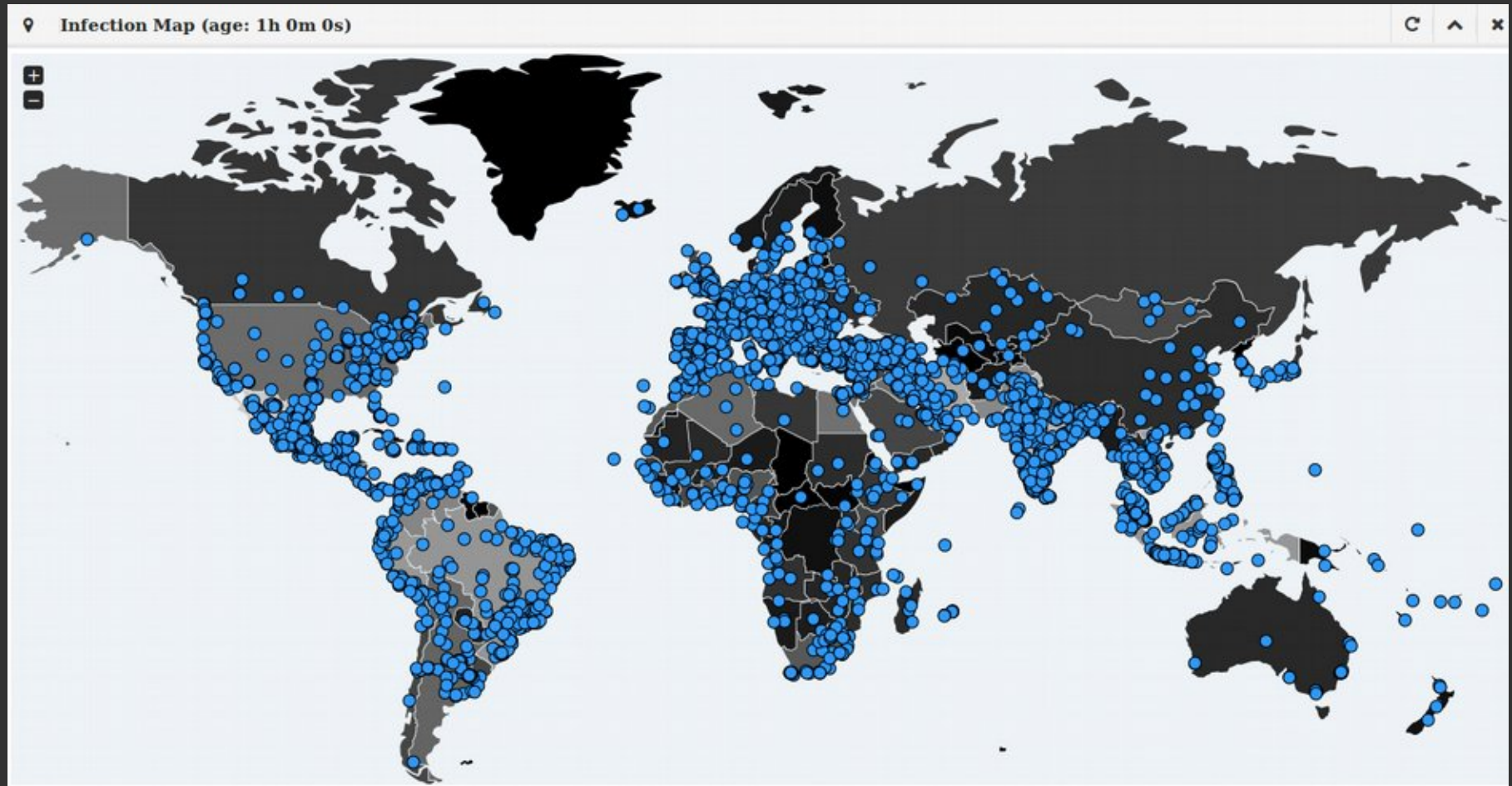



[REAL] Private browsing



@_dead_beef_


About me:

- Researching computer privacy and security as a hobby for about 20 years
- I try to protect things, by using the tools attackers would use to gain access
- Got my first computer, a PC in 1991
- After some time I bought 2400 baud modem and started to explore local BBS scene...
- With the spread of the internet in the second half of the 90's, combination of slow modems and obnoxious ads/banners made way for a new technology – ad blocking
- And so it begins...



??????????????????????
 ?????????????????


?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????



?????????????????????
 ?????????????????

?????????????????????????????

?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????



?????????????????????
 ?????????????????

?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????
 ????????????????????????????????????????????????????? <link rel="preload"> ?

 ?????????????????????????????????????????????????????
 ?????????????????????????????????????????????????????

About this talk:

Couple of topics:

- Threats to privacy
 - Techniques for tracking users on the web
- Threats to security
 - Threat actors
 - Techniques they use for spreading malware
- Ways to protect your devices

Privacy 101

- "This is something I'm willing to do only if no one else is watching."
- There is a huge difference between legal programs, legitimate spying, legitimate law enforcement – where individuals are targeted based on a reasonable, individualized suspicion - and these programs of dragnet mass surveillance that put entire populations under an all-seeing eye and save copies forever.
- These programs were never about terrorism: they're about economic spying, social control, and diplomatic manipulation. They're about power.

Privacy 101

- UN Special Rapporteur on Freedom of Expression: “Encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection”

A portrait of Edward Snowden, a man with short brown hair and glasses, wearing a dark blue button-down shirt. He is looking slightly to the left with a serious expression. The background is blurred and has a warm, orange-toned lighting.

**"ARGUING THAT
YOU DON'T CARE
ABOUT THE RIGHT
TO PRIVACY
BECAUSE YOU
HAVE NOTHING
TO HIDE IS NO
DIFFERENT THAN
SAYING YOU DON'T
CARE ABOUT FREE
SPEECH BECAUSE
YOU HAVE NOTHING
TO SAY."**

Edward Snowden

FIGHT FOR THE FUTURE ❤️

Broad division of problems

- Guys after your private data
- Guys after your money / devices

Threats to privacy

Types of attackers:

- Nation-state level actors (a.k.a. any government agencies)
- Advertising companies / social networks
- “FREE” products

“If you're using a product that you're not paying for, remember, you ARE the product...”

Nation-state level actors

- You really can't do anything about these attacks
- If you think you need to worry about such things, this talk is not for you
- Just be aware of these shenanigans
- It's not just the NSA, it's everybody
- NSA is just immense in scope, and they're only ones that got their files dumped :)
- While US citizens have a tiny slither of protection from abuse by these systems, we in the other 96% of planet's population are classified as FORN and as such, a valid intelligence targets

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

High Speed Optical Cable
Covert, Clandestine or Cooperative Large Accesses
20 Access Programs Worldwide

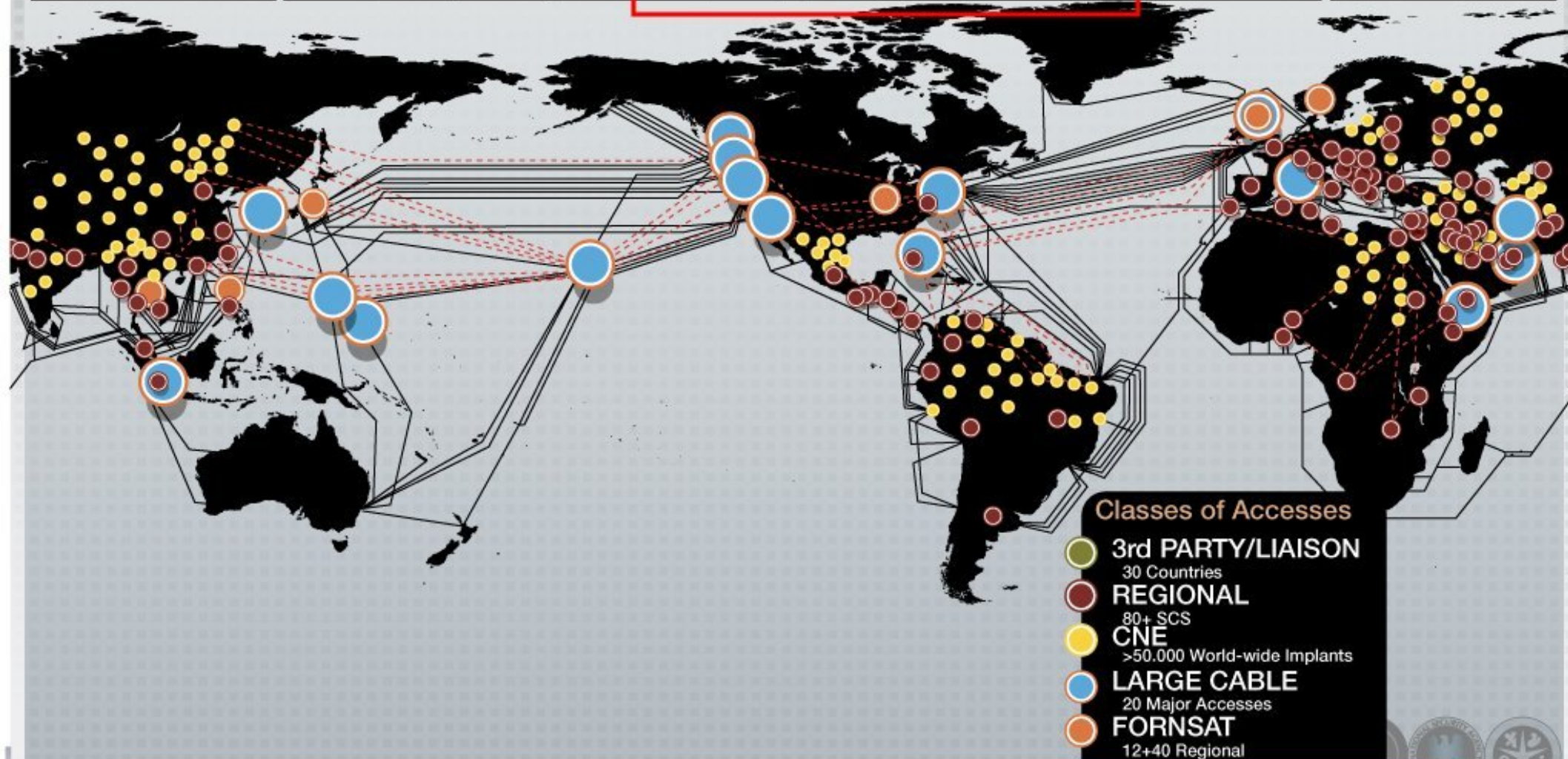
Regional

Caracas	Havana	Kinshasa	Sofia	Berlin	Pristina	Guatemala City
Tegucigalpa	Panama City	Lusaka		Bangkok	Tirana	RESC
Geneva	Bogota			New Delhi	Phnom Penh	
Athens	Mexico City		Budapest	Frankfurt	Sarajevo	Milan
Rome	Brasilia		Prague	Paris		
Quito	Managua	Lagos	Vienna	Rangoon		La Paz
San Jose				Zagreb		Langley
						Vienna Annex
						Reston

FORNSAT

STELLAR
SOUNDER
SNICK
MOONPEN
NY
LADYLOVE

INDRA
IRONSAND
JACKKNIFE
CARBOY
TIMBERLIN
E



TOP SECRET//COMINT//REL TO USA, FVEY



Selector Types

Machine IDs

- **Cookies**
 - Hotmail GUIDs
 - Google prefIDs
 - YahooBcookies
 - mailruMRCU
 - yandexUid
 - twitterHash
 - ramblerRUID
 - facebookMachine
 - doubleclickID
- **Serial numbers**
- **Browser tags**
 - Simbar
 - ShopperReports
 - SILLYBUNNY
- **Windows Error IDs**
- **Windows Update IDs**

Attached Devices

- **IMEIs for Phones**
 - Apple IMEIs
 - Nokia IMEIs
- **UDIDs**
 - Apple UDIDs
- **Bluetooth?**
 - Device Name
 - Device Address

Cipher Keys

- **Cipher Keys uniquely identified to a user**
 - ejKeyID

User Leads

- **User selectors from Cookies, Registry, and Profile Folders**
 - msnpassport
 - google
 - yahoo
 - Youtube
 - Skype
 - Paltalk
 - Fetion
 - QQ
 - hotmailCID
- **STARPROC-identified active users**

Network

- **Wireless MACs**
- **VSAT MACs and IPs**
- **Remote Administration IPs**
 - Putty
 - WinSCP

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(C) Legacy QUANTUMTHEORY techniques

- (TS//SI//REL) QUANTUMINSERT
 - HTML Redirection
- (TS//SI//REL) QUANTUMSKY
 - HTML/TCP resets
- (TS//SI//REL) QUANTUMBOT
 - IRC botnet hijacking



TOP SECRET//COMINT//REL TO USA, FVEY//20320108

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(U) New Hotness

- (TS//SI//REL) QUANTUMBISCUIT
 - Redirection based on keyword
 - Mostly HTML Cookie Values
- (TS//SI//REL) QUANTUMDNS
 - DNS Hijacking
 - Caching Nameservers
- (TS//SI//REL) QUANTUMBOT2
 - Combination of Q-BOT/Q-BISCUIT for web based Command and controlled botnets



TOP SECRET//COMINT//REL TO USA, FVEY//20320108

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(U) Experimental

- (TS//SI//REL) QUANTUMCOPPER
 - File download disruption
- (TS//SI//REL) QUANTUMMUSH
 - Virtual HUFFMUSH / Targeted Spam Exploitation
- (TS//SI//REL) QUANTUMSPIM
 - Instant Messaging (MSN chat, XMPP)
- (TS//SI//REL) QUANTUMSQUEEL
 - Injection into MySQL persistent database connections
- (TS//SI//REL) QUANTUMSQUIRREL
 - Truly covert infrastructure, be any IP in the world

