SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE VARAŽDIN

Ljiljana Pintarić

KNJIGA IZ KOLEGIJA SIGURNOST INFORMACIJSKIH SUSTAVA

MALWARE

Mentor:

Prof. dr.sc. Željko Hutinski

mag. Inf. Tonimir Kišasondi

Varaždin, 2013.

Sadržaj

1. Malware

1.1. Najpoznatiji slučajevi

ILOVEYOU virus, nastalo 90-tih godina prošlog stoljeća, bio je implementiran u Microsoftovom VBScript jeziku a prenosio se kao privitak LOVE-LETTER-FOR-YOU.TXT.vbs. Budući da je imao dvije ekstenzije, txt za tekstualnu datoteku i vbs za skriptu, korisnici bi otvorili privitak na računalima koja su skrivala ekstenzije, misleći da se radi o tekstualnoj datoteci, dok bi Windows Script Host pokrenuo skriptu, i virusi bi se počeli širiti. Virus je slao svoju kopiju e-mailom svim ljudima iz adresara.

Back Orifice – (od Microsoft BackOffice Server) trojanac iz 1998. Koji se u mjesec dana proširio na 100 000 računala, nakon čega je napadaču omogućavao potpunu kontrolu nad žrtvinim računalom.

Sasser crv širio se zahvaljujući ranjivosti Windows XP i 2000 OS-ova, koristeći ranjive mrežne portove. Prvi put je uočen 2004. godine. Širi se iskorištavajući „buffer overflow“ u komponenti LSASS (Local Security Authority Subsystem Service). Naime, crv skenira različite raspone IP adresa te se spaja na računala žrtava preko TCP porta 445 ili 139. Sasser je primjerice blokirao satelite AFP (Agence France-Presse) agencije, a zbog njega je Delta Air Lines bila prisiljena otkazati nekoliko transatlantskih letova. Zbog Sasser-a oštećene su i tvrtke British Coastguard, Goldman Sachs, Deutsche Post, kao i Europska komisija, Lund Sveučilišna Bolnica, te Missouri Sveučilište. Tvorac mu je Sven Jaschan iz Rotenburga.

Conficker crv, znan još i kao Conficker virus, Downadup i Kido, jedna je od najbržih i najšire rasprostranjenih infekcija još od Sasser infekcije. Napada Windowse, a prvi je put uočen 2008. Koristi sigurnosne ranjivosti u Windowsima, te „dictionary“ napade (brute force probijanje lozinke) kako bi dobio pristup administrativnim računima te tako formirao botnet. Budući da koristi različite napredne maliciozne tehnike, teško ga je uočiti. Conficker je zarazio milijune računala; ne samo ona običnih korisnika, već i računala vlada i korporacija, a do sada je poznato pet njegovih verzija.

STUXNET crv otkriven je 2010. godine (zahvaljujući WikiLeaksu), a izrađen je od strane američke NSA (Unit 8200) i Izraela, za sabotažu centrifuga za obogaćivanje urana u Iranu. Naime, 2009. došlo je do nuklearnog incidenta u Natanzu, gdje je oko 1000 od 5000 centrifuga oštećeno. Smatra se dijelom Operation Olympic Games. Osim Irana, ovaj je crv uzrokovao štetu u Indoneziji, Indiji, Azerbejđanu, SAD-u te Pakistanu. Inicijalno se širi

Windowsima, a meta su mu Siemens SCADA (Supervisory Control and Data Acquisition) sustavi koji su konfigurirani za kontrolu i praćene specifičnih industrijskih procesa. Stuxnet napada Windowse koristeći 4 zero-day te 20 uobičajenih exploita. Inicijalno se širi koristeći zaražene USB flash driveove, nakon čega koristi druge exploite i tehnike za inficiranje i ažuriranje drugih računala unutar privatnih mreža, koja nisu direktno povezana na internet.

Rustock botnet bio je spamming botnet, aktivan pet godina, sve do ožujka 2011. Njegovi kreatori još nisu otkriveni, a Microsoft nudi 250 tisuća dolara osobi koja bi pružila informacije koje bi dovele do identifikacije i osude počinitelja. Ovaj je botnet mogao poslati 25 000 spam poruka na sat odnosno 192 spama u minuti sa jednog zaraženog računala, a zadaća mu je bila i instalirati trojance i rootkitove na računala žrtava. Procjenjuje se da je zarazio 2.4 milijuna računala.

