *attachment*) u okviru elektronske pošte, poseta zaraženom sajtu, pokretanje neproverene izvršne datoteke ili povezivanje zaraženog prenosnog uređaja sa računarom. Računarski

virus može raditi na dva načina. Može se aktivirati čim dospe u sistem ili naknadnom akcijom korisnika [9, 7].

Tipovi virusa

- **Virus sektora za podizanje sistema**
  Virus sektora za podizanje sistema (*eng. boot sector virus*) napada uređaje za skladištenje podataka, kao što su tvrdi (eng. *hard drive*) ili flopi (eng. *floppy*) diskovi, tako što izmeni njihovu glavnu sekciju za podizanje sistema. Kada se sistem jednom podigne sa zaraženim programom, virus se učita u radnu memoriju i dalje širi na sve flopi diskove ubačene u računar. Kako se u moderne operativne sisteme ugrađuju čuvari te kritične sekcije (eng. *safeguard*), a flopi diskovi su izašli iz upotrebe, ovaj tip virusa je prevaziđen [9, 7].
- **Virus direktnih akcija**
  Virus direktnih akcija (*eng. direct action virus*) se aktivira čim dospe u sistem, ne sakriva se u memoriji i cilj mu je da se svakim izvršavanjem dodatno proširi kroz sistem. Virus inficira najpre tipove datoteka koje napadač odredi, a zatim i sistemske datoteke odgovorne za određene operacije prilikom podizanja sistema. Ovaj tip virusa nema za cilj brisanje datoteka ili smanjivanje performansi računara već prikupljanje i menjanje pristupa određenim podacima. Antivirusi veoma lako primete aktivnosti ovog tipa virusa [16].
- **Prikriveni virus**
  Nasuprot virusu direktnih akcija prikriveni virus (*eng. resident virus*) je specifičan po tome da ga je teško identifikovati i odstraniti. Virus se instalira na sistem i krije u memoriji računara. Modularan je, pa je tako svaki deo virusa zadužen za različitu zlonamernu aktivnost. Korišćenje ovakvog tipa virusa indukovano je poznavanjem značajnih propusta na samom sistemu [7].
- **Polimorfni virus**
  Polimorfni virus (*eng. polymorphic virus*) je imun na tradicionalne antivirus programe. Ovaj tip virusa menja svoj izvršni kôd svaki put kada se kopira. Ovo dovodi do otežanog lociranja virusa pomoću antivirus programa, kao i do toga da se sam virus brzo širi kroz ceo sistem [7].
- **Prepisujući virus**
  Prepisujući virus (*eng. overwrite virus*) je jedan od najjednostavnijih virusa. Odlikuje se time što briše originalan kôd zaraženog programa i menja ga novim, zlonamernim kôdom. Kada se novonastali program pokrene, virus se širi kroz sistem. Kako zlonamerni program briše zaraženu datoteku parcijalno ili u celosti, nije moguće povratiti je [14].
- **Virus koji koristi prazan prostor**
  Virus koji koristi prazan prostor (*eng. spacefiller*) popunjava prazna mesta na zaraženom disku ili u izvršnom kôdu zaraženih datoteka. Prostor popunjava sopstvenim kopijama pri čemu se veličina originalne datoteke ne menja, stoga ga je veoma teško primetiti [5].

3.2 Softver za špijuniranje

Softver za špijuniranje (*eng. Spyware*) je neželjeni softver koji upada u sistem i krade poverljive informacije. Ovaj softver sakuplja lične podatke

korisnika i šalje ih zlonamernim pojedincima ili kompanijama, koje se bave reklamama ili obradom podataka. Cilj softvera je da dođe do lozinki i finansijski osetljivih podataka žrtve. Virus prati aktivnost korisnika na internetu i čuva njegove informacije pri prijavljivanju na veb stranice. Neki tipovi softvera za špijuniranje mogu da instaliraju dodatne neželjene programe na uređaj, kao i da menjaju podešavanja [4].

Tipovi softvera za špijuniranje

- **Adver**

  Adver (*eng. Adware*) se koristi u svrhu marketinga, tako što prati istoriju pretraživanja i preuzete podatke sa interneta, sa namerom da predvidi kakvi bi proizvodi zainteresovali korisnika i te informacije prosleđuje marketinškim agencijama. Može znatno da uspori računar [4].

