*International Journal of Scholarly Papers for Media and Society Research*

Media dialogues
MEDIJSKI DIJALOZI
ISSN 1800-7074 (*print*)
ISSN 2536-5622 (*on line*)

**Miladinovic Bogavac, Z. (2018), „Concept, Types and Methods of Operation of Malware for Producing Internet Frauds",**
***Media dialogues / Medijski dijalozi*, Vol. 11, No. 1, pp. 97-113.**

dr **ŽIVANKA MILADINOVIĆ BOGAVAC**, docent
Fakultet za poslovno industrijski menadžment,
Univerzitet Union Nikola Tesla
Srbija

# CONCEPT, TYPES AND METHODS OF OPERATION OF MALWARE FOR PRODUCING INTERNET FRAUDS

***Abstract:*** *Malicious or unwanted software (malware ) means every program that can go into the computer system without the knowledge and will of the users, with the intent to compromise computer content or network. This group includes software which are created for Win-dows and Linux operating systems and also Macintosh and Palm computers. They use the Internet for their expansion, especially email end World Wide Web (WWW). The paper will be displayed their classification , mode of operation and spread.*
***Key words:*** *Internet Fraud, Malware, Cyber Crime, Internet.*

# POJAM, VRSTE I NAČINI DELOVANJA MALICIOZNIH PROGRAMA KOJIMA SE SPROVODE INTERNET PREVARE

***Apstrakt:*** *Pod zlonamernim ili nepoželjnim programom podrazumeva se svaki program koji može da se useli u računarski sitem bez znanja i volje korisnika, a napravljen je s namerom da ugrozi računarski sadržaj ili mrežu. U tu grupu spadaju softveri kreirani za Windows i Linux operativne sisteme i Macintosh i Palm računare, a koji za svoje širenje koriste internet, posebno*

*imejl i World Wide Web (WWW). U radu će biti prikazana njihova klasifikacija i način delovanja i širenja.*
***Ključne riječi:*** *Internet prevara, maliciozni program, sajber kriminal, Internet.*

## 1. UVOD

Za uspešno sproveden napad malicioznim programom potrebne su 3 komponente:

- motivisan napadač;
- nedostatak odgovarajuće zaštite;
- pogodna meta (može da bude bilo koja osoba ili imovina nad kojima napadač želi da preuzme kontrolu) - Više o tome: Bossler, Holt and Malware Victimization, 2011, pp. 320–321.

Nakon inficiranja računarskog sistema neautorizovanim i za korisnika neočekivanim procesima, maliciozni softver koristi se za:

- narušavanje performansi sistema i dovođenje sistema u nestabilno stanje. Prvobitni oblici malicioznih programa u 80-im i 90-im obično su bili oblik vandalizma, ili neslane šale koja se koristila za onemogućavanje ili otežavanje izvođenja pojedinih operacija na računaru. Međutim, ,,apetiti" sajber prevaranata ubrzo su porasli, pa su maliciozne programe, osim za šalu i vandalizam, iskoristili za sticanje profita. Maliciozni program korišćen je za uspostavljanje kontrole nad dial-up modemom i pozivanje skupih telefonskih brojeva (premium-rate), te korisnik na kraju meseca dobija ogroman telefonski račun za koji su zaslužni prevaranti;
- neovlašćen pristup sistemu računara. Kada se uspostavi kontrola, zaraženi računari koriste se da rade za autora malicioznog softvera. Tako se spomenuti računari koriste kao proxy za slanje spam poruka. To su zombi ra-čunari (zombie computers). Prednost korišćenja zaraženih računara za slanje spam poruka je anonimnost koju pružaju.
- prikupljanje informacija koje uzrokuje njihovu zloupotrebu i gubitak privatnosti korisnika. Koristeći malver, sajber prevaranti prikupljaju sve informacije koje su im potrebne za napad, tj. prevaru, kao što su, npr., spisak poslovnih partnera, brojevi računa, dosada-

šnje transakcije, poslovna prepiska, administratorske šifre ovlašćenih osoba koje obavljaju transakcije, korisnička imena i lozinke;
- ostale zlonamerne aktivnosti.

## 2. KLASIFIKACIJA ZLONAMERNIH MALICIOZNIH PROGRAMA

Po kriterijumu samostalnosti, tj. potrebe za programom u kom će maliciozan program biti sakriven, malvere možemo podeliti na: a) one kojima je neophodan nosilac, tj. program u kom će biti sakriveni (trojanski konji, virusi) i b) samostalne, tj. one kojima nije neophodan nosilac (crvi, špijunski programi). Po kriterijumu mogućnosti repliciranja, možemo napraviti podelu na: a) malvere koji se repliciraju (virusi, crvi) i b) malvere koji se ne repliciraju (trojanski konji).

Jedna od najobuhvatnijih klasifikacija, ako se ima na umu njihovo svakodnevno uvećavanje i težnja da broj malicioznih programa pretekne broj onih legitimnih, jeste klasifikacija na:

- zarazne, čiji su tipični primeri virus i crv;
- sakrivene, čiji su tipični primeri trojan horse i rootkit;
- koristoljubive – čiji su tipični primeri spayware, adware i dialer (Više o tome: Ranđelović i Popović, 2010, str. 19–24).

