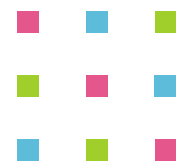
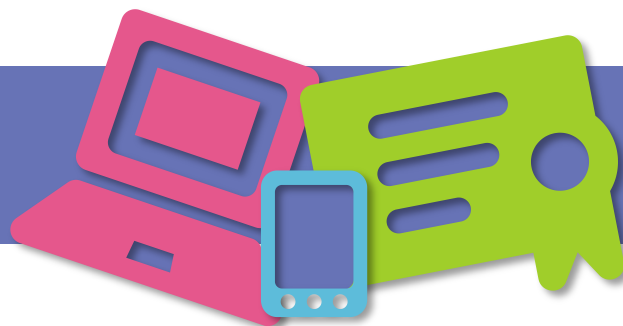


SECURITY 2014



22. ročník konference o bezpečnosti v ICT



Malware v roce 2013 – lépe už bylo

Petr Šnajdr

ESET software spol. s r.o.



Agenda

- Rok 2013 v číslech
- Nejzajímavější kousky malware
- Svět na sociálních sítích
- Mobilní malware
- Budoucnost antivirů
- Dotazy / Diskuze



Rok 2013 v číslech

- Využívání sociálního inženýrství
- Ransomware
- Cryptolocker (Filecoder)
- Win32/Hesperbot
- 200 000 – 250 000 nových vzorků malware každý den
- Nárůst vzorků mobilního malware



Vzorky malware 2013

Hesperbot
Filecoder malware Ransomware Filecode

-





Win32/Filecoder - Cryptolocker

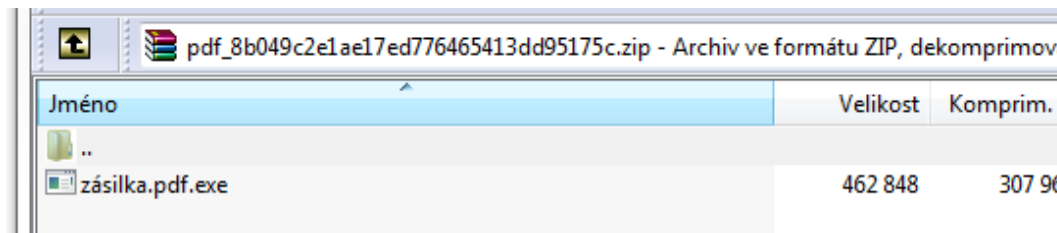
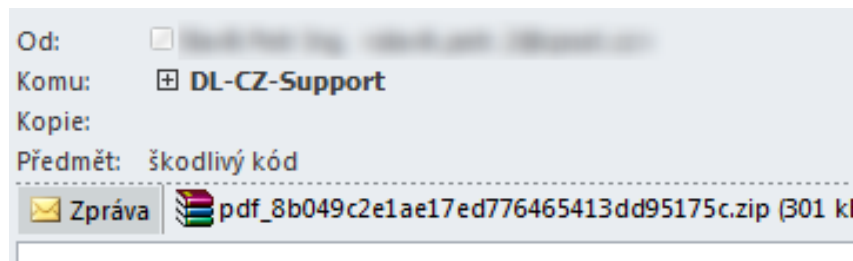
- Šifrování disku (2048bit RSA)
- 1,4% vzorků malware je BITCOIN RELATED!





Win32/Hesperbot

- Phishing zneužívající Českou Poštu k distribuci bankovního trojana
- *www.ceskaposta.net (czpost.com, cz-post.org)*
- Malware v příloze emailu
- Krádeže informací
- Screenshoty obrazovky
- Skrytý VNC server
- WebInject



Win32/Hesperbot

The screenshot displays the Czech Post (Česká pošta) website interface. At the top, there is a navigation bar with the logo and contact information. Below this, a blue banner advertises 'UŽITEČNÉ NÁSTROJE A NÁVODY' (Useful tools and instructions) for tracking parcels. The main content area is titled 'Sledování zásilek (Track&Trace)' and includes a search bar with the number '853833' entered. To the right, there is a 'Klientská zóna' (Client zone) with links for registration and services. At the bottom, a footer contains copyright information and additional links.

