Poznaním malvéru k efektívnej obrane

alebo ako udržať krok so škodlivým kódom...

Maroš Rajnoch, SOITRON, s.r.o.

presales support

maros@soitron.com

dôvernosť informácií:

Táto prezentácia je určená výhradne pre návštevníkov semináru

SOITRON DEFENSE 2017 (23. marca 2017, Zochova chata)

Ako taká nesmie byť poskytovaná tretím stranám a to ani ako celok, ani žiadna jej časť. Mimo účel, na ktorý je určená nesmie byť rozmnožovaná a/alebo zasielaná mechanickou, fotochemickou alebo elektronickou cestou.

TÜV NORD
TÜV NORD CERT GmbH
ISO 27001

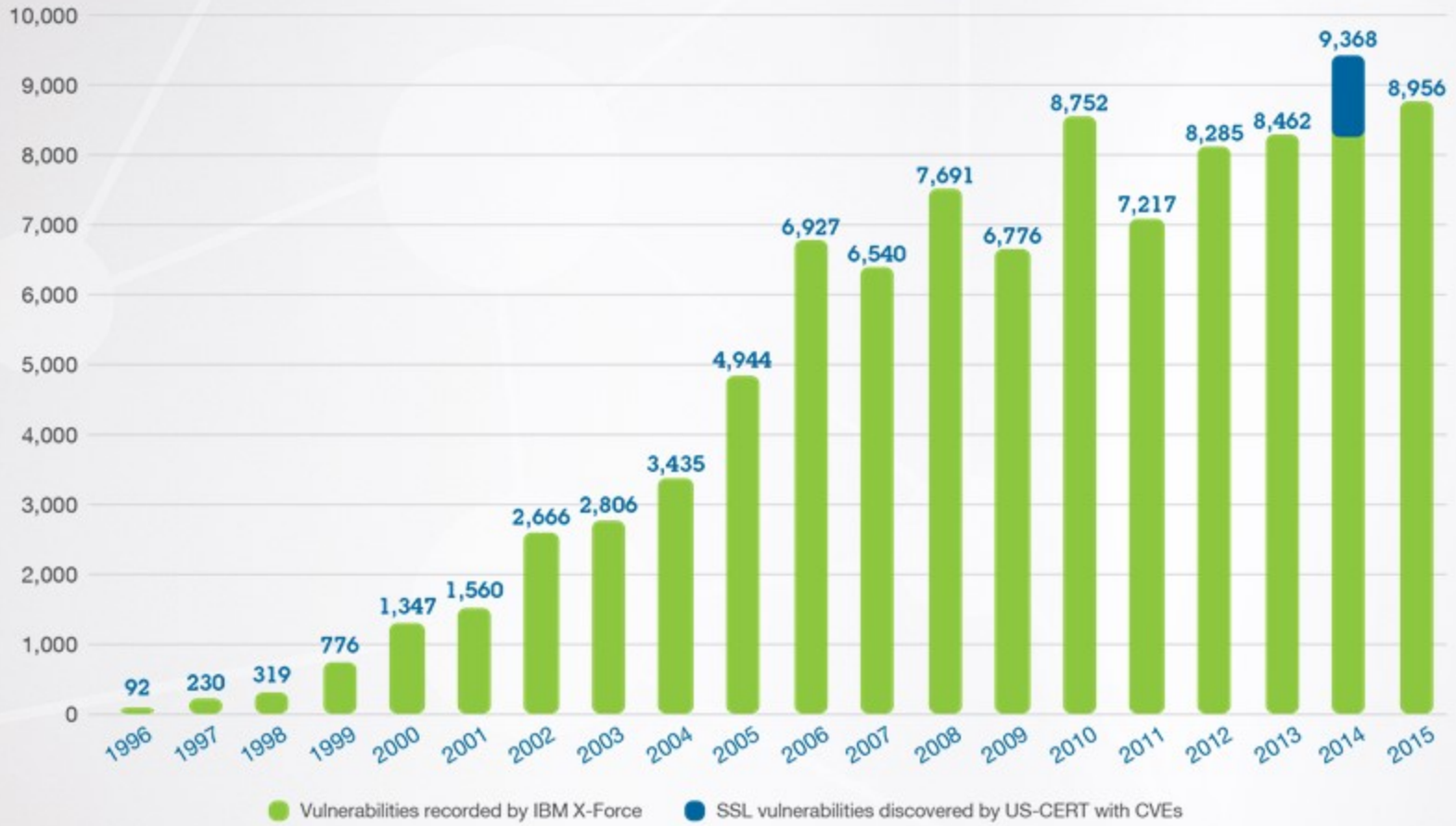
TÜV NORD
TÜV NORD CERT GmbH
ISO 9001

Dokument	Poznaním malvéru k efektívnej obrane
Podnázov	Ako udržať krok so škodlivým kódom...
Verzia	1. X58D7BFCF
Klasifikácia	SELECTED AUDIENCE
OID	1.3.158.35955678.299039. X58D7BFCF

Vypracoval	Maroš Rajnoch
Konzultant	N/A
Preveril	Štefan Porubčan
Schválil	N/A

Vulnerability disclosures growth by year

1996 through 2015



Vulnerability disclosures growth by year, 1996 through 2015

Source: IBM X-Force® Research and Development

Flash						Silverlight
CVE-2015-7645	CVE-2015-8446	CVE-2015-8651	CVE-2016-1019	CVE-2016-1001	CVE-2016-4117	CVE-2016-0034
Nuclear		Nuclear	Nuclear		Nuclear	
Magnitude			Magnitude		Magnitude	
Angler	Angler	Angler		Angler	Angler	Angler
Neutrino		Neutrino				
RIG						RIG

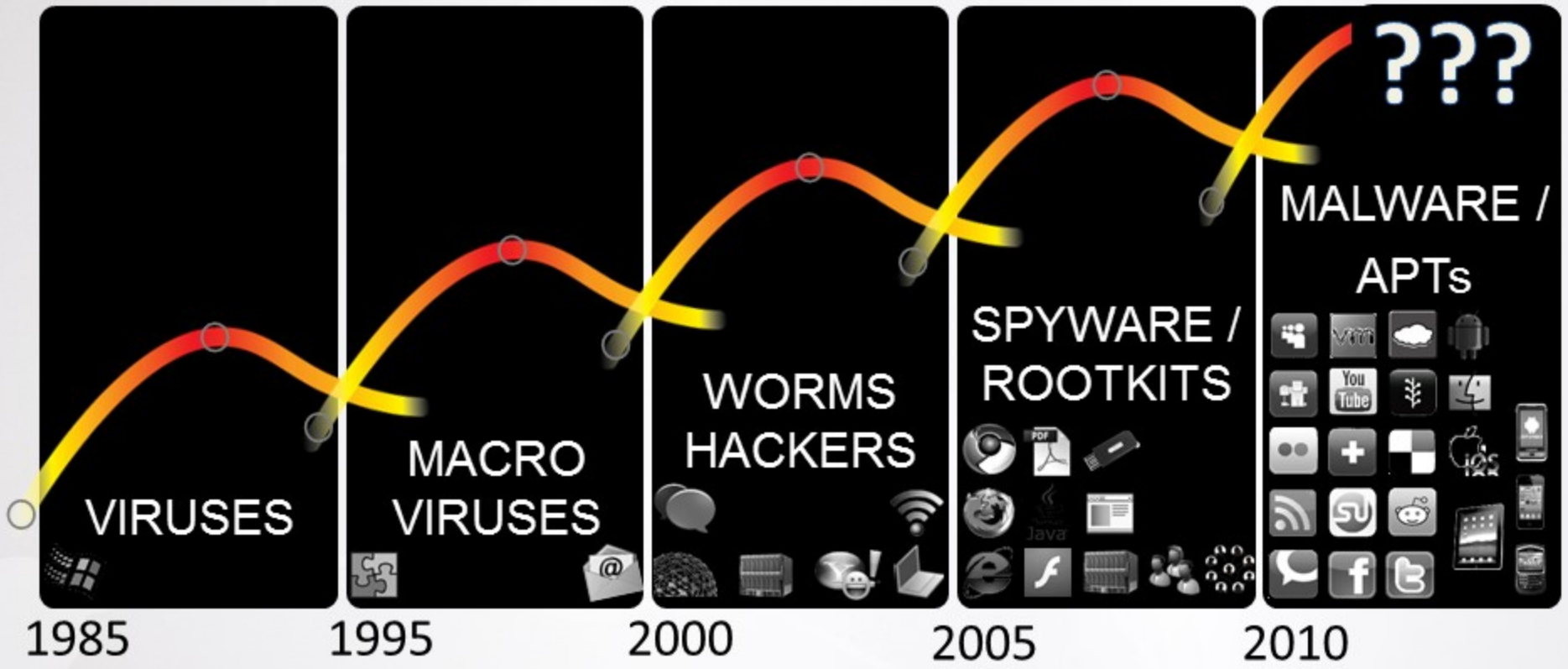
Source: Cisco Security Research

A New Zero-Day Vulnerability Discovered Every Week in 2015

Advanced attack groups continue to profit from previously undiscovered flaws in browsers and website plugins.

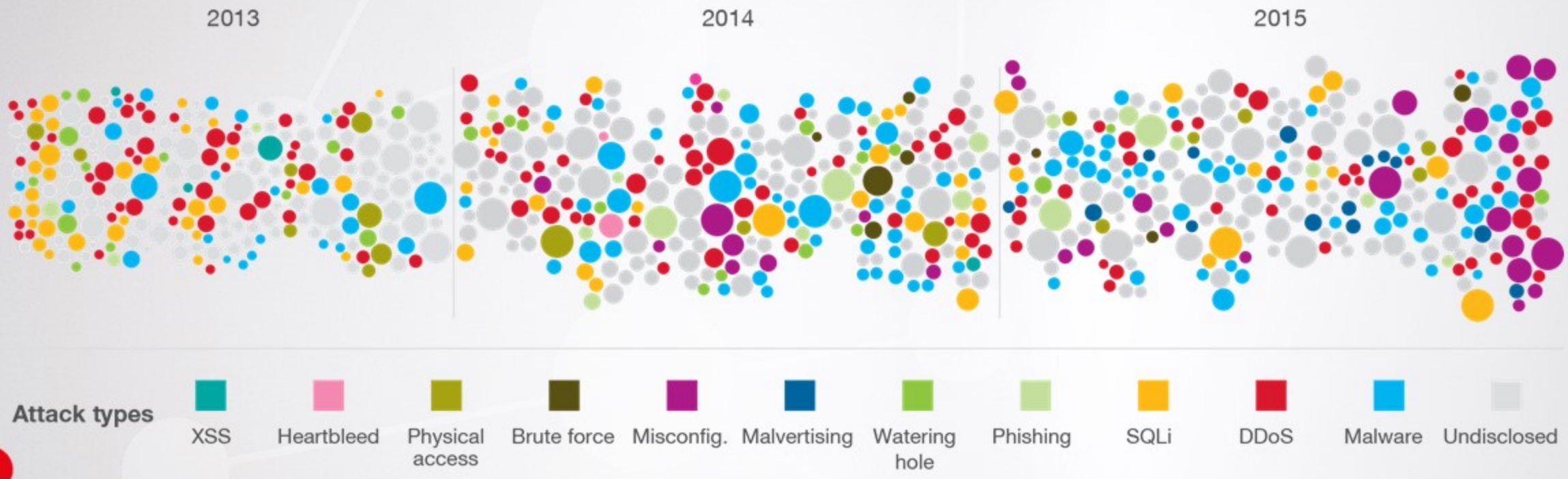
In 2015, 54 zero-day vulnerabilities were discovered.

zdroj: Symantec


VIRUSES
MACRO VIRUSES
WORMS HACKERS
SPYWARE / ROOTKITS
MALWARE / APTs
???
1985
1995
2000
2005
2010

Sampling of security incidents by attack type, time and impact, 2013 through 2015

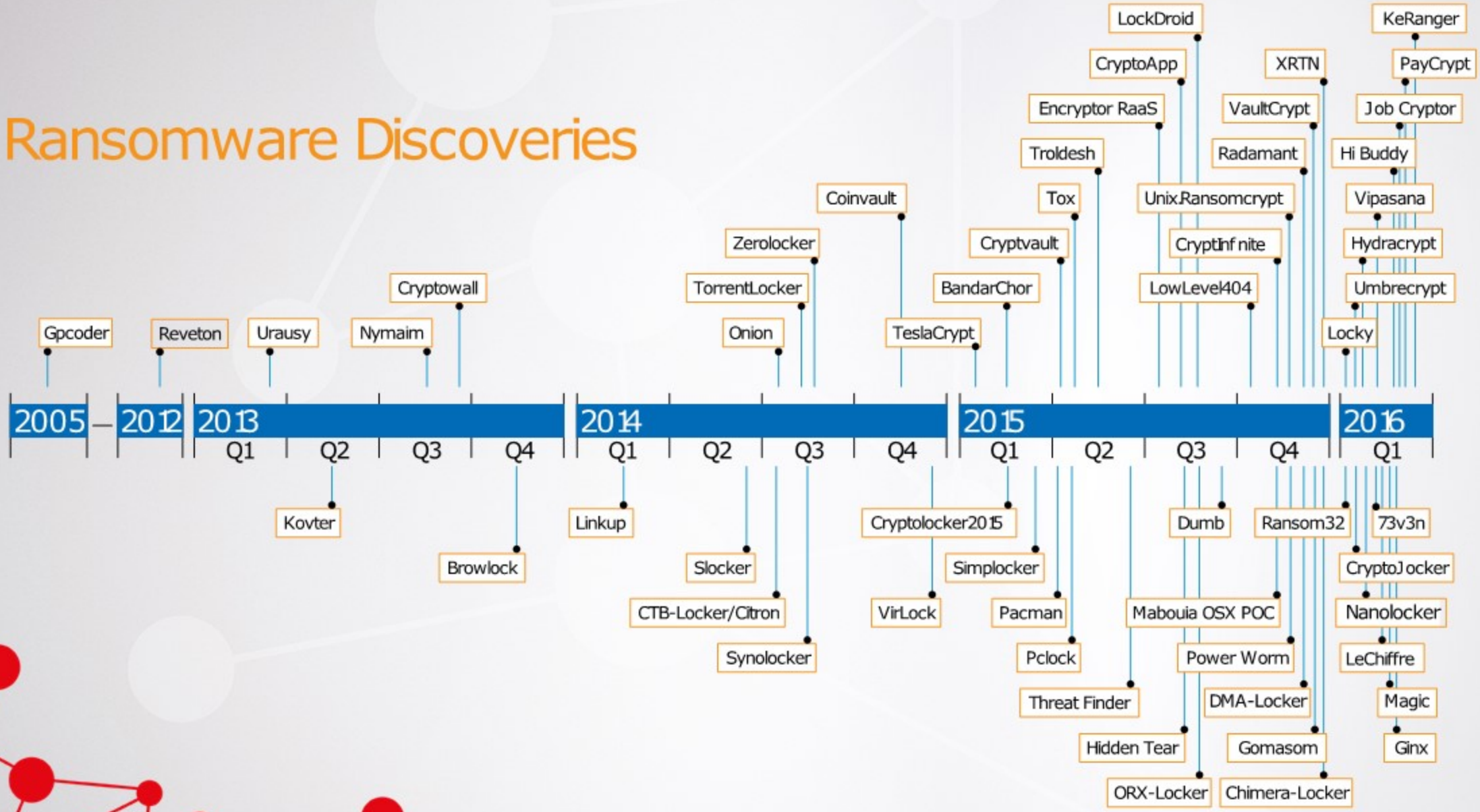
Size of circle estimates relative impact of incident in terms of cost to business, based on publicly disclosed information regarding leaked records and financial losses.



Sampling of security incidents by attack type, time and impact, 2013 through 2015

Source: IBM X-Force® Research and Development

Ransomware Discoveries



zdroj: Symantec

KASPERSKY lab

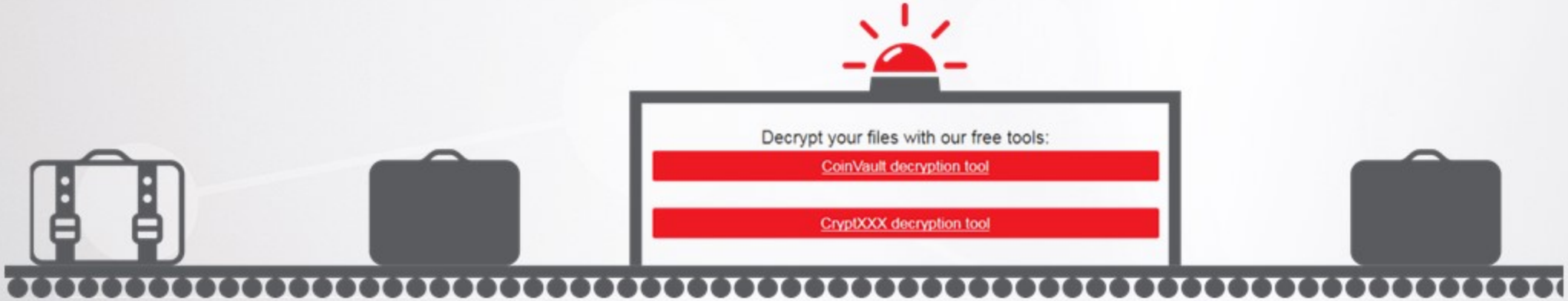
RANSOMWARE DECRYPTOR

Are you a ransomware victim? The National High Tech Crime Unit (NHTCU) of the Netherlands' police, the Netherlands' National Prosecutors Office and Kaspersky Lab, have been working together to fight the CoinVault and Bitcryptor ransomware campaigns. During our joint investigation we have obtained data that can help you to decrypt the files being held hostage on your PC. We are now able to share a new decryption application that will automatically decrypt all files for Coinvault and Bitcryptor victims. For more information please see this how-to guide.

We are considering this case as closed. The ransomware authors are arrested and all existing keys have been added to our database.

CryptXXX has been decrypted. Kaspersky Lab developed a decryption tool which is now available for downloading. How to know that you are Trojan CryptXXX victim: in case of an infection your files extensions will be changed according to the template <original name>.crypt. For more information please see this how-to guide.

April 26, 2016 update: CryptXXX has been decrypted
October 28, 2015 update: ALL Coinvault and Bitcryptor keys (14k+) added to the database
April 29, 2015 update: 13 decryption keys added to the database



zdroj: https://noransom.kaspersky.com/

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

Patients diverted to other hospitals after ransomware locks down key software

Crypto-extortion increasingly targets bigger victims; most stay silent about it.

SEAN GALLAGHER - 2/17/2016, 3:56 PM

Hollywood Presbyterian Medical Center has shut down much of its network for the past week because of ransomware, causing the diversion of some emergency patients to other hospitals, according to sources at the hospital.

zdroj: arstechnica.com

MalwareHunterTeam

ID Ransomware

ID Ransomware is a free website that helps victims identify what ransomware may have encrypted their files. The site is able to identify over 300+ ransomware families by specific filename extensions and patterns, ransom note names, known hex patterns, email addresses, BitCoin addresses, and more. If a ransomware is identified, ID Ransomware will give the victim a distinct status on whether it is known to be decryptable or not, and will provide a link to a credible source for more information.

Open

zdroj: https://id-ransomware.malwarehunterteam.com/

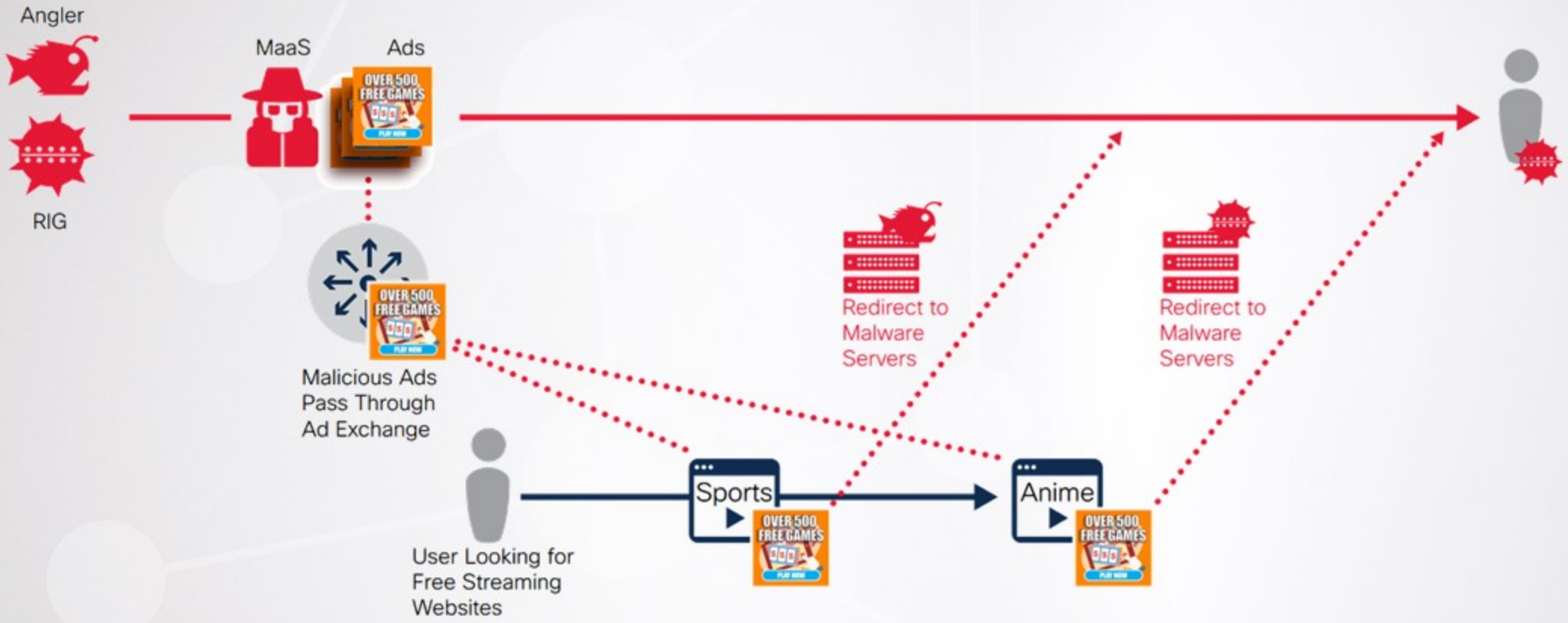
Which ransomwares are detected?