Crvi i virusi su najpoznatiji tipovi malicioznih softvera. Oni su karakterisani kao zarazni maliciozni softveri jer stvaraju probleme inficiranom računaru tako što otežavaju njegovo funkcionisanje. Razlikuju se po načinu širenja: crv se širi preko mreže sa ciljem da zarazi druge računare, a virus inficira izvršni program, koji, kada se pokrene, počinje da se širi i na druge programe. Uz to, virus, da bi se širio, koristi korisnikovu intervenciju, dok crv automatski vlada računarom. S obzirom na navedeno, može se zaključiti da crvi mogu napraviti veću štetu zbog mrežnog prometa koji generišu prilikom širenja internetom. Finansijska šteta uslovljena virusima samo za 2000. je iznosila 17 milijardi dolara u SAD. 2003. ona je bila veća od 12 milijardi dolara.

## 3. CRVI

Crvi su samostalni maliciozni programi koji se šire putem elektronske pošte, web-a i instant messenger-a. Mogu se smatrati podgrupom virusa, to su kompjuterski programi koji se sami prave i prave štetu sistemu tako što iniciraju mnoštvo procesa koji prenose podatke. Prvi crv koji su se širili mrežom bili su namenjeni za Unix uređaje. Tadašnji Internet Worm pojavio se 1988.

godine i ugrožavao je SunOS i VAX BSD sastave. Elektronske poruke koje sadrže crv obično koriste tehnike socijalnog inženjeringa da bi navele primaoca da otvori prilog. U najvećem broju slučajeva naziv i ekstenzija priloženog fajla dozvoljavaju crvu da se kamuflira kao neizvršni program (fajl, na primer, ima ekstenziju slike ili filma). Pojedini crvi koriste softverske greške (engl. bug) najpopularnijih programa za razmenu elektronske pošte (poput programa Microsoft Outlook Express), tako da se automatski aktiviraju u trenutku prikazivanja inficirane poruke. Primeri tih crva su: Netsky, MyDoom i Sasser.a.Svi napredniji crvi falsifikuju adresu pošiljaoca i na taj način stvaraju neprijatan kolateralni efekt širenja inficiranih poruka – antivirusni programi instalirani na serveru vraćaju zaraženu poruku na adresu s koje je poslata, ali, s obzirom na to da je lažna, zaražena poruka stiže nekom drugom, a ne pravom pošiljaocu poruke elektronske pošte (Mailer i mass-mailer).

Crvi se mogu prenositi putem:

- e-pošte (tzv. imejl crvi). Imejl crvi koriste metode socijalnog inžinjeringa da bi naterali korisnika da pokrene program koji se nalazi u prilogu ili da pristupi hiperlinku. Poruke su da bi bile primamljivije često sledeće sadržine: „an important thing about you", „critical windows update", ili „meet the love of your life". Kada korisnik pristupi predloženoj vezi ili pokrene poslat program, crv se aktivira. Nakon inficiranja računara crv će svoje kopije poslati na imejl adrese memorisanih na zaraženom računaru;
- instant poruka (IM crvi). Ovi crvi koriste servise za komunikaciju poput Microsoft MSN-a, Skype-a, Yahoo Messenger-a, ICQ-a, AOL AIM-a i druge. U ovom slučaju crv će se širiti kada korisnici pristupe inficiranoj veb-lokaciji ili datoteci predloženoj putem poruka ovog tipa;
- interneta. Ovo je najlakši način da se iskoriste računari koji nemaju sigurnosne programe ili firewall, kao i iskorišćavanje otvorenih portova;
- deljenja datoteka (file-sharing crvi). Crv će u ovom slučaju težiti da se iskopira u deljeni fajl pod imenom koje će asocirati korisnika na to da se radi o uslužnoj aplikaciji koja je neophodna za rad računara;
- P2P mreže. Tada se crv kopira u P2P deljeni fajl. P2P mreža nakon toga pomaže dalje širenje crva tako što informiše druge korisnike o postojanju novog resursa i obezbeđuje preuzimanje deljenog fajla.

Apsolutna zvezda u svetu malicioznih programa je kompjuterski crv Stuxnet, prvi maliciozni program napravljen da napadne industrijske sisteme kao što su elektrane i nuklearni reaktori. Taj crv napravljen je sa ciljem da usporava i ubrzava centrifugu, tj. šuplje cevi koje se okreću velikom brzinom i koriste se za fiziju izotopa U-235 u U-238, a koji se nalazi u prirodnom uranijumu. Stuxnet je otkriven u junu 2010. godine kada je njegova meta bio Iran, koji je svoj projekat gasnih centrifuga započeo 1987. godine njihovom instalacijom u podzemnom postrojenju Natanz u centralnom Iranu. Stuxnet je pogodio kompjuterske sisteme širom Irana, uključujući i one koji nisu kritični za rad nuklearnih reaktora. Za opisane koordinisane akcije usmerene protiv iranskog nuklearnog programa optužene su zapadne zemlje i Izrael[1]. Za razliku od kompjuterskih crva koji zaražavaju ceo sistem, napadi DoS-a su usmereni na konkretne kompjuterske sisteme. Napad DoS-a čini resurse kompjutera nedostupnim za legalne korisnike. Tokom 2000 zabeleženi su napadi na CNN e-bay, Amazon A 2009. su zabeleženi napadi na državne i komercijalne veb sajtove u SAD i Južnoj Koreji i onesposobile sistem za nekoliko sati. Kazne za ove napade DoS su teško ostvarive, s obzirom na to da ovi napadi mogu da ne proizvedu fizičko oštećenje kompjutera. Kompjuterski crv SQL Slammer je zarazio 90% kompjuterskih sistema tokom prvih 10 minuta širenja. Finansijska šteta koja je proistekla od ranjavanja kompjuterskog sistema crvom je 2000. iznosila 17 milijardi američkih dolara, dok je 2003. bila preko 12 milijardi dolara.

