Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

6. TAKSONOMIJA PRETNJI I MALICIOZNIH PROGRAMA

Ciljevi

- **Razumeti i naučiti:**
  - **značaj** taksonomije pretnji, napada i *malvera*
  - **tipove** malicioznih programa (**malvera**)
  - **mere zaštite i oporavka sistema** od malicioznih napada

Taksonomija pretnji (T)

1. **Taksonomija:** *princip klasifikacije na bazi definisanih kriterijuma*
2. **Cilj** : obezbedi **lakše definisanje i identifikovanje** različitih **T**
3. **Taksonomija izvora pretnji (**najčešća **ISO/IEC 27005):**
   – *slučajne-**SI*** i *namerne-**Na,** prirodni događaji*.
4. **Redukovana taksonomija izvora T** za izbor **U, O, T** k/z (**NIST**):
   - *greške, prirodni događaji, namerni napadi*
4. **Taksonomija tipa pretnji (**najčešća**):**
   – *maliciozne zloupotrebe ranjivosti i kompjuterski kriminal*
   – *nebriga*, *ljudska greška, pad sistema, uticaj okruženja*

Taksonomija napada i napadača

- **Taksonomija napada:**
  - *Destrukcije*
  - *Izmena podataka*
  - *Prekid servisa (DoS i DDoS)*
  - *Neovlašćeno korišćenje*
  - *Špijunaža*
  - *Informaciono ratovanje…*

- **Profili napadača:**
  - *Amateri*
  - *Profesionalci*
  - *Hakeri (kreativci, destruktivci, kriminalci)*
  - *Krekeri, Vandali, Lameri*
  - *Kompjuterski kriminalci…*

5. Taksonomija kombinovanih napada (NIST):

- *Posledica uticaja*: štetan-**Št,** neškodljiv-**Nš,**
- *Izvor nastanka*: iznutra-**Un,** spolja-**Va**
- *Način izvođenja*: sofisticiran – **So,** nesofisticiran – **Ns,**
- *Kombinovani napadi: $2^3 = 8$ kombinacija*

ŠtSoUn, ŠtSoVa, ŠtNsUn, ŠtNsVa, NšSoUn, NšSoVa, NšNsUn, NšNsVa

Primer: Taksonomija namernih napada

TIP NAPADA	
Lokalni	zahteva se fizičko prisustvo napadača na mestu napada i razmeštaja IKTS
Mrežni	napadač inicira napad sa mreže
SPOSOBNOST NAPADAČA	
Niska	uobičajene sposobnosti i ograničeno znanje o IKTS i ne koristi posebne alate
Visoka	ima jednu/obe sposobnosti: koristi sofisticirane alate i/ili napredne IKT tehnike
PRISTUP IS	
Iznutra	napadač nije korisnik, nije privilegovan korisnik ili je privilegovan korisnik IKTS
Izvana	napadač je legalan ili nelegalan ili javni korisnik IKTS
NAMERA NAPADAČA	
Nemaliciozan	nema nameru da ošteti IKTS, napada iz znatiželje, dosade ili izazova
Maliciozan	ima jasnu nameru da ošteti IKTS, ili izazove štetu organizaciji
RESURSI NAPADAČA	
Minimalni	(I) samoinicijativan i samo–motivisan; (II) radi nezavisno i (III) izvršava napad sa minimalnim računarskim resursima
Srednji	(I) deo grupe/organizacije, koje se ne bave komercijalnom špijunažom, kriminalom, ili terorizmom); (II) radi pod uticajem grupe/organizacije i (III) izvršava napad sa prosečnim resursima
Značajni	(I) deo grupe/organizacije, uključujući obaveštajne, informacionog ratovanja ili državno–sponzorisanog terorizma; (II) radi direktno pod upravom grupe/organizacije i (III) napada sa značajnim resursima

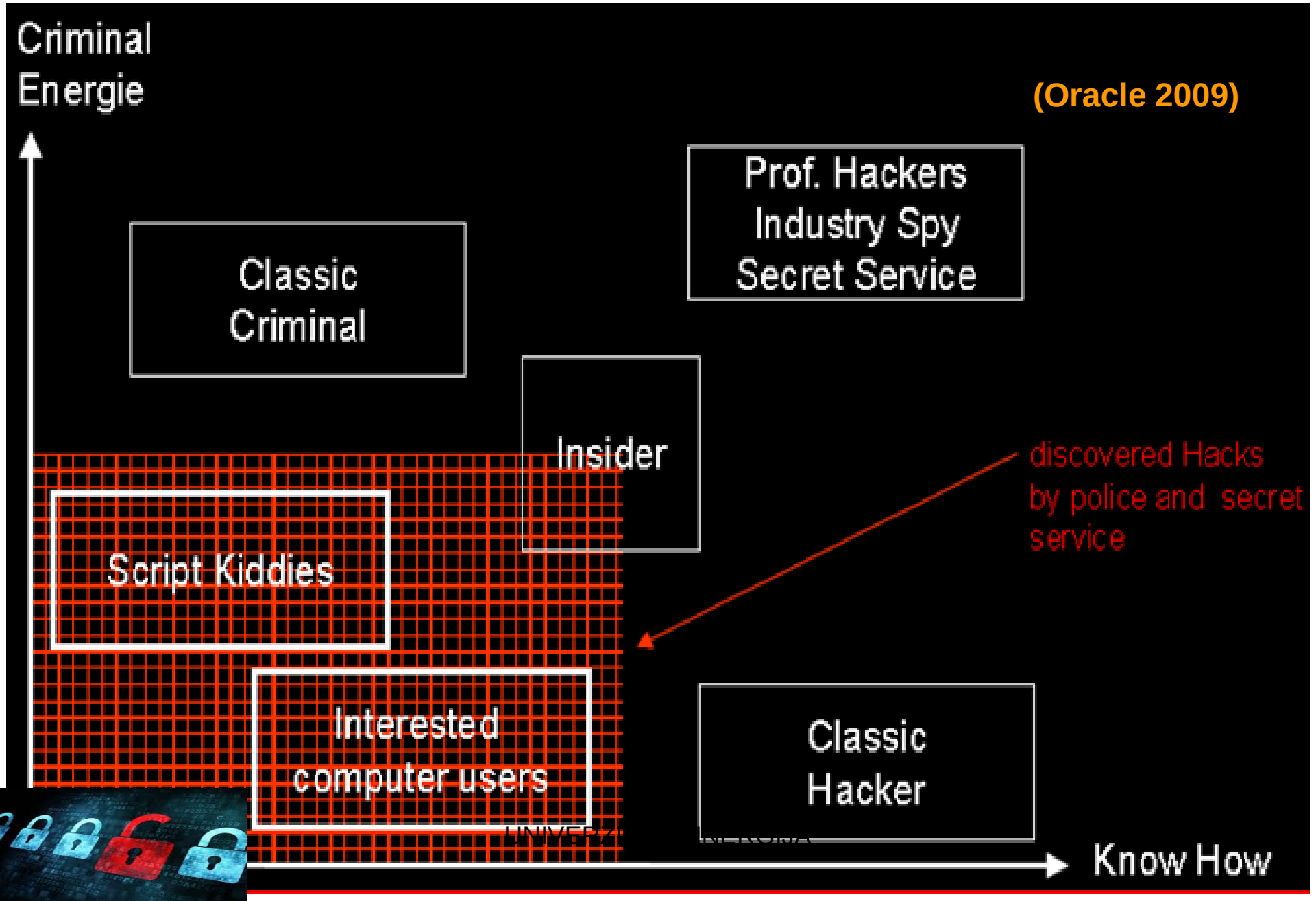
Taksonomija pretnji - *napad, napadač*

- **Hakeri** prema kriterijumu *namere*:
  - *Kreativci* - najčešće ne prave štetu
  - *Destruktivci* - uništavaju, brišu i menjaju podatke
  - *Kriminalac* - ostvaruje ličnu korist
- **Opšti profil hakera:** *tipično mlad, inteligentan, uzoran i odgovoran radnik na poslu, visoko motivisan i istraživački orijentisan. Ima razvijeno logičko mišljenje, dobro poznaje i koristi RS, samo mu treba* ***jak motiv****, da postane pohlepan, osvetoljubiv i sl.*

Taksonomije pretnji - *motiv, sredstva*

- *Opšti motivi napadača*:
  – znatiželja, novac, moć, osveta i sl
- *Posebni motivi*:
  – intelektualni izazov, radoznalost, avanturizam, zabava, potreba za trijumfom, opijenost znanjem, kompenzacija inferiornosti…
- *Sredstva za napad*:
  – tehnički kapaciteti, nivo znanja i veština
- *Prilika za napad*:
  – iskoristiva ranjivost *hw, sw, konfiguracije, ljudi*
  – teško se određuje zbog postavljanja *rutkit* tehnika

Primer: Profil hakera/stopa otkrivanja



Primer: Hakerske usluge na crnom tržištu (*PandaLab, 2011*)

Roba/usluga	Cena
Bankarski podaci bez verifikacije dostupnosti	$2/kartici
Bankarski podaci sa verifikacijom dostupnosti (mali račun-$82.000)	$80 - $700
Klonirana kartica/debitna kartica	$180
Mašina za kloniranje kartice	$200-$1.000
Lažna ATM mašina	$3.500
Usluga pranja novca - provizija	10-40 centi od iznosa
Kupovina lažnom karticom umesto klijenta (zavisno od proizvoda)	$30 - $300
Botnet rentiranje (zavisno od perioda, broja računara i frekvencije spama)	$15 - $20

Primer: Ponuda malicioznih usluga

Nude projekat za vlastiti sajt za krađu identiteta i novca	Zavisi od projekta
Nude probni pristup ukradenoj kartici ili detaljima kreditne kartice, garantuju povraćaj novce i objavljuju „radno vreme“ – zbog velike konkurencije	Besplatno
Zahtev za anonimnost obavezan – dogovor preko IM, generičkog e-mail naloga; za naplatu koriste *Western Union, Liberty Reserve* i *WebMoney*	

Ponuda maliciozne aktivnosti	**Cena/akciji**
Infekcija virusom po svakom *upload-u*, zavisno od lokacije, uz proveru zaobilaska AVP	9,5 do 4,5 centa
Polimorfno šifrovanje sekvence malvera	$25 do $50
Sprečavanje detekcije malvera sa AVP (1 sedmicu-1 mesec)	$20 - $100
Zavisno od procenta infekcije mrežnog saobraćaja od 1.000 entiteta (3% , 4%, >20%)	$4.5, $6, $30

Primer: Generičko stablo pretnji

Prilog: Taksonomija pretnji ISO/IEC 27005

- **D** – *namerna akcija prema informacionoj imovini*
- **A** – *slučajna ljudska akcija, koja može oštetiti informacionu imovinu*
- **E –** *prirodni događaj bez uticaja čoveka* **(Primer)**

Kvar erkondišna	*A, D, E*
Bombaški napad	*A, D*
Intercepcija komunikacija	*D*
Oštećenje linija	*A, D*
Kvar medija za skladištenje	*E*
Prašina	*E*
Zemljotres	*E*
Prisluškivanje	*D*
Elektromagnetsko zračenje	*A, D, E*
Elektrostatički naboj	*E*
Ekstremne temperature i vlažnost	*A, D, E*
Pad komunikacionih (mrežnih) servisa)	*A, D*
Gubitak napajanja	*A, D, E*
Nestanak vode	*A, D, E*

Primer: Tipične bezbednosne grešake

- **Upravne strukture:**
  - neobezbeđenje odgovarajućeg broja stručnih lica u zaštiti
  - primena samo organizacionih vidova zaštite bez primene k/z
  - rešavanje samo pojedinačnih bezbednosnih problema
  - korišćenje samo mrežnih barijera (*firewall*)
  - neshvatanje vrednosti informacija
  - primena kratkotrajnih rešenja zaštite
  - ignorisanje bezbednosnih problema
- **Korisnika**:
  - otvaranje nezahtevanog e-mail
  - ne instaliranje bezbednosnih *patch*-eva (zakrpa)
  - instaliranje i *download*-ovanje *screen saver*-a i igrica
  - izostanak operacija bekapovanja
  - korišćenje modema dok je PC vezan u LANu

Primer: Tipične bezbednosne grešake

- **Informatičkih profesionalaca**
  - priključivanje RS na Internet bez primene mera zaštite
  - priključivanje test/razvojnih RS na Internet sa *default* lozinkama
  - neažuriranje nekih bezbednosnih problema
  - korišćenje nešifrovanih protokola za upravljanje
  - davanje/izmena lozinki preko tel. bez autentifikacije
  - propust u procedurama bekapovanja sistema
  - korišćenje nepotrebnih Internet servisa
  - primena slabo konfigurisanih mrežnih barijera
  - propust u implementaciji i ažuriranju AVP
  - propust u obuci korisnika (prijava incidenta)