This service currently detects **339** different ransomwares. Here is a complete, dynamic list of what is currently detected:

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, AngryDuck, Anubis, Apocalypse, Apocalypse (New Variant), ApocalypseVM, ASN1 Encoder, AutoLocky, AxCrypter, BadBlock, BadEncript, Bandarchor, BankAccountSummary, Bart, Bart v2.0, BitCrypt, BitCrypt 2.0, BitCryptor, BitStak, Black Feather, Black Shades, Blocatto, Booyah, **BrainCrypt**, Brazilian Ransomware, BTCamant, Bucbi, BuyUnlockCode, Cancer, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberTear, Chimera, CHIP, CockBlocker, Coin Locker, CoinVault, Comrade Circle, Coverton, Cripton, **CrptXXX**, 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**, CryptON, Crypton, CryptorBit, CryptoRoger, CryptoShield, CryptoShocker, CryptoTorLocker, 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, Deadly, DEDCryptor, DeriaLock, Dharma (.dharma), Dharma (.wallet), Digisom, DirtyDecrypt, DMA Locker, DMA Locker 3.0, DMA Locker 4.0, DMALocker Imposter, Domino, Done, DXXD, DynA-Crypt, ECLR Ransomware, EdgeLocker, EduCrypt, El Polocker, EncrypTile, EncryptoJJS, Encryptor RaaS, Enigma, Enjey Crypter, EnkripsiPC, Erebus, Evil, Exotic, Fabiansomware, Fadesoft, Fantom, FenixLocker, **FindZip**, FireCrypt, FLKR, Flyper, FS0ciety, FuckSociety, FunFact, GC47, GhostCrypt, Globe, Globe3, GlobeImposter, GlobeImposter 2.0, **GOG**, GoldenEye, Gomasom, GPCode, HadesLocker, Heimdall, HelpDCFile, Herbst, **Hermes**, **Hermes 2.0**, Hi Buddy!, HollyCrypt, HolyCrypt, Hucky, HydraCrypt, IFN643, iRansom, Ishtar, Jack.Pot, Jager, JapanLocker, Jigsaw, Jigsaw (Updated), JobCrypter, JuicyLemon, Kaenlupuf, Karma, **Karmen**, Kasiski, KawaiiLocker, KeRanger, KeyBTC, KEYHolder, KillerLocker, KimcilWare, **Kirk**, Kolobo, Kostya, Kozy.Jozy, Kraken, KratosCrypt, Krider, Kriptovor, KryptoLocker, L33TAF Locker, LambdaLocker, LeChiffre, Lock2017, Lock93, Locked-In, LockLock, Locky, Lortok, LoveServer, LowLevel04, Magic, Maktub Locker, Marlboro, MarsJoke, Matrix, MirCop, MireWare, Mischa, MNS CryptoLocker, Mobef, **MOTD**, MRCR1, n1n1n1, NanoLocker, NCrypt, Negozl, Nemucod, Nemucod-7z, Netix, Nhtnwcuf, NMoreira, NMoreira 2.0, Nuke, NullByte, ODCODC, OpenToYou, OzozaLocker, PadCrypt, PayDay, PaySafeGen, PClock, PClock (Updated), Philadelphia, Pickles, Polski Ransomware, PopCornTime, Potato, PowerLocky, PowerShell Locker, PowerWare, PrincessLocker, PrincessLocker 2.0, **Project34**, Protected Ransomware, PyL33T, R980, RAA-SEP, Radamant, Radamant v2.1, RanRan, RansomCuck, RansomPlus, RarVault, Razy, REKTLocker, RemindMe, RenLocker, Roga, Rokku, **RoshaLock**, RotorCrypt, Roza, Russian EDA2, Sage 2.0, SamSam, Sanction, Satan, Satana, SerbRansom, Serpent, ShellLocker, Shigo, ShinoLocker, Shujin, Simple_Encoder, Smrss32, SNSLocker, Spora, Sport, SQ_, Stampado, 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, UmbreCrypt, UnblockUPC, Ungluk, Unknown Crypted, Unknown Lock, Unknown XTBL, Unlock26, Unlock92, Unlock92 2.0, UserFilesLocker, USR0, Uyari, V8Locker, VaultCrypt, VenisRansomware, VenusLocker, VindowsLocker, **Vortex**, VxLock, Wcry, WildFire Locker, Winnix Cryptor, WinRarer, WonderCrypter, X Locker 5.0, XCrypt, Xorist, Xort, XRTN, XTP Locker 5.0, XYZWare, YouAreFucked, YouRansom, zCrypt, Zekwacrypt, ZeroCrypt, ZimbraCryptor, **ZinoCrypt**, Zyklon

zdroj: https://id-ransomware.malwarehunterteam.com/

zdroj: Ahnlab



Source: Cisco Security Research

Figure 14 IP Blocks by Country, December 2015–November 2016

Source: Cisco Security Research

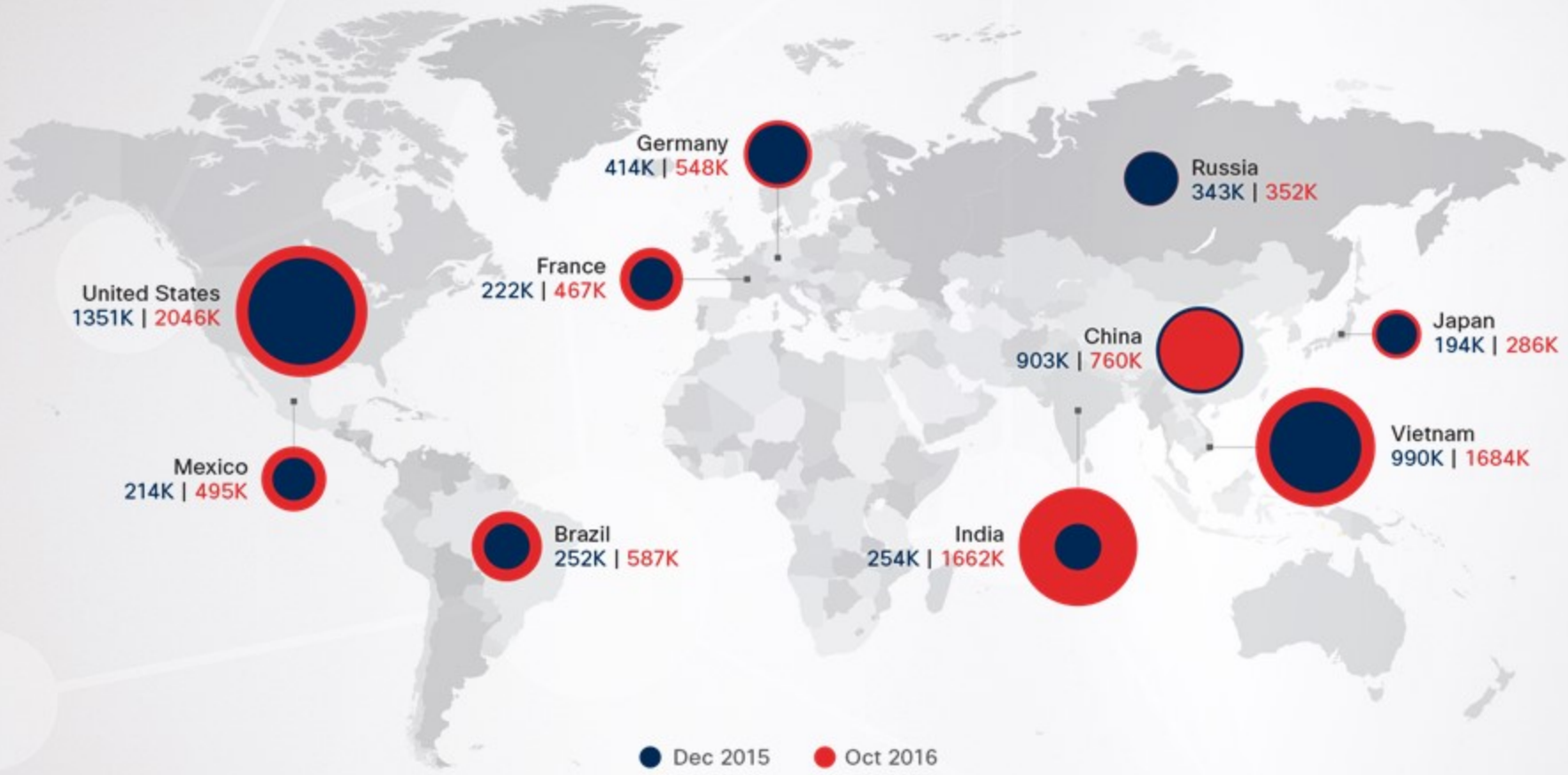


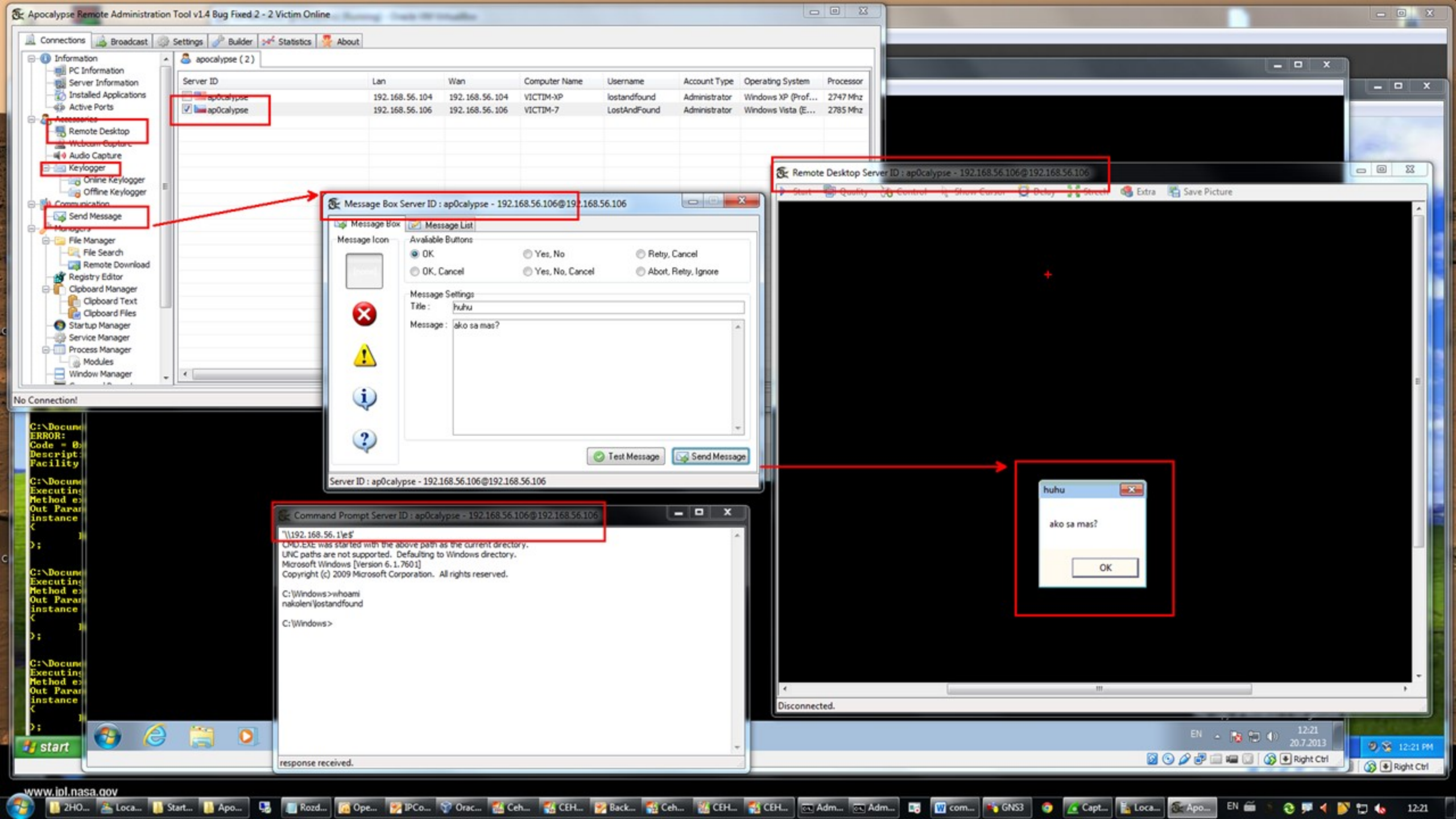
Figure 18 Comparison of Hailstorm and Snowshoe Spam Attacks

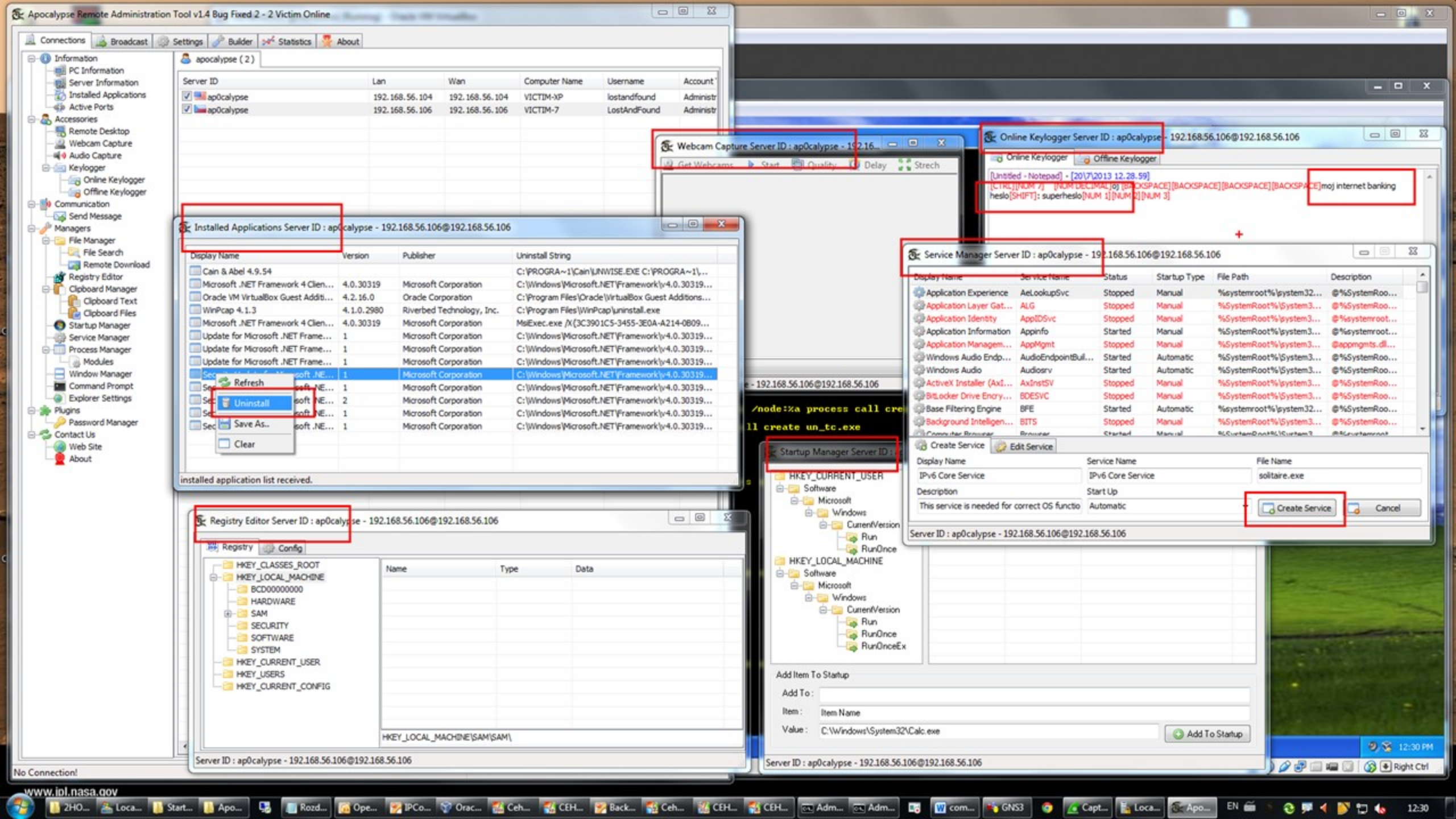
Source: Cisco Investigate

Advanced Malware		Ransomware
	vs.	
A new or unknown malware plays key role in security breach		Advanced malware causes financial damages and interferes with access to information assets
Advanced Uses various advanced attack techniques	=	**Advanced** Uses various advanced attack techniques
Targeted Specific targets	≠	**Non-Targeted** Random targets
Persistent Infects and remains stealthy	≠	**Non-Persistent** Exposes infection and demands ransom by the set time

APT skupina známá jako Sofacy, APT28, Fancy Bear, Sednit či Pawn Storm šíří malware zvaný Komplex na Mac OS X. **Tento trojský kůň se šíří phishingovou kampaní a zaměřuje se na osoby působící v leteckém průmyslu.**

Malware používá několik anti-analysis a sandbox technik, jedna z kampaní uměla využít chybu MacKeeper antiviru ke svému šíření a velmi se podobá Carberpu. Dropper je instalován do /tmp/content a jeho SHA256 hash je:
`96a19a90caa41406b632a2046f3a39b5579fbf730aca2357f84bf23f2cbc1fd3`.


Apocalypse Remote Administration Tool v1.4 Bug Fixed 2 - 2 Victim Online
Connections
Broadcast
Settings
Builder
Statistics
About
Information
PC Information
Server Information
Installed Applications
Active Ports
Remote Desktop
Audio Capture
Keylogger
Online Keylogger
Offline Keylogger
Send Message
File Manager
File Search
Remote Download
Registry Editor
Clipboard Manager
Clipboard Text
Clipboard Files
Startup Manager
Service Manager
Process Manager
Modules
Window Manager
apocalypse (2)
Server ID
Lan
Wan
Computer Name
Username
Account Type
Operating System
Processor
192.168.56.104
192.168.56.104
VICTIM-XP
lostandfound
Administrator
Windows XP (Prof...
2747 Mhz
ap0calypse
192.168.56.106
192.168.56.106
VICTIM-7
LostAndFound
Administrator
Windows Vista (E...
2785 Mhz
No Connection!
Message Box Server ID : ap0calypse - 192.168.56.106@192.168.56.106
Message Box
Message List
Message Icon
Available Buttons
OK
Yes, No
Retry, Cancel
OK, Cancel
Yes, No, Cancel
Abort, Retry, Ignore
Message Settings
Title :
huhu
Message :
ako sa mas?
Test Message
Send Message
Server ID : ap0calypse - 192.168.56.106@192.168.56.106
Remote Desktop Server ID : ap0calypse - 192.168.56.106@192.168.56.106
Start
Quality
Control
Show Cursor
Delay
Stretch
Extra
Save Picture
Disconnected.
huhu
ako sa mas?
OK
Command Prompt Server ID : ap0calypse - 192.168.56.106@192.168.56.106
'\\192.168.56.1\e$'
CMD.EXE was started with the above path as the current directory.
UNC paths are not supported. Defaulting to Windows directory.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows>whoami
nakoleni\lostandfound
C:\Windows>
response received.
start
www.ipl.nasa.gov


Apocalypse Remote Administration Tool v1.4 Bug Fixed 2 - 2 Victim Online
Connections
Broadcast
Settings
Builder
Statistics
About
Information
PC Information
Server Information
Installed Applications
Active Ports
Accessories
Remote Desktop
Webcam Capture
Audio Capture
Keylogger
Online Keylogger
Offline Keylogger
Communication
Send Message
Managers
File Manager
File Search
Remote Download
Registry Editor
Clipboard Manager
Clipboard Text
Clipboard Files
Startup Manager
Service Manager
Process Manager
Modules
Window Manager
Command Prompt
Explorer Settings
Plugins
Password Manager
Contact Us
Web Site
About
apocalypse (2)
Server ID
Lan
Wan
Computer Name
Username
Account
ap0calypse
192.168.56.104
192.168.56.104
VICTIM-XP
lostandfound
Administr
ap0calypse
192.168.56.106
192.168.56.106
VICTIM-7
LostAndFound
Administr
No Connection!
Webcam Capture Server ID : ap0calypse - 192.16...
Get Webcams
Start
Quality
Delay
Strech
Online Keylogger Server ID : ap0calypse - 192.168.56.106@192.168.56.106
Online Keylogger
Offline Keylogger
[Untitled - Notepad] - [20\7\2013 12.28.59]
[CTRL][NUM 7] [NUM DECIMAL]oj [BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE]moj internet banking
heslo[SHIFT]: superheslo[NUM 1][NUM 2][NUM 3]
Installed Applications Server ID : ap0calypse - 192.168.56.106@192.168.56.106
Display Name
Version
Publisher
Uninstall String
Cain & Abel 4.9.54
C:\PROGRA~1\Cain\UNWISE.EXE C:\PROGRA~1\...
Microsoft .NET Framework 4 Clien...
4.0.30319
Microsoft Corporation
C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Oracle VM VirtualBox Guest Additi...
4.2.16.0
Oracle Corporation
C:\Program Files\Oracle\VirtualBox Guest Additions...
WinPcap 4.1.3
4.1.0.2980
Riverbed Technology, Inc.
C:\Program Files\WinPcap\uninstall.exe
Microsoft .NET Framework 4 Clien...
4.0.30319
Microsoft Corporation
MsiExec.exe /X{3C3901C5-3455-3E0A-A214-0B09...
Update for Microsoft .NET Frame...
1
Microsoft Corporation
C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Refresh
Uninstall
Save As..
Clear
installed application list received.
Service Manager Server ID : ap0calypse - 192.168.56.106@192.168.56.106
Display Name
Service Name
Status
Startup Type
File Path
Description
Application Experience
AeLookupSvc
Stopped
Manual
%systemroot%\system32...
@%SystemRoo...
Application Layer Gat...
ALG
Stopped
Manual
%SystemRoot%\System3...
@%SystemRoo...
Application Identity
AppIDSvc
Stopped
Manual
%SystemRoot%\system3...
@%systemroot...
Application Information
Appinfo
Started
Manual
%SystemRoot%\system3...
@%systemroot...
Application Managem...
AppMgmt
Stopped
Manual
%SystemRoot%\system3...
@appmgmts.dll...
Windows Audio Endp...
AudioEndpointBuil...
Started
Automatic
%SystemRoot%\System3...
@%SystemRoo...
Windows Audio
Audiosrv
Started
Automatic
%SystemRoot%\System3...
@%SystemRoo...
ActiveX Installer (AxI...
AxInstSV
Stopped
Manual
%SystemRoot%\system3...
@%SystemRoo...
BitLocker Drive Encry...
BDESVC
Stopped
Manual
%SystemRoot%\System3...
@%SystemRoo...
Base Filtering Engine
BFE
Started
Automatic
%systemroot%\system32...
@%SystemRoo...
Background Intelligen...
BITS
Stopped
Manual
%SystemRoot%\System3...
@%SystemRoo...
Create Service
Edit Service
Display Name
IPv6 Core Service
Service Name
IPv6 Core Service
File Name
solitaire.exe
Description
This service is needed for correct OS functio
Start Up
Automatic
Create Service
Cancel
Server ID : ap0calypse - 192.168.56.106@192.168.56.106
/node:%a process call cre
ll create un_tc.exe
Registry Editor Server ID : ap0calypse - 192.168.56.106@192.168.56.106
Registry
Config
HKEY_CLASSES_ROOT
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
HKEY_CURRENT_USER
HKEY_USERS
HKEY_CURRENT_CONFIG
Name
Type
Data
HKEY_LOCAL_MACHINE\SAM\SAM\
Server ID : ap0calypse - 192.168.56.106@192.168.56.106
Startup Manager Server ID :
HKEY_CURRENT_USER
Software
Microsoft
Windows
CurrentVersion
Run
RunOnce
HKEY_LOCAL_MACHINE
Software
Microsoft
Windows
CurrentVersion
Run
RunOnce
RunOnceEx
Add Item To Startup
Add To :
Item :
Item Name
Value :
C:\Windows\System32\Calc.exe
Add To Startup
Server ID : ap0calypse - 192.168.56.106@192.168.56.106
www.ipl.nasa.gov
12:30 PM
Right Ctrl

virustotal

SHA256: 29d8537a4f60902501c280758788212293b472095a7a1c715395aec779529714

File name: receipt_4676373.doc

Detection ratio: 6 / 56

Analysis date: 2016-05-09 08:14:55 UTC (1 minute ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
AhnLab-V3	W97M/Downloader	20160508
Avast	MO97:Downloader-MN [Trj]	20160509
CAT-QuickHeal	W97M.Dropper.CB	20160509
ClamAV	Doc.Downloader.Macro-26	20160508
Fortinet	W97M/Agent.29D8ltr	20160509
Ikarus	Trojan-Downloader.VBA.Agent	20160509
ALYac	✓	20160509
AVG	✓	20160509
AVware	✓	20160509
Ad-Aware	✓	20160509
AegisLab	✓	20160509
Alibaba	✓	20160509
Antiy-AVL	✓	20160509


Justin Schuh
@justinschuh
Sledovať
@Allan_Wirth @tqbf That's fair. Defender is the only one I know of that hasn't broken Chrome's security mechanisms. /CC @taviso
POČET RETWEETOV: 9
PÁČI SA MI TO: 22
17:34 - 30. 1. 2017
1
9
22
Will Harris @parityzero · 31. 1.
@justinschuh @Allan_Wirth @tqbf @taviso This is correct - and we have data
support this statement.
3
5
18
Tavis Ormandy
@taviso
Follow
Srsly Avast? If you're gonna mitm chrome's SSL at least get an intern to skim your X.509 parsing before shipping it.
explorer.exe 0.09 12.4 MB 3.0 MB 44,280 K 59,412 K 243
vmtoolsd.exe 0.07 28.2 KB 33.7 KB 7,808 K 15,860 K 255
AvastUI.exe 0.01 9.1 MB 1.2 MB 30,952 K 51,504 K 395
calc.exe 60 B 4,956 K 10,464 K 470
RETWEETS 371
LIKES 258
3:54 PM - 25 Sep 2015
14
371
258

Avast Antivirus: X.509 Error Rendering Command Execution

Project Member Reported by taviso@google.com, Sep 25 2015

Avast will render the commonName of X.509 certificates into an HTMLLayout frame when your MITM proxy detects a bad signature.
Unbelievably, this means CN="<h1>really?!?!?</h1>" actually works, and is pretty simple to convert into remote code execution.

