

SECURITY 2011

19. ročník konference o bezpečnost v ICT

Malware v České republice

Ondřej Novotný

AVG Technologies CZ, s.r.o.





Obsah

- Malware obecně
 - Malware - definice
 - Prohlížeč - vstupní brána malware
 - Klíče k bráně - exploit toolkity

- Malware v České republice
 - Specifika prostředí
 - Statistika
 - Jak to vidí český uživatel

- Jak se bránit



Malware - definice

- **Malware** - **MAL**icious soft**WARE**
 - Exploity
 - Spyware
 - Keyloggery
 - Downloadery, Dropery
 - Wormy
 - Adware
 - Viry (infektory)



Prohlížeč – distribuční kanály

- Společenské sítě (Facebook, Twitter atd.)
- Kompromitace důvěryhodných stránek
- “Otrávené” výsledky vyhledávačů
- Phishing (rhybaření)



Prohlížeč - zranitelnosti

Cesta k nenápadné infekci počítače malwarem:

- Chyba v prohlížeči samotném
- Chyba v některém z doplňků:
 - Sun JVM
 - Adobe Acrobat Reader
 - Flash Player
 - Quick Time
 - Real Player



Klíče k bráně - exploit toolkity

■ Exploit Toolkit

- Sada exploitů pro infekci klienta
- Rozhraní pro řízení a monitoring infikovaných strojů

■ Exploit Toolkity

- | | | |
|------------|-------------|--------------|
| ■ Phoenix | ■ Crimepack | ■ Siberia |
| ■ Eleonore | ■ Seosploit | ■ GromSploit |
| ■ Liberty | ■ Fragus | ■ Gpack |