1.2. Općenito o malicioznom kodu...

Računalni kriminal je sva aktivnost na i uz pomoć računala, kojom se neovlašteno otuđuje tuđi podatkovni sadržaj ili onemogućava ili usporava korištenje računalnih resursa, s ciljem stjecanja protupravne koristi. (Prof. dr.sc. Željko Hutinski)

Maliciozan kod je kod namijenjen izvršavanju računalnog kriminala. Namjena mu je različita: krađa podataka, DoS i DDoS napadi, uzrokovanje financijske štete, špijuniranje, uništavanje podataka i mnoge druge. Ključne komponente strategije napada su infekcija, perzistencija, komunikacija te komanda i kontrola. Nakon što napadač korištenjem exploita zadobije tzv. „shell access“, u mogućnosti je instalirati maliciozan kod kroz otvorenu aplikaciju ili vezu. Jedan od načina izbjegavanja detekcije je infekcija putem kanala kojima se vjeruje (SSL promet, IM, i sl.). Komunikacija je ključna za dobivanje naredaba, te prenošenje povjerljivih podataka, dok se komanda i kontrola obično ostvaruju preko aplikacija kao što su webmail, društveni mediji, P2P mreže, blogovi i sličnima. [10]

U sljedećoj tablici možemo vidjeti usporedbu nekih osnovnih tipova malicioznog koda.

	Spyware	Virusi	Crvi	Trojanski konji
Rezidentnost u radnoj memoriji	Ne	Da/Ne	Da	Ne
Mogućnost replikacije	Ne	Da	Da	Ne
Zapisivanje na tvrdi disk	Da	Da	Ne	Da
Razina rizika	Visoka	Srednje visoka	Visoka	Visoka
Primjetnost prisutnosti na računalu	Da	Da	Ne	Ne
Izvori zaraze	Internet	Internet, prijenosni računalni mediji (CD, DVD, USB)	Internet	Internet
Učinak na normalan rad računala	Da	Da	Da/Ne	Da/Ne
Utjecaj na pouzdanost podataka na računalu	Ne	Da	Da	Da
Otvaranje mogućnosti za drugu vrstu napada	Ne	Ne	Da	Da
Mogući napadi	-	-	DDoS, MITM	DDoS, MITM
Opasnost od uništavanja podataka	Ne	Da	Da	Ne
Opasnost od krađe podataka	Da	Ne	Da	Da
Nadgledanje aktivnosti na računalu	Da	Ne	Ne	Da

Tabela 1, Izvor: [7]

1.3. Virusi

A virus is a piece of bad news wrapped up in protein.

Sir Peter Medawar, (Biolog nobelovac)

Actually, a computer virus is a piece of bad news wrapped up in software.

Moderna inačica

Računalni virus je maliciozni komad izvršnog koda koji se širi kao privitak dokumenta domaćina (host) koji je obično neka izvršna datoteka. [1] Sastoji se od dijela zaduženog za propagaciju virusa te payloada (korisnog tereta koji je zapravo suština virusa – obavlja radnje na zaraženom računalu specifične za taj virus). Tipični domaćini su, osim izvršnih datoteka koje mogu biti poslane kao e-mail privitak (.com, .exe, .elf), boot sektori floppy i hard diskova, dokumenti koji sadrže makronaredbe (MS Word dokumenti, Excel spreadsheets, Access dokumenti itd.), datoteke za općenitu (grupne datoteke u MS-DOS-u i MS Windowsima te skripte na UNIX platformama) i određenu uporabu i sl. Virusi se obično ugrađuju u izvršne datoteke zato što trebaju dozvolu za izvršenje koda i učitavanje u memoriju.

Prema ponašanju prilikom izvršavanja, viruse možemo podijeliti na rezidentne i nerezidentne. [2] Nerezidentni virusi automatski traže druge domaćine koje mogu inficirati, inficiraju ih i predaju kontrolu programu kojeg su zarazili. Rezidentni virusi se učitaju u memoriju tokom izvršavanja, predaju kontrolu programu domaćinu, te ostaju aktivni u pozadini kako bi zarazili nove domaćine (učitaju se u memoriju odakle se dio za kopiranje pokreće svakom novom akcijom OS-a). Izvršavanje se prekida zatvaranjem programa domaćina, osim u slučajevima skrivenog izvršavanja u pozadini.

Da bi spriječili nekontrolirani rast inficiranih datoteka, virusi koriste takozvani „virus signature“. On se nalazi na nekoj specifičnoj lokaciji u datoteci te označava već inficiranu datoteku, a može biti nešto kao string koji predstavlja neki nepostojeći datum. [1]

Prilikom vlastitog širenja, postoje domaćini koje virusi izbjegavaju. Takvi su primjerice dijelovi antivirusnih programa, budući da antivirusni programi redovito provjeravaju svoj kod, ili pak mamci – mali programi, programi sa ponavljanjima ili pak nevažnim instrukcijama, kreirani od antivirusnog software-a ili programera. Ovi domaćini uzrokovali bi

brzu detekciju virusa, te njihovo uklanjanje. Mamci tako služe i za uzimanje uzoraka virusa kako bi se proučilo njihovo ponašanje i procijenila efikasnost metoda detekcije. [2]

Da bi izbjegli detekciju i uklanjanje, virusi koriste tehnike poput jednostavne automatske modifikacije, enkripcije, polimorfizma te metamorfizma. Od nabrojenih jedino su polimorfizam i metamorfizam učinkovite. Polimorfni virusi inificiraju datoteke kriptiranom kopijom koja se dekriptira dekripcijskim modulom, pri čemu se dekripcijski modul mijenja prilikom svake infekcije, što čini direktnu detekciju potpisom nemogućom. Metamorfni virusi se prilikom svake infekcije u potpunosti reprogramiraju, čemu im, poput polimorfnih, služi metamorfni algoritam.