Maliciozni program - *malver*

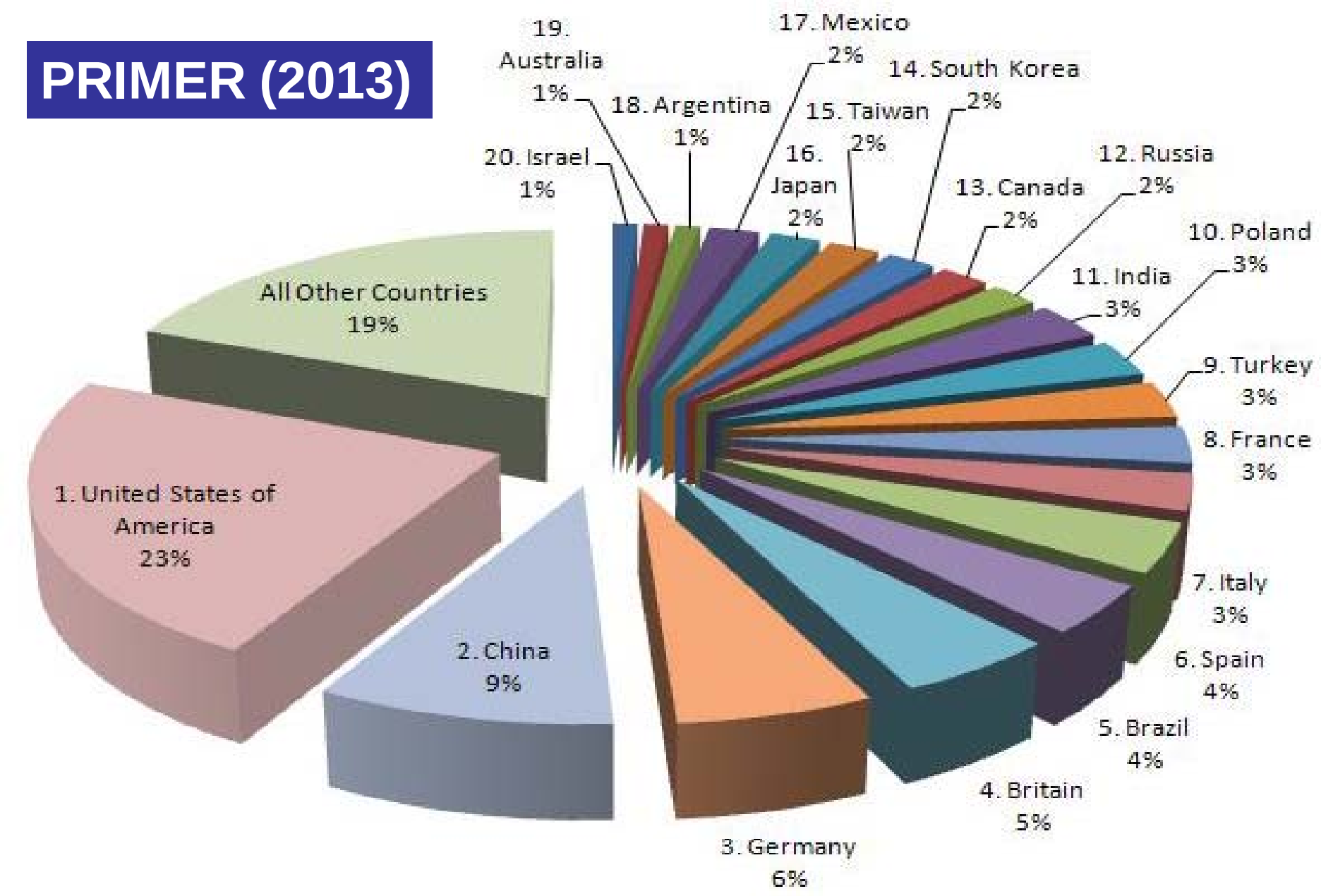
- ***Definicija :***
  - *tajno ubačen/izbačen/promenjen kôd u drugom programu da uništi p/i, pokrene destruktivni program, kompromituje bezbednost, naruši CIA, spreči namanjeno funkcionisanje...*
- **Tipovi *malvera***:
  - *virusi, crvi, trojanci, mobilni kôdovi (skriptovi), kombinovani napadi (lažni virus/trojanac)....*
- **Opšte karakteristike malvera**

– najznačajnije pretnje sa Interneta

– granice između različitih malvera sve su slabije

– **Internet preplavljen malverima**:
  - **200.000**/dnevno (kraj **2013**.) novih sofisticiranih malvera
  - od toga 40 % izmeni svoju definiciju za **24 sata**
  - **Napadi *Zero-day* tipa, višestruki, sofisticirani!**

PRIMER (2013)



Cybercrime: Top 20 Countries

Taksonomija malvera

- **Moguća podela na bazi brojnih kriterijuma**
- **Razlikuju ih tri dominantne karakteristike**:

  1. ***Samoreprodukujući* malveri**
     – virus, crv
  2. ***Rast populacije* malvera**
     – malveri koji se ne reprodukuju uvek imaju nultu populaciju
     – malveri sa nultom populacijom samoreprodujući (npr. *rabit*)
  3. ***Parazitski* malveri**
     – zahtevaju tuđi izvršni kôd

Primeri: kôd *boot* sektora na HD, binarni kôd aplikacije, izvorni kôd…

Primer: Matrica zajedničkih karakteristika malvera

	Logička bomba	**Trojanac**	**Zadnja vrata**	**Virus**	**Crv**	**Rabit**	**Spayware**	**Adware**
Samoreprod-ukujući	Ne	Ne	Ne	Da	Da	Da	Ne	Ne
Rast populacije	Nulti	Nulti	Nulti	Da	Da	Nulti	Nulti	Nulti
Parazitski	Moguće	Da	Moguće	Da	Ne	Ne	Ne	Ne

Primeri: Kôdovi malvera

Primer koda logičke bombe:

legitimate code
if date is Friday the 13th: crash^computerO
legitimate code

Zadnja vrata - bilo koji mehanizam koji zaobilazi bezb. proveru

Primer koda za zaobilazak procesa autentifikacije

username = read_username()
password = read_password()
if user name is "133t h4ck0r":
return ALLOW^LOGIN
if username and password are valid:
return ALLOW_LOGIN
e l s e:
return DENY^LOGIN

Poseban: *RAT* (*Remote Administration Tool/Remote Access Trojan*)

Kompjuterski virus

- **Krakteristike*:***
  - **program**: ˝inficira˝ ostale programe
  - **modifikuje**: legalne programe
  - **koristi**: autorizaciju korisnika da inficira program
  - **pokreće se**: aktiviranjem izvršavanja, inficira datoteku
  - **širi se**: kroz sistem/mrežu
  - **inficiran program**: ponaša se kao virus
  - **razmnožavanje**: "ugnjezde" se u druge datoteke
  - **šteta**: brišu ili menjaju datoteke na disku
- **Najčešći prenosioci:**
  - *Boot* sektor
  - *Master boot* zapis (**MBR**)
  - Izvršne datoteke (**npr**. **.COM i .EXE**)
  - Datoteke sa izvršnim kôdom (**npr**. **Word i Excel**)

Taksonomija virusa

- **Virusi BOOT sektora:**
  - „kače“ se uz **MBR** program u *boot* sektoru HD/pr. medija
  - najnezgodniji, nalaze se u najdubljem delu OS
  - mogu preuzeti kontrolu i nadgledati svaku operaciju
  - nakon uključenja, prvi se aktiviraju
  - detekcija/uklanjanje - reinstalacija OS sa *butabilnog* CD (uz AVP)
  - **kad se otkriju lako se uklanjaju**

  Primer: *Michelangelo, Stoned, …*

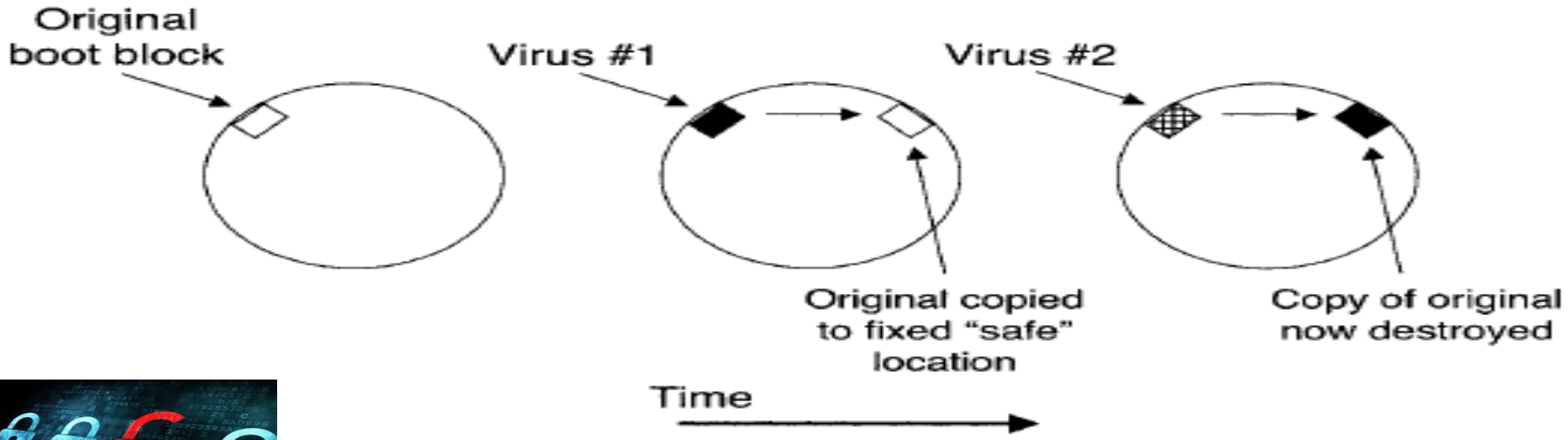


Figure 3.1. Multiple boot sector infections

Taksonomija virusa 1

- **Virusi komandnog procesora**:
  - slično prethodnim, učitavaju se malo kasnije u boot procesu
  - slabije deluju na OS - **kada se otkriju, lako se uništavaju**
- **Univerzalni virusi (infektori) -** najrašireniija kategorija virusa:

1. ***lepe se za određene tipove datoteka***

- nemaju veze sa **OS,** cilj su **.EXE** i **.COM** datoteke
- učitaju se u prvi zaraženi program
- sele se u memoriju, čekaju da zaraze naredni ***.exe*** program

2. modifikuju način na koji računar otvara neku datoteku

- **virus se aktivira prvi**, a onda se aktivira program
- glavna strategija -da od ***.exe*** fajla **naprave Trojanca**

Primer: *Jerusalem* i *Cascade*.

Taksonomija virusa 2

- **Složeni virusi *:***
  - veoma opasni - kombinuju tehnike, vrlo su fleksibilni
  - vrhunac su tehnologije programiranja virusa
- **Usmereni virusi:**
  - strogo su namenski programi
  - uništavaju određeni broj određenih tipova datoteka
- **Šifrovani virusi**
  - sakrivaju kôd ili inficiranu datoteku
  - jedini **otvoreni tekst - procedura (**rutina**) dešifrovanja**
  - najčešće šifrovani jedinstvenom procedurom
  - (**XOR-**e svakog bajta slučajnim ključem za svaku novu kopiju
  - **detekcija** - pronalaženje procedure za dešifrovanje na početk kôda

Taksonomija virusa 3

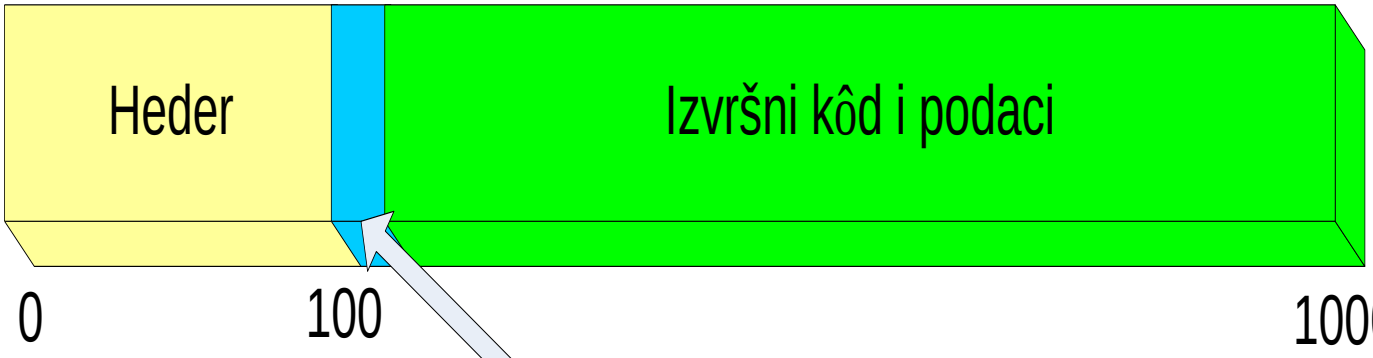
- **Makrovirusi**
  - **preovlađujući tipovi virusa** napisani u makro jezicima
  - najčešći su makrovirusi za **MS Word, Excel, Office, Access** baze i dr.
  - preuzimaju kontrolu kada se otvori/zatvori virusom inficirana datoteka.
  - **sami se zakače za dokument koriste** aplikacije **makro programskog jezika**
  - zahvataju standardne funkcije programa, **oštećuju sam sadržaj datoteke**
  - zatim **inficiraju svaku narednu datoteku** koja se otvori

