# Streľba na pohyblivý terč

Peter Košinár
*kosinar@eset.sk*

12. apríla 2011

# Čo dnes uvidíme...

1. Úvod
2. Škodlivý softvér
   - Trocha histórie
   - Zdroj problémov
3. Čo? Ako? Prečo?
   - Motivácia
   - Implementácia
   - Strach, strach, strach
4. Obrana
   - Metódy obrany
   - Implementácia
   - Porovnávanie

# Čo sa mi to deje s počítačom?!

- “Môj počítač je dnes dajáky zabrzdený!”
- “Nefunguje mi Internet!”
- “Zmizli mi súbory!”
- “Myš sa mi hýbe sama od seba!”

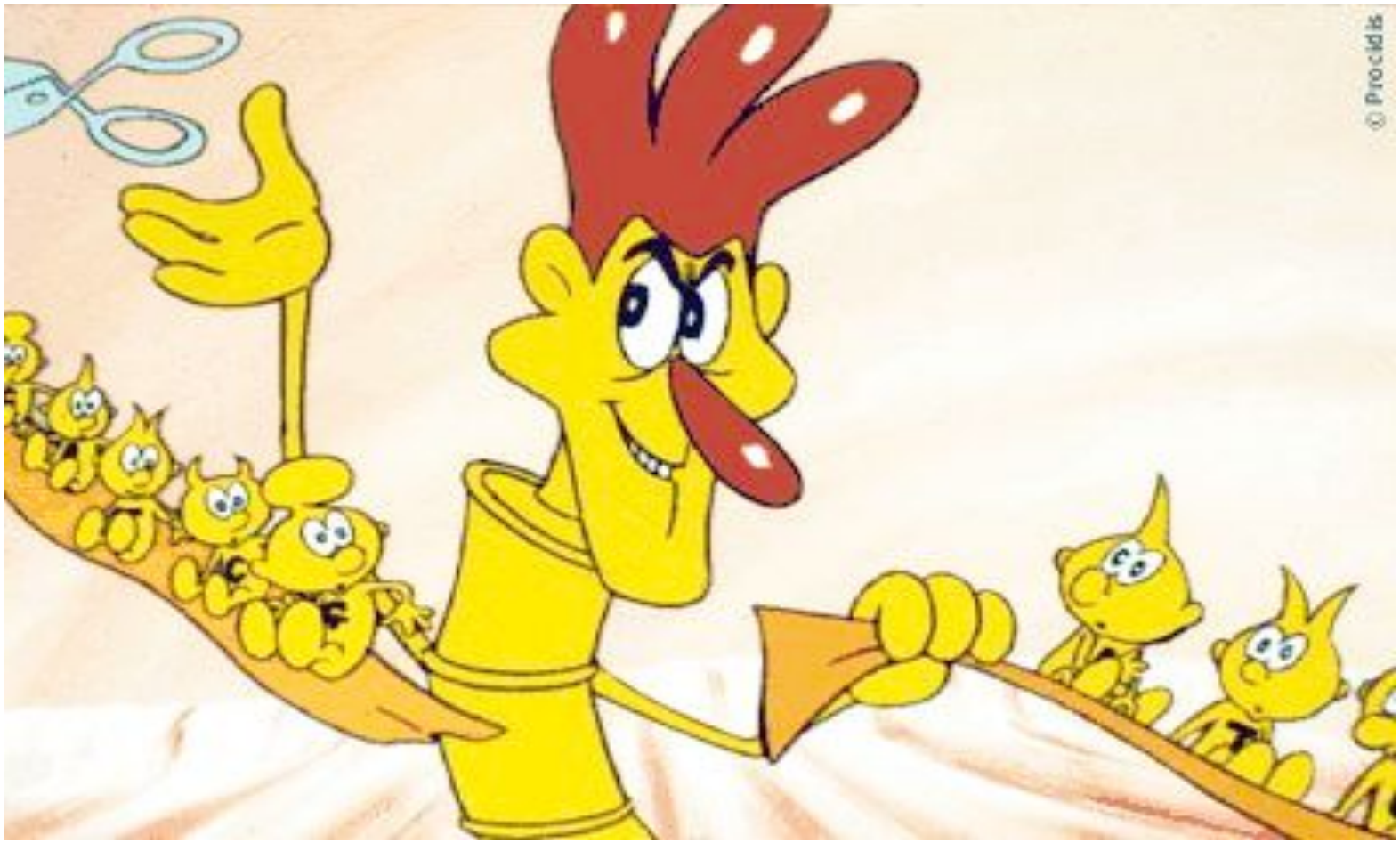
# Čo sa mi to deje s počítačom?!

