SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 7:
Zlonamerni programi

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Zlonamerni programi

- Sadržaj poglavlja i predavanja:
  - 7.1. Vrste zlonamernih programa
  - 7.2. Zaštita od zlonamernih programa
  - 7.3. Rootkit

Quote

What is the concept of defense: The parrying of a blow. What is its characteristic feature: Awaiting the blow.

—*On War,* Carl Von Clausewitz

Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Internet

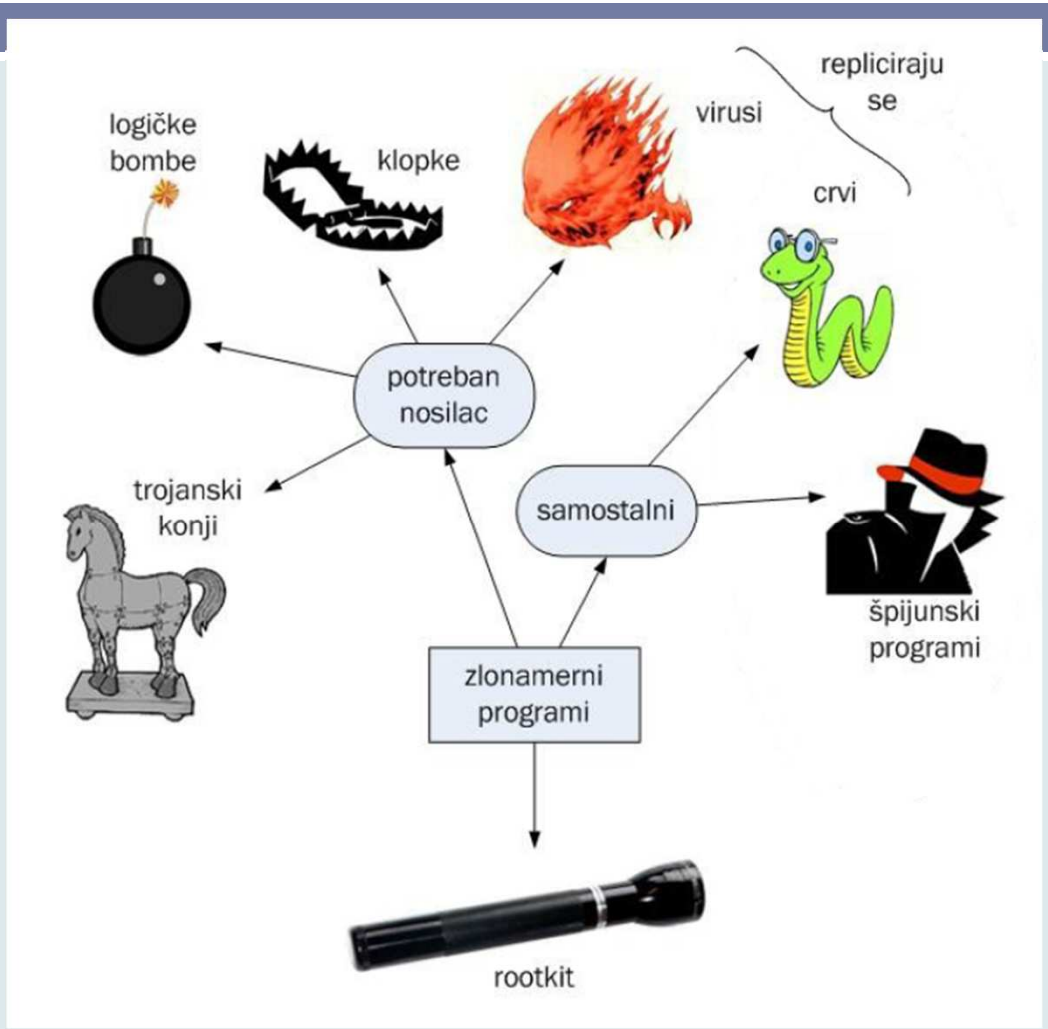
Šta su zlonamerni programi

- Stroga i precizna definicija zlonamernog programa ne postoji.
- U zlonameran softver (engl. *malware, malicious software*) ubraja se svaki program napravljen u nameri da na bilo koji način ošteti umrežen ili neumrežen računar, i/ili otežа ili onemogući njegovo korišćenje.
- Ponekad se programi, koji inače služe u korisne (dobronamerne) svrhe, mogu upotrebiti u zlonamerne svrhe, što otežava raspoznavanje i zaštitu.

