F-SECURE @REGIONAL CONFERENCE ON CYBERCRIME 2017


WE ARE
F-SECURE
F-Secure.

F-Secure.

F-Secure in Malaysia

Since 2006

MSC status in May 2006

200+ employees

- R&D, software development
- Malware detection (AMU)
- Technical Support
- Finance services
- Sales and Marketing services


OVER 29 YEARS
OF DIGITAL SECURITY EXPERIENCE
F-Secure.

CNN Philippines

Search CNN Philippines

Home | The Presidency | News | Business | Entertainment | Regional | Sports | World | Life | Videos | Transportation

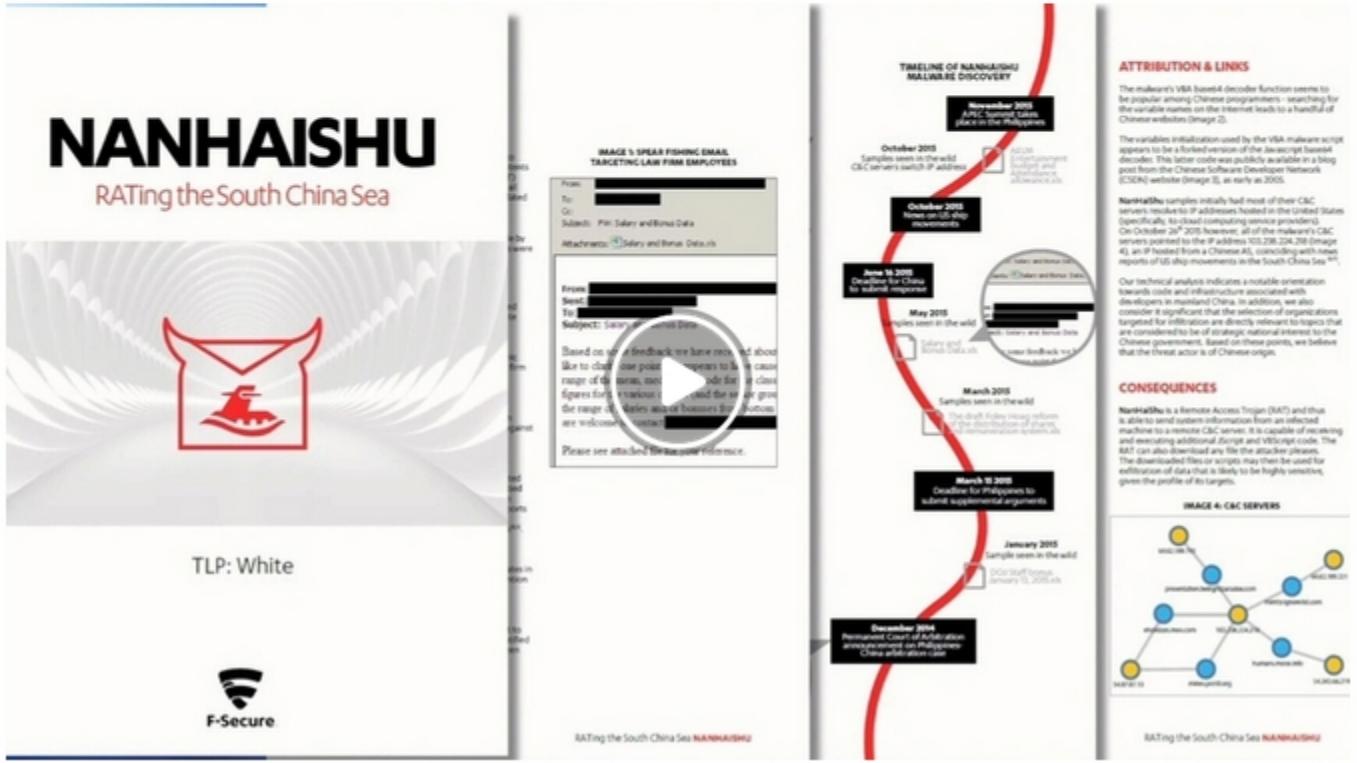
FRONT PAGE / NEWS

Suspected Chinese malware used to spy on PH gov't – security firm

By JC Gotinga, Lara Tan, CNN Philippines

Updated 22:54 PM PHT Fri, August 5, 2016

7.2K 76



More From CNN Philippines

Supreme Court allows parts of travel ban to go

Jason Ivler found guilty of murder, sentenced to

NANHAISHU

RATing the South China Sea


"Based on the organizations that have been targeted by this particular threat, it definitely seems to be of Chinese origin and those that are interested in that kind of issue would most likely be the Chinese government."
VOICE OF:
KARMINA AQUINO
Senior Manager
F-SECURE THREAT INTELLIGENCE TEAM
WEB SECURITY FIRM: CHINA 'LIKELY' SPYING ON PH
HEADLINES
REBEL WILSON TO STAR IN 'DIRTY ROTTEN SCOUNDRELS' REMAKE
NETWORK NEW


THREAT LANDSCAPE
GETTING MORE COMPLEX BY THE DAY
F-Secure.

2016 – H1 2017 Observed Threats

Malicious macro document

Ransomware Festival

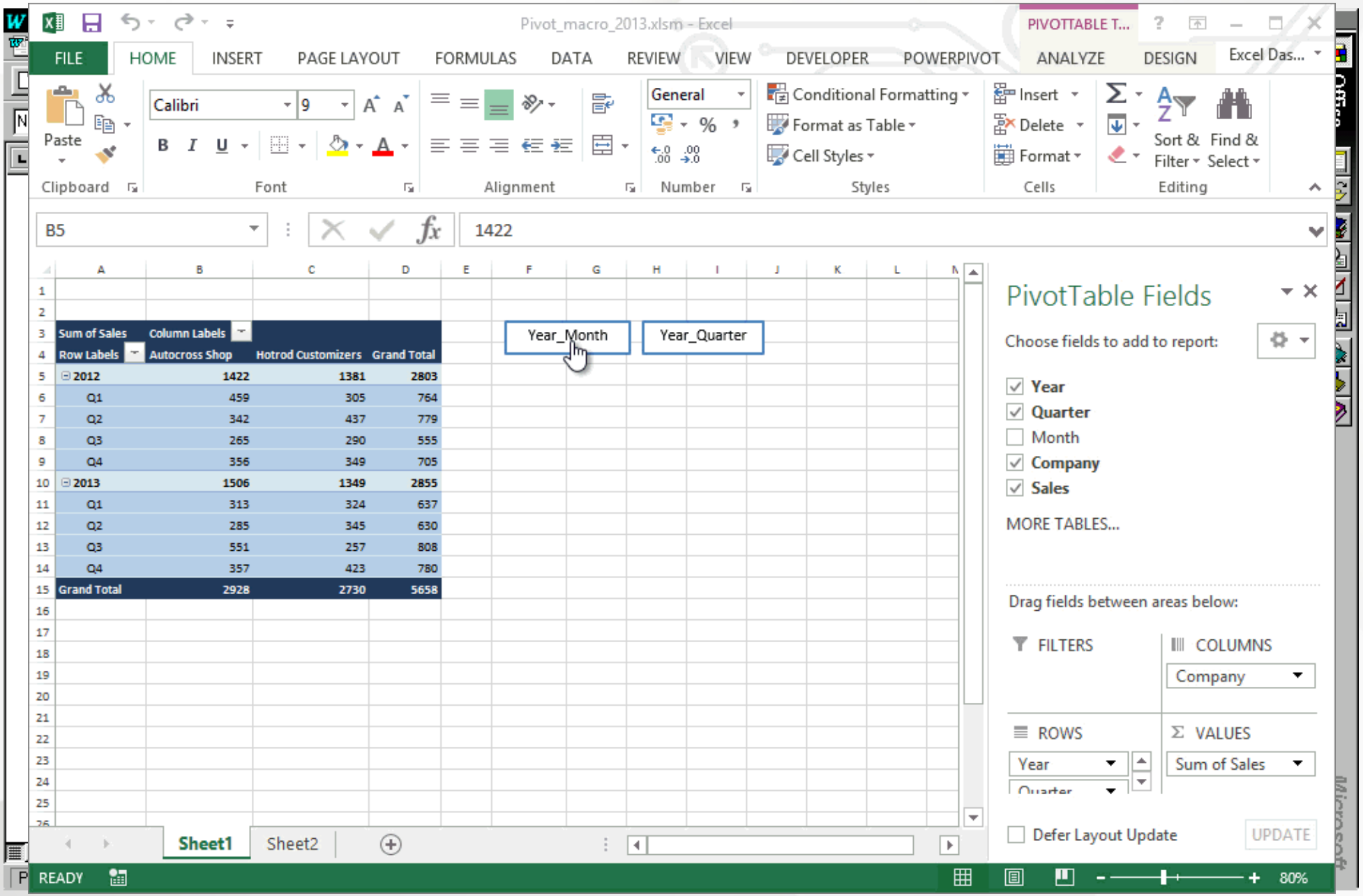
Social Engineering / Phishing

Android Malware

Data breach

2016 – H1 2017 Observed Threats

Rise of Malicious Macro in .DOC format


Pivot_macro_2013.xlsm - Excel
FILE
HOME
INSERT
PAGE LAYOUT
FORMULAS
DATA
REVIEW
VIEW
DEVELOPER
POWERPIVOT
PIVOTTABLE T...
ANALYZE
DESIGN
Excel Das...
Paste
Clipboard
Calibri
9
Font
Alignment
General
Number
Conditional Formatting
Format as Table
Cell Styles
Styles
Insert
Delete
Format
Cells
Sort & Filter
Find & Select
Editing
B5
1422
Sum of Sales
Column Labels
Row Labels
Autocross Shop
Hotrod Customizers
Grand Total
2012 1422 1381 2803
Q1 459 305 764
Q2 342 437 779
Q3 265 290 555
Q4 356 349 705
2013 1506 1349 2855
Q1 313 324 637
Q2 285 345 630
Q3 551 257 808
Q4 357 423 780
Grand Total 2928 2730 5658
Year_Month
Year_Quarter
PivotTable Fields
Choose fields to add to report:
Year
Quarter
Month
Company
Sales
MORE TABLES...
Drag fields between areas below:
FILTERS
COLUMNS
Company
ROWS
Year
Quarter
VALUES
Sum of Sales
Defer Layout Update
UPDATE
Sheet1
Sheet2
READY
80%

F-Secure

20742083495.doc - Microsoft Word

File | Home | Insert | Page Layout | References | Mailings | Review | View

Paste | Clipboard | Font | Paragraph | Styles | Editing

Emphasis | Heading 1 | Heading 2 | Change Styles | Find | Replace | Select

Security Warning Macros have been disabled. Enable Content

An error occurred while preparing to display the contents. Macro is not enabled.
Please enable macros in order to correctly view the contents of the document.

Words: 26 | 125%

F-Secure

2016 – H1 2017 Observed Threats

Rise of Malicious Macro in .DOC format

Ransomware Festival

We present a special software - **Locky Decrypter** -
which allows to decrypt and return control to all your encrypted files.

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://[redacted]tor2web.org/[redacted]
2. http://[redacted]onion.to/[redacted]
3. http://[redacted]onion.cab/[redacted]
4. http://[redacted]onion.link/[redacted]

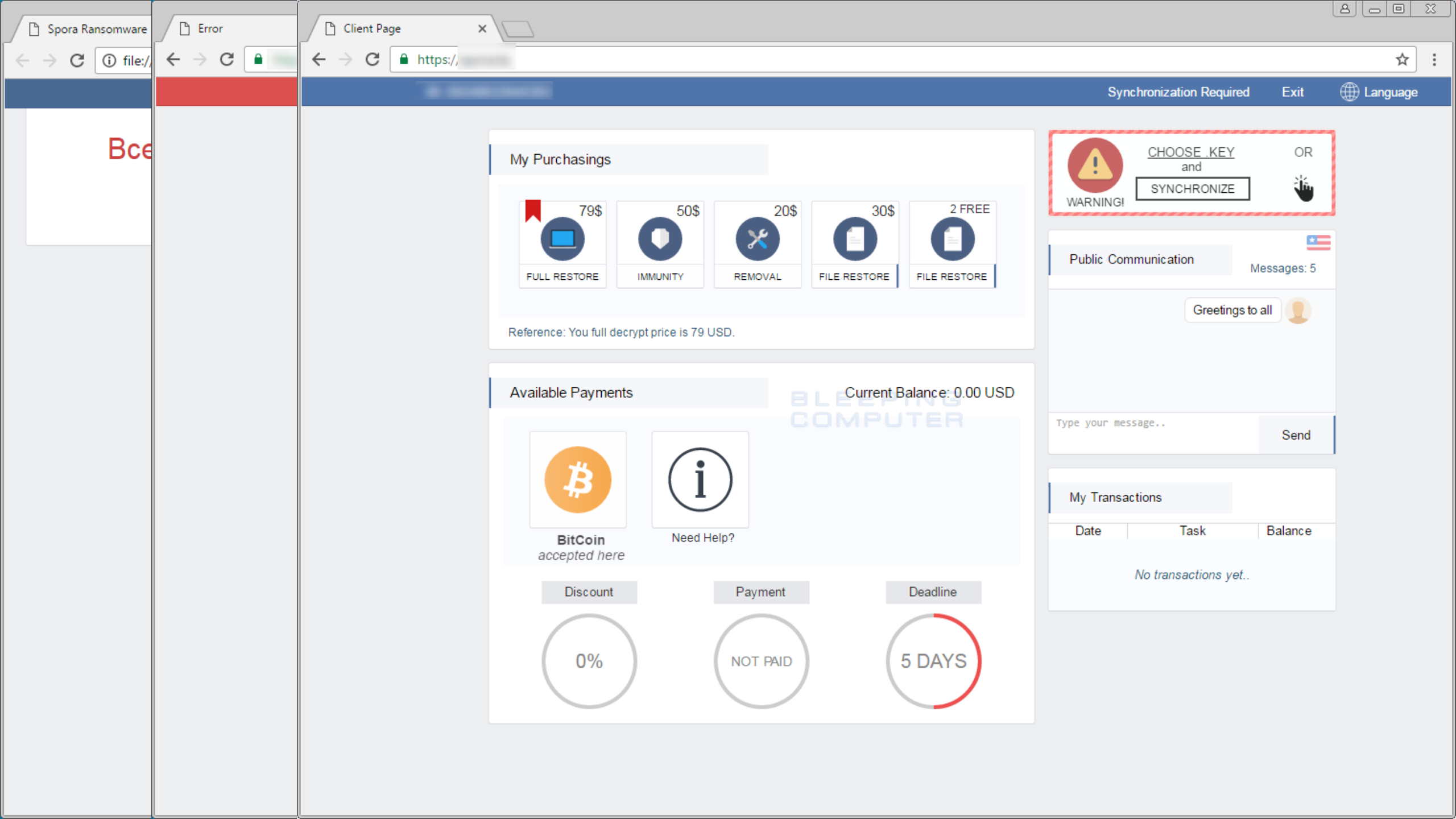
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [redacted].onion/[redacted]
4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted]!!!

[redacted]

5. Refresh the page and download decoder.

F-Secure.


Spora Ransomware
Error
Client Page
Synchronization Required
Exit
Language
My Purchasings
79$
FULL RESTORE
50$
IMMUNITY
20$
REMOVAL
30$
FILE RESTORE
2 FREE
FILE RESTORE
Reference: You full decrypt price is 79 USD.
WARNING!
CHOOSE .KEY
and
SYNCHRONIZE
OR
Public Communication
Messages: 5
Greetings to all
Type your message..
Send
Available Payments
Current Balance: 0.00 USD
BitCoin
accepted here
Need Help?
My Transactions
Date
Task
Balance
No transactions yet..
Discount
0%
Payment
NOT PAID
Deadline
5 DAYS

Warning Message!!

We are sorry to say that your computer and **your files have been encrypted**,
but wait, don't worry. There is a way that you can restore your computer and all of your files

0 years, 1 days, 05 hours, 17 min and 29 sec

Time remain when your files will lost forever!

Your personal unique ID: 0e72b

Please send at least 1.0 Bitcoin to address 1LEiPgvh6S9VEXW

Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

https://3hnuhydu4pd2

all governments all over the world (Encryption - Wikipedia). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!

If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.

and my little sister in 2015. The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day.
The world remained silent and no one helping us so we decided to take an action. (Syria War in Wikipedia)

Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people.
We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.

How to buy Bitcoins?

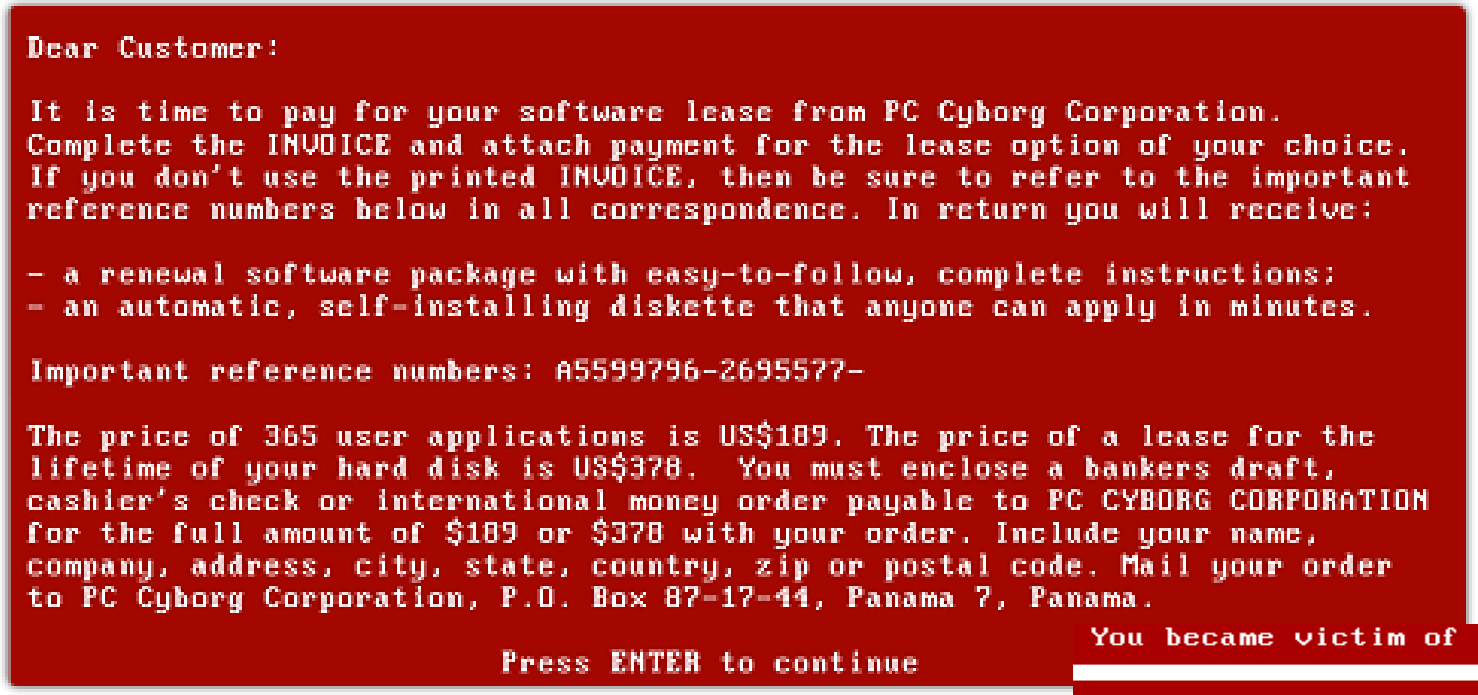
If you aren't familiar with Bitcoin and don't know what is it, please visit the official Bitcoin website (https://bitcoin.org/en/getting-started), follow the steps and you'll get your Bitcoins.
To understand more you can check also on the FAQ page (https://bitcoin.org/en/faq).
Please check this website (https://coinatmradar.com/) where you can find Bitcoin ATM all over the world.