Česká pošta Zákaznická linka: 840 111 244 [English](#)

[Úvodní stránka](#) | [O České poště](#) | [Kariéra](#) | [Kontakty](#)

Občané a domácnosti **Firmy a podnikatelé** **Korporace a velké firmy**

Vyhledej [Rozšířené](#)

UŽITEČNÉ NÁSTROJE A NÁVODY
[Úvodní stránka](#) » [Užitečné nástroje a návody](#) » [Sledování zásilek \(Track & Trace\)](#)

Klientská zóna
[Přihlášení, registrace](#)
[Proč se registrovat?](#)
[Služby v Klientské zóně](#)

Užitečné nástroje a návody
☐ Vyhledat poštu nebo PSČ
☐ Spočítejte si poštovné
Sledování zásilek (Track & Trace)
☐ Změna dispozice balíků
☐ Dokumenty ke stažení (vč. ceníků)
☐ Služby pro příjemce a adresáty
☐ Užitečné informace a návody
☐ Online žádosti
☐ Průzkum spokojenosti se službami
☐ Časté otázky k celnímu řízení
☐ Mobilní aplikace Česká pošta

Sledování zásilek (Track&Trace)
Stáhněte si prosím informace o vaší zásilce (pdf, 450 kB)
Chcete-li zobrazit informace o vaší zásilce zadejte číslo je znázorněno na obrázku níže.
853833
Stážení

Filatelie **Poštovní muzeum** **PostShop eshop**

Související dokumenty
[Průzkum spokojenosti se službami](#) »
[Doporučený balíček](#) »
[Cenný balík](#) »
[Cenné psaní](#) »
[Balík Expres](#) »

Macron Software© 2011 Česká pošta | [Audit přístupnosti](#) | [RSS](#) | [Mapa stránek](#) | [Call centrum](#) | E-mail: info@cpost.cz | Zákaznická linka: 840 111 244