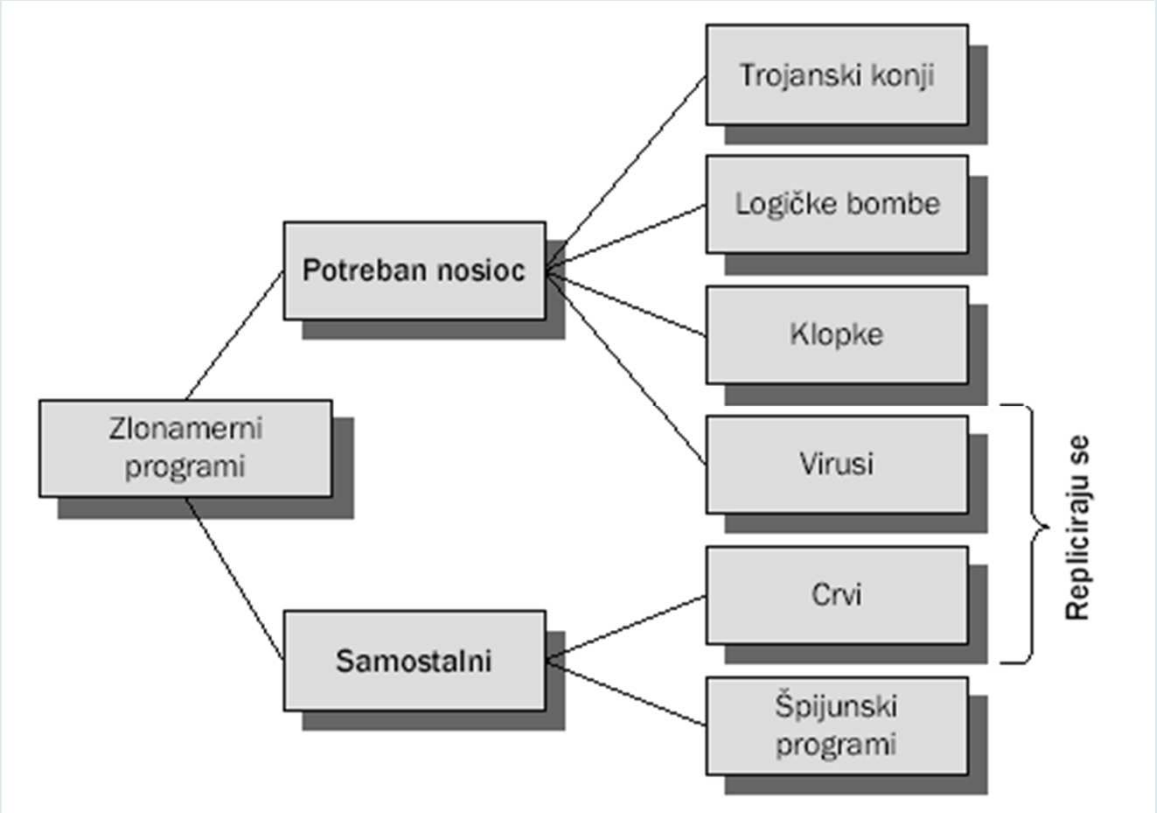
7.1 Vrste zlonamernih programa

- Kriterijum: da li zahtevaju nosioca?
  - Zahtevaju nosioca, tj. program u kome će biti sakriveni (trojanski konji, virusi),
  - Samostalni, tj. one koji ne zahtevaju nosioca (crvi, špijunski programi).
- Kriterijum: da li se repliciraju?
  - Oni koji se repliciraju (virusi, crvi)
  - Oni koji se ne repliciraju (trojanski konji, logičke bombe).

Podela zlonamernih programa



Podela zlonamernih programa…



Trojanski konji

- **Trojanski konji** (engl. *Trojan horses*) ili kraće, trojanci zlonamerni su programi koji se maskiraju i reklamiraju kao korisni programi kako bi se korisnici prevarili, tj. naterali da te programe pokrenu (društveni inženjering na delu).

- Na primer, trojanac može da bude zlonamerni crv upakovan u formu programa za instalaciju neke manje aplikacije (na primer: setup.exe).