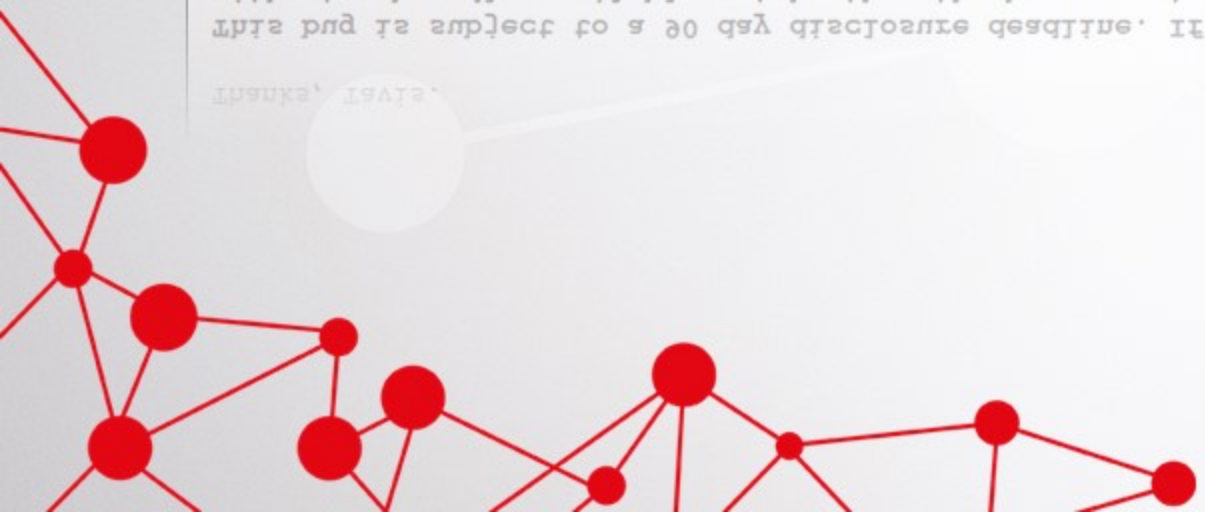
To verify this bug, I've attached a demo certificate for you. Please find attached key.pem, cert.pem and cert.der. Run this command to serve it from a machine with openssl:

```
$ sudo openssl s_server -key key.pem -cert cert.pem -accept 443
```

Then visit that https server from a machine with Avast installed. Click the message that appears to demonstrate launching calc.exe.

Thanks, Tavis.

This bug is subject to a 90 day disclosure deadline. If 90 days elapse without a broadly available patch, then the bug report will automatically become visible to the public.



Project Member Comment 1 by taviso@google.com, Dec 15 2015

I sent the angry email below to the vendor:

Hello, I've just been looking at your antivirus product, and the first thing I noticed was you force install a Chrome extension called "AVG Web TuneUp" with extension id chfdnecihphmhljaaejmgoiahnihplgn. I can see from our statistics it has nearly 9 million active Chrome users.

Apologies for my harsh tone, but I'm really not thrilled about this trash being installed for Chrome users. The extension is so badly broken that I'm not sure whether I should be reporting it to you as a vulnerability, or asking the extension abuse team to investigate if it's a PuP.

Nevertheless, my concern is that your security software is disabling web security for 9 million Chrome users, apparently so that you can hijack search settings and the new tab page.

There are multiple obvious attacks possible, for example, here is a trivial universal xss in the "navigate" API that can allow any website to execute script in the context of any other domain. For example, attacker.com can read email from mail.google.com, or corp.avg.com, or whatever else. I hope the severity of this issue is clear to you, fixing it should be your highest priority.

```
<script>
    for (i = 0; i < 256; i++) {
        window.postMessage({ origin: "web", action: "navigate", data: {
           url: "javascript:document.location.hostname.endsWith('.avg.com')"
                + "?"
                    + "alert(document.domain + ':' +document.cookie)"
                + ":"
                    + "false",
           tabID: i
        }}, "*");
    }
</script>
```

This demo will just alert(document.cookie) if you have a tab open on avg.com, but you get the idea. That's not all, basically every API I look at is just plain broken. For example, you're exposing browsing history to the internet via the "recently" api. This code should tell you all your recent navigations:

```
<script>
window.addEventListener("message", receiveMessage, false);
window.postMessage({ from: "web", to: "content", method: "recently" }, "*")
```

zdroj: https://bugs.chromium.org/p/project-zero/issues/detail?id=675&redir=1

Your computer files have been encrypted. _

Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.

Thank you _

59:56

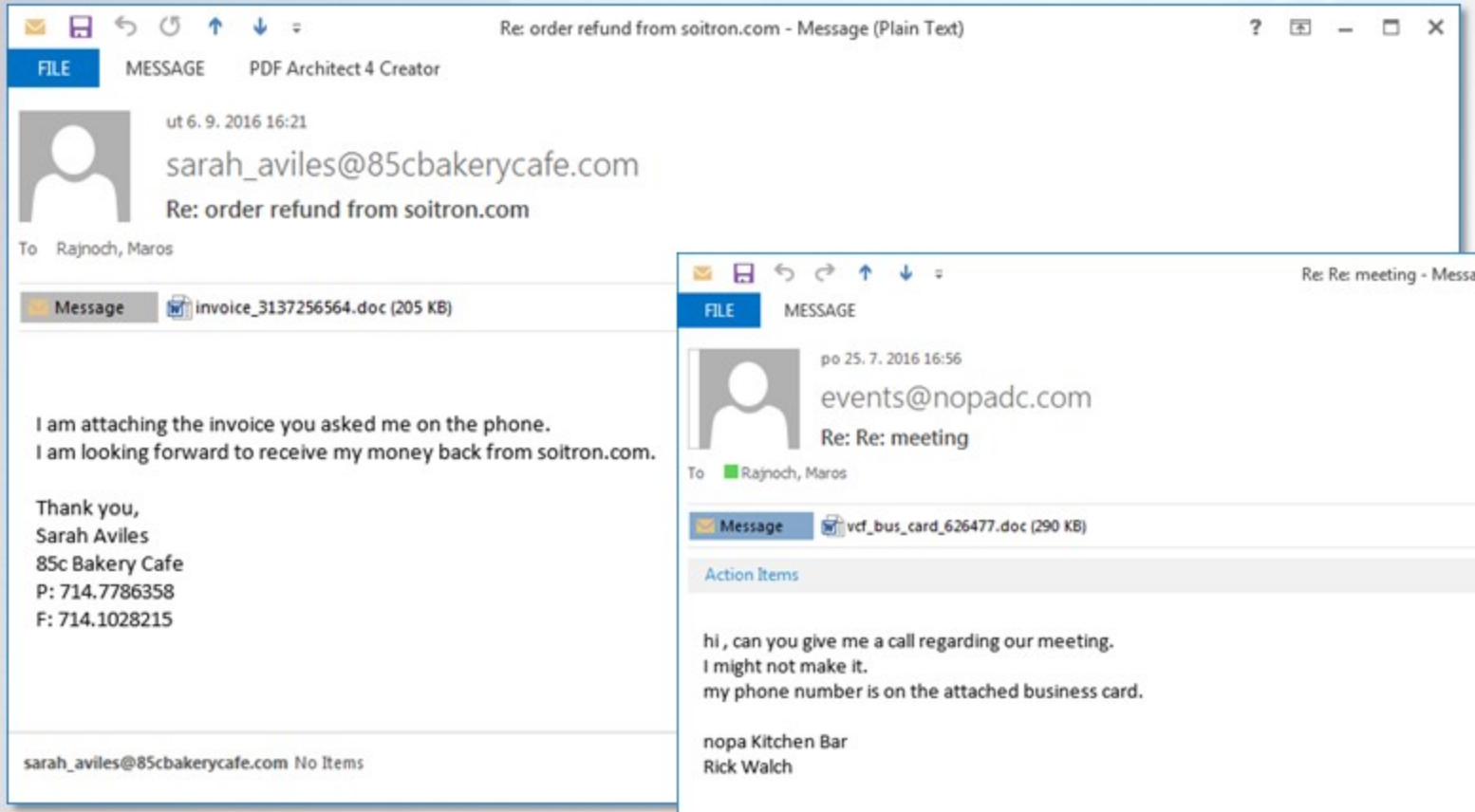
1 file will be deleted.

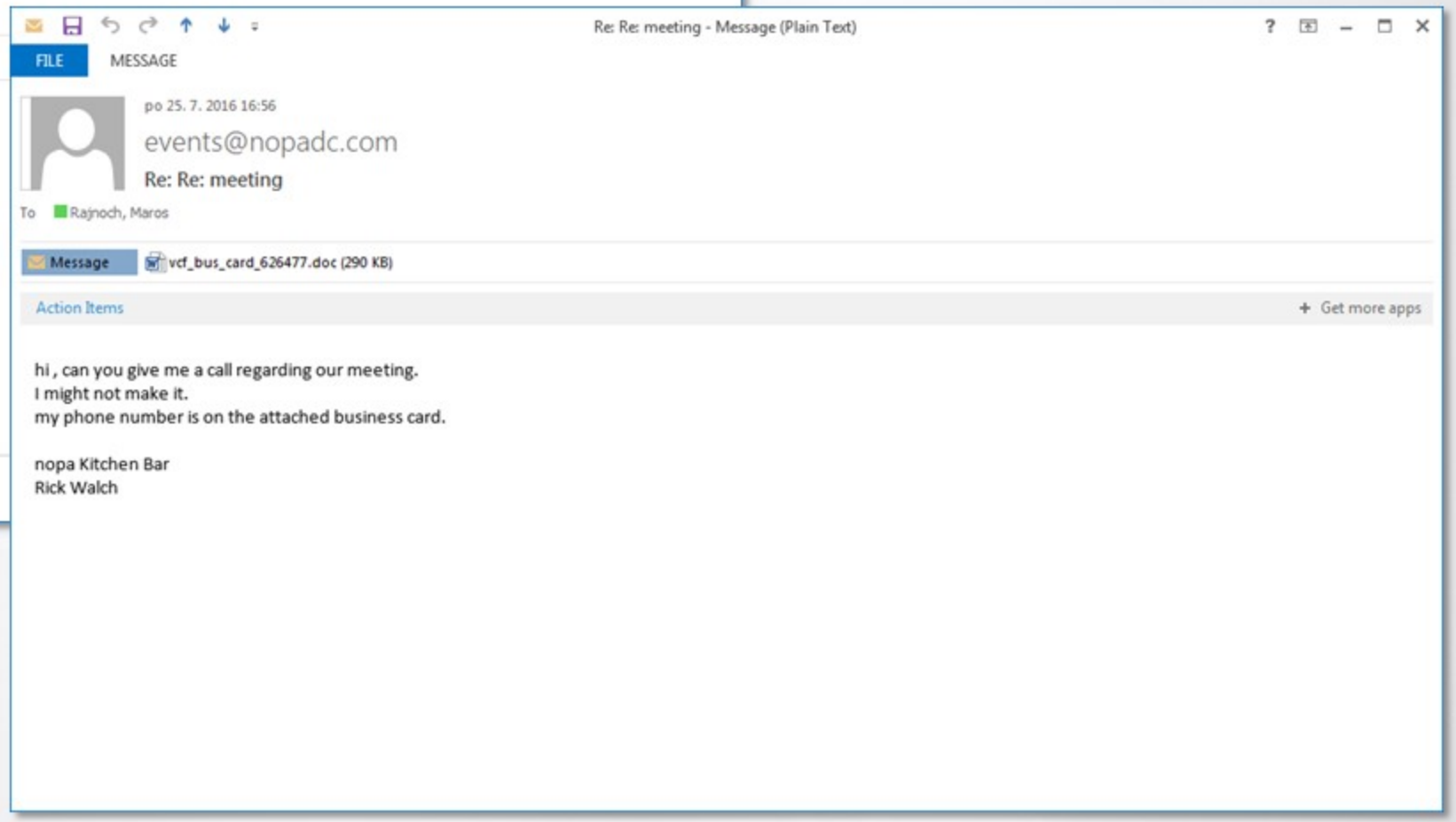
View encrypted files

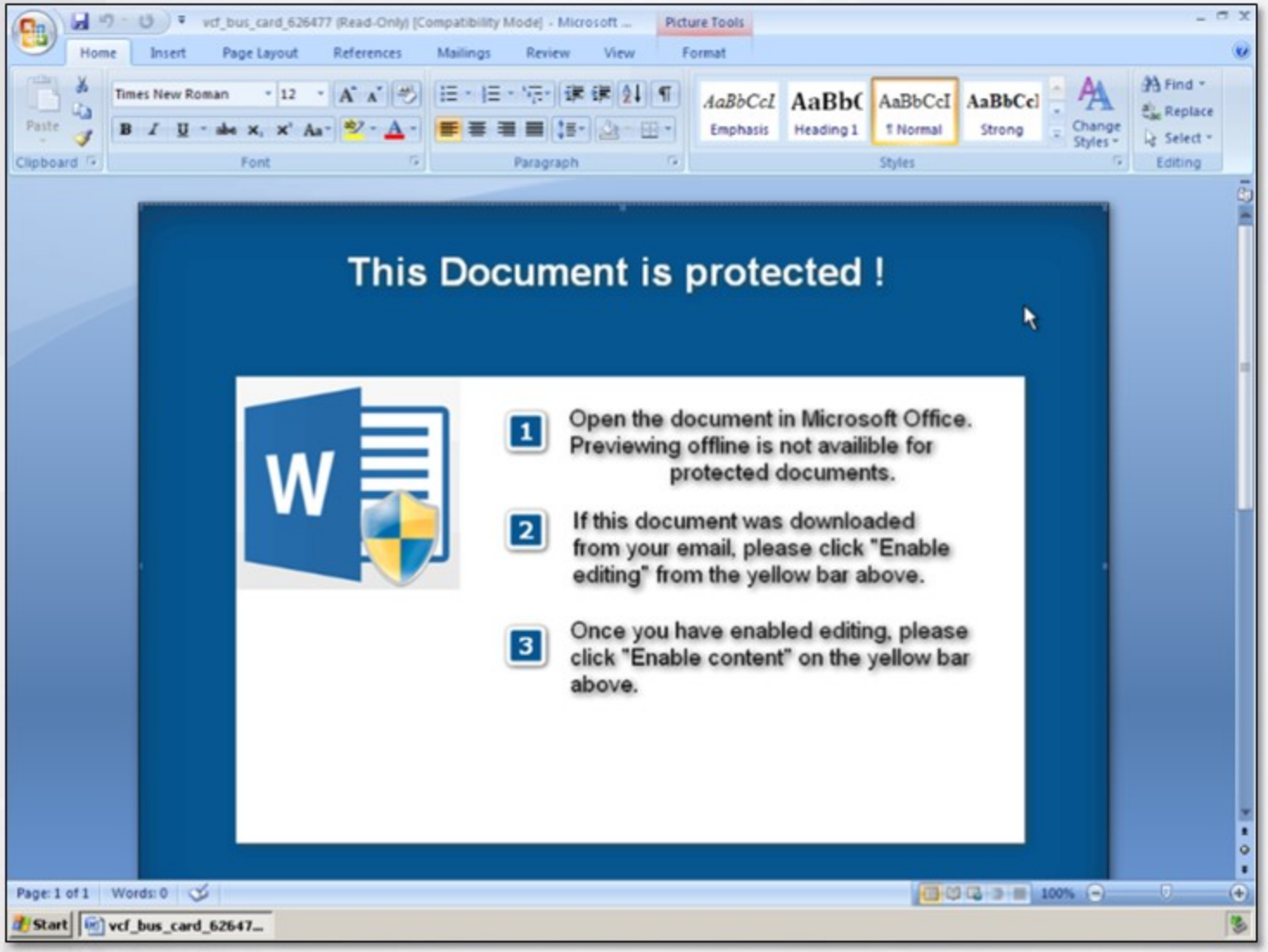
Please, send $150 worth of Bitcoin here:

15fbyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ

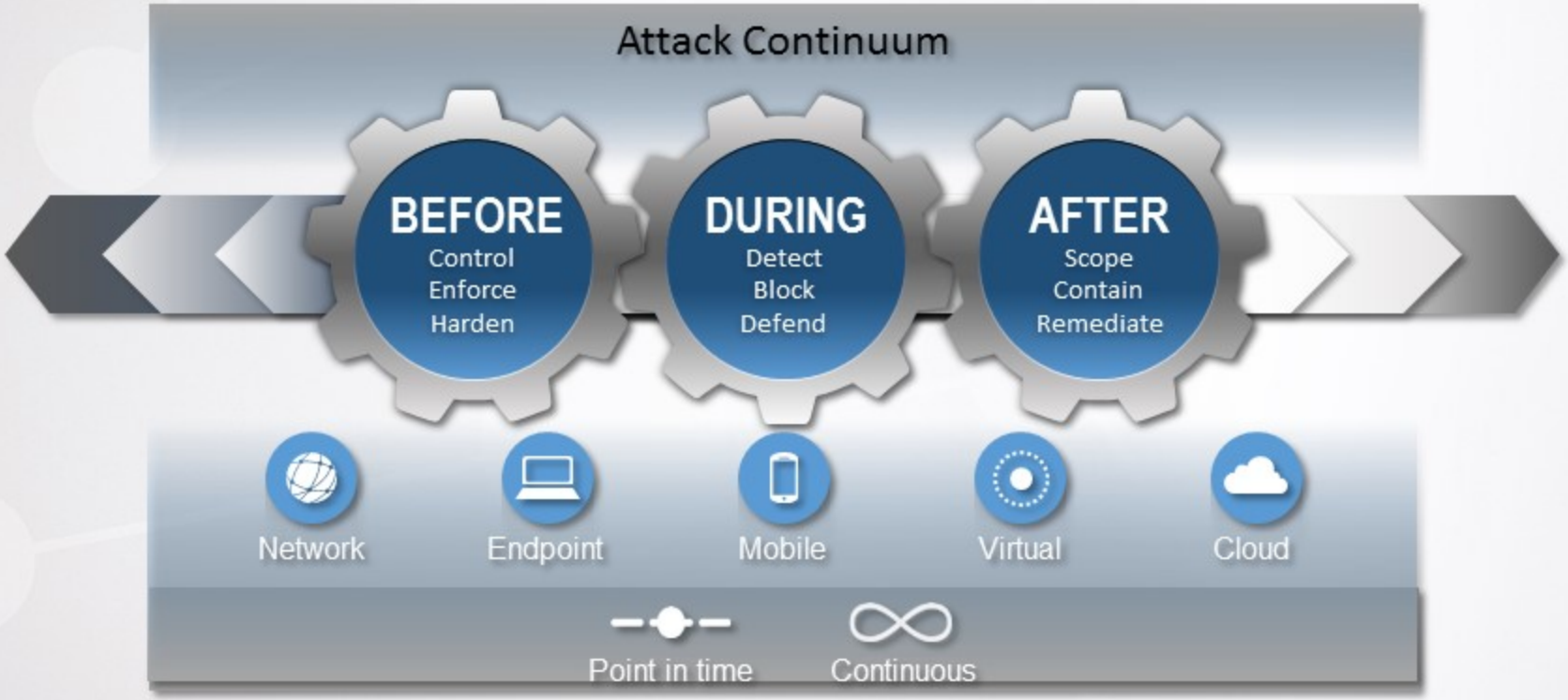
I made a payment, now give me back my files!

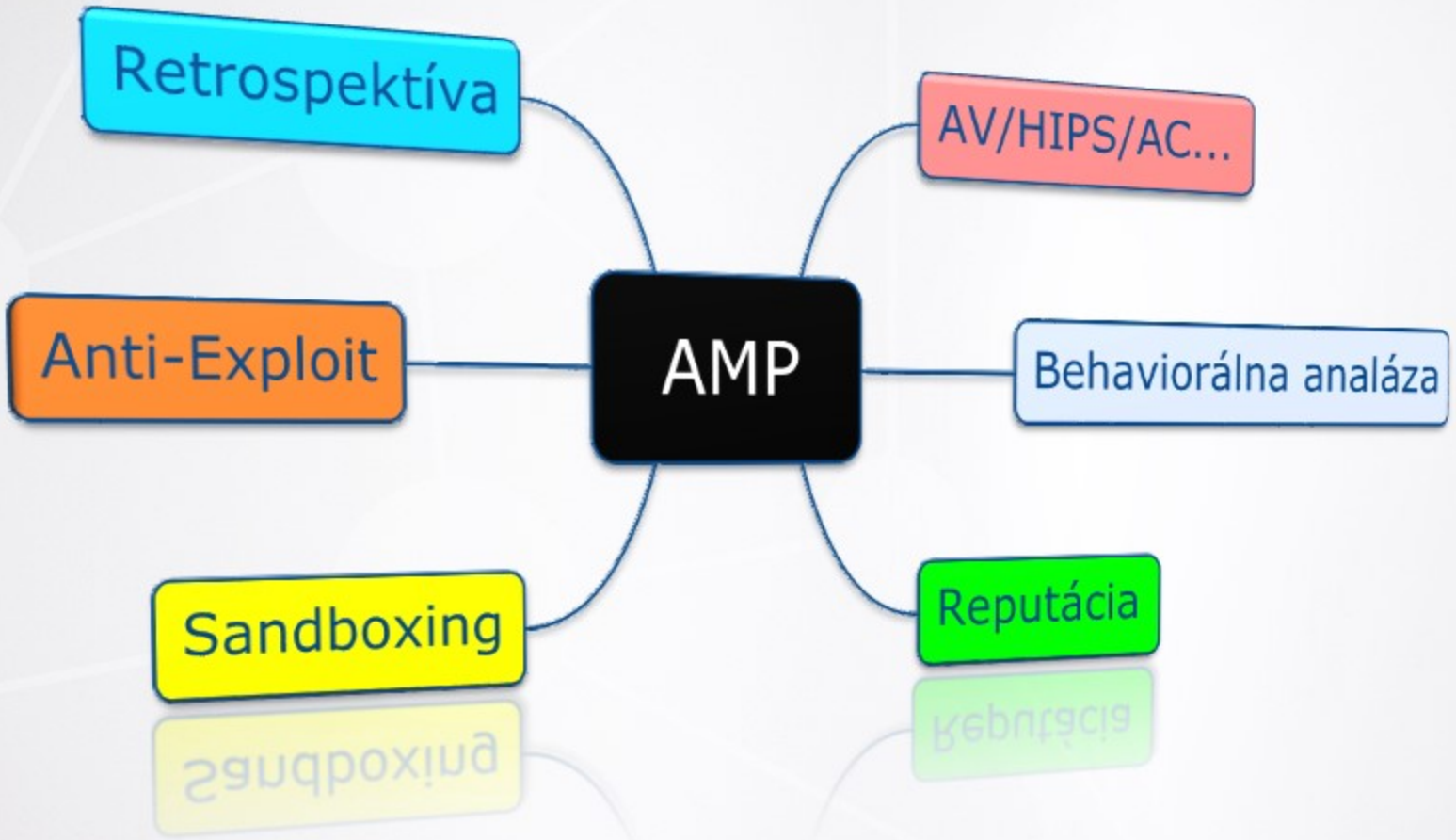

Re: order refund from soitron.com - Message (Plain Text)
FILE
MESSAGE
PDF Architect 4 Creator
ut 6. 9. 2016 16:21
sarah_aviles@85cbakerycafe.com
Re: order refund from soitron.com
To Rajnoch, Maros
Message
invoice_3137256564.doc (205 KB)
I am attaching the invoice you asked me on the phone.
I am looking forward to receive my money back from soitron.com.
Thank you,
Sarah Aviles
85c Bakery Cafe
P: 714.7786358
F: 714.1028215
sarah_aviles@85cbakerycafe.com No Items


Re: Re: meeting - Message (Plain Text)
FILE
MESSAGE
po 25. 7. 2016 16:56
events@nopadc.com
Re: Re: meeting
To Rajnoch, Maros
Message
vcf_bus_card_626477.doc (290 KB)
Action Items
+ Get more apps
hi , can you give me a call regarding our meeting.
I might not make it.
my phone number is on the attached business card.
nopa Kitchen Bar
Rick Walch


vcf_bus_card_626477 (Read-Only) [Compatibility Mode] - Microsoft ...
Picture Tools
Home
Insert
Page Layout
References
Mailings
Review
View
Format
Times New Roman
12
Paste
Clipboard
Font
Paragraph
Emphasis
Heading 1
Normal
Strong
Change Styles
Find
Replace
Select
Editing
Styles
This Document is protected !
1
Open the document in Microsoft Office. Previewing offline is not availible for protected documents.
2
If this document was downloaded from your email, please click "Enable editing" from the yellow bar above.
3
Once you have enabled editing, please click "Enable content" on the yellow bar above.
Page: 1 of 1
Words: 0
100%
Start
vcf_bus_card_62647...