## 4. VIRUSI

Termin „virus" je u informatičkom smislu prvi upotrebio Fred Koen (Fred Cohen), student Univerziteta Južne Kalifornije, u članku objavljenom 1984. godine pod naslovom Eksperimenti s računarskim virusima (Experiments with Computer Viruses)[2]. Virus sam po sebi nije program koji se autonomno instalira, kao što i njegov biološki imenjak nije sam po sebi oblik života. Informatički virus ne koristi mrežne resurse, već ubacuje svoje kopije u instalacioni program. Na taj način, kada korisnik aktivira program, prvo se neprimetno aktivira virus, a zatim i program.

---

[1] Više o tome: The Real Story of Stuxnet How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, poslednji put pristupili 12.04.2016.godine.

[2] Više o tome: Cohen, F., Computer Viruses Theory and Experiments, „Computers and Security", vol. 6, 1987 r. 22–35.

Virus je deo složenijeg koda koji se širi unutar jednog računara ili računarske mreže kopirajući se unutar drugih programa ili u određenom delu hard-diska računara, tako da se može aktivirati otvaranjem inficiranog fajla. Nakon instaliranja softvera virus samo replikacijom inficira ostale fajlove u računaru ili mreži, i to najčešće bez znanja korisnika. Virus obično sadrži nekoliko „instrukcija" koje se mogu odnositi na proizvođenje sopstvenih kopija i širenje epidemije. Međutim, virus može sadržati i mnogo štetnije instrukcije, poput brisanja ili uništavanja fajlova, formatizovanja hard-diska, ili otvaranja sporednih vrata.

Pre veće dostupnosti interneta virusi su se širili tako što bi zarazili boot sektor ili disketu. Ti virusi bili su napisani za Apple II i Macintosh, ali su se počeli širiti s pojavom IBM PC-a i MS-DOS-a[3]. Godine 1981. i zvanično je potvrđeno postojanje računarskog virusa Elk Cloner[4]. Godinu 1988. obeležilo je haranje virusa Jerusalim, koji je brisao sve pokrenute programe[5]. Sledeću godinu, osim što je obeležila ekspanzija virusa Datacrime, koji je bio sposoban da izvrši low-lewel format nulte staze na disku, karakterisalo je i to što se prvi put pojavila firma virusa u Bugarskoj[6]. Ranije verzije virusa bile su napisane da deluju kao šala, tj. kao bezopasni i dosadni programi. Virusi David i crv Melissa[7], koji su inficirali ukupno 20% tadašnjih korisnika interneta, predstavljali su eksperiment njihovih tvoraca, bez ikakve štetne namere vandalizma[8].

Globalno informaciono-komunikaciona mreža je doprinela da osnovni način prenošenja zaraze postane razmena fajlova putem elektronske pošte, programa za komunikaciju i razmenu fajlova među korisnicima. Taj period obeležila je pojava takozvanih makrovirusa, čije su „instrukcije" napisane rečnikom skripting-programa (engl. Scripting program), kao što su „MS-Word" i „Outlook". Ti virusi su posebno usmereni na inficiranje različitih verzija Majkrosoftovih (Microsoft) programa razmenom dokumenata. Nadalje, operativni

---

[3] Više o tome: History of Mac malware: 1982 – 2011, https://nakedsecurity.sophos.com/2011/10/03/ mac-malware-history/

[4] Više o tome: 6 Computer Viruses That Changed The World, http://www.makeuseof.com/tag/6-computer-viruses-changed-world/

[5] Više o tome: VB – Virus Bulletin, https://www.virusbtn.com/pdf/magazine/1990/199003.pdf

[6] Više o tome: Computer Virus History I, http://www.mindpride.net/root/Extras/ Viruses/computer_virus_history_1.htm

[7] Više o tome: Melissa (computer virus), https://en.wikipedia.org/wiki/Melissa_(computer _virus)

[8] Više o tome: Top Ten Most Destructive Computer Viruses of All Time, http://crunkish.com/top-ten-worst-computer-viruses/

sistemi Majkrosofta najviše su pogođeni virusima zato što su i najrasprostranjeniji među takozvanim nestručnim korisnicima. U svakom slučaju, činjenica je da ne postoje sistemi koji su potpuno, ili teorijski imuni na viruse, budući da anatomija interneta dozvoljava računarskim virusima da se mnogo efikasnije šire nego ranije.

S porastom popularnosti interneta, maliciozni softver sve više nastaje zbog želje za profitom, a ne za šalom i destrukcijom, kao što je bio slučaj s DOS-virusima, koji su brisali podatke s diska ili menjali sastav foldera zapisivanjem nepravilnih podataka u njih. Od 2003. godine većina rapidno širećih virusa i crva dizajnirana je za preuzimanje kontrole nad računarima korisnika namenjenim za crno tržište. Virus može da konzumira memoriju tako što se upisuje na kraj exe izvršnih fajlova koji se pokrenu na zaraženom računaru. Veličina zaraženih fajlova povećava se za oko 1 kilobajt a virusom biva zaražen i svaki drugi računara kom pokrene neki od zaraženih fajlova[9]. Takav virus, pod nazivom 5lo, otkriven je oktobra 1992. godine[10]. Virus može da funkcioniše kao P2P program za šerovanje koji s drugih zaraženih računara skida fajlove razne sadržine, poput muzike, pornografije, pa čak i celih igara i, po mogućnosti, instalira ih. Zaraženi računar takođe služi kao izvor fajlova drugim zaraženim računarima. Primer ovog virusa je Ares.exe, verzija crva Gaobot.ee[11], koji bitiše pod imenom ARES. Postoje sumnje da ovaj virus skida i instalira spajver, druge viruse, trojance i crve, mada te tvrdnje nisu nikada zvanično dokazane.

