



Poznaním malvéru k efektívnej obrane

alebo ako udržať krok so škodlivým kódom...

Maroš Rajnoch, SOITRON, s.r.o.

presales support

maros@soitron.com


dôvernost' 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.

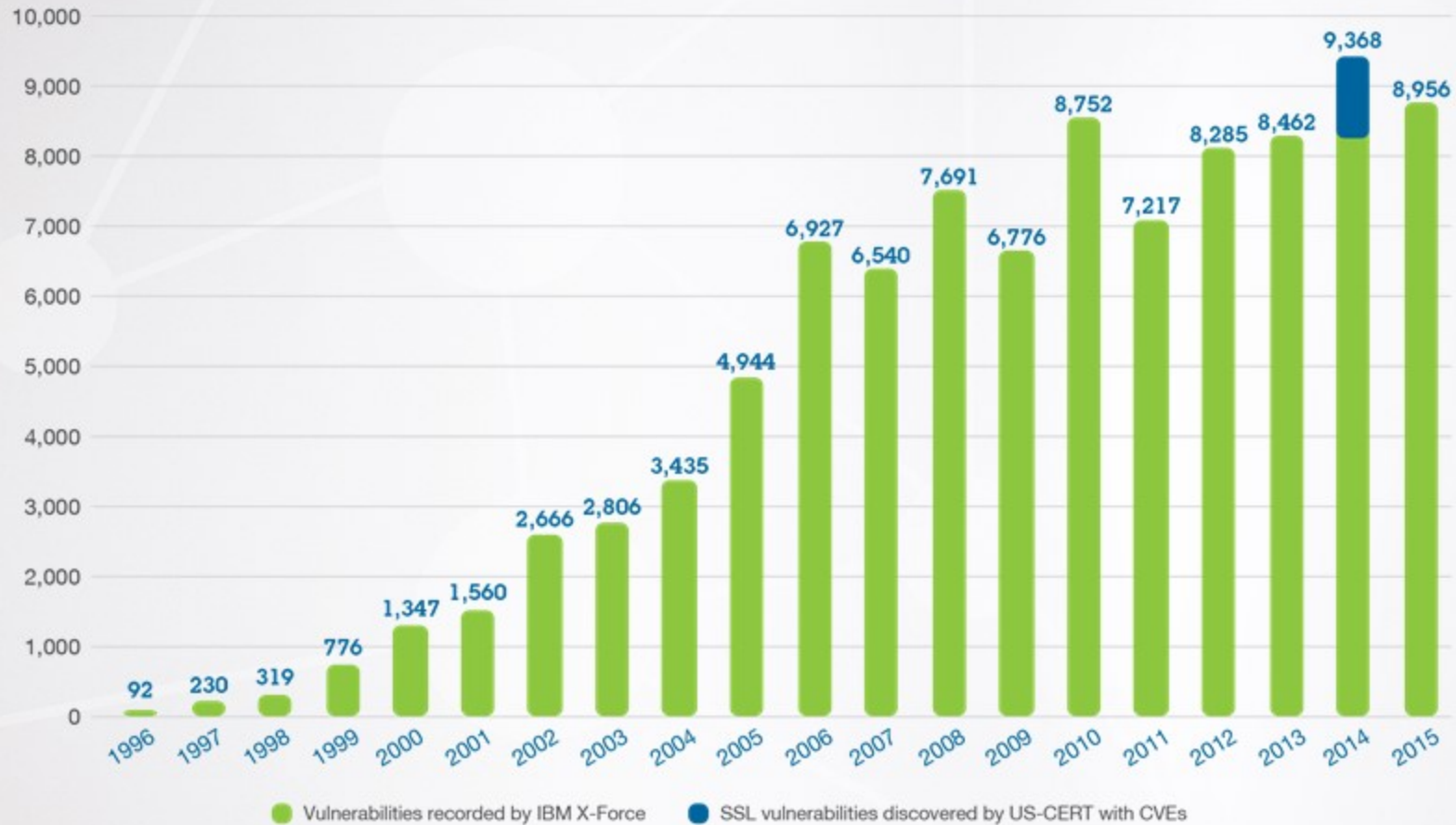




Dokument	Poznaním malvéru k efektívnej obrane
Podnázov	Ako udržať krok so škodlivým kódom...
Verzia	1. X58D7BFCF
Klasifikácia	SELECTED AUDIENCE
OID	1.3.158.35955678.299039.X58D7BFCF
Vypracoval	Maroš Rajnoch
Konzultant	N/A
Preveril	Štefan Porubčan
Schválil	N/A

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
Magnitude
Angler
Neutrino
RIG

Angler

Nuclear
Angler
Neutrino

Nuclear
Magnitude

Angler

Nuclear
Magnitude
Angler

Angler

RIG

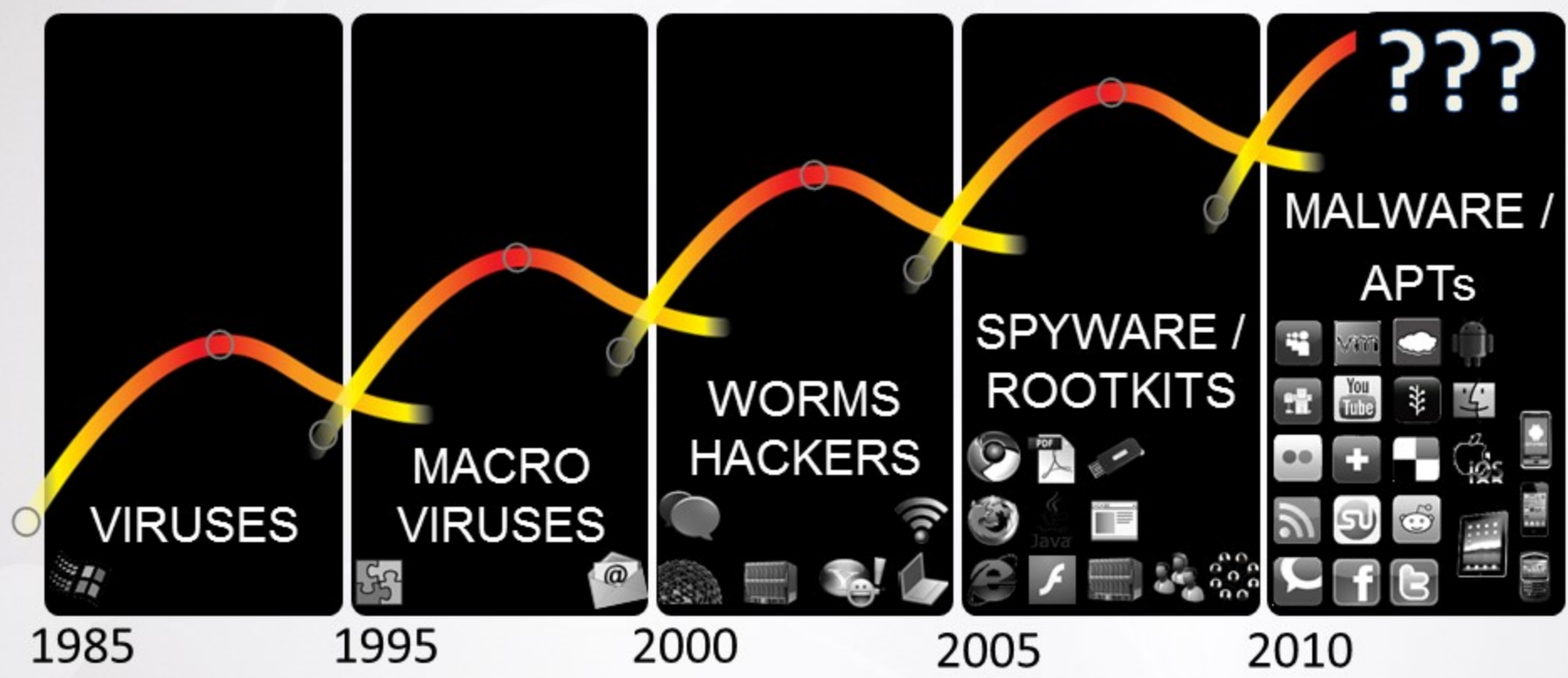
Source: Cisco Security Research

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.