- **Kolačići za praćenje**

  Kolačići za praćenje (eng. *tracking cookies*) prate sve akcije korisnika na internetu, kao što su istorija pretraživanja ili razmena podataka. Njihova podrazumevana namena nije zlonamerna, ali mogu da se iskoriste od strane sajber kriminalaca (eng. *cyber criminal*) [1].

- **Posmatrači sistema**

  Posmatrači sistema (eng. *system monitors*) prate sve akcije korisnika na računaru, registruju svaki pritisak dugmeta na tastaturi, pročitanu elektronsku poštu, razgovor na internetu, posećene veb stranice i korišćene programe [4].

3.3 Trojanski konj

Trojanski konj (eng. *Trojan horse*), nazvan po čuvenom Trojanskom konju iz Homerovog epa *Odiseja*, predstavlja štetni program. Maskiran je u program koji je koristan, dok u pozadini izvršava zlonamerne akcije bez znanja korisnika [2].

Primer trojanskog konja predstavlja softver *Mocmex*, otkriven 2008. godine, koji se nalazio na digitalnim ramovima za slike u Kini. Umesto isključivog učitavanja slika ovaj softver je, kada bi bio priključen na računar, prikriveno krao lične informacije o korisnicima, šifre za MMORPG (eng. *Massively multiplayer online role-playing game*) i slično. [13].

3.4 Mreža botova

Mreža botova (eng. *Botnet*) je kolekcija međusobno povezanih zaraženih uređaja, koji su pod kontrolom istog tipa zlonamernog softvera. Korisnici zaraženih uređaja često nisu svesni da je njihov sistem deo mreže botova.

Zaraženi uređaji se kontrolišu daljinski, bez korišćenja značajnih resursa računara, tako da njihove zlonamerne akcije bivaju sakrivene od korisnika. Mreže botova se koriste za slanje neželjene elektronske pošte ili preusmeravanje korisnika na zlokobne veb stranice. Mreža botova napada nedovoljno zaštićene uređaje, sa ciljem da se proširi na što više uređaja i da se računarska moć i resursi, kojima mreža raspolaže, iskoriste za automatske radnje koje ostaju skrivene od korisnika. Da bi ostala skrivena, mreža koristi neprimetno mali protok podataka.

Mreža koja broji milione uređaja može da proizvede ogroman saobraćaj na željenim veb stranicama i na taj način, potpuno neprimećeno,

napadačima donese materijalnu dobit. Može se koristiti i za *DDoS* napade (eng. *Distributed Denial of Service attack*). Ovi napadi otežavaju rad servera, tako što ga zatrpavaju velikom količinom zahteva [15].

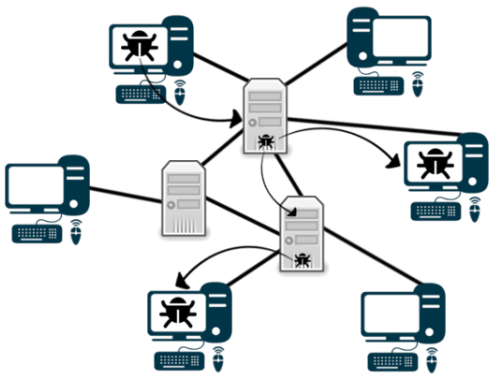
3.4.1 Arhitektura mreže botova

Kada inficiraju željeni broj uređaja, napadači mogu da kontrolišu mrežu na dva različita načina. Tradicionalni klijent/server pristup uključuje postavljanje kontrolnog servera (eng. *Command and Control server*), koji šalje automatske komande botovima koristeći komunikacione protokole, kao što je *IRC* protokol (eng. *Internet Relay Chat*). Botovi su u stanju čekanja, sve dok ne stigne naredba sa kontrolnog servera.

Drugi, decentralizovani pristup uključuje mrežu ravnopravnih korisnika (eng. *peer-to-peer*). Zaraženi uređaji komuniciraju unutar mreže i tako dele nove naredbe najskorije verzije zlonamernog softvera, koji njima upravlja [15].

3.5 Računarski crvi

Računarski crv (eng. *Computer worm*) je zlonamerni program koji se umnožava širenjem kroz mrežu međusobno povezanih računarima. Širenje crva unutar mreže uslovljeno je propustima u toj mreži ili operativnom sistemu [12, 13]. Na slici 1 prikazana je ilustracija širenja računarskog crva kroz mrežu.