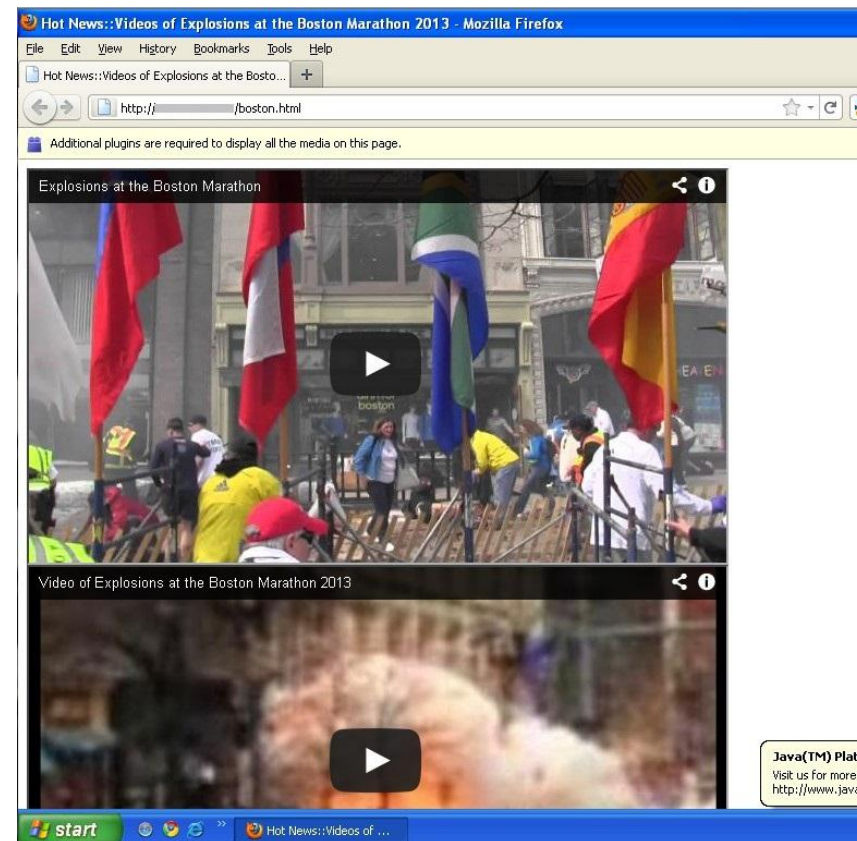
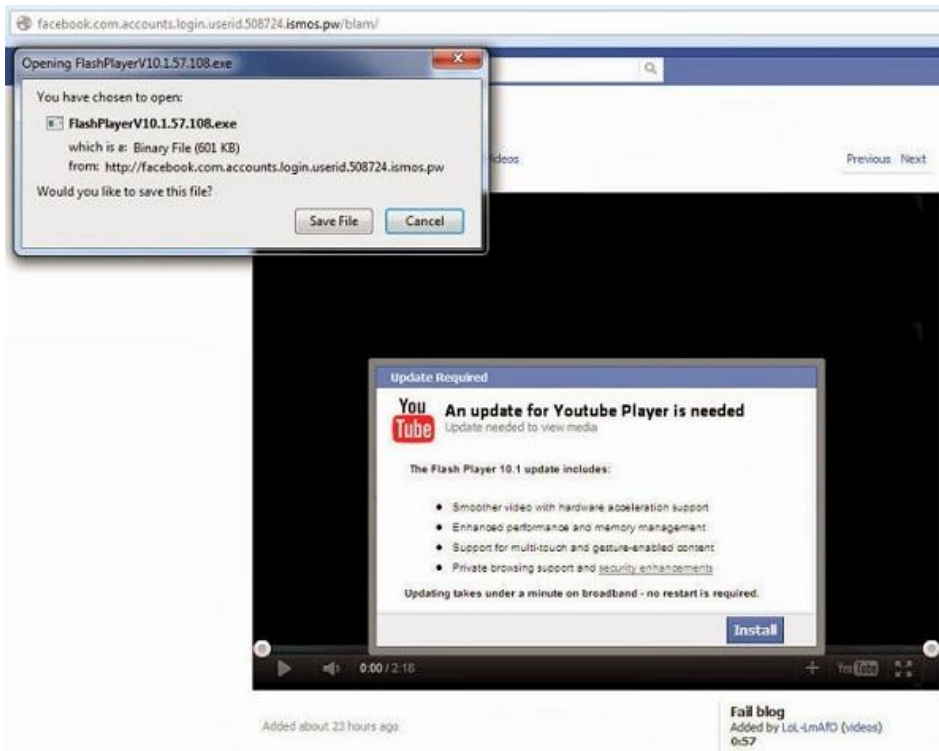
19. února 2014