Trojanski konji…

- Trojanac koji otvara zadnja vrata je program koji omogućava udaljenom korisniku da pristupi inficiranom računaru, i to najčešće tako da vlasnik računara nije ni svestan "posetioca".
  - Primer: Back Orifice 2K (BO2K)

Trojanski konji…

- Kradljivac informacija
- Trojanski špijuni (engl. *trojan spy*)
- „Obaveštajci“ (engl. *trojan notifiers*)
- Špijun miruje na inficiranom računaru i beleži pritisnute tastere (engl. *keylogging*)
- Nosioci softvera su obično realizovani u vidu trojanskih konja koji se nakon instalacije ponašaju kao magnet za drugi zlonameran softver.
- Trojanski proksi server (engl. *trojan proxy*)
- Programi koji pomoću modema pozivaju „egzotične“ telefonske brojeve (engl. *dialers*)

Logičke bombe

- **Logička bomba** (engl. *logical bomb*) je zlonameran *kod* ugrađen u neki koristan program koji će se aktivirati kada se ispune odgovarajući uslovi – na primer, u određeno vreme ili određenog datuma, ukoliko na disku postoji određena datoteka ili ako se na sistem prijavi određeni korisnik.

- Mogućnosti su praktično neograničene i zavise samo od mašte zlonamernih pisaca logičkih bombi.

Zombiji

- **Zombi** (engl. *zombie*) je program koji potajno preuzima kontrolu nad drugim umreženim računarom
- Nakon toga ga koristi da indirektno lansira napad
- Često se koriste da se lansira distribuirani napad odbijanjem usluga (engl. *distributed denial of service (DDoS) attacks*)
- Eksploatiše poznate propuste u mrežnim sistemima

Crvi

- **Crvi** (engl. *worms*) su samostalni (engl. *stand-alone*) programi koji se šire s jednog računara na drugi. Uobičajene metode prenošenja na žrtvu jesu upotreba elektronske pošte i Internet servisa (FTP, HTTP).

- Crv eksploatiše ranjivost žrtve ili koristi metode prevare i obmanjivanja, poznate kao društveni inženjering (engl. *social engineering*), kako bi naterao korisnika da ga pokrene.

Crvi…

- Crvi se mogu prenositi preko:
  - e-pošte (tzv. e-*mail* crvi)
  - instant poruka (IM crvi)
  - Interneta
  - deljenja datoteka (*file-sharing* crvi)
  - razmene datoteka između ravnopravnih računara (P2P crvi)

Primeri crva

- Morris Worm
  - Jedan od najpoznatijih klasičnih crva
  - Pušten od stane Roberta Morrisa 1988.
  - Napadao je Unix sisteme
  - Koristio nekoliko tehnika propagacije
    - Provaljivanje jednostavnih lozinki u lokalnom pw fajlu
    - Eksploatisanje propusta u *finger daemonu*
    - Eksploatisanje *debug trapdoora* u *sendmail daemonu*
  - Ako neki od napada uspe, onda se replicira
- MyDoom
- Sasser
- Code Red i Code Red 2
- Nimda

Virusi

- **Virusi** (engl. *viruses*) su verovatno najpodmuklija vrsta od svog raspoloživog zlonamernog softvera.
- Česti efekti infekcije virusima su brisanje važnih datoteka i/ili dovođenje sistema u stanje u kome ne može normalno da se koristi.
- Za razliku od crva, virusi ne koriste mrežne resurse za širenje, ali se mogu širiti preko mreže kao deo nekog crva.

Kako virus radi?

- Faze:
  - Skriven-uspavan (engl. ***dormant***) – čekanje na događaj koji okida akciju (engl. *on trigger event*)
  - Propagacija (engl. ***propagation***) – repliciranje na programe i/ili diskove
  - Okidanje (engl. ***triggering***) – okidanje na događaj
  - Izvršavanje (engl. ***execution***) – izvršavanje akcije

- Detalji su obično specifični za mašinu i OS
  - eksploaticija funkcija i slabosti

Struktura virusa


```
program V :=
   {goto main;
   1234567;
   subroutine infect-executable :=       {loop:
                file := get-random-executable-file;
                if (first-line-of-file = 1234567) then goto loop
                else prepend V to file; }
   subroutine do-damage := {whatever damage is to be done}
   subroutine trigger-pulled := {return true if some condition holds}
   main: main-program := {infect-executable;
                                  if trigger-pulled then do-damage;
                                  goto next;}
   next:
   }
```

Tipovi virusa

- Mogu se klasifikovati na bazi toga kako napadaju:
  - parasitic virus
  - memory-resident virus
  - boot sector virus
  - stealth
  - polymorphic virus
  - macro virus

Virusi koji napadaju sisteme datoteka

- Virusi ovog tipa za svoje širenje koriste jednu ili više vrsta sistema datoteka. Najveći broj ovih virusa inficira izvršne datoteke. Prema metodama inficiranja, virusi ovog tipa mogu se podeliti na:
  - prepisujuće viruse, tj. viruse koji prepisuju postojeći kôd (engl. *overwriting*),
  - parazitske viruse (engl. *parasitic*),
  - pridružujuće viruse (engl. *companion*),
  - viruse startnog zapisa (engl. *boot-sector*).