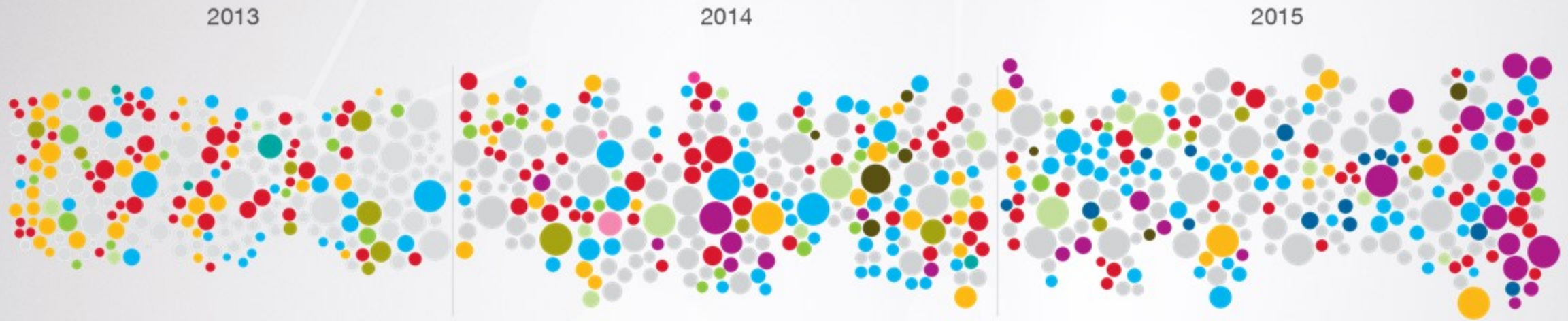
In 2015, 54 zero-day vulnerabilities were discovered.





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.



Attack types



XSS



Heartbleed



Physical
access



Brute force



Misconfig.



Malvertising



Watering
hole



Phishing



SQLi



DDoS



Malware

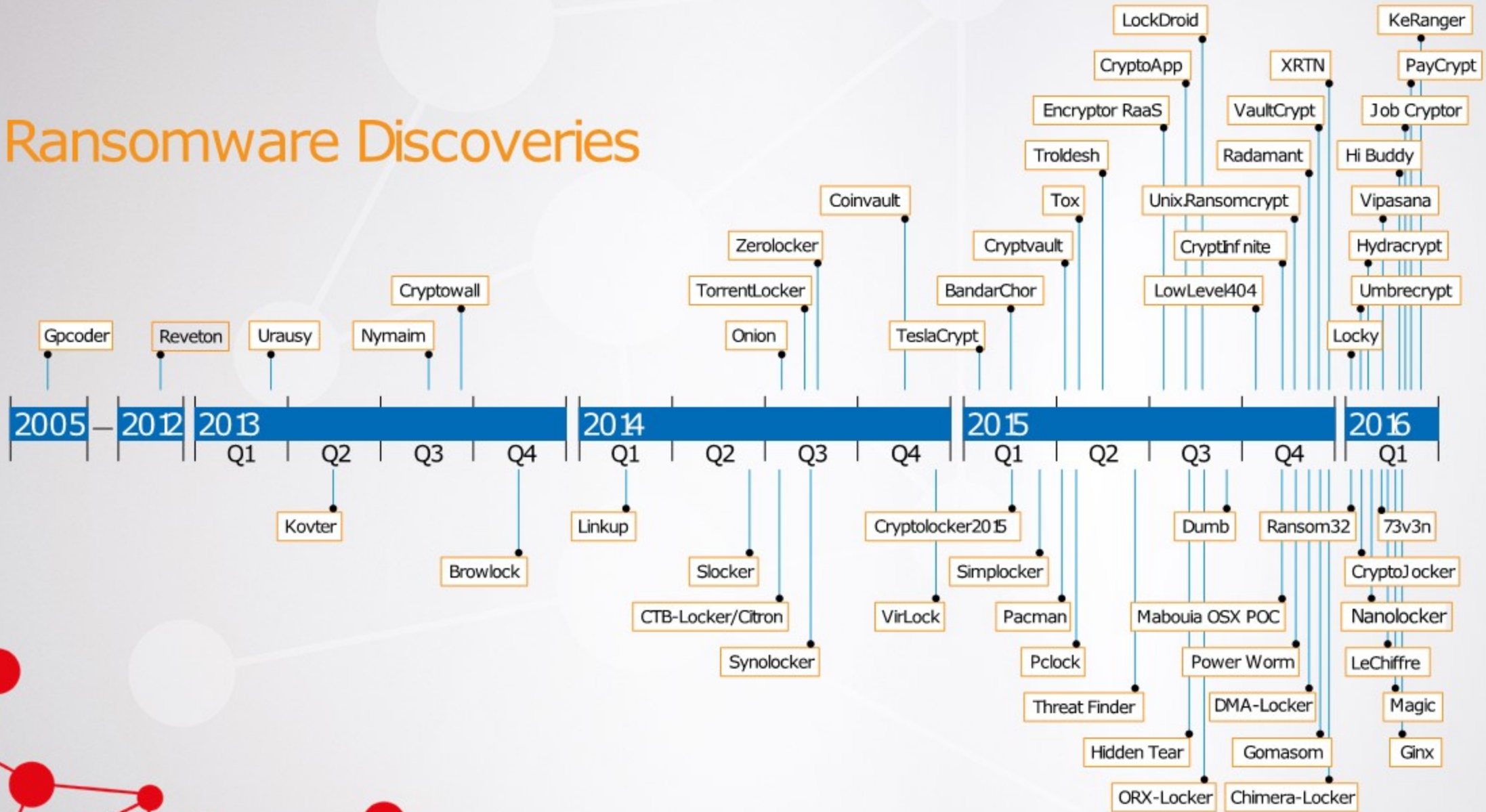


Undisclosed

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

Source: IBM X-Force® Research and Development

Ransomware Discoveries



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



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.

RISK ASSESSMENT —

Maryland hospital group hit by ransomware launched from [Updated]

Samsam malware injected into network from exploited web

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



Baltimore's Green Memorial is one of the hospitals hit by Samsam, an autonomous malware.