---

[9] Pošto je jednom pokrenut, virus se smešta u radnu memoriju koristeći instrukciju INT 21, AX=3521h. Svaki fajl koji će se pokrenuti biće zaražen tako što će virus dodati svoj kod i poruku promenljive sadržine na njegov kraj. Nakon toga virus menja vreme nastanka fajla na vreme kada je zaražen, a i njegovo polje 0Ch u zaglavlju fajla na FFAAh. Dužina inficiranog dela fajla kreće se od 1.000 do 1.100 bajtova, a najčešća dužina je 1.032 bajta. Gde god je neki zaraženi fajl pokrenut, virus se prebaci u radnu memoriju. Virus inficira jedan fajl samo jednom, a u memoriji može postojati samo jedna njegova instanca.Najćešća poruka koju virus dodaje na neposredan kraj fajla je: 92.05.24.5lo.2.23MZ. Druge poruke sadrže se u samom virusu. Virus instaliran u memoriji ne može se naći pomoću MEM/C zato što se instalira tako da ga pokreće sam operativni sistem. Slobodna memorija se smanji za oko 2 kilobajta.

[10] Najpoznatije verzije 5lo su Ares.exe, Brontok, Natas, W32.Mytob.V@mm, W97M.Verlor, Win32.Parite, ZMist i Zenux.

[11] Gaobot.EE je crv koji pomoću spostvenog SMTP mehanizama šalje brojne spam mejlove. Crv na zaraženom računaru takođe otvara slučajno izabran TCP port i obaveštava moguće napadače na prethodno odabranom IRC kanalu, gde pokušava da deaktivira sigurnosne sisteme i alat za nadgledanje operativnog sistema.

Brojni su virusi koji se šire tako što sami sebe šalju na imejl adrese koje pronađu na zaraženom računaru. Za slanje koriste sopstveno okruženje a kao pošiljaoca označavaju osobu sa čijeg računara se šalju. Računarski virus koji na pomenuti način deluje je Brontok (eng. Brontokworm)[12], napravljen u Indoneziji. Kada ga žrtva prvi put pokrene, kopira sam sebe u fajl s podacima o korisničkim aplikacijama. Ovaj virus daje instrukcije da ga operativni sistem startuje zajedno sa svim drugim aplikacijama putem ključa HKLM\Software\Microsoft\Windows\CurrentVersion\Run u Windows Registry i onemogući korisnika da to izmeni tako što postavi zabranu korišćenja Windows Registry korisniku. Svoje fajove učini nedostupnim tako što ih modifikuje u sistemske fajlove i učini ih nevidljivim, a potom ukloni opciju FolderOptions. U slučaju pojave programa koji bi mogao da mu naškodi, aktiviranja MS DOS-a ili preuzimanja fajlova s interneta, računar se restartuje, što je znak infekcije ovim malicioznim programom.

Virusi mogu da budu namenski stvoreni da bi zarazili računare tajnih službi. Pad mreže američke tajne službe na 3 dana prouzrokovao je virus Natas (od eng. satan, čitano unazad, što znači satana, đavo). Ovaj polimorfičan virus prvi put je registrovan u Meksiko Sitiju maja 1994. godine, kada je bio širen putem zaraženih flopi diskova. Ubrzo je postao veoma proširen u Meksiku i jugozapadnom delu SAD.

Virus može da koristi i sopstveni SMTP mehanizam, pomoću kog šalje masovne imejl poruke na adrese koje prikupi iz fajlova na zaraženom računaru. Imejlovi koje šalje imaju promenljive parametre za naslov (eng. subtitle) i prikačeni fajl (eng. attachment). Prikačeni fajl koji sadrži virus može da ima ekstenzije .bat, .cmd, .doc, .exe, .htm, .pif, .scr, .tmp, .txt, ili .zip. Virus W32.Mytob.V@mm[13], otkriven 3. aprila 2005. godine, ima sposobnost da iskoristi uobičajene sigurnosne propuste u sistemu da otvori sebi port preko kog će se širiti kroz mrežu.

Postoje virusi specijalizovani za inficiranje dokumenata Majkrosoft vorda '97 i 2000. Makrovirus W97M.Verlor, poznat kao W97M.Overlord, pokreće se zatvaranjem zaraženog dokumenta tako što na S disku u memoriji

---

[12] Druga imena pod kojima se ovaj crv pojavljuje su: W32/Rontokbro.gen@MM, W32.Rontokbro@mm, BackDoor.Generic.1138, W32/Korbo-B, Worm/Brontok.a, Win32.Brontok.A@mm, Worm.Mytob.GH, W32/Brontok.C.worm i Win32/Brontok.E.

[13] Takođe je poznat kao Win32.Mytob.AA Computer Assoc, Net-Worm.Win32.Mytob.c [Kasper, W32/Mytob.c@MM [McAfee], W32/Mytob-C [Sophos], WORM_MYTOB.V [Trend Micro].

(C:\windows\) snima dva fajla: tempad.dll i tempnt.dll. Svaki sledeći otvoreni dokument i novootvoreni dokument (blanko) inficiraju se tim fajlovima.