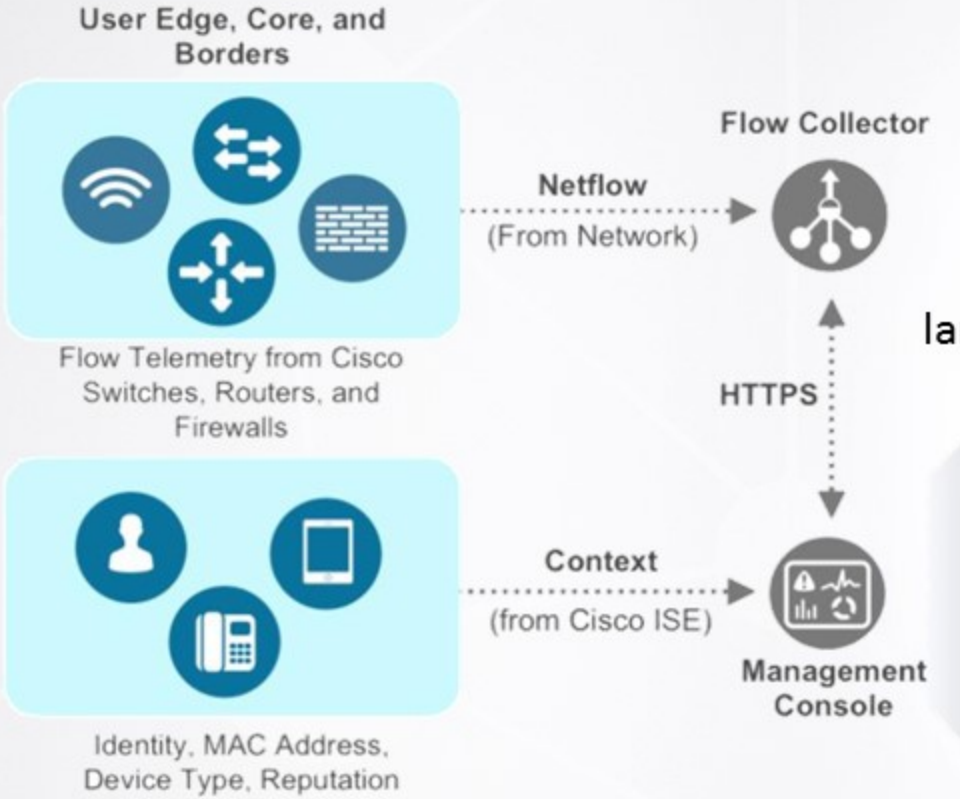

Ransomware Attack Process
Connects to portal and SNS
Downloads malware
Infected by ransomware
Searches for document files
Encrypts files
Demands payment


Attack Continuum
BEFORE
Control
Enforce
Harden
DURING
Detect
Block
Defend
AFTER
Scope
Contain
Remediate
Network
Endpoint
Mobile
Virtual
Cloud
Point in time
Continuous


Retrospektíva
AV/HIPS/AC...
Anti-Exploit
AMP
Behaviorálna analáza
Sandboxing
Reputácia

Behaviorálna analýza

- Reputácia
- Sandboxing
- Anti-Exploit
- Retrospektíva

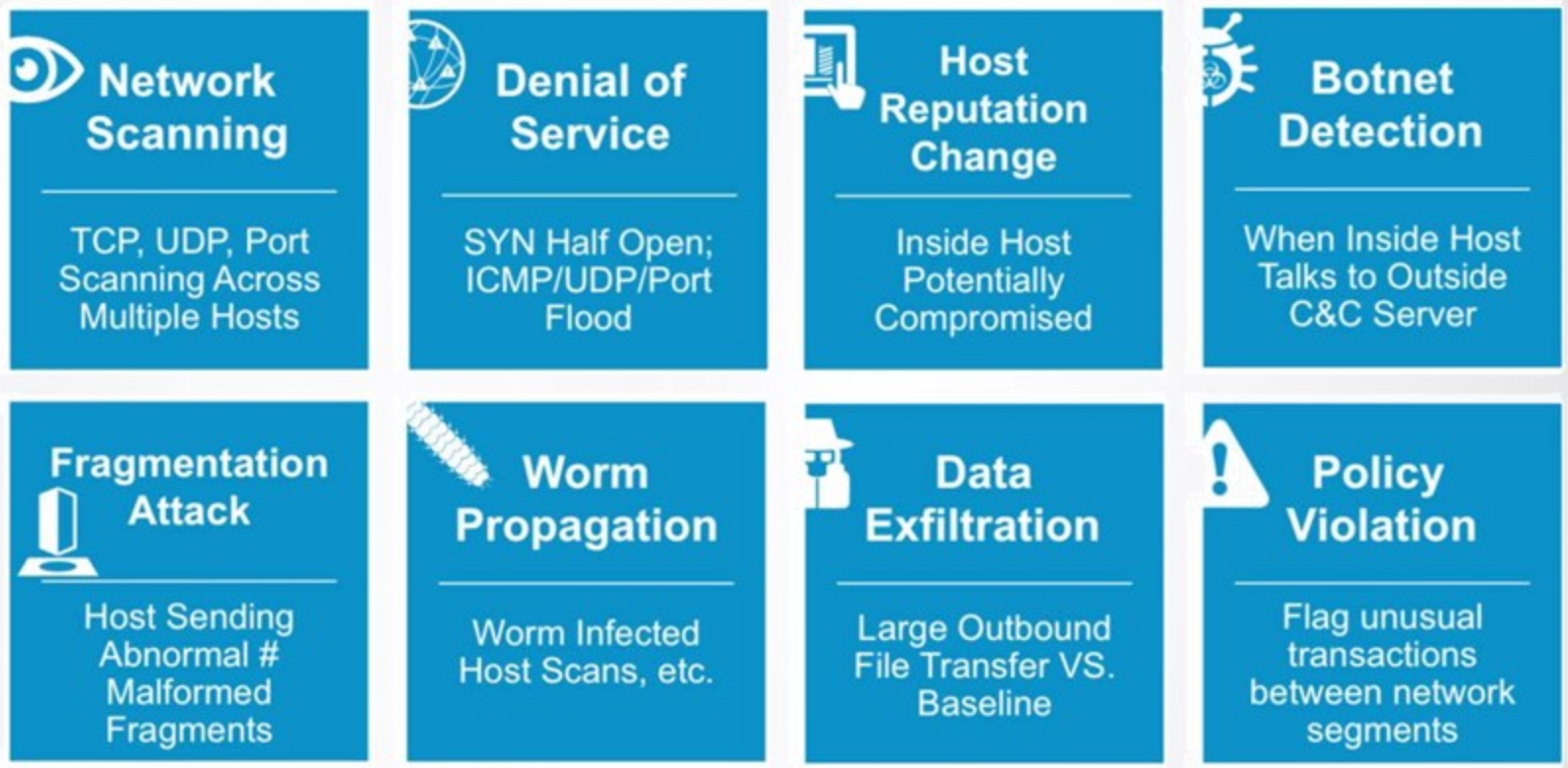


lancope: netflow based anomaly detection

Behaviorálna analýza

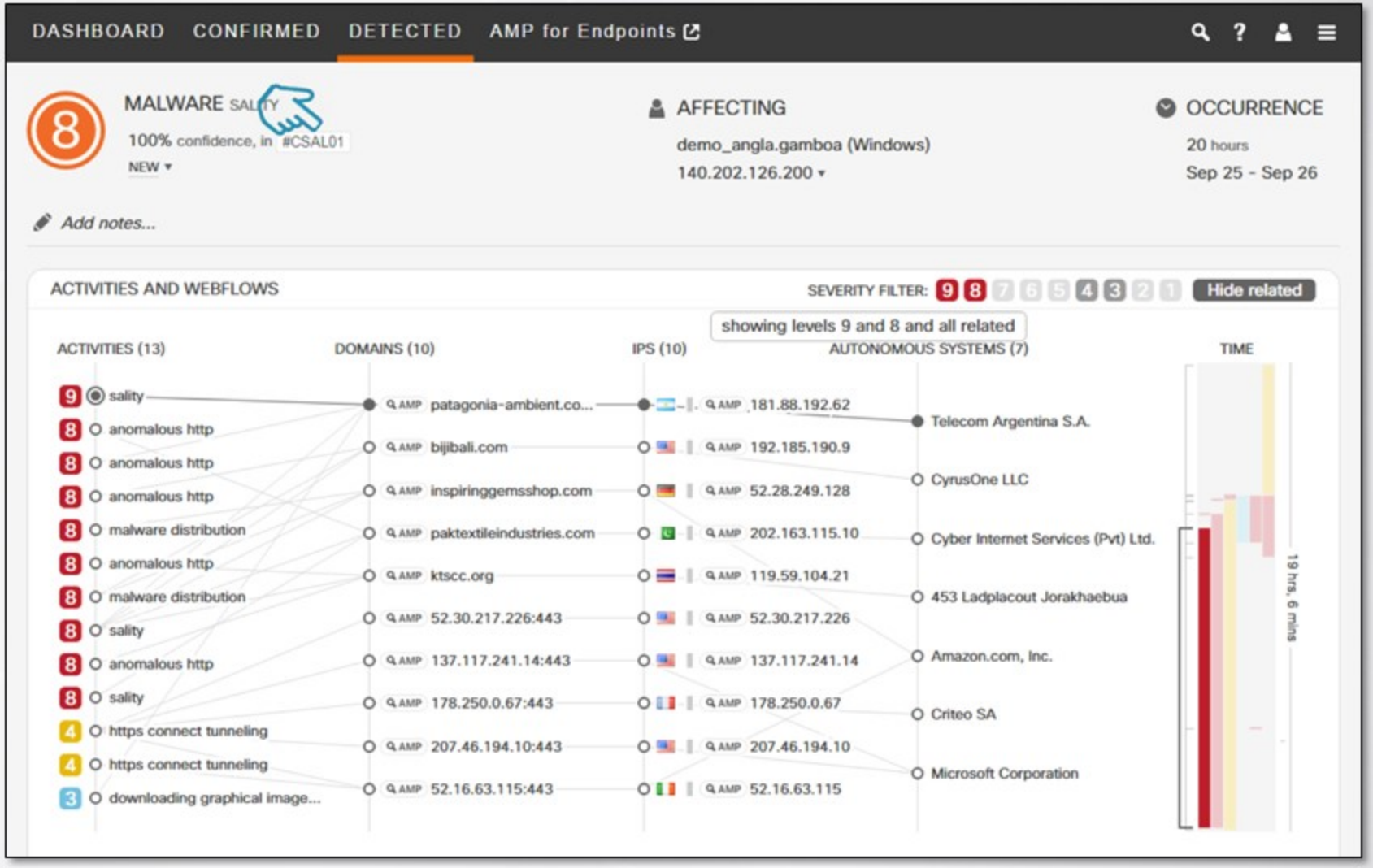
- Reputácia
- Sandboxing
- Anti-Exploit
- Retrospektíva

lancope: netflow based anomaly detection



Behaviorálna analýza

- Reputácia
- Sandboxing
- Anti-Exploit
- Retrospektíva



http://cognitive.cisco.com

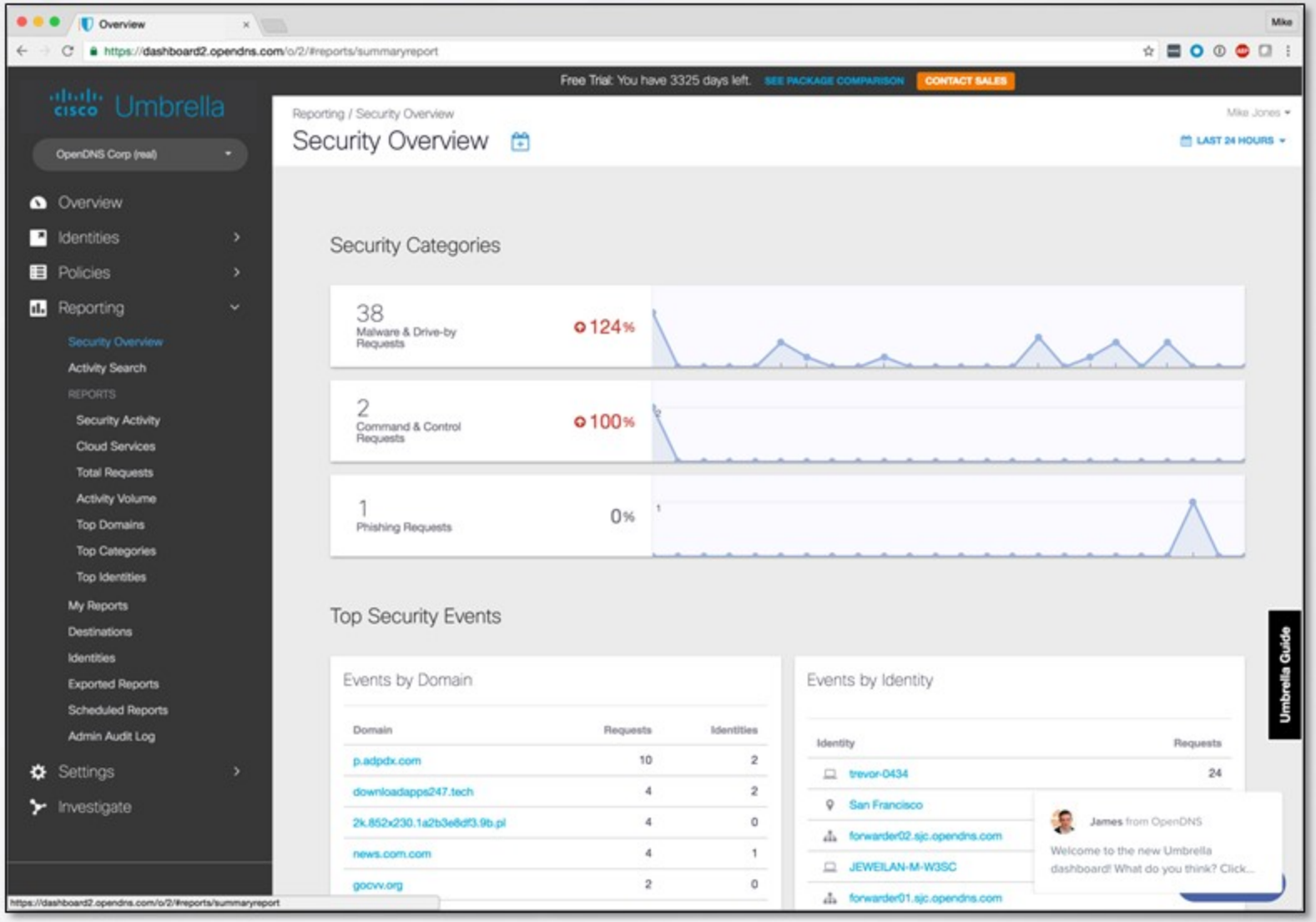
Behaviorálna analýza

Reputácia

Sandboxing

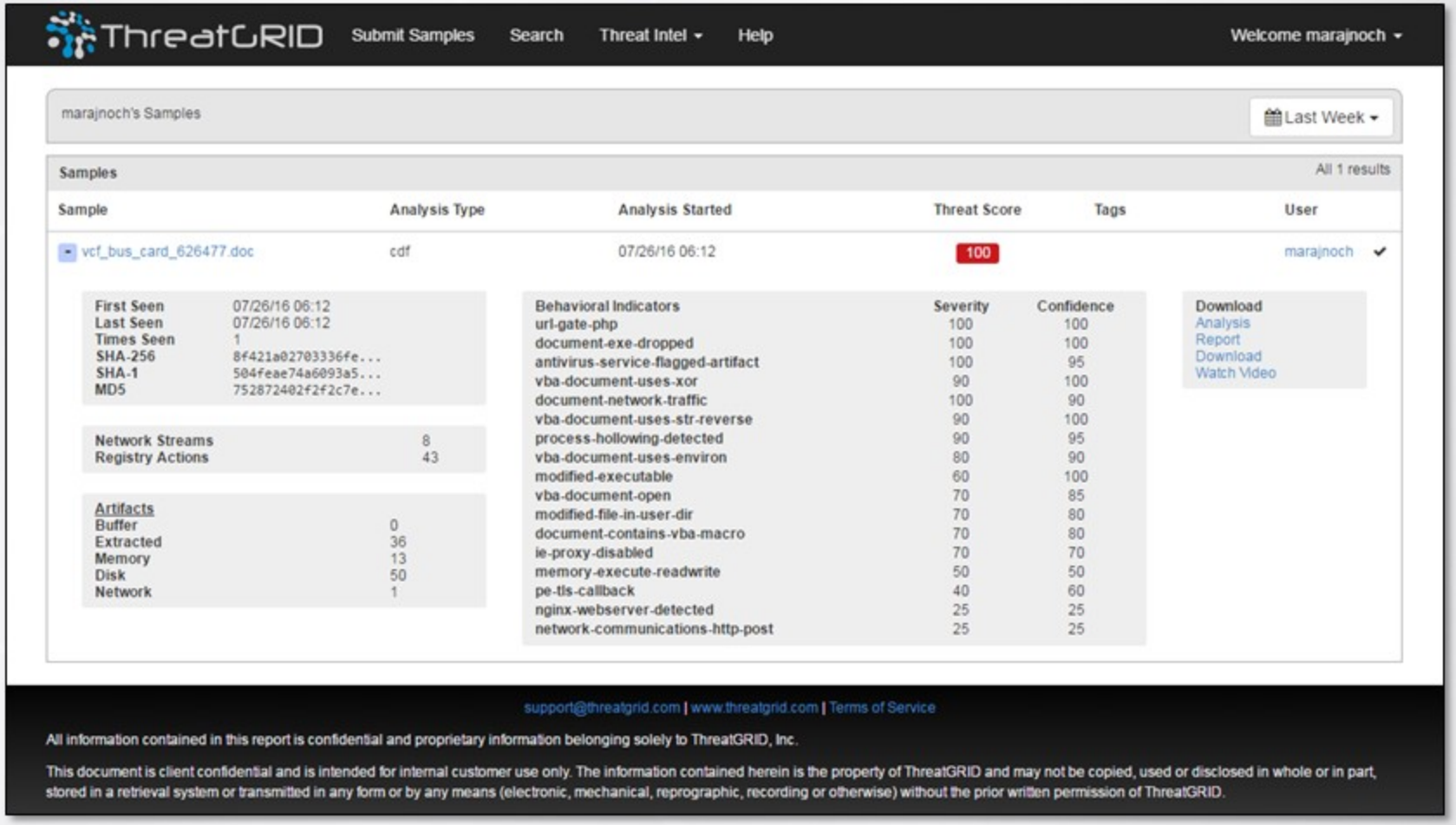
Anti-Exploit

Retrospektíva



Behaviorálna analýza

- Reputácia
- Sandboxing
- Anti-Exploit
- Retrospektíva



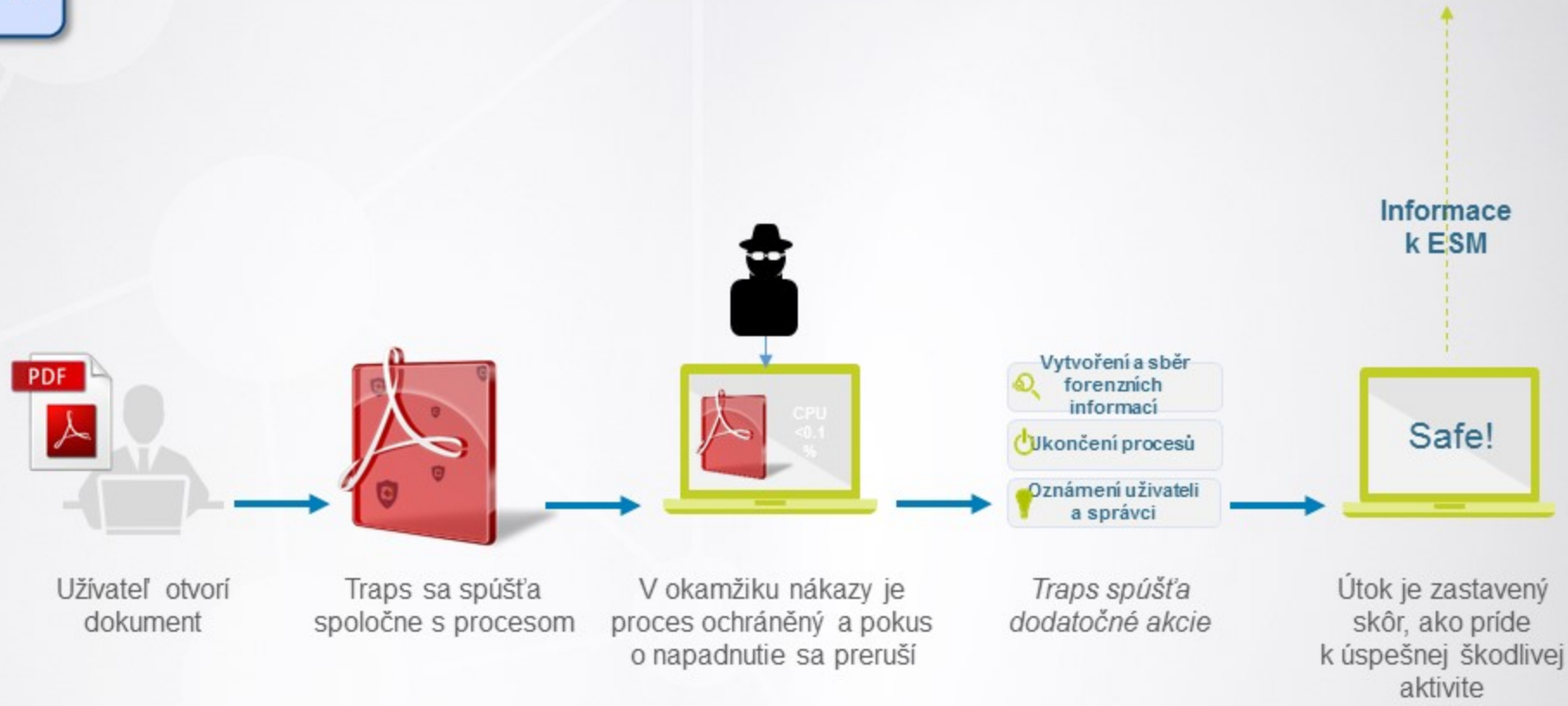
Behaviorálna analýza

Reputácia

Sandboxing

Anti-Exploit

Retrospektíva



Pri pokusu o zneužitie zraniteľnosti narazí útočný kód na pascu (trap) a skončí skôr ako stihne vykonať čokolvek škodlivého.