Maryland hospital: Ransom wasn't IT department's fault

MedStar denies ransom payment, denies earlier IT boss bugs pl

SEAN GALLAGHER - 2/17/2016, 4:12 PM



MedStar's Good Samaritan Hospital in Baltimore, one of 10 affected by a ransomware

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

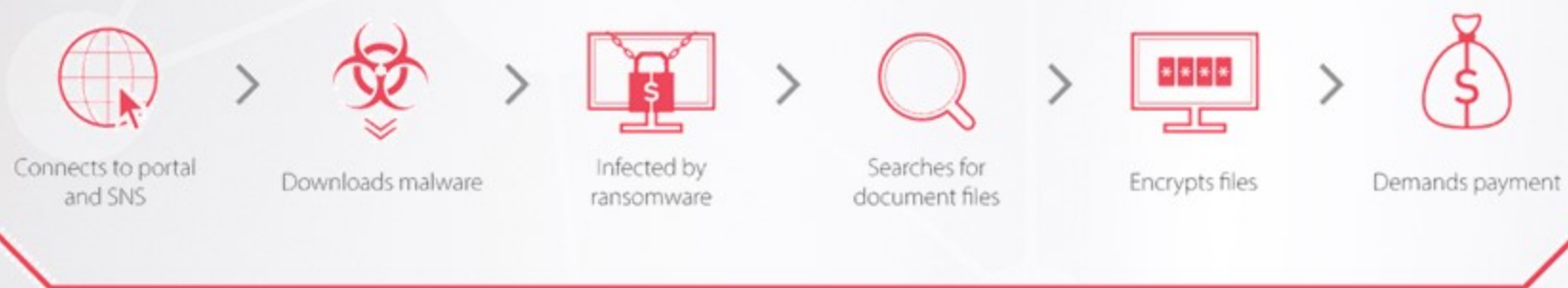


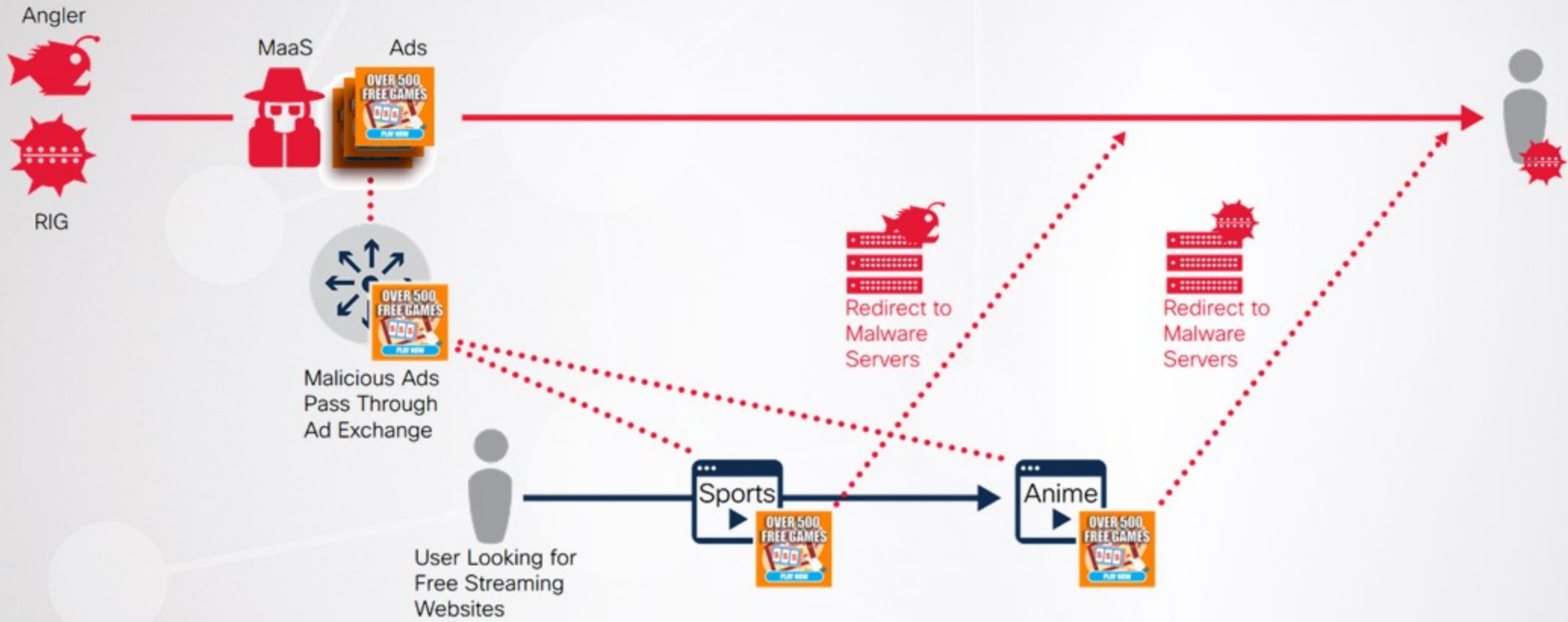
Which ransoms are detected?

This service currently detects **339** different ransoms. 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, BadEncrypt, Bandanchor, 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, Covertor, Cripton, **CrptXXX**, Cryakl, CryFile, CryLocker, CrypMic, CrypMic, Crypren, Crypt0, Crypt0Locker, 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), Digsom, 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, Globelmposter, Globelmposter 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, Negozi, Nemucod, Nemucod-7z, Netix, Nhtnwuf, 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 X RAT, Telecrypt, TeslaCrypt 0.x, TeslaCrypt 2.x, TeslaCrypt 3.0, TeslaCrypt 4.0, TowerWeb, ToxCrypt, Trojan.Encoder.6491, Troidesh / 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

Ransomware **Attack Process**





Source: Cisco Security Research

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

Source: Cisco Security Research

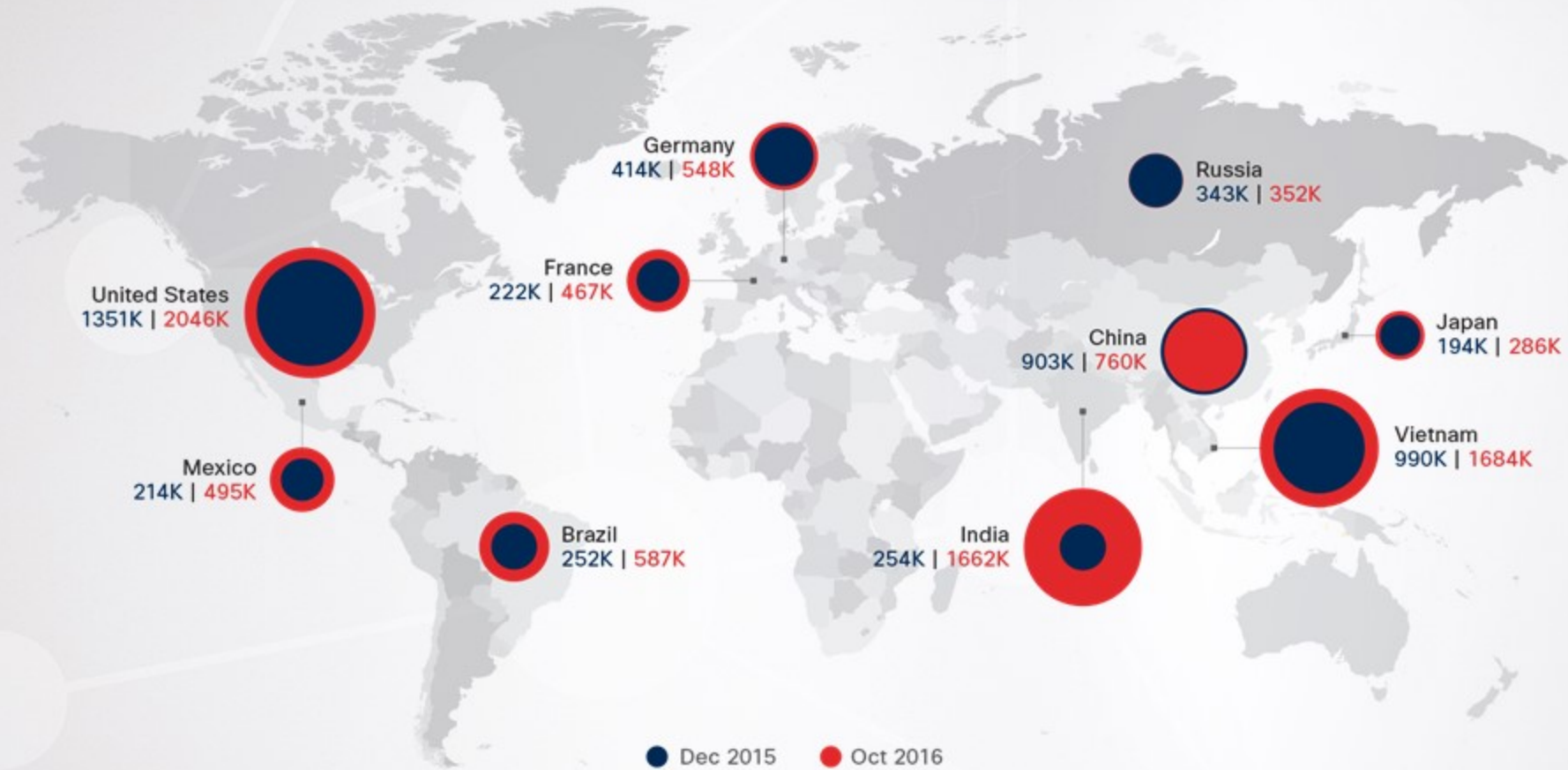


Figure 18 Comparison of Hailstorm and Snowshoe Spam Attacks

Source: Cisco Investigate



Advanced Malware



A new or unknown malware plays key role in security breach

Advanced

Uses various advanced attack techniques

Targeted

Specific targets

Persistent

Infects and remains stealthy

VS.

