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 - MALicious softWARE**
  - 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

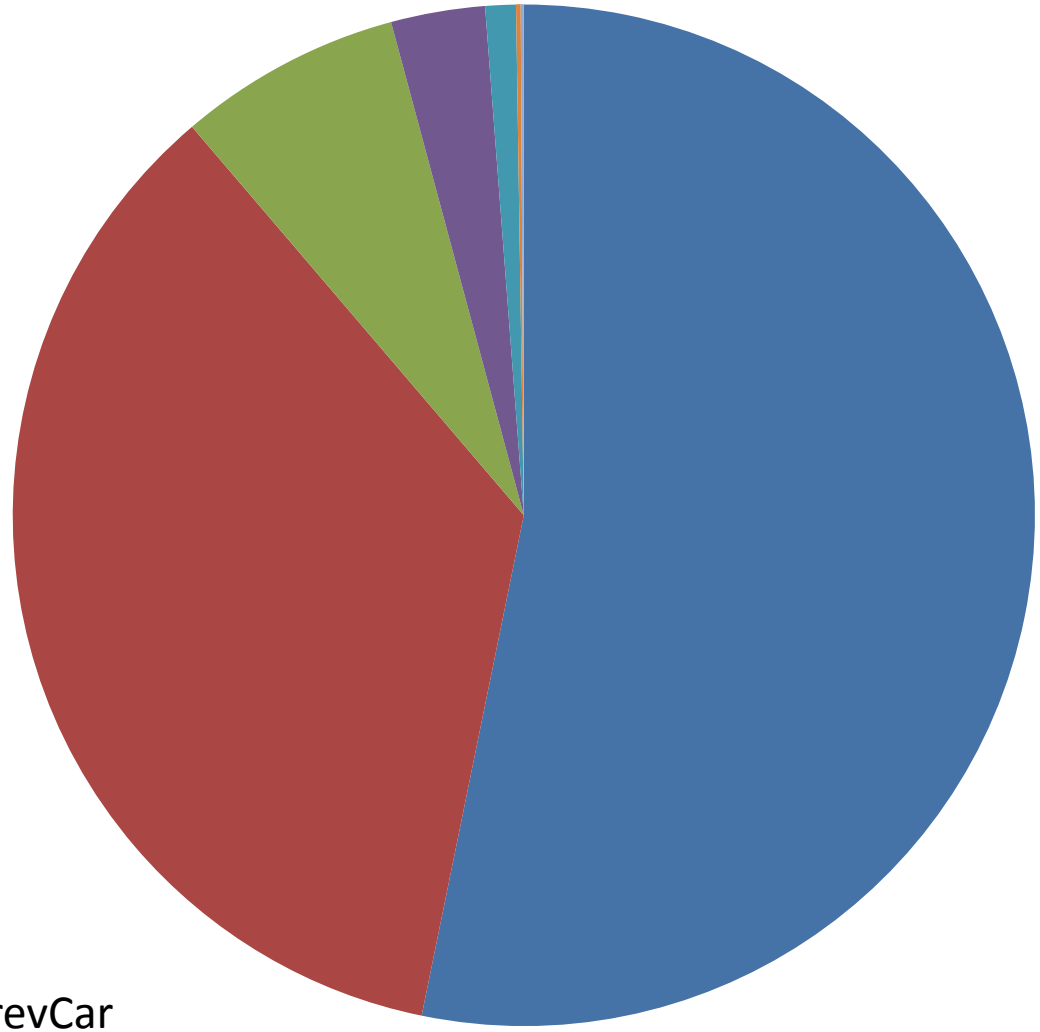
- Exploit Toolkit
  - Sada exploitů pro infekci klienta
  - Rozhraní pro řízení a monitoring infikovaných strojů

- Exploit Toolkity
  - Phoenix
  - Eleonore
  - Liberty
  - Crimepack
  - Seosploit
  - Fragus
  - Siberia
  - GromSploit
  - Gpack