1.4. Crvi

Računalni crvi (eng. worms) su zlonamjerni programi koji se bez sudjelovanja korisnika šire putem računalnih mreža na druga računala. Za razliku od virusa, crvi na ciljanom računalu ne inficiraju datoteke te imaju sposobnost samostalnog širenja i umnožavanja samih sebe, iskorištavajući propuste u operacijskim sustavima i programima, a karakterizira ih uzrokovanje problema s performansama i stabilnošću računala i računalnih mreža. [3]

Crv se sastoji od četiri dijela: [4]

- Oznaka – opcionalan dio; zadatak joj je spriječiti pokušaj ponovne infekcije
- Infekcijski mehanizam – pronalazi ranjiva računala u mreži
- Okidač – uvjeti za prijenos payloada
- Payload – „korisni dio“; instalira trojanca ili inficira datoteke

Razlikujemo dvije vrste crva: [3]

1. **Host computer worms** (na računalu domaćina) – šire se mrežnom komunikacijom, a nalaze se na računalu domaćinu
2. **Network worms** (mrežni crvi) – svaki modul jednog crva nalazi se na posebnom računalu i provodi različitu aktivnost, mrežna komunikacija služi za komunikaciju između modula. Glavni modul naziva se hobotnica, a nalazi se na jednom od računala, dok se šire kopiranjem određenih dijelova na nezaražena računala.

Postoji nekoliko načina propagacije odnosno distribucijskih mehanizama: [4]

- **Self-Carried** - ova vrsta crva prenosi se kao dio infekcijskog procesa.

- **Second Channel –** koriste sekundarne komunikacijske kanale za infekciju (računala žrtava se spajaju na računalo koje ih je zarazilo skidajući tijelo crva te kompletirajući na taj način proces infekcije)
- **Embedded –** crvi se šalju kao dio komunikacijskog kanala, kao privitak ili zamjenjujući poruku, budući da tako postoji manji rizik od detekcije.
- **Internet worm** - odnosi se na crve koji se kopiraju u dostupne mrežne resurse (direktorije) u lokalnoj mreži, one koji iskorištavaju ranjivosti operacijskih sustava, javnih mreža, ili koriste zlonamjerne programe (backdoor) kako bi dobili pristup u računala ili računalne mreže te ih tako inficirali i stekli kontrolu nad njima

Prema načinu djelovanja, crve možemo podijeliti na: [3]

- **Nepostojeće** ili **nefunkcionalne –** nepostojanje payloada ili greške u payloadu. Jedini cilj je opterećenje mreže
- **Daljinski nadzor –** payload je backdoor koji otvara komunikacijske portove te omogućuju pristup s udaljenog računala
- **DOS –** payload izvodi DOS (Denial of Service) napade na zaraženo računalo
- **Sakupljači podataka –** sakupljaju povjerljive podatke i šalju ih kreatoru
- **Brisači podataka –** payload briše podatke
- **Fizička šteta –** payload čini fizičku štetu (primjerice upisuje pogrešne podatke na BIOS čip)

1.5. Trojanski konji

Trojanski konj je oblik malicioznog koda koji se korisniku lažno predstavlja kao neki korisni softver kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju. [6] Termin ima simboličko značenje koje dolazi iz grčke književnosti, točnije Homerove Ilijade. Želeći okončati dugogodišnji rat, Ahejci su se pokupili s obala Troje i za dugo sjećanje Trojancima ostavili drvenog konja. Trojanci, sretni što su Ahejci otplovili, unijeli su konja unutar gradskih zidina i počeli slavlje. Noću, kad su svi pozaspali, iz konja su izašli najveći ahejski junaci na čelu s Odisejem (kreatorom ideje trojanskog konja) te otvorili vrata Ahejcima koji su se pod okriljem noći došuljali do gradskih zidina, što je označilo kraj Troje. Jednako tako, računalni trojanski konji predstavljaju se kao korisne ili zanimljive aplikacije ili video sadržaji koje korisnik skine, nakon čega preuzimaju kontrolu nad računalom te uzrokuju veliku štetu. Raspon njihovih aktivnosti je velik – od „bezazlenog“ prikazivanja oglasa do uzrokovanja novčane štete za vlasnika zaraženog računala. Ukoliko trojanski konj zadobije potpunu

kontrolu nad zaraženim računalom, napadaču se otvaraju različite mogućnosti malverzacija na i pomoću zaraženog računala poput: [6]

- kreiranje botneta
- krađe povjerljivih informacija i ostvarivanje novčane dobiti
- instaliranja drugih oblika malicioznog koda
- slanja, primanja i modificiranja datoteka zaraženog računala
- „keylogger“ aktivnosti
- „spyware“ aktivnosti
- korištenja memorije hard diska
- ...