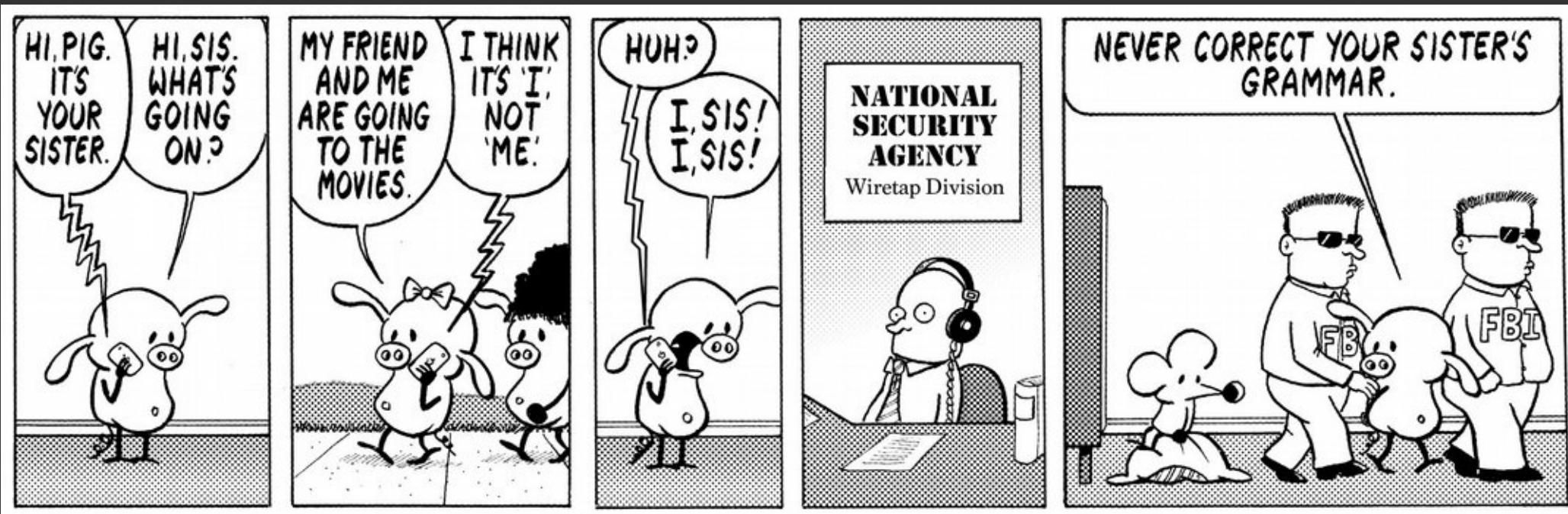


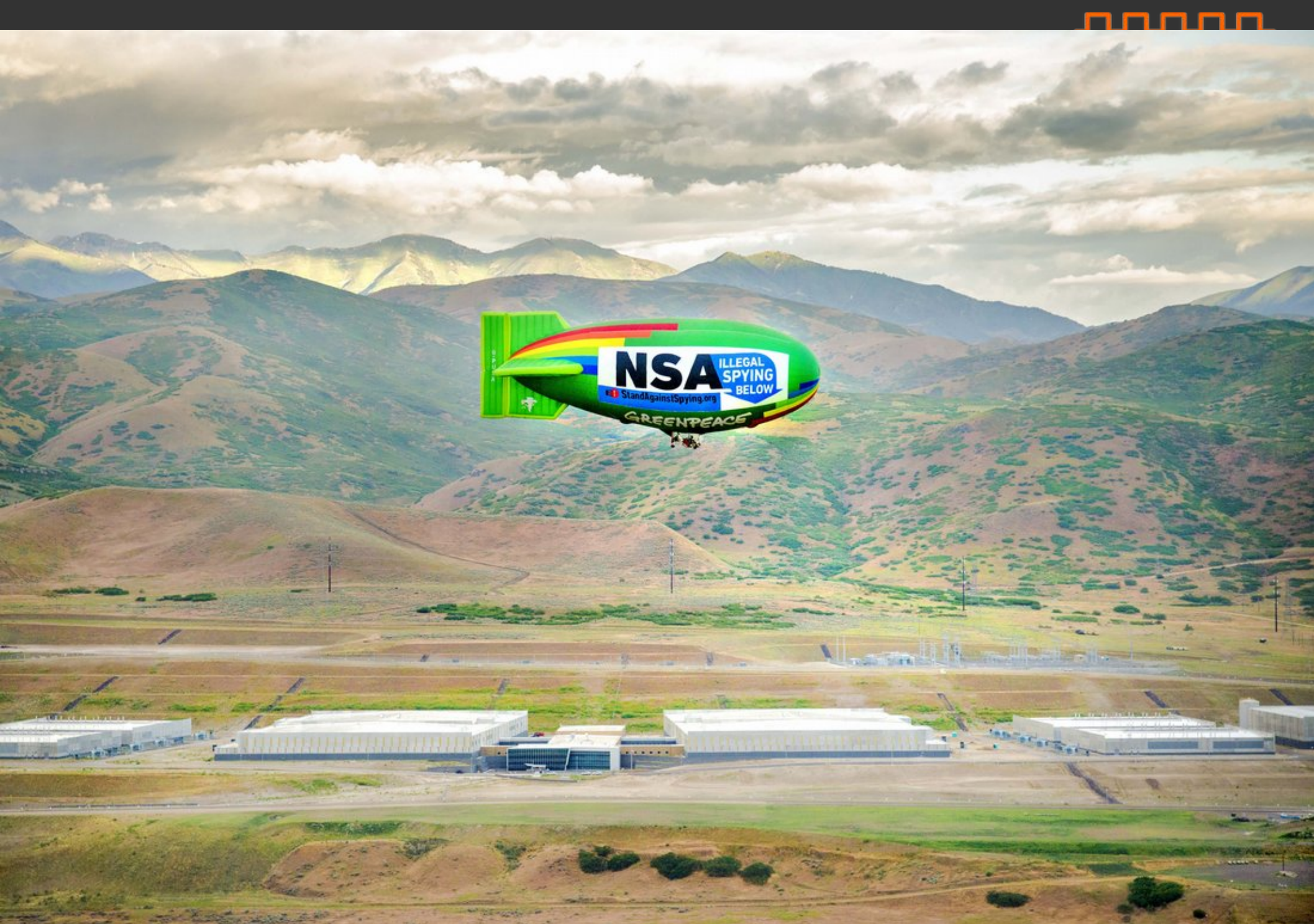
TOP SECRET//COMINT//REL TO USA, FVEY//20320108

Total Information Awareness (2001)

- As a "virtual, centralized, grand database", the scope of surveillance includes, among others, credit card purchases, magazine subscriptions, web browsing histories, academic grades, bank deposits, passport applications, driver's licenses, toll records, judicial records, divorce records, etc.
- Health information collected by TIA include drug prescriptions, medical records, and individual DNA.

The watchlists problem





Total Information Awareness



Total Information Awareness



Reference:

For longtime history of abuse of these powers and efforts to bring them into light, go to:

http://www.historycommons.org/timeline.jsp?timeline=civilliberties&civilliberties_surveillance



To put things in perspective...

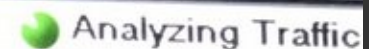


WALL OF SHEEP



login	pass	domain ip	application	cookie / hash
admin	*SS*****	ec2-54-201-295-19.us-w	HTTP	looks like SQL injection
2cec16df-9c80-4653-b292-2cf973a64	3j*****	65.77.227.20	HTTP	zodiak servlet
lououtin@aol.com	red*****	104.31.86.204	HTTP	
47a98e2131b488ab92957f3e02b570a7	08a*****	api.socialhoney.co	HTTP	
sorensop	580*****	earthlink.net	POP3	
lankaesh	!la*****	leguin.freenode.net	IRC	
mail001	SHE*****	mail.emome.net	HTTP	revealed IMEI
ahernandez	sic*****	sicapsrv.sicap.com.mx	HTTP	
wsclient	sup*****	wwwapp.aftonbladet.se	HTTP	
soft001	jun*****	mail.enome.net	HTTP	
sportcaster	one*****	crossports.com	HTTP	
btapi	bt0*****	pdf.businessstimes.com	HTTP	
jdupond@yopmail.com	jdu*****	api.gablys.net	HTTP	
csv	pau*****	csv.pd.appbank.net	HTTP	
tmpark	jud*****	popeye.snu.ac.kr	POP3	
defkor	nie*****	ironhide.gtisc.gatech.edu	HTTP	password change
defkor	qla*****	ironhide.gtisc.gatech.edu	HTTP	
produser	pus*****	pushnotifications.timeso	HTTP	
musah@optonline.net	lib*****	optonline.net	POP3	
visitor	ViS*****	bc3.homeip.net	HTTP	
csrsl1	dNN*****	sgee.samsung.csrlbs.com	HTTP	
2014xzt@sjtu.edu.cn	yua*****	mailstore05.sjtu.edu.cn	POP3	
EAV-015685765	d29*****	update.eset.com	HTTP	
boxer	13f*****	boxerupgrades.getboxer	HTTP	

Wall of Sheep © - Copyright © 2001-2016 - All rights reserved - www.wall-of-sheep.com

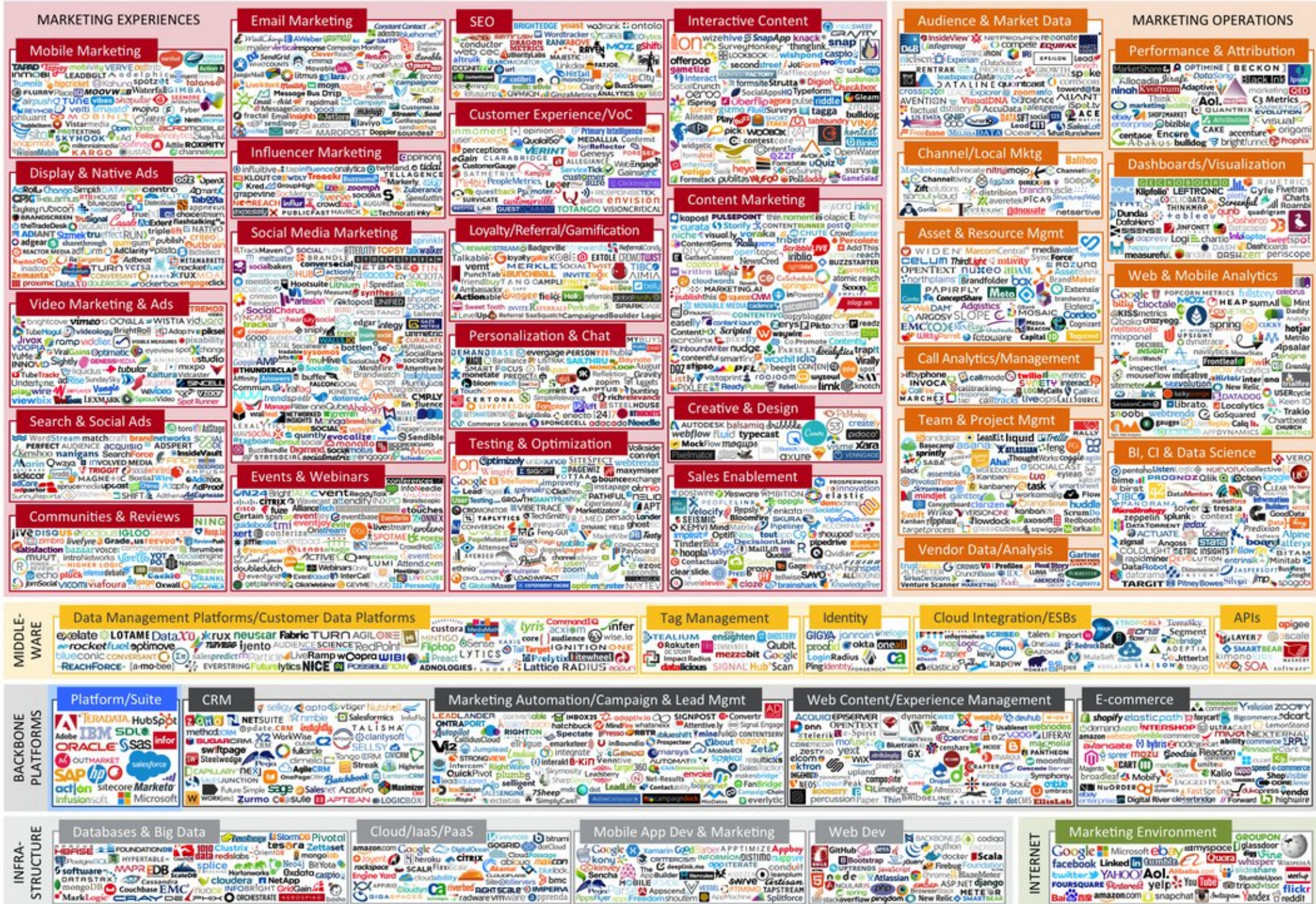


Privacy problem #2

Private entities going after your data

- Social networks, Facebook alone earned \$6.4 BILLION in last quarter from ads
- Advertising companies
- Household devices – tv's, fridges, washing machines, coffee machines, vibrators (?!)
- Some / most of android phones already come preloaded with crapware / adware

Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet.



Lightbeam demo

We'll open 3 (THREE) websites:

- blic.rs
- b92.net
- 24sata.rs

and see that there are 131 (!) third-party requests in a simple browsing session !!!

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did



Kashmir Hill, FORBES STAFF

Welcome to The Not-So Private Parts where technology & privacy collide [FULL BIO](#) ✓

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. [Target](#) TGT -1.19%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Charles Duhigg outlines in the [New York Times](#) how Target tries to hook parents-to-be at that crucial moment before they turn into rampant — and loyal — buyers of all things pastel, plastic, and miniature. He talked to Target statistician Andrew Pole — before Target freaked out and cut off all communications — about the clues to a customer's impending bundle of joy. Target assigns every customer a Guest ID number, tied to their credit card, name, or email address that becomes a bucket that stores a history of everything they've bought and any demographic

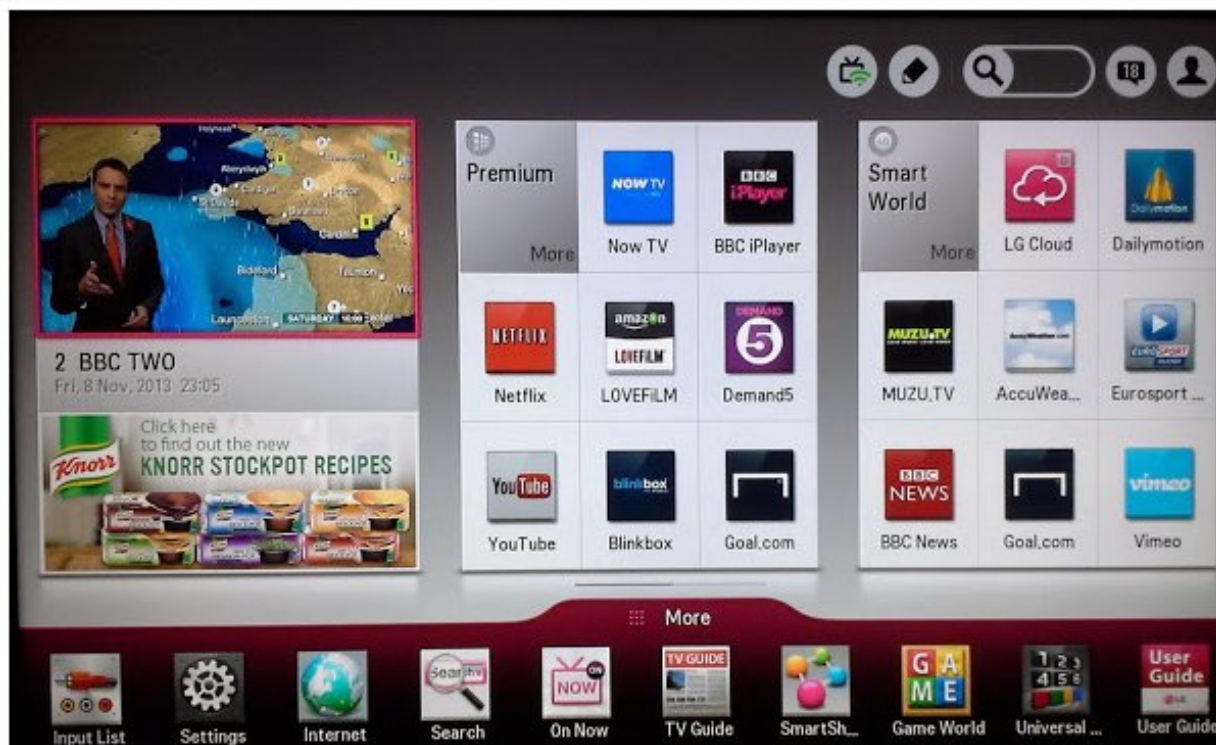


TARGET

Target has got you in its aim

LG Smart TVs logging USB filenames and viewing info to LG servers

Earlier this month I discovered that my new LG Smart TV was displaying ads on the Smart landing screen.