Makro virusi i skript virusi

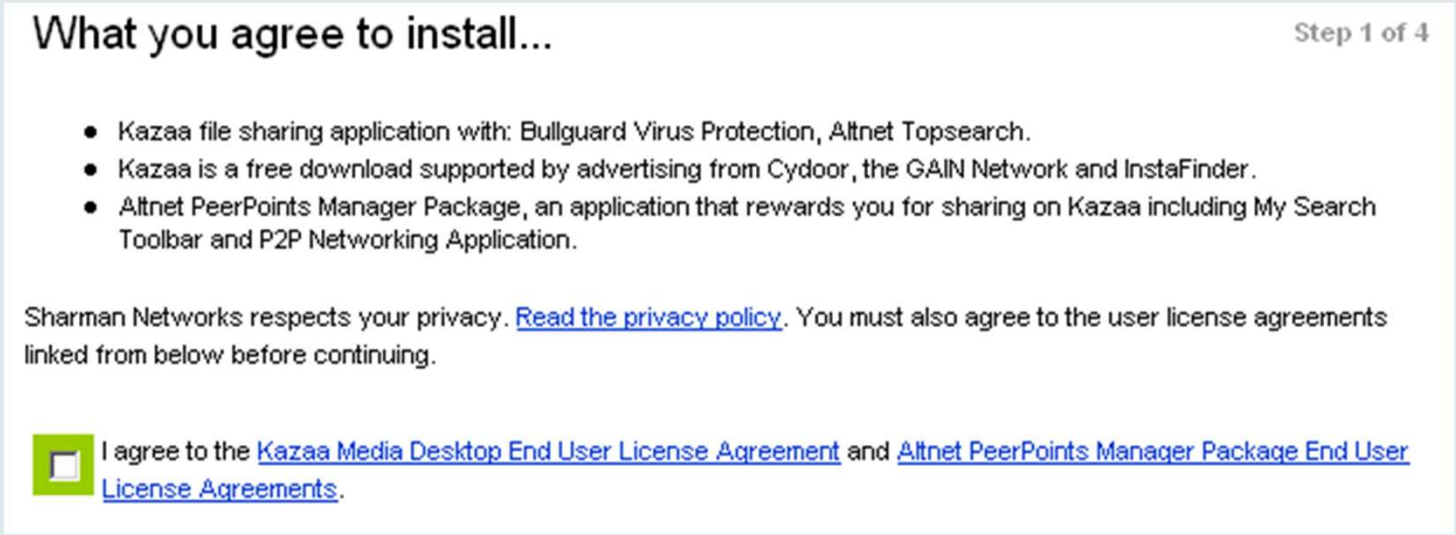
- **Makro virusi** najčešće su napisani i ugrađeni u dokumente koji se otvaraju onim aplikacijama iz paketa Microsoft Office koje koriste tehnologiju povezivanja i ugrađivanja objekata OLE2 (*Object Linking and Embedding*).

- **Skript virusi** su podskup virusa koji napadaju sisteme datoteka, pisani u skript jezicima (VBS, JavaScript, BAT, PHP). Skript virusi su sposobni da inficiraju datoteke u drugom formatu, kao što je HTM, ukoliko datoteke tog formata omogućavaju i dozvoljavaju izvršavanje skriptova.