Malware v České republice

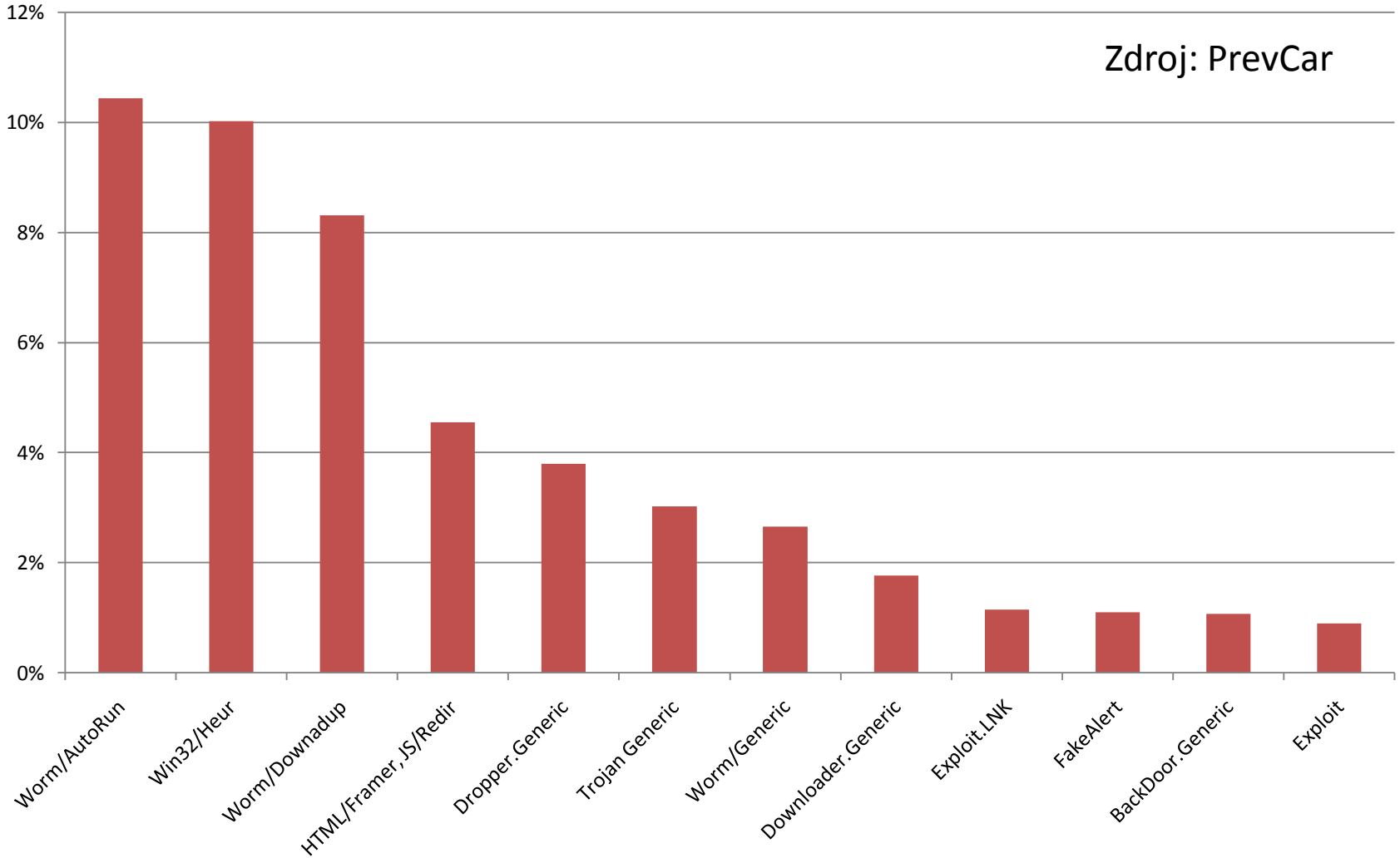
- Malware nezná hranice
- Česká republika není hlavním cílem malware
- Specifika českého prostředí
  - Velikost českého trhu a finanční výnosnost
  - Jazyková bariéra (sociální inženýrství)

Statistika - Exploit toolkity



Zdroj: PrevCar

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.