Slika 1: Širenje računarskog crva kroz mrežu

Računarski crv ne mora nužno biti zlonameran, ali uvek vrši neku vrstu ugrožavanja sistema, makar kroz usporavanje protoka podataka kroz mrežu. Česta primena crva je da kroz veliko širenje omogući uslove za druge vrste napada 3.4. U tom slučaju, crv instalira program pomoću kojeg se tim računarom može daljinski upravljati [13].

Ideja o ovakvom tipu softvera prvi put je predstavljena u naučno-fantastičnom romanu napisanom 1975. godine, autora Džona Brunera, u kom se pominju crvi, programi koji se šire kroz mrežu futurističkih računara. Nedugo zatim, 1979. godine, nekolicina zaposlenih u firmi *PARC* u Kaliforniji pravi i testira ovakav tip programa. Prvi računarski crv je zapravo bio dobronameran. Korišćen je za brzo širenje korisnih informacija kroz mrežu [17].

3.5.1 Internet crv

Termin Internet crv (eng. *Internet worm*) se najčešće poistovećuje sa terminom Morisov crv, odnosno programom Roberta Morisa, koji je drugog novembra 1988. godine naneo višemilionsku štetu korisnicima interneta u Americi. Ovo je prvi napad korišćenjem ovakvog tipa programa i kao takav je dobio veliku pažnju medija i javnosti [13].

Internet crv je koristio greške u samom kôdu *Unix* operativnog sistema, u komandama *fingerd* i *sendmail*, kao i tehnike za otkrivanje jednostavnih lozinki i brzo se proširio kroz mrežu na računare vojske, univerziteta pa i bolnica. Usled greške u samom kôdu crva, program se kopirao na iste računare po par stotina puta. Ovo je dovelo do toga da brojni računari otkažu usled prevelikog broja programa koji se na njima izvršavaju. [17].

3.5.2 Saser

Saser (eng. *Sasser*) je vrsta računarskog programa, koji je izazvao velike troškove i podigao svest javnosti o važnosti ažuriranja softvera. Pušten je u opticaj 2004. godine. Saser je za širenje na skoro 18 miliona računara širom sveta iskoristio grešku u starijoj verziji *Windows* operativnog sistema. Tako su računari koji nisu imali aktuelnu verziju operativnog sistema, među kojima su bili računari austrijske železnice i britanske obalske straže, postali neupotrebljivi [13].

3.6 Ukrštanje veb lokacija

Koristeći tehniku ukrštanja veb lokacija (eng. *Cross-Site scripting*), zlonamerni korisnik može postaviti kôd unutar veb stranice, iskorišćavajući propuste u bezbednosti. Postavljen kôd se izvršava u trenutku kada korisnik poseti datu stranicu i tada napadač najčešće dolazi do informacija o njemu. [13, 6].

Primer propusta na veb stranicama je način čuvanja komentara na serveru. Komentari se čuvaju u bazi podataka bez obrade ili provere, a zatim prikazuju na klijentskoj strani veb aplikacije. Napadač, ostavljanjem komentara u određenom formatu, postavlja zlonamerni kôd. Kôd može izmeniti stranicu, tako da se prilikom posete korisnika veb aplikaciji aktivira program, koji šalje podatke korisnika napadaču. Ti podaci su uglavnom kolačići, ali mogu predstavljati lozinke i druge osetljive podatke [6].

3.7 Usputno preuzimanje podataka

Usputno preuzimanje podataka (eng. *Drive by downloads*) predstavlja napad na računar posetioca zaražene veb stranice, tako što se na njegov računar kopiraju zlonamerne datoteke. Napadač može izmeniti loše obezbeđenu veb stranicu, tako da se na računar svakog posetioca te stranice kopira određeni zlonamerni program, bez znanja korisnika. Posetilac može postati žrtva napada i svesnim preuzimanjem softvera sa zaražene veb stranice, čija namena je različita od predstavljene [18, 13].

3.8 Mere zaštite od zlonamernog softvera

Nemoguće je u potpunosti se odbraniti od napada, ali je moguće rizik svesti na minimum. Tri odbrambene mere, koje su najvažnije za očuvanje sistema navedene su u narednoj listi.

- **Bezbednosne zakrpe softvera**

  Bezbednosne zakrpe softvera (eng. *Security patches*) predstavljaju ažurirane delove softverskog rešenja, koje je u svojim prethodnim verzijama sadržalo određene propuste, od kojih su neki otkriveni nakon pretrpljenih posledica.