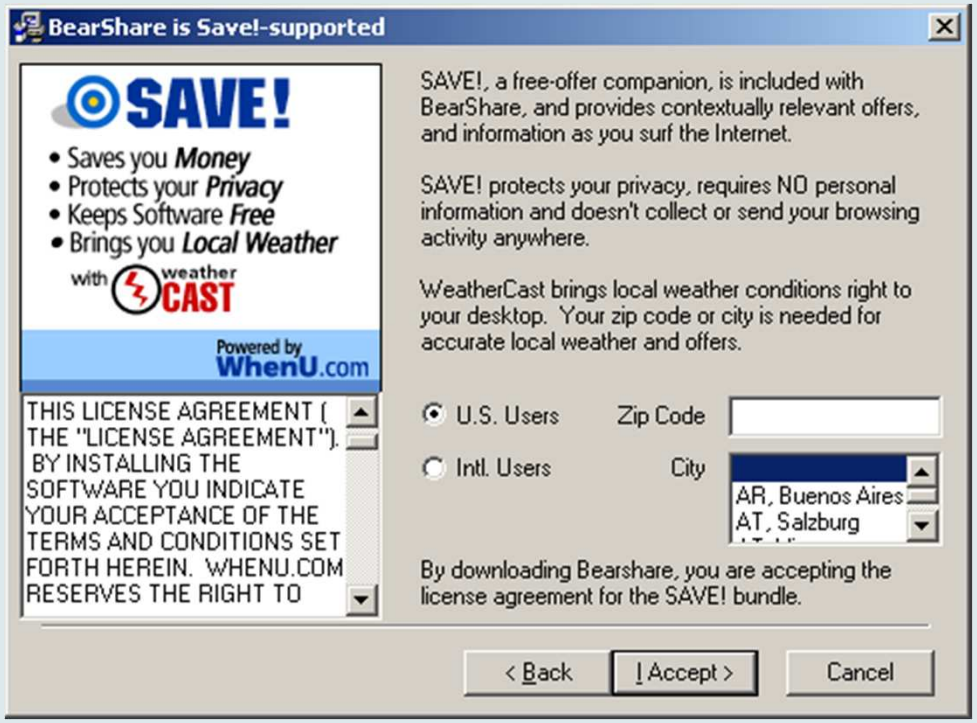
Špijunski programi

- Špijunski softver (engl. ***spyware***) je neželjeni program, instaliran na računaru bez znanja (ili odobrenja) korisnika, koji prikuplja informacije o aktivnosti korisnika (na primer, softver koji se koristi i posećene Web stranice), lozinke i finansijske informacije.
- U špijunske programe mogu se ubrojiti i trojanski konji iz kategorije kradljivaca informacija (na primer, ***keylogger***).
- Reklamni špijunski programi (engl. ***adware***) ove informacije prikuplja i šalje kompanijama koje se bave posebnom vrstom marketinga zasnovanom na praćenju vaših navika pri pretraživanju Weba i na oglašavanju (engl. *behavioural marketing*).