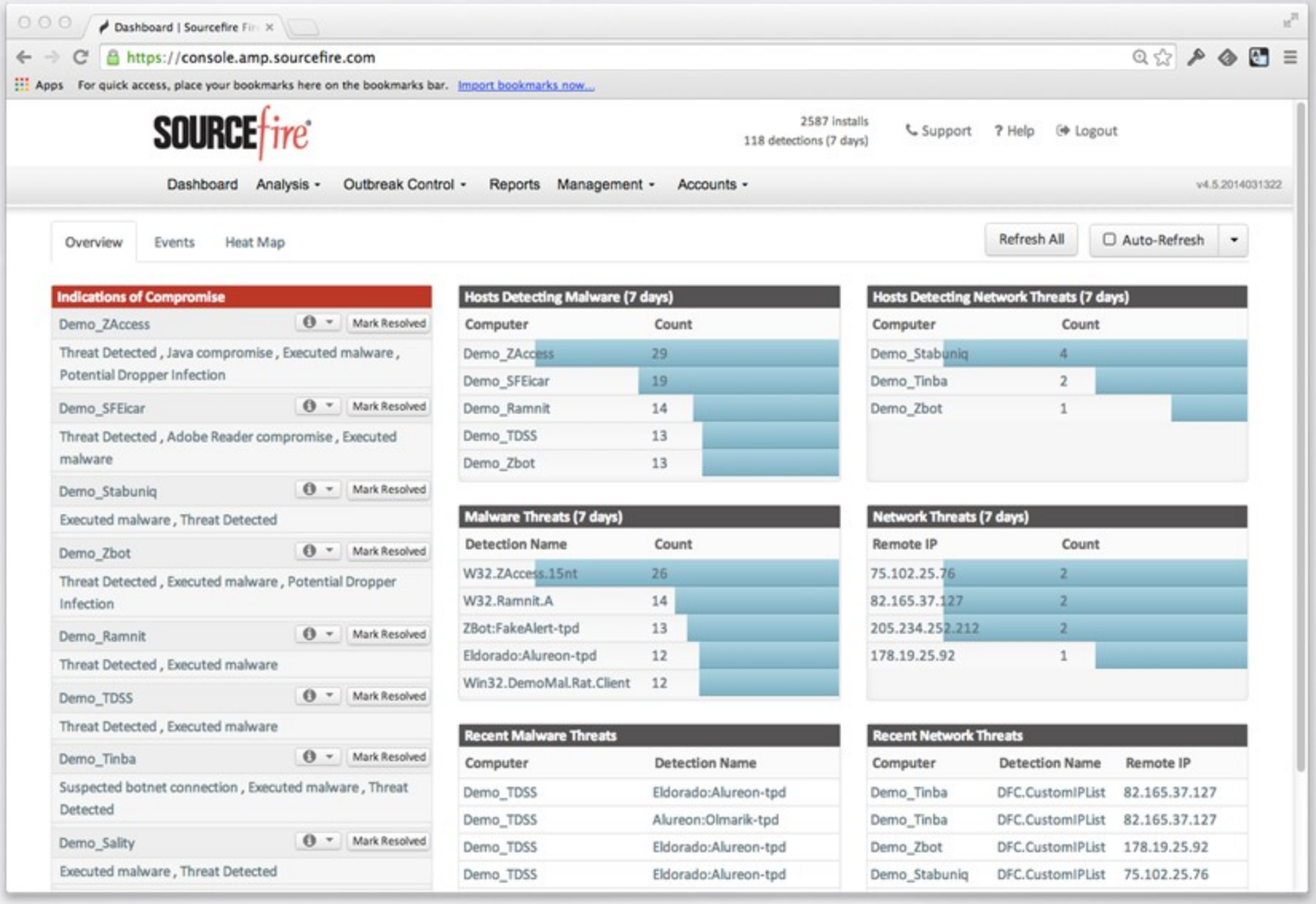
Behaviorálna analýza

Reputácia

Sandboxing

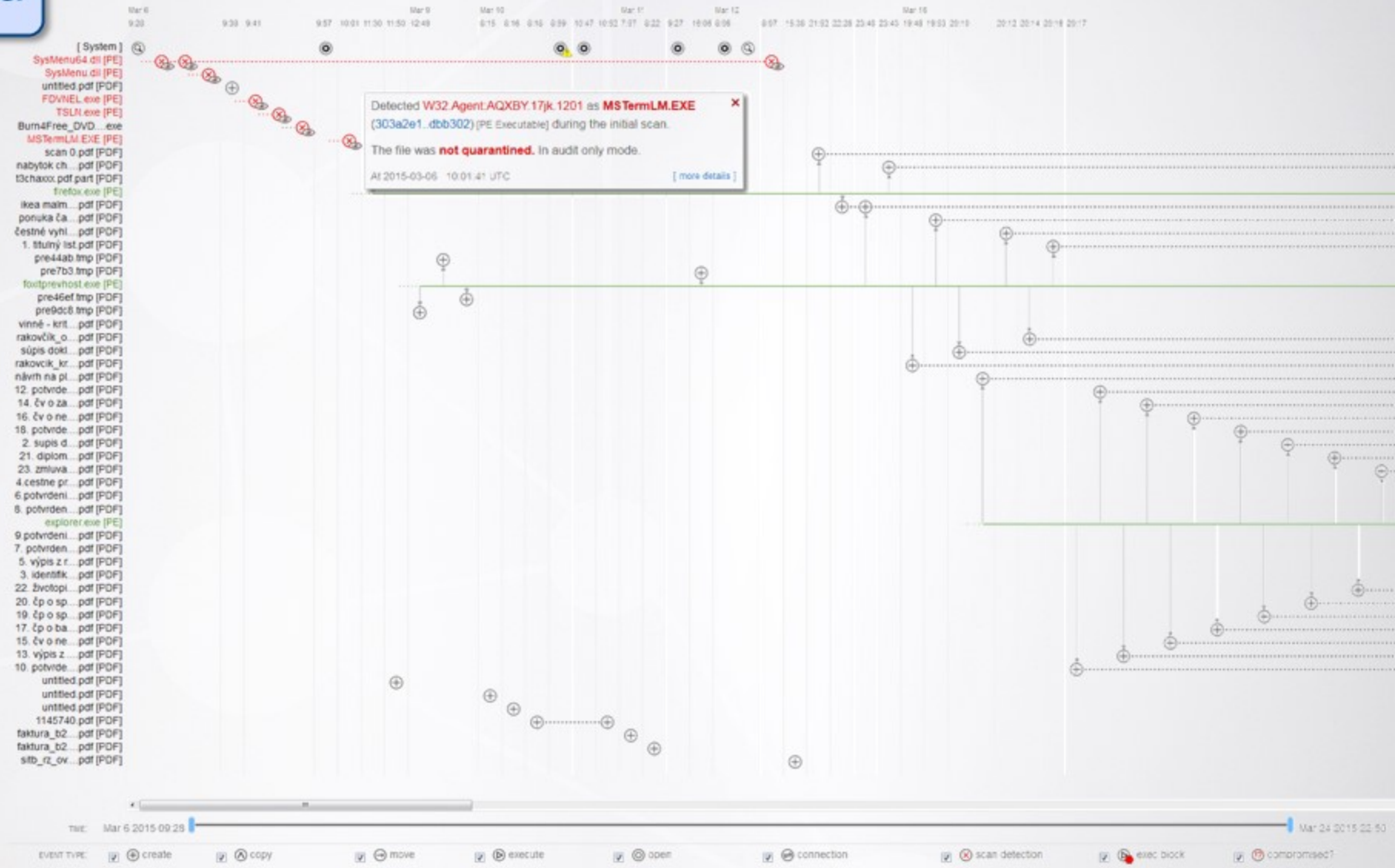
Anti-Exploit

Retrospektíva



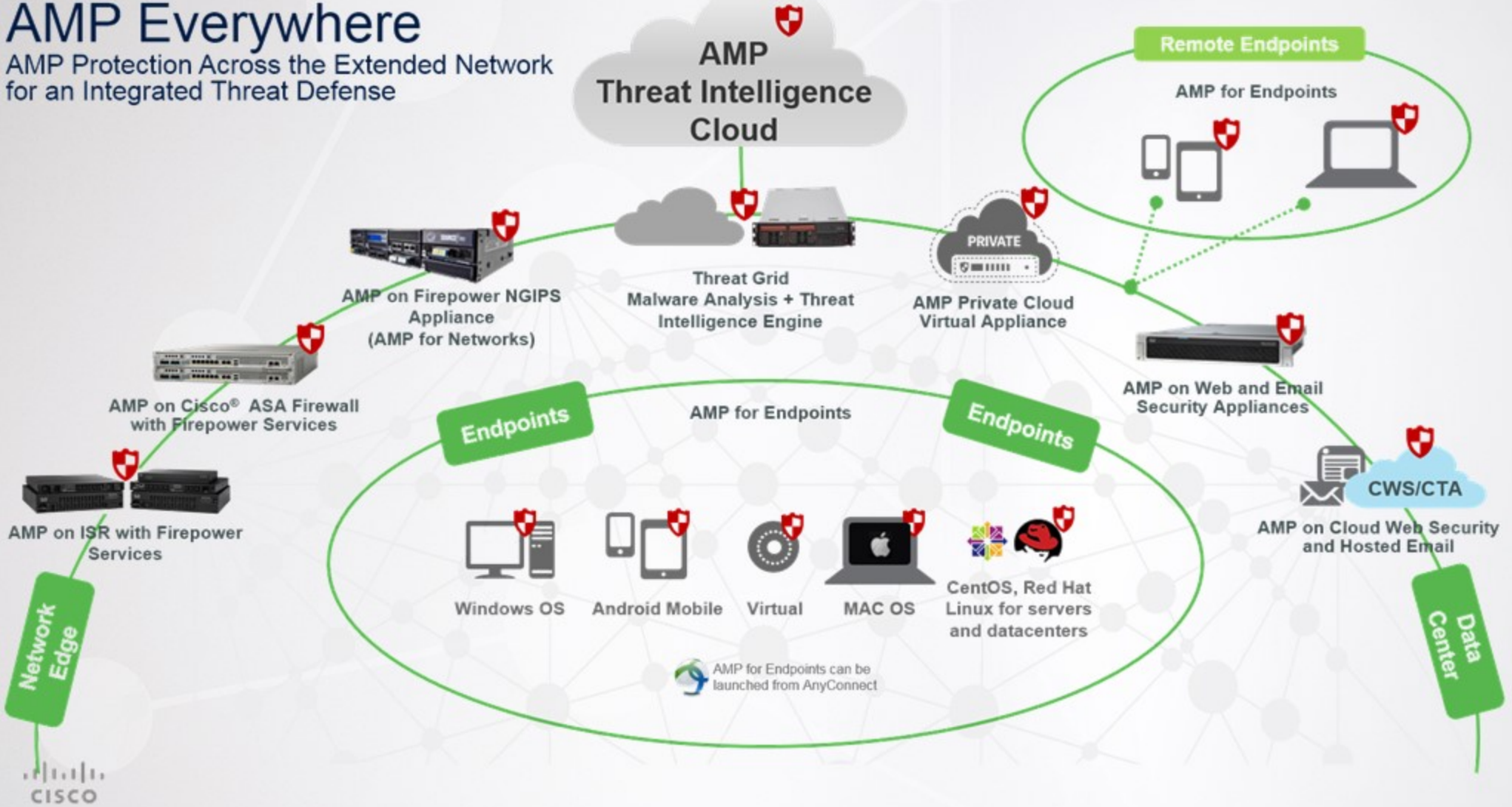
Behaviorálna analýza

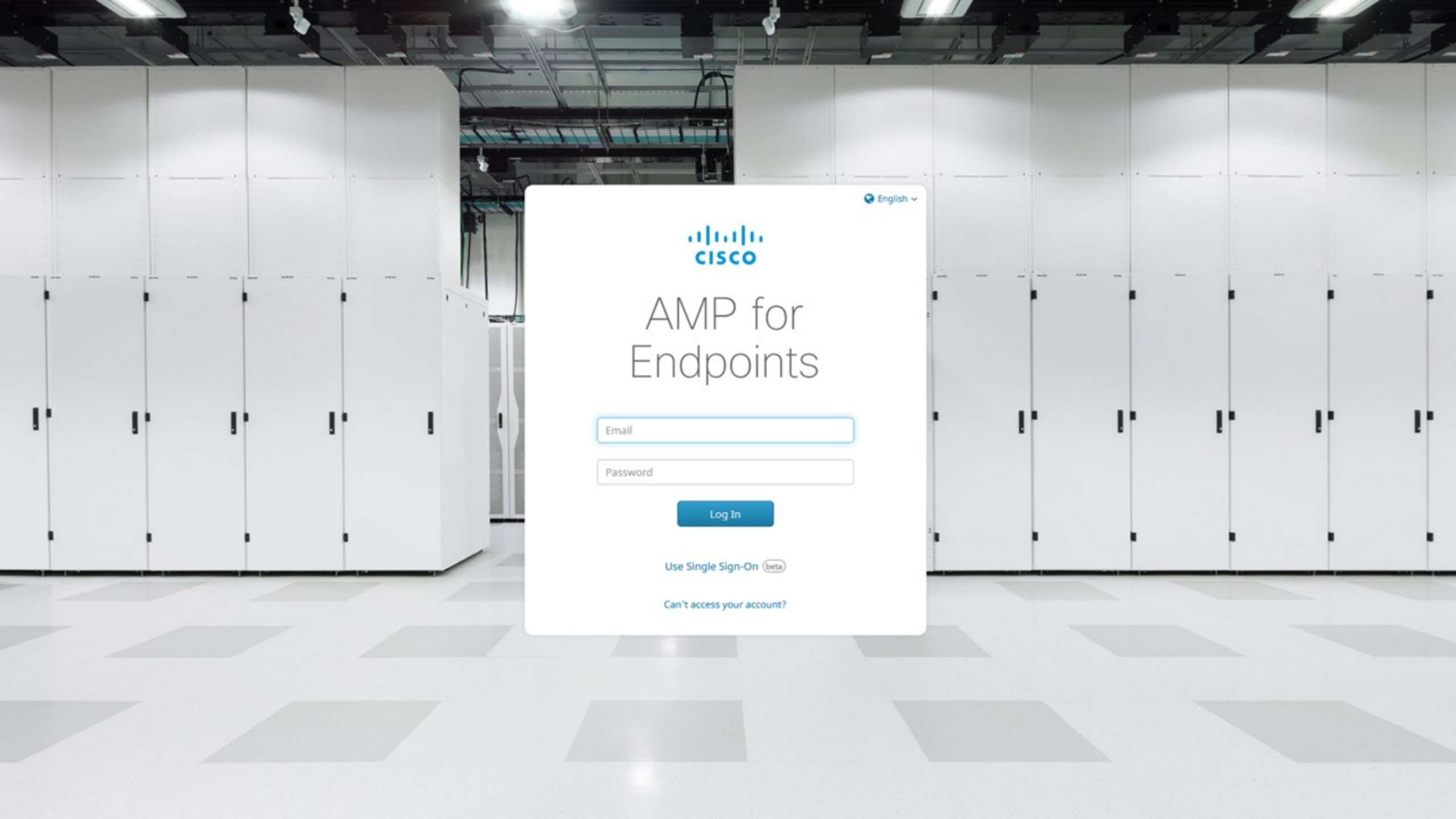
- Reputácia
- Sandboxing
- Anti-Exploit
- Retrospektíva



AMP Everywhere

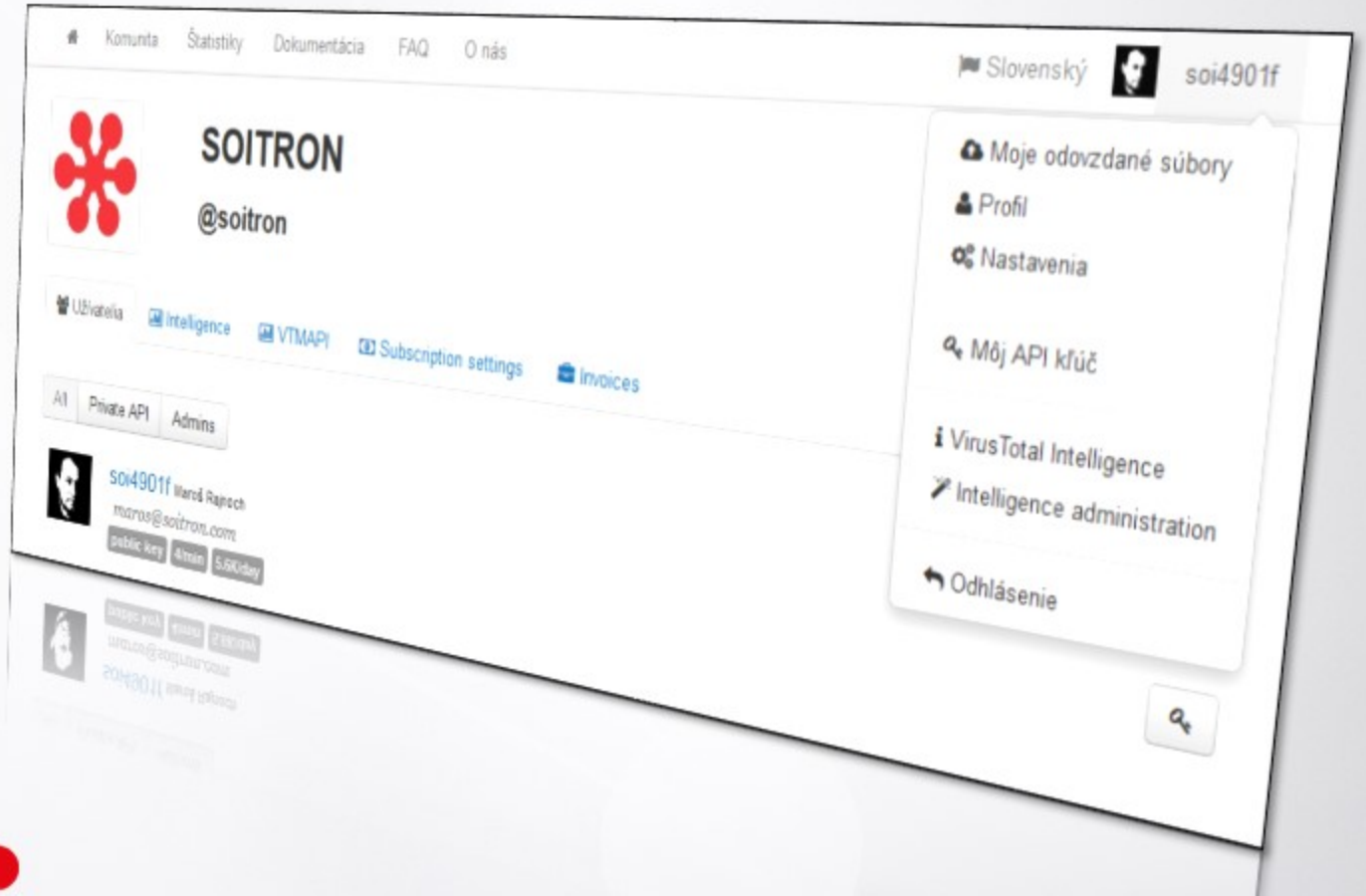
AMP Protection Across the Extended Network for an Integrated Threat Defense



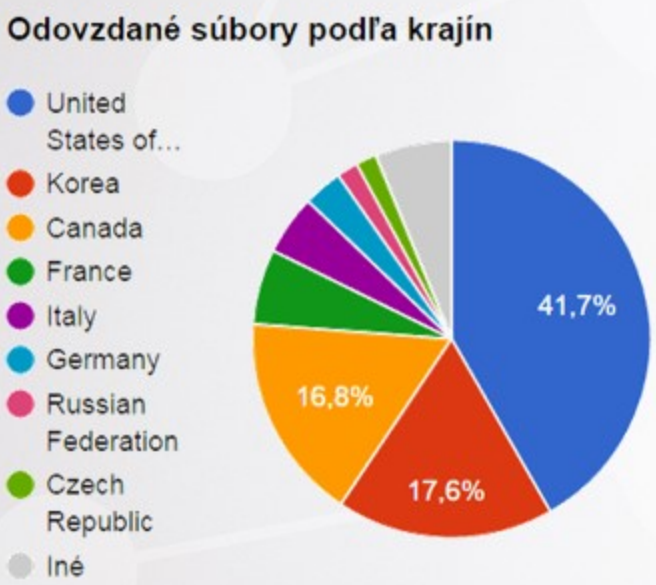

English
cisco
AMP for Endpoints
Email
Password
Log In
Use Single Sign-On beta
Can't access your account?