Ransomware



Advanced malware causes financial damages and interferes with access to information assets

Advanced

Uses various advanced attack techniques

Non-Targeted

Random targets

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
- Necessaries
 - 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

apocalypse (2)

Server ID	Lan	Wan	Computer Name	Username	Account Type	Operating System	Processor
apocalypse	192.168.56.104	192.168.56.104	VICTIM-XP	lostandfound	Administrator	Windows XP (Prof...	2747 Mhz
apocalypse	192.168.56.106	192.168.56.106	VICTIM-7	LostAndFound	Administrator	Windows Vista (E...	2785 Mhz

Message Box Server ID : apOcalypse - 192.168.56.106@192.168.56.106

Message Box Message List

Message Icon

Available Buttons

- OK
- Yes, No
- OK, Cancel
- Yes, No, Cancel
- Retry, Cancel
- Abort, Retry, Ignore

Message Settings

Title : huhu

Message : ako sa mas?

Test Message Send Message

Server ID : apOcalypse - 192.168.56.106@192.168.56.106

Remote Desktop Server ID : apOcalypse - 192.168.56.106@192.168.56.106

Start Quality Control Show Cursor Delay Screen Extra Save Picture

Disconnected.

Command Prompt Server ID : apOcalypse - 192.168.56.106@192.168.56.106

```

\\192.168.56.1\efs
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
nakolen\lostandfound

C:\Windows>
  
```

response received.

```

C:\Documents\
ERROR:
Code = 0
Descript:
Facility

C:\Documents\
Executing
Method e
Out Param
instance

C:\Documents\
Executing
Method e
Out Param
instance

C:\Documents\
Executing
Method e
Out Param
instance
  
```

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
 - 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

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 Clie...	4.0.30319	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Oracle VM VirtualBox Guest Addi...	4.2.16.0	Oracle Corporation	C:\Program Files\Oracle\VirtualBox Guest Addition...
WinPcap 4.1.3	4.1.0.2980	Riverbed Technology, Inc.	C:\Program Files\WinPcap\uninstall.exe
Microsoft .NET Framework 4 Clie...	4.0.30319	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Update for Microsoft .NET Frame...	1	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Update for Microsoft .NET Frame...	1	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Update for Microsoft .NET Frame...	1	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Sec...	1	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Sec...	1	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Sec...	2	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Sec...	1	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...
Sec...	1	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319...

Refresh Uninstall Save As... Clear

installed application list received.

Registry Editor Server ID : ap0calypse - 192.168.56.106@192.168.56.106

Registry Config

Name	Type	Data
HKEY_CLASSES_ROOT		
HKEY_LOCAL_MACHINE		
BCD00000000		
HARDWARE		
SAM		
SECURITY		
SOFTWARE		
SYSTEM		
HKEY_CURRENT_USER		
HKEY_USERS		
HKEY_CURRENT_CONFIG		

HKEY_LOCAL_MACHINE\SYSTEM\SYSTEM

Server ID : ap0calypse - 192.168.56.106@192.168.56.106

Webcam Capture Server ID : ap0calypse - 192.168.56.106@192.168.56.106

Get Webcams Start Quality Delay Stretch

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 DECI...][SPACE][BACKSPACE][BACKSPACE][BACKSPACE]moj internet banking
 heslo[SHIFT]: superheslo[NUM 1][NUM 2][NUM 3]

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.dl...
Windows Audio Endp...	AudioEndpointBul...	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 Service Name File Name

IPv6 Core Service IPv6 Core Service solitaire.exe

Description Start Up

This service is needed for correct OS functio Automatic

Server ID : ap0calypse - 192.168.56.106@192.168.56.106

Create Service Cancel

Startup Manager Server ID : ap0calypse - 192.168.56.106@192.168.56.106

node:%a process call cre
 ll create un_tc.exe

HKEY_CURRENT_USER

- Software
- Windows
 - CurrentVersion
 - Run
 - RunOnce

HKEY_LOCAL_MACHINE

- Software
- 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



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 Sledovat

@Allan_Wirth @tqbf That's fair. Defender is the only one I know of that hasn't broken Chrome's security mechanisms. /CC @tavis


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 @tavis This is correct - and we have data support this statement.

3 5 18

 **Tavis Ormandy**
@tavis 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 tavis@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.

become visible to the public.
without a broadly available patch, then the bug report will automatically
become visible to the public. If 90 days elapse

Thanks, Tavis.