Postoji nekoliko vrsta trojanaca prema načinu djelovanja: [5]

- RAT (Remote Access Trojans)
- DST (Data Sending Trojans) – šalju povjerljive podatke kreatoru
- Destructive Trojans – uništavaju podatke
- Proxy Trojans – djeluju kao proxy poslužitelji
- FTP Trojans – djeluju na File Transfer Protocol ili ga iskorištavaju za svoje djelovanje
- Trojanski konji koji sabotiraju sigurnosne programe poput antivirusa i sličnih
- DOS (Denial of Service) – izazivaju DOS napade
- Logičke bombe – izvršavaju se nakon što su zadovoljeni uvjeti za njihovo pokretanje
- Vremenske bombe – izvršavaju se u specifičnom trenutku

Načini širenja trojanaca: [6]

- preuzimanjem zaraženog softvera
- e-mail privicima
- zloćudnim web stranicama sa dinamičkim sadržajem
- kao dio softvera ili iskorištavajući njegove ranjivosti (programi za komunikaciju u realnom vremenu (WLM, AIM...), neki poslužitelji (FTP, SMTP, HTTP...)) kao što su otvaranje komunikacijskih portova

1.6. Spyware

Spyware je vrsta malicioznog programa čija je namjena sakupljanje informacija te preuzimanje kontrole na računalu korisnika bez njegova znanja ili dozvole. [7] Spyware nije u mogućnosti replicirati se, kao što to mogu virusi i crvi.

Možemo ga podijeliti u dvije skupine: [7]

1. **Domestic Spyware** – legalni programi koje na računalo postavljaju vlasnici poduzeća s ciljem nadgledanja aktivnosti zaposlenika, odgovorne osobe koje žele nadgledati djecu ili maloljetnike, ili pak vlasti kako bi pratili osobe za koje se sumnja da krše zakone, nisu besplatni, štite intelektualno vlasništvo, podatke te mrežu
2. **Commercial Spyware** – ilegalni spyware koji služi za prikupljanje informacija o korisnicima na webu, koje se zatim prodaju zainteresiranim stranama (obično neke marketinške tvrtke)

Prema namjeni dijele se na: [7]

- **Internet URL Loggers** – prate web adrese koje korisnik posjećuje, tako što se pozicioniraju na hard disku te su aktivni tijekom pretraživanja
- **Screen Recorders** – rade screenshotove ili video zapise korisničkih aktivnosti, nakon aktivacije okidača (pokretanje web browsera i sl.), a snimke se šalju napadaču
- **e-mail Recorders** – podatke o primljenim i poslanim e-mailovima spremaju u datoteke te šalju napadaču
- **Chat Loggers** – prate komunikaciju putem IM programa
- **Keyloggers** – bilježe aktivnost s tipkovnice, spremaju u .txt datoteku te šalju napadaču. Budući da ih je teško instalirati samostalno, dolaze u kombinaciji sa virusom ili trojanskim konjem
- **Password Recorders** – prate aktivnost tipkovnice prilikom upisivanja znakova u polje za lozinku
- **Tracking Cookies** – prate korisnikova pretraživanja
- **Browser Hijackers** – otimači web preglednika koji ometaju rad preglednika zamjenjujući početnu stranicu, stranicu pogreške i tražilicu vlastitom.
- **Modem Hijackers** – kod dial-up modema biraju skupe brojeve prilikom spajanja na internet te tako uzrokuju financijsku štetu
- **PC Hijackers** – napadač preuzima nadzor nad računalom i šalje e-mailove na ciljane adrese

Posljedice zaraze računala spywareom su prvenstveno spor rad računala te čudno ponašanje. Nakon toga, tu su i simptomi poput visoke aktivnosti procesora, zauzeća memorije, pojavljivanje reklama, smrzavanja programa i računala, nemogućnost spajanja na internet ili LAN i slični.

1.7. Rootkit

Rootkit je maliciozan kod koji je dizajniran kako bi prikrio prisutnost drugog malicioznog koda. Obično dolazi u kombinaciji sa backdoorom, kako bi ga korisnik što teže detektirao te kako bi napadaču omogućio udaljeni pristup. Nakon što zarazi računalo, rootkit postaje nevidljiv OS-u, antivirusnim programima i sistemskim alatima.