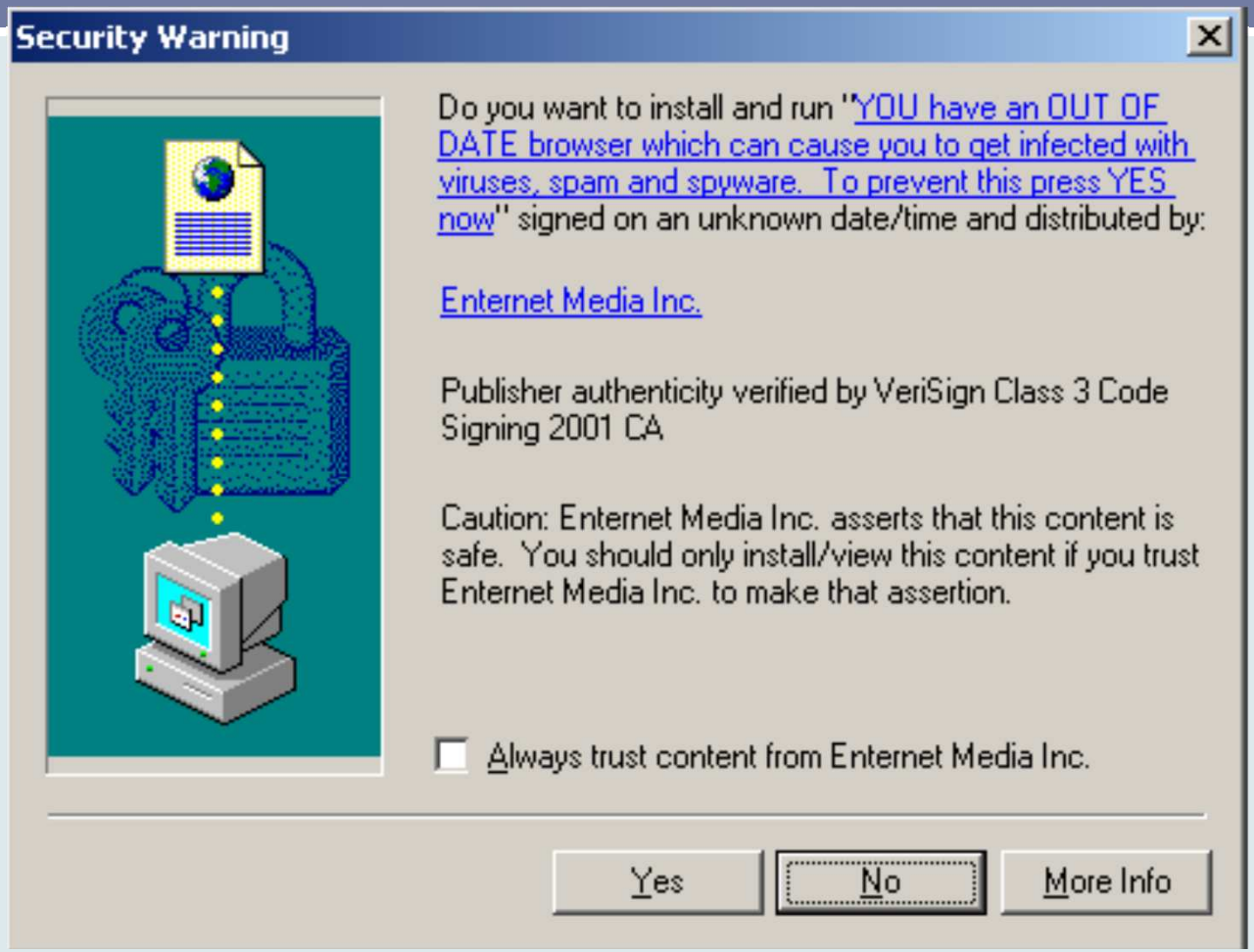
Primeri



Primeri...



Primeri...



Softpedia, čist softver

7.2 Zaštita od zlonamernih programa

- „Bolje sprečiti nego lečiti“
- Obavezno napraviti plan akcije za slučaj da dođe do “zaraze”
- Redovno pravljenje rezervnih kopija važnih podataka ili arhiviranje celog sistema
- Instalirati i redovno ažurirati odgovarajući zaštitni softver (antivirus, antispyware itd.)
- Pažljivo proveriti programe koje instalirate
- Biti oprezan od koga uzimate medije nosioce podataka
- Voditi računa o tome koje Web lokacije posećujete i šta sa njih preuzimate
- Ne dozvoliti pokretanje sumnjivih programa

Virusi - protivmere

- Virusni napadi koriste nedostatak controle integriteta u sistemu
- Da bi se sistem odbranio, potrebno je da se dodaju takve kontrole
- Tipično, to može biti jedna ili više od sledećih mera:
  - **Prevencija** (engl. *prevention*) – mehanizam za blokiranje virusnih infekcija
  - **Otkrivanje** (engl. *detection*) – virusa u inficiranom sistemu
  - **Reakcija** (*engl. reaction*) – vraćanje sistema u čisto stanje, čišćenje sistema

Antivirusni softver - generacije

- **Prva generacija**
  - Skener koristi potpise virusa ili promene u dužini programa da otkrije virus
- **Druga generacija**
  - Koriste se heuristička pravila ili kontrolne sume (engl. *checksum*) da se uoče promene i virusna infekcija
- **Treća generacija**
  - Programi rezidentni u memoriji identifikuju virus na osnovu akcija
- **Četvrta generacija**
  - Paketi sa raznovrsnim antivirusnim tehnikama kao što su skeniranje, "zamke za aktivnosti" (engl. *activity traps*), kontrola pristupa itd.

Napredne antivirusne tehnike

- Generičko dešifrovanje
  - Koristi CPU simulator da proveri potpise programa i ponašanje pre nego što ih stvarno i pokrene
- Primer: digital immune system (IBM) – digitalni imuni sistem
  - Sistem opšte namene za emulaciju i otkrivanje virusa
  - Bilo koji virus koji ulazi u organizaciju se hvata, analizira, pravi se sistem za otkrivanje i zaštitu, i virus se uklanja

Behavior-Blocking Software

- Softver baziran na blokiranju sumnjivih ponašanja - *Behavior-Blocking Software*
- Integrisan sa operativnim sistemom *host* računara
- Nadgleda ponašanje programa u realnom vremenu
  - Npr. pristup fajlovima, formatiranje diska, režime izvršavanja, promene sistemskih postavki, pristup mreži
- I to u pogledu mogućih zlonamernih akcija
  - Ako se otkriju takve akcije onda može blokirati, terminirati (prekinuti) ih ili tražiti potvrdu korisnika za provodjenje akcija
- Ima prednosti u odnosu na skenere
- Međutim, zlonamerni kod može biti pokrenut i pre otkrivanja