Lista zaraženih virusa smešta se u fajl C:\Himem.sys[14]. Virusova stelt-funkcija aktivira se u slučaju da korisnik pokuša da pristupi Visual Basic editoru (Tools ->Macros ->VisualBasicEditor), čime bi virus mogao da bude otkriven. Ta funkcija menja naziv korisnika na TheOverlord, a potom u fajlu win.ini dodaje liniju: run = <Direktorijum indousa>\overlord.b.vbs. Potom virus sam sebe briše iz glavnog šablona i svih aktivnih dokumenata, što onemogućava njegovo pronalaženje putem pokrenutog alata. Po svom pokretanju overlord.b.vbs ponovo inficira glavni šablon i sve fajlove čija su imena zapisana u C:\Himem.sys. Ukoliko korisnik pokuša da pristupi listi makroa (Tools ->Macros ->Macro), virus se briše iz glavnog šablona i svih aktivnih dokumenata pre otvaranja prozora. To onemogućava da se nađe u listi prisutnih makroa, jer po zatvaranju radnog prozora s podešavanjima virus opet inficira sve aktivne dokumente i glavni šablon.

Postoje i specijalizovani virusi koji inficiraju fajlove s ekstenzijama .exe i .scr na računarima koji rade pod operativnim sistemom Microsoft Windows. Jedan od njih je parazitski virus Win32.Parite[15], koji ima tri verzije, A, B i C. Prve dve verzije razlikuju se samo u sadržaju vrednosti kojom se instanciraju u Windows Registry, dok treća verzija ima poboljšan sistem skrivanja svoje instance[16].

Jednom ovako instaliran virus zaražava sve .exe i .scr fajlove koji su bili i koji će biti pokrenuti ze vreme njegovog dejstva. To rezultira vrlo brzim širenjem virusa. Izuzeti su samo fajlovi koje sistem zaključa pre nego što se virus učita u memoriju, što automatski sprečava bilo kakvu infekciju. No, takvih fajlova ima izuzetno malo ili ih uopšte nema, u zavisnosti od instalacije. Posledice delovanja ovog virusa s povećanje zaraženih fajlova za 200 kilobajta i delimično ili potpuno gubljenje funkcionalnosti programa.

---

[14] Virus takođe za sobom ostavlja ili koristi fajlove overlord.b.vbs i overlord.b.dll.

[15] Ovaj virus je takođe poznat kao W32/Pate, W32/Pinfi i PE_PARITE. Verzija virusa označava se dodavanjem crte ili tačke pre slova oznake, na primer, Win32.Parite.C. Virus čine dva dela. Prvi je malo jezgro napisano u asembleru koje se brine o širenju tela virusa, a drugi je telo virusa napisano u borlandovom C++, koje je od zaražavanja računara smešteno u direktorijumu windows\temp

[16] Pošto je na nekom računaru virus prvi put pokrenut, instancira vrednost PINF u ključu HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\ Explorer (verzije A i B) u registru vindousa?, kopira svoje telo u direktorijum windows\temp. Time osigurava da će uvek biti pokrenut zajedno sa sistemom i da će ostati u njegovoj senci.

Prvi virus koji koristi tehniku poznatu pod nazivom integracija koda je ZMist ili Zombie.Mistfall, kog je napravio ruski tvorac virusa poznat pod imenom Z0mbie. Ovaj virus podržava potpuno novu tehniku: integraciju koda. Mistfall mehanizam koji virus sadrži sposoban je da dekompajlira prenosive izvršive fajlove do njihovih najmanjih elemenata, iziskujući 32 megabajta memorije. Po ovome, Zmist se ubacuje u kod tako što pomera blokove koda s mesta gde će se ubaciti, nakon čega regeneriše kod uključivanjem informacije o napravljenim pomeranjima, i ponovo gradi izvršni fajl.

Viruse prema okruženju i metodama infekcije možemo podeliti na:

- boot sektor virusi (tj. virusi startnog zapisa) – napadaju Master Boot sektor;
- parazitski – zaraze izvršne datoteke dodavanjem svog sadržaja u stru-kturu programa, pri čemu one ostaju delimično ili potpuno funkcio-nalne;
- svestrani virusi – napadaju boot sektore i izvršne programe;
- virusi pratioci – stvori .com datoteku koristeći ime već postojećeg .exe programa i ugradi u nju svoj kod;
- link virusi – u trenu inficiraju napadnuti računarski sistem, što može izazvati veliku štetu na disku;
- makrovirusi – koji mogu sami sebe da kopiraju, brišu i da menjaju dokumente.

Prema mestu u memoriji, viruse možemo podeliti na:

- one koji su u pritajnoj memoriji – ostaju u memoriji računara nakon aktiviranja koda virusa;
- one koji nisu u pritajnoj memoriji.

## 5. TROJANSKI KONJ

Naziv ovog malicioznog programa nastao je po poznatoj priči o osvajanju grada Troje zloupotrebom poverenja. Svoj naziv ovi maliciozni programi opravdavaju tako što koriste metodu lažnog predstavljanja. Naime, oni se predstavljaju kao korisni ili poželjni programi, koji prilikom pokretanja zajedno s nameravanom funckijom u pozadini sprovode neželjene aktivnosti bez korisnikovog znanja. Primer su antivirusi ili antispyware programi, koji se na engleskom zovu rogue ili fake antivirus. Korisnik, kada posećuje internet stranice njihovog proizvođača, može da se zarazi njima, i to često prilikom postojanja sigurnosnih rupa u internet pretraživaču. Programi poput Trojan-Fa-

keAV-a detektuju izmišljen maliciozni softver na korisnikovom računaru, a potom nastoje da uvere korisnika da će ukloniti viruse...". Ovi programi, osim što uznemire korisnika i izazovu njegove nesmotrene rakcije, mogu i blokirati aktivaciju pravih antivirusnih i antispajver programa, kao i instalirati ostale vrste malicioznog softvera[17]. Zahvaljujući programu port skener (port scanner), osoba koja nije zaslužna za inficiranje računara može iskoristiti to što je određeni računar zaražen trojanskim konjem da bi na taj način mogla da pristupi tom računaru.