Na UNIX-u, administratorski se račun zove još i „root“, dok se kompromitiranje računala i prisvajanje administratorskih prava naziva „rooting računala“. Nakon što maliciozni kod zarazi računalo, na neki način mora ostati sakriven. Tome služi rootkit, poznat i kao „kit for maintaining root“. Rootkit je set binarnih i konfiguracijskih datoteka te skripta, koji omogućava zadržavanje pristupa i kontrole na računalu, bez uznemiravanja korisnika. [9]

Rootkit možemo podijeliti na kernel i user mode verzije. **Kernel** mode rootkitovi napadaju na Windows API nivou, pa će aplikacije koje vuku podatke iz Native API nivoa prikazivati promijenjene podatke. Naime, jedina zadaća Native API funkcija je pozivanje sistemskih servisa u kernel modu, a na nivou jezgre izvršavaju se procesi pristupanja hardwaru preko funkcija za rukovanje memorijom, uređajima i procesima. **User** mode rootkitovi imaju mogućnost prikrivanja svakog, pa tako i malicioznog procesa pod istim korisničkim računom, te tako dobivaju kontrolu nad svim procesima računala.[8] Prema preživljavanju reboota, dijele se na trajne ili **perzistentne**, koji se pokreću automatski, te **memorijske** koji budu likvidirani rebootanjem.

Rootkit može biti instaliran na različite načine. Primjerice, može biti dio payloada nekog exploita, dok se unutar payloada nalazi dropper, program koji ga instalira na računalo, nakon čega se pristojan dropper obriše. Dropper također može promijeniti rootkit (kompresirati ga, kodirati ili kriptirati) i zatim ga enkapsulirati kao internu strukturu podataka, sve kako bi prošao sigurnosna skeniranja. Višerazinski dropperi ne sadrže rootkit, već programe (sftp.exe, stub.exe) čija je zadaća preuzeti rootkit sa neke zadane lokacije, ili pak neki veći program koji će zatim skinuti rootkit i instalirati ga. Na taj se način smanjuje količina tragova koju dropper ostavlja, te čak i ako dođe do otkrivanja droppera koji se nije obrisao, neće biti moguće analizirati rootkit. Rootkit također može neposredno ili posredno biti instaliran zahvaljujući tehnikama poput socijalnog inženjeringa, zaraženih USB stickova, softverskih paketa itd. [9]

1.8. Botnet

Bot je individualno zaraženo računalo, dok je botnet široka mreža botova koji zajedno rade na ostvarenju nekog cilja, sukladno uputama kreatora. Cilj kreiranja botneta je velika moć koju njihovo posjedovanje daje njihovom kreatoru, a koju on gotovo uvijek iskorištava za određene ilegalne, maliciozne radnje. Botovi koji se nalaze pod kontrolom napadača (tzv. „bot-herder“) mogu se ažurirati, odnosno, napadač im može promijeniti agendu - preusmjeriti ih - kako bi radili sukladno njegovim interesima. Jedna od opasnosti botova je da često prikupljaju povjerljive podatke te ih šalju na zadane udaljene lokacije. Također, botnet može biti multifunkcionalan – napadač može određene dijelove botneta koristiti za različite operacije (slanje spama, krađu povjerljivih podataka i sl.). Ukoliko botovima onemogućimo vezu sa njihovim serverima, neutralizira se njihovo djelovanje (budući da ovise o instrukcijama napadača, a serveri im također služe za upload podataka), što se još poznato i pod nazivom „takedown“ ili „decapitation“.

Botnetovi predstavljaju veliku prijetnju korporacijama, budući da su njihove funkcionalnosti gotovo bezgranične. Botnete možemo podijeliti na špijunske i financijske botnetove, te one koji služe za „ciljane upade“ (eng. targeted intrusion). Špijunski su oni koji se bave slanjem spamova bez korisnikova znanja. Ovi botnetovi se često koriste za izazivanje DDoS (Distributed Denial of Service) napada – opterećivanja ciljnih servera slanjem prometa sa mnogo botova, pri čemu dolazi do popunjenja mrežnih ili serverskih kapaciteta i nemogućnosti pružanja usluga korisnicima. Cilj ovih napada također može biti i iznuđivanje novca. Financijski botneti obično uzrokuju ogromnu financijsku štetu kradući podatke o brojevima kreditnih kartica, narušavajući ugled kompanija i sl. Određena vrsta botneta manje veličine, specijalizirala se za kompromitiranje sustava visoke važnosti koji će im mogućiti kasnije provaljivanje u ciljane mreže. Zaražena im računala služe kako bi dobili pristup zaštićenim sustavima i uspostavili backdoor u njihove mreže. Ovo je možda i najopasnija vrsta botneta budući da ju je vrlo teško detektirati antivirusnim programima, a cilj su joj najvrednije informacije korporacije (vezane uz istraživanje i razvoj, intelektualno vlasništvo, strateško planiranje, financijski i korisnički podaci). [10]

1.9. Detekcija i uklanjanje

Već smo nabrojili neke od simptoma infekcije računala. Osim nabrojenih, tu su još i čudna ponašanja prilikom pretraživanja (zamjena pretraživača), mijenjanje korisničkih postavki u zadanom pregledniku (favorites, bookmarks, home page), pop-up oglašivački prozori kad postoji veza na internet i kad ne postoji i slični.