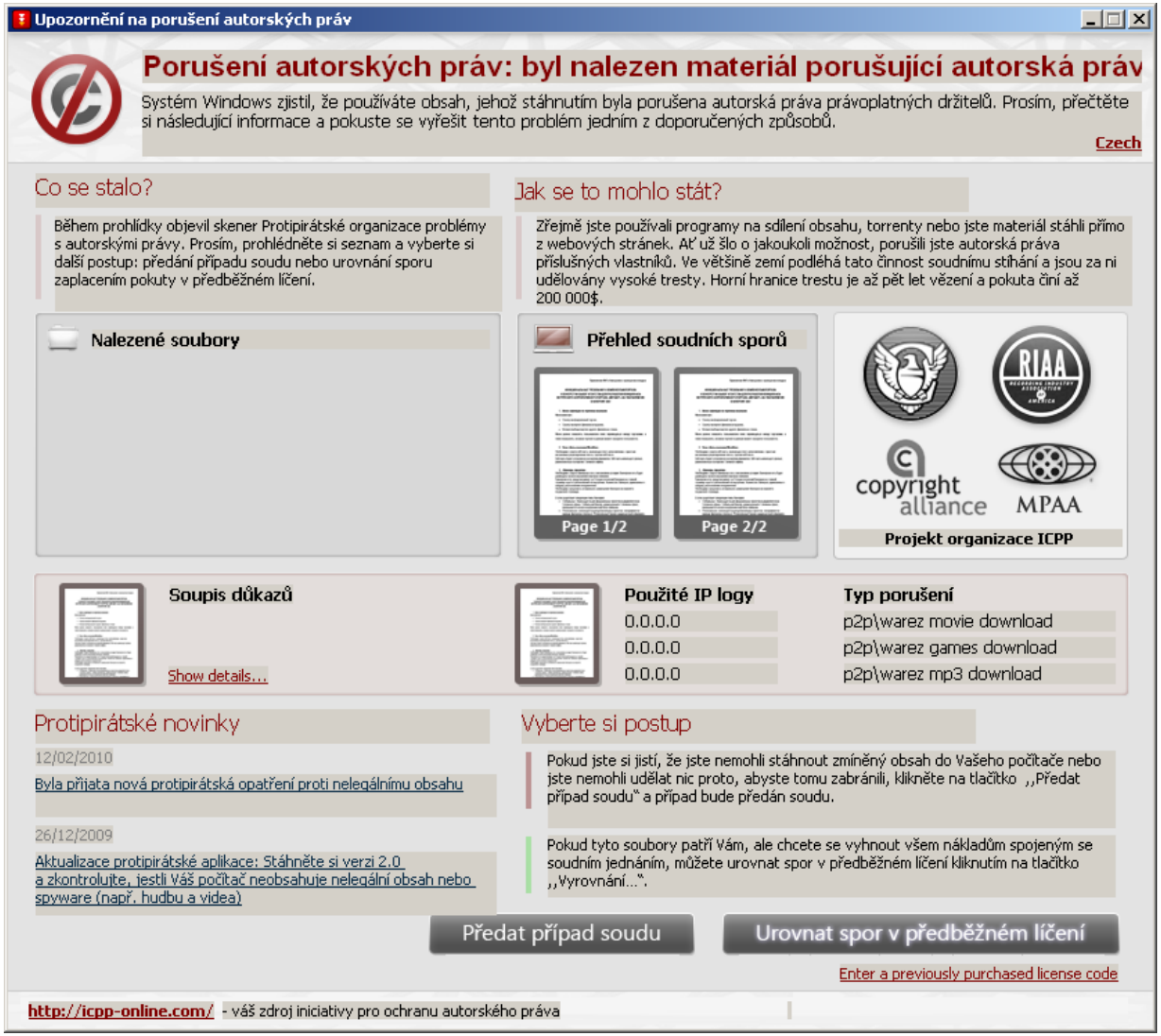
Zdroj: Novinky.cz (diskuse)

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.