Mogućnosti koje su na raspolaganju hakerima pošto instaliraju ovu vrstu malvera su velike: krađa lozinki i drugih osetljivih podataka (password stealers ili infostealers), omogućavanje udaljenog pristupa inficiranom računaru neovlašćenoj osobi (backdoors), instaliranje drugog malicioznog softvera (downloaders), korišćenje sistema kao dela botneta (npr. za automatsko spamiranje ili za DOS napade), rušenje sistema, anonimno internet surfovanje, brisanje ili izmenjivanje datoteka itd.

Teško je odrediti preciznu klasifikaciju ove vrste malicioznog softvera zbog njihovog svakodnevnog javljanja i unapređivanja njihovih mogućnosti. Međutim, s obzirom na kriterijum njihovih mogućnosti, trojanske konje možemo podeliti na: Bekdor (eng. Backdoor)[18] , što je program koji instaliraju trojanski konji (bez znanja vlasnika) i koji služi da trećim osobama omogućava nesmetan i od vlasnika neovlašten pristup računaru. Bekdor koristi slabosti operativnog ili zaštitnih sistema (zaštitnog zida ili antivirusnog programa). Kad se trojanac instalira na korisnikovom sistemu, haker može udaljeno da mu pristupi i izvodi razne operacije. Govorilo se da proizvođači računara predinstaliraju bekdor na sastave svojih kupaca radi lakše tehničke podrške, no to nikada nije pouzdano dokazano[19].

Downloader je trojanski konj koji obično miruje na računaru i pristupa različitim internet stranicama da bi s njih skinuo obično maliciozne fajlove koje su na kraju i pokrenuli.

PSW (password) trojanac je specijalizovan da pretražuje računar radi otkrivanja lozinki, ključeva (privatnih i javnih), sertifikata i podataka o kredi-

[17] Najpoznatiji trojanski konji ove vrste su: SpySheriff, ErrorSafe, WinAntivirus i XP Antivirus.
[18] Bekdor je termin koji se u engleskom jeziku koristi za vrata okrenuta dvorišnoj strani kuće. To su vrata koja su najslabije zaštićena i odakle provalnici najlakše ulaze u kuću.
[19] Trojans And Backdoors, http://www.webpronews.com/trojans-and-backdoors-2005-08/

tinim karticama. Sve korisne informacije, koje su rezultat pretrage PSW trojanaca, bitie prosleđene njegovom vlasniku.

Trojanski špijun (trojan spy) je vrsta trojanskog konja koji posle infekcije računara miruje u memoriji ne prikazujući svoje prisustvo i omogućava napadaču da prati rad korisnika računara bilo tako što beleži pritisnute tastere (keylogging), snima ekrane, ili na neki drugi sličan način. Informacije do kojih dođe prilikom praćenja rada korisnika, vlasnik i upravljač trojanskog konja najčešće koristi za ucenu.

Primer je trojanski konj Kenzero, koji pogađa korisnike koji nelegalno s interneta preuzimaju Hentai igre za odrasle preko japanskog file/sharing sajta Winni. Kada korisnik pokrene igru, trojanski konj maskiran kao instalacioni ekran traži od korisnika da unese određene podatke, a za to vreme prave screenshotove s informacijama o poslednjim otvaranim stranicama. Screenshotov-i istorije brauzer inficiranog korisnika automatski se objavljuju, a zatim korisniku stiže poruka, pop-ap ili imejl s ponudom sadržine: ako korisnik uplati 1.500 jena, vrednost od 1.200 dinara, sajt s podacima o njegovim internet navikama biće izbrisani[20]. Prema poslednjim podacima, oko pet i po hiljada ljudi priznalo je da su bili žrtva Kenzera[21].

Trojanac obaveštajac (trojan notifiers) svom autoru šalje informacije kao što su IP adrese, adrese elektronske pošte i stanje portova (često se koristi kao deo zlonamernog softverskog paketa koji obaveštava autora o uspešnoj instalaciji crva ili zadnjih vrata trojanaca)[22] [23]

Trojanski proksi server (engl. proxy server) je trojanski konj koji pokušava da pretvori inficirani računar u proksi server i na taj način omogući udaljenom korisniku da pristupi internetu anonimno putem udaljenog računara. Na taj način inficirani računar postaje tzv. Zombi (slepo sluša naredbe) i može da se iskoristi za slanje neželjenih poruka (spama) ili učestvovanje u DOS napadu.

---

[20] Više o tome: Kenzero Porn Virus Publishes Web History Of Victims On The Net--Unless They Pay, http://www.huffingtonpost.com/2010/04/16/kenzero-porn-virus-publis_n_540133.html

[21] Više o tome: 5.500 hentai pirates afflicted by blackmailing malware, http://www.geek.com/news/5500-hentai-pirates-afflicted-by-blackmailing-malware-1191821/

[22] Poznat je i slučaj delovanja trojanskog konja Topig, koji je kompromitovao i ukrao podatke za prijavu za 250.000 bankovnih računa i jednak broj kreditnih i debitnih kartica, imejl adresa i FTP računa.

[23] Više o tome: 250.000 Credit Cards Stolen in Wine Industry Hack, http://svbwine.blogspot.rs/2015/07/250000-credit-cards-stolen-in-wine.html, poslednji put pristupili 12.04.2016.godine.