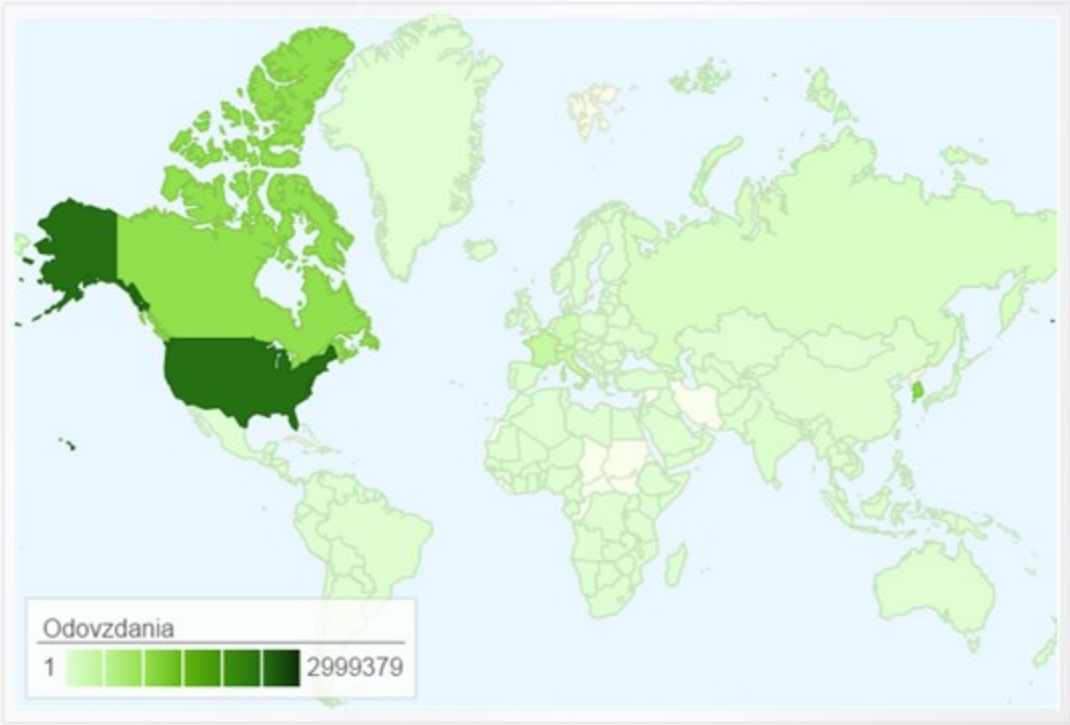
http://malwaredb.malekal.com/

https://github.com/krmaxwell/maltrieve

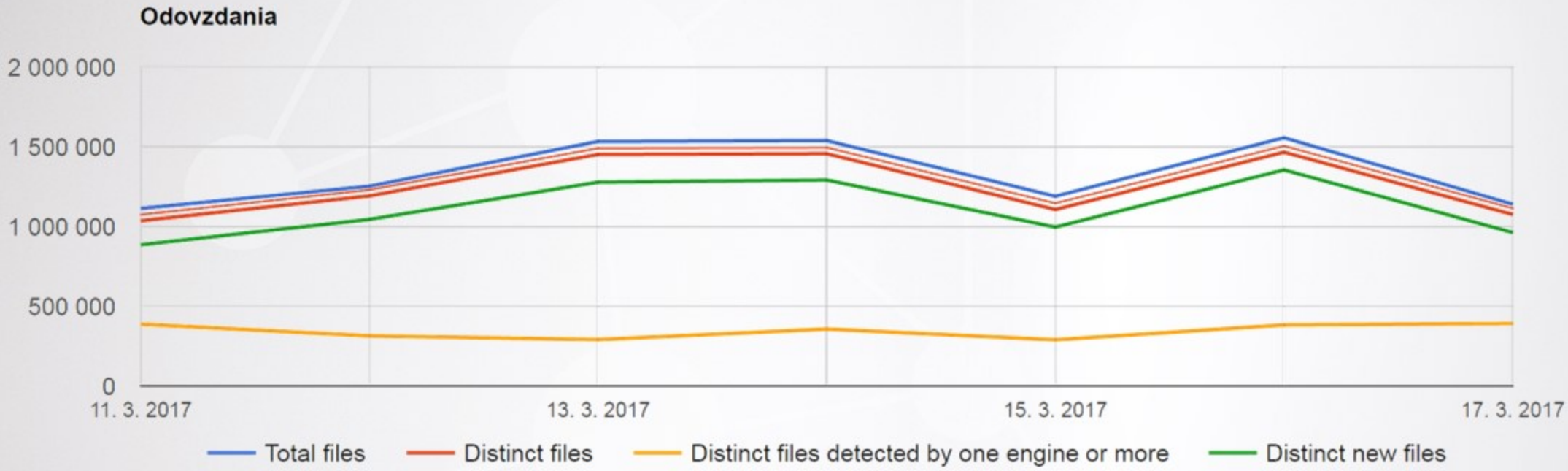


Štatistiky súboru počas posledných 7 dní

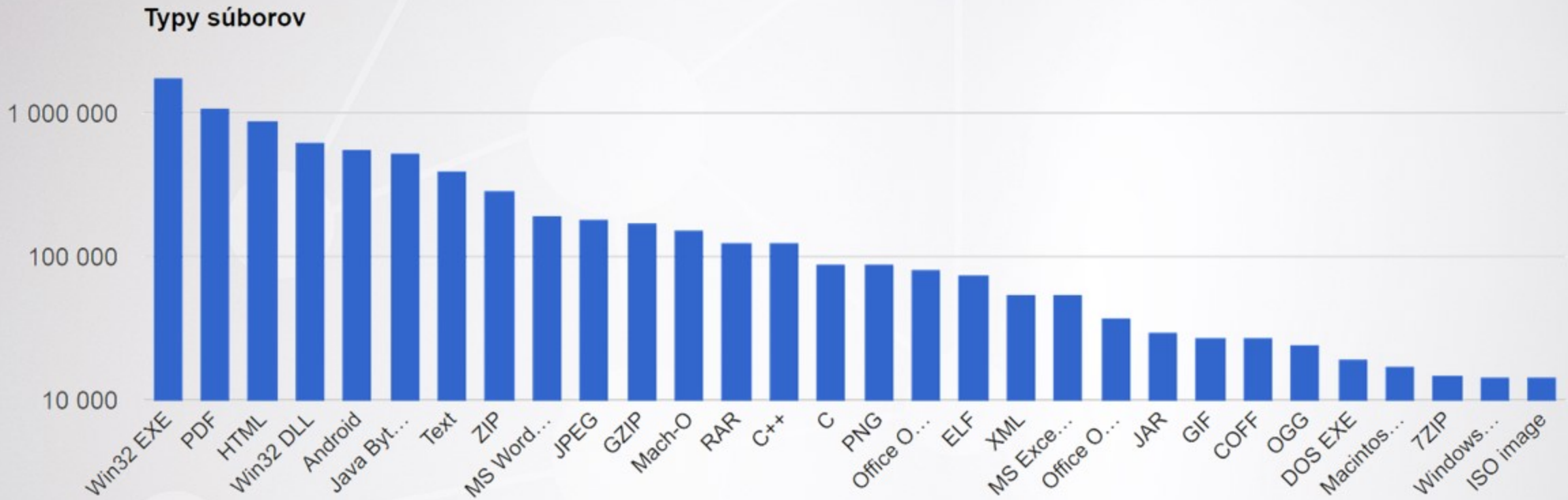




zdroj: https://www.virustotal.com/

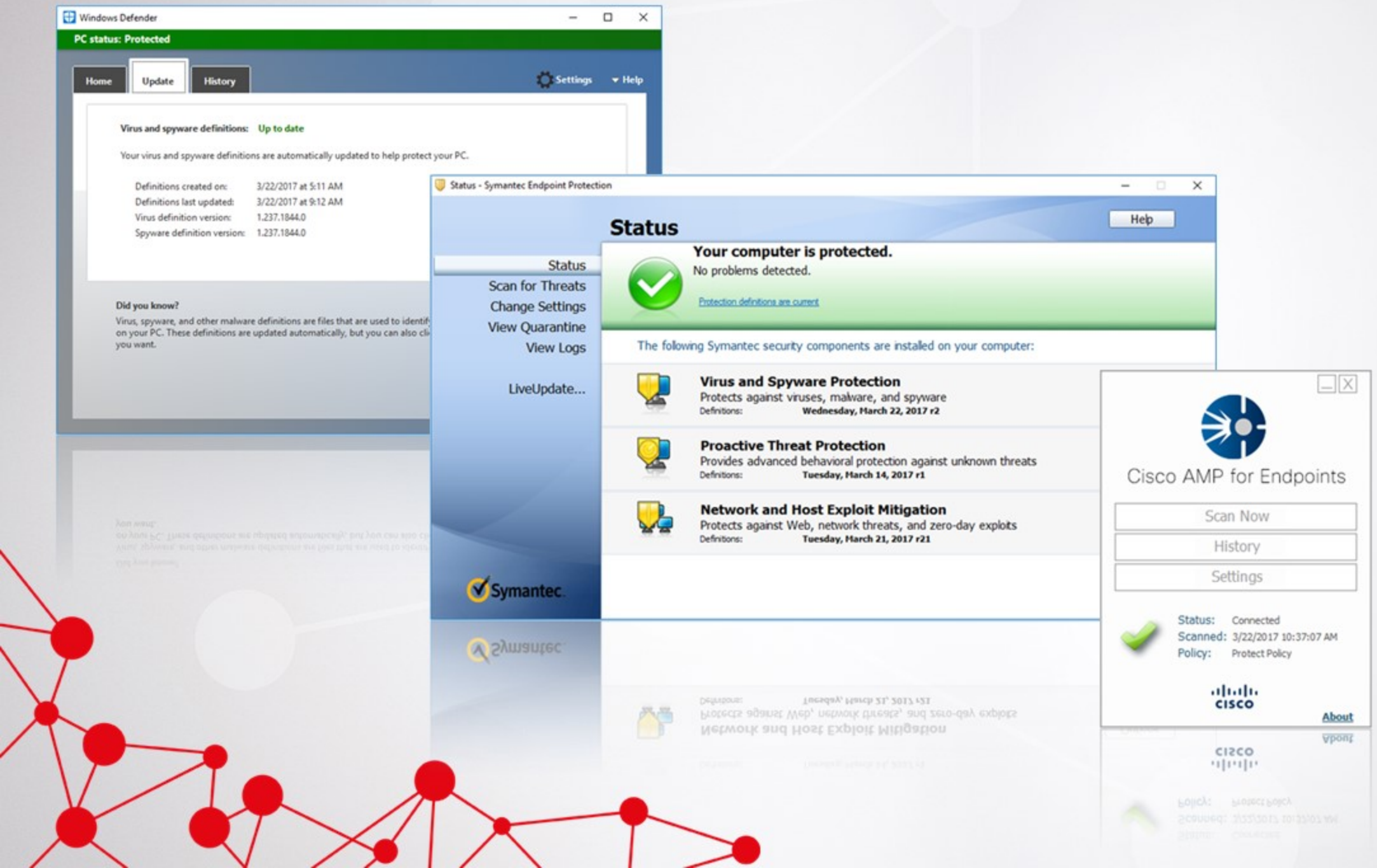


zdroj: https://www.virustotal.com/

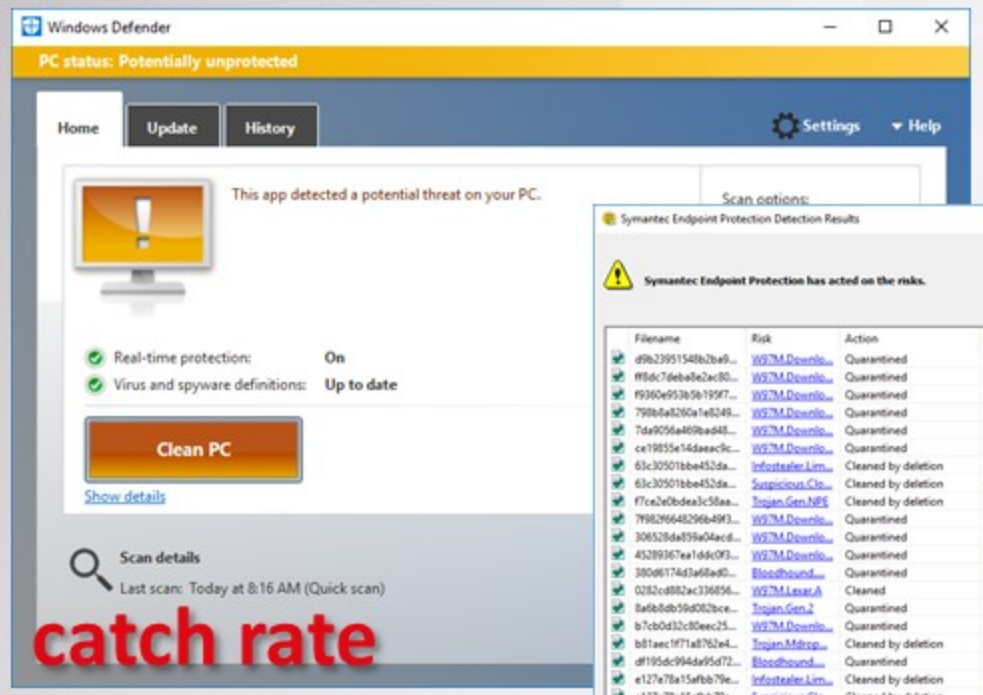


zdroj: https://www.virustotal.com/


250 vzoriek

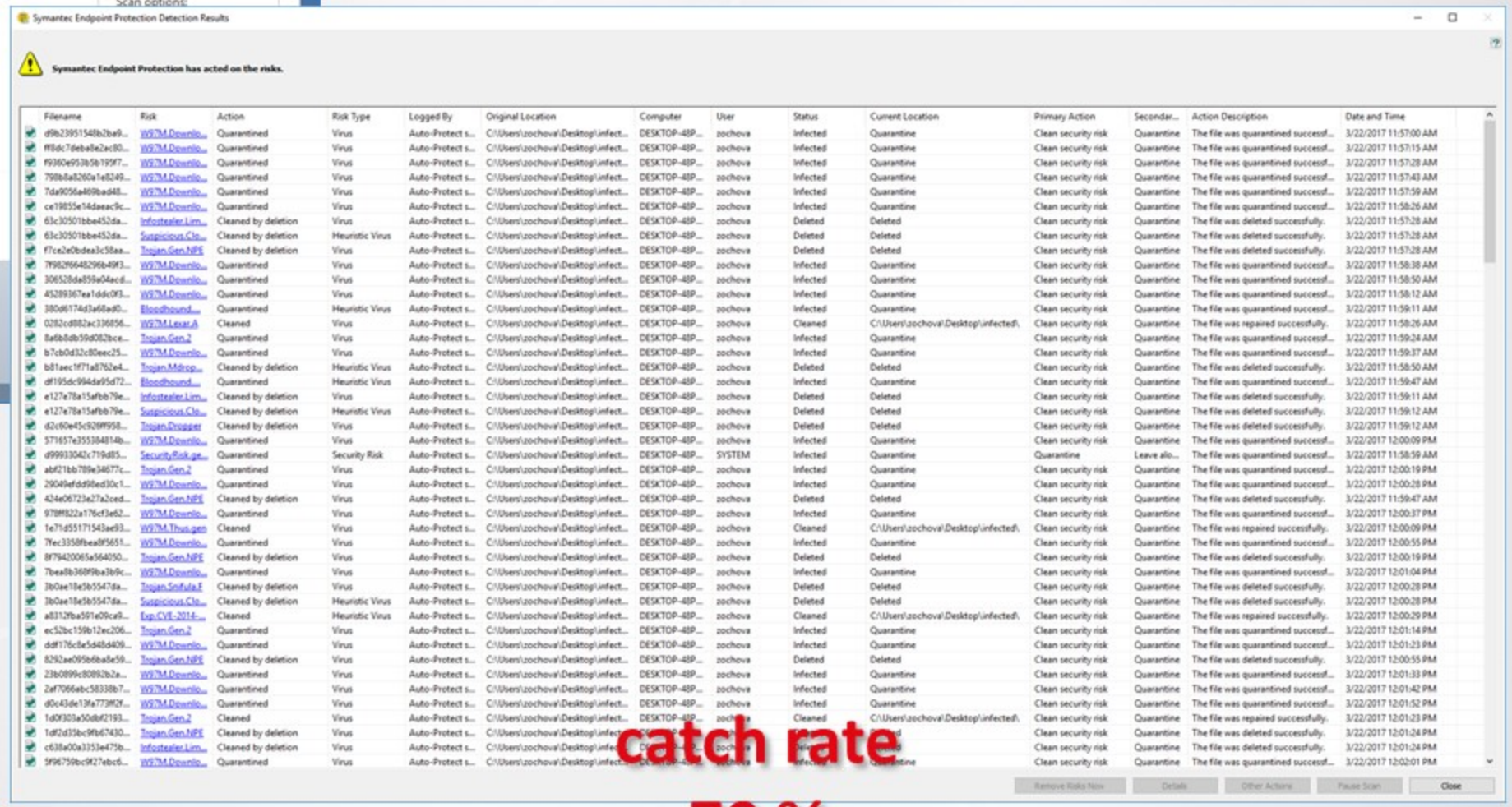

Windows Defender
PC status: Protected
Home
Update
History
Settings
Help
Virus and spyware definitions: Up to date
Your virus and spyware definitions are automatically updated to help protect your PC.
Definitions created on: 3/22/2017 at 5:11 AM
Definitions last updated: 3/22/2017 at 9:12 AM
Virus definition version: 1.237.1844.0
Spyware definition version: 1.237.1844.0
Did you know?
Virus, spyware, and other malware definitions are files that are used to identif
on your PC. These definitions are updated automatically, but you can also cl
you want.
Status - Symantec Endpoint Protection
Status
Help
Status
Scan for Threats
Change Settings
View Quarantine
View Logs
LiveUpdate...
Your computer is protected.
No problems detected.
Protection definitions are current
The following Symantec security components are installed on your computer:
Virus and Spyware Protection
Protects against viruses, malware, and spyware
Definitions: Wednesday, March 22, 2017 r2
Proactive Threat Protection
Provides advanced behavioral protection against unknown threats
Definitions: Tuesday, March 14, 2017 r1
Network and Host Exploit Mitigation
Protects against Web, network threats, and zero-day exploits
Definitions: Tuesday, March 21, 2017 r21
Symantec
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Connected
Scanned: 3/22/2017 10:37:07 AM
Policy: Protect Policy
cisco
About


And the winner
is...



catch rate

57 %



catch rate

70 %

SHA256: d0c43de13fa773ff2f383777f5e4e76588fc5f7042222f884e93915e56bacf8a

File name: Scan1.doc

Detection ratio: 19 / 57

Analysis date: 2017-02-27 12:42:20 UTC (3 weeks, 2 days ago)

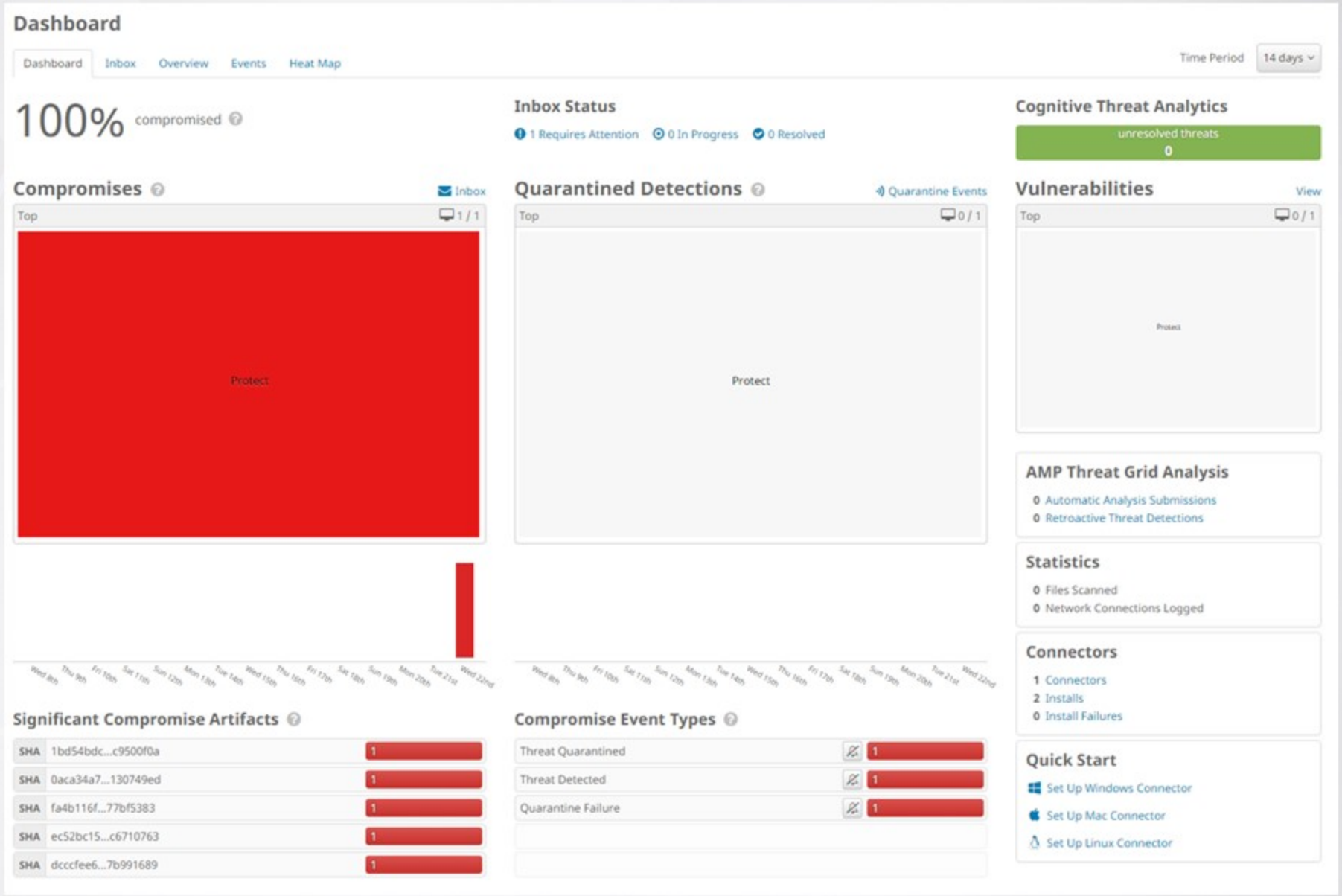
Analysis | File detail | Additional information | Comments 0 | Votes

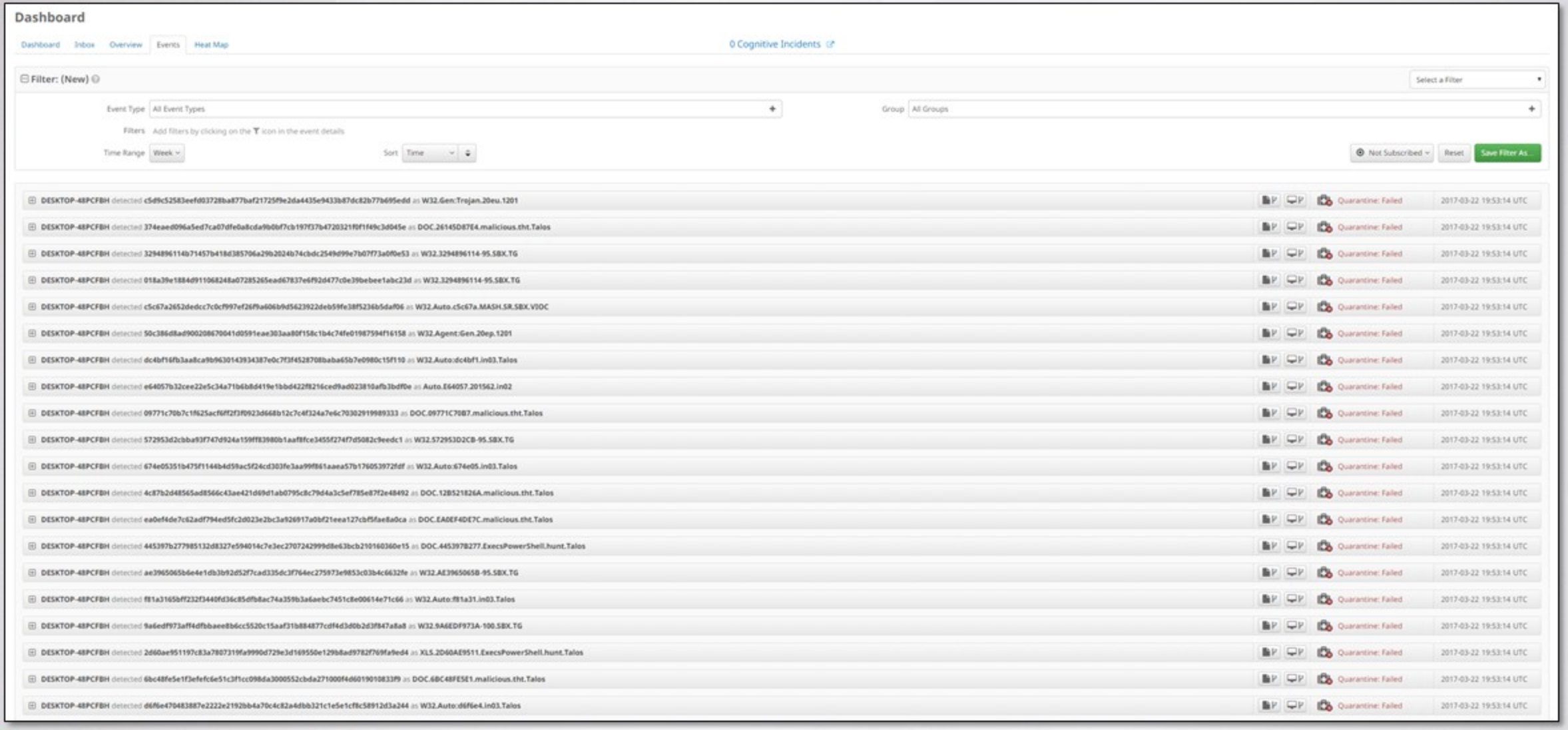
Antivirus	Result	Update
Ad-Aware	Exploit.OLE-JS.Gen	20170227
AhnLab-V3	DOC/Dropper	20170227
ALYac	Exploit.OLE-JS.Gen	20170227
Arcabit	Exploit.OLE-JS.Gen	20170227
Avast	VBS:Obfuscated-gen [Trj]	20170227
Baidu	JS.Trojan-Downloader.Nemucod.tf	20170227
BitDefender	Exploit.OLE-JS.Gen	20170227
Emsisoft	Exploit.OLE-JS.Gen (B)	20170227
ESET-NOD32	JS/TrojanDownloader.Nemucod.CIU	20170227
F-Secure	Exploit.OLE-JS.Gen	20170227
Fortinet	JS/Nemucod.CIU!tr.dldr	20170227
GData	Exploit.OLE-JS.Gen	20170227
Ikarus	Trojan-Downloader.JS.Nemucod	20170227
Kaspersky	HEUR:Trojan-Downloader.Script.Generic	20170227
eScan	Exploit.OLE-JS.Gen	20170227
Qihoo-360	virus.js.qexvmc.1	20170227
Rising	Downloader.Nemucod!8.34 (cloud:1FYxMS7UG1F)	20170227
Symantec	W97M.Downloader	20170226
Tencent	Js.Trojan-downloader.Nemucod.Hqbs	20170227

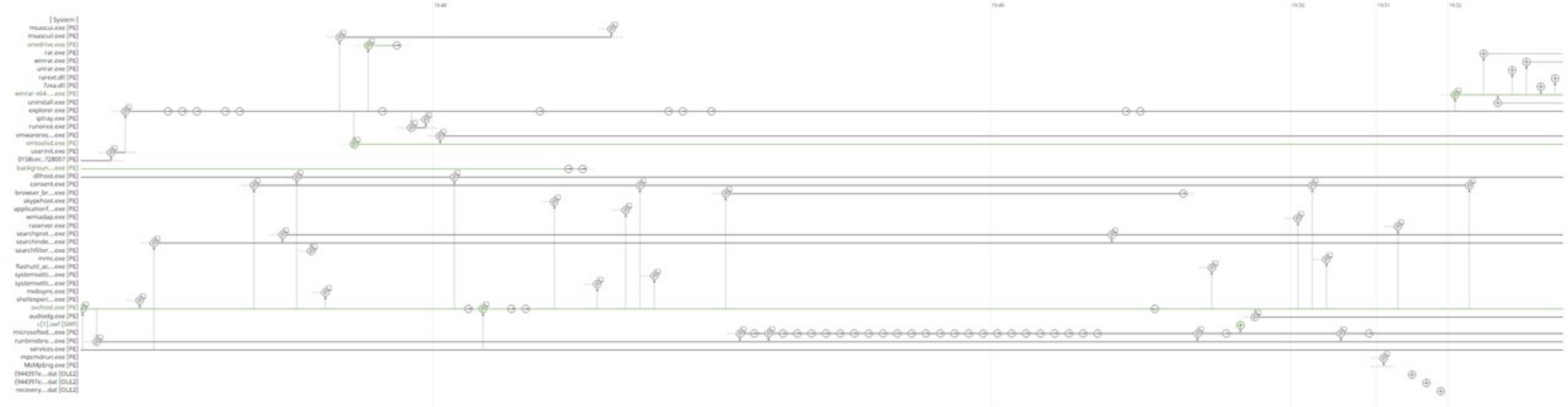
AegisLab	✓	20170227
Alibaba	✓	20170227
Antiy-AVL	✓	20170227
AVG	✓	20170227
Avira (no cloud)	✓	20170227
AVware	✓	20170227
CAT-QuickHeal	✓	20170227
ClamAV	✓	20170227
CMC	✓	20170227
Comodo	✓	20170227
CrowdStrike Falcon (ML)	✗	20170130
Cyren	✓	20170227
DrWeb	✓	20170227
Endgame	✗	20170222
F-Prot	✓	20170227
Invincea	✗	20170203
Jiangmin	✓	20170227
K7AntiVirus	✓	20170227
K7GW	✓	
Kingsoft	✓	
Malwarebytes	✓	
McAfee	✓	
McAfee-GW-Edition	✓	
Microsoft	✓	
NANO-Antivirus	✓	
nProtect	✓	
Panda	✓	
Sophos	✓	
SUPERAntiSpyware	✓	
TheHacker	✓	
TotalDefense	✓	

Sophos	✓
SUPERAntiSpyware	✓
TheHacker	✓
TotalDefense	✓
TrendMicro	✓
TrendMicro-HouseCall	✓
Trustlook	✗
VBA32	✓
VIPRE	✓
ViRobot	✓
Webroot	✓
WhiteArmor	✓
Yandex	✓
Zillya	✓
Zoner	✓

catch rate
96 %




Dashboard
Dashboard
Inbox
Overview
Events
Heat Map
0 Cognitive Incidents
Filter: (New)
Select a Filter
Event Type
All Event Types
Group
All Groups
Filters
Add filters by clicking on the icon in the event details
Time Range
Week
Sort
Time
Not Subscribed
Reset
Save Filter As...
DESKTOP-48PCFBH detected c5d9c52583eefd03728ba877baf21725f9e2da4435e9433b87dc82b77b695edd as W32.Gen:Trojan.20eu.1201
DESKTOP-48PCFBH detected 374eaed096a5ed7ca07dfe0a8cda9b0bf7cb197f37b4720321f0f1f49c3d045e as DOC.26145D87E4.malicious.tht.Talos
DESKTOP-48PCFBH detected 32948961l4b71457b418d385706a29b2024b74cbdc2549d99e7b07f73a0f0e53 as W32.3294896114-95.SBX.TG
DESKTOP-48PCFBH detected 018a39e1884d911068248a07285265ead67837e6f92d477c0e39bebee1abc23d as W32.3294896114-95.SBX.TG
DESKTOP-48PCFBH detected c5c67a2652dedcc7c0cf997ef26f9a606b9d5623922deb59fe38f5236b5daf06 as W32.Auto.c5c67a.MASH.SR.SBX.V3OC
DESKTOP-48PCFBH detected 50c386d8ad900208670041d0591eae303aa80f158c1b4c74fe01987594f16158 as W32.Agent:Gen.20ep.1201
DESKTOP-48PCFBH detected dc4bf16fb3aa8ca9b9630143934387e0c7f3f4528708baba65b7e0980c15f110 as W32.Auto:dc4bf1.in03.Talos
DESKTOP-48PCFBH detected e64057b32cee22e5c34a71b6b8d419e1bbd422f8216ced9ad023810afb3bdf0e as Auto.E64057.201562.in02
DESKTOP-48PCFBH detected 09771c70b7c1f625acf6ff2f3f0923d668b12c7c4f324a7e6c70302919989333 as DOC.09771C70B7.malicious.tht.Talos
DESKTOP-48PCFBH detected 572953d2cbba93f747d924a159ff83980b1aaf8fce3455f274f7d5082c9eedc1 as W32.572953D2CB-95.SBX.TG
DESKTOP-48PCFBH detected 674e05351b475f1144b4d59ac5f24cd303fe3aa99f861aaea57b176053972fdf as W32.Auto:674e05.in03.Talos
DESKTOP-48PCFBH detected 4c87b2d48565ad8566c43ae421d69d1ab0795c8c79d4a3c5ef785e87f2e48492 as DOC.12B521826A.malicious.tht.Talos
DESKTOP-48PCFBH detected ea0ef4de7c62adf794ed5fc2d023e2bc3a926917a0bf21eea127cbf5fae8a0ca as DOC.EA0EF4DE7C.malicious.tht.Talos
DESKTOP-48PCFBH detected 445397b277985132d8327e5940l4c7e3ec2707242999d8e63bcb2101603 60e15 as DOC.4453978277.ExecsPowerShell.hunt.Talos
DESKTOP-48PCFBH detected ae3965065b6e4e1db3b92d52f7cad335dc3f764ec275973e9853c03b4c6632fe as W32.AE3965065B-95.SBX.TG
DESKTOP-48PCFBH detected f81a3165bff232f3440fd36c85dfb8ac74a359b3a6aebc7451c8e00614e71c66 as W32.Auto:f81a31.in03.Talos
DESKTOP-48PCFBH detected 9a6edf973aff4dfbbaee8b6cc5520c15aaf31b884877cdf4d3d0b2d3f847a8a8 as W32.9A6EDF973A-100.SBX.TG
DESKTOP-48PCFBH detected 2d60ae951197c83a7807319fa9990d729e3d169550e129b8ad9782f769fa9ed4 as XLS.2D60AE9511.ExecsPowerShell.hunt.Talos
DESKTOP-48PCFBH detected 6bc48fe5e1f3efefc6e51c3f1cc098da3000552cbda271000f4d601901 0833f9 as DOC.6BC48FE5E1.malicious.tht.Talos
DESKTOP-48PCFBH detected d6f6e470483887e2222e2192bb4a70c4c82a4dbb321c1e5e1cf8c58912d3a244 as W32.Auto:d6f6e4.in03.Talos
Quarantine: Failed
2017-03-22 19:53:14 UTC



TIME Mar 22, 2017, 20:45 — Mar 22, 2017, 21:46

EVENT TYPE: create, copy, move, execute, open, connection, scan detection, exec block, compromised?, restore, reboot, scan, defs update, policy update, connector update, scan schedule, uninstall

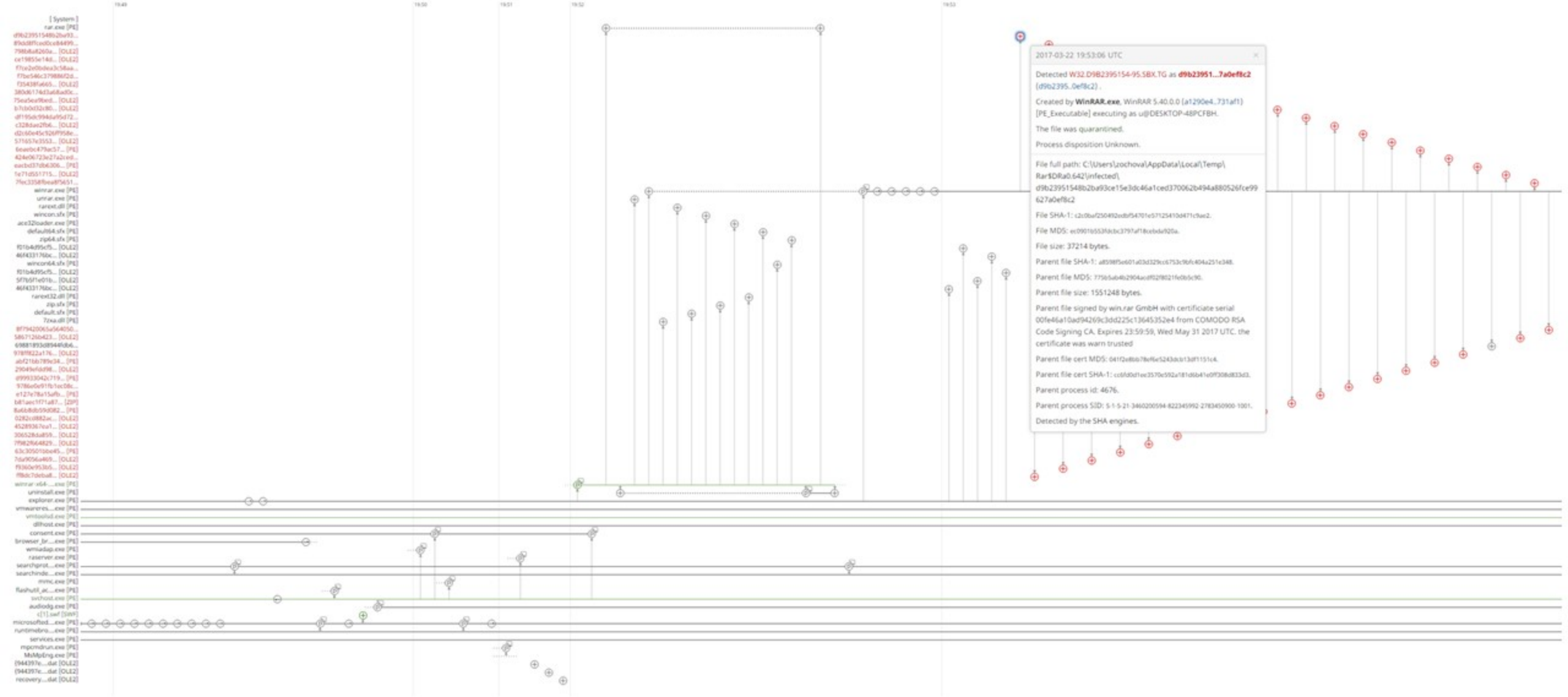
EVENT DISPOSITION: benign, malicious, unknown

EVENT FLAGS: none, warning, audit only, command-line

FILE TYPE: executable, ms office (ole2), pdf, ms cabinet, flash, zip archive, other, unknown

Search

Uncheck All | Check All



TIME Mar 22, 2017, 20:45 — Mar 22, 2017, 21:46

EVENT TYPE: create, copy, move, execute, open, connection, scan detection, exec block, compromised?, restore, reboot, scan, defs update, policy update, connector update, scan schedule, uninstall

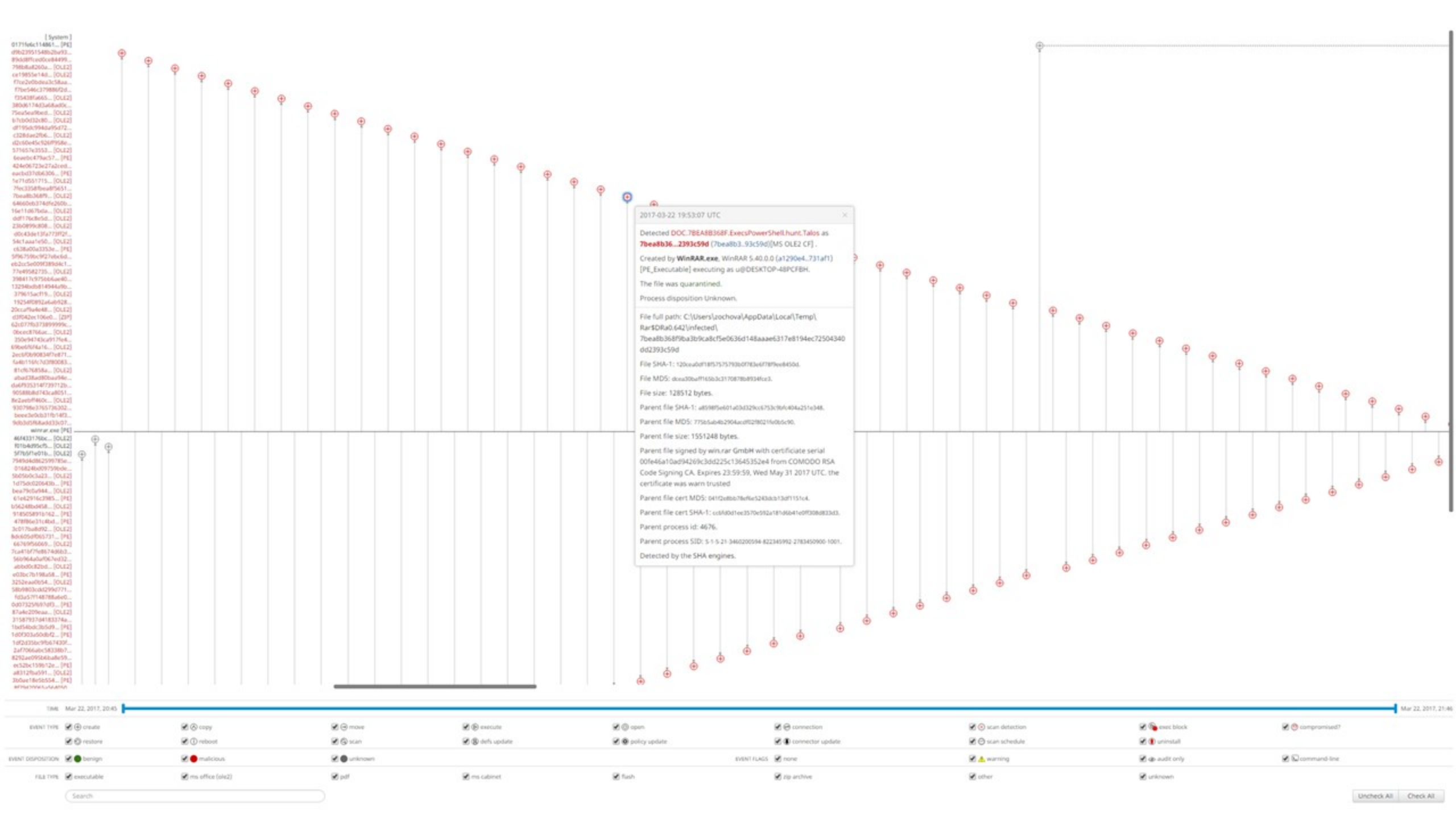
EVENT DISPOSITION: benign, malicious, unknown

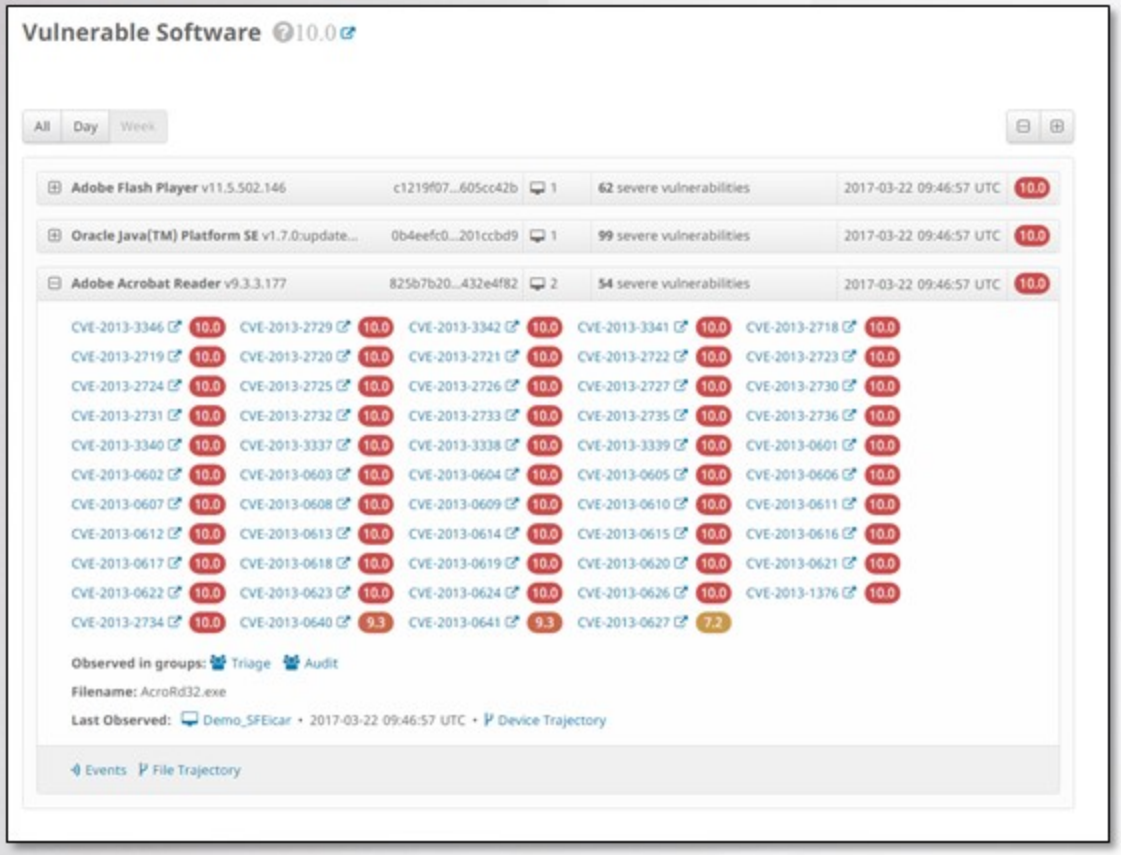
EVENT FLAGS: none, warning, audit only, command-line

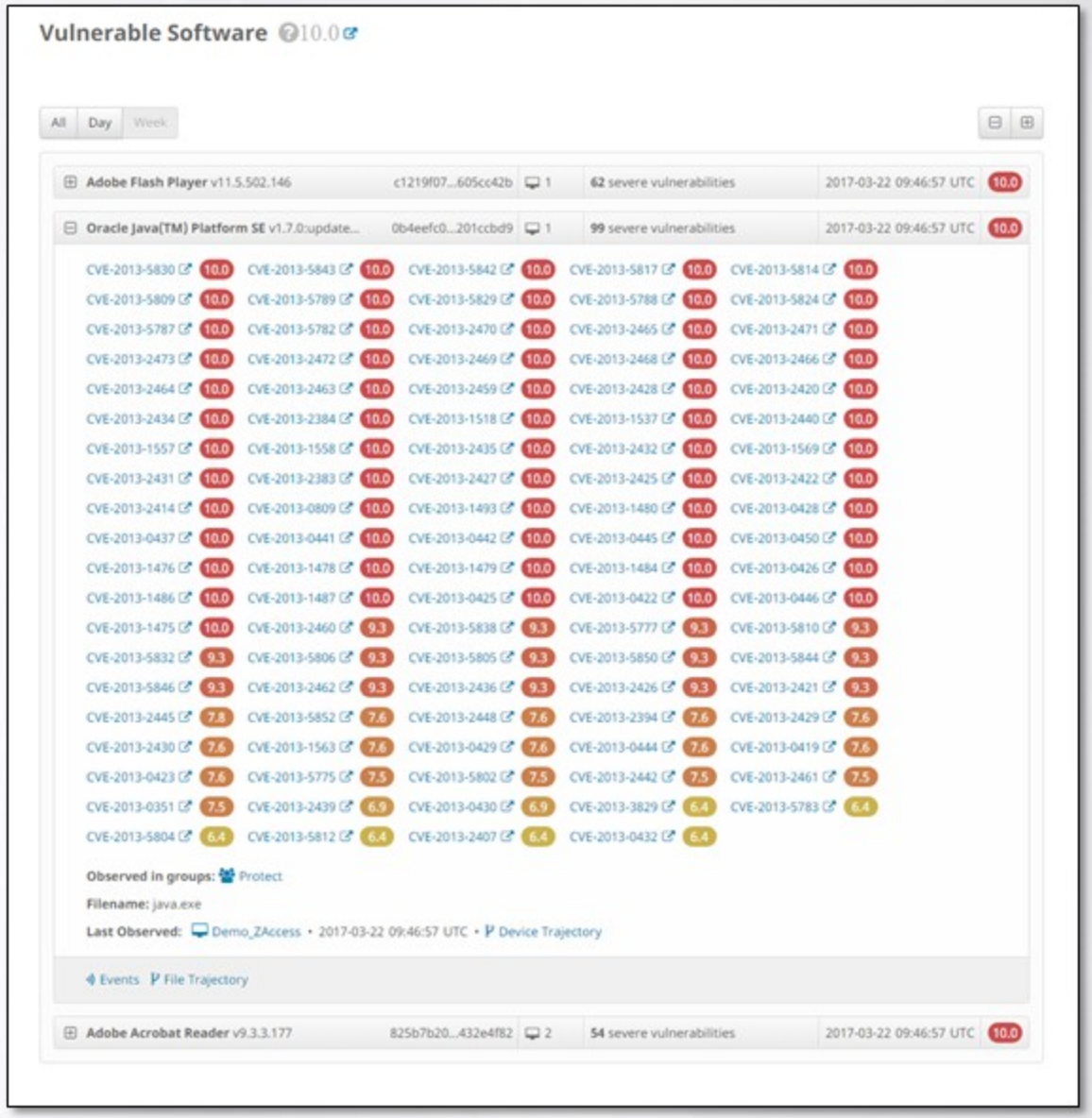
FILE TYPE: executable, ms office (ole2), pdf, ms cabinet, flash, zip archive, other, unknown

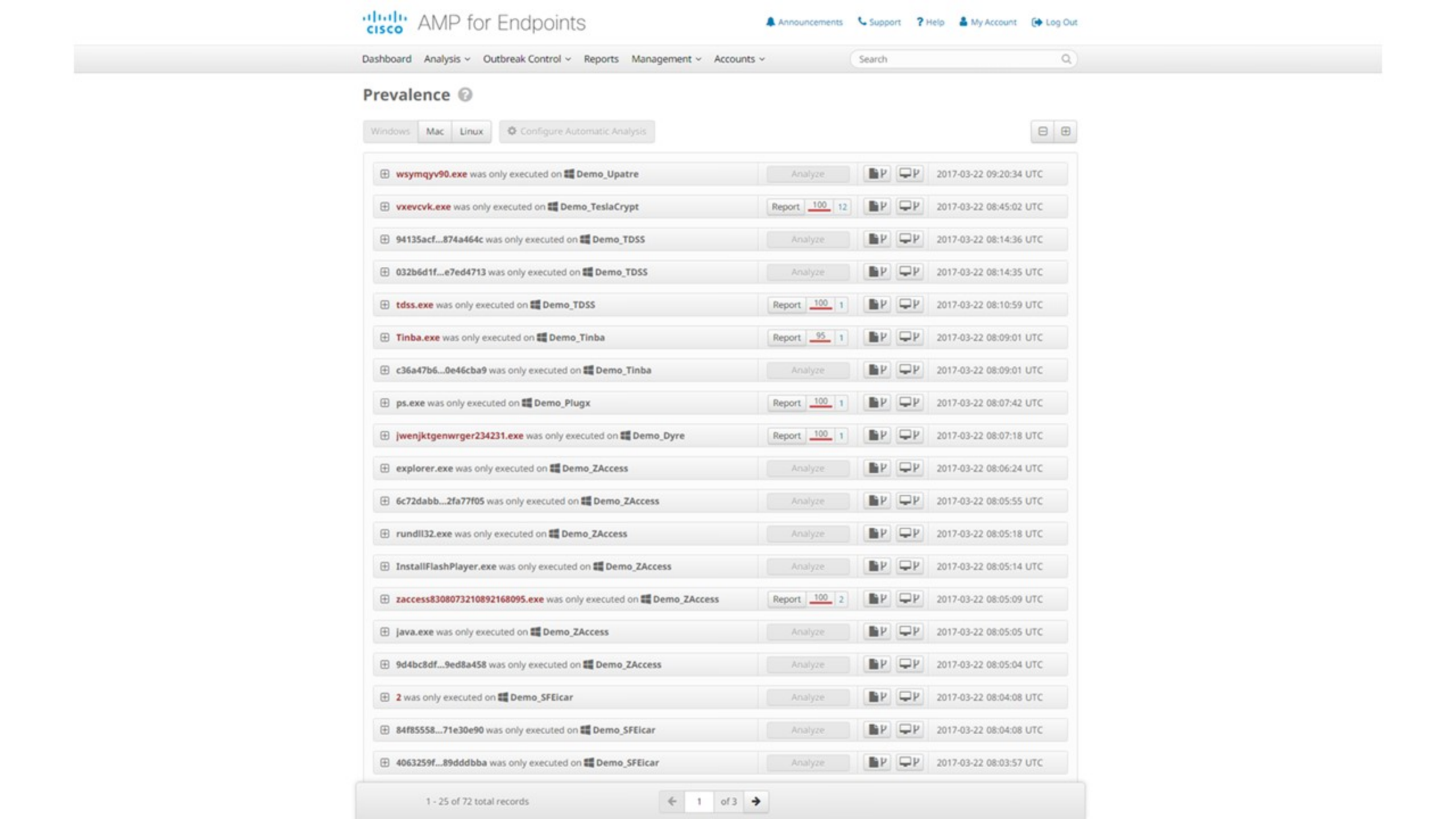
Search

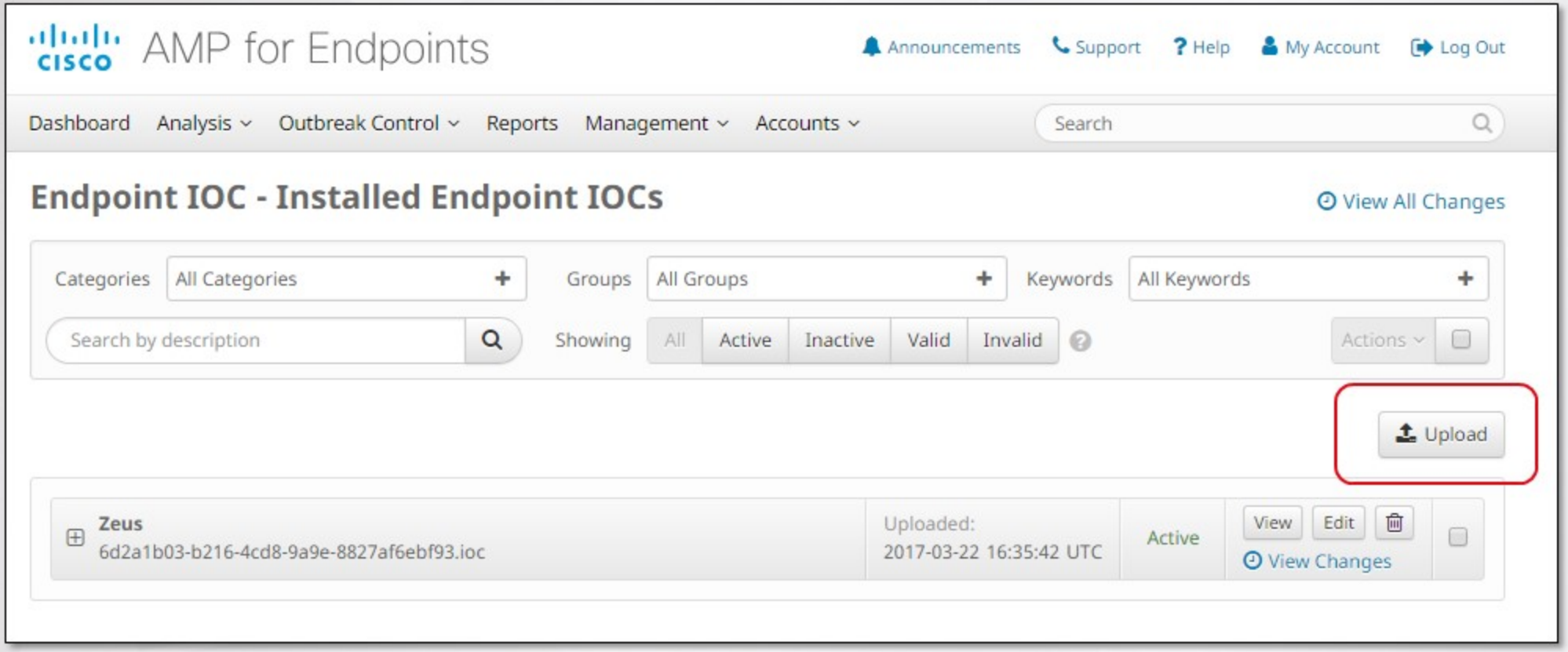
Uncheck All | Check All


[System]
winrar.exe [PE]
2017-03-22 19:53:07 UTC
Detected DOC..7BEA8B368F.ExecsPowerShell.hunt.Talos as 7bea8b36...2393c59d (7bea8b3..93c59d)[MS OLE2 CF] .
Created by WinRAR.exe, WinRAR 5.40.0.0 (a1290e4..731af1) [PE_Executable] executing as u@DESKTOP-48PCFBH.
The file was quarantined.
Process disposition Unknown.
File full path: C:\Users\zochova\AppData\Local\Temp\Rar$DRa0.642\infected\7bea8b368f9ba3b9ca8cf5e0636d148aaae6317e8194ec72504340dd2393c59d
File SHA-1: 120cea0df185757593b0f783e4f78f9ee8450d.
File MD5: dcea30baff165b3c3170878bd934fce3.
File size: 128512 bytes.
Parent file SHA-1: a859815e601a03d329cc6753c9bfc404a251e348.
Parent file MD5: 775b5ab4b2904acdf02f80219e0b5c90.
Parent file size: 1551248 bytes.
Parent file signed by win.rar GmbH with certificiate serial 00fe46a10ad94269c3dd225c13645352e4 from COMODO RSA Code Signing CA. Expires 23:59:59, Wed May 31 2017 UTC. the certificate was warn trusted
Parent file cert MD5: 041f2e8bb78ef6e5243dcb13df1151c4.
Parent file cert SHA-1: cc6fd0d1ee3570e592a181d6b41e0ff308d833d3.
Parent process id: 4676.
Parent process SID: S-1-5-21-3460200594-822345992-2783450900-1001.
Detected by the SHA engines.
TIME
Mar 22, 2017, 20:45
Mar 22, 2017, 21:46
EVENT TYPE
create
copy
move
execute
open
connection
scan detection
exec block
compromised?
restore
reboot
scan
defs update
policy update
connector update
scan schedule
uninstall
EVENT DISPOSITION
benign
malicious
unknown
EVENT FLAGS
none
warning
audit only
command-line
FILE TYPE
executable
ms office (ole2)
pdf
ms cabinet
flash
zip archive
other
unknown
Search
Uncheck All
Check All