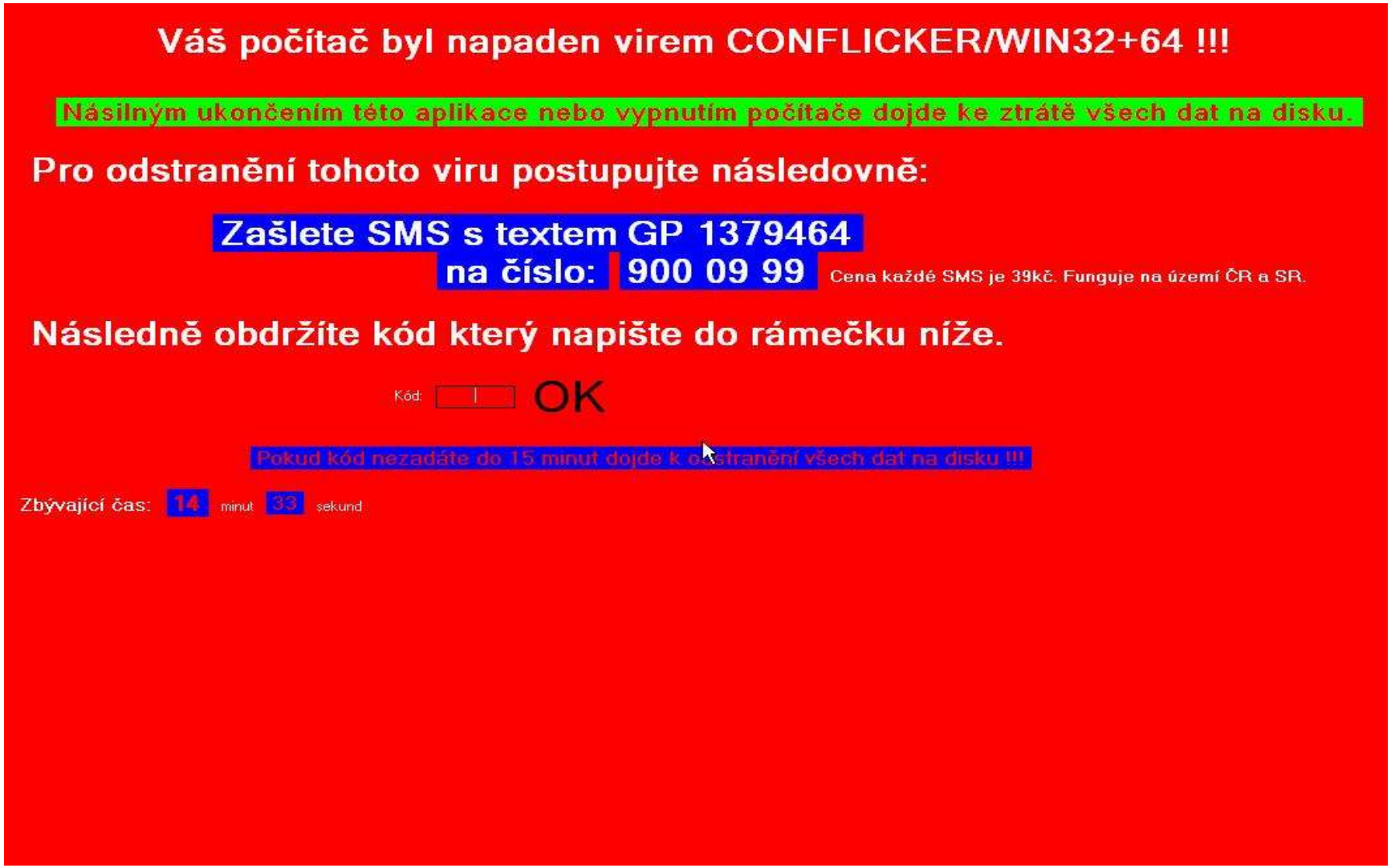
Zdroj: Digiweb (diskuse)

Jak to vidí uživatel – falešný antivirus

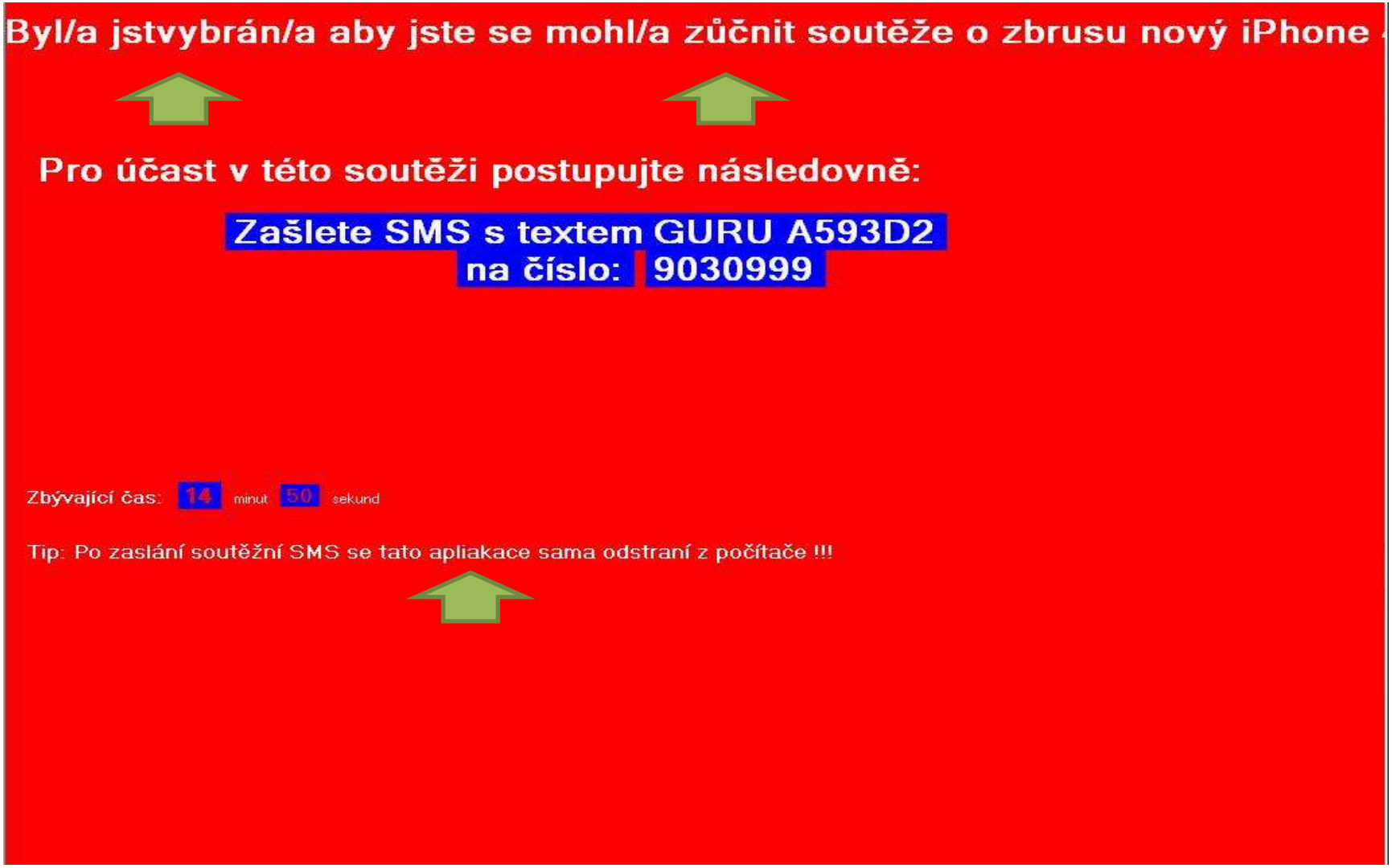
Jak to vidí uživatel – copyright fraud



Jak to vidí uživatel - lockscreen



Jak to vidí uživatel - lockscreen



Jak to vidí uživatel – IQ test

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