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" }, "")
```

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 normal.
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 

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 

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

The image shows a screenshot of a Microsoft Word window. The title bar reads "vcf_bus_card_626477 (Read-Only) [Compatibility Mode] - Microsoft ...". The ribbon is set to "Picture Tools" with the "Format" tab selected. The ribbon includes sections for "Clipboard", "Font" (Times New Roman, size 12), "Paragraph", "Styles" (Normal, Strong), and "Editing" (Find, Replace, Select). The main content area has a dark blue background with the text "This Document is protected !" in white. Below this is a white box containing a Word icon with a shield and a list of three instructions:

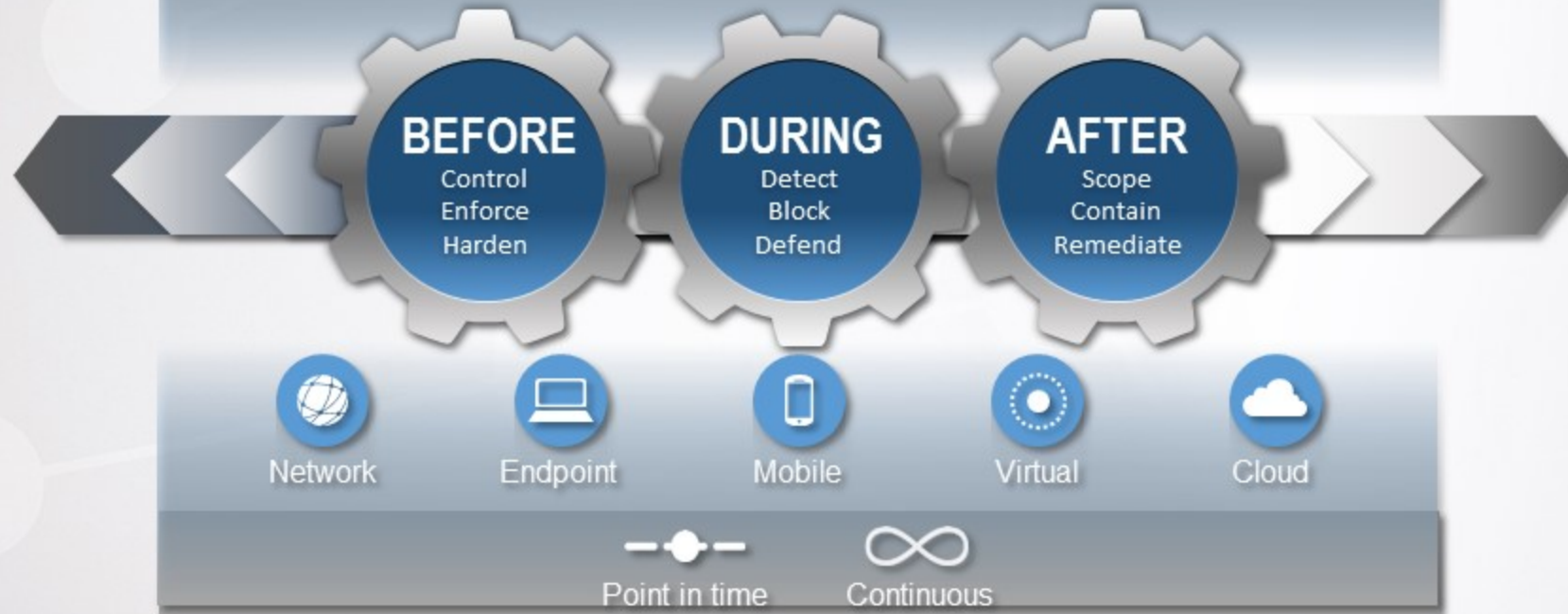
- 1 Open the document in Microsoft Office. Previewing offline is not available for protected documents.
- 2 If this document was downloaded from your email, please click "Enable editing" from the yellow bar above.
- 3 Once you have enabled editing, please click "Enable content" on the yellow bar above.

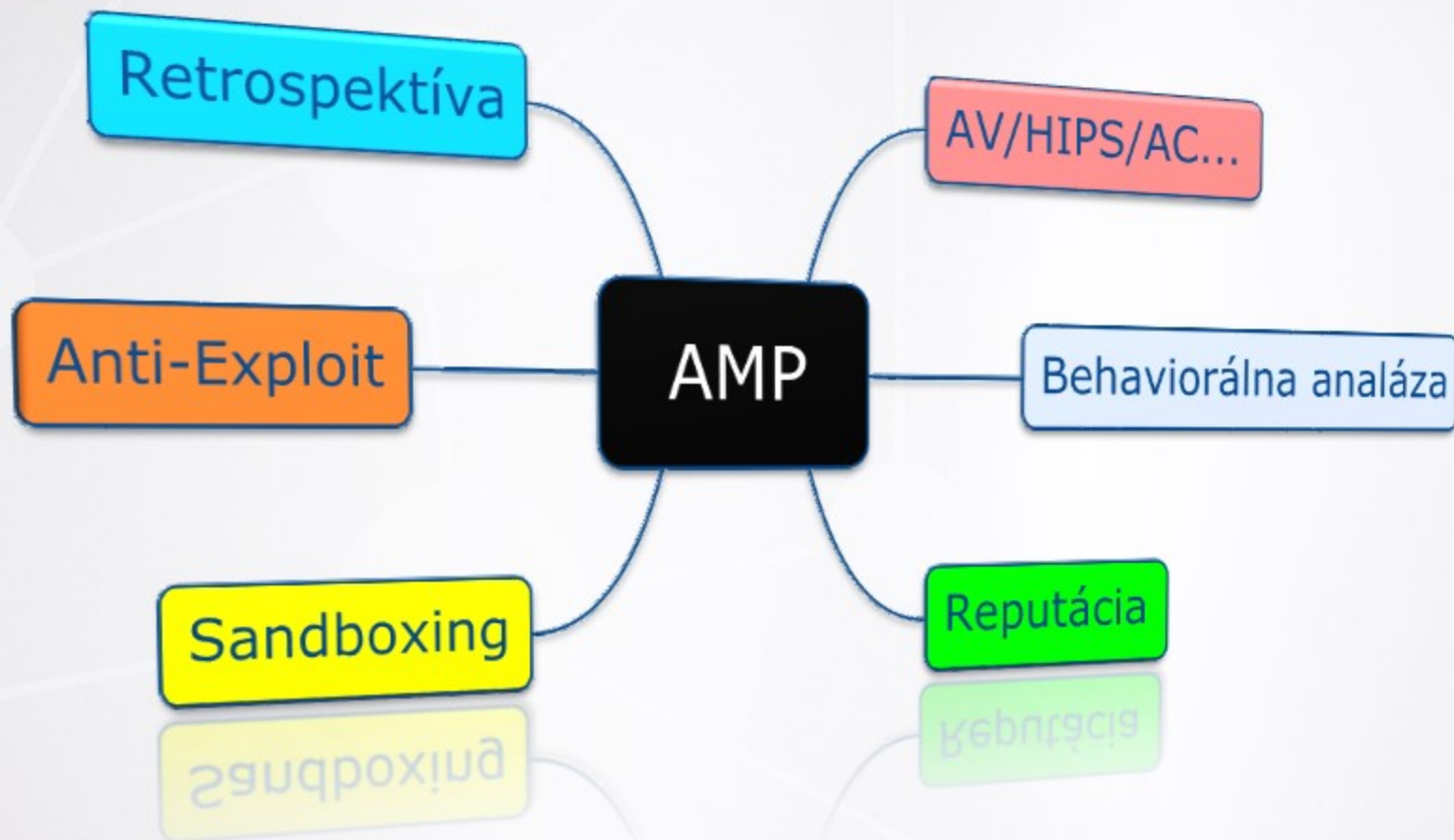
The status bar at the bottom shows "Page: 1 of 1", "Words: 0", and "100%". The taskbar at the very bottom shows the Start button and the active window "vcf_bus_card_62647...".

Ransomware Attack Process



Attack Continuum





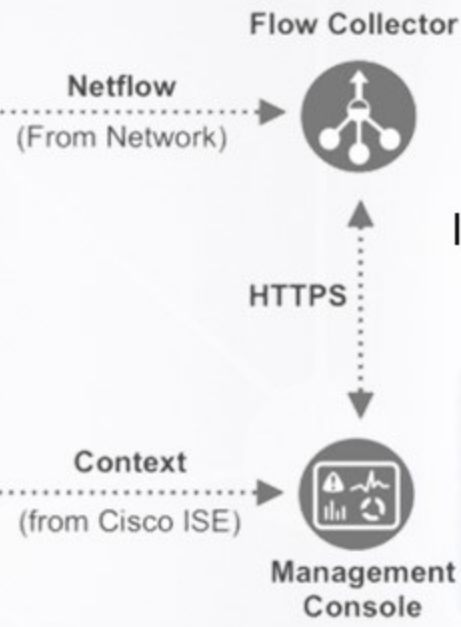
Behaviorálna analýza

Reputácia

Sandboxing

Anti-Exploit

Retrospektíva



lancope: netflow based anomaly detection



Behaviorálna analýza

Reputácia

Sandboxing

Anti-Exploit

Retrospektíva

lancope: netflow based anomaly detection

 **Network Scanning**

TCP, UDP, Port Scanning Across Multiple Hosts

 **Denial of Service**

SYN Half Open; ICMP/UDP/Port Flood

 **Host Reputation Change**

Inside Host Potentially Compromised

 **Botnet Detection**

When Inside Host Talks to Outside C&C Server

 **Fragmentation Attack**

Host Sending Abnormal # Malformed Fragments

 **Worm Propagation**

Worm Infected Host Scans, etc.

 **Data Exfiltration**

Large Outbound File Transfer VS. Baseline

 **Policy Violation**

Flag unusual transactions between network segments

Behaviorálna analýza

Reputácia

Sandboxing

Anti-Exploit

Retrospektíva