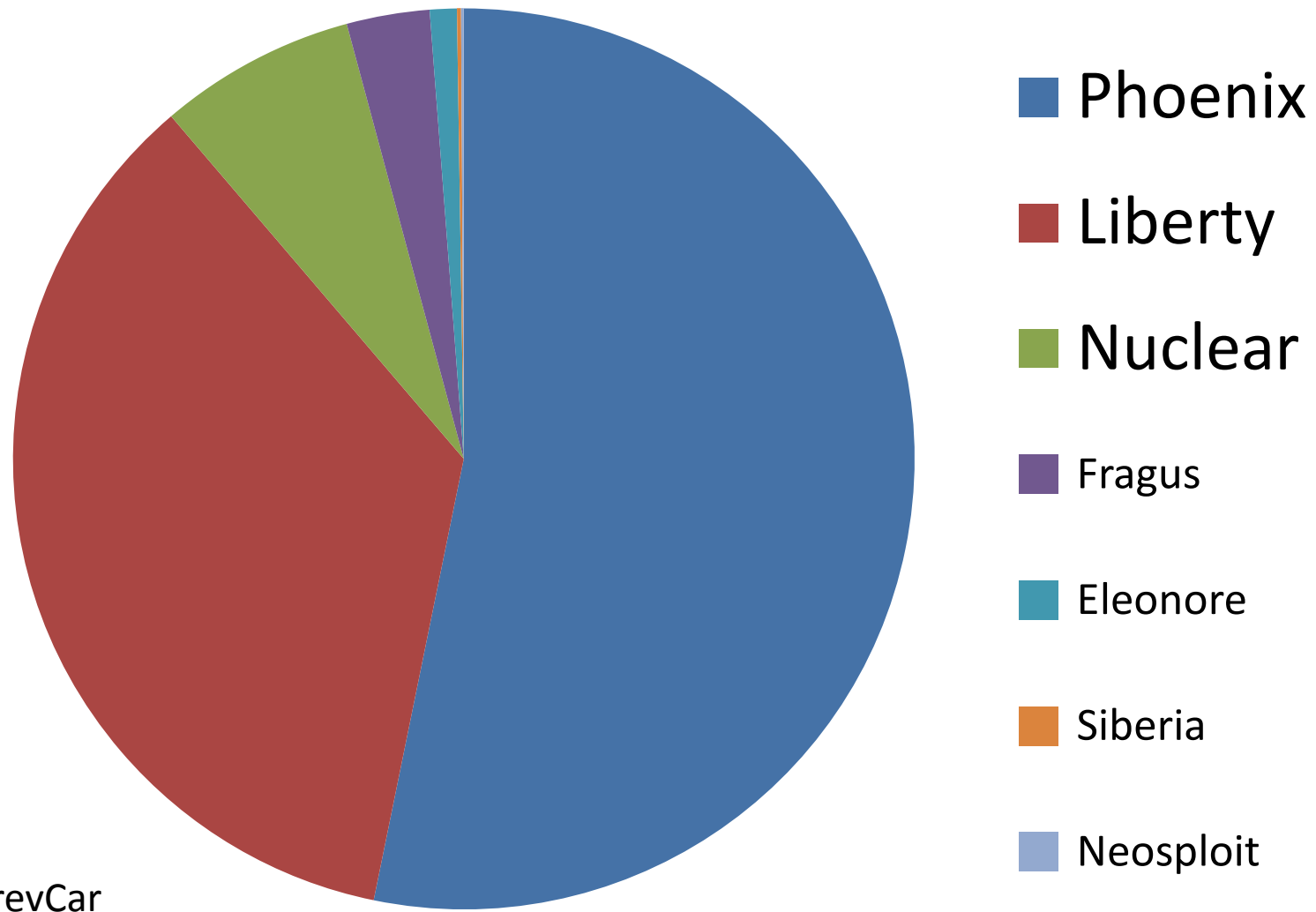


Malware v České republice

- Malware nezná hranice
- Česká republika není hlavním cílem malware
- Specifika českého prostředí
 - Velikost českého trhu a finanční výnosnost
 - Jazyková bariéra (sociální inženýrství)