After some investigation, I found a rather [creepy corporate video](#) (since removed, [mirror here](#)) advertising their data collection practices to potential advertisers. It's quite long but a sample of their claims are as follows:

LG Smart Ad analyses users favourite programs, online behaviour, search keywords and other information to offer relevant ads to target audiences. For example, LG Smart Ad can feature sharp suits to men, or alluring cosmetics and fragrances to women.

Furthermore, LG Smart Ad offers useful and various advertising performance reports. That live broadcasting ads cannot. To accurately identify actual advertising effectiveness.

Left: Samsung SmartTV privacy policy, warning users not to discuss personal info in front of their TV Right: 1984 pic.twitter.com/osywjYKV3W

— Parker Higgins (@xor) February 8, 2015

Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage data so that

Behind Winston's back the voice from the telescreen was still babbling away about pig-iron and the overfulfilment of the Ninth Three-Year Plan. The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live--did live, from habit that became instinct--in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

Some things are THE VERY definition of private stuff

Sex toy sends intimate data to its creator

It shares temperature and vibration levels that could reveal a little too much about your personal life.



Jon Fingas, @jonfingas
08.10.16 in [Sex](#)

Comments

804
Shares



98 personal data points that Facebook uses to target ads to you

Targeting options for Facebook advertisers*

1. Location
2. Age
3. Generation
4. Gender
5. Language
6. Education level
7. Field of study
8. School
9. Ethnic affinity
10. Income and net worth
11. Home ownership and type
12. Home value
13. Property size
14. Square footage of home
15. Year home was built
16. Household composition
66. Users who are active credit card users
67. Credit card type
68. Users who have a debit card
69. Users who carry a balance on their credit card
70. Users who listen to the radio
71. Preference in TV shows
72. Users who use a mobile device (divided by what brand they use)
73. Internet connection type
74. Users who recently acquired a smartphone or tablet
75. Users who access the Internet through a smartphone or tablet
76. Users who use coupons
77. Types of clothing user's household buys
78. Time of year user's household shops most
79. Users who are "heavy" buyers of beer, wine or spirits
80. Users who buy groceries (and what kinds)
81. Users who buy beauty products
82. Users who buy allergy medications, cough/cold medications, pain relief products, and over-the-counter meds

*Not even conclusive!



Zuck: Yeah so if you ever need info about anyone at Harvard

Zuck: Just ask.

Zuck: I have over 4,000 emails, pictures, addresses, SNS

[Redacted Friend's Name]: What? How'd you manage that one?

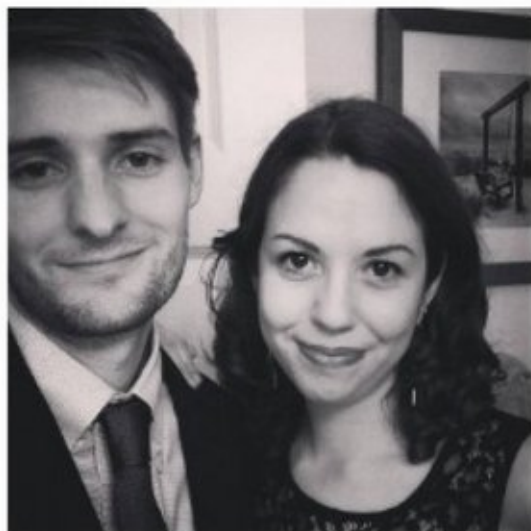
Zuck: People just submitted it.

Zuck: I don't know why.

Zuck: They "trust me"

Zuck: Dumb fucks.

Report Details



Caitlin Dewey

Requested
Connected

8th June 2016
8th June 2016

Score Assured Rating

4/5

Low risk

Social Proximity

Washington Post

Anthony Weiner

John McCain

Michelle Obama

Barack Obama

Paul Ryan

Chris Christie

Edwards

Activity Times



Connected Account Age

Age

7+ years

Financial Stress

22nd December 2015

staying in

30th January 2013

a loan

17th October 2012

no money

17th September 2012

loan

24th May 2012

being poor

29th November 2011

loans

3rd November 2011

loans

26th October 2011

loan

19th October 2011

loans

15th September 2011

Loan

Crime

6th April 2016

murderer

3rd December 2015

in prison

25th March 2015

terrorist

2nd June 2014

blackmail

6th February 2014

stealing

3rd February 2014

steal

23rd October 2013

stealing

14th August 2013

terrorist

10th May 2013

fraud

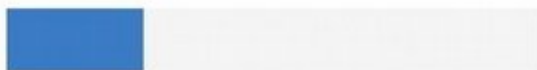
22nd September 2012

justice

Pets

Personality

Open 26.15%



Conscientious 86.01%



Extravert 95%



Agreeable 90.71%



Neurotic 50%



Personality

Select the personality type for a full breakdown...

Openness

Openness is positively related to tenant turnover and those high in it are more likely to up sticks and leave a property.

They have a tendency for looking for 'better' suited or more aspirational property.

They are often of the opinion that 'the grass may be greener...'

However someone low in the trait, will typically be more reserved and less likely to raise an issue with a landlord.

An ideal situation is an applicant towards the middle of the range.

Technologies used to track users

- HTTP (non HTTPS) browsing can be sniffed by:
 - Your ISP
 - Anyone providing you WiFi internet access
 - Anyone who can monitor traffic between your provider and your destination server
- Cookies
 - They're so 90's technology, but they're still being used both legitimately and non-legitimately

Technologies used to track users

- Javascript
 - You can't disable it completely, it breaks websites
- Adobe Flash
 - Just kill it, and go the HTML5 way
- Flash local stored objects (LSOs), a.k.a. "Flash Cookies"
 - They are stored in one location for all browsers

Technologies used to track users

- HTML5 Local Storage
 - “HTML5 Databases” , similar to cookies, but hold more data
- WebRTC
 - Used for browser-to-browser direct connections, can leak local LAN ip address, and hash of unique identifier for webcam / microphone
- HTTP Referrer
 - Refers to the site from which site you arrived

Technologies used to track users

- HTML5 Canvas fingerprinting
 - When visiting a site, a browser is instructed to render a hidden picture, and report a hash of it back. Due to variations in CPU, GPU, OS, browser, hash is different for every computer



Technologies used to track users

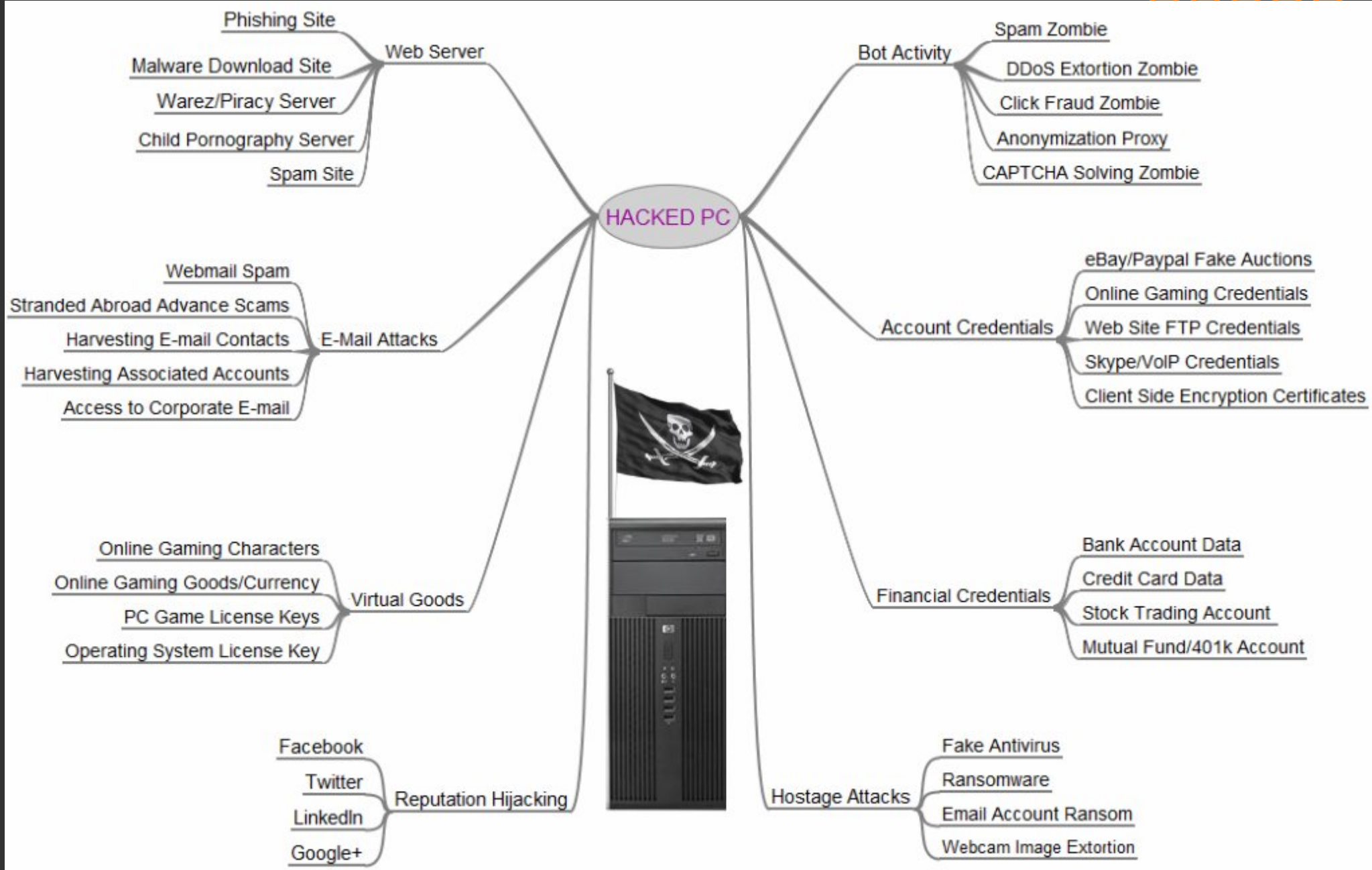
- Evercookie, a.k.a. Zombie Cookie, scariest of them all, in that it restores it's value after you have cleaned the cache, if you miss some of the places it hides itself:
 - Standard HTTP cookies
 - Local Shared Objects (Flash cookies)
 - Silverlight Isolated Storage
 - Storing cookies in RGB values of auto-generated, force-cached PNGs using HTML5 Canvas tag to read pixels (cookies) back out
 - Storing cookies in Web history
 - Storing cookies in HTTP ETags
 - Storing cookies in Web cache
 - window.name caching
 - Internet Explorer userData storage
 - HTML5 Session Web storage
 - HTML5 Local Web storage
 - HTML5 Global Storage
 - HTML5 Web SQL Database via SQLite
 - Caching in HTTP Authentication
 - Using Java to produce a unique key based on NIC information.

The good news:

- You can block 99.99% of all this cruft, you just need:
 - a little bit of education
 - proper tool to clean-up the system
 - way to hide your IP address / network traffic and
 - hardened browser
- That's the demo for at the end of the talk :)

Threats to security

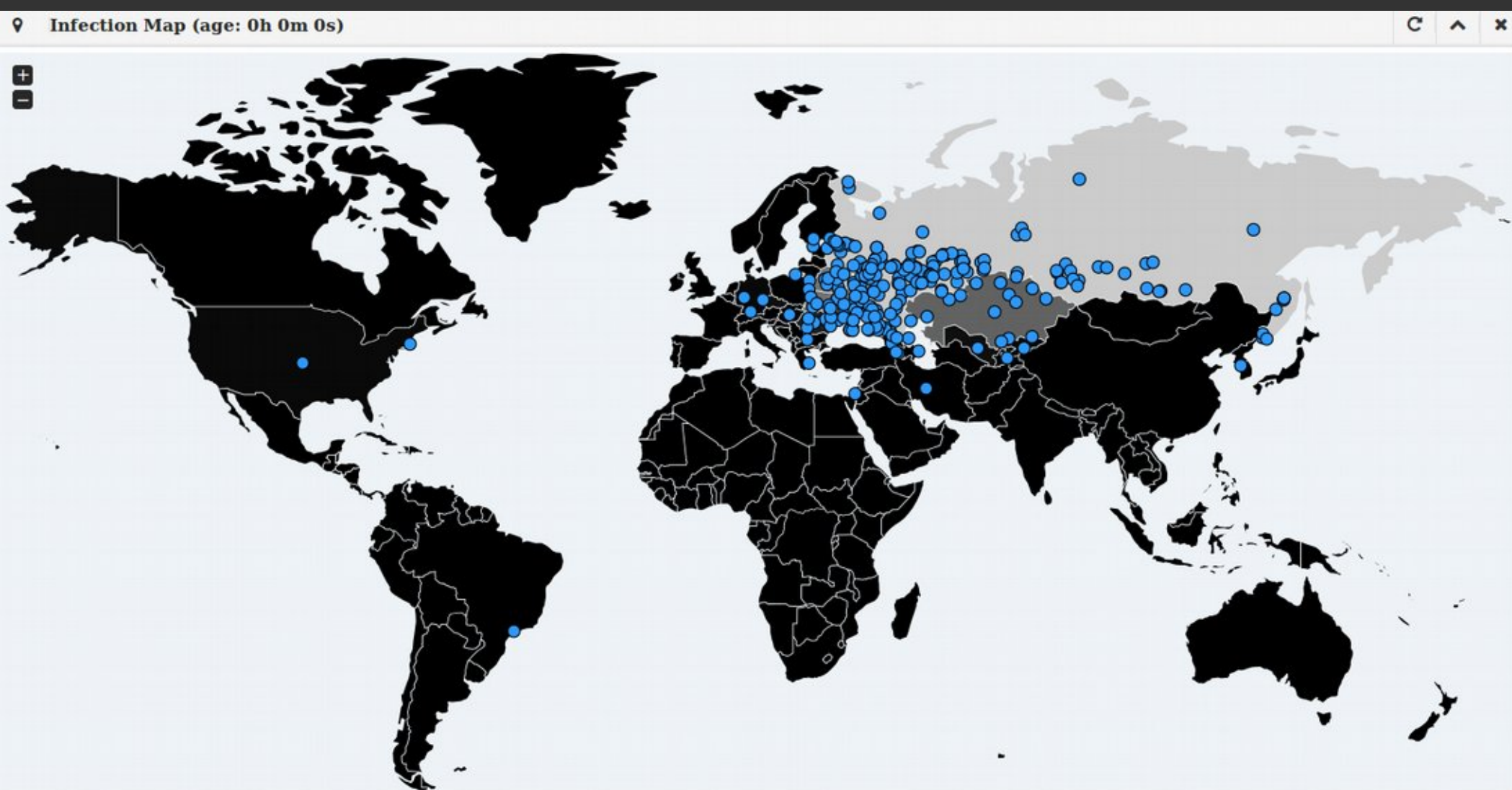
- Ransomware is #1 threat
- Banking trojans
- Fake tech support scams
- Remote Access Tools (RATs)
- Click fraud
- DDOS



50k hosts infected in 1 hour



Not everything is from Russians



Who are the attackers



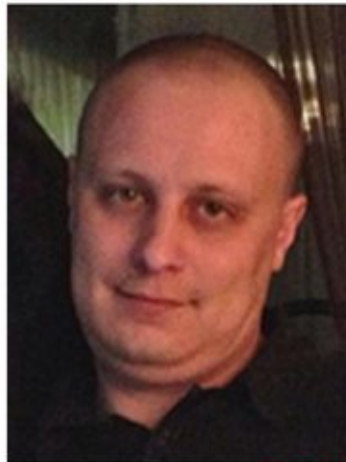




WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud



DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

Date(s) of Birth Used: October 28, 1983

Eyes: Brown

Weight: Approximately 180 pounds

Race: White

Hair: Brown (usually shaves his head)

Height: Approximately 5'9"

Sex: Male

Occupation: Bogachev works in the Information Technology field.



Peter Guttman, Malware Biz (2012)

Example: Rock Phish (ctd)

Some of the people behind this are really, really scary

- This is established, organised crime

Example: Anti-cybercrime investigator in Russia working with the St.Petersburg police

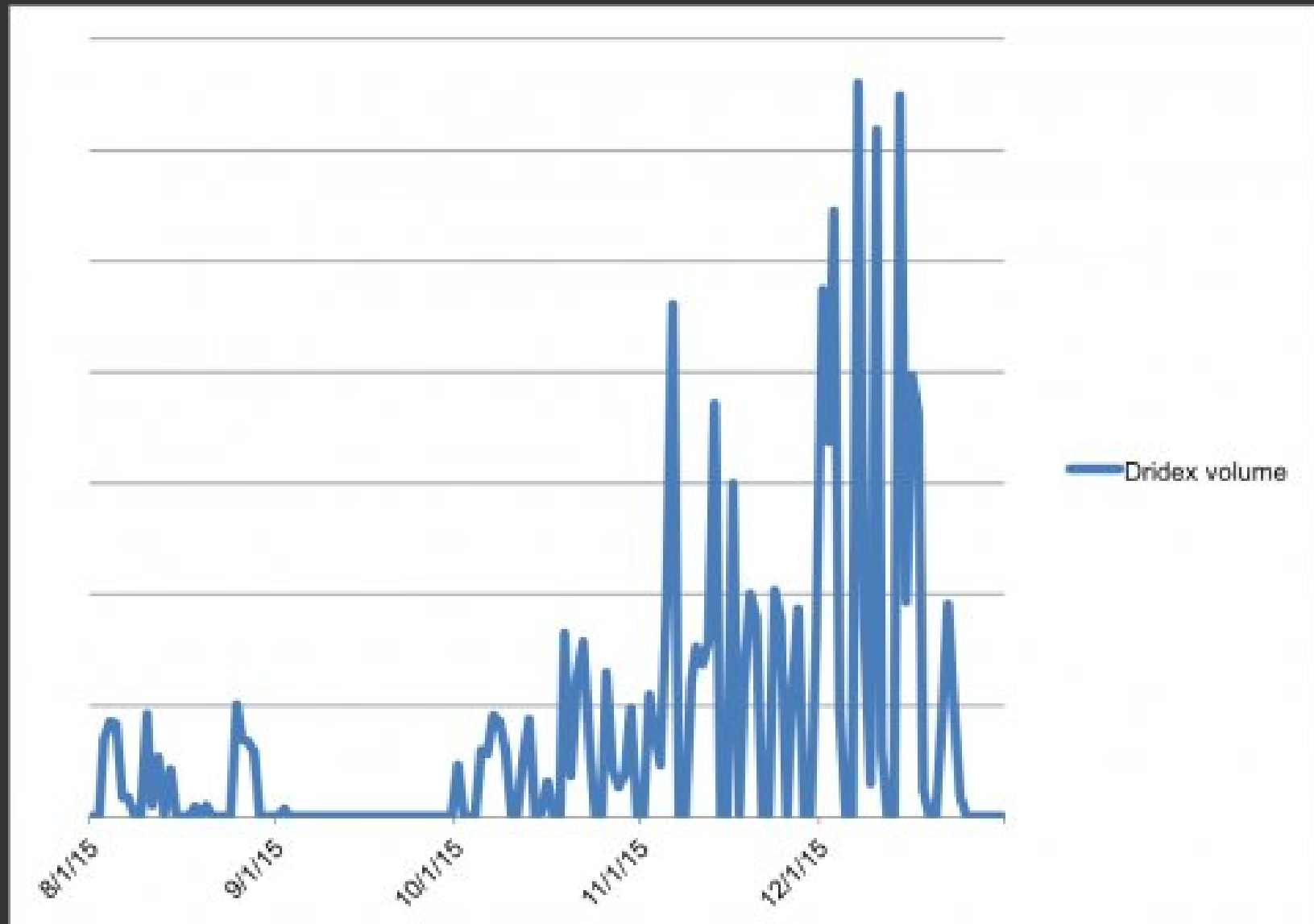
- One of his teenage daughters, living in a western country, is kidnapped
- “If you drop the case, the rest of your children might be OK”
- Five years later she’s located in Kazakhstan

She was fed drugs and used to service men

— Joseph Menn, author of “Fatal System Error”

These are people you don’t ever want to mess with

Even they must go on vacations...



But you really don't need to travel that far to
find assholes

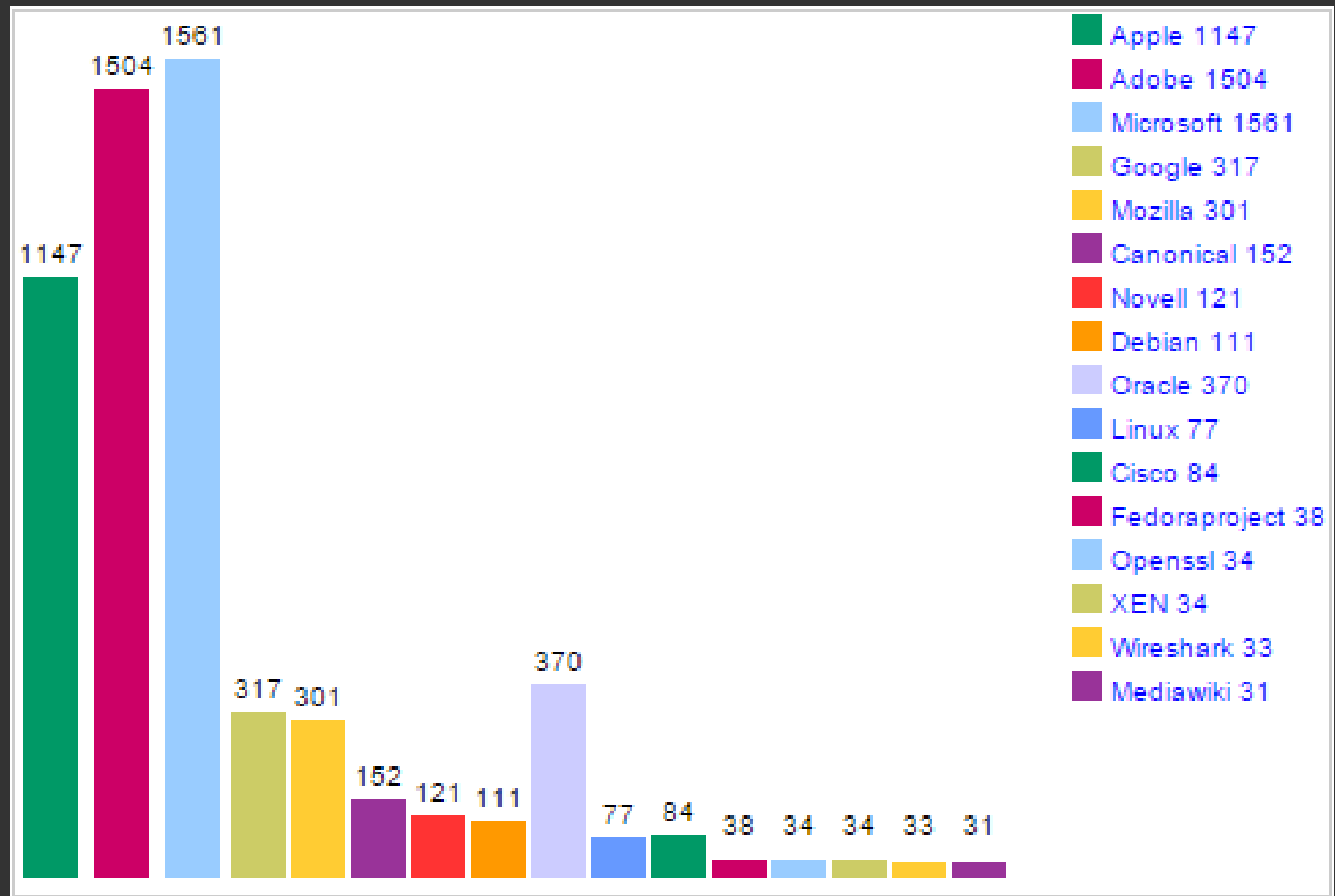


So, how do they do it?

Two primary methods of infection:

- Malicious mail attachments sent during the massive spam / phishing campaigns
- Infections while surfing websites, a.k.a drive-by-downloads, using exploits for popular software
 - Java
 - Flash, Microsoft Silverlight
 - Adobe PDF reader
 - Browsers themselves, especially Internet Explorer


Because every software has bugs



Because every software has bugs


Yesterday, 06:15 PM

Tweet this Post! #1

hunter_exploitkit 

Junior Member

Join Date: Aug 2015
Posts: 7

 **Sell Hunter ExploitKit**

Hello every buddy
 I'm Seller of Exploitkit
 Internet Explorer 6 7 8 9 10 11
 Firefox exploit that work on version 35.0 and Under it
 Adobe Flash Player that work on 11.x 12.x 13.x 14.x 15.x 16.x 17.x 18.x
 Java 6 and 7 and update 25 nad early


Microsoft Office Word that work on 2007 2010 2013
 Microsoft Office Powerpoint that work on 2007 2010 2013
 Adobe Acrobat Reader

.chm client side 0day (don't have update patch from microsoft) work on all windows version and by default have on windows