- “Môj počítač je dnes dajáky zabrzdený!”
- “Nefunguje mi Internet!”
- “Zmizli mi súbory!”
- “Myš sa mi hýbe sama od seba!”
- JE TO VÍRUS!

# Čo sa mi to deje s počítačom?!

- “Môj počítač je dnes dajáky zabrzdený!”
- “Nefunguje mi Internet!”
- “Zmizli mi súbory!”
- “Myš sa mi hýbe sama od seba!”
- JE TO VÍRUS!
- “Nainštaloval som si SuperAntiUltraMegaAntivirus 2011 a vôbec to nepomohlo!”

# Čo sú vírusy?



# No ale fakt. . . čo sú vírusy?

**Vírus**

A program that can ‘infect’ other programs by modifying them to include a possibly evolved copy of itself. [Fred Cohen, 1983]

# No ale fakt. . . čo sú vírusy?

**Vírus**

A program that can ‘infect’ other programs by modifying them to include a possibly evolved copy of itself. [Fred Cohen, 1983]

Ale keďže slovo “vírus” sa skloňovalo až príliš často v médiach, stratilo svoj pôvodný význam a dnes znamená “skoro čokoľvek”.

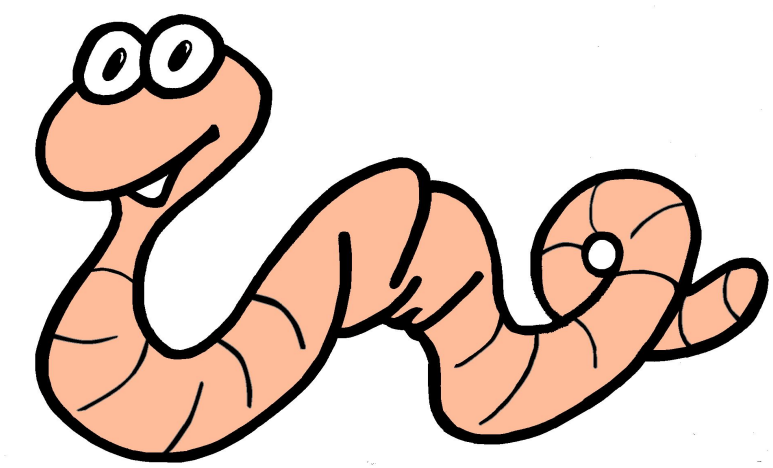
# Vírus $\subsetneq$ Škodlivý program

- Existuje veľa kritérii pre klasifikáciu škodlivého softvéru.
- Môžeme sa pozrieť na funkcionalitu – backdoory, rootkity, adware, spyware, keyloggery, downloadery, ...
- Alebo nás môžu zaujímať metódy šírenia sa – vírusy, drive-by downloady, USB červy, ...
- Platforma? Pôvod?

# Parazitické vírusy

- Najstarší druh hávede.
- Infikuje existujúce súbory, *parazituje* na nich; sám o sebe neexistuje.
- Zvyčajne sa aktívne šíri v rámci jedného počítača.
- Ak máme šťastie, dá sa zo súboru “vyčistiť”.
- V súčasnosti skoro vymierajúci druh – výnimky ako Virut a Sality.

# Sieťový červ



- Šíri sa cez sieť (zdieľané adresáre, slabé heslá, chyby, ...).
- Vo väčšine prípadov sú jednotlivé inštancie nezávislé – aj keď občas dokázali aj spolupracovať.
- Čistenie = odstránenie = zmazanie.