The screenshot displays a security dashboard with the following components:

- Navigation:** DASHBOARD, CONFIRMED, DETECTED (active), AMP for Endpoints
- Alert Summary:** MALWARE SALITY (8), 100% confidence, in #CSAL01, NEW. AFFECTING demo_angla.gamboa (Windows), 140.202.126.200. OCCURRENCE: 20 hours, Sep 25 - Sep 26.
- Activities and Webflows:** A network diagram showing connections between activities, domains, IPs, and autonomous systems. A severity filter is set to levels 9 and 8.
- Activity List:**

Severity	Activity	Domain	IP	Autonomous System
9	salicy	Q AMP patagonia-ambient.co...	Q AMP 181.88.192.62	Telecom Argentina S.A.
8	anomalous http	Q AMP bijibali.com	Q AMP 192.185.190.9	CyrusOne LLC
8	anomalous http	Q AMP inspiringgemsshop.com	Q AMP 52.28.249.128	CyrusOne LLC
8	malware distribution	Q AMP paktexileindustries.com	Q AMP 202.163.115.10	Cyber Internet Services (Pvt) Ltd.
8	anomalous http	Q AMP ktscc.org	Q AMP 119.59.104.21	453 Ladplacout Jorakhaebua
8	malware distribution	Q AMP 52.30.217.226:443	Q AMP 52.30.217.226	453 Ladplacout Jorakhaebua
8	salicy	Q AMP 137.117.241.14:443	Q AMP 137.117.241.14	Amazon.com, Inc.
8	anomalous http	Q AMP 178.250.0.67:443	Q AMP 178.250.0.67	Criteo SA
8	salicy	Q AMP 207.46.194.10:443	Q AMP 207.46.194.10	Microsoft Corporation
4	https connect tunneling	Q AMP 52.16.63.115:443	Q AMP 52.16.63.115	Microsoft Corporation
4	https connect tunneling			
3	downloading graphical image...			
- Timeline:** A bar chart on the right shows the duration of the event, labeled '19 hrs, 6 mins'.

Behaviorálna analýza

Reputácia

Sandboxing

Anti-Exploit

Retrospektíva

The screenshot displays the Cisco Umbrella Security Overview dashboard. The left sidebar contains navigation options: Overview, Identities, Policies, Reporting (with sub-items: Security Overview, Activity Search, REPORTS, Security Activity, Cloud Services, Total Requests, Activity Volume, Top Domains, Top Categories, Top Identities, My Reports, Destinations, Identities, Exported Reports, Scheduled Reports, Admin Audit Log), Settings, and Investigate. The main content area is titled 'Security Overview' and includes a 'LAST 24 HOURS' filter. It features three security category charts: Malware & Drive-by Requests (38, 124%), Command & Control Requests (2, 100%), and Phishing Requests (1, 0%). Below these are two tables: 'Events by Domain' and 'Events by Identity'. A welcome message from James at OpenDNS is also visible.