Statistika - Exploit toolkity

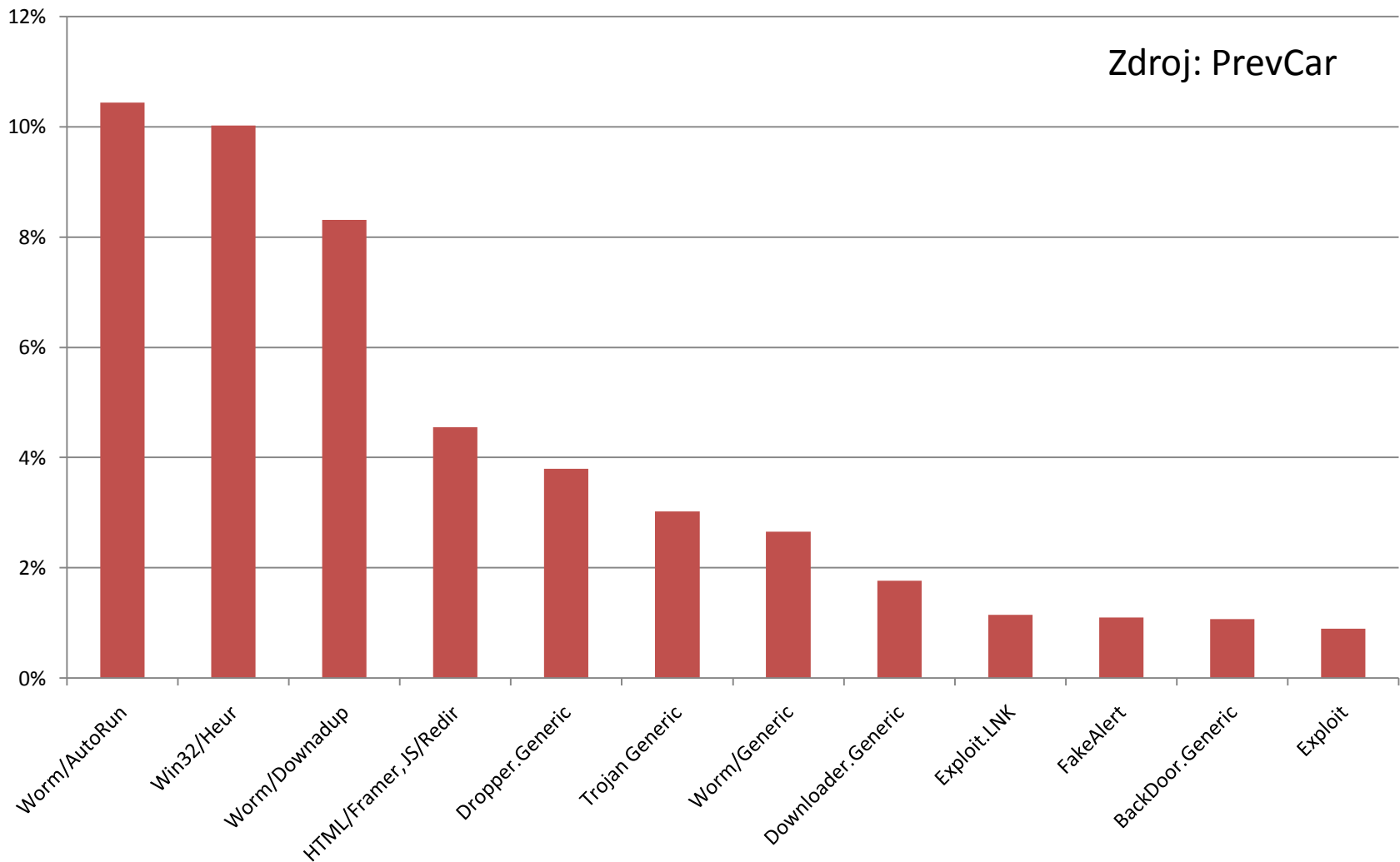


Zdroj: PrevCar

16. února 2011

SECURITY 2011

Statistika - Malware





Jak to vidí uživatel

Mně jako normálnímu uživateli PC je to naprosto jedno... Musela by to být sakra náhoda aby se to stalo zrovna někomu z nás.

Zdroj: Novinky.cz (diskuse)

Clanok je jasna inzercia - za 5 rokov studia informatiky som totiz nikdy nepocul o "infikovanej stranke"... a to sme mali i par predmetov z informacnej bezpecnosti.

Zdroj: Digiweb (diskuse)



Jak to vidí uživatel – falešný antivirus





Jak to vidí uživatel – copyright fraud

Upozornění na porušení autorských práv

**Porušení autorských práv: byl nalezen materiál porušující autorská práva**

Systém Windows zjistil, že používáte obsah, jehož stáhnutím byla porušena autorská práva právoplatných držitelů. Prosím, přečtěte si následující informace a pokuste se vyřešit tento problém jedním z doporučených způsobů.

Czech

Co se stalo?

Během prohlídky objevil skener Protipirátské organizace problémy s autorskými právy. Prosím, prohlédněte si seznam a vyberte si další postup: předání případu soudu nebo urovnání sporu zaplacením pokuty v předběžném líčení.

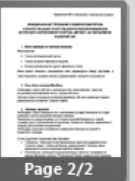
Jak se to mohlo stát?

Zřejmě jste používali programy na sdílení obsahu, torrenty nebo jste materiál stáhli přímo z webových stránek. Ať už šlo o jakoukoli možnost, porušili jste autorská práva příslušných vlastníků. Ve většině zemí podléhá tato činnost soudnímu stíhání a jsou za ni udělovány vysoké tresty. Horní hranice trestu je až pět let vězení a pokuta činí až 200 000\$.