Za detekciju i uklanjanje virusa možemo koristiti za to specijalizirane programe. Također, postoje komercijalna i besplatna sigurnosna rješenja, koja su u stanju zaštititi računala korisnika od „neželjenih posjetioca“. To su rješenja tvrtci kao što su Avast!, Avira, Misrosoft (Security Essentials), Panda, Comodo, Norton, BitDefender, G-Data, Kaspersky, Eset i drugih.Također, Carnet CERT preporuča Spybot Search & Destroy, te Ad-aware, kao dva programska alata za zaštitu osobnih računala kroz detekciju i uklanjanje svih vrsta spyware-a, adware-a, dialera i sl. Za uklanjanje malicioznih kodova preporučaju Wintasks Pro, koji služi za nadgledanje procesa te provjeravanje vrste procesa (spyware, trojanac, legitiman proces), razvrstane u tri kategorije (security risks, system processes, applications). Pritom također daje informacije o autoru procesa, aplikaciji kojoj proces pripada, sigurnosnom riziku i sličnom. Tu je također i System Safety Monitor, koji sprečava instalaciju malicioznog programa ubacivanjem u legitiman proces, kontrolirajući aktivne programe i procese.

Malware ima mogućnost automatskog pokretanja postavljanjem u Startup, ili pak instalacijom kao driver/servis. Da bi se neutraliziralo takav malware, potrebno je ukloniti njegovu auto-start metodu. Te su metode najčešće mapa Autostart (sadrži popis svih auto-start programa i njihovih dijelova), datoteka Win.ini (sadrži popis programa koji su se u inačici 3.x Windowsa automatski pokretali), System.ini (sadrži popis objekata koji su spremni za rad prilikom ponovnog pokretanja OS-a), ili pak Registry datoteka . Kod Windowsa, pomoću System Configuration Tool (kartica Startup), moguće je onemogućiti automatsko pokretanje određenih programa. Spyware programe je također moguće obrisati iz Win.ini kao i System.ini datoteke. [11]

Windows Sysinternals je stranica koju su 1996. Izradili Mark Russinovich i Bryce Cogswell, a sadrži različite programe programske podrške (eng. Utilities). Tako tu možemo naći različite alate za borbu protiv malicioznog koda kao što su Process Explorer (sadrži popis aktivnih procesa sa njihovim detaljnim informacijama), AutoRuns (prikazuje sve programe koji se automatski pokreću prilikom dizanja sustava ili prijave), Process Monitor (prikazuje real-time file system, Registry te aktivnost procesa i dretvi), RootkitRevealer (prikazuje Registry i file system API nekonzistentnosti koje upućuju na postojanje rootkita), TcpView (prikazuje koje aplikacije komuniciraju s kojim IP adresama) i slično.

Na kraju, važno je naglasiti da je najbolja metoda borbe s malicioznim kodom prevencija.

2. Stuxnet

Za Stuxnet se može reći da je maliciozni kod nove ere – upotrijebljen u cyber ratovanju, on je razoran kod koji može uništiti zgrade, strojeve, pa čak i uzrokovati smrt ljudi. Njegova je primarna svrha bila sabotirati iranski nuklearni program, o kojem se još danas vode pregovori između najmoćnijih zemalja svijeta. Da bi ostao skriven dovoljno dugo, koristio je čak četiri „zero-day" ranjivosti Windowsa, Windows rootkit, PLC rootkit, tehnike za izbjegavanje antivirusnih programa, kompleksni proces ubacivanja, „peer-to-peer" ažuriranja i drugo, dok se u iranski nuklearni program infiltrirao inificirajući PLC-ove (Programmable Logic Controller) koji služe za kontrolu strojeva, te oštetio iranski nuklearni reaktor radeći promjene u ponašanju strojeva što je dovelo oštećivanja ili uništavanja centrifuga. To mu je uspjelo korištenjem „default" lozinke Siemens uređaja kako bi dobio pristup programima koji kontroliraju i modificiraju kod PLC-ova. Stuxnet se može koristiti za sabotažu bilo kojih industrijskih kontrolnih sustava.