Inovacija u razvoju trojanskih konja je mogućnost iskorišćavanja bezbednosnog propusta u starijoj verziji IE-a ili Google Chrome-a da bi se inficiran računar koristio kao anonimni proksi da se efektivno prikrije korišćenje interneta. Haker na taj način može da surfuje internetom i pogleda internet sajt dok se kolačići, IP logovi i slično nalaze na računaru domaćina.

U istoriji posećenih stranica na računaru žrtve može da se, ali i ne mora da se nalazi i spisak sajtova kojima je haker koji koristi računar kao proxy posećivao. Prva generacija takvih trojanskih konja često nije prikrivala tragove, dok novije to rade efektivnije. Nekoliko verzija Slavebot-a široko se rasprostranilo u SAD i Evropi i najviše su distribuirani primeri ove vrste trojanaca.

Legalni trojanski konji su trojanski konji u službi policije koji se bave prikupljanjem informacija sa ciljem otkrivanja krivičnog dela (engl. Remote Forensic Software). Ovo je oblik špijuniranja građana koji je u nekim zemljama legalan i vrši se po sudskom nalogu (npr., SAD, Australija). Različita su stanovišta u vezi s pitanjem prihvatanja ove metode dokazivanja. Većina država odbila je ovu mogućnost smatrajući da je legalni trojanski konj u sukobu s Ustavom, jer krši osnovna ljudska prava, dok je u nekim državama u fazi pripreme (Nemačka, Austrija, Švajcarska)[24]. Legalni trojanski konji šire se instalacijom ili aktualizacijom komercijalnih operativnih sistema i drugih softverskih komponenti računara i propagande, kao i putem ISP-ova infiltriranjem u postojeće mehanizme prenosa podataka, koji poznaju takvu mogućnost u svojim proizvodima i uslugama.Trojanski konji koji su odneli najviše žrtava su: Back Orifice, Netbus i SubSeven.

Poslednjih godina, trojanski konji postaju sve veća opasnost korisnicima prilikom surfovanja internetom zbog popularnosti botnetova među hakerima i pristupačnosti oglašivačkih servisa koji dopuštaju autorima da krše privatnost njihovih korisnika. Prema statistikama BitDefender-a iz 2009, 83% detektiranog malicioznog softvera činili su trojanski konji[25]. Za razliku od već navedenog softvera, postoji i maliciozan softver namenjen krađi podataka (data-stealing malware). Kako naziv kaže, to je softver koji je dizajniran tako da prikupi informacije i prosledi ih trećoj strani bez pristanka ili znanja žrtve,

---

[24] Više o tome: German Government Fesses Up to Spying on Citizens With Trojan, Says It's Legal, http://www.themarysue.com/german-gov-trojan/

[25] Više o tome: Top 10 malicious programs sent by email, Q2 2015 Most common form of malware,http://www.guinnessworldrecords.com/world-records/most-common-form-of-malware

a s namerom oštećivanja žrtve direktnim korišćenjem podataka ili njihovom underground distribucijom.

## 6. MALVERI ZA KRAĐU PODATAKA - DATA-STEALING MALWARE

U kradljivce podataka spadaju: keyloggeri, spyware, adware, backdoorov-i i botov-i. Tehnike koje koriste ovi zloćudni programi rapidno se umnožavaju.

Ova vrsta malicioznih softvera može se instalirati putem drive-by-download-a, a internet stranica koja je domaćin malicioznom softveru je neretko privremena ili lažna, pri čemu se koristi više načina enkripcije, a podaci se kradu prilikom dekripcije. Zahvaljujući ovim malicioznim programima, njihovi tvorci i korisnici mogu steći pravo bogatstvo. Uspeh hakera Alberta Gonzaleza (rođ. 1981. godine) ogleda se u krađi putem malicioznih programa i prodaji više od 170 miliona brojeva kreditnih kartica u 2006. i 2007. godini. To je bila najveća računarska prevara u istoriji. Osim pojedinaca oštećene su i mnoge firme poput: BJ's Wholesale Club, TJX, DSW Shoes, OfficeMax, Barnes & Noble, Boston Market, Sports Authority i Forever 21.

Spyware je široka kategorija malicioznog softvara s namenom da presreće ili preuzima delimično kontrolu rada na kompjuteru bez znanja ili dozvole korisnika. Sam naziv sugeriše da je reč o programima koji nadgledaju rad korisnika. Međutim, Spyware označava široku paletu programa koji iskorišćavaju korisnikov kompjuter za sticanje koristi za neku treću osobu ili komercijalnu dobit. Pojam spyware prvi put se spominje 1995. godine na Usenetu u poruci koja je ismevala Microsoft poslovni model. Reč spyware označavala je softver namenjen špijunaži ili prisluškivanju. Početkom 2000. godine osnivač Zone Labs-a Gregor Freund koristio je ovaj pojam u pres izdanju za ZoneAlarm-ov zaštitni mehanizam. Kasnije te iste godine otkriveno je da je Reader Rabbit, edukativni dečji softver koji je razvila firma Mattel, tajno slao podatke spomenutoj firmi. Od tada je spyware postupno počeo zauzimati svoj sadašnji oblik.

Uglavnom se tajno instaliraju na lične računare da bi pratili rad korisnika bez njihovog znanja. Međutim, često se ovi programi i dobrovoljno instaliraju na javnim, deljenim ili kompjuterima neke firme da bi vlasnik pratio aktivnosti korisnika, tj. zaposlenih. Nije redak slučaj da neka osoba koristi spyware da nadzire internet aktivnosti svog partnera. Maliciozni softver Loverspy posebno je dizajniran da tajno prati aktivnosti korisnika tako što će

njegov partner moći daljinski da kontroliše računar žrtve, uključujući tu i pristup, promenu i brisanje fajlova, kao i uključivanje kamere. Drugi način inficiranja je korišćenje slabe zaštite sistema, tj. nedostatka antivirusne (brojne antivirusne firme, kao što su Symantec, PC Tools, McAfee i Sophos su svoje antivirus programe obogatile antispyware dodacima) i antišpijunske zaštite, tzv. antispyware programa (npr., Ad-Aware, WindowsDefender, SpywareBlaster, Spybot Search & Destroy, Spyware Doctor (PC Tools), Ad-Adware SE (Lavasoft) i Spybot Search & Destroy Patrika Kola (Patrick Kolla).