all exploit have FUD and update all panel everyday

300\$ peer week and 800\$ peer month

exploitkit@jabb3r.org

 QUOTE

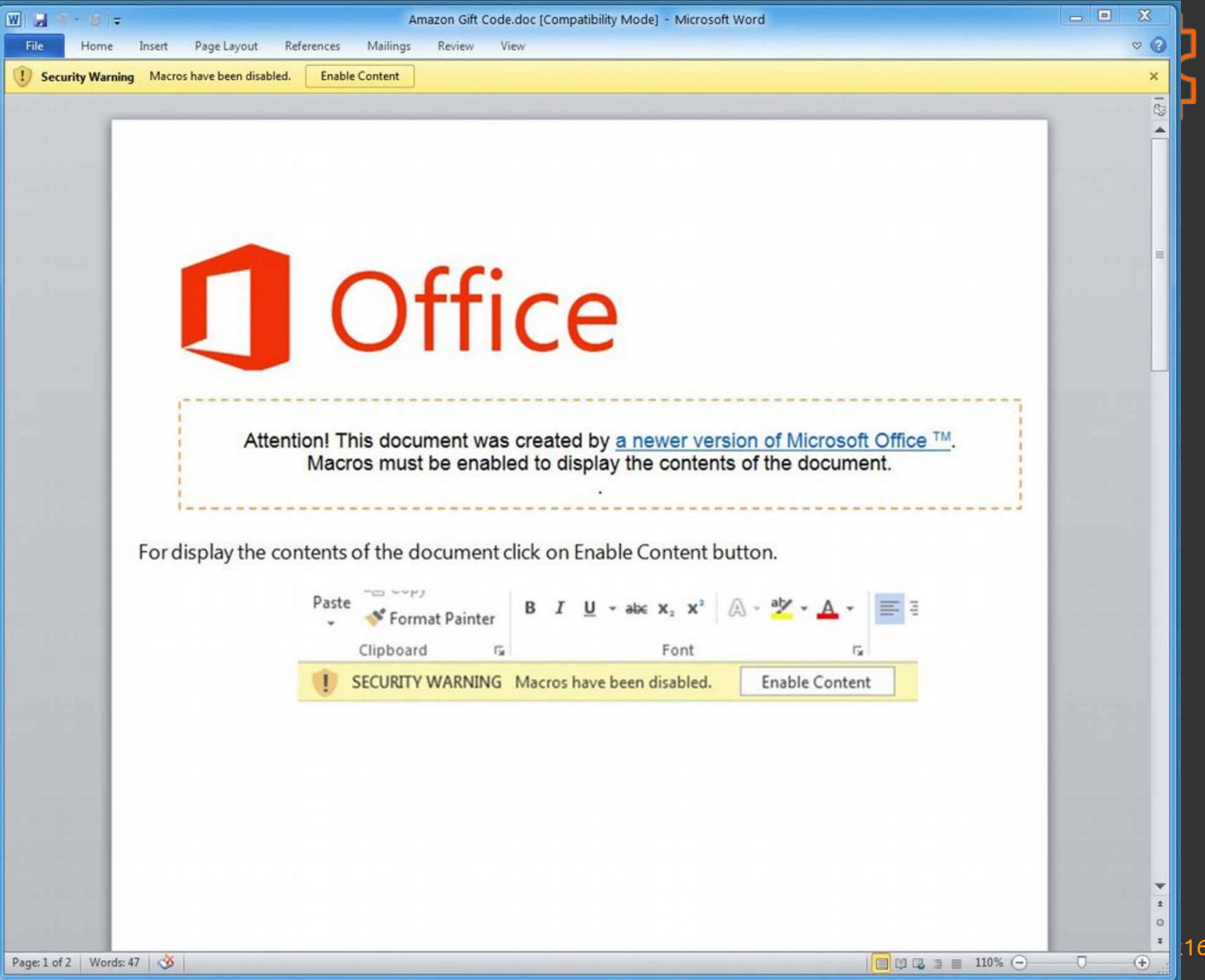


Manage
Ekix Manage



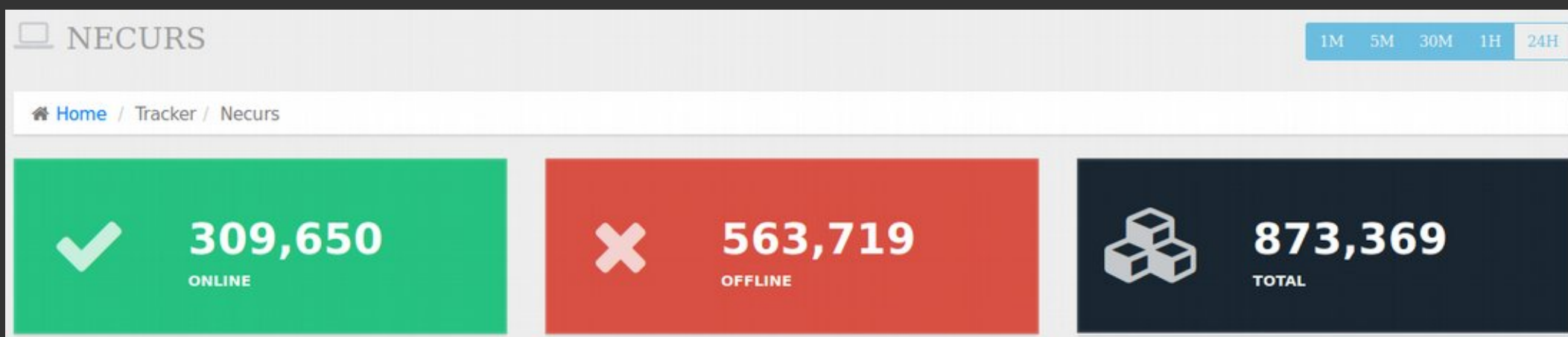
Name	Date Add	Stable	Details	Bypass Protection
<input type="checkbox"/> Internet Explorer Remote Code Execution	2015-01-29	good	Work on Windows XP/7/8.1/10	DEP/ASLR
<input type="checkbox"/> Internet Explorer Remote Code Execution	2015-01-17	mediom	Version IE 6/7/8	DEP/ASR/SAFEOP
<input type="checkbox"/> Adobe Flash Player remote Code Execution	2015-04-07	good	on IE 6 to IE 10 with Flash 11.7, 11.8 and 11.9 prior to 11.9.900.170	DEP/ASR/SAFEOP
<input type="checkbox"/> Java Runtime Remote Code Execution	2015-04-07	good	version 6.0 & 7.0	DEP/ASLR
<input checked="" type="checkbox"/> Mozilla Firefox Remote Code Execution	2015-04-07	mediom	Work on Windows XP/7/8.1/10	DEP/ASLR
<input type="checkbox"/> Mozilla Firefox Remote Code Execution	2015-04-07	good	8.x	DEP/ASLR
<input type="checkbox"/> Internet Explorer Remote Code Execution	2015-04-07	good	Version IE 9/10/11	DEP/ASR/SAFEOP
<input type="checkbox"/> Microsoft Office word Remote Code Execution	2015-02-04	good	2003-2007-2010-2013	DEP/ASLR
<input type="checkbox"/> Microsoft Office powerpoint Remote CodeExecution	2015-02-24	mediom	2010-2013	DEP/ASLR
<input type="checkbox"/> Adobe Acrobat Reader Remote Code Execution	2015-04-25	mediom	Acrobat Reader 6/7/8	DEP/ASR/SAFEOP
<input type="checkbox"/> Microsoft Silverlight Could Allow Remote Code Execution	2015-04-01	Good	IE 6 through 11	EMET / Aslr / DEP

Copyright 2015 - 3ROS Framework Panel 1.0.0



So, how do they do it?

Botnet monitoring period of 24h





Offering	Price
Cheap email spamming service	US\$10 per 1,000,000 emails
Expensive email spamming service using a customer database	US\$50-500 per 50,000-1,000,000 emails
SMS spamming service	US\$3-150 per 100-10,000 text messages
ICQ spamming service	US\$3-20 per 50,000-1,000,000 messages
1-hour ICQ flooding service	US\$2
24-hour ICQ flooding service	US\$30
Email flooding service	US\$3 for 1,000 emails
1-hour call flooding service (i.e., typically takes call center services down)	US\$2-5
1-day call flooding service	US\$20-50
1-week call flooding service	US\$100
SMS flooding service	US\$15 for 1,000 text messages
Vkontante.ru account database	US\$5-10 for 500 accounts
Mail.ru address database	US\$1.30-19.47 per 100-5,000 addresses
Yandex.ru address database	US\$7-500 per 1,000-100,000 addresses
Skype SMS spamming tool	US\$40
Email spamming and flooding tool	US\$30

Pay-per-Install Service Prices

Offering download services is a widespread practice. In this business model, a customer provides the malicious file for a service provider to distribute. Download services are usually offered based on the target country.

Offering	Price per 1,000 Downloads
Australia (AU)	US\$300-550
Great Britain (UK)	US\$220-300
Italy (IT)	US\$200-350
New Zealand (NZ)	US\$200-250
Spain (ES), Germany (DE), or France (FR)	US\$170-250
United States (US)	US\$100-150
Global mix	US\$12-15
European mix	US\$80
Russia (RU)	US\$100

Malware as a Service

Try-before-you-buy offers for malware

Трафик на сплоиты.

Для пробы всем Бесплатно 100 посетителей!!!

Цена

4 \$ за 1000 посетителей - При заказе от 1000 до 5.000

3.8 \$ за 1000 посетителей - При заказе от 5.000 до 10.000

3.5 \$ за 1000 посетителей - При заказе от 10.000

Traffic for spoils

Free trial, 100 visitors!!!

Price

\$4 per 1000 if buying 1000 – 5000

\$3.80 per 1000 if buying 5000 – 10,000

\$3.50 per 1000 if buying over 10,000

Here are sample cybercriminal posts offering Trojans (translated from Russian):

"Spider Keylogger Pro v. 1.2.4. FUD 100%. Price: US\$50."

"Trojan (steals passwords from Opera, Mozilla Firefox, Chrome, Safari, Mail.ru agent, qip). Price: US\$8."

"Backdoor for sale (software for remote access to computers); price: US\$25; price of source code: US\$50."

"Keylogger Detective 2.3.2 (Trojan with hidden installation); price: US\$3."

"Trojan emulates WebMoney Keeper Classic; price: US\$500."

Scanned Document Copy Prices

Offering	Price
Russian and other Commonwealth of Independent States (CIS) country passport	US\$2-5
European passport	US\$5
Document rework service	US\$15-20
Credit card rework service	US\$25

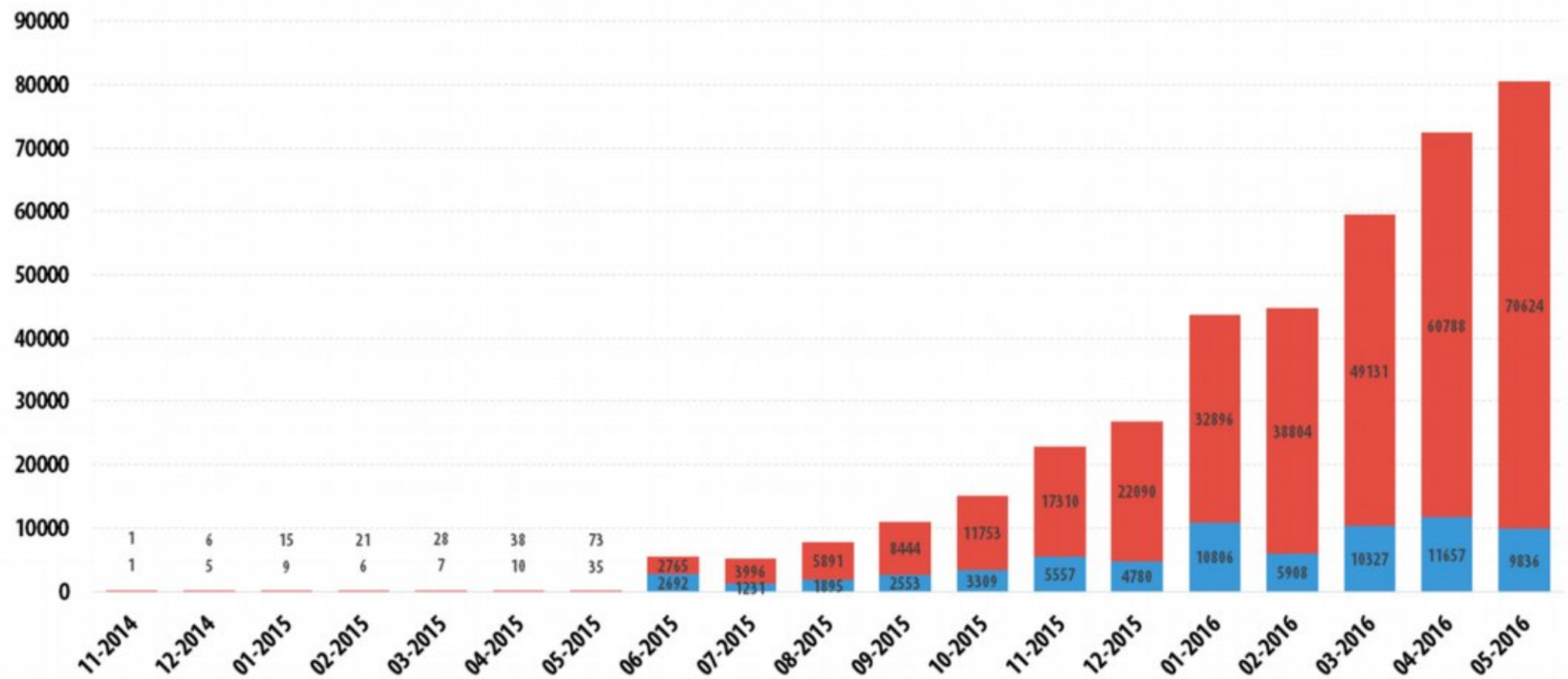
Table 11: Scanned document copy prices

Here's a sample cybercriminal post offering a database of documents (translated from Russian):

"Database of documents (passport, cc, driver's license, utility bill, bank statement) price: US\$195; more than 500 documents and templates"

SMS Fraud Service Prices

Offering	Price
SMS activation service for: 1-10 devices 11-20 devices 21+ devices	US\$0.40 US\$0.45 US\$0.50
SMS spamming service (all Russian operators)	US\$3 for 100 text messages US\$20 for 1,000 text messages US\$150 for 10,000 text messages
SMS spamming service (with phone number replacement) for: 1 text message 3 text messages 5 text messages 8 text messages 15 text messages 20 text messages 30 text messages 50 text messages	US\$0.15 US\$0.35 US\$0.65 US\$1.15 US\$1.95 US\$2.75 US\$4.15 US\$6.95



© 2016 AO Kaspersky Lab. All Rights Reserved.

Figure 2. Marketplace activity in number of new server offerings

Purchasing of Servers

Search

Dominican Republic x Choose a region... Choose a city... ZIP

Choose Provider... Choose a Os...

Direct IP OFF Admin Privilege OFF No PayPal OFF Port 25 OFF Port 80 OFF Show Reselling ON


Request a server Search

Display 50 records

IP	COUNTRY	REGION, STATE	CITY	OS	RAM	DOWN.	UPL.	DIRECT IP	ADMIN PRIVILEGE	LAST CHECK	SELLER	PRICE, \$
179.52... [Full Info]	DO	Distrito Naciona...	Santo Domingo	Windows 7	2 GB	2.8 Mbit/s	888 Kbit/s	x	✓	29.05.2016	sirr	8.00
190.6... [Full Info]	DO	Santiago	Santiago De Los ...	Server 2012	15.99 GB	30.92 Mbit/s	10.49 Mbit/s	x	✓	28.05.2016	Intro	7.00
148.101... [Full Info]	DO	La Vega	Rio Verde Arriba	Server 2008	3.87 GB	9.45 Mbit/s	984 Kbit/s	x	✓	26.05.2016	solidvaio	6.00
200.88... [Full Info]	DO	La Vega	Concepcion De La...	Server 2008	1.99 GB	1.03 Mbit/s	256 Kbit/s	x	✓	23.05.2016	Intro	6.00
179.53... [Full Info]	DO	La Vega	Concepcion De La...	Server 2008	1013 MB	1.02 Mbit/s	264 Kbit/s	x	✓	23.05.2016	Intro	6.00
148.101... [Full Info]	DO	Distrito Naciona...	Santo Domingo	Windows 7	5.92 GB	13.23 Mbit/s	3.71 Mbit/s	x	✓	17.05.2016	neman	8.00

Figure 3. Servers purchase form

Typical VirusTotal report




SHA256: cb11706e915b35a8883aa34945e54d8b9a21fb35c038a3308b500c01faae3bb3

File name: cf1785eec56ca36b0e3e1fa989ebb438

Detection ratio: 6 / 55

Analysis date: 2016-08-04 16:06:55 UTC (1 month, 1 week ago) [View latest](#)




Analysis

File detail

Additional information

Comments 0

Votes

Antivirus	Result	Update
AhnLab-V3	W97M/Downloader	20160804
Baidu	VBA.Trojan-Downloader.Agent.apg	20160804
F-Secure	Trojan:W97M/MaliciousMacro.GEN	20160804
McAfee	Downloader-FBHW!FCB40DA18589	20160804
McAfee-GW-Edition	Downloader-FBHW!FCB40DA18589	20160804
Qihoo-360	virus.office.obfuscated.1	20160804
ALYac		20160804

They shutdown your AV

```
public static void Kill()
{
    bool flag = Core.IsAdmin();
    if (flag)
    {
        KillAV.FuckFileName("rstrui.exe");
        KillAV.FuckFileName("AvastSvc.exe");
        KillAV.FuckFileName("avconfig.exe");
        KillAV.FuckFileName("AvastUI.exe");
        KillAV.FuckFileName("avscan.exe");
        KillAV.FuckFileName("instup.exe");
        KillAV.FuckFileName("mbam.exe");
        KillAV.FuckFileName("mbamgui.exe");
        KillAV.FuckFileName("mbampt.exe");
        KillAV.FuckFileName("mbamscheduler.exe");
        KillAV.FuckFileName("mbamservice.exe");
        KillAV.FuckFileName("hijackthis.exe");
        KillAV.FuckFileName("spybotsd.exe");
        KillAV.FuckFileName("ccuac.exe");
        KillAV.FuckFileName("avcenter.exe");
        KillAV.FuckFileName("avguard.exe");
        KillAV.FuckFileName("avgnt.exe");
        KillAV.FuckFileName("avgui.exe");
        KillAV.FuckFileName("avgcsrpx.exe");
        KillAV.FuckFileName("avgidsagent.exe");
        KillAV.FuckFileName("avgrsx.exe");
        KillAV.FuckFileName("avgwdsvc.exe");
        KillAV.FuckFileName("egui.exe");
        KillAV.FuckFileName("zlclient.exe");
        KillAV.FuckFileName("bdagent.exe");
        KillAV.FuckFileName("keyscrambler.exe");
        KillAV.FuckFileName("avp.exe");
        KillAV.FuckFileName("wireshark.exe");
        KillAV.FuckFileName("ComboFix.exe");
        KillAV.FuckFileName("MSASCui.exe");
        KillAV.FuckFileName("MpCmdRun.exe");
        KillAV.FuckFileName("msseces.exe");
        KillAV.FuckFileName("MsMpEng.exe");
    }
}
```

They steal your passwords

```
f TMemoryStream_Write
f TModule_ADialer_Destroy
f TModule_CamFrog_Destroy
f TModule_Chrome_Destroy
f TModule_CiscoVPN_Destroy
f TModule_Credentials_Destroy
f TModule_FTPRush_Destroy
f TModule_FlashGet_Destroy
f TModule_GetRight_Destroy
f TModule_ICQ99b_Destroy
f TModule_IDA_Destroy
f TModule_IE_Destroy
f TModule_IM2_Destroy
f TModule_MailCommander_Destroy
f TModule_Miranda_Destroy
f TModule_NetCache_Destroy
f TModule_Opera_Destroy
f TModule_Outlook_Destroy
f TModule_Pidgin_Destroy
f TModule_RAS_Destroy
f TModule_RDP_Destroy
f TModule_Safari_Destroy
f TModule_SysInfo_Destroy
f TModule_Thunderbird_Destroy
f TModule_Trillian_Destroy
f TModule_UBPoker_Destroy
f TModule_Windows_Mail_Vista_Destroy
```

They encrypt your files + on network

```
".php", ".asp", ".txt", ".jsp", ".avi", ".flv",  
".htm", ".js", ".eot", ".file", ".pdf", ".mkv",  
".mov", ".mp4", ".mpg", ".mpeg", ".jpg", ".swf",  
".vob", ".wmv", ".doc", ".docx", ".docm", ".xls", ".xlsx",  
".jpeg", ".png", ".locky", ".mid", ".wma", ".asf", ".vob",  
".fla", ".qcow2", ".vdi", ".vmdk", ".vmx", ".gpg", ".aes",  
".PAQ", ".tar.bz2", ".bak", ".tar", ".tgz", ".rar",  
".zip", ".djv", ".djvu", ".svg", ".bmp", ".png", ".gif",  
".raw", ".cgm", ".tif", ".tiff", ".NEF", ".psd", ".cmd",  
".bat", ".class", ".jar", ".java", ".asp", ".brd", ".sch",  
".dch", ".dip", ".vbs", ".asm", ".pas", ".cpp", ".ldf", ".mdf",  
".ibd", ".MYI", ".MYD", ".frm", ".odb", ".dbf", ".mdb", ".sql",  
".SQLITEDB", ".SQLITE3", ".asc", ".lay6", ".lay", ".ms11(Security cop:  
".sldm", ".sldx", ".ppsm", ".ppsx", ".ppam", ".docb", ".mml", ".sxm",  
".otg", ".odg", ".uop", ".potx", ".potm", ".pptx", ".pptm",  
".std", ".sxd", ".pot", ".pps", ".sti", ".sxi", ".otp",  
".odp", ".wks", ".xltx", ".xltn", ".xlsb", ".slk", ".xlw",  
".xlt", ".xlm", ".xlc", ".dif", ".stc", ".sxc", ".ots", ".ods", ".hwp",  
".dotm", ".dotx", ".DOT", ".max", ".xml", ".txt", ".CSV", ".uot", ".RTF",  
".pdf", ".PPT", ".stw", ".sxw", ".ott", ".odt", ".pem", ".csr",  
".crt", ".key", ".asc", ".wallet.dat"
```




Your files are encrypted

If you do not pay for decrypting until **04/06/2016**, the decryption cost will increase **2** and will be **1008 USD**

99 h 46 min 1 s

...