- **Alati za odbranu od zlonamernog softvera**

  Alati za odbranu od zlonamernog softvera (eng. *antimalware tools*) se koriste u preventivne svrhe ili za analizu i otklanjanje zaraženih datoteka, uz prethodnu saglasnost korisnika. Zbog naglog povećanja broja vrsta zlonamernog softvera i tehnika napada, potrebno je redovno ažurirati ove alate.

- **Zaštitni zidovi**

  Zaštitni zidovi (eng. *firewalls*) predstavljaju softver koji se koristi za regulisanje mrežnog saobraćaja na računaru. Zaštitni zidovi omogućavaju korisniku da odabere koja će aplikacija imati pristup internetu. Ne pružaju dovoljnu zaštitu ukoliko su računari već zaraženi tipom zlonamernog softvera koji može onesposobiti zaštitni zid [13].

4 Zaključak

Kroz ovaj rad se moglo ustanoviti da je obezbeđenje često iluzija sigurnosti [10]. Kroz osvrt na različite vrste napada i tehnika obmane se mogao steći utisak o manama bezbednosnih sistema. Unapređivanjem tih sistema unapređuju se i tehnike napada, pa njihov odnos predstavlja povratnu spregu bez konačnog pobednika. Prednost napadača je to što sigurnosni sistem mora da pobedi svaki put, dok je njemu dovoljno da pobedi samo jednom [11].

Literatura

[1] AVG Academy. What are tracking cookies. on-line at:https://support.avg.com/SupportArticleView?l=en&urlname=What-are-tracking-cookies.

[2] John P. McDermot William S. Chot Carl E. Landwehr, Alan R. Bull. A Taxonomy of Computer Program Security Flaws, with Examples. *ACM Computing Surveys*, 3(26), 1994. on-line at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a465587.pdf.

[3] Budapest University of Technology CrySyS Lab. sKyWIper(a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks, 2012. on-line at: https://www.crysys.hu/publications/files/skywiper.pdf.

[4] Symantec employee. What is spyware? And how to remove it, 2017. on-line at:https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html.

[5] Fakehackers. Spacefiller virus, 2018. on-line at:https://fakehackers.com/spacefiller-virus/.

[6] Irene Lobo Valbuena Jakob Kallin. Excess XSS, 2016. on-line at: https://excess-xss.com/.

[7] Kevin Judge. What is a computer virus?, 2018. on-line at:https://antivirus.comodo.com/blog/computer-safety/what-is-virus-and-its-definition/.

[8] P.N.V.S. Pavan Kumar K. Bala Chowdappa, S. Subba Lakshmi. Ethical Hacking Techniques with Penetration Testing. *International Journal of Computer Science and Information Technologies*, 5, 2014.

[9] Eugene Kaspersky. Viruses and worms. on-line at: https://encyclopedia.kaspersky.com/knowledge/viruses-and-worms/.

[10] Steve Wozniak Kevin D. Mitnick. *The Art of Deception*. John Wiley & Sons, New Jersey, United States, 2002.

[11] Kevin D. Mitnick. *The Art of Intrusion*. John Wiley & Sons, New Jersey, United States, 2005.

[12] Symantec Corporation Norton. What is a computer worm, and how does it work?, 2018. on-line at: https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html.

[13] Michael J. Quinn. *Ethics for the information age*, volume 6. Pearson Education, United States of America, 2015.

[14] Virus Radar. Overwriting viruses. on-line at:https://www.virusradar.com/en/glossary/overwriting-viruses.

[15] Margaret Rouse. Botnet. on-line at:https://searchsecurity.techtarget.com/definition/botnet.

[16] David E. Sorkin. Understanding the Direct Action Virus. on-line at:https://www.spamlaws.com/direct-action-virus.html.

[17] Eugene H. Spafford. The Internet Worm Program: An Analysis. *Purdue Technical Report*, pages 2–7, 2004.

[18] Danilo Bruschi Ulrich Flegel. *Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, Como, Italy, 2009.

A Dodatak

A.1 Hakovanje zarad uzbuđenja

Džonatan Džejms, u potpisu *Comrade*, je najmlađa osoba ikada osuđena za hakovanje na teritoriji Sjedinjenih Američkih Država. Njegov prijatelj *Ne0h* je već sa deset godina počeo da se bavi hakovanjem. *Comrade* i *Ne0h* su se upoznali preko sajtova koji su predstavljali sobe u kojima su ljudi sličnih interesovanja mogli da razmenjuju informacije u tekstualnom formatu (eng. *Internet Relay Chat, IRC*). Hakeri se često udružuju u grupe kako bi razmenjivali informacije i organizovali grupne napade.