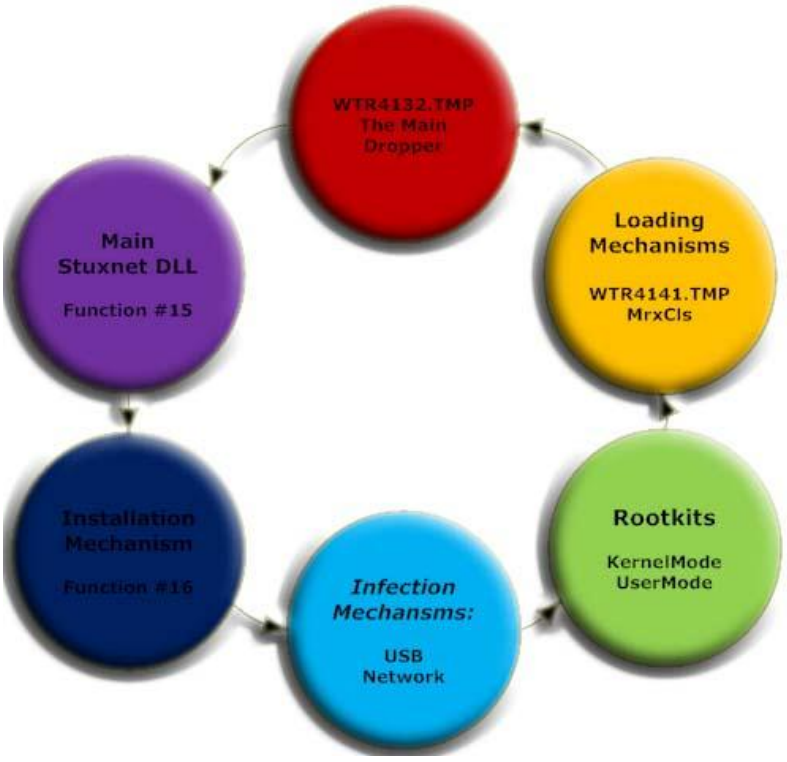
Nakon što zarazi određeno računalo, Stuxnet prvo prenese informacije o konfiguraciji sustava na komandno-kontrolni server, nakon čega je moguće reprogramiranje mete. Neke od njegovih karakteristika su: [13]

- Koristi ranjivost koja omogućuje automatsko izvršavanje, samoreplicirajući se kroz prijenosne diskove (*Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability*)
- Širi se LAN-om koristeći ranjivost u Windows Print Spooler-u (*Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability*)
- Širi se kroz SMB (Server Message Block) (*Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability*)
- Kopira se i izvršava na udaljenim računalima kroz mrežni promet (dijeljenja)
- Kopira se i izvršava na udaljenim računalima koristeći WinCC poslužitelj baze podataka
- Kopira se u Step 7 projekt, te se automatski izvršava kad se projekt učita
- Ažurira se koristeći peer-to-peer mehanizme LAN-a
- Kontaktira komandni i kontrolni server što omogućuje hakeru da preuzme i izvrši kod
- Sadrži Windows rootkit
- Zaobilazi sigurnosne aplikacije

- Modificira kod Siemens PLC-ova s ciljem sabotaže sustava
- Sakriva modificirani kod na PLC-ovima (PLC Rootkit)

Industrijskim kontrolnim sustavima (ICS) upravljaju kodovi poput PLC-ova koji su često namijenjeni za računala koja nisu spojena u mrežu. Zbog toga je napadaču primaran cilj da uspostavi vezu. Da bi to mogao, mora nabaviti ICS shemu, nakon čega treba postaviti zrcaljeno okruženje (eng. mirrored environment) koje će uključivati potreban hardver za testiranje koda (nove verzije Stuxneta). Da bi se izbjegla sumnja, datoteke moraju biti digitalno potpisane. Nakon što upozna okružje mete, inificirajući neku treću stranu, možda i neizravno uključenu, kao što je to primjerice osoba vezana ugovorom, spreman je zaraziti računala unutar organizacije, i to obično koristeći prijenosne diskove. Kroz LAN se širi koristeći Step 7 projekt „zero-day“ ranjivost, i putem prijenosnih diskova. Nakon što pronađe pogodno računalo, Stuxnet će promijeniti PLC kod, te će tako sabotirati sustav, pri čemu žrtva neće biti svjesna da je PLC kod modificiran, te da postrojenje ne radi kako bi trebalo. [13]

Nedostatak ovog pristupa je što, kada pokušavaju sabotirati metu, napadači usput zaraze i računala izvan mete, koja se smatraju kolateralnom štetom. Također, to uvećava i rizik da će maliciozni kod biti otkriven prije nego postigne svoju svrhu, zbog čega je potrebno da se napad ostvari u što kraćem vremenskom periodu.



Slika 1, Životni ciklus, Izvor [12]

Jezgra Stuxneta je velika .dll datoteka koja sadrži mnogo različitih resursa, te dva kriptirana konfiguracijska bloka. Dropper komponenta je wrapper program koji sadrži sve ove komponente u sekciji koja se zove „stub“, a koja je suština načina na koji Stuxnet radi – wrapper ekstrahira .dll datoteku iz stub sekcije, i mapira je u memoriju kao modul, nakon čega se poziva jedan od DLL „exportova“.

Table 3

DLL Exports

Export #	Function
1	Infect connected removable drives, starts RPC server
2	Hooks APIs for Step 7 project file infections
4	Calls the removal routine (export 18)
5	Verifies if the threat is installed correctly
6	Verifies version information
7	Calls Export 6
9	Updates itself from infected Step 7 projects
10	Updates itself from infected Step 7 projects
14	Step 7 project file infection routine
15	Initial entry point
16	Main installation
17	Replaces Step 7 DLL
18	Uninstalls Stuxnet
19	Infects removable drives
22	Network propagation routines
24	Check Internet connection
27	RPC Server
28	Command and control routine
29	Command and control routine
31	Updates itself from infected Step 7 projects
32	Same as 1

Slika 2, Izvor [13]

Glavna .dll datoteka sadrži sav kod potreban da se kontrolira crv, a svaki njen export ima neku od funkciju prikazanih na Slici 1. Exporti koriste resurse kako bi lakše kontrolirali crva, a resursi mogu biti .dll datoteke ili predlošci izvršivi od strane konfiguracijskih datoteka ili exploit modula.