# Trójsky kôň

- Všeobecný termín pre program, ktorý okrem deklarovanej funkcie robí aj čosi navyše.
- Sám sa nešíri.
- Čistenie = zmazanie.
- Veľakrát sa dá detegovať obyčajným hashom.

# Bot(net)

- (Ro)bot – program počúvajúci príkazy.
- Botnet – sieť botov.
- Dajú sa ľahko kontrolovať a obchodovať.

# Bot(net)

- (Ro)bot – program počúvajúci príkazy.
- Botnet – sieť botov.
- Dajú sa ľahko kontrolovať a obchodovať.

1. Robot nesmie ublížiť človeku, ani svojou nečinnosťou umožniť, aby bolo človeku ublížené.
2. Robot musí splniť príkazy zadané človekom, pokiaľ nie sú v rozpore s prvým zákonom.
3. Robot musí chrániť svoju existenciu, pokiaľ takáto ochrana neodporuje prvému alebo druhému zákonu.

# IRC C&C

```
DUPX 190.43.70.226 PrivateIRCD.TeRRoR.Net IGBVN H :0 FEPKC
ESYLDU 190.42.56.252 PrivateIRCD.TeRRoR.Net FUEVXU H :0 AAIOHR
NHONCPXM 190.232.27.109 PrivateIRCD.TeRRoR.Net SGJOVLYW H :0 ULKCVB
DYYUIKB 190.43.149.9 PrivateIRCD.TeRRoR.Net OUONVA H :0 BLNFYI
VSYEWWSN 190.254.135.189 PrivateIRCD.TeRRoR.Net CYOCEUM H :0 YAZDF
BGRYSJ 190.42.251.4 PrivateIRCD.TeRRoR.Net PEOM H :0 JHHEO
MDUE 186.114.22.8 PrivateIRCD.TeRRoR.Net PLPWV H :0 LDUCU
BENTJCNI 190.236.172.70 PrivateIRCD.TeRRoR.Net OUZF H :0 KKULMJDY
KQBMUXJ 186.112.100.250 PrivateIRCD.TeRRoR.Net KDEFFJ H :0 GTRLSIX
APOKVA 186.113.200.75 PrivateIRCD.TeRRoR.Net INTLPL H :0 ZIWWSBC
```

# Suma sumárum

Škodlivého softvéru je veľa druhov a v súčasnosti už ostrá hranica neexistuje.

# Skadiaľ to všetko pochádza?

- Klasické – diskety, CD
- Neoklasické – e-mail, stránky so “zaujímavým” obsahom, bundle, . . .
- Moderný prístup – ICQ, IRC, AIM, USB kľúče, P2P, sociálne siete, drive-by downloady, cielené kampane, . . .

```
05.03.07 21:30:51 * Authorization request : Privet
tu HOTEL DENEG TAK ZABIRAY
http://ppc.moy.su/dengi.exe

http://ppc.moy.su/dengi.exe
05.03.07 21:31:06 Privet tu HOTEL DENEG TAK ZABIRAY
http://ppc.moy.su/dengi.exe

http://ppc.moy.su/dengi.exe
```

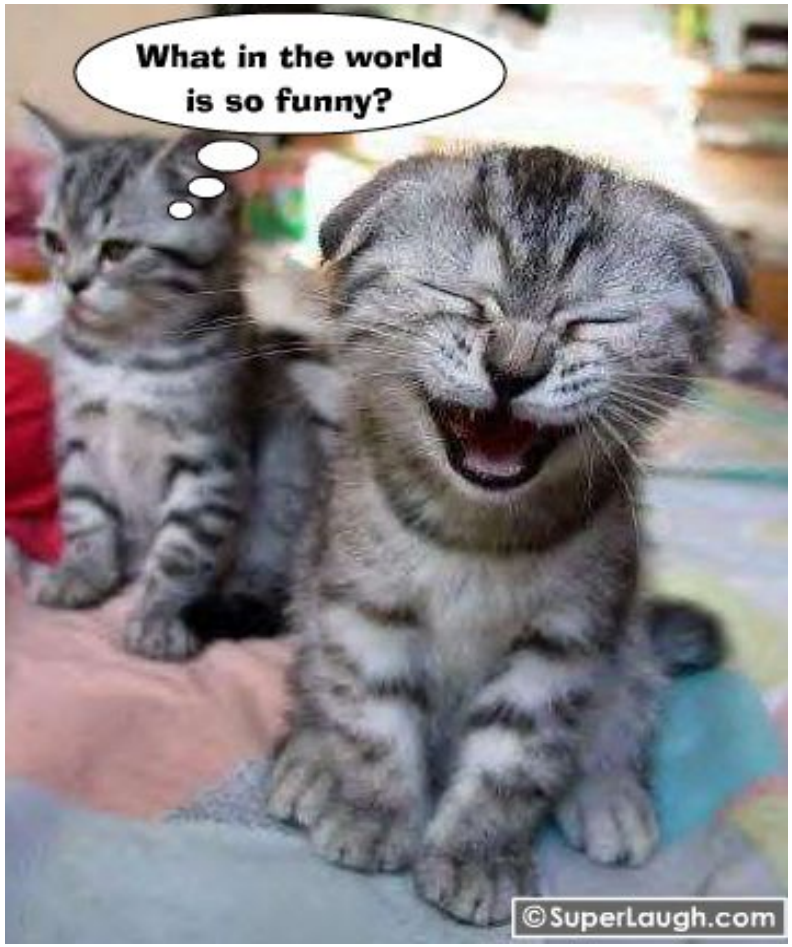
# E-mail

From: illegal@fbi.gov
To: helmut@sajrajt.von
Subject: Illegal content
Date: Fri, 1 Apr 2011 03:13:37 +0200

You have been downloading illegal content!
See the attached list for details.

Attachment: server_logs.txt .exe

# Pekné stránky



# Čo môže byť škodlivé?

- Klasicky to boli spustiteľné súbory (.exe, .com, .bat, . . . )
- Nová platforma – Dokumenty (makrá), skriptovacie jazyky (JS, VBS, . . . )
- Moderný prístup – obrázky, Flash, Java; skrátka takmer všetko a ešte trochu viac.

# Prečo je vôbec nejaký škodlivý softvér?

Staré zlaté časy:

- Demonštrácia schopností, sláva, patriotizmus, ...
- Vyššia konštruktívnosť autorov (ale aj vyššia deštruktívnosť ich tvorby).
- Žiaden priamy zisk (iba ak dobrý pocit).

# Prečo je vôbec nejaký škodlivý softvér?

Staré zlaté časy:

- Demonštrácia schopností, sláva, patriotizmus, ...
- Vyššia konštruktívnosť autorov (ale aj vyššia deštruktívnosť ich tvorby).
- Žiaden priamy zisk (iba ak dobrý pocit).

Dnes:

- D o l á r
- E u r o
- L i b r a
- **Z I S K !**

# Stará háveď

- Zábavné akcie – padajúce písmenká, húsenice, sanitky, ...
- Deštrukcia – synchronizácia disku, zmazávanie súborov, pomalé zmeny, ...
- Pokusy o výkupné – vyhraj alebo zaplať, ak chceš svoje dáta!

# Súčasnosť

- Kradnú informácie, ktoré sa dajú speňažiť – CC#, meno/heslo k Internet bankingu, MMO kontá, . . .
- Lákajú obete na kúpu (potenciálne) falošných produktov.
- Berú zajatcov – dáta, siete, . . .

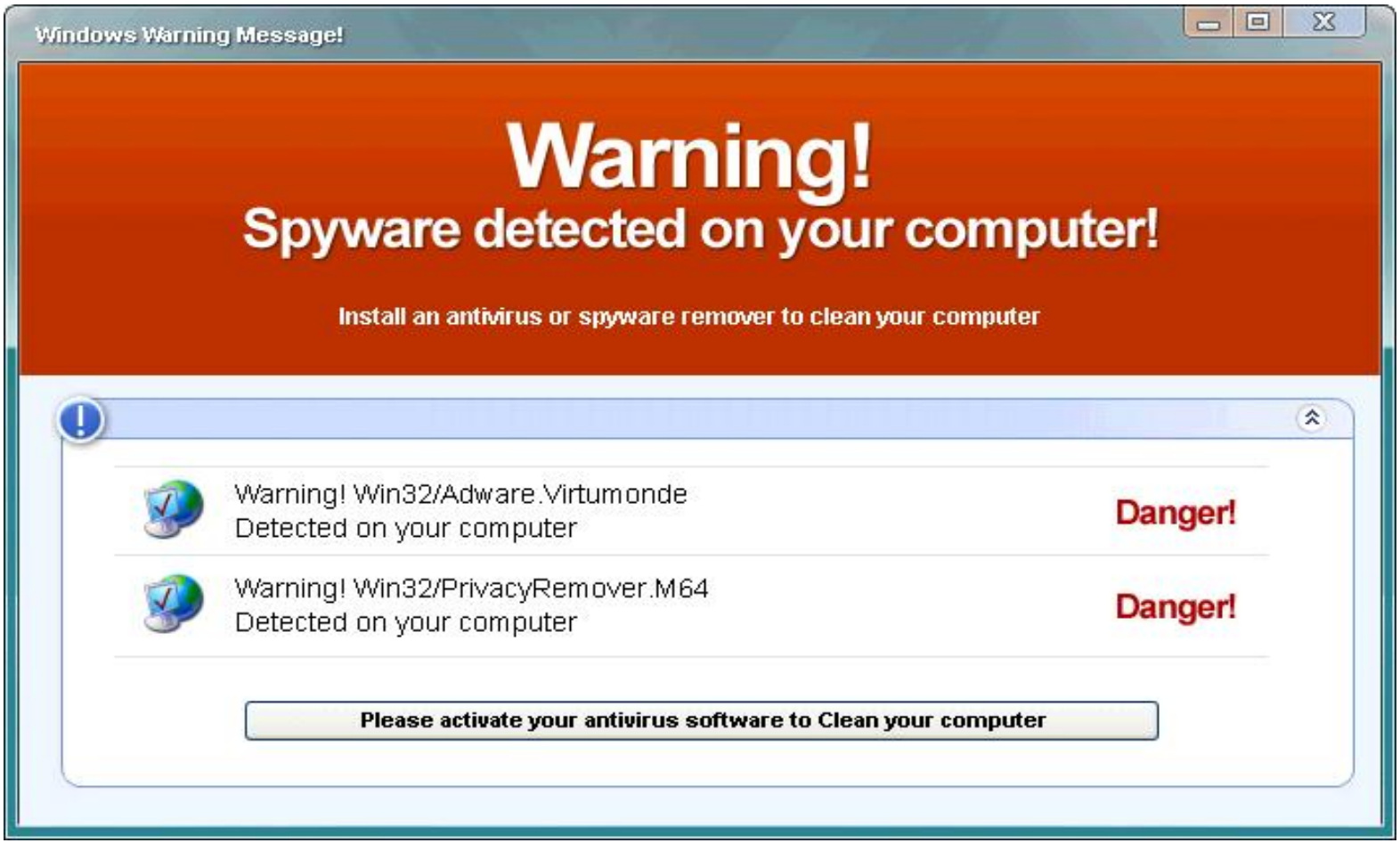
# Spam


PREMIER PHARMACY
• Lowest VIAGRA, CIALIS,
VIAGRA 30 $134.95
CIALIS 30 $169.95
VALIUM 30 $85.45
SOMA 30 $75.95
PROPECIA 30 $64.95
AMBIEN 30
• XANAX 30 $123.45
VIAGRA SOFT 50 $250.99
✓New CIALIS SOFT 30 $224.95
up to 80% on your prescription Meds!
6RX.ORG
Do not click, type in your browser

# Spam

- Obyčajne posielajú napadnuté počítače.
- Poslať tony spamu = lacné.
- Aj malé percento odpovedí = zisk.

# Falošné antivírusy



# Strach & výkupné

# Adware

- Ako zarobiť na reklame.
- Zvyčajne inštalované so “súhlasom” užívateľa = právne problémy.
- Zvyčajne sú vnímané ako “neškodné”, a občas dokonca “žiadané”.
- Občas skutočne nevinné, ale zďaleka nie vždy.

# Spyware

- Zber dát bez toho, aby o tom užívateľ skutočne vedel.
- Tiež v zásade “ok”.

# Spyware

- Zber dát bez toho, aby o tom užívateľ skutočne vedel.
- Tiež v zásade “ok”.
- Však koho zaujímajú stránky, po ktorých chodíme?
- A čo takto výška bankového konta?
- Alebo napríklad zoznam kamarátov na ICQ?

# Spyware

- Zber dát bez toho, aby o tom užívateľ skutočne vedel.
- Tiež v zásade “ok”.
- Však koho zaujímajú stránky, po ktorých chodíme?
- A čo takto výška bankového konta?
- Alebo napríklad zoznam kamarátov na ICQ?
- A čo ak ide o šéfa nadnárodnej spoločnosti?

# Manažment rizika

Riziko sa nesmie podceniť. . . ale preháňanie môže byť rovnako zlé. Médiam netreba veľa na to, aby spravili z komára somára (a naopak).

# Conficker

- Koniec sveta sa blíži! Deň ustúpi pred nocou a po oblohe budú lietať mačky na fúrikoch!. . .
- Ani svetoví experti netušia, čo sa stane! Zachráň sa, kto môžeš!
- To všetko nastane prvého apríla 2009.

# Conficker

- Koniec sveta sa blíži! Deň ustúpi pred nocou a po oblohe budú lietať mačky na fúrikoch!. . .
- Ani svetoví experti netušia, čo sa stane! Zachráň sa, kto môžeš!
- To všetko nastane prvého apríla 2009.
- Syndróm Michelangelo ’92.
- Nič významné sa nestalo, len malá zmena v kóde červa.
- Samozrejme, niečo by sa stať *MOHLO*, dnes, zajtra, o týždeň, . . . alebo aj nikdy.

Háveď je poháňaná peniazmi $\Rightarrow$ Tak skoro nezmizne.

# Dobrá rada nad zlato. . . alebo nie?

Dobrých rád existuje veľa, ale občas môžu narobiť viac škody ako úžitku.

- Neotvárajte e-maily od neznámych!
- Ak zistíš, že známy má nakazený počítač, upozorni ho na to!
- Keď sa dozvieš o probléme, daj vedieť aj ostatným!
- Používaj antivírus, firewall, antispyware, antiphishing, anti-toto, anti-tamto, . . .

# Treba čističa?

# Antivírus

- NEVYRIEŠI všetky problémy.
- Je len JEDNOU z obranných línii (a potenciálne ďalšou zraniteľnosťou!)
- NESMIE vládnuť užívateľovi.
- Ale VIE označiť veľmi veľkú časť škodĺivých programov ako zlé.

# Často kladené otázky a mýty

- Koľko vírusov chytá váš antivírus?
- Chytá aj háveď XYZ? Čo tá háveď robí?
- Odkedy mám tento antivírus, nemal som ani jedno varovanie o hávedi!
- Používam Linux/BSD/MacOS, háveď sa ma netýka.

# Ako to funguje vnútri?

Pozrime sa dovnútra antivírusu.

# Ako to funguje?

Staré vírusy boli jednoduché:

> Pozri sa na posledných 7 bajtov súboru.
> Je tam reťazec "sUMsDos"?
> Ak áno, ohlás vírus Jerusalem.

alebo

> Pozri sa na posledných 4096 bajtov súboru.
> Obsahujú reťazec "Dark Avenger"?
> Ak áno, ohlás vírus Dark Avenger.

# Ako to spraviť efektívnejšie?

- Jediný rozdiel je v reťazci, dĺžke a umiestnení.
- Spoločná časť detekcie bude kód, zvyšok bude “vzorka”.
- V širšom zmysle vzorkou môže byť skoro čokoľvek, nie len postupnosť bajtov niekde z tela hávede.

# Rôzne AV = rôzne vzorky

- Vzorky neboli rovnaké ani dávnych časoch, nieto ešte dnes.

  NIEčo, NIEkto, NIEmand, . . .

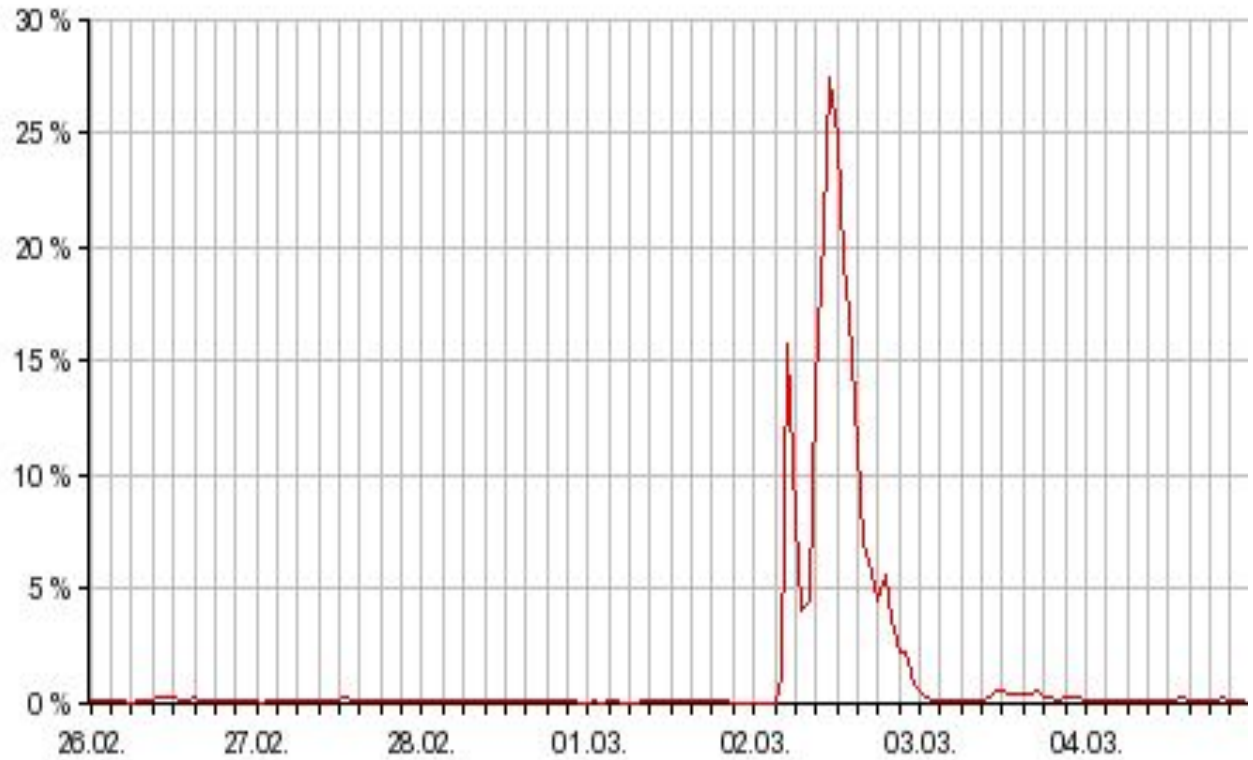
  nieČO, hociČO, voľaČO, . . .
- Počet vzoriek v databáze nehovorí nič o kvalite AV.
- Mená sa líšia od AV k AV, nedajú sa porovnávať.

# Menej exaktnej vedy, viac štatistiky

- Heuristické metódy – zamerané na typické vlastnosti hávede.
- “Vlastnosť” môže byť skoro čokoľvek – veľkosť, packer, knižnice, . . .
- Vyššia pravdepodobnosť nekorektnej klasifikácie – false positive.
- Nedá sa presne opísať, čo takto detegovaná háveď robí.

# Outbreak

Kolaboratívne metódy + cloud – ak je toho naraz veľa, je to čudné.



# Reaktívne vs. proaktívne

- Reaktívne = “po”, poznajúc nepriateľa.
  Podstatný je čas odozvy.
- Proactive = “pred”, boj s neznámom.
  Teoreticky nulový čas odozvy.