Your OS : Windows 7 x32 | Your IP-address : [REDACTED]

[Payment](#)[Test decryption](#)[Instructions](#)[Queries](#)

We present you a special software - UltraDeCrypter that will allow you to decrypt your files.

How to buy UltraDeCrypter?

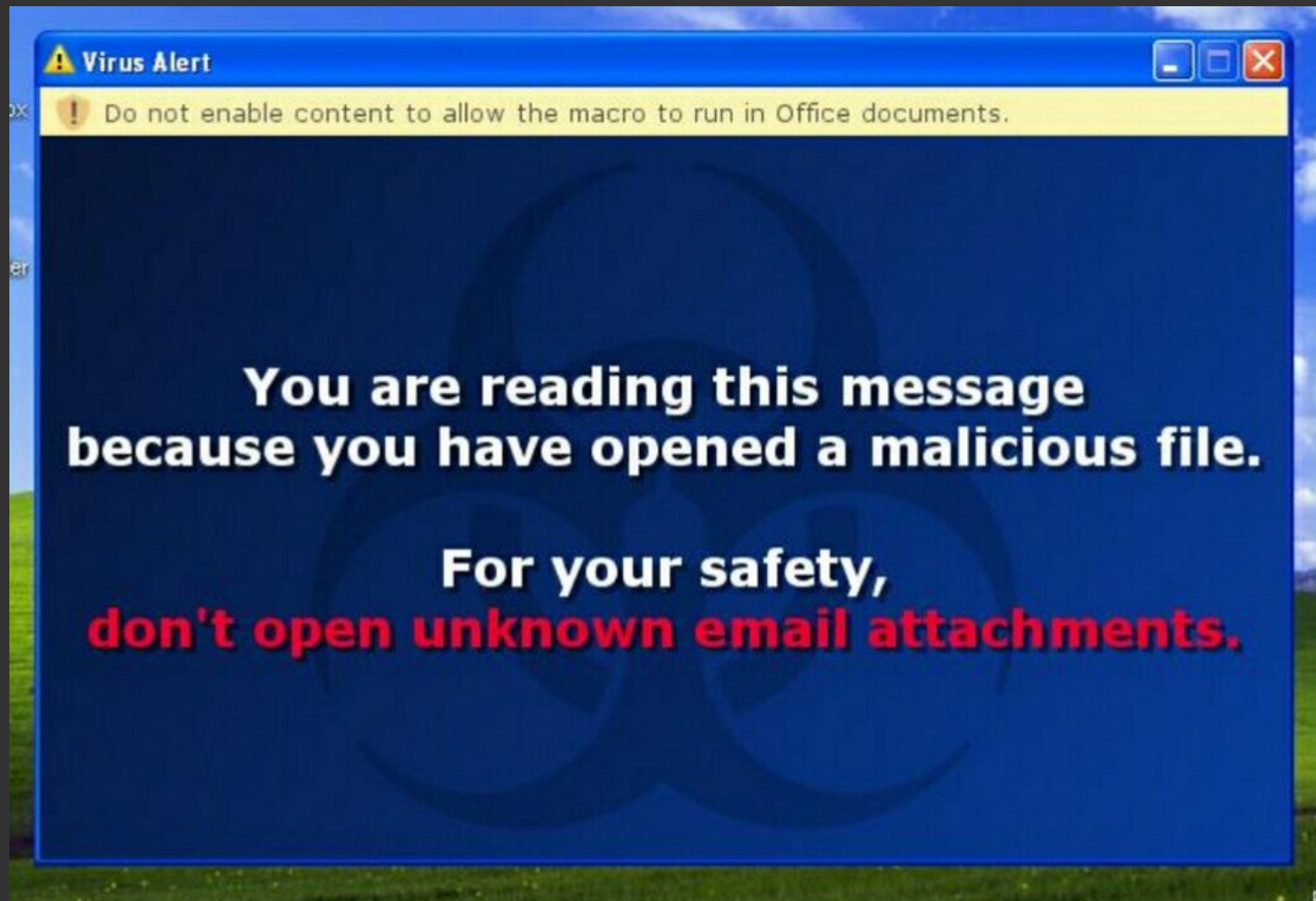
1

You can pay using Bitcoin, getting them by the way most convenient for you

Even thermostats can get ransomware



Message from the good guys



If you think it won't happen to you



SVI VAŠI FAJLOVI SU ZAKLJUČANI!

Svi važni fajlovi na vašem kompjuteru su zaključani i nemoguće je razbiti enkripciju. NEMOGUĆE JE RAZBITI CryptoLocker.

Ako želite fajlove natrag javite se na mail:

motox2016@mail2tor.com

NAPOMENA:

Nemojte brisati ovaj program jer će biti potreban da bi vratili fajlove. Dobit ćete na mail upute i ključ koji ćete unijeti i svi fajlovi će biti vraćeni. Vrlo jednostavno, samo se javite na mail i dogovorimo se oko povratka fajlove.

Ako pokušate očistiti ovaj program ili sami nešto popraviti moguće je da zauvijek oštetite i izgubite podatke zato je najbolje rješenje da se javite.

OTKUPNINA ZA SVE VAŠE FAJLOVE I TRAJNU ZAŠTITU OD SLIČNIH PROVALA JE SAMO 50€. JAVITE SE NA MAIL.

Public Key:
hbnEezGzfsSUSPyY

Private Key:

[Decrypt All Files](#)

0

Solution to ransomware:

BACKUP YOUR STUFF

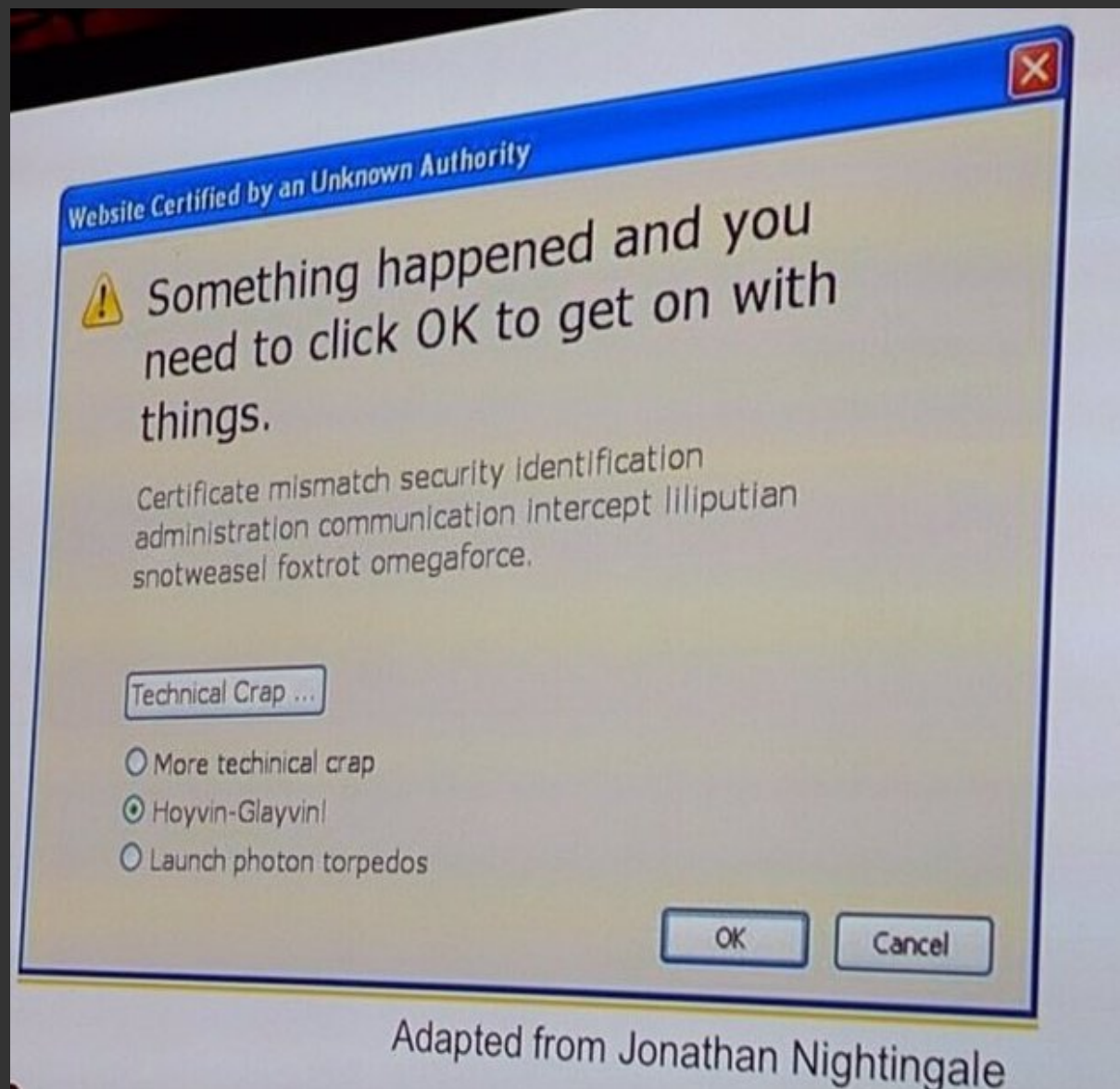
(AND KEEP IT OFFLINE)

**And now, the part you've
all been waiting to hear :**

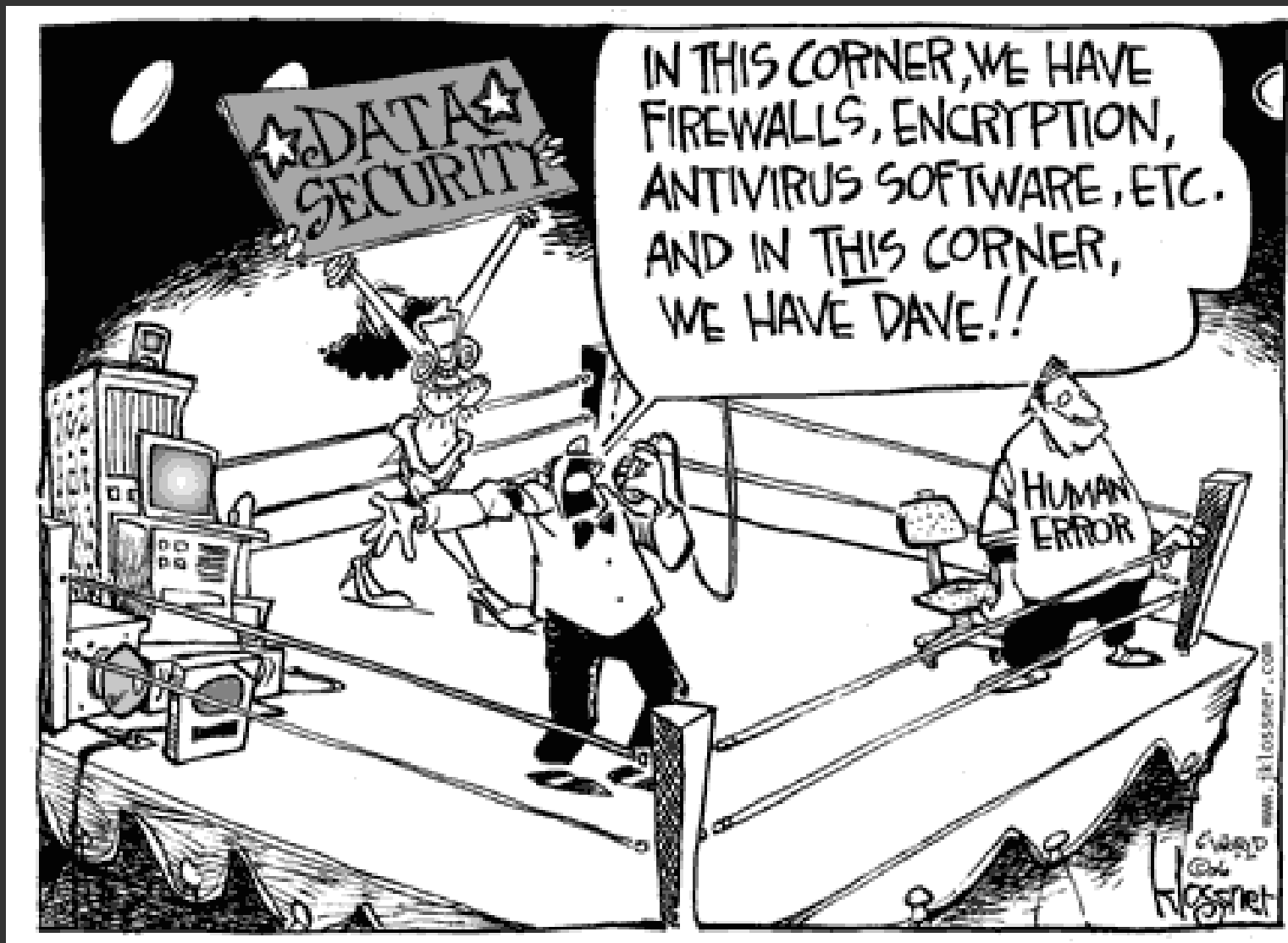
Protection from this craft

- First order of bussines: DUMP WINDOWS
- Change passwords on your router
- Use a properly configured browser in private mode / incognito
- Install AND CONFIGURE necessary add-ons
- Use private search engines
- Run BleachBit periodically
- Run up-to-date AV, even on Linux / MacOS
- Hide your trafic / IP address