Aktivni korisnici usluga interneta često su zaraženi s više oblika spyware-a. Kao posledicu postojanja spyware-a korisnik zaraženog kompjutera može primetiti čudno ponašanje sistema ili značajan pad sistemskih performansi (brzine), što je samo po sebi značajan problem. Špijunski softver može da utiče na povećanu aktivnost procesora i veći promet interneta. Takođe, javljaju se problemi sa stabilnošću, programi se naglo ruše, sistem se redovno smrzava, a povremeno nije moguće uspostaviti internet vezu, ili je ona veoma spora.

Sve to može da stvori utisak korisnika da su uzroci tih problema loše performanse računara, problemi s hardverom, Windowsim-a, ili zaraza nekim drugim malicioznim softverom. Neki korisnici teško inficiranih sistem kontaktiraju tehničku podršku ili kupe novi kompjuter zato što im je postojeći sistem „postao je prespor". U većini slučajeva vrlo zaraženi sistemi iziskuju čistu instalaciju Windows-a (jer se reinstalacijom ne brišu svi podaci s diska), a da bi se povratile funkcionalnost i brzina.

U ovu grupu malicioznih softvera spada i Keylogger ili keystroke logging program, maliciozni softver koji prati pritisnute tastere na računaru, a koristi se za krađu korisničkih lozinki, brojeva kreditnih kartica i ostalih osetljivih informacija koje potom šalje napadaču – neautorizovanom trećem licu.

U trenutku instalacije malicioznog softvera na računar veoma je bitno da ostane neprimećen i nedetektovan, te potom uklonjen. Navedena neprimećenost malicioznih programa ostvariva je zahvaljujući tehnici rutkit. Rutkit kao skup alata prikriva prisustvo napadača tako što omogućuje sakrivanje malicioznog prgrama u Task Manager-u (engl. hidden process – skriveni proces) ili može da spreči čitanje njegovih fajlova.

## 7. ZAKLJUČAK

Zbog brzine širenja i usavršavanja maliciozne programe nije moguće precizno nabrojati, data klasifikacija je samo trenutna slika vladajućih malici-

oznih programa koje broje najviše žrtava. Svakodnevno smo svedoci i žrtve novih verzija malicioznih programa, koje antivirusi i drugi programi za zaštitu nisu u mogućnosti da preduprede. Zato je neophodna obazrivost pri radu na računaru i zaobilaženje preuzimanja sadržaja nepoznatog pošiljaoca.

**REFERENCES (Literatura)**


Bossler, A., Holt, T. (2011), *Malware Victimization, A routine activities framework*, CRS Press, Taylor and Francis Group, Unitet States of America

Cohen, F. (1987), "Computer Viruses Theory and Experiments", *Computers and Security*, vol. 6, pp. 22–35.

Ranđelović, D., Popović, B. (2010), „Zlonamerni programi", *Tehnika*, 5/2010, *Elektrotehnika* (59), br. 5, Beograd.


**Internet izvori**


250.000 Credit Cards Stolen in Wine Industry Hack, http://svbwine.blogspot.rs/2015/07/250000-credit-cards-stolen-in-wine.html, poslednji put pristupili 12.04.2016.godine.

5.500 hentai pirates afflicted by blackmailing malware, http://www.geek.com/news/5500-hentai-pirates-afflicted-by-blackmailing-malware-1191821/, poslednji put pristupili 12.04.2016.godine.

Computer Viruses That Changed The World, http://www.makeuseof.com/tag/6-computer-viruses-changed-world/, poslednji put pristupili 12.04. 2016. godine.

Computer Virus History I, http://www.mindpride.net/root/Extras/ Viruses/computer_virus_history_1.htm, poslednji put pristupili 12.04.2016. godine.

German Government Fesses Up to Spying on Citizens With Trojan, Says It's Legal, http://www.themarysue.com/german-gov-trojan/, poslednji put pristupili 12.04.2016.godine.

History of Mac malware: 1982 – 2011, https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/

http://www.huffingtonpost.com/2010/04/16/kenzero-porn-virus-publis _n_540133.html, poslednji put pristupili 12.04.2016.godine.

Kenzero Porn Virus Publishes Web History Of Victims On The Net--Unless They Pay,

Melissa (computer virus), https://en.wikipedia.org/wiki/Melissa_(computer_virus), poslednji put pristupili 12.04.2016.godine.

Top 10 malicious programs sent by email, Q2 2015 Most common form of malware, http://www.guinnessworldrecords.com/world-records/most-common-form-of-malware, poslednji put pristupili 12.04.2016.godine.

Top Ten Most Destructive Computer Viruses of All Time, http:// crunkish.com/top-ten-worst-computer-viruses/, poslednji put pristupili 12.04.2016. godine.

Trojans And Backdoors, http://www.webpronews.com/trojans-and-backdoors-2005-08/, poslednji put pristupili 12.04.2016.godine.

VB – Virus Bulletin, https://www.virusbtn.com/pdf/magazine/1990/199003.pdf, poslednji put pristupili 12.04.2016.godine.

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet