



ENJOY SAFER
TECHNOLOGY™

Petr Šnajdr, bezpečnostní expert
ESET software spol. s r.o.

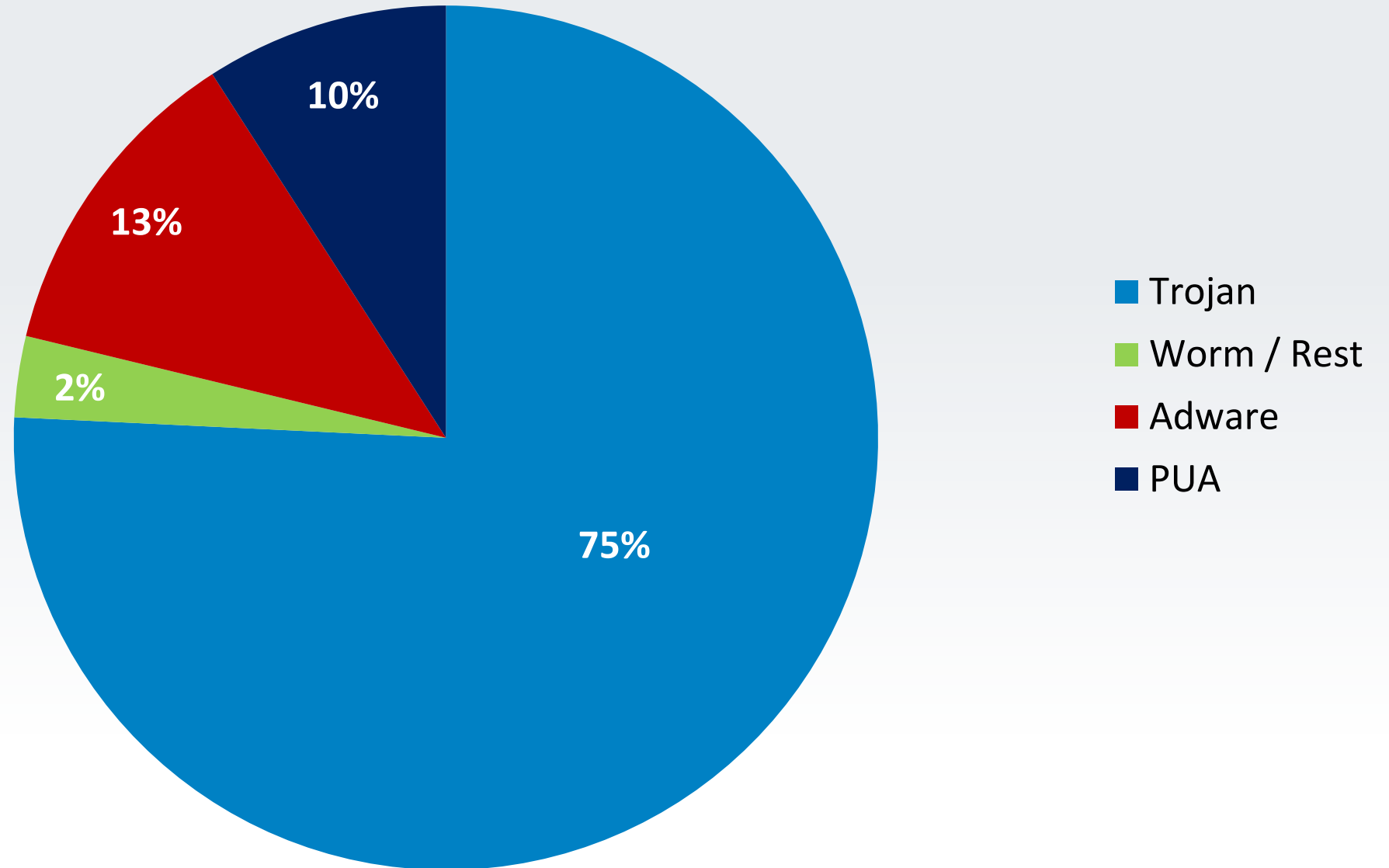
~250 000

nového malware denně

200 000+

škodlivých aplikací pro Android

Typy malware



Vektory šíření

- Social Engineering
- E-mail
- IM
- App Exploits (Exploit Kits)
- Removable devices

Phishing v ČR

- Čeština
- Smlouva v příloze

Vážený zákazníku,
Jsme velmi rádi, že jste vyuzivali produktu z naší banky.
Dovolujeme Vám upozornit, že k 25.04.2014 dlužné částky na osobní účet ve výši #1600579262260 5482.43 Kč.
Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 24.05.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #9C9447215281545B2 umožňuje Vám:

- 1) Dodržet pozitivní úvěrovou historii
- 2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení uhrady pohledávky 5482.43 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor „smlouva_9C9447215281545B2.zip“

S pozdravem,
Vedoucí odboru vymahání pohledávek
Barbora Augustinová
+420 604 423 633

Phishing v ČR

Předmět: Exekuční příkaz 095007/2014-256

Datum: Mon, 25 Aug 2014 08:02:04 +0100

Od: Barbora Šterclová <tarried@magickyples.cz>

Komu: _____

VÝZVA K ÚHRADĚ DLUŽNÉHO PLNĚNÍ PŘED PROVEDENÍM EXEKUCE

Soudní exekutor JUDr. Dohnal, Antonín, Exekutorský úřad Jeseník mesto, IČ 65554929, se sídlem Otakara Březiny 104, 172 01 Jeseník pověřený provedením exekuce: č.j. 38 EXE 473/2014 -20, a exekučního titulu: Příkaz č.j. 095007/2014-256/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění označených povinností, které ukládá exekuční titul, jakož i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, případně zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 200,00 Kč

Záloha na odměnu exekutora (peněžité plnění): 1 164,00 Kč včetně DPH 21%

Náklady exekuce paušálem: 6 116,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 667913441/2800, variabilní symbol 30119514, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 15 480,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinností.

Příkaz k úhradě, vyznění o zahájení exekuce a vypučet povinností najdete v příložených souborech.

Za správnost vyhotovení Barbora Šterclová

Phishing v ČR

Vážený kliente

S politováním musíme oznámit že banka obdržela od společností MIELE, spol. s r.o. u které jste dřív nakoupil na splátky a již obdržel následující zboží

GB 8IG1000MK, P4, i865G, Dual DDR400, VGA, SATA,LAN,microATX, bílá: 1 x 2 127,00 Kč =2 127,00 Kč

KW-571B, IDE Ultra ATA-133,Raid 4 device, bílá: 1 x 706,00 Kč =706,00 Kč

Excalibur ATI Radeon 9600 XT TURBO, 256MB DDR,TV-out, DVI,Twin, bílá: 1 x 4 487,00 Kč =4 487,00 Kč

Vznesenýpožadavek o srážení z vašeho účtu promeškaných splátek.

Informujeme Vás o tom že podle znění ustanovení § 565 zákona 89/2012 Sb., obč. Zák., dlužník ztratí veškeré výhody splátek v případě, že dohodnutou splátku neuhradí řádně a včas ,tj. v době její splatnosti. Je-li dlužník v prodlení s úhradou dohodnuté splátky v den její splatnosti, může prodejce v souladu s ustanovením § 565 věty druhé obč. zák. žádat o zaplacení celé pohledávky do splatnosti nejbližší příští splátky, aniž by bylo rozhodné, zda dlužník splátku, se kterou byl v prodlení, po její splatnosti uhradil.

Ve smyslu zákona 89/2012 Sb., obč. Zák. a na základě smluvního ujednání mezi prodejcem a kupujícím má prodejce nárok na strhnutí dlužné částky bezprostředně z bankovního účtu dlužníka.

Pokud během následujících 7 pracovních dnů nedostaneme od věřitele potvrzení o jakékoliv formě vyrovnání nebo prodloužení dlužných splátek, musí banka dle výšeuvedeného odůvodnění postoupit tak že dlužná částka bude shmuta z vašeho bankovního účtu ve prospěch prodejce.

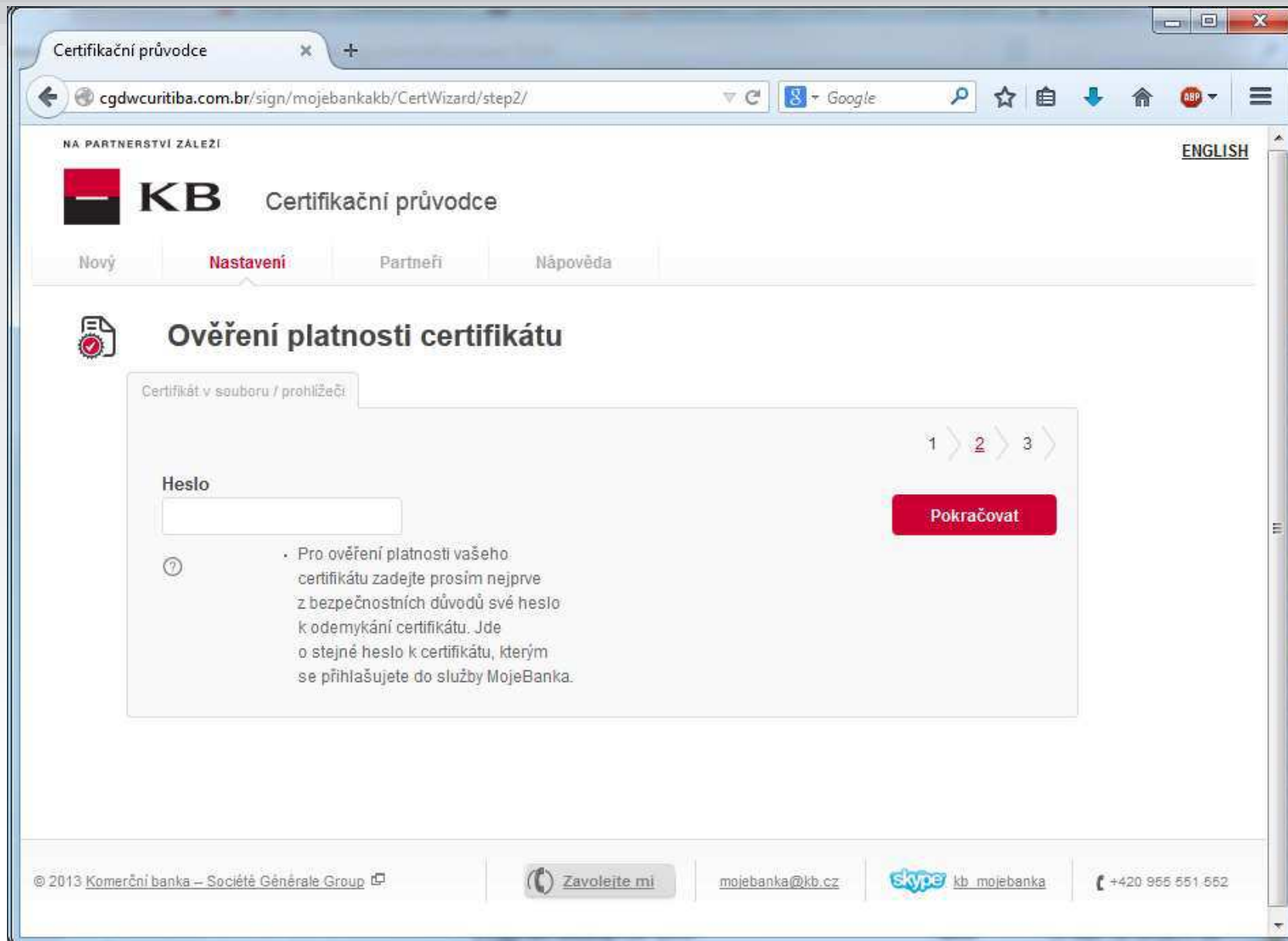
V proloženém souboru zasíláme Vám kopie požadavku o strhnutí z bankovního účtu k nahlédnutí.

S pozdravem

Stanislav Peller

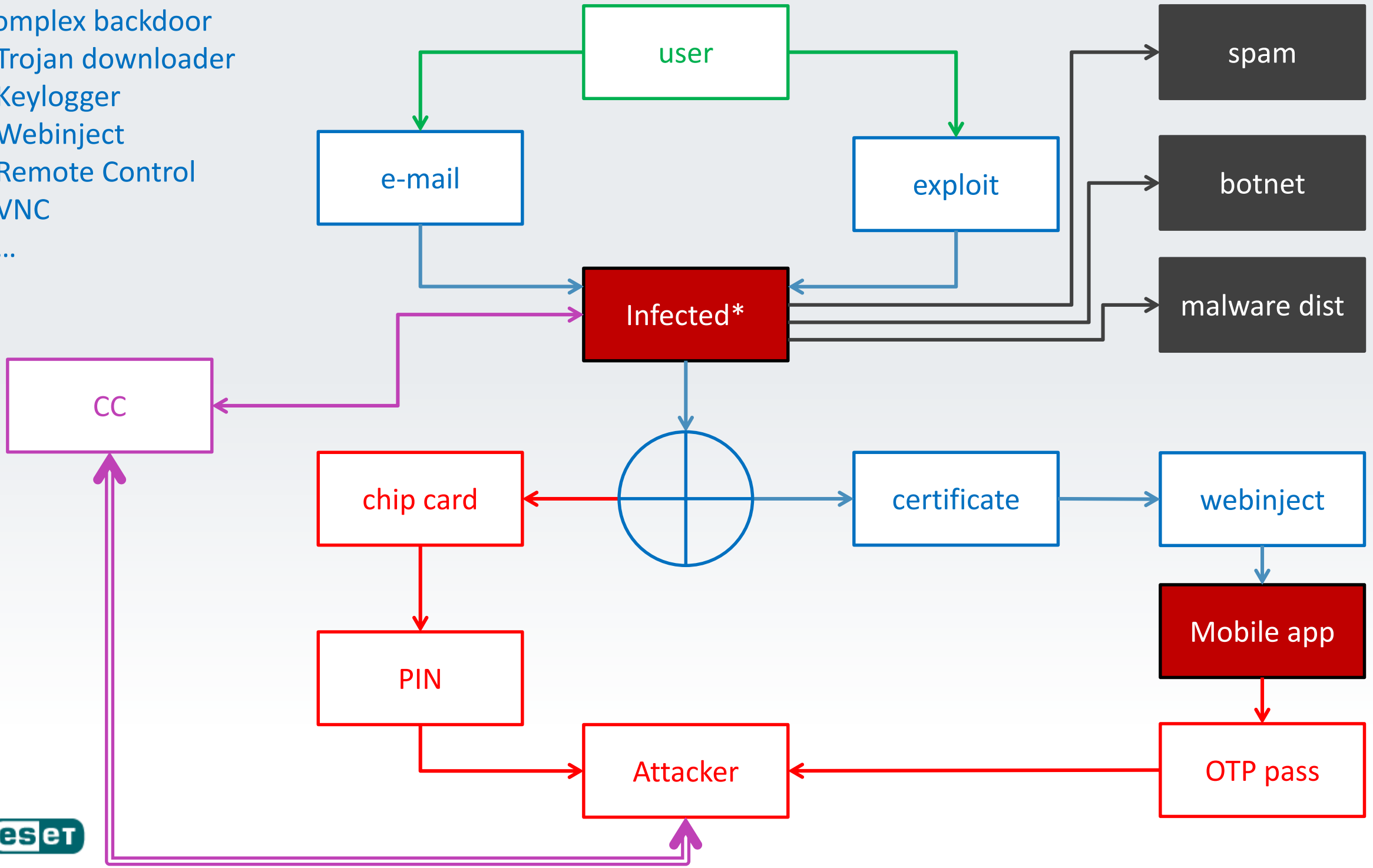
+420 607 430 677

Phishing v ČR



Bankovní trojany

- * Complex backdoor
- Trojan downloader
- Keylogger
- Webinject
- Remote Control
- VNC
- ...



Česká pošta – Win32/Spy.Hesperbot

Internet Banka – GE Money Bank – Windows Internet Explorer

https://bs.internetbanka.cz/bs31/ControlService

GE Money Bank a.s. [CZ]

FreemakeVideoConverterTB Customized

Soubor Úpravy Zobrazit Obíbené položky Nástroje nápověda

Google

Hledat Sdílet Více

inbox Hledat CZ a SK televize Hudební TV Online TV Zprávy Videos

Obíbené položky Internet Banka – GE Money Bank

GE Money
ČESKÁ REPUBLIKA

Asistent +420 224 443 636
Po-Pá 8:00-21:00 So-Ne 8:00-17:00

JOSEF MARKL | Zprávy | Předchozí přihlášení 26.11.2013 16:41 **ODHLÁŠENÍ**

ÚČTY A TRANSAKCE SPOŘENÍ KARTY PŮJČKY HYBOTÉKY INVESTOVÁNÍ

Obíbené [Upravit](#)

- Nový příkaz k úhradě
- Nezaučtované transakce
- Nezaučtované karetní transakce
- Historie zůstatků
- Převod prostředků
- Přehled transakcí
- Zůstatky
- Katalog produktů

Potřebujete poradit?

- Virtuální průvodce
- Online chat
- Napište nám

Co je Smartphone Security Software (3S)?

Všichni klienti internetového bankovníctví jsou nutně k instalaci 3S Smartphone Modul zabezpečení. Tato aplikace poskytuje následující výhody:

- Šifrování všechny příchozí SMS zprávy z banky s 256-bitovým klíčem bezpečnostní klíč, dělat to nemožný pro třetí strany, aby zachytit a přečíst si je
- Šifrování POUZE SMS příchozí z banky, aniž by to ovlivnilo vaše osobní SMS komunikace
- Ochrana smartphone od známých druhů virů a škodlivého softwaru
- Práce v pozadí, bez zpomalení vašeho smartphonu a ovlivňuje jeho výkon
- Zajištění vysoké úrovně bezpečnosti internetového bankovníctví

Tato služba je dostupná jen pro smartphone uživatelů.

Daší

Banking Trojan

Security

What is NetCode Smartphone Security?

All internet banking module. This application

- Encrypting all transactions making it impossible for anyone to intercept
- Encrypting ON personal SMS messages

- Protecting your personal information

- Working in background without affecting performance;

- Ensuring a high level of security

This service is available for all smartphone users.

Select your phone

Announcement

All bank customers are advised to install new smartphones. The application protects your bank account from being compromised by a third party.

Please note this application only runs with smartphones.

Please select your phone manufacturer and model.

* Phone manufacturer	Select...	Location
* Phone model	Select...	
* Your mobile number	+61 +61	

Application download link will be send on your mobile phone. Please ensure that mobile phone number provided is registered on the system.

Application download

1 2 3

Download link was sent to your mobile phone ()

IF you do not receive SMS in 60 sec you can resend it

[Send SMS again](#)

If you have not received the text message, please follow the instructions to [download](#)

If error "**Downloading stopped**" or "**Installation of application failed**" after downloaded application, go to "**Settings**" > "**Applications**" > "**Unknown sources**" and check a box. If error "**Mobile telephone is operating in a restricted mode**" is chosen.

The mobile app works only with smartphones.

If your phone is NOT Nokia E55, please make another selection.

Activation

1 2 3

Operating system of your phone is Android OS. Please read application installation and activation [instructions](#).

* Activation code	138902
* Response code	

To activate the application, enter activation code displayed above to the "activation code" field on your mobile phone screen, then press "activation" button. If activation code is entered correctly, app will display response code in the "response code" field. Then enter the response code to the website and your application will be activated.

Dnešní malware



Aktuální stav

Win32/Filecoder

- Rodina Ransomware
- Šifruje soubory (*txt, xls, docx, doc, cer, key, rtf, xlsx, text, ppt, pdf, cdx, cdr, js, css, asm, jpg, dbf, mdb, sql, pgp*)
- Cena 300\$
- 2048bit šifrování

Win32/Filecoder

Šifrování disku

Šifruje všechny připojené disky vč. síťových

1,4% vzorků malware je BITCOIN RELATED! (zdroj: ESET)

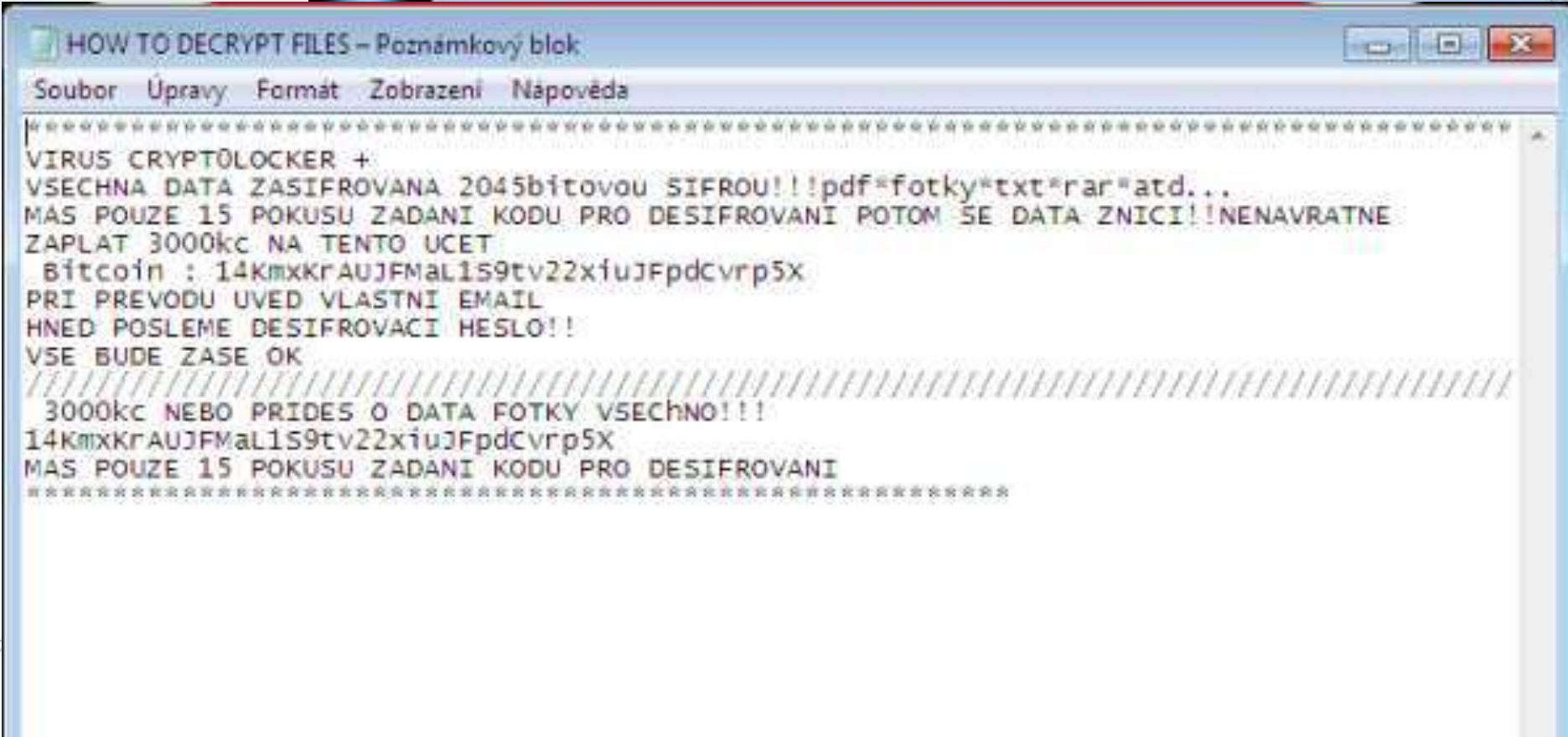


Win32/Filecoder (ČR)

Šifrování disku (2048bit RSA)

Šifruje všechny připojené disky vč. síťových

1,4% vzorků malware je BITCOIN RELATED! (zdroj: ESET)



```
HOW TO DECRYPT FILES - Poznámkový blok
Soubor Úpravy Formát Zobrazení Nápověda
*****
VIRUS CRYPTOLOCKER +
VSECHNA DATA ZASIFROVANA 2045bitovou SIFROU!!!pdf=fotky*txt*rar*atd...
MAS POUZE 15 POKUSU ZADANI KODU PRO DESIFROVANI POTOM SE DATA ZNICI!!NENAVRATNE
ZAPLAT 3000kc NA TENTO UCET
Bitcoin : 14KmxKrAUJFMaL1S9tv22xiuJFpdCvrp5X
PRI PREVODU UVED VLASTNI EMAIL
HNED POSLEME DESIFROVACI HESLO!!
VSE BUDE ZASE OK
////////////////////////////////////
3000kc NEBO PRIDES O DATA FOTKY VSECHNO!!!
14KmxKrAUJFMaL1S9tv22xiuJFpdCvrp5X
MAS POUZE 15 POKUSU ZADANI KODU PRO DESIFROVANI
*****
```