Primeri: *Concept, Marker i Melissa.*

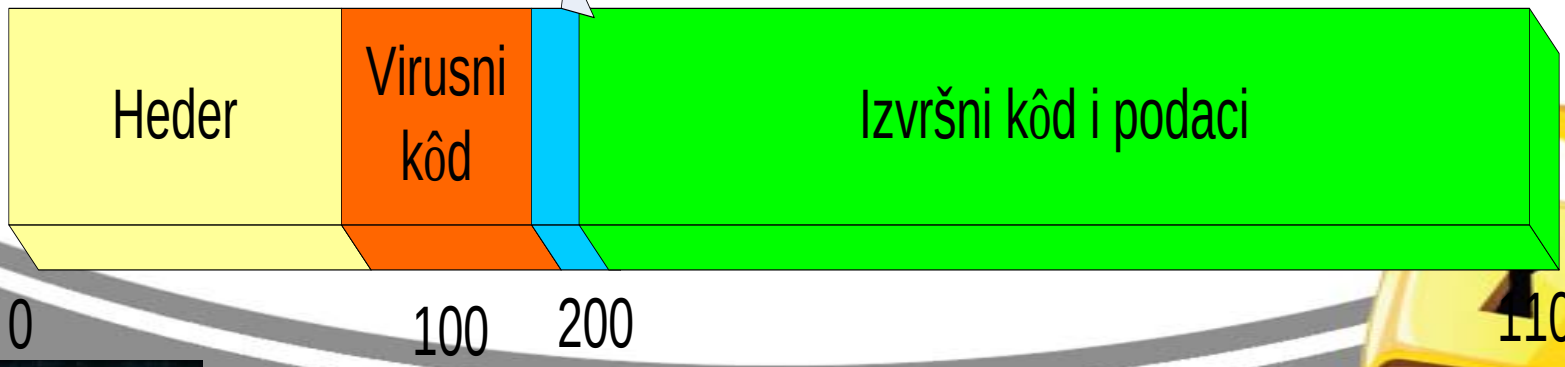
- **Lažni virusi**
  - daju lažne alarme virusnog napada i zahteva trenutnu akciju za zaštitu
  - izazivaju neznatne štete, troše operativno vreme i *mogu nositi Trojanca*

Primeri: *Good Times i Bud Frogs.*

Primer: Šifrovani virusi



Prva programska instrukcija koju treba izvršiti



Primer: Šifrovani virusi

Prvo se očita - jedini otvoreni tekst

Ključ za dešifrovanje

Virusni kôd

Rutina za dešifrovanje

Šifrovani virusni kôd

Mehanizam širenja i efikasnost virusa

- ***Direktni infektori***
  - **direktno inficiranju datoteku** , ne ostaju u RAM-u nisu univerzalni
  - mehanizam inficiranja nije efikasan, indikator je **dodatni rad diska**
- ***Indirektni infektori***
  - pokretanjem inficiranog programa **smešta se u RAM memoriju**
  - efikasnije širenje, inficira svaku datoteku, učitanu u RAM
- ***Brzi infektori***
  - inficiraju sve datoteke koje se izvršavaju i one kojima se pristupa
  - koristi čak i **AVP** da zarazi datoteke
- ***Spori infektori***
  - **inficiraju samo datoteke u fazi kreiranja/modifikacije**
  - zaobilaze programe za kontrolu integriteta (**ispravna veličina datoteke sa virusom**)

Primer: Rutina virusa

- **Primeri rutina .exe virusa *Microsoft Word* sesije:**
  - *Rutina()* - izvršava se u toku sesije *word* dokumenta:
    - *Document_Close()* - zatvara dokument (**Melisa**)
    - *AutoExec()*— startuje word
    - *AutoClose(), FileExit()*—zatvori dokument
    - *AutoExit()*—zatvara word
    - *AutoOpen(), FileOpen()*—otvori word dokument
    - *AutoNew(), FileNew()*—kreira dokument
    - *FileSave()*—memoriše dokument

Primer: Tok procesa analize malvera

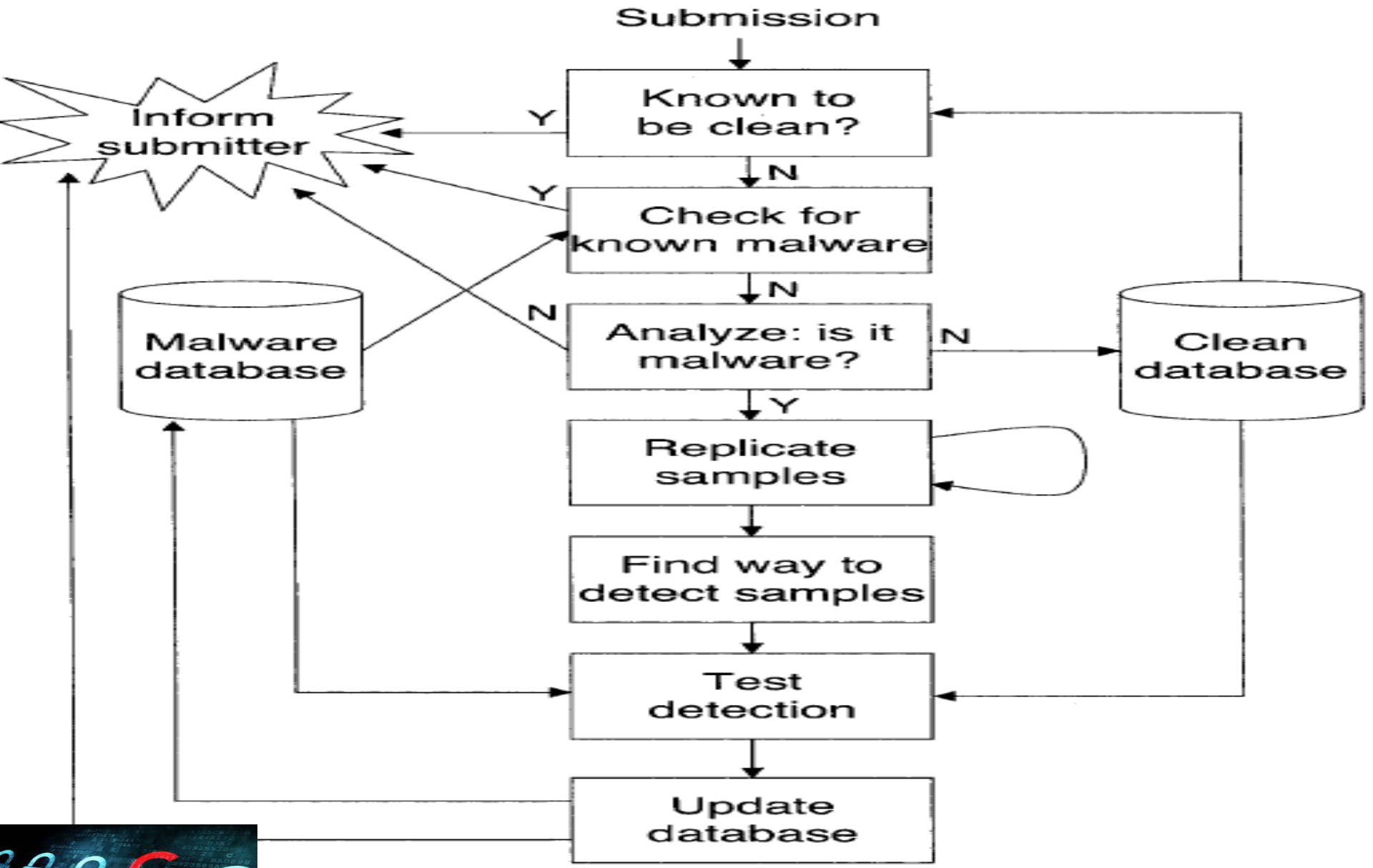


Figure 10.1. Malware analysis workflow

Primer: Otkrivanja virusa

CERT® Advisory CA-1992-02 Michelangelo PC Virus Warning

Original issue date: February 6, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information concerning a personal computer virus known as Michelangelo. The virus affects IBM PCs and compatibles. A description of the virus, along with suggested countermeasures, is presented below.

Crvi (*Worms*)

- **Programi koji menjaju ili uništavaju podatke:**
  - ima neke karakteristika virusa, šire kopije na druge RS preko RM
  - ne zahtevaju host programe i ne *prilepljuju* se uz izvršne programe
  - samoreprodukuju se i šire preko slučajno izabrani IP dresa, ali su **samostalni programi**
  - maliciozni su, zagušuju HD, mreže ili e-mail servere i prave druge štete

    Primer: *Happy 99 exe, Blaster worm, SQL Slammer worm;*

    ***Conficker* crv** se može naći na >1.7 million računara u svetu

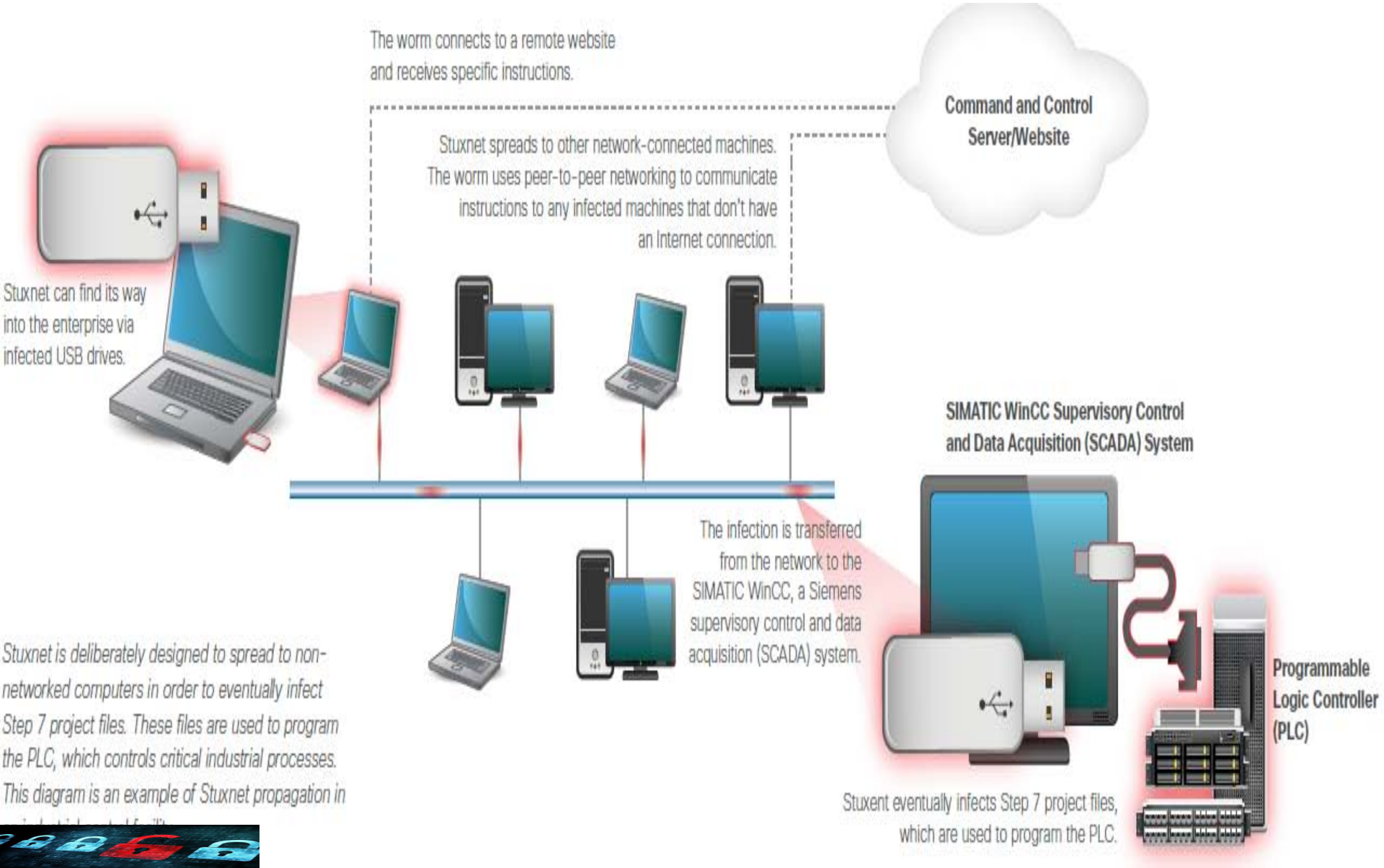
    ACAD/Medre crv kopira sve crteže u *AutoCAD*-u i šalje u šifrovanomm **.rar** dokumentu u Kinu (na 2 ULR adrese).
  - **Tipična struktura crva**

```
def worm():
    propagate()
    if trigger() is true:
        payload()
```

- ***Rabbits:***
  - Retko se sreću u praksi, brzo šire (kao *bakterije*), imaju dva tipa:
    - program koji **troši prostor HD** i
    - koji se **replicira kroz mrežu, ali briše prethodnu kopiju**

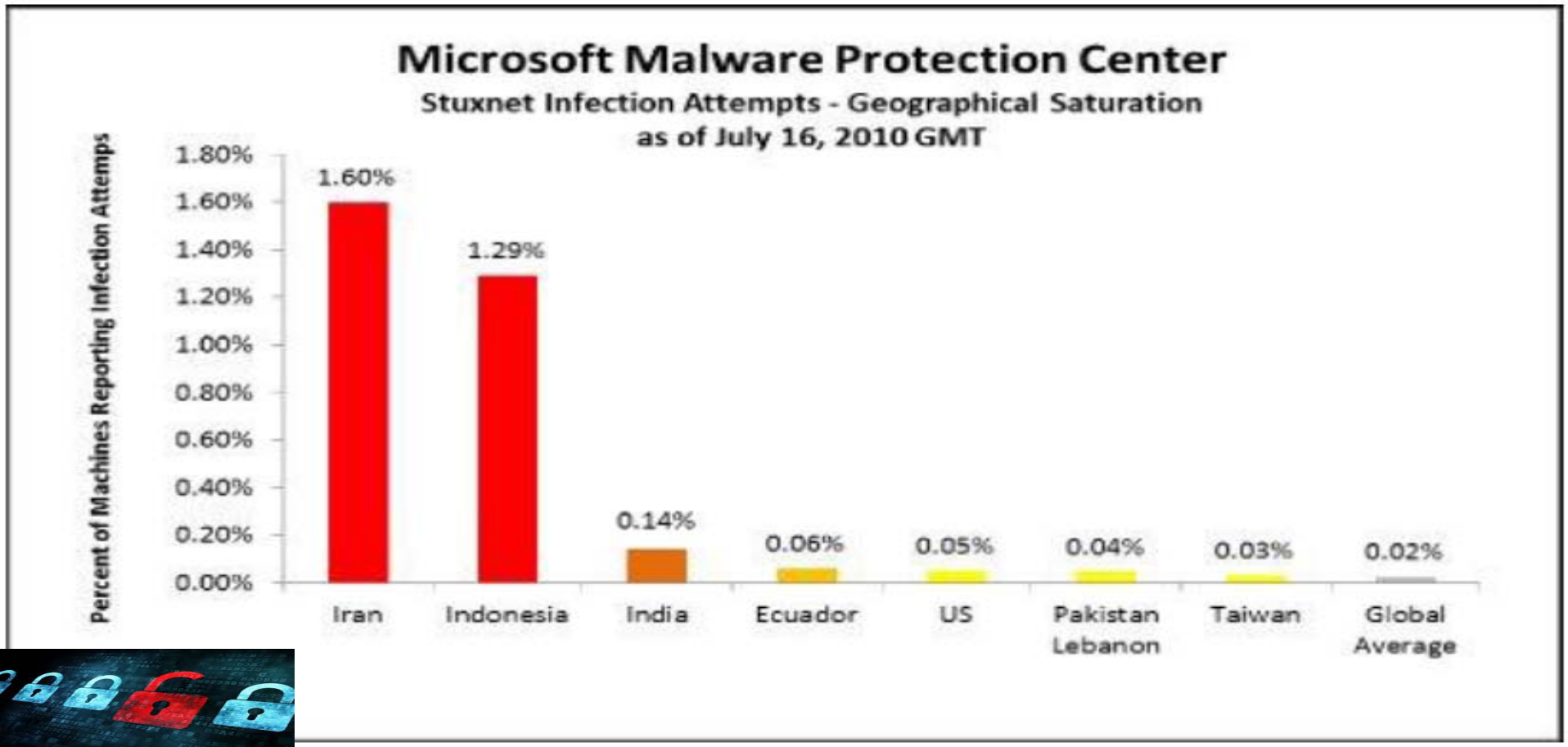
Primer: Propagacija *Stuxnet* crva

- Napada SCAD (*A supervisory control and data acquisition*) sisteme



Primer: Širenje Stuxnet crva

- CIA i Izrelska ambasada u SAD razvile sistem ***Flame*** **da:**
  - mapira i monitoriše Iransku računarsku mrežu
  - procenjuje pravo vreme *cyber* napada na zemlju
  - pripremi put za napad Stuxsnet crva na iransku nuklearnu centralu-Natanz
  - Stuxnet je sabotirao rad centrifuga upravljanih Simensovim PLC



Trojanci

- **Opšta svojstva:**
  - prosta forma, zabavna manifestacija, nisu virusi, ne inficiraju, ne umnožavaju se, čekaju pokretanje
- **Šteta**:
  - kopiraju, brišu datoteke/diskove, **šalju na računar napadača**
  - troše Internet-vreme, koriste računar za zloupotrebu/ kriminal
  - ubacuju se: *direktnim ili indirektnim unosom*
- **Modeli malizioznog izvršavanja**:
  1. ***nastavljajući funkciju*** originalnog programa
  2. ***nastavljajući i modifikujući funkciju*** originalnog programa
  3. ***kompletno zamenjujući*** originalne programe

Trojanci – ciljevi

- **Udaljeni pristup i puna kontrola nad računarom:**
  - imaju *klijentsku i serversku* komponentu
  - *klijentska komponenta* - na računaru napadača
  - *serverska komponenta* - na napadnutom računaru
  - *ako je uspostavljena veza* - napadač izvršava akcije
- **Najpoznatiji tipovi:**
  - *Keylogger*
  - *Downloader...*
- **Agenti distribuiranih DoS (DDoS) napada:**
  - prikriva dokaz o prisustvu (**rutkit tehnike**)
  - skupljaju pasvorde i šalju *pasvord-liste* e-poštom ...

Primeri: Napadi trojancem

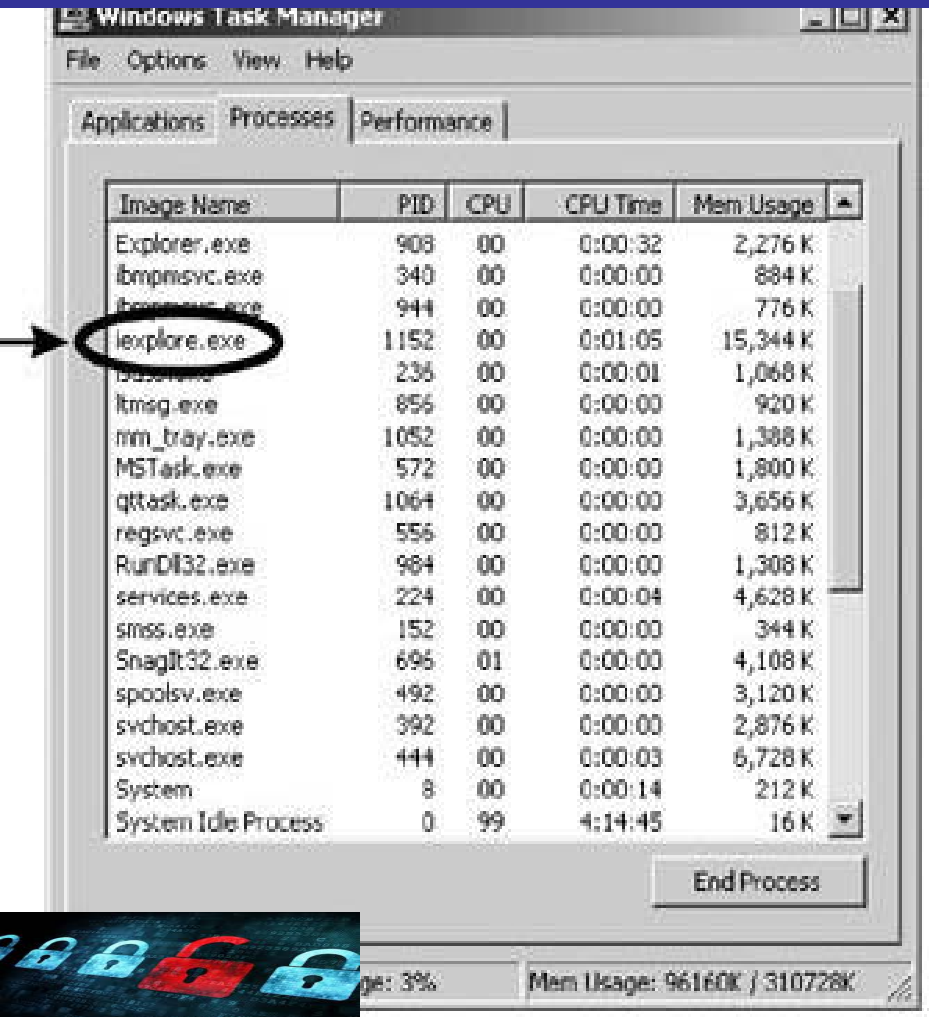
- **Primer 1: *Zeus-in-the-mobile ("Zitmo")*** trojanac za Android korisnike: maskira se kao "*Android Security Suite Premium*“; kad se instalira i pokrene pokazuje generisani aktivacioni kod
- **Primer 2**: Trojanac iz 2009 **'*URLZone*' izvlači bankarske podatke i krade novac** sa kompromitovanog računa; **nemoguće ga je otkriti**
- **Primer 3:** online krađa novca (Italija); napadač koristio *SpyEye* i *Zeus* Trojanca; napadač ubacuje skriven *iFRAME tag* i preuzima račun žrtve; inicira transakciju lokalno bez aktivnog učešća napadača

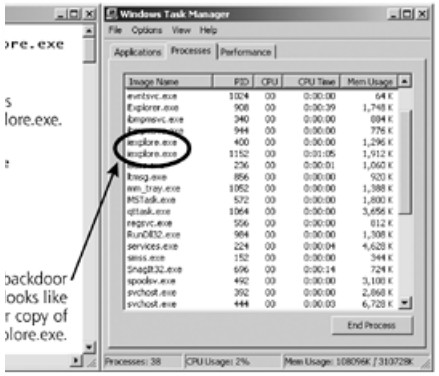
Primer: *Zitmo* trojanac maskiran kao AVP

Zitmo je trojanac *Zeus* za mobilne uređaje

Primer: Napad trojanca

- **iexplorer.exe** – normalan proces u Task manager-u (levo)
- novi **iexplorer.exe** (*trojanac*) kreira **Ncat** kopiju koja pokreće zadnja vrata za slušanje na **TCP** portu **2222** (desno)





Primer: Anatomija trojanca ***Coreflood (2008)***

- **Osnovni podaci:**
  - Jedna od najstarijih *botnet* mreža, radi >6 godina
  - Sa DDoS prešla na prodaju **servisa za anonimizaciju** u cilju bankarske prevare
  - Ceo Windows domen inficira odjednom (1000-de računara u nekim organizacijama)
  - Preko 378.000 računara infictirano u toku 16-meseci
  - Inficirani računari i IS poslovnih organizacija, bolnica, državnih agencija i organizacija, čak i policijske agencije

Vremenska bomba, mobilni kôd

- **Vremenske bombe, slična *trojancima*** mogu da unište p/i:
  - imaju ugrađeni **vremenski tempirani "*triger*"**
  - aktivira se u određeno vreme i pravi štetu
  - aktivira se u unapred isprogramiranom trenutku
  - ne pokreće ga korisnik – slučajno ili nesvesno
- **Mobilni kôdovi –*skriptovi:***
  - aktivni program/string u fajlu, prenosi se sa udaljenog na lokalni RS
  - izvršava se na lokalnom sistemu na komandu napadača
  - služi kao mehanizam za prenos malvera
  - **koristi ranjivosti sistema** da izvrši svoje akcije

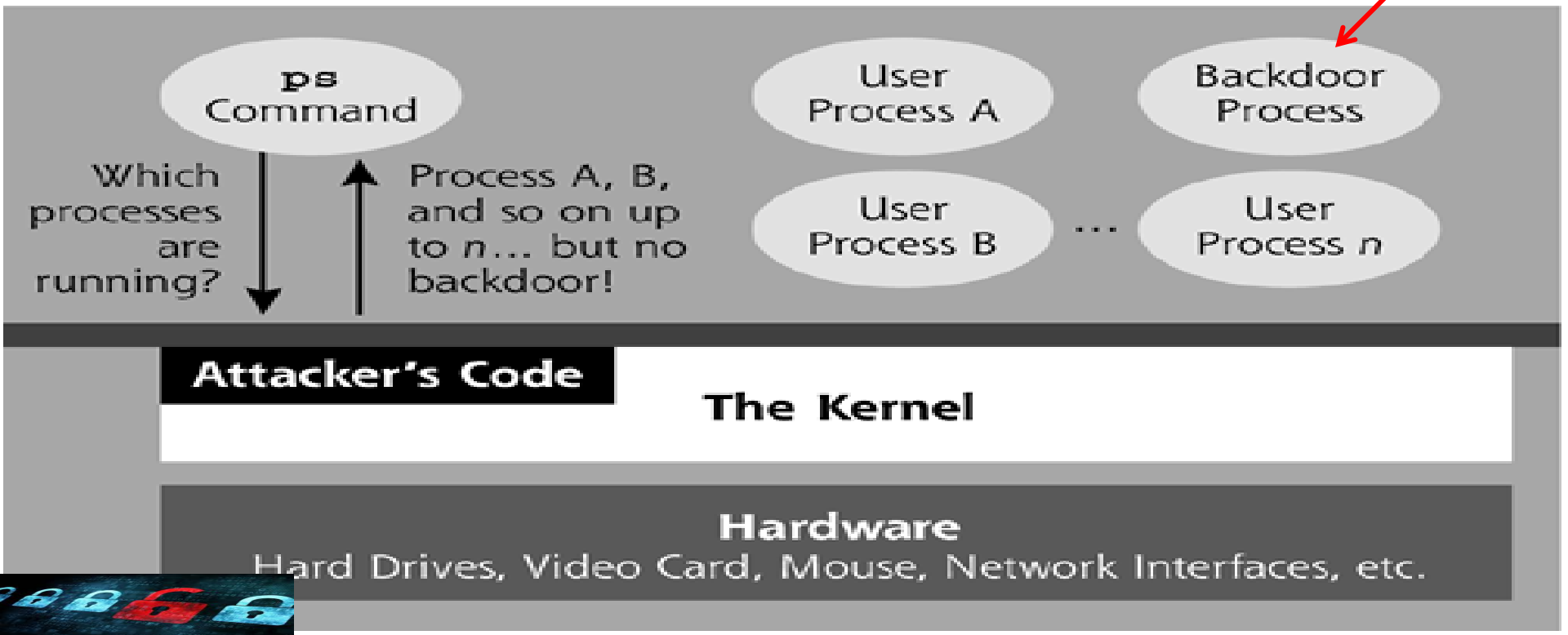
Primer: *Java applets, ActiveX,* ***JavaScript,*** *VBScript*

Rutkit tehnike

- Malveri za *zadnja vrata* za unos *trojanaca,* menjaju postojeći sistemski sw ili se upisuju u njega, **skrivaju prisustvo**
- Napadaju **kernel** OS, manipulišu, menjaju program na app. nivou

Primer 1: *Task Manager* ne pokazuje proces

Primer 2: *Secure shell daemon* (**sshd**) ili *Windows Explorer* **GUI**



Rutkit tehnike (1)

- **Za manipulaciju kernela *rutkit* generiše sledeće tehnike**:
  - **Skrivanje fajlova i direktorijuma** - *od korisnika i admin*.
  - **Skrivanje procesa** – *alati ne mogu otkriti zadnja vrata*
  - **Skrivanje mrežnog porta TCP/UDP** - *otvoren ulaz*
  - **Skrivanje promiskuitetnog moda** –*snifer napadča u RM*
  - **Preusmeravanje izvršavanja** - npr. **otvara zadnja vrata izmenom sshd šela**
  - **Intercepcija i kontrola U/I uređaja u RS** – modifikuje kernel da snima svaki otkucaj tastature u lokalni fajl (*keystroke logger trojanac*)

Primer: Kineski *bootkit*, *Kaspersky Lab* (6.04.2011)

- **Kernel-mod rutkit** otvara vrata za višestruku infekciju
  - Distribuiran sa *Trojancem daunloderom* sa kineskog porno sajta
  - Memoriše **MBR na 3. sektor** i zamenjuje ga samim sobom
  - Instalira **šifrovan drajver** i **ostatak koda** od 4. sektora na dalje
  - Kad se računar podiže, malver se izvršava i obnavlja originalni MBR
- **Windows se podiže bez otkrivanja prisustva *bootkit*:**
  - Kada se specifični deo **but procesa** izvrši, *bootkit* presretne funkciju ***ExVerifySuite***
  - Instalirana maska zameni sistemski **drajver *fips.sys*** sa malicioznim drajverom
  - **Drajver *fips.sys*** se ne zahteva za korektan rad OS, pa sistem neće pasti, ako se zameni
  - Maliciozni kod je napisan da startuje HD u šifrovanom formatu

Primer: Kineski *bootkit*, *Kaspersky Lab* (6.04.2011)-1

- Drajver ***fips.sys*** **detektuje** brojne AVP i **sprečava** njihov rad:
  - *Trend Micro, BitDefender, AVG, Symantec, Kaspersky Lab, ESET* itd.
- Zatim, drajver ***fips.sys*** kompromituje ***explorer.exe*** **proces** i ubacuje u računar varijantu ***bootkit daunlodera***
- Maliciozni program šalje na zahtev klijenta (hakera) :
  - informacije o računaru žrtve
  - IP address, MAC addresu itd.
- Ovaj ***butkit*** dalje daunloduje Trojanca ***keylogger-a*** koji
  - krade podatke o nalogu za *online* igru (npr**.** *LineAge2*)

Kombinovani napad (*Blended Attack*)

- **Koristi višestruke metode za širenje:**
  - E-mail
  - *Windows* zajedničke datoteke (*Share files*)
  - Web servere
  - Web klijente
  - slanja poruka i zajedničke datoteke u direktnoj arhitekturi (*peer-to-peer*)

Primer: ***Nimda*** (karakt. virusa, crva i mobilnog kôda)

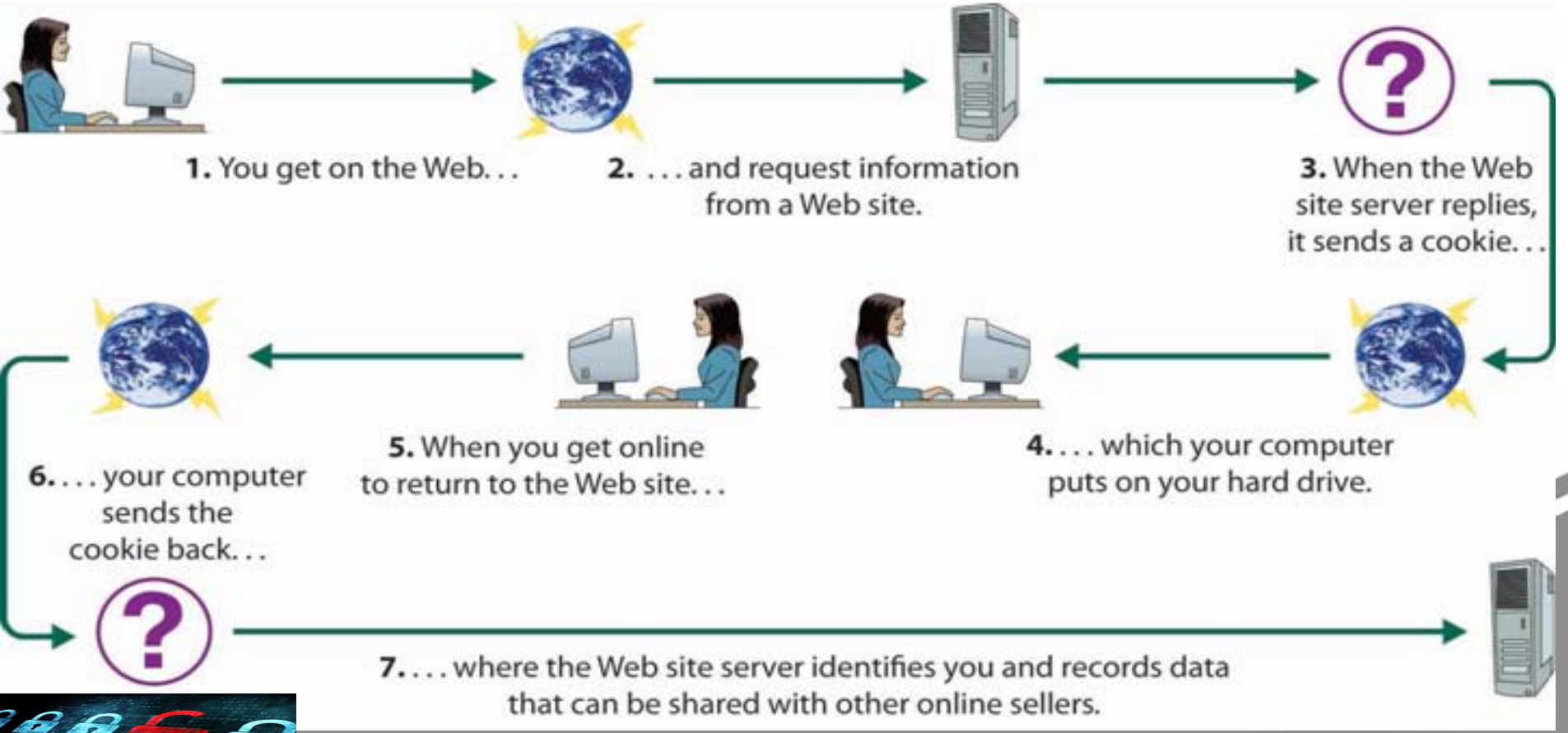
Fišing&farming i Spyware & Adware

- ***Fišing*** (socijalni inženjering)***:***
  - lažnim predstavljanjem poverljive web stranice za krađu identiteta
- ***Farming:***
  - Preusmeravanje na lažnu web stranicu ili korupcija DNS servera
- ***Spyware* skuplja**:
  - **Korisničko ime i pasvord** koristeći **aktivni *key logger***.
    (Keylogger trojanca pasivno skuplja otkucaje tastature)
  - ***Email* adrese**, korisne za spamere.
  - **Bankarske račune i brojeve kreditnih kartica**
  - **Ključeve softverskih licenci** za pirateriju
- ***Adware*** skuplja:
  - Reklamne podatke o ponašanju klijenata na web sajtu

Cookes (kolačići)

Sve pretrage, svaka ukucana reč u personalnom browser-u, svaka poseta nekoj web stranici se ostavlja u cookie!

Šema rada cookija



Primer: Uticaj napada malvera na CIA informacija

Maliciozni program/napad	Poverljivost	Integritet	Raspoloživost
Otvorena zadnja vrata	+	+	
Logovanje otkucaja tastature	+		
Korupcija BIOSa		+	+
Korupcija podataka/fajlova		+	+
DOS napad			+
Uznemiravanje/poruke		+	+
Nepotrebni e-mail/ spam		+	
Onemogućavanje AVP		+	
Instalacija trojanca		+	

Savremene pretnje i zaštita od neovlašćenog pristupa sa Interneta

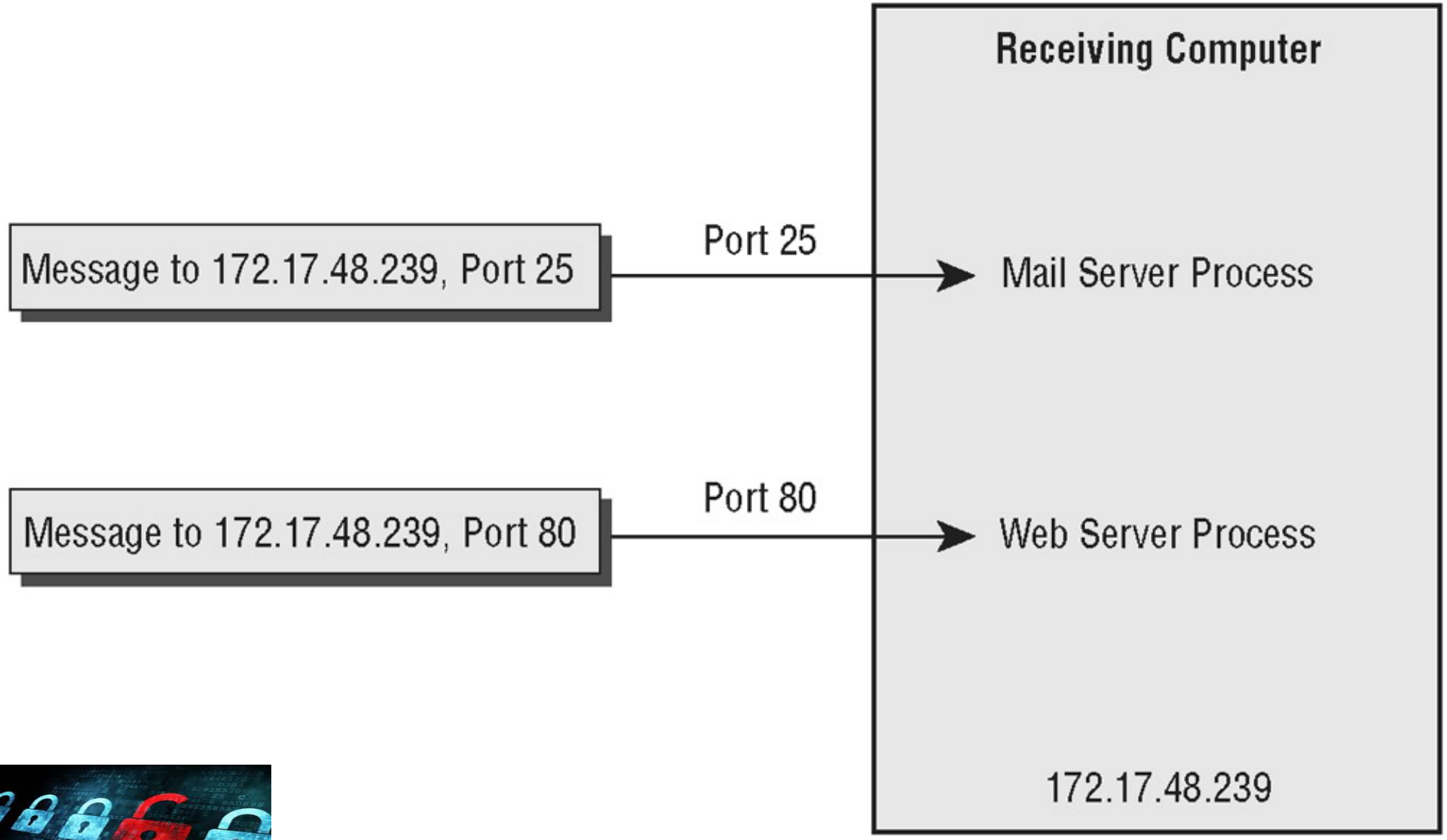
Tipične tehnike napada sa Interneta

- **maliciozni napadi** – uništavanje podataka
- **odbijanje servisa (**DoS/DDoS**)** – onemogućavanje rada
- **ponavljanje poruka** (*spam*) –sprečavanje prenosa p/i
- **pogađanje lozinke** – neovlašćeni pristup podacima
- **trojanci** – distribucija zlonamernih sw
- **lažno predstavljanje**–neautorizovani pristup
- **prisluškivanje** – neovlašćeno pristupanje podacima
- **kriptoanaliza** – otkrivanje tajnih ključeva i podataka
- ……

Napad na portove

- ***Port*** je logička pridružena tačka za komunikaciju računara u mreži
- U RM port nije fizički uređaj već jednostavno broj
- Preko portova računar održava tragove različitih komunikacija u mreži
- Na nivou računarskog sistema portovi su i tačke spajanja periferija na računar
- Većina *standardnih portova* je definisana Internet standardima (za protokole)
- U TCP/IP RM ima ukupno 65.535 TCP i 65.535 UDP portova
- Napadači koriste nestandardne portove da izbegnu *firewalls* i detekciju napada

Napad na portove



UDP portovi i protokoli

Port	Protocol
67	Dynamic Host Configuration Protocol (DHCP)
68	DHCP
123	Network Time Protocol
137	NetBIOS over TCP (NBT) Name Service
138	NBT Datagram Service
445	SMB over TCP
500	Internet Security Association and Key Management Protocol
1434	SQL Server
1900	Universal Plug and Play
4500	NAT Traversal protocol

TCP portovi i protokoli

Port	Protocol
88	Kerberos
135	RPC Endpoint Mapper
139	NBT Session Service
389	Lightweight Directory Access Protocol
445	SMB over TCP
464	Kerberos Password
593	RPC over HTTP
636	Secure LDAP
1433	SQL Server
3268	Microsoft Global Catalog
3269	Secure Global Catalog
3389	Remote Desktop Protocol

Standardni protokoli

Port	Protocol
20	File Transfer Protocol (FTP), Data
21	File Transfer Protocol (FTP), Control
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol (version 3) (POP3)
143	Interactive Mail Access Protocol (IMAP)
443	Secure Socket Layer (SSL)

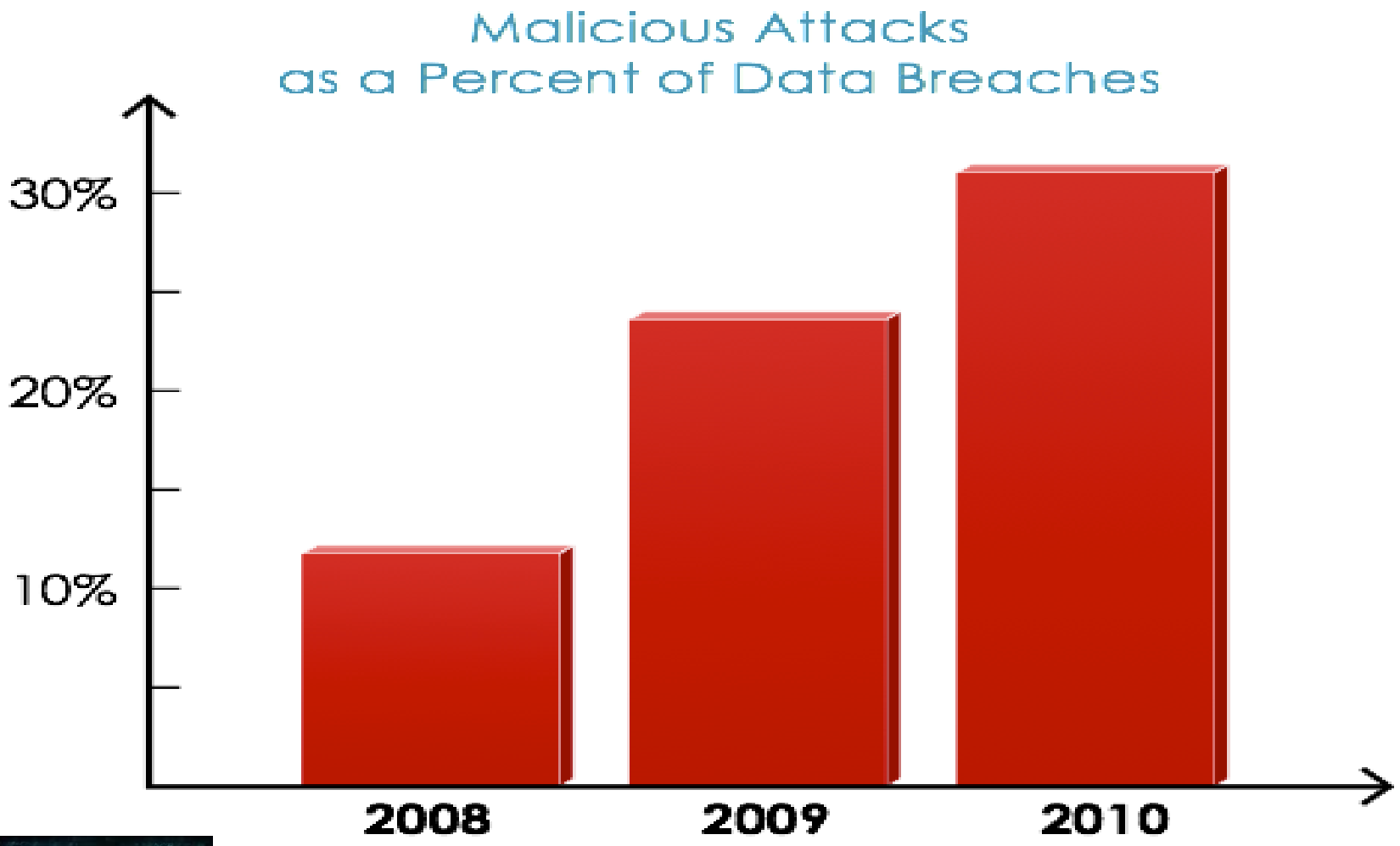
Pomeranje vektora napada sa Interneta

Vektor napada poslednjih godina pomera se sa relativno dobro zaštićenih servera lokalnih mreža, na *web* servere, baze podataka na *web*–u i pojedinačne nezaštićene računare umrežene na Internet

1996. godine	2009/2010. godine
Hakeri iz hobija	Profesionalni hakerski napadi na *web* servise
Prevaranti na *web* sajtovima	Organizovani kompjuterski kriminalci
Virusi i drugi maliciozni programi	Napadi odbijanja servisa (DoS, DDoS)
Retki napadi na *web* servere	Krađa identiteta, iznuđivanje, ucene
	Stalni napadi na *web* servere i društvene mreže

Pregled napada sa Interneta (2006- 2011)

Porast malicioznih napada (*Source: Ponemon*)



Primer: Statistika pretnji 2010. *(SpiderLabs, 2011)*

Izvor pretnje	Procenat (%)
Najčešći napad na industriju hrane i drugih stavki potrebnih za život	57
Napadi uspešno zbog nebezbednosg TTP softvera i slabe prakse upravljanja	88
Krađa podataka kreditnih kartica *online* (u tranzitu)	66
Od svih napada u 2010, odgovorna jedna organizacija kompjuterskih kriminalaca	30
Sofisticirani napadi na mobilne uređaje i sajtove društvenih mreža (malveri i socijalni inženjering) ciljanim napadom	najčešći
GSM lokacija olakšava napade na autentifikacione podaci IKT sistema kompanija, osetljivi podaci i poslovne tajne	najčešće
Antivirusni softveri gube bitku protiv malvera, potreba za proaktivnom zaštitom	

Primer: Evolucija malvera

(*Luis Corrons, PandaLabs*, 24.11.2010.)

- **U 2010. – generisano 34% (1/3) od svih malvera do sada kreiranih:**
  - automatski detektovale baze podataka kompanija širom sveta
  - analiziraju i klasifikuju **99,4% od svih primljenih pretnji**
  - u **134 miliona fajlova** - 60 miliona malvera (virusa, crva...)
  - kreirano **20 milion** novih i modifikovanih kodova malvera
  - prosečno je dnevno generisano na Internetu **63.000** (53.000 u 2009)
  - prosečno je dnevno generisano na Internetu **75.000 (2011.)**
  - od toga je 54% tipova malvera aktivno samo 24 časa
  - **relativni godišnji porast je u opadanju** ???:
    - u 2003. – 100%, u odnosu na 2002.
    - u 2010. – 50% u odnosu na 2009.
  - *Google Security Team (2012):*
    - detektuje oko **9.500** novih **malicioznih web sajtova** dnevno
    - izdaje nekoliko miliona upozorenja korisnicima

Primer: Napadi malvera (2012)

- **Kiber špijunaža**, napad na **privatnost** i **socijalni inženjering**
- **Glavno oružje za napad**:
  - **Trojanci**
  - **Socijalni inženjering** za krađu ličnih podataka sa društvenih mreža
  - **Olakšavaju ih mobilni uređaji**
  - Korisnici se **lažno osećaju bezbednim**, okruženi prijateljima i porodicom na društvenim mrežama
  - Hakeri koriste tu lažnu sigurnost za krađu identiteta

2011_cwe_sans_top25

Primer: Napadi malvera (2012) -1

1. Destruktivni *Disstrack* malver (Sept 2012)

- Inicijalno ubacuje komponentu za prepisivanje (*wiper*)
- Prvo prepisuje prioritenu listu fajlova iz:
  - *Documents and Settings, Users* i *System32\Config* foldera
- Prepisuje fajlove sa 192KB blokovima sa slučajnim podacima i delovima JPEG slika zapaljene SAD zastave
- Zatim prepisuje *Master Boot Record* i aktivnu particiju
- Napad (tzv.*Shamoon*) je veoma ciljan
- Detektuje ga većina AVP, a uklanja se brisanjem servisa ddr:
  - ddr.sys u %System%\Drivers folderi i
  - ddrisk.sys u %System%\Drives folderu

Primer: Napadi malvera (2012)-2

2. Mobilni malveri

- Postaju profitabilna industrija
- Deo mehanizma za plaćanje namenjen za finansijske prevare (tzv. "*Toll Fraud*")
- Preovlađuje u poslednjih nekoliko godina
- Tip *Toll Fraud* malvera ***FakeInst***, zauzima 82 % napada u junu 2012
- Ukradeni milioni dolara u Rusiji, Srednjem Istoku i delovima Evrope

3. Lažni AVP: "Windows 8 Security System"

Primer: Napadi malvera (2012) -3

(*PandaLab; ISACA Verizon Lab*)

- **Malveri za mobilne uređaje***:*
  - **android OS**
  - zaštita podataka na svakoj pristupnoj tački (**jaka autentifikacija**)
  - početak **integracije mobilnih i medicinskih** uređaja
  - veća potreba za zaštitu **zdravstvenih IS**
- **Veća infekcija skladišta aplikacija nego brauzera***:*
  - posebno neautorizovanih
  - razvoj sistema za evaluaciju bezbednosti skladišta aplikacija
- **Malveri za Mac OS-e:**
  - *PC malveri – rastu eksponencijalno* tokom nekoliko poslednjih godina- 75% malvera u 2011 bili su trojanci
- **Napadi na mala i srednja preduzeća***:*
  - DB gde su kreditne kartice uskladištene u otvorenom tekstu
  - **nemaju posvećene timove za zaštitu**

Primer: Napadi malvera (2012) - 4 (*PandaLab; ISACA Verizon Lab*)

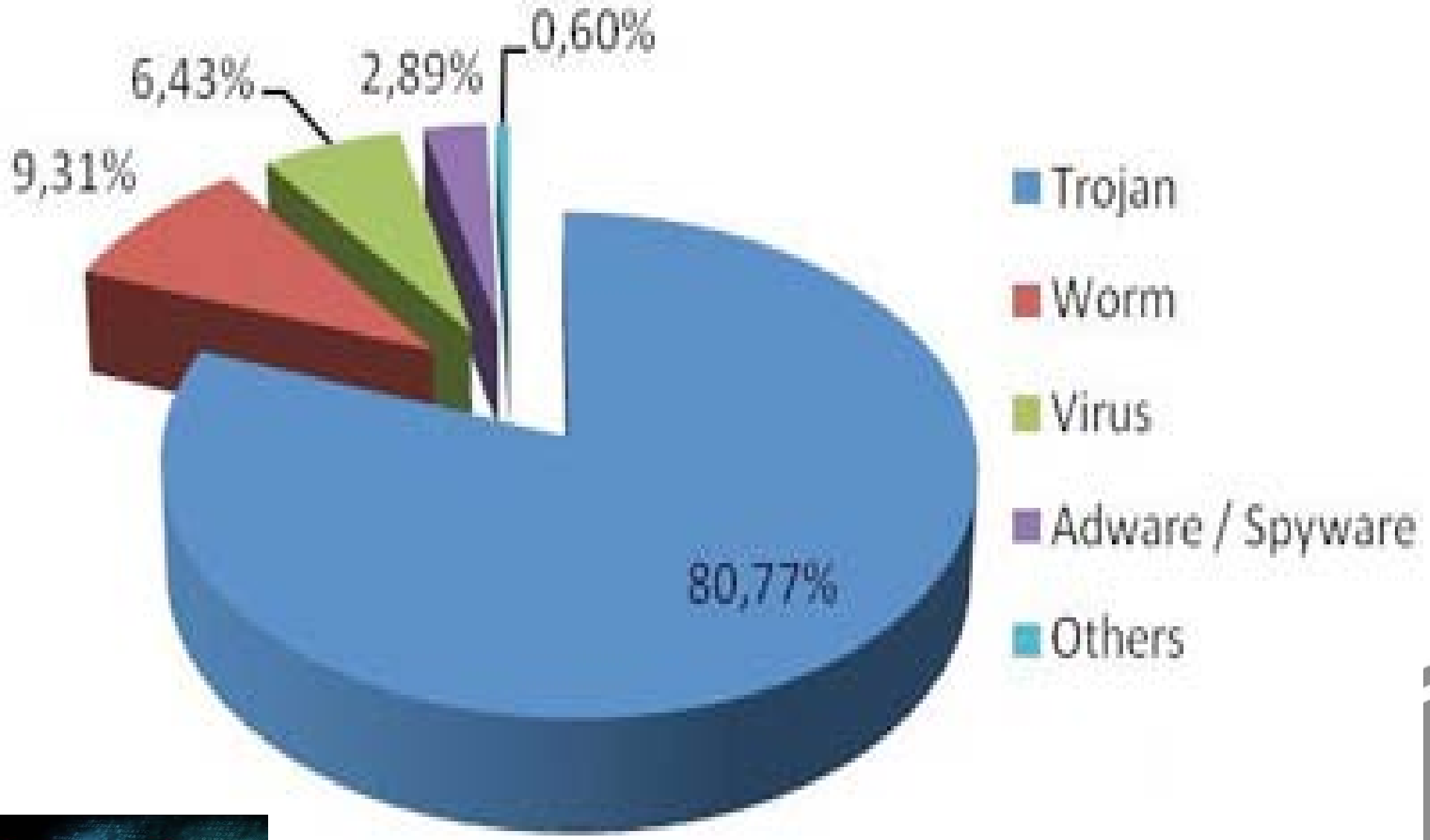
- **Napadi na** *Windows 8 OS* **(planiran za novembar 2012):**
  - Win 8 će omogućiti korisnicima da naprave malver za gotovo svaki uređaj
- **Online kupovina**:
  - **Veća upotreba mobilnih uređaja** nego računara na poslu
  - **Veća briga za zaštitu ličnih mobinih uređaja** nego računara na poslu
  - Nedovoljna pokrivenost upotrebe mobilnih uređaja **u politici zaštite**
  - Razvoj mehanizma zaštite u sloju aplikacija za online kupovinu
- **Migracija** na **IPv6 protokol** i nove generacije **BGP i DNS**:
  - Otkriće se nove ranjivosti izazvaće generisnje novih eksplita
- **Povećana sertifikacija bezbednosti informacija:**
  - **Zbog većeg poverenja** u bezbednosnom haosu na Internetu
  - **Zaštita identiteta na Internetu biće obavezna**

Primer: Statistika pretnji 2012. *(PandaLab)*

- **(PandaSecurity Lab) U 1. kvartalu 2012:**
  - Generisano **6 miliona** novih malvera
  - Kompjuterski kriminalcii koriste najviše Trojance, a ne crve
  - Prosečan broj inficiranih PC: svet (35,51%); Kina (54,25%); Tajvan i Turska; Japan najmanje - (30%) ...

	2011 (%)	2012 (%) -1.kvartal
Trojanci	73	80
Crvi	9,30	8
Virusi	6,43	14,25

Primer: Zastupljenost malvera (juni 2012)



Primer: Proces skupljanja podataka botnet-a

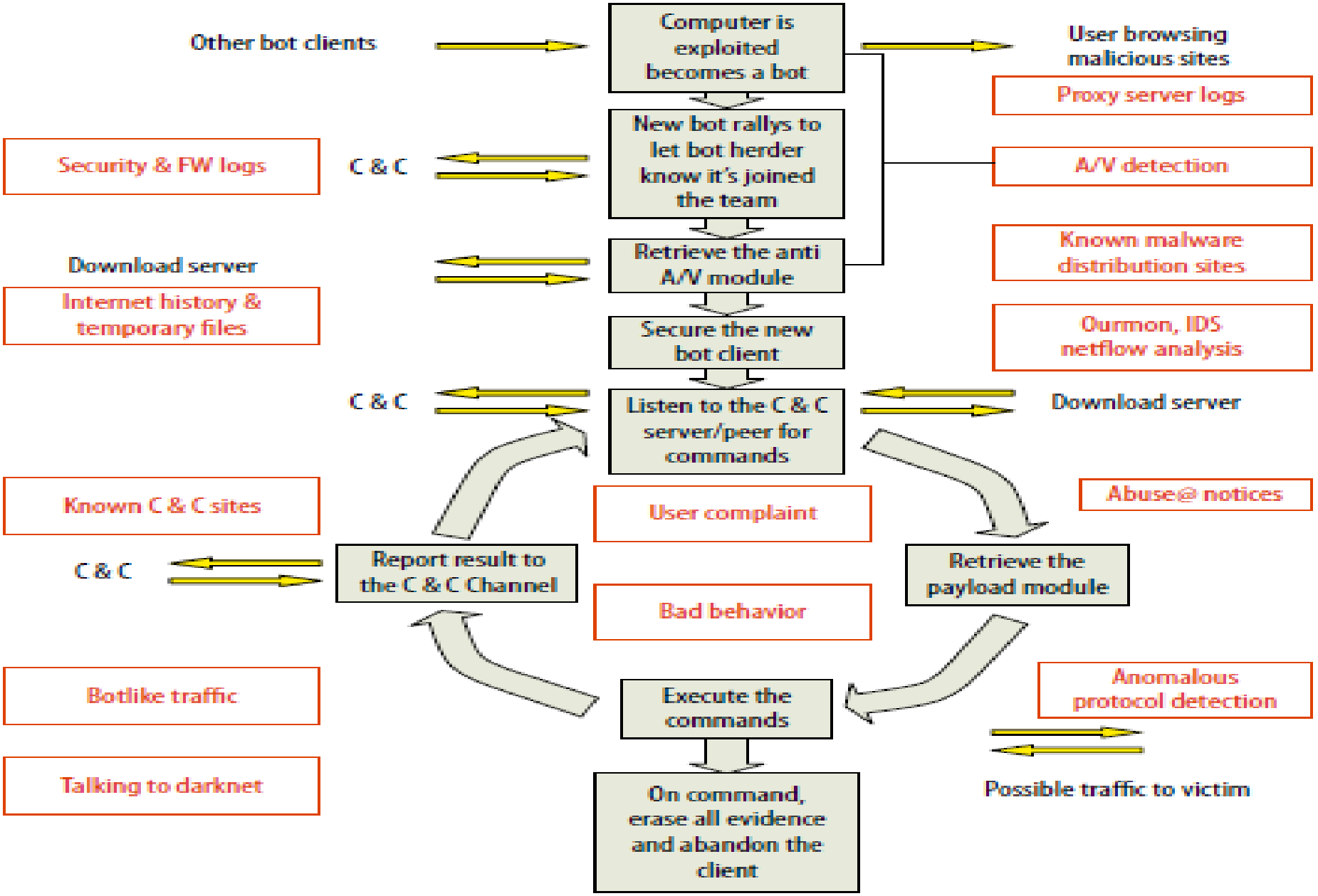


FIGURE 3.2 Botnet communications collection

Primer: Botnet - eksperimet

(*ESET's istraživač Pierre-Marc Bureau i timteam at Ecole Polytechnique de Montreal, 20.12.2010***)**

- *Botnet* - mreža **zombira računare**, koja šalje *spam* sa M/P i napada web sajtove
- Za hvatanje kriminalca morate misliti kao on – *profilisati ga*
- Umrežen klaster od **98** servera sa **VM** sa **3.000 Win XP OS**, **izolovan od Interneta** (eksperimentalna RM)
- Instaliran **C&C server** za kontrolu određenog broja botova, koji šalju naredbe ostatku *botnet-a*
- Mašine su inficirane sa poznatim crvom **Waledac,** lansiran početkom 2010 i koji kontroliše **100 hiljada** računara i šalje preko **1,5 mlrd *spam*** poruka dnevmo (*Microsoft*)

Primer: Botnet – eksperimet (1)

- Izvršeni su brojni napadi koji na realnom *botnet-u* ne bi bili mogući
- Jedan napad je bio tzv. ***Sybil* napad** koji ubacuje lažne *botove* da izazovu promene ponašanja i zaustave slanje spama *botnet* - a
- **Rezultati testa:**
  - *botnet* **mreža koristi slabu šifru** za komunikaciju između *botova* i C&C centra
  - u velikom *botnet-u* **sa jakim šifarskim sistemom C&C centar ne bi mogao upravljati zahtevima**
  - nije poznato kako utiče saobraćaj drugih RM na Internetu na rad *botnet-a* u realnom sistemu

Primer: Botnet – eksperimet (1)

Eksperiment Microsoft-a (2012):

- Istraživački tim je otkrio da je 20% novih PC, kupljenih iz nepoverljivih izvora snabdevanja već inficirano sa malverom
- Uključivanjem na Internet, malver (trojanac) korisnički računar automatski uključi u botnet mrežu
- Računar špijunira vlasnika i sve druge računare preko USB-a

Pretnje nove generacije

(*FireEye, Inc, White Paper*, **april 2014**)

- **Kompjuterski kriminalci**:
  - prilagodili tehnike frontalnog napada na ***skrivene, personalizovane i ciljane računare***
  - i dalje traže informacije za identifikaciju lica
- ***Spam*** **i** ***fishing su*** **dominantne tehnike napada:**
  - za kompromitaciju RM i krađu poslovnih podataka
  - *spam* često nosi malver (*Adobe reade* apdejt, lažna skype stranica itd.)

Pretnje NG - Glavni ciljevi napada

- **Krađa intelektualne imovine, baknarskih podataka, poverljivih informacija firmi**

Primer 1 (2011, mart): krađa RCA rešenja za dvoslojnu autentifikaciju

- tehnika *fishinga* zaposlenog - otvorio sp*readsh*eet na zaraženom sajtu
- instalirao *Backdor trojanca* – *Poison Ivy*
- ugroženi korisnici kompanija širom sveta

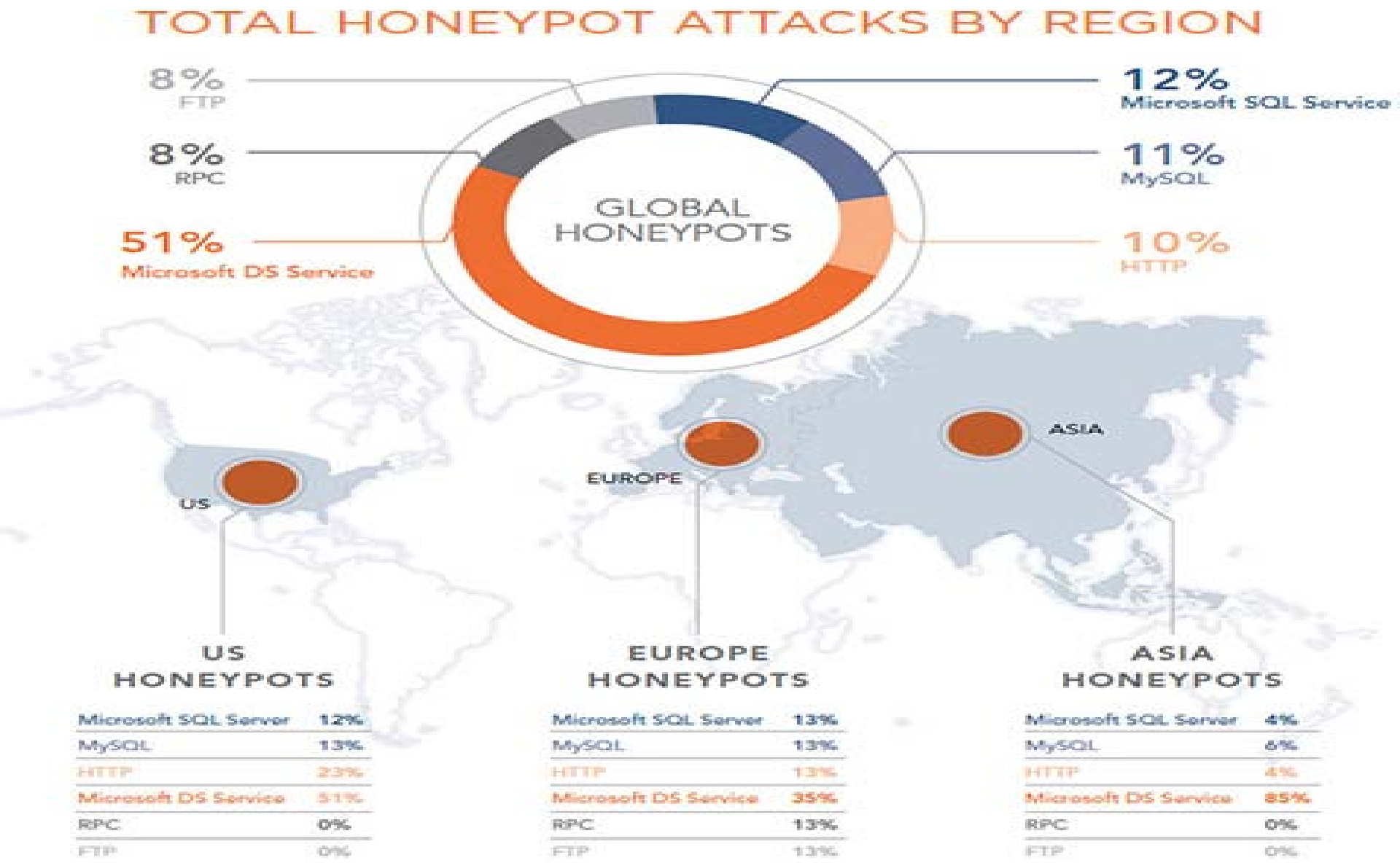
Primer 2: Operacija *Aurora* krađa izvornog koda:

- Simanteka, Googla, Adobe, Intela i organizacije *Stanely* preko IP
- višefazni napad, korišćeni podaci ukradeni sa društvenih mreža i ranjivosti nultnog dana (“0 –day”)
- ovi podaci mogu omogućili administraciju DB, krađu sa računa firme itd.

Pretnje NG - Glavni ciljevi napada

- **Haker u kompromitovanom računaru može**:
  - presresti, izbrisati, modifikovati, preusmeravati svu komunikaciju u i iz računara
  - ako kompromitovani račnar nema neku vrednost – postaje **deo botnet mreže**
- **Korisnici društvenh mreža (2014)**:
  - Oko **500 miliona** u svetu (**2 miliona** u Srbiji)
  - 2/3 primali spam,
  - *fishing* napadi porasli sa **30%** (2009) na **43%** (2010)
  - novi napad malvera **svake sekude (**2010**)**

Trendovi napada na CC (22.04.2014)



Generičke mere zaštite od malvera

- *razvoj svesti o potrebi zaštite*
- *sistem za kontrolu pristupa*
- *provera integriteta*
  - *blokiranje nepoznatog saobraćaja*
  - *kriptološki mehanizmi*
  - *primena DS i jaka autentifikacija*
  - *jaki Kz ključevi, česta izmena*
  - *zaštita IP adresa servera (od DOS/DDoS),*
  - *PKI i smart kartice - za generisanje DS i čuvanje Kz parametara*
  - *višeslojna AV zaštita na bazi:*

- **Ključne oblasti zaštite**

1. Fizička zaštita
2. Softverska zaštita
3. Pravna zaštita

1. Fizička zaštita

- Magnetne kartice
- Kartice sa RFID čipom
- Vrata sa numeričkim šiframa
- Skener za otisak prsta, šake
- Skener oka...

Fizička zaštita - manipulacije

- **Magnetne kartice** --> dostupni čitači i pisači za kopiranje
- **Kartice sa RFID čip**om --> dostupni čitači i pisači za kopiranje
- **Vrata sa numeričkim** šiframa --> dostupni softveri
- **Skener za otisak prsta** --> plastelin rešava u 90% slučajeva
- **Skener oka** --> sintetizovane slike oka...

2. Sw zaštita - LAC

- Kontrola pristupa (LAC)
- Korisničke grupe (privilegije)
- Organizacija mreže (*Firewalls*)
- Pametni sistemi (smart kartice...)

2. Sw zaštita - manipulacije

- Nezadovoljni zaposleni
- Konkurencija

Pravni aspekti (KZ)

- **Neovlašćeno korišćenje RS/RM (**Član 186a) - od **3 m. do 5g.**
- **Računarska sabotaža (**Član 186b) - **od 1 do 8 g.**
- **Izrada i unos računarskih virusa (**Član 186v)- od **3m. do 3 g.**

Ključni servisi za zaštitu web servisa (WS-a)

1. **Servisi za upravljanje SOA* WS-a**:
   – obezbeđuju mehanizme za instalaciju, održavanje, monitoring i otklanjanje grešaka u funkcionisanju WS-a
2. **Servisi za komunikacije SOA WS-a**:
   – obezbeđuju podršku za modele komunikacija između WS-a
3. **Proceduralni servisi** (politika i procedura):
   – obezbeđuju okvir za kreiranje, administriranje i upravljanje politikama za zaštitu, alokaciju resursa i performanse WS-a
4. **Servisi za zaštitu** (*Tehničke kontrole zaštite*):
   – obezbeđuju podršku za različite modele i tehnologije zaštite, koje proširuju ključne protokole zaštite WS-a

***SOA – sevisno orijentisane aplikacije**

Zaštita od novih tipova pretnji

- **Klasični *Firewalls, IPS, AVP, Web gatways alati***:
  - *Sprečavaju samo **poznate** malvere, ponovljene stare i sa crne liste URL adresa*
  - **Ne mogu sprečiti**
    - "0-day", jednokratni, multifazni i multi-aplikacioni napad malvera
  - **Moraju se modifikovati** za dinamičku analizu *nepoznatih pre*tnji u realnom vremenu
- Savremeni malveri lako zaobilaze ove mehanizme
- Potreba prediktivne zaštite

Zaštita od novih tipova pretnji

- ***Firewalls* nove generacije dodaje sloj**:
  - zasnovan na politici zaštite kosisnika i aplikacija i konsoliduje AVP i IPS
  - ne dodaje dinamičku zaštitu od pretnji NG
- ***IPS*** detektuje malvere na bazi *potpisa, ispitivanja paketa, DNS analize i heuristike* :
  - ne detektuje “0-day “eksploite, maskirane i isporučene u fazama
- ***AVP&Web filteri***: propustiće nove tipove napada
- **Filtriranje spama e-mejlova:**
  - za oporavak prosečnog fishing sajta treba najmanje **2 dana**
  - prenošenje malvera mašinama (laptop) i uređajima (USB)
  - neće detektovati dinamičke URL sajtove ni interni web filteri
- Sajber kriminalci napadaju simultano u odvojenim akcijama:
  - *skeniranje mejla, istraga eksploita, skeniranje fajla na malvere, analiza URL crne liste*...
  - **Ni jedan alat ne može pratiti sve ovo u realno vremenu!**

Bezbednost društvenih mreža

- *Whots-up, Facebook Messenger, Sky*pe
- Svaka aplikacija testirana na 7 kriterjuma- Da li su vaši podaci:

1. *Encrypted in transit?*
2. *Encrypted so the provider can't read it?*
3. *Can you verify contacts' identities?*
4. *Are past communications secure if your security keys are stolen?*
5. *Is the app code open to independent review?*
6. *Is security design properly documented?*
7. *Has the code been audited?*

Najbezbednije aplikacije (7I7)

- **Chatsecure** - slobodan, messaging app za Android i iOS,
  - zahteva registraciju na *Facebook, Google ili Jabber*
- **Cryptocat** -najflexiblnija, za Chrome, Firefox, Safari, Opera, OS X i iOS.
- **Signal** / **RedPhone** / **Textsecure** -slobodna (by Whisper Systems),
  - Šifruje pozive visoko bezbedan
- **Silent Phone** / **Silent Text** – slobodna, zahteva pretplatu (by Silent Circle),
  - Šifruje pozive i šalje poruke na iOS i Android

Srednje bezbedne aplikacije (2/7)

- WhatsApp, Facebook, Skype and Google Hangouts
  - **Vrlo slabe u pogledu** privatnosti i bezbednosti informacija

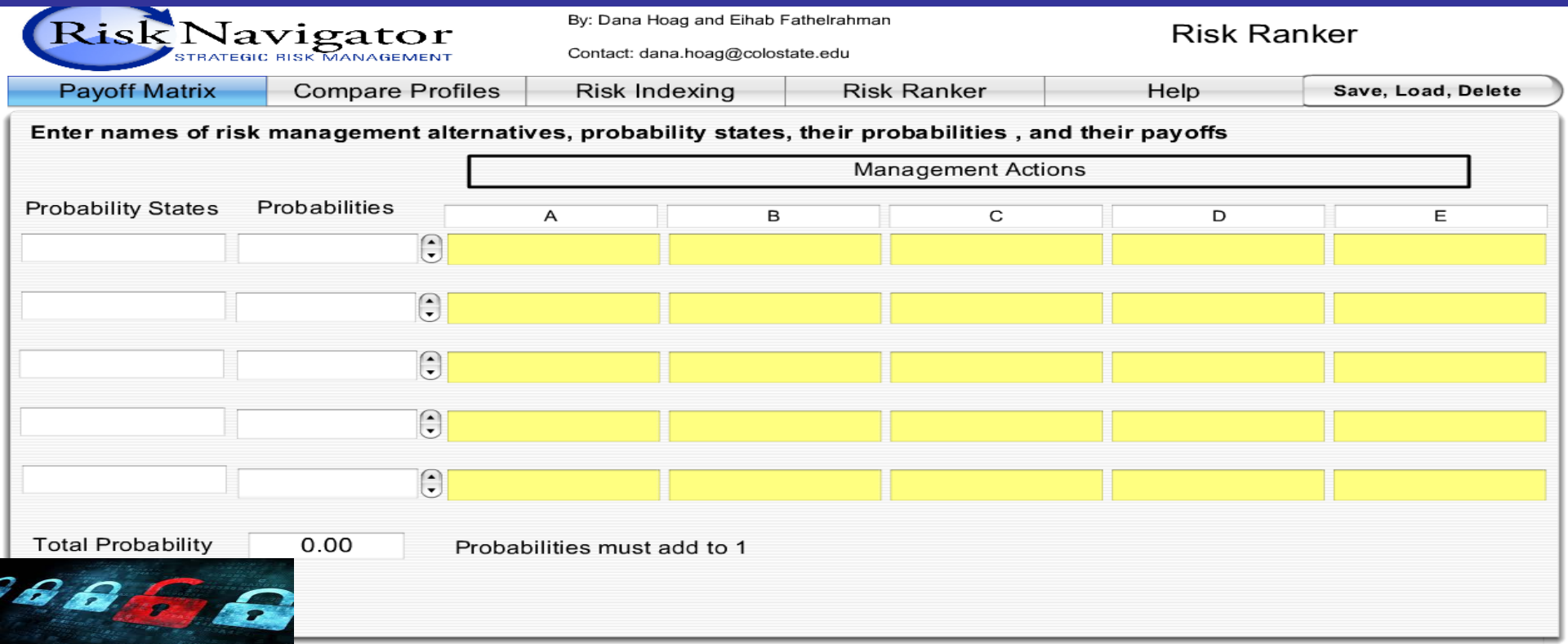
Najnebezbednijeaplikacije

- AIM, BlackBerry Messenger, Ebuddy XMS, Hushmail, Kik Messenger, Mxit (0/7), QQ (0/7),Secret, Viber, Yahoo! Messenger.

Primer: Novi metod AVP za zaštitu mobtela

(NQ Mobile'sMobileSecurityResearch Center i North Carolina State University):

- Otkrili novi metod AVP za detekciju malvera bez uzorka/potpisa
- ***RiskRanker*** osnovna metoda:
  - jedinstven sistem za proaktivnu analizu rizičnog ponašanja aplikacija pre uvođenja u mobtel
  - koristi dvostepeni metod otkrivanja malvera
  - povećava tačnost (od >100.000 skeniranih app. otkrio 718 pretnji malvera od čega **322 nultog dana**)



Primer:Bitdefender Anti-Theft AVP

(http://goo.gl/arwbE)

- Namenjen za zaštitu *Android* i drugih smart telefona od krađe:
  - povezauje se sa e-mapom
  - alarmira vlasnika kad lopov pokušava zameniti SIM karticu
  - može zaključati uređaj, uključiti alarm i izbrisati podatke na uređaju koji je kod lopova

Pitanja