# Reaktívne vs. proaktívne

- Reaktívne = “po”, poznajúc nepriateľa.
  Podstatný je čas odozvy.
- Proactive = “pred”, boj s neznámom.
  Teoreticky nulový čas odozvy.
- Čo ak autori hávede začnú byť tiež proaktívni?

# Reaktívne vs. proaktívne

- Reaktívne = “po”, poznajúc nepriateľa.
  Podstatný je čas odozvy.
- Proactive = “pred”, boj s neznámom.
  Teoreticky nulový čas odozvy.
- Čo ak autori hávede začnú byť tiež proaktívni?
- Oni už dávno sú.

# Cielené útoky

- Ak útočník pozná vaše obranné prostriedky, môže sa na ne adaptovať.
- Jediná šanca je odstrašiť ho tak, aby sa venoval niekomu inému.
- Obrana by mala pozostávať z viacerých vrstiev.
- Heterogenita môže, ale nemusí pomôcť.

# Ako si vybrať ten pravý?

Takmer všetky AV majú podobné základné nápady, implementačne sa ale líšia. Ako vybrať ten najlepší?

# Ľahký prístup

Stačí vybrať ten, čo pochytá najviac!

1. Zozbieraj čo najviac škodlivých súborov.
2. Spusť na ne všetky testované AV.
3. Usporiadaj výsledky podľa počtu chytaných súborov.

Jednoduché a účinné, nie?

# Zozbieraj čo najviac škodlivých súborov...

Ľahšie povedať, ako spraviť.

- Je ich dosť?
- Sú reprezentatívnou vzorkou?
- Je to iba háveď?

# Zozbieraj čo najviac škodlivých súborov...

Ľahšie povedať, ako spraviť.

- Je ich dosť? Ľahké!
- Sú reprezentatívnou vzorkou? Ťažšie.
- Je to iba háveď? ŤAŽKÉ!

# Reprezentatívne?

Pozrime sa opäť na vzorky:

AV1: NIE detekcia.

AV2: ČO detekcia.

Sada 1 { NIEČO, NIEkto, NIEmand } $\Rightarrow$ AV1 vyhral!

Sada 2 { NIEČO, voľaČO, hociČO } $\Rightarrow$ AV2 vyhral!

- Špeciálne viditeľné, pokiaľ testovacia sada bola deduplikovaná použitím jedného konkrétneho produktu.
- Reprezentuje to vlastne reálny svet?
- Možno by pomohol Satoshi?

# Reprezentatívne?

Pozrime sa opäť na vzorky:

AV1: NIE detekcia.

AV2: ČO detekcia.

Sada 1 { NIEČO, NIEkto, NIEmand } $\Rightarrow$ AV1 vyhral!

Sada 2 { NIEČO, voľaČO, hociČO } $\Rightarrow$ AV2 vyhral!

- Špeciálne viditeľné, pokiaľ testovacia sada bola deduplikovaná použitím jedného konkrétneho produktu.
- Reprezentuje to vlastne reálny svet?
- Možno by pomohol Satoshi? Ash Ketchum

# Len háveď?

- Ešte ťažšie!
- Vec presnej definície – veľa hávede je blízko hranice.
- Obrovské množstvá dát na spracovanie (desiatky miliónov súborov).
- Iba čiastočne rozhodnuteľný problém, a aj to len v najmiernejšej verzii.
- Jednoduchý nápad – prebehneme všetko testovanými AV a to, čo niekto chytí je zlé.

# Gratulujeme!

The Perfect Antivirus od Dr. Alana Solomona práve vo vašom teste vyhral!

# Gratulujeme!

The Perfect Antivirus od Dr. Alana Solomona práve vo vašom teste vyhral! A vy ste spravili kvalitný FAIL.

# Falošné poplachy nemožno ignorovať

- False negative = zločinec na slobode
- False positive = nevinný vo väzení
- Čo je dôležitejšie pre *VÁS*?

# Sumár

Programovanie antivírusov je ľahšie ako ich testovanie.

# To je už fakt všetko!

Ďakujem za pozornosť! Ak sú nejaké otázky, nebojte sa spýtať teraz[1].

[1] Máte tiež právo mlčať, ale potom vaše otázky zrejme nezodpoviem.