SECURITY 2014



Sociální sítě

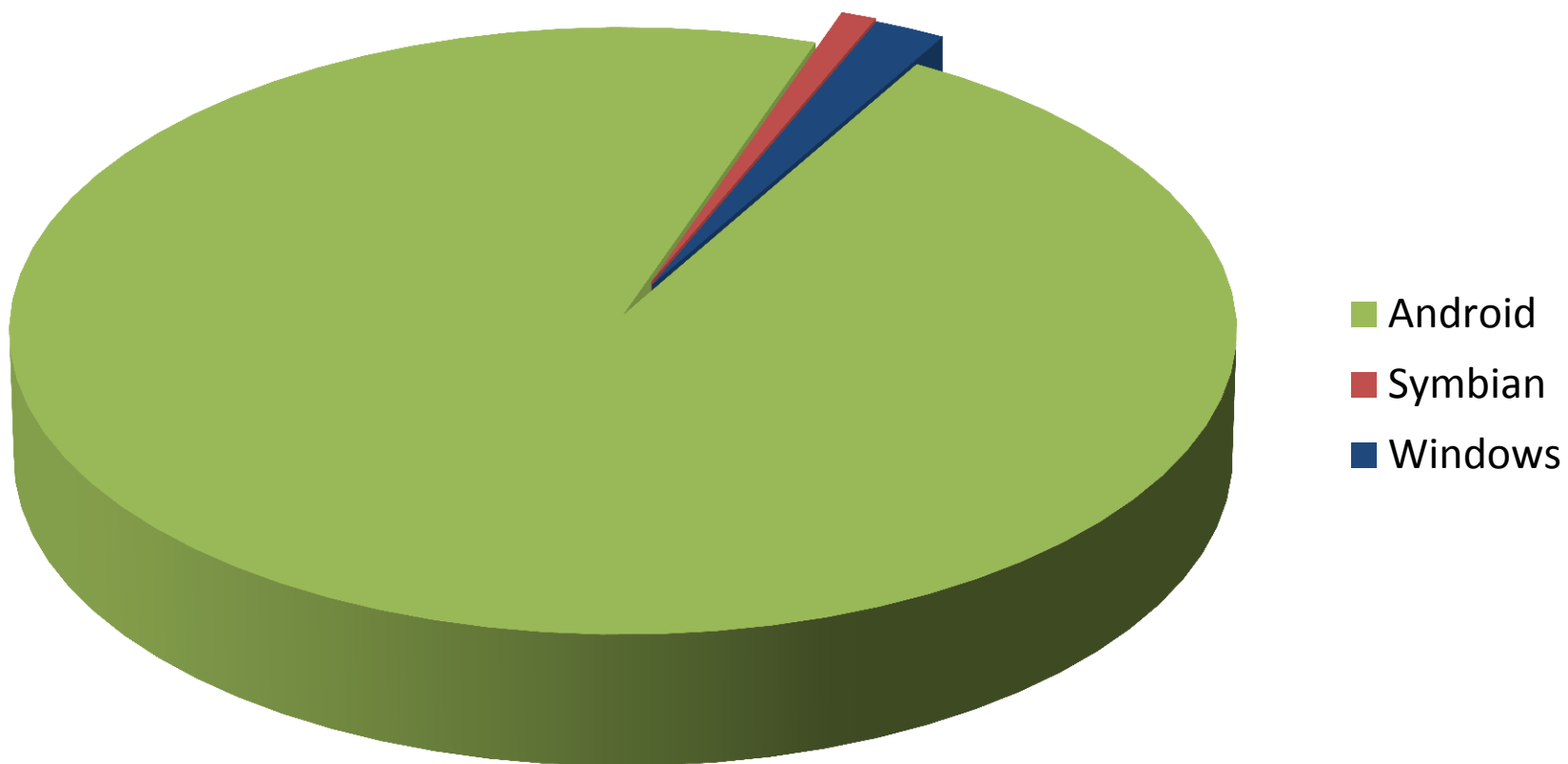
- Odkazy na “senzační obsah”
- Instalace falešných doplňků
- SCAM





Mobilní malware

Podíl malware





Mobilní malware

- 5000 -7000 detekcí malware denně (ESET Mobile Security)
- 97% Android

Android/Adware.AirPush.G	31.84%
Android/Plankton.I	16.84%
Android/Leadbolt.C	9.46%



Malware

- Jeho množství neklesá...
- ... stal se profesionální a sofistikovanou komoditou
- Používá se pro špionáže všeho druhu
- Je distribuován i skrze exploity
- Problémem zůstává nevzdělaný uživatel ...



Dotazy / Diskuze

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Petr Šnajdr

ESET software spol. s r.o.

snajdr@eset.cz