Full list of encrypted files

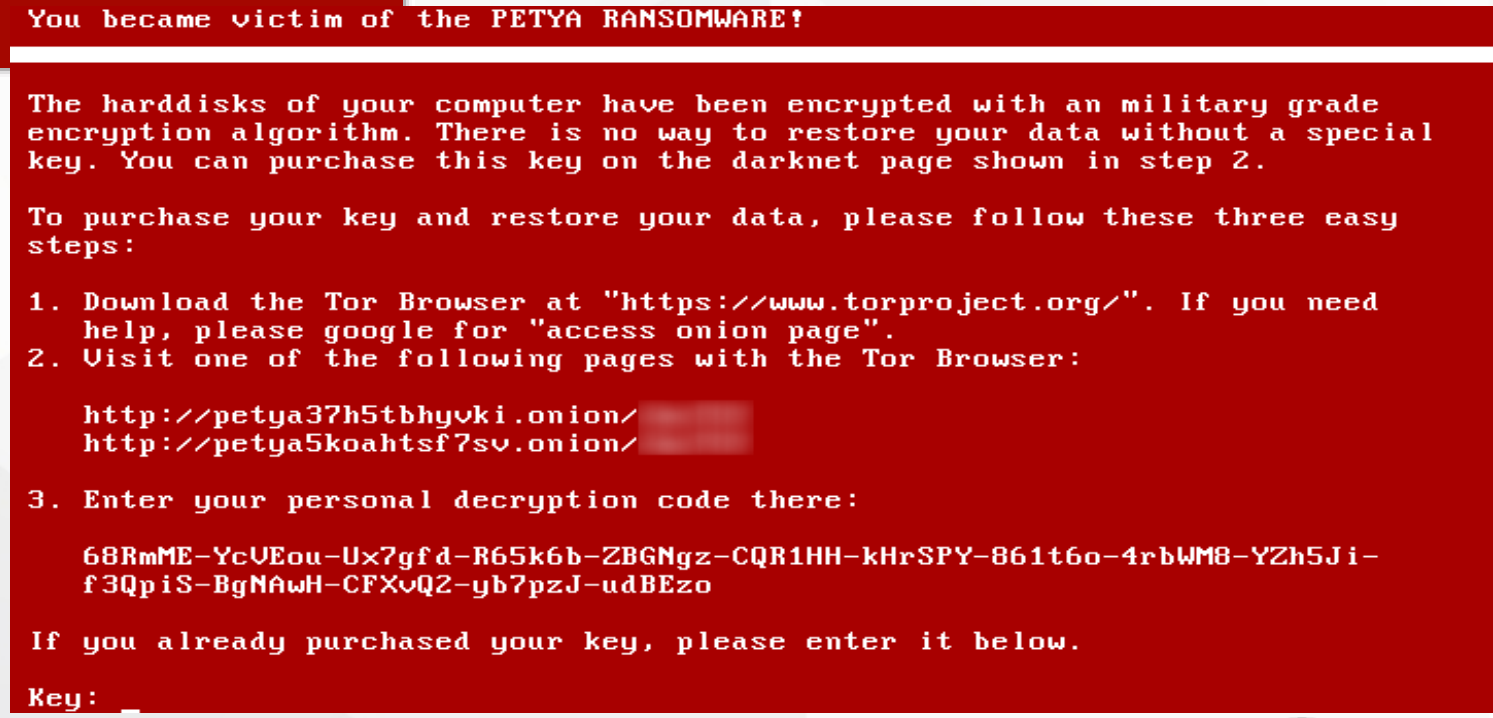
[FILES_LIST]