7.3 Rootkit

- **Rootkit** je komplet (engl. *kit*) koji se sastoji od malih i korisnih programa koji omogućavaju napadaču da održava pristup *rootu*, korisniku sa najvećim privilegijama na sistemu. Drugim rečima, **rootkit** je skup programa i koda koji omogućava permanentno i/ili konzistentno, neprimećeno (neotkriveno) prisustvo u sistemu (računaru)
  - "**undetectable**" – dizajniran da sakrije programski kod i podatke na sistemu.
  - obično za udaljeni pristup i prisluškivanje (engl. *eavesdropping*) – npr. Za "njuškanje" paketa sa mreže.
  - prvenstveno bio namenjen za korisne primene (recimo udaljeno administriranje), nije nužno loš tj. nije uvek korišten od stane "loših momaka"
  - *rootkit* je, u stvari, korisna tehnologija koja može biti zloupotrebljena i time vrlo opasna

Linux Rootkit

- Napadači su morali da pronađu načine „zavaravanja“ ovih mehanizama kako bi sakrili svoje prisustvo u sistemu
- U te svrhe, napadači koriste *rootkit* alate. Napad na sistem zasnovan na *rootkit* alatima izvodi se u četiri faze:
  - sakupljanje informacija o ciljnom sistemu (koji je operativni sistem u pitanju, koja verzija jezgra, koji korisnički nalozi postoje itd.),
  - sticanje administratorskih prava, tj. prava koja ima korisnik *root*, i koja su najčešće neophodna za instalaciju,
  - instaliranje *rootkit* alata i
  - uspostavljanje kontrole nad ciljnim sistemom.

Podela *rootkit* alata

- *Rootkit* alati se mogu podeliti na dve grupe:
  - aplikacioni *rootkit* alati, koji - kao i sve ostale aplikacije - rade u neprivilegovanom (korisničkom) režimu (engl. *user mode*)
  - *rootkit* alati koji se integrišu u samo jezgro i rade na nivou jezgra (engl. *kernel mode*).
- Ove dve vrste alata razlikuju se po mestu u sistemu na kome su smešteni i načina na koji skrivaju svoje prisustvo u sistemu.

Aplikacioni rootkit alati

- Rad aplikacionih *rootkit* alata zasniva se na zameni legitimnih aplikacija zlonamernim datotekama. Ubačene datoteke omogućavaju napadaču da prikrije svoje prisustvo i da obavi željene aktivnosti na sistemu (na primer, alat može da obezbedi "zadnja vrata" tj. skriveni ulaz koji napadač može da iskoristi).
- U grupu programa koje napadač menja kako bi sakrio svoje prisustvo na sistemu spadaju programi koji:
  - skrivaju zlonamerne datoteke i direktorijume koje je napadač podmetnuo (ls, find, du),
  - skrivaju procese koje je napadač pokrenuo (na primer, ps),
  - sprečavaju ubijanje procesa koje je pokrenuo napadač (kill, killall),
  - prikrivaju aktivnosti napadača na mreži – otvorenih portova, mrežnih veza (netstat, ifconfig),
  - skrivaju unos u datoteku crontab
  - skrivaju zapise u dnevničkoj datoteci o vezama koje napadač ostvaruje sa udaljenim sistemom (syslogd)

Rootkit alati na nivou jezgra

- Rootkit alati na nivou jezgra otkrivaju se teže od aplikacionih, jer se integrišu u samo jezgro operativnog sistema, što znači da ih može zaobići provera integriteta sistema obavljena u neprivilegovanom režimu rada.

- *Rootkit* alati jezgra zasnovani su na činjenici da je jezgro Linux sistema modularno – korisnik sa *root* privilegijama može u jezgro učitati neki modul (engl. *Loadable Kernel Module*, *LKM*) i na taj način proširiti funkcionalnost operativnog sistema

Zaštita od rootkit alata

- Za *rootkit* alate važi isto što i za crve i za viruse – mnogo je lakše sprečiti instaliranje ovih alata nego ih kasnije otkriti i ukloniti.

- Administratorima su na raspolaganju i određeni programi namenjeni za otkrivanje rootkit alata.
  - Chkrootkit
  - Rkscan
  - Rkdet

Windows rootkit

- Upotreba postojećeg interfejsa za ubacivanje zlonamernog koda
- Deaktiviranje sistema zaštite datoteka
- Napadi DLL injection i API hooking

- Detekcija rootkit alata – RootkitRevealer

Upotreba postojećeg interfejsa za ubacivanje zlonamernog koda

- Operativni sistem Windows sadrži određene komponente (interfejse) koji omogućavaju nadogradnju sistema alatima drugih proizvođača. Na primer, proces prijavljivanja na sistem (engl. *user logon process*) može se proširiti novim programima i/ili bibliotekama. Standardna procedura prijavljivanja na Windows sistem počinje zadavanjem kombinacije tastera Ctrl+Alt+Delete.
- Nakon toga, proces winlogon (koji nastaje pokretanjem datoteke winlogon.exe) poziva standardnu Windows biblioteku msgina.dll (*Graphical Identification aNd Authentication*, *GINA*) koja proverava identitet korisnika na osnovu unetog korisničkog imena i lozinke.
- Proces prijavljivanja može da se izmeni korišćenjem trojanskog alata FakeGINA, koji zapravo predstavlja *rootkit* alat.