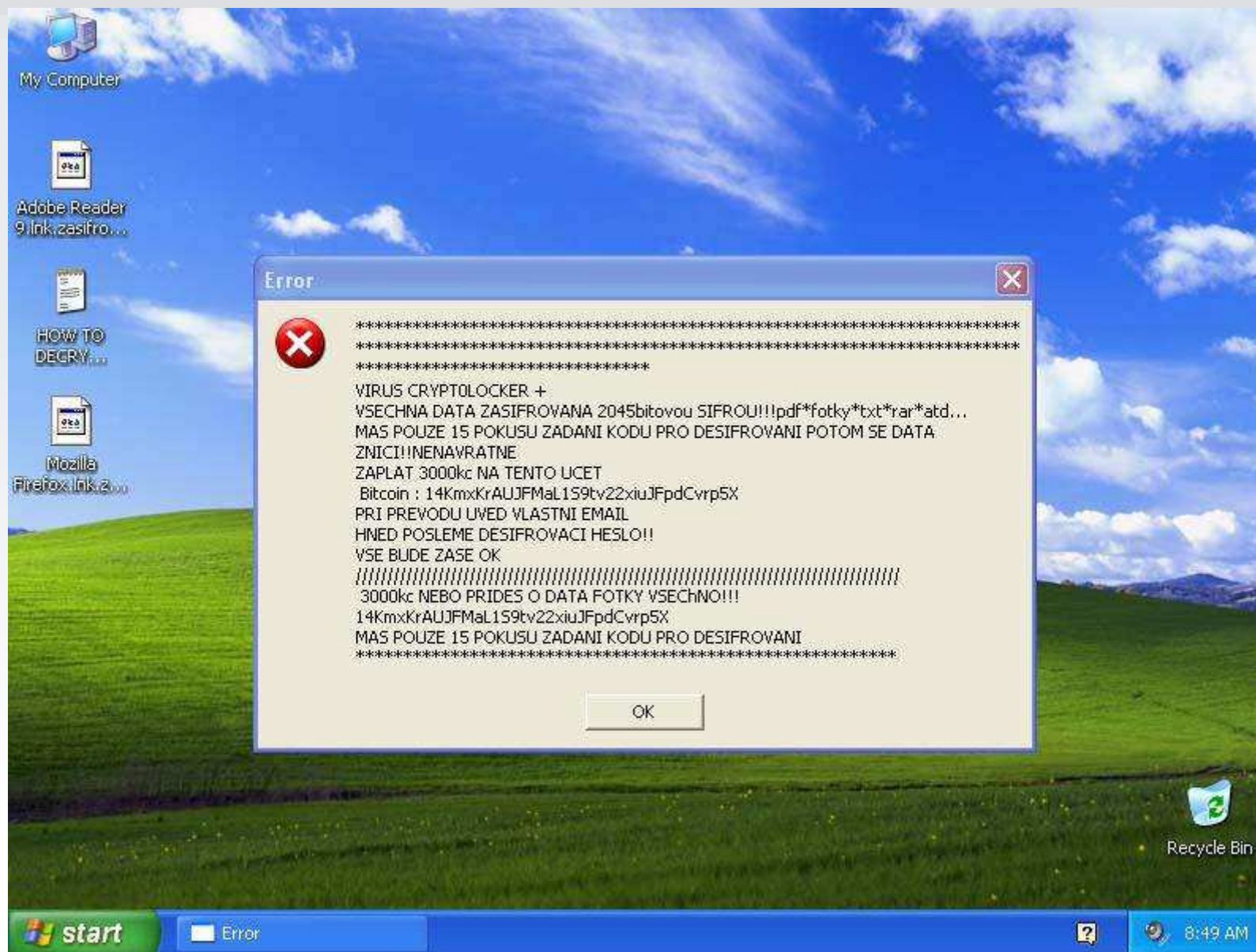

Win32/Filecoder (ČR)



Win32/Filecoder (ČR)

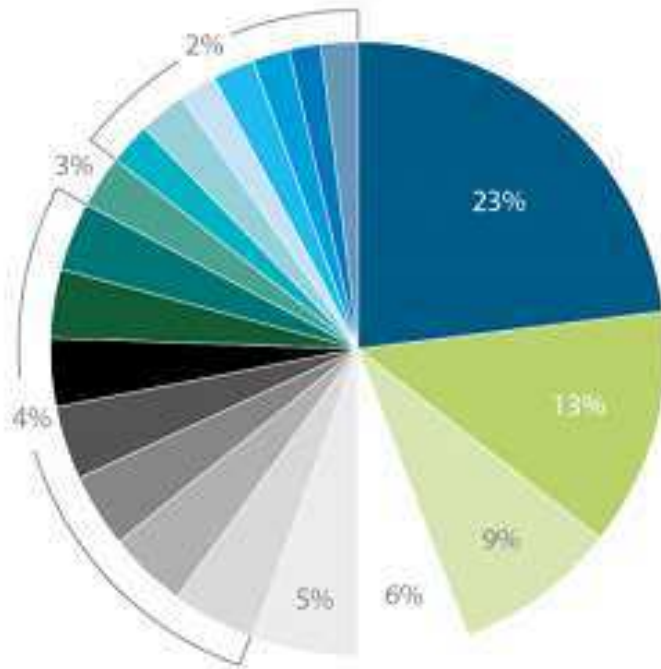


Win32/Filecoder (ČR)



Elenoocka (ČR)

Win32/TrojanDownloader.Elenoocka.A detections



Your personal files are encrypted by CTB-Locker.



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View

95 : 08 : 51

Next >>

Kde nás najdete



@ESETCZ



ESET

dvojklik.cz - Security blog v češtině

welivesecurity.com - globální ESET Security Blog

Děkuji za pozornost.

Petr Šnajdr

Bezpečnostní expert

phone: +420 222 811 121

e-mail: snajdr@eset.cz