F-Secure

1989 AIDS

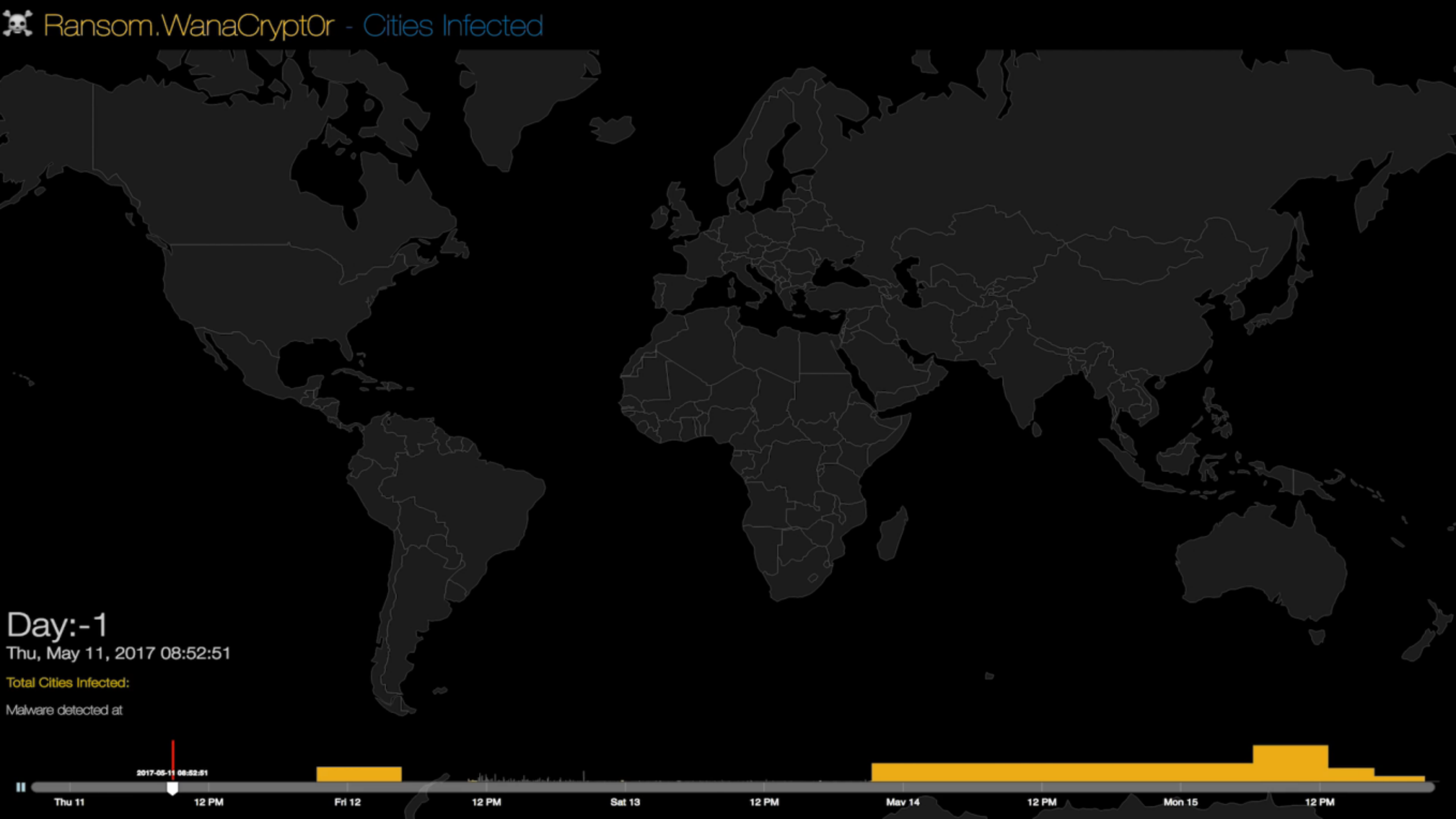


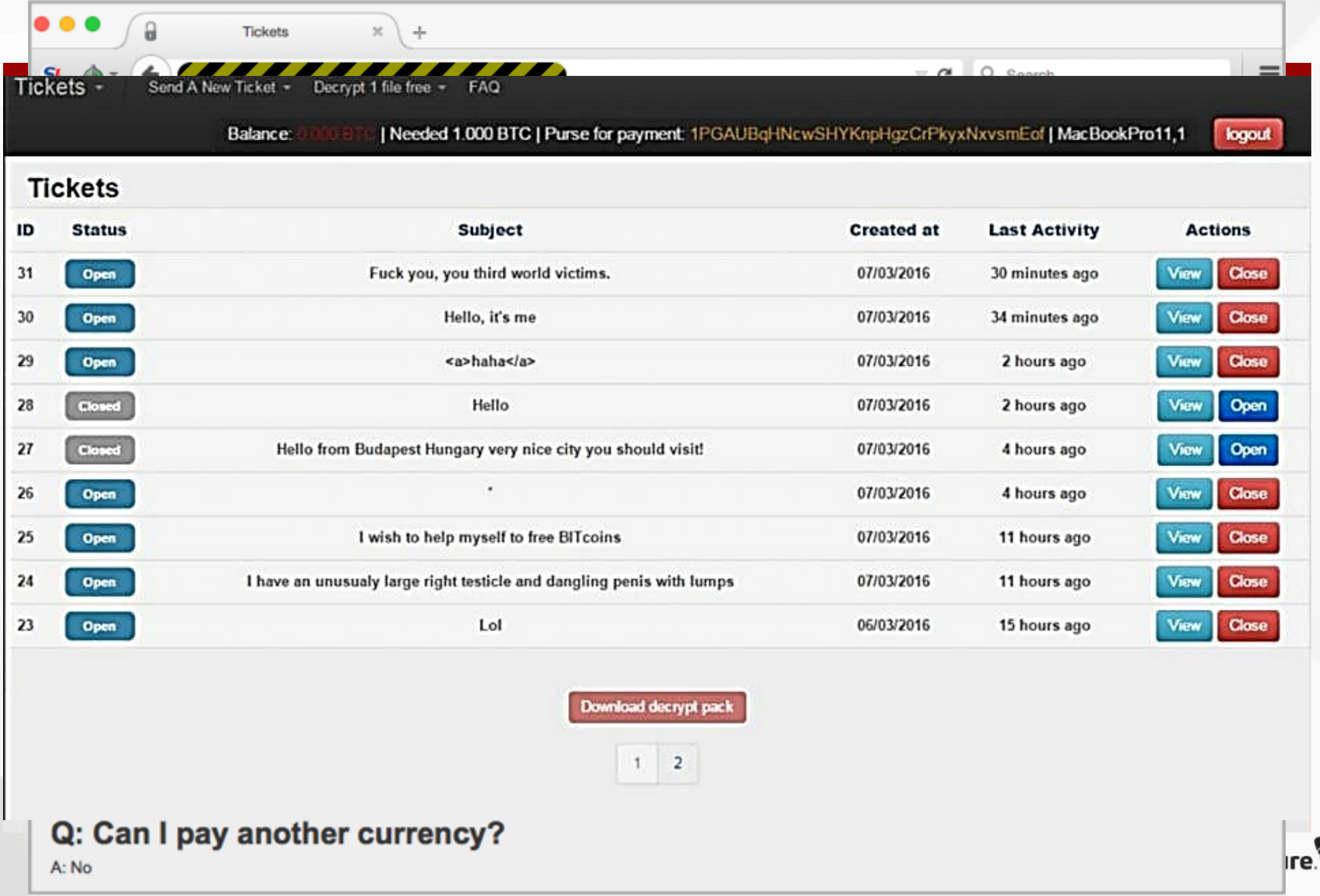
2016 PETYA



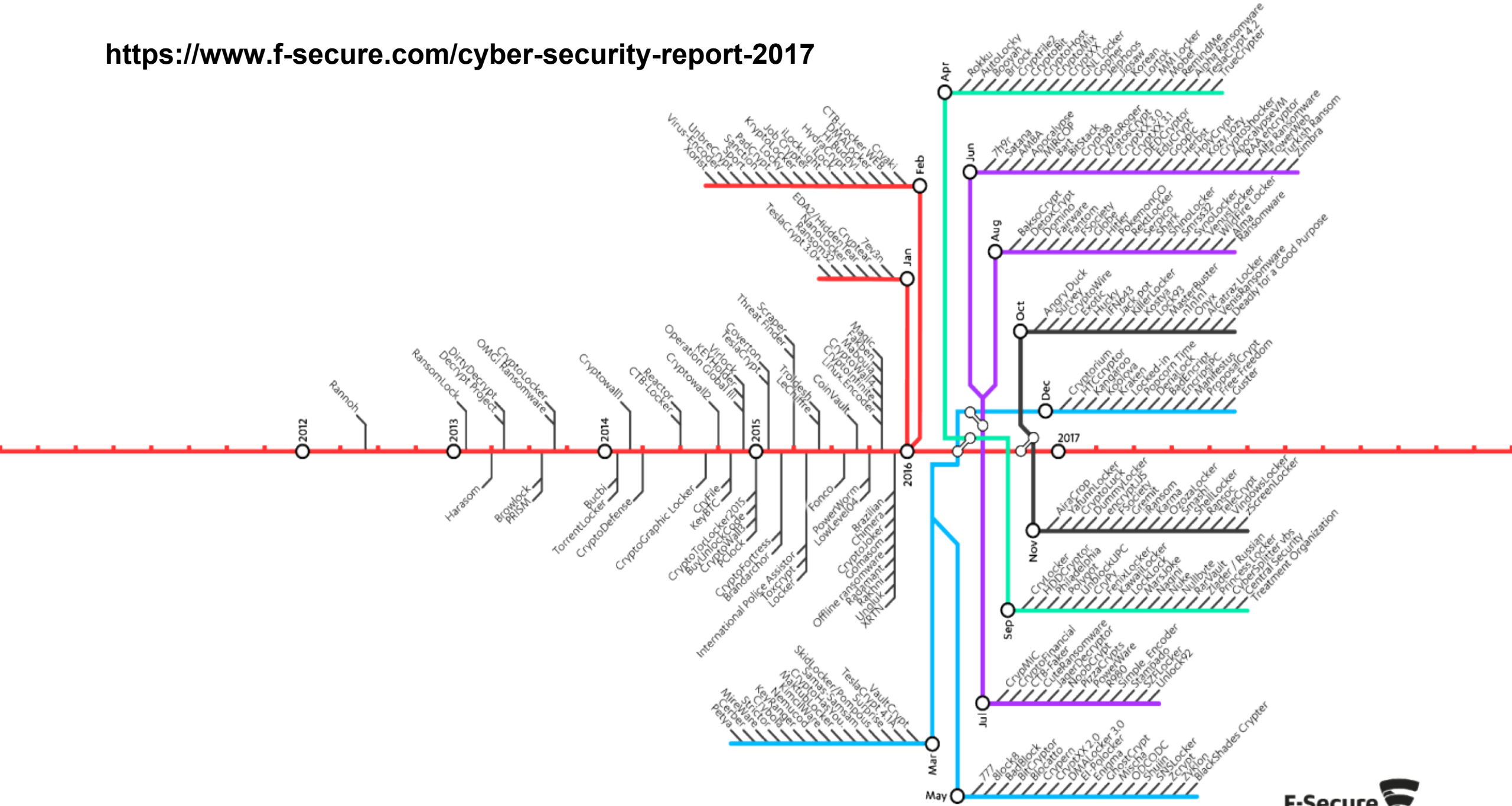
F-Secure


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/29/2017 15:30:23
Time Left
02:23:59:50
Your files will be lost on
6/2/2017 15:30:23
Time Left
06:23:59:50
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt
Start
_Tools
3:30 PM

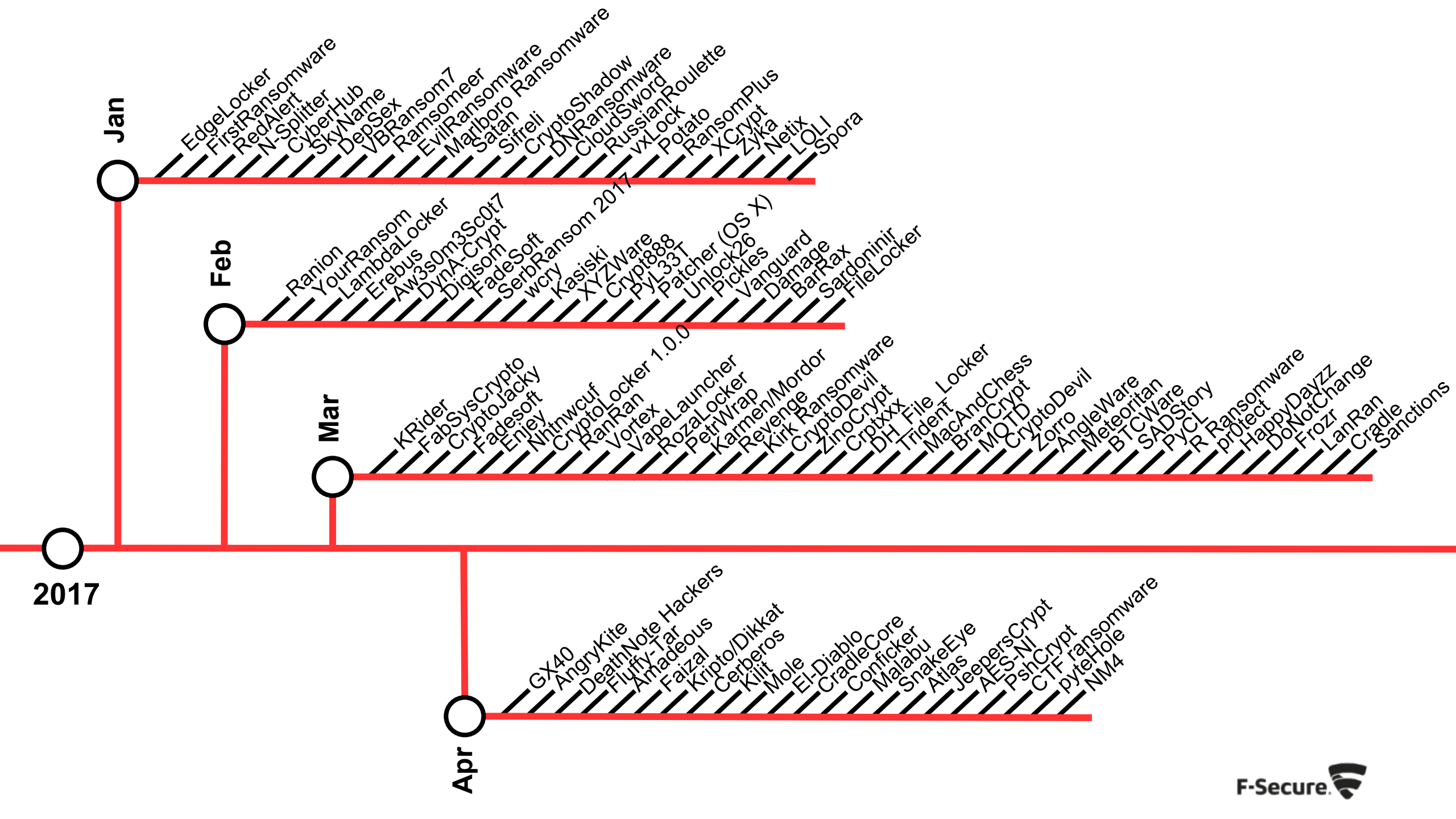

Ransom.WanaCrypt0r - Cities Infected
Day:-1
Thu, May 11, 2017 08:52:51
Total Cities Infected:
Malware detected at
2017-05-11 08:52:51
Thu 11
12 PM
Fri 12
12 PM
Sat 13
12 PM
May 14
12 PM
Mon 15
12 PM


Tickets
Tickets
Send A New Ticket
Decrypt 1 file free
FAQ
Balance: 0.000 BTC | Needed 1.000 BTC | Purse for payment: 1PGAUBqHNcwSHYKnpHgzCrPkyxNxvsmEof | MacBookPro11,1
logout
Tickets
ID
Status
Subject
Created at
Last Activity
Actions
31 Open Fuck you, you third world victims. 07/03/2016 30 minutes ago View Close
30 Open Hello, it's me 07/03/2016 34 minutes ago View Close
29 Open <a>haha 07/03/2016 2 hours ago View Close
28 Closed Hello 07/03/2016 2 hours ago View Open
27 Closed Hello from Budapest Hungary very nice city you should visit! 07/03/2016 4 hours ago View Open
26 Open . 07/03/2016 4 hours ago View Close
25 Open I wish to help myself to free BITcoins 07/03/2016 11 hours ago View Close
24 Open I have an unusualy large right testicle and dangling penis with lumps 07/03/2016 11 hours ago View Close
23 Open Lol 06/03/2016 15 hours ago View Close
Download decrypt pack
1
2
Q: Can I pay another currency?
A: No

https://www.f-secure.com/cyber-security-report-2017



F-Secure


2017
Jan
EdgeLocker
FirstRansomware
RedAlert
N-Splitter
CyberHub
SkyName
DepSex
VBRansom7
Ramsomeer
EvilRansomware
Marlboro Ransomware
Satan
Sifreli
CryptoShadow
DNRansomware
CloudSword
RussianRoulette
vxLock
Potato
RansomPlus
XCrypt
Zyka
Netix
LOLI
Spora
Feb
Ranion
YourRansom
LambdaLocker
Erebus
Aw3s0m3Sc0t7
DynA-Crypt
Digisom
FadeSoft
SerbRansom 2017
wcry
Kasiski
XYZWare
Crypt888
PyL33T
Patcher (OS X)
Unlock26
Pickles
Vanguard
Damage
BarRax
Sardoninir
FileLocker
Mar
KRider
FabSysCrypto
CryptoJacky
Fadesoft
Enjey
NhtnwcufCryptoLocker 1.0.0
RanRan
Vortex
VapeLauncher
RozaLocker
PetrWrap
Karmen/Mordor
Revenge
Kirk Ransomware
CryptoDevil
ZinoCrypt
Cryptxxx
DH_File_Locker
Trident
MacAndChess
BranCrypt
MOTD
CryptoDevil
Zorro
AngleWare
Meteoritan
BTCWare
SADStory
PyCL
R Ransomware
pr0tect
HappyDayzz
DoNotChange
Frozr
LanRan
Cradle
Sanctions
Apr
GX40
AngryKite
DeathNote Hackers
Fluffy-Tar
Amadeous
Faizal
Kripto/Dikkat
Cerberos
Kilit
Mole
El-Diablo
CradleCore
Conficker
Malabu
SnakeEye
Atlas
JeepersCrypt
AES-NI
PshCrypt
CTF ransomware
pyteHole
NM4
F-Secure.

FAQ

Which ransomwares are detected?

This service currently detects **405** different ransomwares. Here is a complete, dynamic list of what is currently detected:

4rw5w, 777, 7ev3n, 7h9r, 7zipper, 8lock8, ACCDFISA v2.0, AdamLocker, AES_KEY_GEN_ASSIST, **AES-NI**, Al-Namrood, Al-Namrood 2.0, Alcatraz, Alfa, Alma Locker, Alpha, AMBA, Amnesia, **Amnesia2**, AnDROid, AngryDuck, Anubis, Apocalypse, Apocalypse (New Variant), ApocalypseVM, ASN1 Encoder, AutoLocky, AxCrypter, BadBlock, BadEncript, BandarChor, BankAccountSummary, Bart, Bart v2.0, BitCrypt, BitCrypt 2.0, BitCryptor, BitKangoroo, BitStak, Black Feather, Black Shades, Blocatto, BlockFile12, **Blooper**, Booyah, BrainCrypt, Brazilian Ransomware, **BrickR**, BTCamant, BTCWare, Bucbi, BuyUnlockCode, Cancer, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberTear, Chimera, CHIP, Clouded, CockBlocker, Coin Locker, CoinVault, Comrade Circle, Conficker, Coverton, CradleCore, Cripton, Cry128, Cry9, Cryakl, CryFile, CryLocker, CrypMic, CrypMic, Crypren, Crypt0, Crypt0L0cker, Crypt38, CryptConsole, CryptFuck, CryptInfinite, CryptoDefense, CryptoDevil, CryptoFinancial, CryptoFortress, CryptoHasYou, CryptoHitman, CryptoJacky, CryptoJoker, CryptoLocker3, CryptoLockerEU, CryptoLuck, CryptoMix, **CryptoMix Revenge**, CryptoMix Wallet, CryptON, Crypton, CryptorBit, CryptoRoger, CryptoShield, CryptoShocker, CryptoTorLocker, CryptoViki, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, CryptoWire, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, CryptXXX 4.0, CryPy, CrySiS, CTB-Faker, CTB-Locker, Damage, DarkoderCryptor, Deadly, DEDCryptor, DeriaLock, Dharma (.dharma), Dharma (.onion), Dharma (.wallet), Digisom, DirtyDecrypt, DMA Locker, DMA Locker 3.0, DMA Locker 4.0, DMALocker Imposter, Domino, Done, DoNotChange, DXXD, DynA-Crypt, ECLR Ransomware, EdgeLocker, EduCrypt, El Polocker, EncrypTile, EncryptoJJS, Encryptor RaaS, Enigma, Enjey Crypter, EnkripsiPC, Erebus, Evil, Exotic, Extractor, Fabiansomware, Fadesoft, Fantom, FartPlz, FenixLocker, FindZip, FireCrypt, Flatcher3, FLKR, Flyper, FrozrLock, FS0ciety, FuckSociety, FunFact, GC47, GhostCrypt, Globe, Globe (Broken), Globe3, GlobeImposter, GlobeImposter 2.0, GOG, GoldenEye, Gomasom, GPCode, GX40, HadesLocker, HappyDayzz, Heimdall, Help50, HelpDCFile, Herbst, Hermes, Hermes 2.0, Hi Buddy!, HiddenTear, HollyCrypt, HolyCrypt, Hucky, HydraCrypt, IFN643, **ImSorry**, iRansom, Ishtar, Jack.Pot, Jaff, Jager, JapanLocker, JeepersCrypt, Jigsaw, Jigsaw (Updated), JobCrypter, JuicyLemon, Kaenlupuf, Karma, Karmen, Kasiski, KawaiiLocker, Kee Ransomware, KeRanger, KeyBTC, KEYHolder, KillerLocker, KimcilWare, Kirk, Kolobo, Kostya, Kozy.Jozy, Kraken, KratosCrypt, Krider, Kriptovor, KryptoLocker, L33TAF Locker, LambdaLocker, LeChiffre, **LightningCrypt**, LLTP, LMAOxUS, Lock2017, Lock93, Locked-In, **LockedByte**, LockLock, Lockout, Locky, Lortok, LoveServer, LowLevel04, MafiaWare, Magic, Maktub Locker, Marlboro, MarsJoke, Matrix, Maykolin, Maysomware, Meteoritan, Mikoyan, MirCop, MireWare, Mischa, MNS CryptoLocker, Mobef, MOTD, **MoWare**, MRCR1, n1n1n1, NanoLocker, NCrypt, Negozl, Nemucod, Nemucod-7z, Netix, NewHT, Nhtnwcuf, NM4, NMoreira, NMoreira 2.0, NotAHero, Nuke, NullByte, NxRansomware, ODCODC, **OoPS**, OpenToYou, OzozaLocker, PadCrypt, PayDay, PaySafeGen, PClock, PClock (Updated), PEC 2017, Philadelphia, Pickles, PopCornTime, Potato, PowerLocky, PowerShell Locker, PowerWare, Pr0tector, PrincessLocker, PrincessLocker 2.0, Project34, Protected Ransomware, PshCrypt, PyL33T, R980, RAA-SEP, Radamant, Radamant v2.1, RanRan, Rans0mLocked, RansomCuck, RansomPlus, RarVault, Razy, REKTLocker, RemindMe, RenLocker, RensenWare, Roga, Rokku, RoshaLock, RotorCrypt, Roza, RSAUtil, Ruby, Russian EDA2, SADStory, Sage 2.0, Salsa, SamSam, Sanction, Sanctions, Satan, Satana, SerbRansom, Serpent, ShellLocker, Shigo, ShinoLocker, Shujin, Simple_Encoder, Smrss32, SNSLocker, Spora, Sport, SQ_, Stampado, Stupid Ransomware, SuperCrypt, Surprise, SZFLocker, Team XRat, Telecrypt, TeslaCrypt 0.x, TeslaCrypt 2.x, TeslaCrypt 3.0, TeslaCrypt 4.0, TowerWeb, ToxCrypt, Trojan.Encoder.6491, Troldesh / Shade, TrueCrypter, TrumpLocker, UCCU, UIWIX, Ukash, UmbreCrypt, UnblockUPC, Ungluk, Unknown Crypted, Unknown Lock, Unknown XTBL, Unlock26, Unlock92, Unlock92 2.0, UserFilesLocker, USR0, Uyari, V8Locker, VaultCrypt, vCrypt, VenisRansomware, VenusLocker, VindowsLocker, VisionCrypt, VMola, Vortex, VxLock, WannaCryptor, **WhatAFuck**, WildFire Locker, Winnix Cryptor, WinRarer, WonderCrypter, X Locker 5.0, XCrypt, **XData**, Xorist, Xort, XRTN, **XTP Locker 5.0**, XYZWare, YouAreFucked, YourRansom, **Yyto**, zCrypt, Zekwacrypt, ZeroCrypt, ZimbraCryptor, ZinoCrypt, ZipLocker, Zyklon

F-Secure

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

Summary	
Address	1
Hash 160	1
Tools	R

Summary	
Address	1
Hash 160	1
Tools	R

Summary	
Address	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Hash 160	00e8fd98ca34f195b020af4a8b1c7238663d4212
Tools	Related Tags - Unspent Outputs

Transactions		
No. Transactions	107	
Total Received	13.83436451 BTC	
Final Balance	13.83436451 BTC	

Request Payment Donation Button

Transactio Transactio Transactions (Oldest First)

Filter

6ac937a7ccca1865	c5af561acec8d177	48b8f24f10c2cb9c30e2bb94ce86927ad87841e281ebdbdb1f89b9ee0960530a		2017-05-25 12:59:55
1N7AQvLLXkhak	1HhCNSukwMol 1Cy1Pihmhm3S 1Hy41sNjFAMtW	3CKLEK7RkR6d4YyDsp6A2xedrhmYjareqM	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	0.01252403 BTC 0.01252403 BTC
75233255b1545cd	f0888e210188b55	aad12b42f65d8df9b2c22875db292b5bbed02446c0229fa6ddc2ca70278c59b9		2017-05-25 12:52:55
13hCjrqPc2TNrE	15CvtWzjYALEq	3CKLEK7RkR6d4YyDsp6A2xedrhmYjareqM	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	0.00834935 BTC 0.00834935 BTC

2016 – H1 2017 Observed Threats

Rise of Malicious Macro in .DOC format

Ransomware Festival

Android Malware

DroidJack Uses Side-Load...It's Super Effective! Backdoored Pokemon GO Android App Found

- Press Releases >
- Proofpoint in the News >
- Proofpoint Blog >
- Threat Insights blog >
- Events >
- Media Contacts >

Overview

Pokemon GO is the first Pokemon game sanctioned by Nintendo for iOS and Android devices. The augmented reality game was first released in Australia and New Zealand on July 4th and users in other regions quickly clamored for versions for their devices. It was released on July 6th in the US, but the rest of the world will remain tempted to find a copy outside legitimate channels. To that end, a number of publications have provided tutorials for "side-loading" the application on Android. However, as with any apps installed outside of official app stores, users may get more than they bargained for.

In this case, Proofpoint researchers discovered an infected Android version of the newly released mobile game Pokemon GO [1]. This specific APK was modified to include the malicious remote access tool (RAT) called DroidJack (also known as SandroRAT), which would virtually give an attacker full control over a victim's phone. The DroidJack RAT has been described in the past, including by Symantec [2] and Kaspersky [3]. Although we have not observed this malicious APK in the wild, it was uploaded to a malicious file repository service at 09:19:27 UTC on July 7, 2016, less than 72 hours after the game was officially released in New Zealand and Australia.

Super Mario Run for Android? No, it's malware

It's a me… malwario!

David Bisson | January 8, 2017 8:05 pm | Filed under: **Android**, **Google**, **Malware** 1

Attackers have created a fake version of Super Mario Run for Android in an attempt to trick unsuspecting smartphone users into downloading the Marcher trojan.

Marcher is a type of banking malware that acquires administrative privileges on every Android device it infects. It then waits for a victim to open a banking or payment app as well as other well-known services installed on their phones such as Gmail and Facebook.

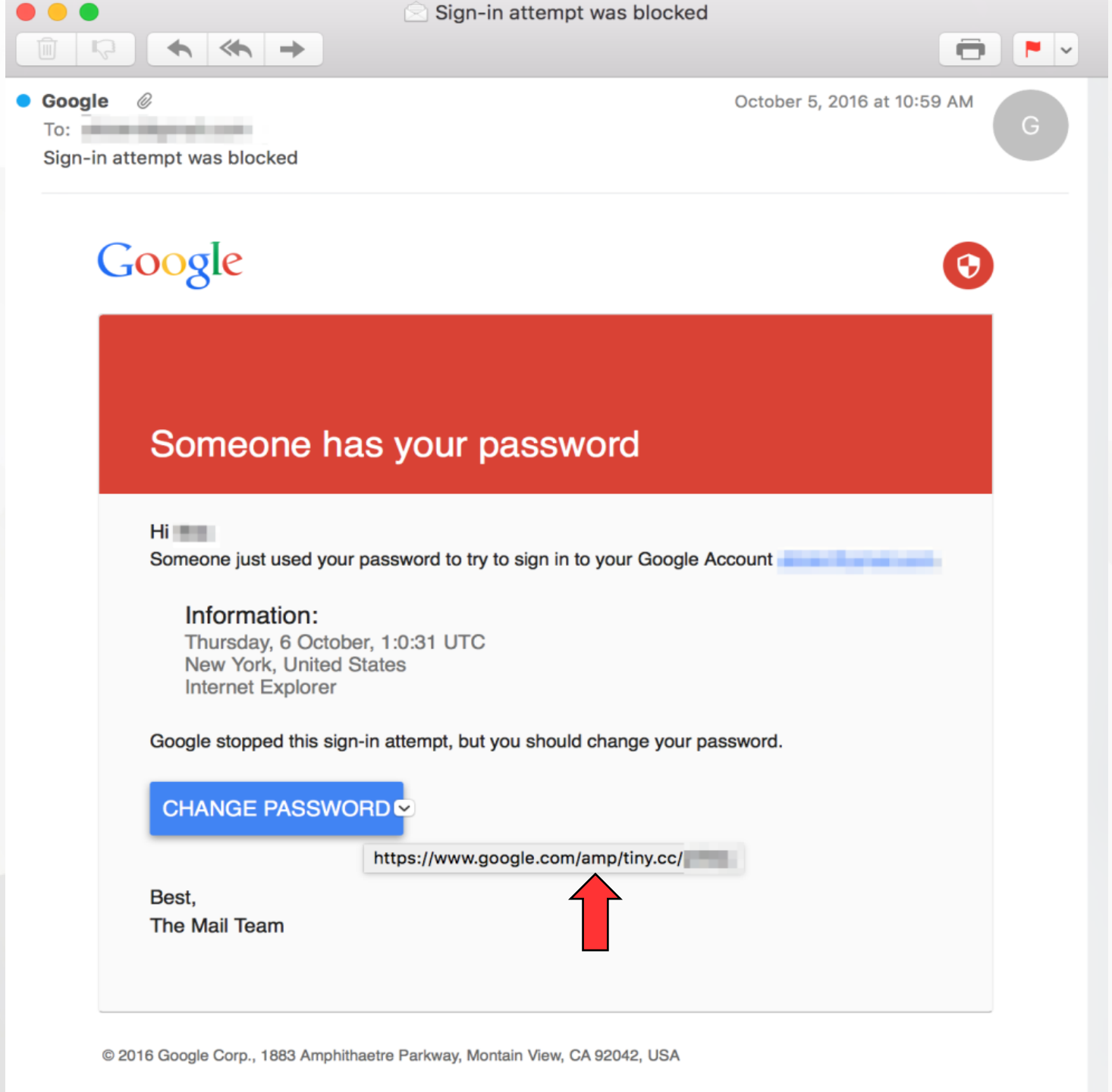
2016 – H1 2017 Observed Threats

Rise of Malicious Macro in .DOC format

Ransomware Festival

Social Engineering / Phishing

Android Malware


Sign-in attempt was blocked
Google
To:
Sign-in attempt was blocked
October 5, 2016 at 10:59 AM
G
Google
Someone has your password
Hi
Someone just used your password to try to sign in to your Google Account
Information:
Thursday, 6 October, 1:0:31 UTC
New York, United States
Internet Explorer
Google stopped this sign-in attempt, but you should change your password.
CHANGE PASSWORD
https://www.google.com/amp/tiny.cc/
Best,
The Mail Team
© 2016 Google Corp., 1883 Amphithaetre Parkway, Montain View, CA 92042, USA

F-Secure

Technology | CyberSecurity

Facebook and Google employees fa phishing scam, losing $100m to ha

- Tech giants were tricked into authorising payments over two year

By Mary-Ann Russon
April 28, 2017 13:23 BST

Facebook and Google have admitted that a hacker scammed their employees out of $100m by h impersonating a Chinese hardware supplier (IStock)

Employees from Facebook and Google were tricked into transferring $10 to a hacker's bank account overseas as part of a sophisticated email phishi

Evaldas Rimasauskas, 48, from Lithuania is alleged to have hacked into Fa Taiwanese computer hardware parts supplier Quanta in order to figure ou departments and in charge of issuing, authorising and paying invoices.

Technology | CyberSecurity

Cable giant Leoni AG loses €40m after C transfers funds to hacker's bank account

- Leoni AG shares dropped by 7% after a CFO fell for phishing scam.

By Mary-Ann Russon
Updated March 20, 2017 17:44 GMT

Phishing email scams are still the best way for attackers to hack into a power plant (IStock)

Europe's largest manufacturer of electrical cables and wires Leoni AG has seen its sha between 5-7% after reporting that an email phishing scam caused the company to lose ($44.7m, £33.7m) overnight.

Leoni AG is a German firm, but it has a factory located in Bistrita, a city in northern Ro According to Romanian newspapers, on 12 August, the funds disappeared because the Bistrita factory was tricked into transferring money into an unknown bank account be email looked like it came from one of the manufacturer's top executives in Germany.

Technology | CyberSecurity

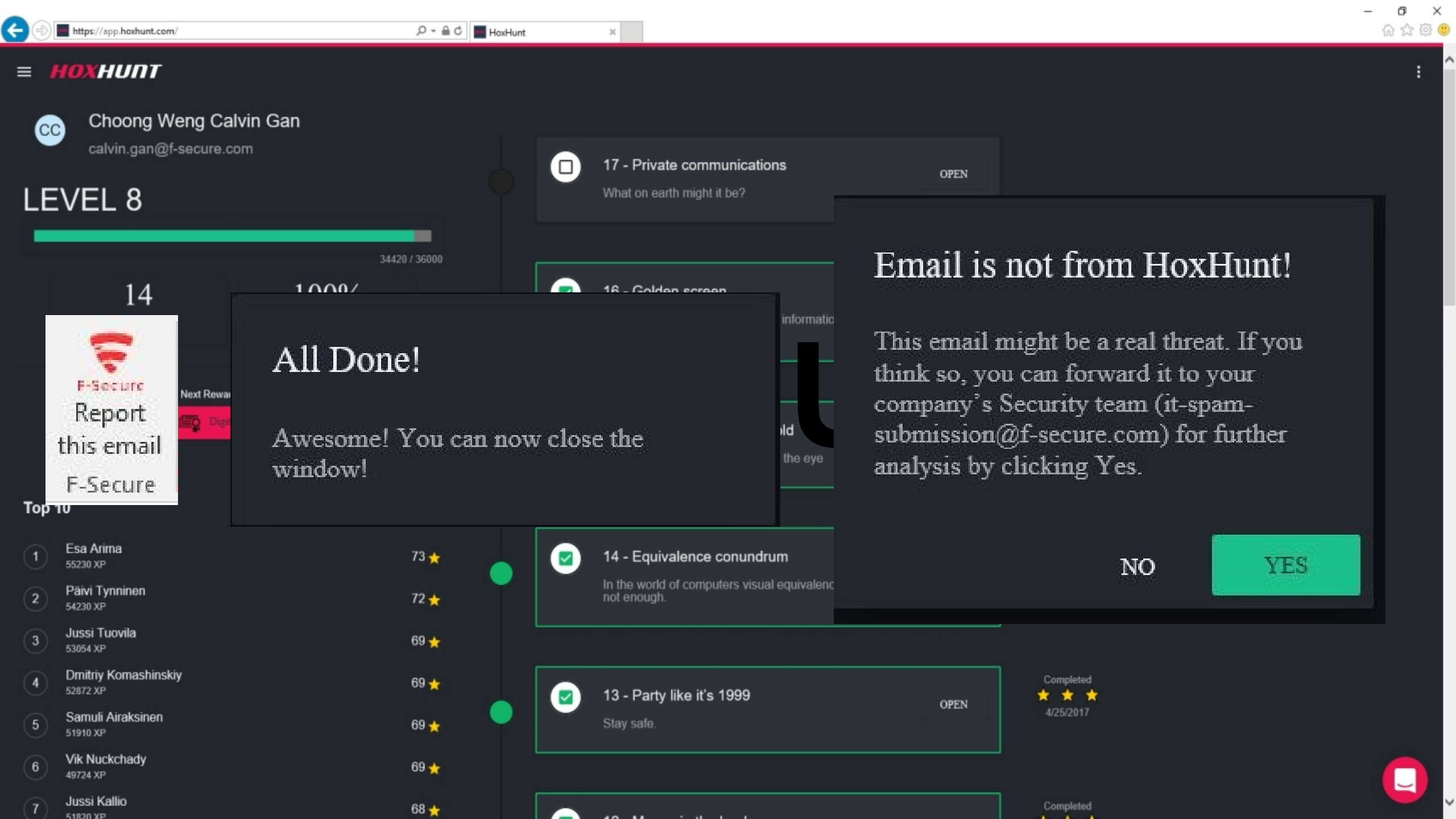
Mattel loses $3m in email phishing scam but Chinese authorities save the day

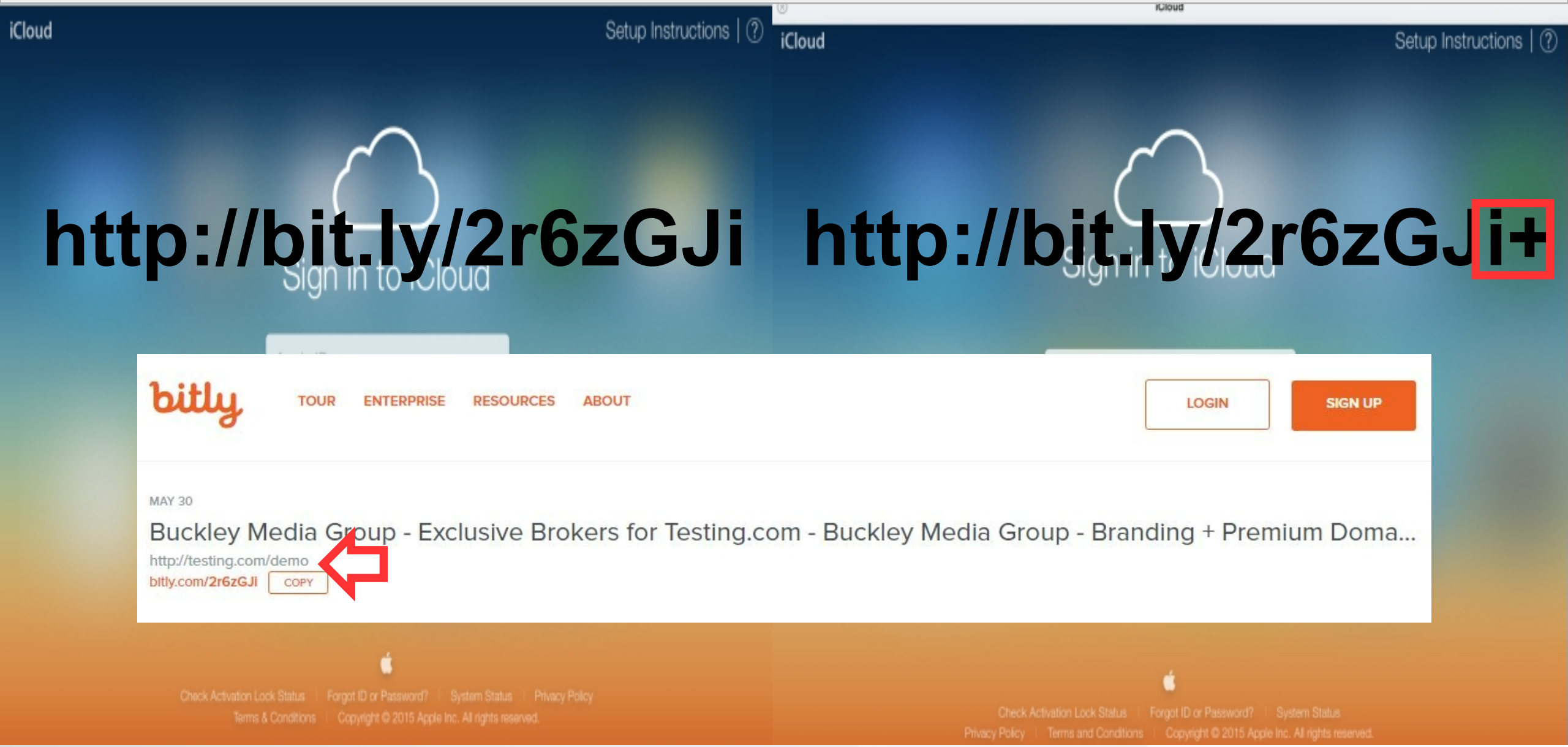
By Mary-Ann Russon
March 30, 2016 13:33 BST

Mattel, known for its Barbie dolls, was the victim of an email phishing scam that almost cost the firm $3m (Reuters)

US toy company Mattel, the maker of Barbie dolls and Hot Wheels cars, was the victim of a sophisticated email phishing scam in 2015 that enabled cybercriminals to almost get away with $3m (£2.1m), but luckily a Chinese bank holiday and efforts by Chinese authorities managed to prevent the loss.

In April 2015, Mattel underwent corporate change, firing its CEO Bryan Stockton and instating Christopher Sinclair to take his place. Crafty Chinese cyber thieves sought to use this to their advantage by sending an email in Sinclair's name to an unnamed financial executive on Thursday 30 April 2015 requesting a new vendor payment to China, according to an Associated Press investigation into financial crimes in Wenzhou, Zhejiang province.


https://app.hoxhunt.com/
HoxHunt
HOXHUNT
Choong Weng Calvin Gan
calvin.gan@f-secure.com
LEVEL 8
34420 / 36000
14
17 - Private communications
What on earth might it be?
OPEN
16 - Golden screen
14 - Equivalence conundrum
In the world of computers visual equivalenc
not enough.
13 - Party like it's 1999
Stay safe.
OPEN
Completed
4/25/2017
Completed
F-Secure
Report this email
F-Secure
All Done!
Awesome! You can now close the window!
Email is not from HoxHunt!
This email might be a real threat. If you think so, you can forward it to your company's Security team (it-spam-submission@f-secure.com) for further analysis by clicking Yes.
NO
YES
Top 10
1 Esa Arima 55230 XP 73
2 Päivi Tynninen 54230 XP 72
3 Jussi Tuovila 53054 XP 69
4 Dmitriy Komashinskiy 52872 XP 69
5 Samuli Airaksinen 51910 XP 69
6 Vik Nuckchady 49724 XP 69
7 Jussi Kallio 51820 XP 68


iCloud
Setup Instructions
Sign in to iCloud
http://bit.ly/2r6zGJi
http://bit.ly/2r6zGJi+
bitly
TOUR
ENTERPRISE
RESOURCES
ABOUT
LOGIN
SIGN UP
MAY 30
Buckley Media Group - Exclusive Brokers for Testing.com - Buckley Media Group - Branding + Premium Doma...
http://testing.com/demo
bitly.com/2r6zGJi
COPY
Check Activation Lock Status
Forgot ID or Password?
System Status
Privacy Policy
Terms & Conditions
Copyright © 2015 Apple Inc. All rights reserved.