Deaktiviranje sistema zaštite datoteka

- Napadači često moraju da promene neku sistemsku datoteku koja nije predviđena da se menja. Da bi u tome uspeli, potrebno je da „nadjačaju“ Windowsov sistem zaštite datoteka (engl. *Windows File Protection*, *WFP*). Prilikom instalacije operativnog sistema generiše se spisak značajnih sistemskih datoteka. Njihova zamena drugom verzijom moguća je jedino ukoliko administrator instalira neku zvaničnu zakrpu (engl. *hotfix*) ili Service Pack.

Napadi DLL injection i API hooking

- Ove dve tehnike napada usmerene su na procese – napadač ubacuje zlonameran kôd u neki proces i na taj način menja originalnu funkciju procesa. Tehnika ubrizgavanja DLL biblioteke (engl. *DLL injection*), tj. ubacivanja zlonamerne DLL biblioteke u memorijski prostor aktivnog procesa, izvodi se u nekoliko faza.
- Tehnika *API hooking* nadovezuje se na *DLL injection* – ona predviđa ubacivanje zlonamernih *rootkit* funkcija u legitimne DLL datoteke.
- Jedan od alata koji kombinuje tehnike *DLL Injection* i *API hooking* jeste AFX Windows Rootkit. Ova aplikacija prikriva aktivne procese u sistemu, direktorijume, datoteke, zapise u bazi registry, TCP i UDP portove itd. Ovaj alat ne formira zadnja vrata (engl. backdoor) – zato se najpre formira „ulaz“ u sistem pomoću nekog drugog alata čije se prisustvo krije koristeći AFX Windows Rootkit.

Detekcija rootkit alata – RootkitRevealer

- Jedan od tragova koji *rootkit* alati ostavljaju za sobom je razlika u „slici“ sistema, tj. u rezultatima skeniranja sistema na najvišem nivou (Windows API) i rezultatima skeniranja na najnižem nivou („sirov“ sadržaj sistema datoteka ili baze Registry na disku).
- Zato se *rootkit* alati (aplikacioni ili alati jezgra) koji manipulišu API-jem da bi se sakrili, mogu otkriti na osnovu razlike između informacija pribavljenih od API-ja i informacija dobijenih pri skeniranju strukture sistema datoteka.
- Rootkit Revealer otkriva *rootkit* alate na taj način.

Neetička primena *rootkit* alata – DRM softver

- Kompanija Sony BMG (trenutno druga najveća izdavačka kuća na svetu) pokušala je problem piraterije da reši uvođenjem novog DRM softvera – takozvane „XCP“ (eXtended Copy Protection) tehnologije, koju je Sony licencirao od britanske kompanije First 4 Internet. XCP tehnologija radi samo na operativnim sistemima Windows, dozvoljava reprodukciju muzike na računaru samo iz pratećeg plejera i sprečava korisnike da naprave više od par kopija originalnog diska.

- Mark Russinovich, stručnjak za operativne sisteme Windows, izložio je i opisao u članku „*Sony, Rootkits and Digital Rights Management Gone Too Far*“ slučaj sada već čuvenog rootkit alata podmetnutog u DRM softver koji je Sony isporučivao sa svojim audio diskovima. Autor članka je *rootkit* otkrio nakon kupovine DRM zaštićenog albuma „Get Right with the Man“ (benda Van Zant) preko servisa za elektronsku trgovinu Amazon. U članku je detaljno opisano kako XCP funkcioniše.

- Na blogu: www.conwex.info/blog/

Literatura

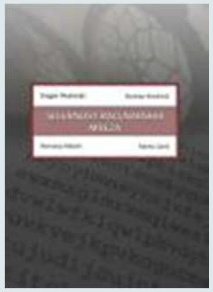
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

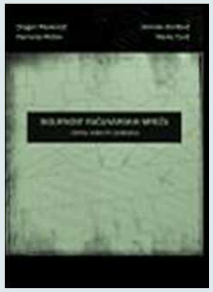
- Za predavanje 7:
  - Poglavlje 7: Zlonamerni programi

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?