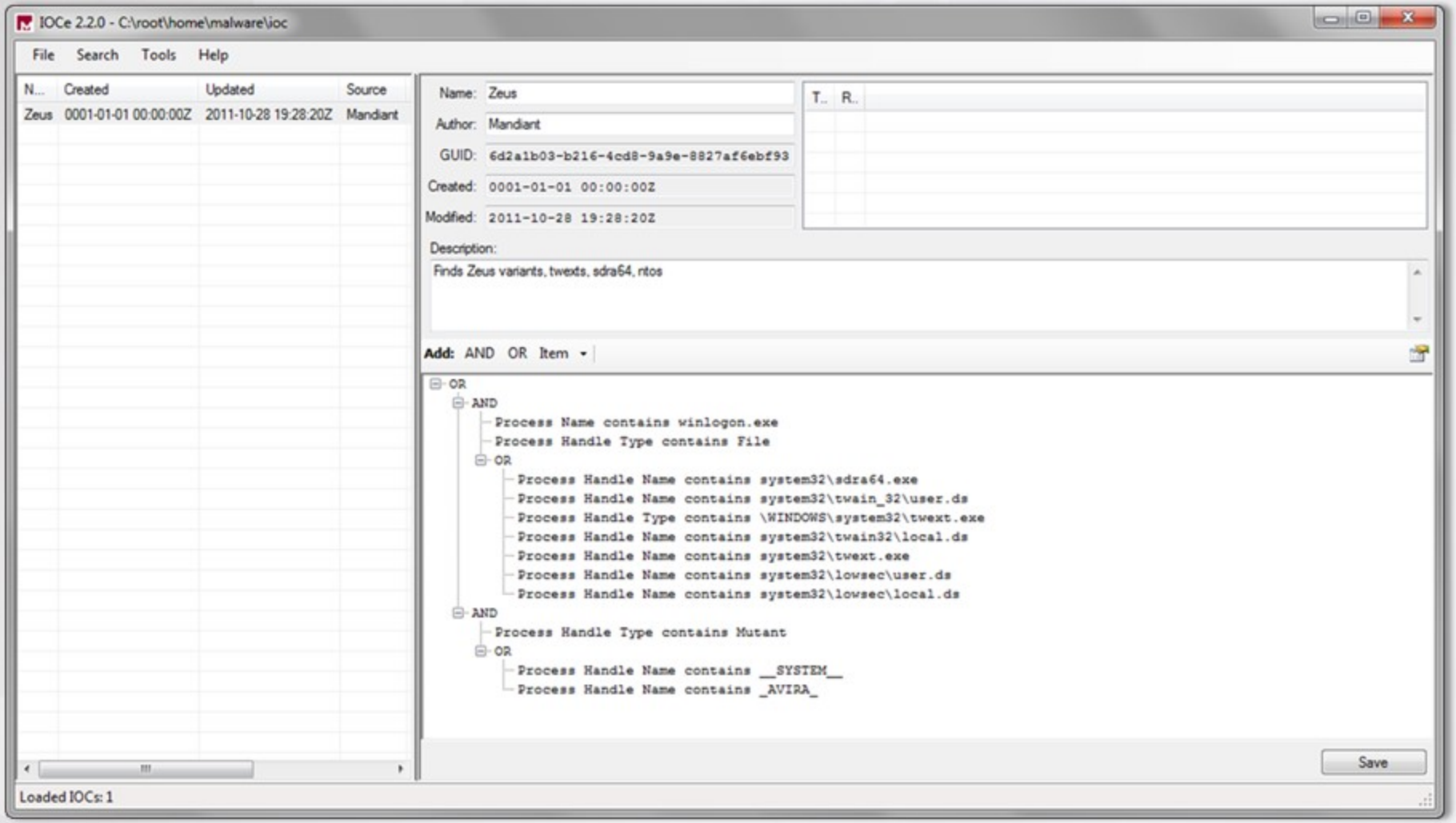

Vulnerable Software 10.0
All Day Week
Adobe Flash Player v11.5.502.146 c1219f07...605cc42b 1 62 severe vulnerabilities 2017-03-22 09:46:57 UTC 10.0
Oracle Java(TM) Platform SE v1.7.0:update... 0b4eefc0...201ccbd9 1 99 severe vulnerabilities 2017-03-22 09:46:57 UTC 10.0
Adobe Acrobat Reader v9.3.3.177 825b7b20...432e4f82 2 54 severe vulnerabilities 2017-03-22 09:46:57 UTC 10.0
CVE-2013-3346 10.0 CVE-2013-2729 10.0 CVE-2013-3342 10.0 CVE-2013-3341 10.0 CVE-2013-2718 10.0
CVE-2013-2719 10.0 CVE-2013-2720 10.0 CVE-2013-2721 10.0 CVE-2013-2722 10.0 CVE-2013-2723 10.0
CVE-2013-2724 10.0 CVE-2013-2725 10.0 CVE-2013-2726 10.0 CVE-2013-2727 10.0 CVE-2013-2730 10.0
CVE-2013-2731 10.0 CVE-2013-2732 10.0 CVE-2013-2733 10.0 CVE-2013-2735 10.0 CVE-2013-2736 10.0
CVE-2013-3340 10.0 CVE-2013-3337 10.0 CVE-2013-3338 10.0 CVE-2013-3339 10.0 CVE-2013-0601 10.0
CVE-2013-0602 10.0 CVE-2013-0603 10.0 CVE-2013-0604 10.0 CVE-2013-0605 10.0 CVE-2013-0606 10.0
CVE-2013-0607 10.0 CVE-2013-0608 10.0 CVE-2013-0609 10.0 CVE-2013-0610 10.0 CVE-2013-0611 10.0
CVE-2013-0612 10.0 CVE-2013-0613 10.0 CVE-2013-0614 10.0 CVE-2013-0615 10.0 CVE-2013-0616 10.0
CVE-2013-0617 10.0 CVE-2013-0618 10.0 CVE-2013-0619 10.0 CVE-2013-0620 10.0 CVE-2013-0621 10.0
CVE-2013-0622 10.0 CVE-2013-0623 10.0 CVE-2013-0624 10.0 CVE-2013-0626 10.0 CVE-2013-1376 10.0
CVE-2013-2734 10.0 CVE-2013-0640 9.3 CVE-2013-0641 9.3 CVE-2013-0627 7.2
Observed in groups: Triage Audit
Filename: AcroRd32.exe
Last Observed: Demo_SFEicar • 2017-03-22 09:46:57 UTC • Device Trajectory
Events File Trajectory


Vulnerable Software 10.0
All Day Week
Adobe Flash Player v11.5.502.146 c1219f07...605cc42b 1 62 severe vulnerabilities 2017-03-22 09:46:57 UTC 10.0
Oracle Java(TM) Platform SE v1.7.0:update... 0b4eefc0...201ccbd9 1 99 severe vulnerabilities 2017-03-22 09:46:57 UTC 10.0
CVE-2013-5830 10.0 CVE-2013-5843 10.0 CVE-2013-5842 10.0 CVE-2013-5817 10.0 CVE-2013-5814 10.0
CVE-2013-5809 10.0 CVE-2013-5789 10.0 CVE-2013-5829 10.0 CVE-2013-5788 10.0 CVE-2013-5824 10.0
CVE-2013-5787 10.0 CVE-2013-5782 10.0 CVE-2013-2470 10.0 CVE-2013-2465 10.0 CVE-2013-2471 10.0
CVE-2013-2473 10.0 CVE-2013-2472 10.0 CVE-2013-2469 10.0 CVE-2013-2468 10.0 CVE-2013-2466 10.0
CVE-2013-2464 10.0 CVE-2013-2463 10.0 CVE-2013-2459 10.0 CVE-2013-2428 10.0 CVE-2013-2420 10.0
CVE-2013-2434 10.0 CVE-2013-2384 10.0 CVE-2013-1518 10.0 CVE-2013-1537 10.0 CVE-2013-2440 10.0
CVE-2013-1557 10.0 CVE-2013-1558 10.0 CVE-2013-2435 10.0 CVE-2013-2432 10.0 CVE-2013-1569 10.0
CVE-2013-2431 10.0 CVE-2013-2383 10.0 CVE-2013-2427 10.0 CVE-2013-2425 10.0 CVE-2013-2422 10.0
CVE-2013-2414 10.0 CVE-2013-0809 10.0 CVE-2013-1493 10.0 CVE-2013-1480 10.0 CVE-2013-0428 10.0
CVE-2013-0437 10.0 CVE-2013-0441 10.0 CVE-2013-0442 10.0 CVE-2013-0445 10.0 CVE-2013-0450 10.0
CVE-2013-1476 10.0 CVE-2013-1478 10.0 CVE-2013-1479 10.0 CVE-2013-1484 10.0 CVE-2013-0426 10.0
CVE-2013-1486 10.0 CVE-2013-1487 10.0 CVE-2013-0425 10.0 CVE-2013-0422 10.0 CVE-2013-0446 10.0
CVE-2013-1475 10.0 CVE-2013-2460 9.3 CVE-2013-5838 9.3 CVE-2013-5777 9.3 CVE-2013-5810 9.3
CVE-2013-5832 9.3 CVE-2013-5806 9.3 CVE-2013-5805 9.3 CVE-2013-5850 9.3 CVE-2013-5844 9.3
CVE-2013-5846 9.3 CVE-2013-2462 9.3 CVE-2013-2436 9.3 CVE-2013-2426 9.3 CVE-2013-2421 9.3
CVE-2013-2445 7.8 CVE-2013-5852 7.6 CVE-2013-2448 7.6 CVE-2013-2394 7.6 CVE-2013-2429 7.6
CVE-2013-2430 7.6 CVE-2013-1563 7.8 CVE-2013-0429 7.6 CVE-2013-0444 7.6 CVE-2013-0419 7.6
CVE-2013-0423 7.6 CVE-2013-5775 7.5 CVE-2013-5802 7.5 CVE-2013-2442 7.5 CVE-2013-2461 7.5
CVE-2013-0351 7.5 CVE-2013-2439 6.9 CVE-2013-0430 6.9 CVE-2013-3829 6.4 CVE-2013-5783 6.4
CVE-2013-5804 6.4 CVE-2013-5812 6.4 CVE-2013-2407 6.4 CVE-2013-0432 6.4
Observed in groups: Protect
Filename: java.exe
Last Observed: Demo_ZAccess • 2017-03-22 09:46:57 UTC • Device Trajectory
Events File Trajectory
Adobe Acrobat Reader v9.3.3.177 825b7b20...432e4f82 2 54 severe vulnerabilities 2017-03-22 09:46:57 UTC 10.0


AMP for Endpoints
Announcements
Support
Help
My Account
Log Out
Dashboard
Analysis
Outbreak Control
Reports
Management
Accounts
Search
Prevalence
Windows
Mac
Linux
Configure Automatic Analysis
wsymqyv90.exe was only executed on Demo_Upatre
Analyze
2017-03-22 09:20:34 UTC
vxevcvk.exe was only executed on Demo_TeslaCrypt
Report 100 12
2017-03-22 08:45:02 UTC
94135acf...874a464c was only executed on Demo_TDSS
Analyze
2017-03-22 08:14:36 UTC
032b6d1f...e7ed4713 was only executed on Demo_TDSS
Analyze
2017-03-22 08:14:35 UTC
tdss.exe was only executed on Demo_TDSS
Report 100 1
2017-03-22 08:10:59 UTC
Tinba.exe was only executed on Demo_Tinba
Report 95 1
2017-03-22 08:09:01 UTC
c36a47b6...0e46cba9 was only executed on Demo_Tinba
Analyze
2017-03-22 08:09:01 UTC
ps.exe was only executed on Demo_Plugx
Report 100 1
2017-03-22 08:07:42 UTC
jwenjktgenwrger234231.exe was only executed on Demo_Dyre
Report 100 1
2017-03-22 08:07:18 UTC
explorer.exe was only executed on Demo_ZAccess
Analyze
2017-03-22 08:06:24 UTC
6c72dabb...2fa77f05 was only executed on Demo_ZAccess
Analyze
2017-03-22 08:05:55 UTC
rundll32.exe was only executed on Demo_ZAccess
Analyze
2017-03-22 08:05:18 UTC
InstallFlashPlayer.exe was only executed on Demo_ZAccess
Analyze
2017-03-22 08:05:14 UTC
zaccess8308073210892168095.exe was only executed on Demo_ZAccess
Report 100 2
2017-03-22 08:05:09 UTC
java.exe was only executed on Demo_ZAccess
Analyze
2017-03-22 08:05:05 UTC
9d4bc8df...9ed8a458 was only executed on Demo_ZAccess
Analyze
2017-03-22 08:05:04 UTC
2 was only executed on Demo_SFEicar
Analyze
2017-03-22 08:04:08 UTC
84f85558...71e30e90 was only executed on Demo_SFEicar
Analyze
2017-03-22 08:04:08 UTC
4063259f...89dddbba was only executed on Demo_SFEicar
Analyze
2017-03-22 08:03:57 UTC
1 - 25 of 72 total records
1
of 3


AMP for Endpoints
Announcements
Support
Help
My Account
Log Out
Dashboard
Analysis
Outbreak Control
Reports
Management
Accounts
Search
Endpoint IOC - Installed Endpoint IOCs
View All Changes
Categories
All Categories
Groups
All Groups
Keywords
All Keywords
Search by description
Showing
All
Active
Inactive
Valid
Invalid
Actions
Upload
Zeus
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93.ioc
Uploaded:
2017-03-22 16:35:42 UTC
Active
View
Edit
View Changes

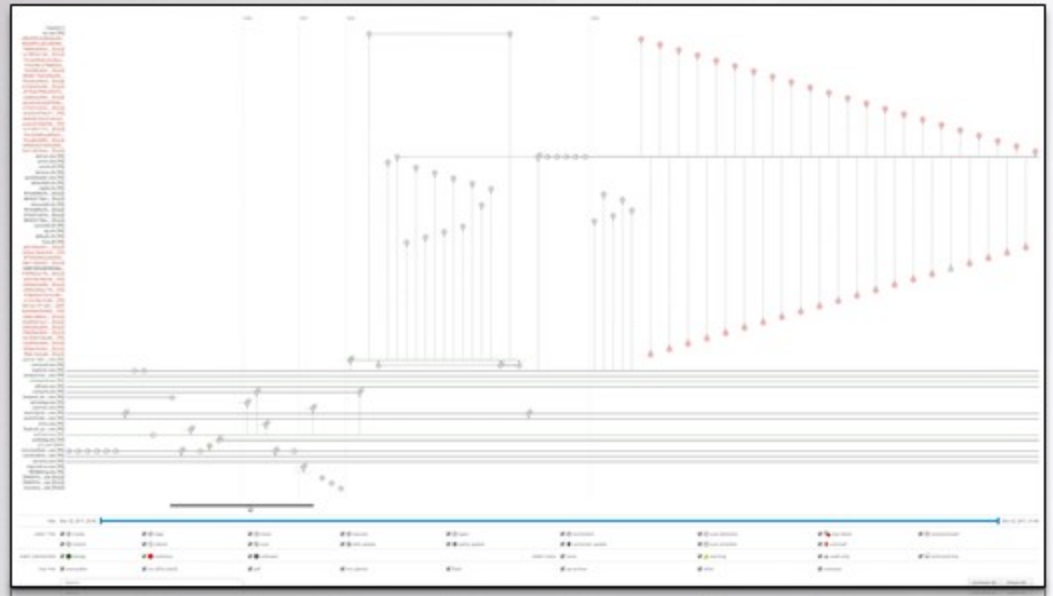
```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="6d2a1b03-b216-4cd8-
  <short_description>Zeus</short_description>
  <description>Finds Zeus variants, twexts, sdra64, ntos</description>
  <keywords />
  <authored_by>Mandiant</authored_by>
  <authored_date>0001-01-01T00:00:00</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="9c8df971-32a8-4ede-8a3a-c5cb2c1439c6">
      <Indicator operator="AND" id="0781258f-6960-4da5-97a0-ec35fb403cac">
        <IndicatorItem id="50455b63-35bf-4efa-9f06-aeba2980f80a" condition="contains">
          <Context document="ProcessItem" search="ProcessItem/name" type="mir" />
          <Content type="string">winlogon.exe</Content>
        </IndicatorItem>
        <IndicatorItem id="b05d9b40-0528-461f-9721-e31d5651abdc" condition="contains">
          <Context document="ProcessItem" search="ProcessItem/HandleList/Handle/Type" type="mir" />
          <Content type="string">File</Content>
        </IndicatorItem>
        <Indicator operator="OR" id="67505775-6577-43b2-bccd-74603223180a">
          <IndicatorItem id="c5ae706f-c032-4da7-8acd-4523f1dae9f6" condition="contains">
            <Context document="ProcessItem" search="ProcessItem/HandleList/Handle/Name" type="mir" />
            <Content type="string">system32\sdra64.exe</Content>
          </IndicatorItem>
          <IndicatorItem id="25ff12a7-665b-4e45-8b0f-6e5ca7b95801" condition="contains">
            <Context document="ProcessItem" search="ProcessItem/HandleList/Handle/Name" type="mir" />
            <Content type="string">system32\twain_32\user.ds</Content>
          </IndicatorItem>
          <IndicatorItem id="fea11706-9ebe-469b-b30a-4047cfb7436b" condition="contains">
            <Context document="ProcessItem" search="ProcessItem/HandleList/Handle/Type" type="mir" />
            <Content type="string">\WINDOWS\system32\twext.exe</Content>
          </IndicatorItem>
          <IndicatorItem id="94ac992c-8d6d-441f-bfc4-5235f9b09af8" condition="contains">
            <Context document="ProcessItem" search="ProcessItem/HandleList/Handle/Name" type="mir" />
            <Content type="string">system32\twain32\local.ds</Content>
          </IndicatorItem>
```


IOCe 2.2.0 - C:\root\home\malware\ioc
File
Search
Tools
Help
N...
Created
Updated
Source
Zeus
0001-01-01 00:00:00Z
2011-10-28 19:28:20Z
Mandiant
Name: Zeus
Author: Mandiant
GUID: 6d2a1b03-b216-4cd8-9a9e-8827af6ebf93
Created: 0001-01-01 00:00:00Z
Modified: 2011-10-28 19:28:20Z
T..
R..
Description:
Finds Zeus variants, twexts, sdra64, ntos
Add: AND OR Item
OR
AND
Process Name contains winlogon.exe
Process Handle Type contains File
OR
Process Handle Name contains system32\sdra64.exe
Process Handle Name contains system32\twain_32\user.ds
Process Handle Type contains \WINDOWS\system32\twext.exe
Process Handle Name contains system32\twain32\local.ds
Process Handle Name contains system32\twext.exe
Process Handle Name contains system32\lowsec\user.ds
Process Handle Name contains system32\lowsec\local.ds
AND
Process Handle Type contains Mutant
OR
Process Handle Name contains __SYSTEM__
Process Handle Name contains _AVIRA_
Save
Loaded IOCs: 1

SOITRON

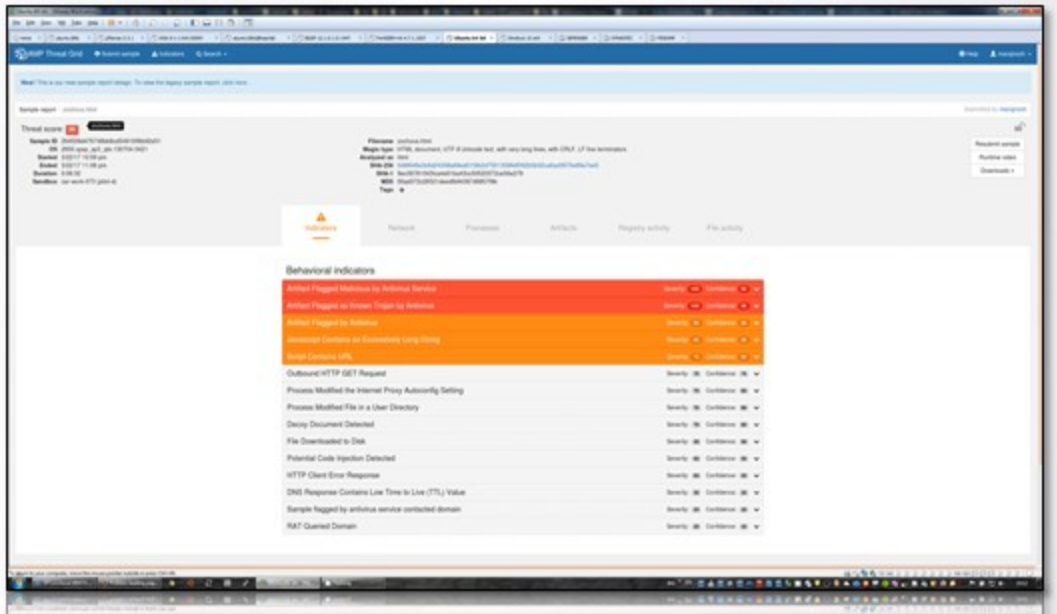
INŠPIRUJEME K NÁROČNOSTI

Cisco FireAMP trajectory



https://youtu.be/F_b25WJ8Q7U

Cisco Threatgrid sandboxing



https://youtu.be/wctsekRoUJY