Category	Count	Percentage
Malware & Drive-by Requests	38	124%
Command & Control Requests	2	100%
Phishing Requests	1	0%

Domain	Requests	Identities
p.adpdx.com	10	2
downloadapps247.tech	4	2
2k.852x230.1a2b3e8d3.9b.pl	4	0
news.com.com	4	1
govv.org	2	0

Identity	Requests
trevor-0434	24

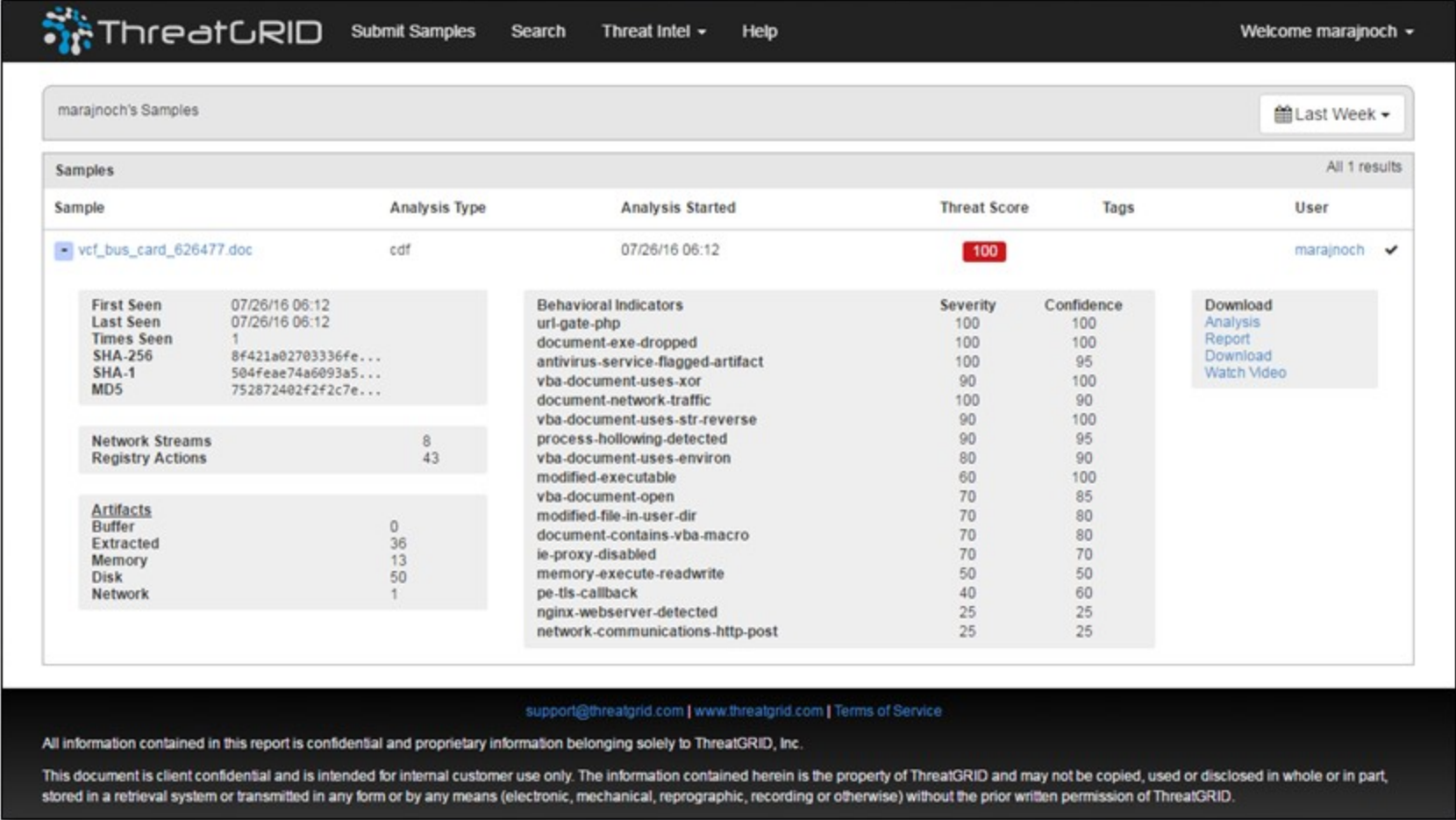
Behaviorálna analýza

Reputácia

Sandboxing

Anti-Exploit

Retrospektíva



The screenshot displays the ThreatGRID web interface. At the top, there is a navigation bar with the ThreatGRID logo, 'Submit Samples', 'Search', 'Threat Intel', and 'Help' menus. A user profile 'Welcome marajnoch' is visible in the top right. Below the navigation bar, a search bar contains 'marajnoch's Samples' and a date filter 'Last Week'. The main content area shows a table of samples with one entry selected: 'vcf_bus_card_626477.doc'. The table columns are 'Sample', 'Analysis Type', 'Analysis Started', 'Threat Score', 'Tags', and 'User'. The selected sample has a threat score of 100. Below the table, there are three detailed sections: 'First Seen' and 'Last Seen' (both 07/26/16 06:12), 'Behavioral Indicators' (a list of indicators with severity and confidence scores), and 'Artifacts' (a list of artifacts with counts). A 'Download' button is also present.

Sample	Analysis Type	Analysis Started	Threat Score	Tags	User
vcf_bus_card_626477.doc	cdf	07/26/16 06:12	100		marajnoch

Field	Value
First Seen	07/26/16 06:12
Last Seen	07/26/16 06:12
Times Seen	1
SHA-256	8f421a02703336fe...
SHA-1	504feae74a6093a5...
MD5	752872402f2f2c7e...

Indicator	Severity	Confidence
url-gate-php	100	100
document-exe-dropped	100	100
antivirus-service-flagged-artifact	100	95
vba-document-uses-xor	90	100
document-network-traffic	100	90
vba-document-uses-str-reverse	90	100
process-hollowing-detected	90	95
vba-document-uses-environ	80	90
modified-executable	60	100
vba-document-open	70	85
modified-file-in-user-dir	70	80
document-contains-vba-macro	70	80
ie-proxy-disabled	70	70
memory-execute-readwrite	50	50
pe-tls-callback	40	60
nginx-webserver-detected	25	25
network-communications-http-post	25	25

Artifact	Count
Buffer	0
Extracted	36
Memory	13
Disk	50
Network	1

support@threatgrid.com | www.threatgrid.com | Terms of Service

All information contained in this report is confidential and proprietary information belonging solely to ThreatGRID, Inc.