Table 8

Comparison of Resources

March 2010		June 2009	
Resource ID	Size	Resource ID	Size
201	26,616	201	19,840
202	14,848	202	14,336
203	5,237		
205	433	205	323
		207	520,192
208	298,000	208	298,000
209	25	209	25
210	9,728	210	9,728
221	145,920	221	145,920
222	102,400	222	102,400
		231	10,752
240	4,171		
241	25,720		
242	17,400		
250	40,960		

Slika 3, Izvor [13]

Na slici 2 vidimo dvije verzije crva iz 2010. i 2009. godine. Zeleni resursi su dodani u posljednjoj verziji, a crveni maknuti iz stare verzije. Vidimo da novije varijante imaju više resursa manje veličine.

Stuxnet ima nekoliko metoda propagacije. To su: [13]

- Mrežna propagacija
    - Peer-to-peer komunikacija i ažuriranja
    - Inficiranje WinCC računala preko „hardcoded“ lozinke poslužitelja baze podataka
    - Propagacija kroz mrežni promet
    - Propagacija koristeći Print Spooler Zero-Day Vulterability
    - Propagacija koristeći Windows Server Service Vulnerability
- Propagacija prijenosnim diskovima

Smatra se da iza ovog napada stoji Izrael, koji javno kritizira iranski nuklearni program, te pokušava sabotirati pregovore o njegovoj „legalizaciji“ odnosno prihvaćanju, tvrdeći da to ugrožava njegovu sigurnost u regiji. Rašireno je mišljenje da je sa Izraelom surađivao njegov „veliki brat“ SAD, te da je Stuxnet bio njihov zajednički projekt. Smatra se da su testiranja izvršena u Dimona nuklearnom kompleksu u Izraelu 2008. i 2009. godine. Iran je razvijena, bogata i moćna zemlja kojoj se Izrael ne može vojno suprotstaviti bez pomoći SAD-a, zbog čega mu odgovara da njegova vojna moć oslabi u usporedbi sa izraelskom (javna je tajna da Izrael posjeduje nuklearno oružje), baš kao i financijska, pod utjecajem sankcija koje je Iranu

nametnuo SAD. Pa ipak, ovih dana svjedočimo djelomičnom porazu Izraela, te pobjedi Irana koji je sa predsjednikom H. Rohanijem na čelu, dogovorio kompromis prema kojem će Iran nastaviti razvijati svoj nuklearni program isključivo u gospodarske svrhe, dok će SAD (možda) zauzvrat ukinuti određene gospodarske sankcije nametnute ovoj zemlji.

Osim Irana, najveću su štetu pretrpjele Indonezija, Indija i Sjeverna Koreja.

3. Literatura

[1] Avi Kak, Purdue University, 2013, Malware: Viruses and Worms, https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture22.pdf Dostupno 24.11.2013.

[2] Milan Vukušić, FER, 2005., Virusi u izvršnim datotekama, http://web.zpr.fer.hr/ergonomija/2005/vukusic/virusi.pdf Dostupno 24.11.2013.

[3] CERT, Conficker, http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-03-294.pdf Dostupno 24.11.2013.

[4] Mohammad Heidari, 2004, Malicious Codes in Depth, http://target0.be/madchat/vxdevl/papers/avers/Mal_Codes_in_Depth.pdf Dostupno 24.11.2013.

[5] Trojanici, Sigurnost@CARNet, https://security.carnet.hr/vise-o-sigurnosti/enciklopedija/trojanci/ Dostupno 24.11.2013.

[6] Trojanski konji, CERT, http://www.cert.hr/malver/trojanski_konji Dostupno 24.11.2013.

[7] Spyware programi, CERT, http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-10-280.pdf Dostupno 24.11.2013.

[8] Rootkiti na Windowsima, Carnet, http://sistemac.carnet.hr/node/6 Dostupno 26.11.2013.

[9] Jones & Bartlett Learning, The Rootkit Arsenal, 2013, LLC, Ascend Learning Company

[10] Lawrence C. Miller, CISSP, MM for Dummies, 2012, LLC, John Wiley & Sons, Inc.

[11] Malware programi, CERT, http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-02-107.pdf Dostupno 26.11.2013.

[12] Amr Thabet, Stuxnet Malware Analysis, http://www.codeproject.com/KB/web-security/StuxnetMalware/Stuxnet_Malware_Analysis_Paper.pdf Dostupno 16.12.2013.

[13] Falliere, Liam O Murchu, Eric Chien, W32.Stuxnet Dossier, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf Dostupno 16.12.2013.