Sredinom 1998. godine na jednom od tih sajtova *Comrade* je stupio u kontakt sa Halidom Ibrahimom, čovekom za koga se u zajednici pričalo da regrutuje ljude za upade na vladine sajtove i koji radi za, tada ne toliko poznatog teroristu, Bin Ladena. Halid je stupio u kontakt i sa *Ne0h*-om kome je obećao 1000$ ukoliko uspe da hakuje tehnički univerzitet u Kini. Ovaj zadatak, koji je bio samo test njegovih sposobnosti, je uspešno obavio.

Nakon nekoliko uspešnih probnih zadataka, od njega je zatraženo da hakuje avio kompaniju Boing (eng. *Boeing*). *Ne0h* je uspeo da provali širi obruč mreže i ostavi program koji mu je dao uvid u sve dolazne i odlazne pakete (eng. *sniffer*). Na ovaj način uspeo je da sazna nekoliko

korisničkih imena i lozinki koji su mu omogućili da uđe dublje u sistem. Uspeo je da dođe u posed i isporuči Halidu šeme vrata na avionu Boing 747, šemu pilotske kabine, kao i celog nosa aviona. Za *Comrade*-a je imao zadatak da hakuje *SIPRNET*[4]. Iako je ovo predstavljalo ogroman rizik uspeo je da na nekoliko računara na mreži ostavi program koji je pratio komunikaciju.

U isto vreme, u Indiji su teroristi oteli avion. Sleteli su u Afganistan i tu čekali osam dana dok vlasti nisu pristale da oslobode trojicu ekstremista iz zatvora. Među njima bio je i Šîh Umer, koji će kasnije postati glavni finansijer Muhameda Ate, vođe terorista koji su izveli napad 9.11.2001. Halid je u razgovoru sa *Comrade*-om rekao da je i on sam bio deo otmice. Nakon ovoga, počeo je da uklanja tragove svojih aktivnosti povezanih sa njim.

Nekoliko dana posle njegovog upada u *SIPRNET*, njegovog oca je kontaktirao *FBI*. Vlasnik računara na koji je uspeo da se infiltrira, bila je *NASA* (eng. *National Aeronautics and Space Administration*). Optužen je za tronedeljni zastoj u radu te organizacije, kao i za presretanje elektronske pošte ministarstva odbrane. Na jednom od njegovih diskova pronađen je program koji bi mu omogućio da kontroliše temperaturu i vlažnost vazduha na Internacionalnoj svemirskoj stanici. Iako star samo petnaest godina, osuđen je na šest meseci zatvora čime je pravosudni sistem poslao jasnu poruku maloletnim hakerima da im neće biti gledano kroz prste.

U intervjuu 2002. godine, indijski general je objavio da je baza Halida Ibrahima, povezanog sa hakerskim organizacijama, bila u Nju Delhiju. Jedna od tih hakerskih organizacija bila je i *gLobaLheLL*, čiji je vođa *Zyklon* takođe imao kontakte sa Halidom. Ta grupa uspela je 1999. godine da upadne na sajt vojnog saveza *NATO*, kao i u mrežu Bele kuće i objavi zvučne i video zapise sa ličnog računara tadašnjeg predsednika Bila Klintona. U toku samog napada, Halid je stupio u kontakt sa *Zyklon*-om kome se ovaj pohvalio da su upravo upali u računarski sistem Bele kuće. Nakon toga, pojavio se sistem administrator i na mrežu instalirao program, koji je pratio svu aktivnost i zabeležio adrese napadača.

Na saslušanju *Zyklon* je imao uvid u dokumente u kojima je pisalo da su nadležni za napad saznali od doušnika FBI-a iz Nju Delhija. Ostalo je nepoznato da li je Halid bio samo doušnik FBI-a ili dupli agent i pravi terorista, kako je kasnije izjavio indijski general i da li su informacije, koje su mu dali mladi hakeri sa kojima je bio u kontaktu, na neki način pomogle u terorističkim napadima koji su sledili.

Vlada je nakon tih događaja shvatila koliku pretnju predstavlja terorizam, kolike su mogućnosti informatičkog ratovanja 2.1.2 i koliko su njihovi sistemi zaista bili izloženi [11].

[4]Mreža koju je koristila vojska i druge vladine bezbednosne agencije za brz prenos naređenja na celoj teritoriji države.