F-Secure

2016 – H1 2017 Observed Threats

Rise of Malicious Macro in .DOC format

Ransomware Festival

Social Engineering / Phishing

Android Malware

Data breach

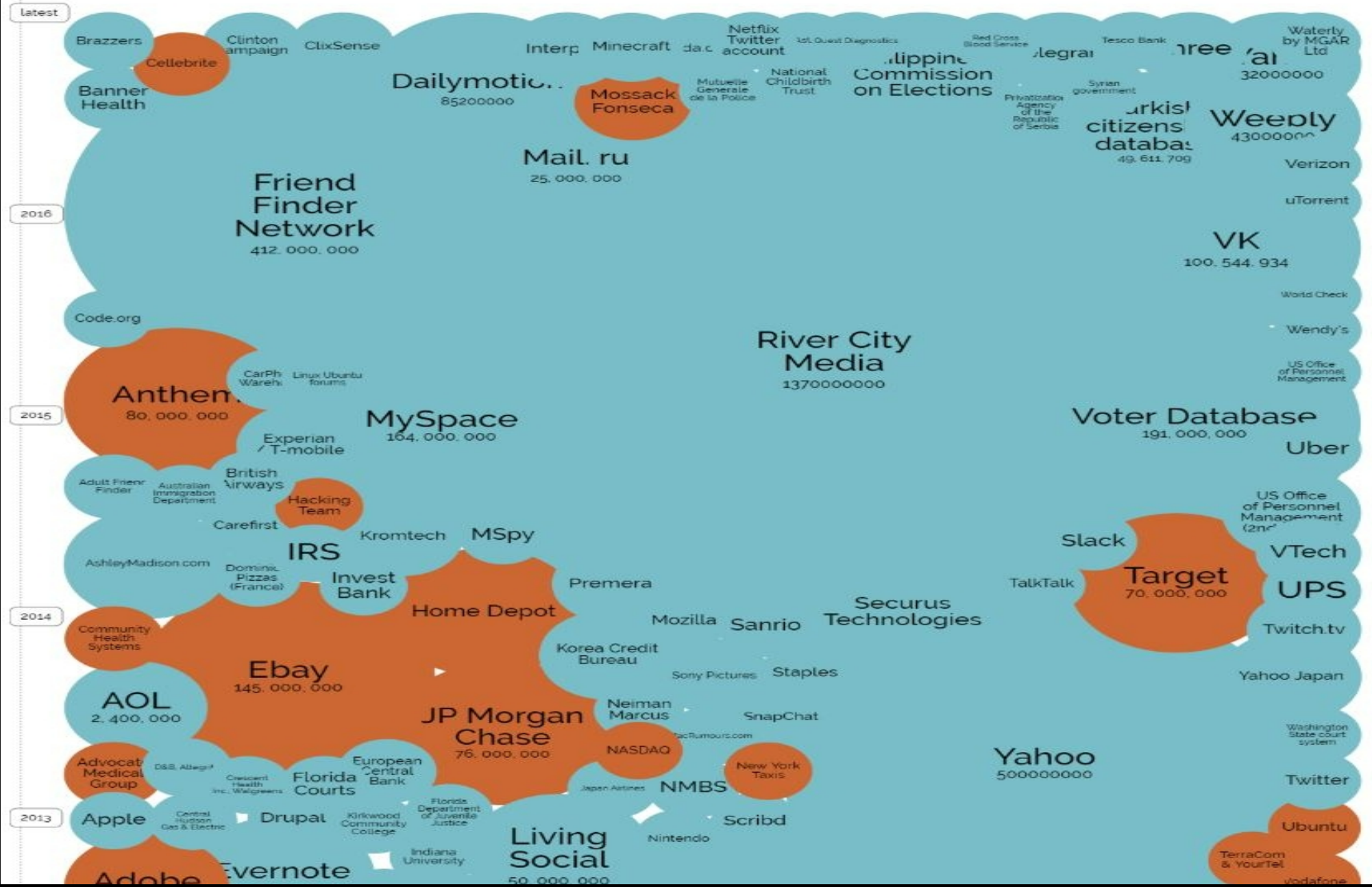
World's Biggest Data Breaches

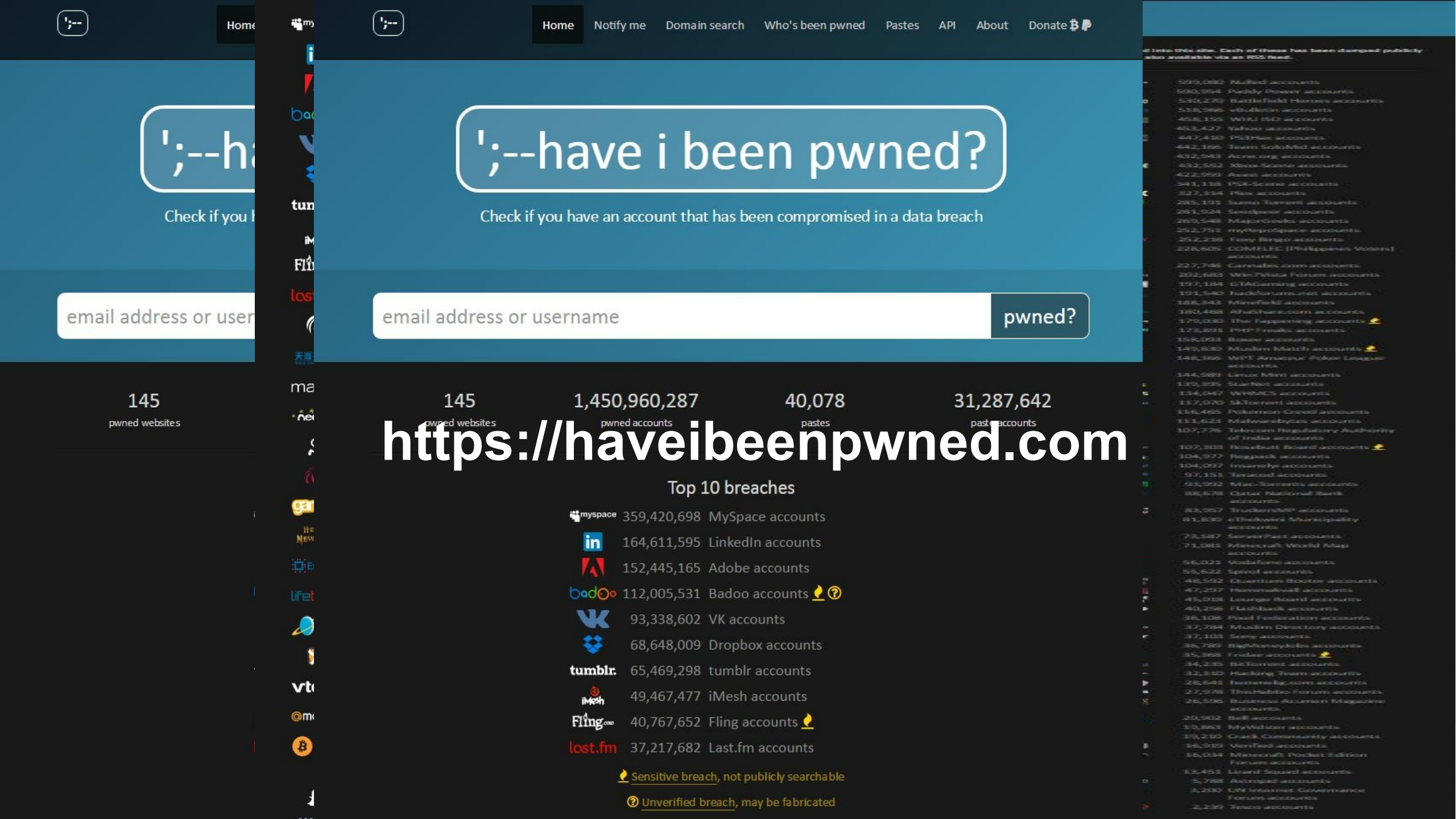
Selected losses greater than 30,000 records

(updated 5th Jan 2017)

interesting story

YEAR | BUBBLE COLOUR: YEAR, METHOD OF LEAK | BUBBLE SIZE: NO OF RECORDS STOLEN, DATA SENSITIVITY | SHOW FILTER




Home
Notify me
Domain search
Who's been pwned
Pastes
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address or username
pwned?
145
pwned websites
1,450,960,287
pwned accounts
40,078
pastes
31,287,642
pastes accounts
https://haveibeenpwned.com
Top 10 breaches
359,420,698 MySpace accounts
164,611,595 LinkedIn accounts
152,445,165 Adobe accounts
112,005,531 Badoo accounts
93,338,602 VK accounts
68,648,009 Dropbox accounts
65,469,298 tumblr accounts
49,467,477 iMesh accounts
40,767,652 Fling accounts
37,217,682 Last.fm accounts
Sensitive breach, not publicly searchable
Unverified breach, may be fabricated


WH.GOV
WH
.GOV
RT
RUPTLY
IDENTITY THEFT, AND THAT'S FREE
ACCESS TO THEIR CREDIT SCORES.

F-Secure

THREATS AND THEIR CHALLENGES

SPAM CAMPAIGNS

- Normally sent by a botnet
- sometimes tracking the actual threat actors may take a while,
- although we know that most of them were spread thru EKs

RANSOMWARE

- Holds one's important documents as hostage, and requires ransom in the form of virtual currency, bitcoins
- Still using their own Tor network for payments to decrypt files
- May become challenging once they start using the cloud

DDOS AS A SERVICE

- Distributed Denial of Service-as-a-Service
- For taking a site offline
- It used to be that you need to have a network of contacts and great technical expertise
- Some offer it for as low as $20
- Ransomware as a service is also available

MALWARE FOOTPRINTS

- We are able analyze and understand its characteristic
  - possible infection vector
  - Possible stolen data storage
  - Geographical location, but not the exact IP or client
- Engagement with local law enforcement agencies

COUNTRIES
167

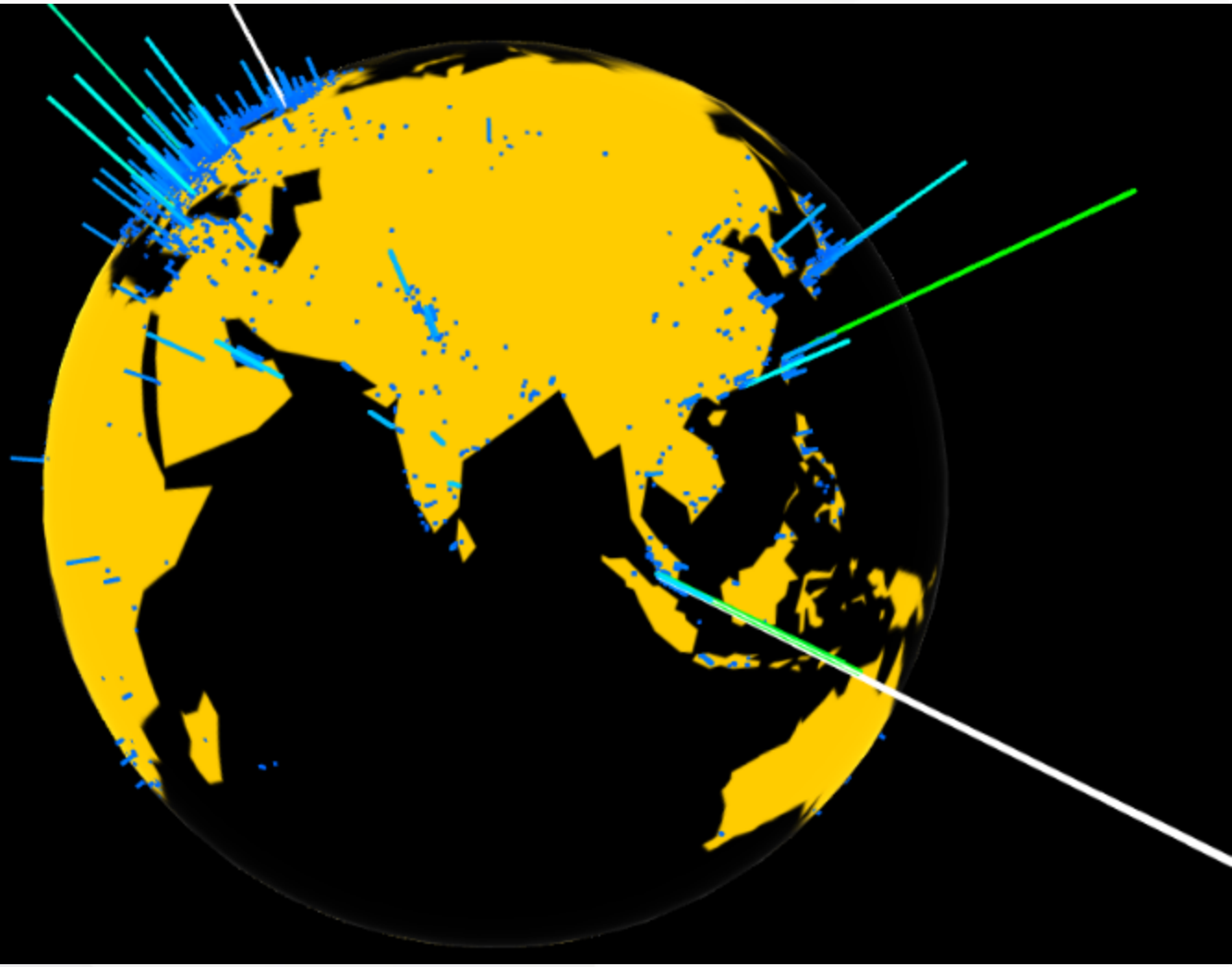
LOCATIONS
7247

VARIANTS
12706

DETECTIONS
46903

TOP LOCATIONS
FOR PAST 24 HOURS

1. Helsinki
2. Shah Alam
3. Taipei
4. Kuala Lumpur
5. Batu Caves
6. Paris
7. Istanbul
8. São Paulo
9. Bucharest
10. Tokyo



F-Secure®