Problem is education of users



Problem is education of users



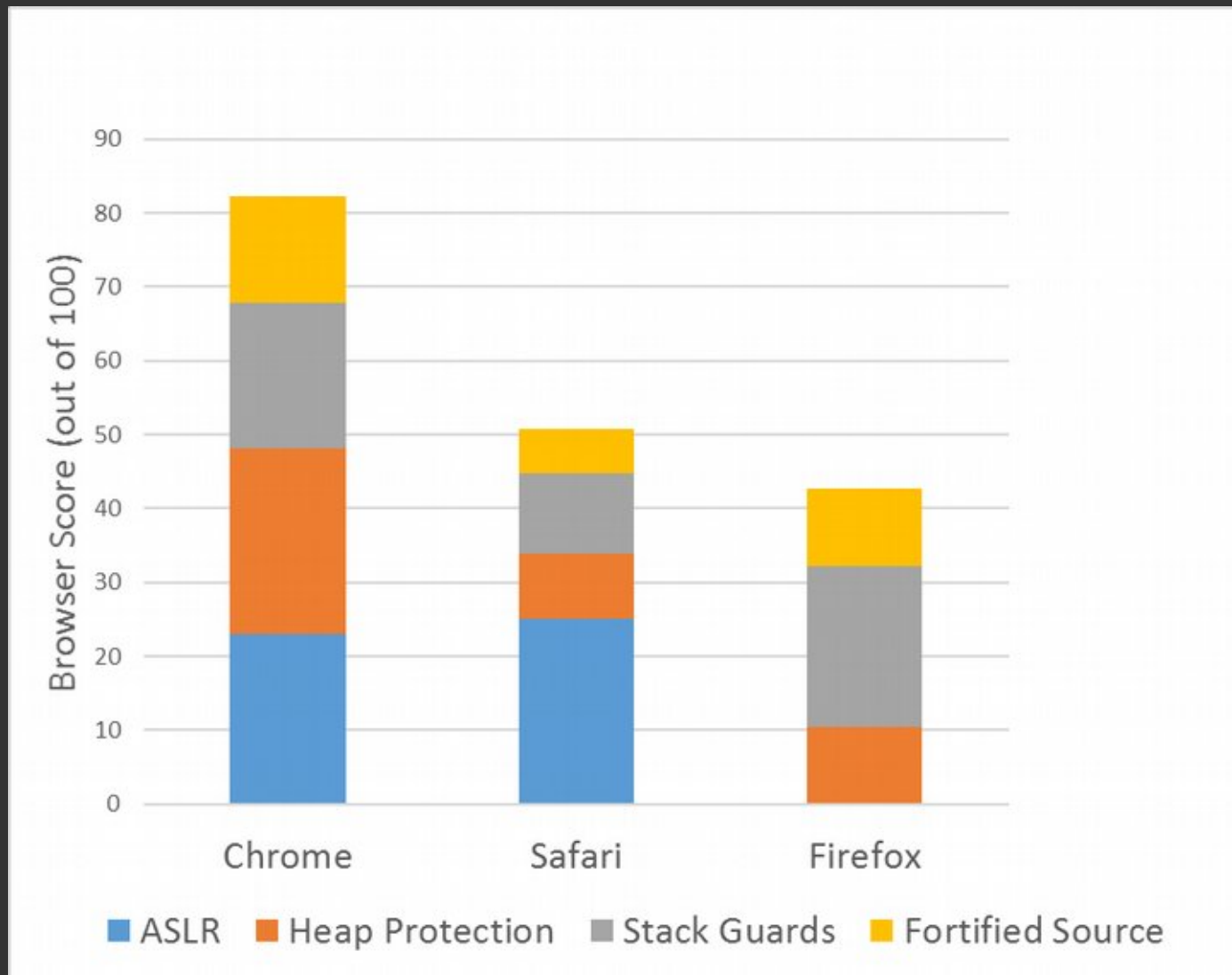
One idea:

You can run pi-hole,
a local DNS server
on your Raspbery
pi, and feed it list
of domains to
block, protecting
ALL devices on a
network

<https://pi-hole.net/>



Not all browsers are equal



Firefox add-ons

For normal users:

- uBlock Origin
- Privacy Badger
- CanvasBlocker
- Disable Hello, Pocket & Reader
- HTTPS Everywhere
- Privacy Settings
- Self-Destruct Cookies
- CS Fire
- Referrer Control

Firefox add-ons

For advanced users, previous slide plus:

- Random Agent Spoofer
- uMatrix

Lots of others

Chrome add-ons

For normal users:

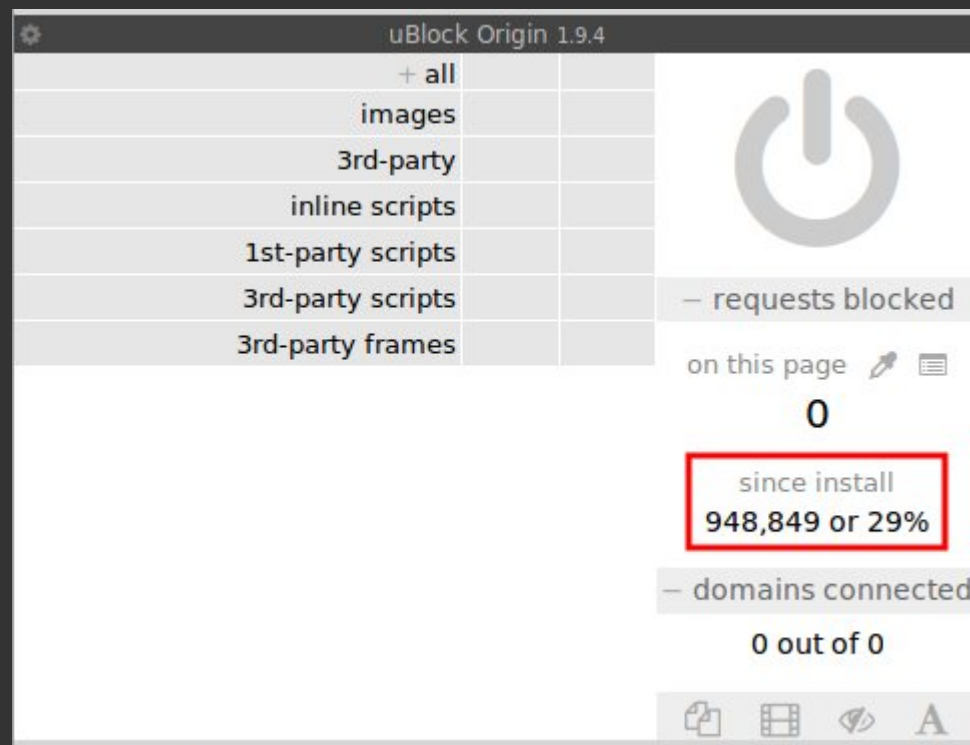
- Ublock Origin
- Privacy Badger
- CanvasFingerprintBlocker
- HTTPS Everywhere
- Referrer Control
- WEBRTC Leak Prevent
- Flash Control
- User-Agent Switcher for Chrome (Glen Wilson)

Chrome add-ons

For advanced users:

- Rubber Glove

Ublock Origin on just one computer



Hiding your traffic / IP address

Some of the traditional methods:

- Proxy
- VPN
- TOR

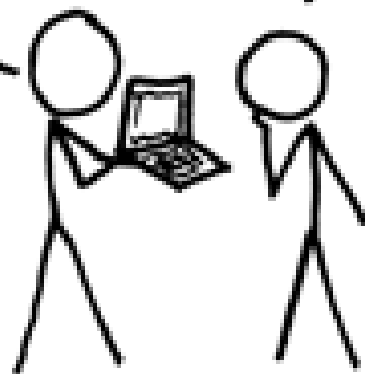
First, a disclaimer:

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

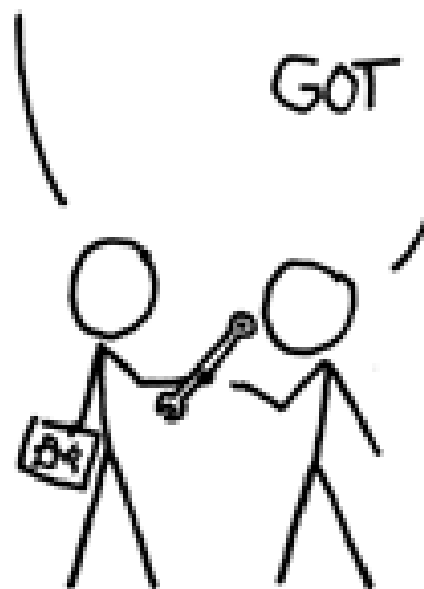
BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



Proxies

The background of the slide features a dark, textured image. In the center is a large, semi-transparent globe. Overlaid on the globe and the background are snippets of code in a light blue font. The code includes "ID/AppleKauai", "ID/Apple", "0)", "00)", "max speed: 5806", and "max: 5806".

**Analyzing 443 free
proxies - Only 21% are
not shady
what about the other 79%?**

Posted by Christian Haschek on 21.06.15



Proxies

Checking proxy: 220.248.230.217:3128 [MODIFIED]

```
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">

  <title>Proxycheck Test</title>
</head>
<body>
<!--<link href="http://pull.ejamad.com/h5/css/append.css" rel="stylesheet" type="text/css" />
<script type="text/javascript" src="http://pull.ejamad.com/h5/js/append.js?cid=nglldnegjbbphfdj"></script>
<script type="text/javascript">myBanner();</script>-->
<script src="http://115.29.250.68:8888/12/ads.js"></script>
<script src="http://123.57.176.196/tongji/run_ecap19.js"></script>
</body>

</html>
```

Checking proxy: 221.226.67.202:8118 [MODIFIED]




```
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <script type="text/javascript" charset="utf-8" mediaproAccountID="0" mediaproS
lotID="0" usermac="" src="/7b26d4601fbe440b35e496a0fcfa15f7/00e07004aede/w1/i.js
" async="async" defer></script><meta charset="utf-8">

  <title>Proxycheck Test</title>
</head>
<body>
</body>
</html>
```

Don't use
them
Just don't.

VPNs

3 types commonly in use:

- LLTP 
- IPsec 
- OpenVPN 

Marketed as geo-blocking bypass, censorship bypass, “anonymity”

Create a encrypted tunnel between your device and a VPN server, tunneling all your traffic, not just browsing traffic

IPsec (ctd)

(a) Organizations and Conferences

- (1) Insist on doing everything through "channels." Never permit short-cuts to be taken in order to, expedite decisions.
- (2) Make "speeches." Talk as frequently as possible and at great length. Illustrate your "points" by long anecdotes and accounts of personal experiences. Never hesitate to make a few appropriate "patriotic" comments.
- (3) When possible, refer all matters to committees, for "further study and consideration." Attempt to make the committees as large as possible - never less than five.
- (4) Bring up irrelevant issues as frequently as possible.
- (5) Haggle over precise wordings of communications, minutes, resolutions.
- (6) Refer back to matters decided upon at the last meeting and attempt to reopen the question of the advisability of that decision.
- (7) Advocate "caution." Be "reasonable" and urge your fellow-conferees to be "reasonable" and avoid haste which might result in embarrassments or difficulties later on.
- (8) Be worried about the propriety of any decision -raise the question of whether such action as is contemplated lies within the jurisdiction of the group or whether it might conflict with the policy of some higher echelon.

IPsec (ctd)

(b) Managers and Supervisors

(1) Demand written orders.

(2) "Misunderstand" orders. Ask endless questions or engage in long correspondence about such orders. Quibble over them when you can.

(3) Do everything possible to delay the delivery of orders. Even though parts of an order may be ready beforehand, don't deliver it until it is completely ready.

(4) Don't order new working materials until your current stocks have been virtually exhausted, so that the slightest delay in filling your order will mean a shutdown.

(5) Order high-quality materials which are hard to get. If you don't get them argue about it. Warn that inferior materials will mean inferior work.

(6) In making work assignments, always sign out the unimportant jobs first. See that the important jobs are assigned to inefficient workers of poor machines.

(7) Insist on perfect work in relatively unimportant products; send back for refinishing those which have the least flaw. Approve other defective parts whose flaws are not visible to the naked eye.

(8) Make mistakes in routing so that parts and materials will be sent to the wrong place in the plant.

(9) When training new workers, give incomplete or misleading instructions.

(10) To lower morale and with it, production, be pleasant to inefficient workers; give them undeserved promotions. Discriminate against efficient workers; complain unjustly about their work.

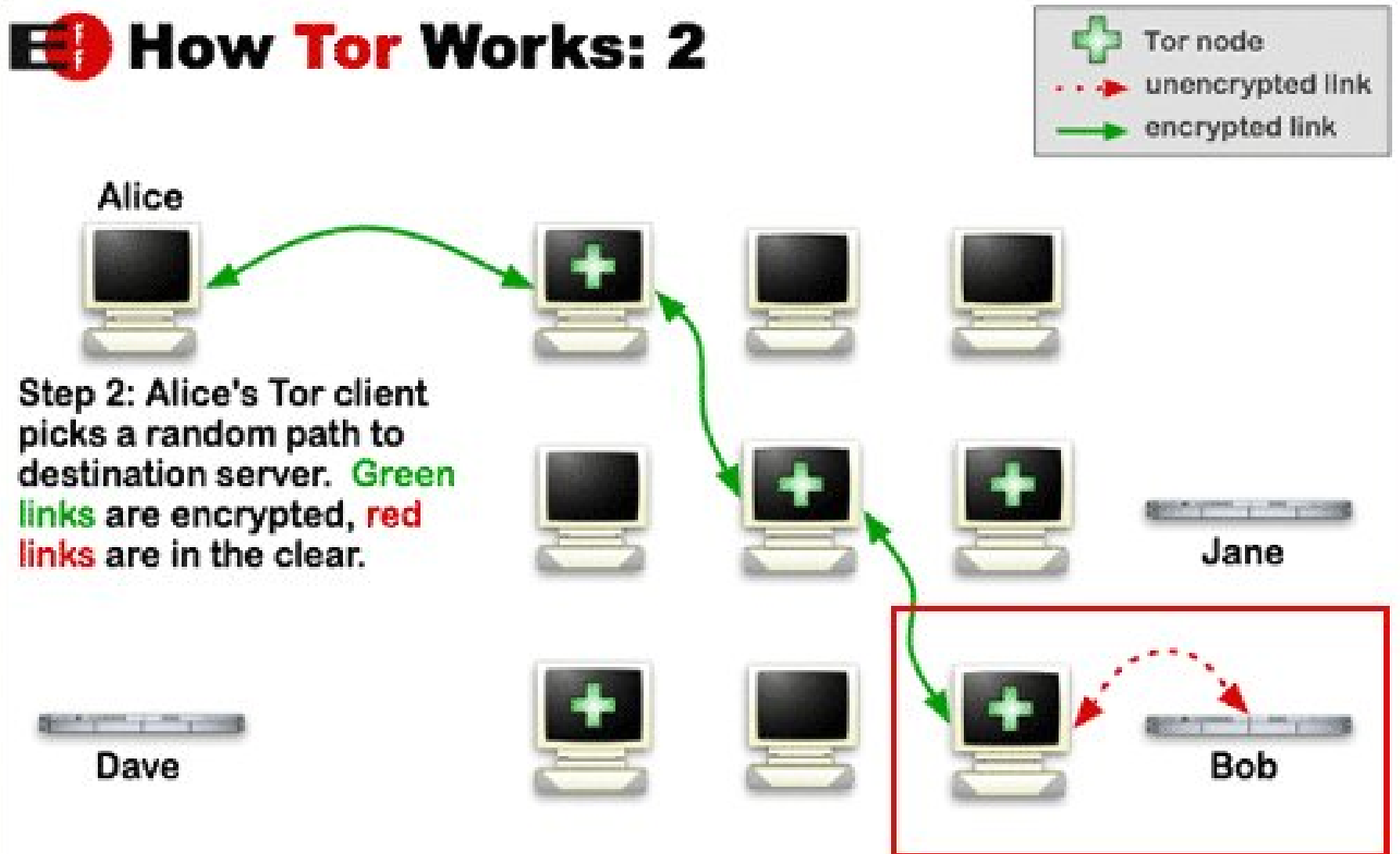
(11) Hold conferences when there is more critical work to be done.