Nalezené soubory

Přehled soudních sporů

**Page 1/2**

**Page 2/2**

**Projekt organizace ICPP**

**Soupis důkazů**

[Show details...](#)

**Použité IP logy**

0.0.0.0
0.0.0.0
0.0.0.0

Typ porušení

p2p\warez movie download
p2p\warez games download
p2p\warez mp3 download

Protipirátské novinky

12/02/2010
[Byla přijata nová protipirátská opatření proti nelegálnímu obsahu](#)

26/12/2009
[Aktualizace protipirátské aplikace: Stáhněte si verzi 2.0 a zkontrolujte, jestli Váš počítač neobsahuje nelegální obsah nebo spyware \(např. hudbu a videa\)](#)

Vyberte si postup

Pokud jste si jisti, že jste nemohli stáhnout zmíněný obsah do Vašeho počítače nebo jste nemohli udělat nic proto, abyste tomu zabránili, klikněte na tlačítko „Předat případ soudu“ a případ bude předán soudu.

Pokud tyto soubory patří Vám, ale chcete se vyhnout všem nákladům spojeným se soudním jednáním, můžete urovnat spor v předběžném líčení kliknutím na tlačítko „Vyrovnání...“.

Předat případ soudu**Urovnat spor v předběžném líčení**

[Enter a previously purchased license code](#)

<http://icpp-online.com/> - váš zdroj iniciativy pro ochranu autorského práva



Násilným ukončením této aplikace nebo vypnutím počítače dojde ke ztrátě všech dat na disku.

Zašlete SMS s textem GP 1379464

na číslo: 900 09 99

Následně obdržíte kód který napíšete do rámečku níže.

Kód: OK

Pokud kód nezadáte do 15 minut dojde k odstranění všech dat na disku !!!

Zbývající čas: 14 minut 33 sekund



Jak to vidí uživatel - lockscreen

Byl/a jste vybrán/a aby jste se mohli/a zúčastnit soutěže o zbrusu nový iPhone



Pro účast v této soutěži postupujte následovně:

**Zašlete SMS s textem GURU A593D2
na číslo: 9030999**

Zbývající čas: **14** minut **50** sekund

Tip: Po zaslání soutěžní SMS se tato aplikace sama odstraní z počítače !!!



Jak to vidí uživatel – IQ test

Pokračujte v řadách těchto písmen nebo čísel
písmenem nebo číslem, které logicky následuje.

cas:0m34s

1, 3, 6, 10, ..



- | | |
|----|----|
| 1 | 18 |
| 2 | 19 |
| 3 | 20 |
| 4 | 21 |
| 5 | 22 |
| 6 | 23 |
| 7 | 24 |
| 8 | 25 |
| 9 | 26 |
| 10 | 27 |
| 11 | 28 |
| 12 | 29 |

- 30
31
32
33

KONEC

--->>>

Write to file "C:\WINDOWS\system32\DRIVERS\Mstart.sys"

Copy file "c:\WORK\MSTART.SYS" to "C:\WINDOWS\system32\Drivers\MSTART.SYS"

Copy file "c:\WORK\test.exe" to "C:\WINDOWS\system32\tokset.dll"

Write to file "C:\WINDOWS\system32\ainf.inf"

---<<<



Jak to vidí uživatel

- Vyskakují okna v prohlížeči
- Varování falešných AV
- Zpomalený internet
- Zpomalené PC
- Nelze otevřít Windows Security Center, spustit Správce úloh, Editor registrů
- Přesměrování prohlížeče při pokusu navštívit stránky AV firem



Jak se bránit...

- Před tím než kliknete...
 - Vyhledávač – filtrace maligních výsledků
 - AV software – ohodnocení výsledků hledání, antispam, antiphishing
 - Znalosti a zdravý rozum uživatele

- Kliknul jsem...
 - Blokace přístupu prohlížečem samotným
 - Aktualizovaný prohlížeč, pluginy a operační systém
 - AV software - kontrola stahovaného obsahu, rezidentní ochrana, behaviorální analýza...

SECURITY 2011

19. ročník konference o bezpečnost v ICT

Děkuji za pozornost.

Ondřej Novotný
AVG Technologies CZ
ondrej.novotny@avg.com