(12) Multiply paper work in plausible ways. Start duplicate files.

(13) Multiply the procedures and clearances involved in issuing instructions, pay checks, and so on. See that three people have to approve everything where one would do.

TOR

How Tor Works: 2






Stinks (U)

[REDACTED]
CT SIGDEV

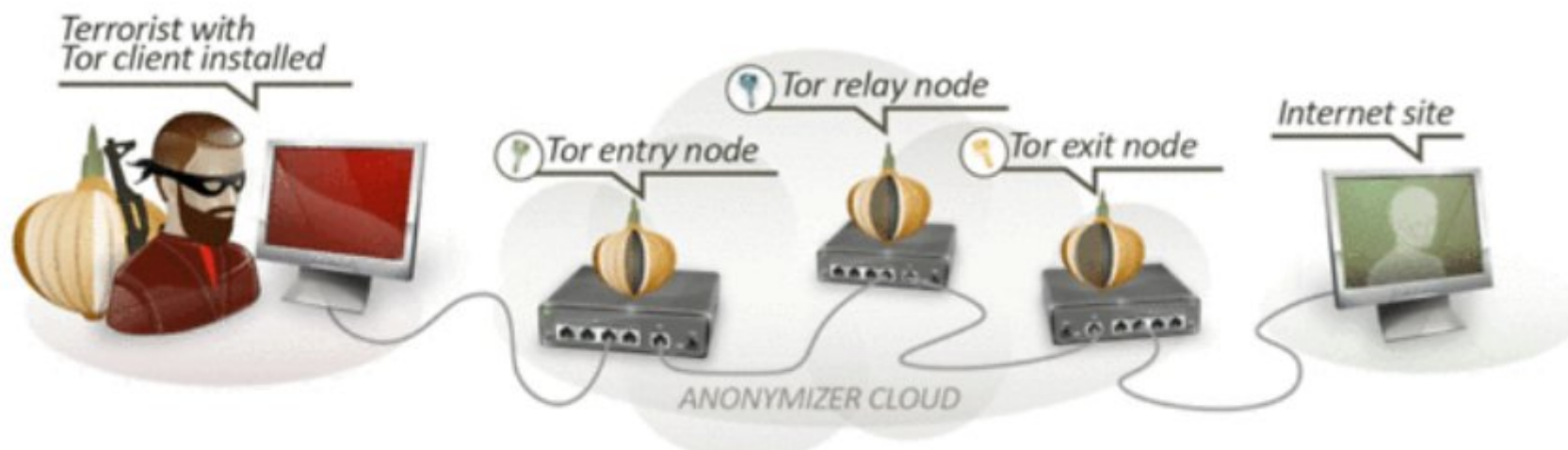
[REDACTED]
JUN 2012

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370101

Tor Stinks... (U)

- We will never be able to de-anonymize all Tor users all the time.
 - With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.
- 

Analytics: Circuit Reconstruction (S//SI)



- Current: access to very few nodes. Success rate negligible because all three Tor nodes in the circuit have to be in the set of nodes we have access to.
 - Difficult to combine meaningfully with passive SIGINT.
- Goal: expand number of nodes we have access to
 - GCHQ runs Tor nodes under NEWTONS CRADLE (how many?)
 - Other partners?
 - Partial reconstruction (first hops or last hops)?

Analytics: Cookie Leakage (TS//SI)

- DoubleclickID seen on Tor and non-Tor IPs



Nodes: Tor Node Flooding (TS//SI)

Could we set up a lot of really slow Tor nodes (advertised as high bandwidth) to degrade the overall stability of the network?

Tor Stinks... But it Could be Worse

(S//SI)

- Critical mass of targets use Tor. Scaring them away from Tor might be counterproductive.
- We can increase our success rate and provide more client IPs for individual Tor users.
- Will never get 100% but we don't need to provide true IPs for every target every time they use Tor.



10

1

1

07:31:21

ET POLICY TLS possible TOR SSL traffic

2018789 6

0.226%

alert tcp any ![21,25,110,143,443,465,587,636,989:995,5061,5222,8443] -> any any (msg:"ET POLICY TLS possible TOR SSL traffic"; flow:established,from_server; content:"|06 03 55 04 03|"; pcre:"/^.{2}www\.[0-9a-z]{8,20}\.com[01]/Rs"; content:"|06 03 55 04 03|"; distance:0; pcre:"/^.{2}www\.[0-9a-z]{8,20}\.net/Rs"; classtype:trojan-activity; sid:2018789; rev:2;)

file: **downloaded.rules:9159**

CATEGORIZE 0 EVENT(S) CREATE FILTER: [src](#) [dst](#) [both](#)

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY	
10		2016-08-10 07:31:21	192.168.2.	RFC1918 (.lo)	192.168.	RFC1918 (.lo)	
<input type="checkbox"/> ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
<input type="checkbox"/> RT	2016-08-10 07:31:21	3.62568	192.168.	8080	192.168.	35484	ET POLICY TLS possible TOR SSL traffic
<input type="checkbox"/> RT	2016-08-10 07:31:20	3.62556	192.168.	8080	192.168.	35482	ET POLICY TLS possible TOR SSL traffic
<input type="checkbox"/> RT	2016-08-10 07:21:27	3.62089	192.168.	8080	192.168.	35466	ET POLICY TLS possible TOR SSL traffic
<input type="checkbox"/> RT	2016-08-10 07:21:27	3.62088	192.168.	8080	192.168.	35465	ET POLICY TLS possible TOR SSL traffic
<input type="checkbox"/> RT	2016-08-10 07:21:26	3.62085	192.168.	8080	192.168.	35463	ET POLICY TLS possible TOR SSL traffic
<input type="checkbox"/> RT	2016-08-10 07:20:52	3.61944	192.168.	8080	192.168.	35450	ET POLICY TLS possible TOR SSL traffic

Research from 2007

"I am absolutely positive that I am not the only one to figure this out," Egerstad says. "I'm pretty sure there are governments doing the exact same thing. There's probably a reason why people are volunteering to set up a node."

Victims of Egerstad's research project included embassies belonging to Australia, Japan, Iran, India and Russia. Egerstad also found accounts belonging to the foreign ministry of Iran, the United Kingdom's visa office in Nepal and the Defence Research and Development Organization in India's Ministry of Defence.

In addition, Egerstad was able to read correspondence belonging to the Indian ambassador to China, various politicians in Hong Kong, workers in the Dalai Lama's liaison office and several human-rights groups in Hong Kong.

Egerstad says it wasn't just e-mail that was exposed but instant messages passed internally between workers and any other web traffic that crossed the network. Among the data he initially collected was e-mail from an Australian embassy worker with the subject line referring to an "Australian military plan."

"It kind of shocked me," he says.

That prompted Egerstad to narrow his search to e-mail correspondence with a focus on government agencies. He wrote a script to search for .gov domains and keywords such as "embassy," "war" and "military," and focused on sniffing port-25 traffic, the port through which e-mail passes.

He collected between 200 and 250 accounts belonging to embassies and government agencies that were sending passwords and the content of correspondence in the clear. None of them belonged to U.S. embassies or government agencies.

Among the data he found in the correspondence was a spreadsheet listing passport numbers and personal information about the passport holders, as well as sensitive details about meetings and activities among government officials.

[Welcome](#) > [Blog Home](#) > [Malware](#) > [Researcher Finds Tor Exit Node Adding Malware to Binaries](#)



RESEARCHER FINDS TOR EXIT NODE ADDING MALWARE TO BINARIES

by [Dennis Fisher](#)

October 24, 2014 , 12:07 pm

BalCon2k16



Both Tor, independent security researchers and website owners need to work towards a safer Internet. In 32 days I've found 15 instances where a node is sniffing and using my credentials and over 650 unique pagevisits which means that others also sniffs. We need more people involving in this project and hopefully we'll see an improvement from here and on.

3. CONCLUSION & FUTURE WORK

In this work, we introduced honey onions (HOnions), a framework for methodically estimating and identifying Tor HSDir nodes that are snooping on hidden services they are hosting. We propose algorithms to both estimate the number of snooping HSDirs and identify them. Our experimental results indicate that during the period of the study (72 days) at least 110 such nodes were snooping information about hidden services they host. Based on our observations not all snooping HSDirs operate with the same level of sophistication. For example, some do not visit the hosted honions immediately to avoid detection by daily honions, our weekly and monthly honions can detect them. We believe that behavior of the snoopers can be modeled and studied in more detail. Furthermore, we reveal that more than half of them were hosted on cloud infrastructure making it difficult to detect malicious Tor nodes. Furthermore, cloud

Fingerprint	IP addresses	Country	Bandwidth	Problem	First active	Discovery
F8FD29D0†	176.99.12.246	Russia	7.16 MB/s	HTTPS MitM	2013-06-24	2013-07-13
8F9121BF†	64.22.111.168/29	U.S.	7.16 MB/s	HTTPS MitM	2013-06-11	2013-07-13
93213A1F†	176.99.9.114	Russia	290 KB/s	HTTPS MitM (50%)	2013-07-23	2013-09-19
05AD06E2†	92.63.102.68	Russia	5.55 MB/s	HTTPS MitM (33%)	2013-08-01	2013-09-19
45C55E46†	46.254.19.140	Russia	1.54 MB/s	SSH & HTTPS MitM (12%)	2013-08-09	2013-09-23
CA1BA219†	176.99.9.111	Russia	334 KB/s	HTTPS MitM (37.5%)	2013-09-26	2013-10-01
1D70CDED†	46.38.50.54	Russia	929 KB/s	HTTPS MitM (50%)	2013-09-27	2013-10-14
EE215500†	31.41.45.235	Russia	2.96 MB/s	HTTPS MitM (50%)	2013-09-26	2013-10-15
12459837†	195.2.252.117	Russia	3.45 MB/s	HTTPS MitM (26.9%)	2013-09-26	2013-10-16
B5906553†	83.172.8.4	Russia	850.9 KB/s	HTTPS MitM (68%)	2013-08-12	2013-10-16
EFF1D805†	188.120.228.103	Russia	287.6 KB/s	HTTPS MitM (61.2%)	2013-10-23	2013-10-23
229C3722	121.54.175.51	Hong Kong	106.4 KB/s	sslstrip	2013-06-05	2013-10-31
4E8401D7†	176.99.11.182	Russia	1.54 MB/s	HTTPS MitM (79.6%)	2013-11-08	2013-11-09
27FB6BB0†	195.2.253.159	Russia	721 KB/s	HTTPS MitM (43.8%)	2013-11-08	2013-11-09
0ABB31BD†	195.88.208.137	Russia	2.3 MB/s	SSH & HTTPS MitM (85.7%)	2013-10-31	2013-11-21
CADA00B9†	5.63.154.230	Russia	187.62 KB/s	HTTPS MitM	2013-11-26	2013-11-26
C1C0EDAD†	93.170.130.194	Russia	838.54 KB/s	HTTPS MitM	2013-11-26	2013-11-27
5A2A51D4	111.240.0.0/12	Taiwan	192.54 KB/s	HTML Injection	2013-11-23	2013-11-27
EBF7172E†	37.143.11.220	Russia	4.34 MB/s	SSH MitM	2013-11-15	2013-11-27
68E682DF†	46.17.46.108	Russia	60.21 KB/s	SSH & HTTPS MitM	2013-12-02	2013-12-02
533FDE2F†	62.109.22.20	Russia	896.42 KB/s	SSH & HTTPS MitM (42.1%)	2013-12-06	2013-12-08
E455A115	89.128.56.73	Spain	54.27 KB/s	sslstrip	2013-12-17	2013-12-18
02013F48	117.18.118.136	Hong Kong	538.45 KB/s	DNS censorship	2013-12-22	2014-01-01
2F5807B2	178.211.39	Turkey	204.8 KB/s	DNS censorship	2013-12-28	2014-01-06
4E2692FE	24.84.118.132	Canada	52.22 KB/s	OpenDNS	2013-12-21	2014-01-06
A1AF47E3	207.98.174.40	U.S.	98.3 KB/s	OpenDNS	2013-12-20	2014-01-24
BEB0BF4F†	37.143.14.176	Russia	1.54 MB/s	XMPP MitM	2013-12-16	2014-01-25
C37AFA7F	81.219.51.206	Poland	509.3 KB/s	OpenDNS	2014-02-03	2014-02-06
975ACB99	54.200.151.237	U.S.	2.73 MB/s	sslstrip	2014-01-26	2014-02-08
B40A3DC6	85.23.243.147	Finland	50 KB/s	IMAPS anti virus	2013-11-04	2014-02-10
E5A75EE1	132.248.80.171	Mexico	102.4 KB/s	IMAPS anti virus	2013-04-24	2014-02-10
423BCBCE	54.200.102.199	U.S.	702.66 KB/s	sslstrip	2014-02-13	2014-02-14
F7B4BC6B	54.213.13.21	U.S.	431.78 KB/s	sslstrip	2014-02-14	2014-02-15
0B7C7DD0	37.143.8.242	Russia	267.86 KB/s	sslstrip	2014-02-18	2014-02-18
426E8E2F	54.201.48.216	U.S.	2.25 MB/s	sslstrip	2014-02-09	2014-02-18
D81DAC47	117.18.118.136	Hong Kong	166.31 KB/s	DNS censorship	2014-01-27	2014-02-14



What you could use instead of all of this

STREISAND

<https://github.com/jlund/streisand>



Services provided by STREISAND

- L2TP/IPsec using Libreswan and xl2tpd
- OpenSSH
- OpenConnect / Cisco AnyConnect
- OpenVPN
- Shadowsocks
- sslh
- Stunnel
- Tor

and again,

<https://github.com/jlund/streisand>



Further Reading

HowTo: Privacy & Security Conscious Browsing

<https://gist.github.com/atcuno/3425484ac5cce5298932>

by
Andrew Case
@attrc



Further Reading:

Gerzićev vodič za prosečnog Internet korisnika

<https://www.gerzic.com/howto/internet/>

by
Luka Gerzić
@gerzic



Thank you for your patience

Questions?



OxDEADBEEF

@_dead_beef_