This document is client confidential and is intended for internal customer use only. The information contained herein is the property of ThreatGRID and may not be copied, used or disclosed in whole or in part, stored in a retrieval system or transmitted in any form or by any means (electronic, mechanical, reprographic, recording or otherwise) without the prior written permission of ThreatGRID.

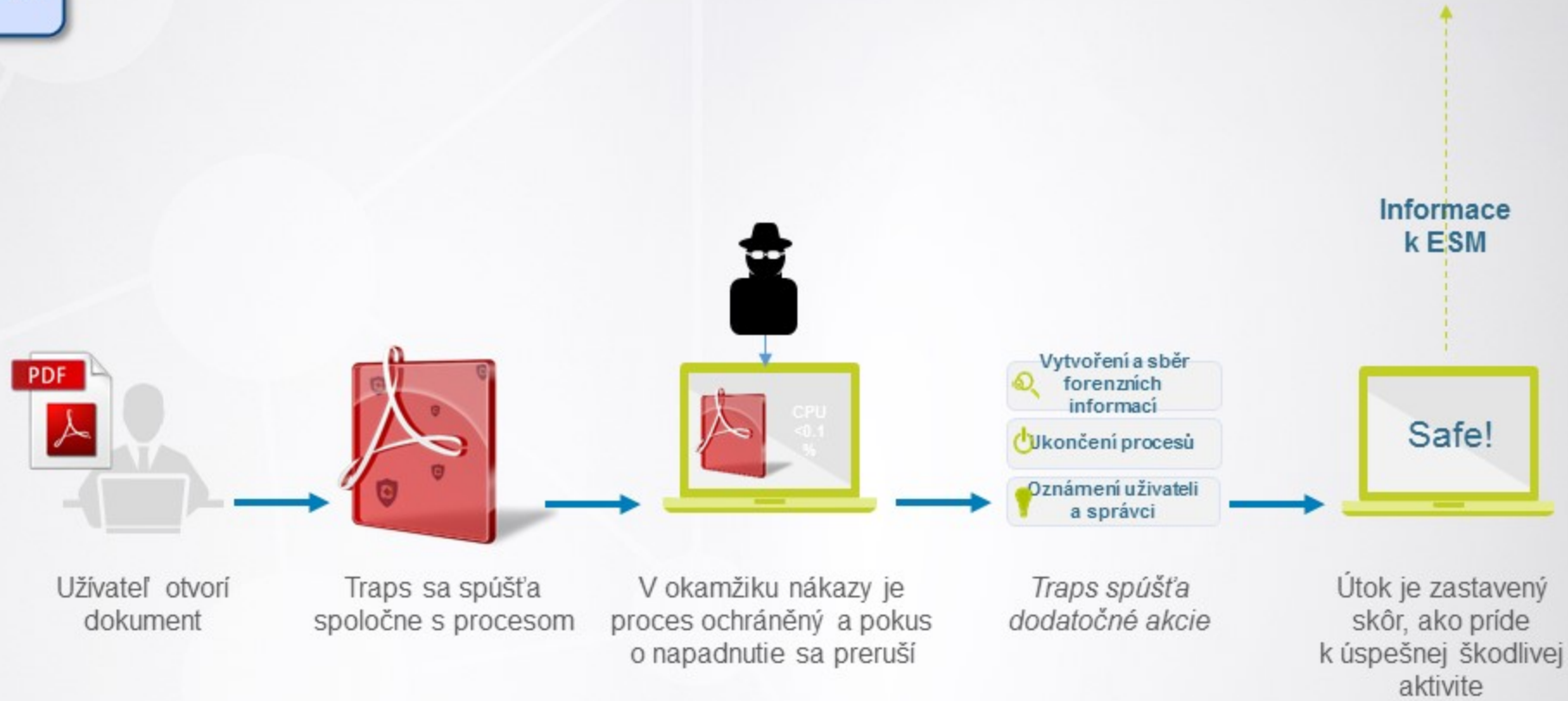
Behaviorálna analýza

Reputácia

Sandboxing

Anti-Exploit

Retrospektíva



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

Behaviorálna analýza

Reputácia

Sandboxing

Anti-Exploit

Retrospektíva

The screenshot shows the Sourcefire console dashboard with the following sections:

- Indications of Compromise:** A list of events with details and 'Mark Resolved' buttons.

Computer	Count
Demo_ZAccess	29
Demo_SFEicar	19
Demo_Ramnit	14
Demo_TDSS	13
Demo_Zbot	13
- Hosts Detecting Malware (7 days):** A bar chart showing the number of detections for various computers.
- Hosts Detecting Network Threats (7 days):** A bar chart showing the number of network threat detections for various computers.
- Malware Threats (7 days):** A table listing specific malware detections.

Detection Name	Count
W32.ZAccess.15nt	26
W32.Ramnit.A	14
ZBot:FakeAlert-tpd	13
Eldorado:Alureon-tpd	12
Win32.DemoMal.Rat.Client	12
- Network Threats (7 days):** A table listing remote IP addresses and their detection counts.

Remote IP	Count
75.102.25.76	2
82.165.37.127	2
205.234.252.212	2
178.19.25.92	1
- Recent Malware Threats:** A table showing the most recent malware detections.

Computer	Detection Name
Demo_TDSS	Eldorado:Alureon-tpd
Demo_TDSS	Alureon:Olmarik-tpd
Demo_TDSS	Eldorado:Alureon-tpd
Demo_TDSS	Eldorado:Alureon-tpd
- Recent Network Threats:** A table showing the most recent network threat detections.

Computer	Detection Name	Remote IP
Demo_Tinba	DFC.CustomIPList	82.165.37.127
Demo_Tinba	DFC.CustomIPList	82.165.37.127
Demo_Zbot	DFC.CustomIPList	178.19.25.92
Demo_StabunIQ	DFC.CustomIPList	75.102.25.76

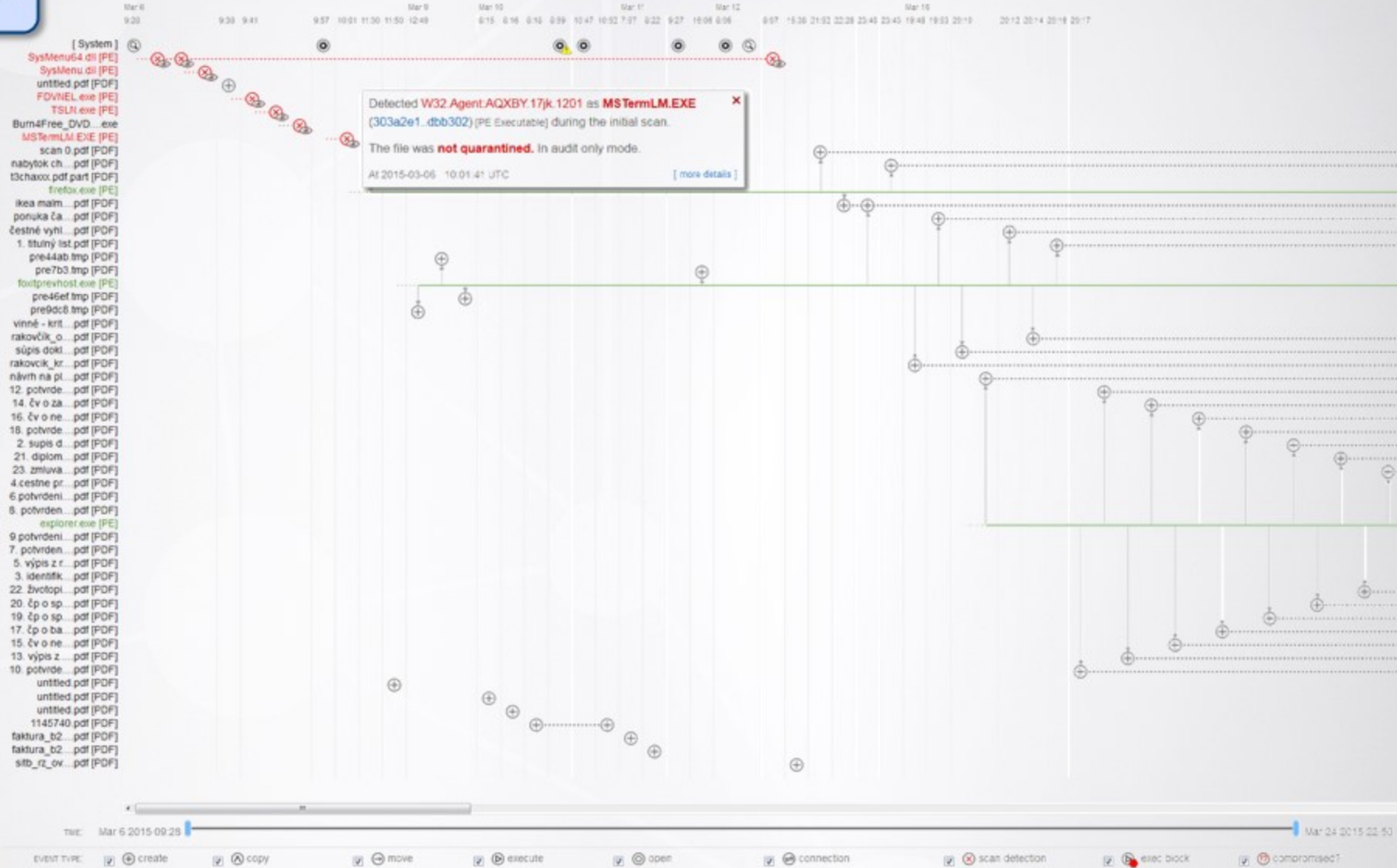
Behaviorálna analýza

Reputácia

Sandboxing

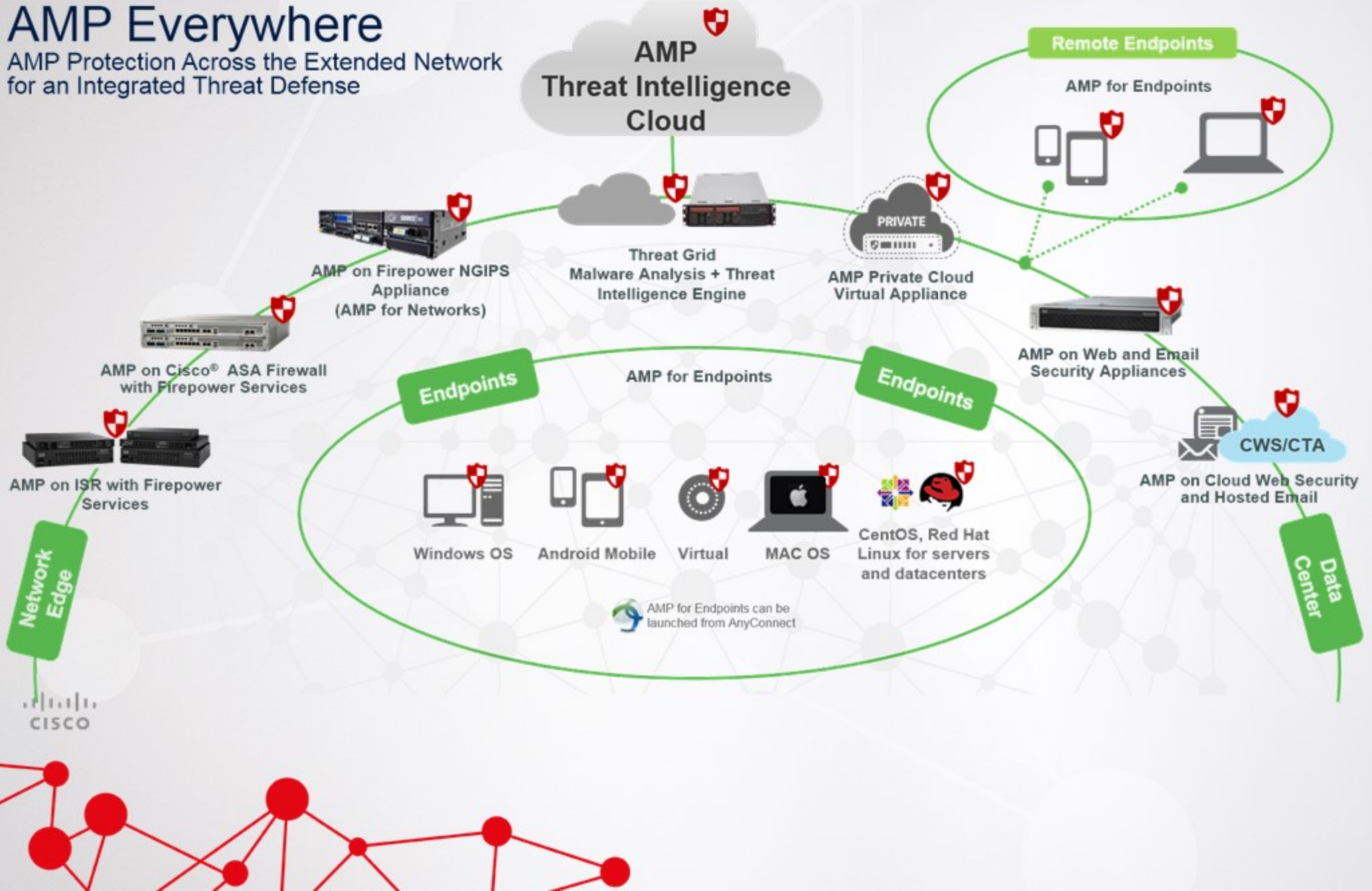
Anti-Exploit

Retrospektíva



AMP Everywhere

AMP Protection Across the Extended Network
for an Integrated Threat Defense



English ▾



AMP for Endpoints

Log In

[Use Single Sign-On](#) (beta)

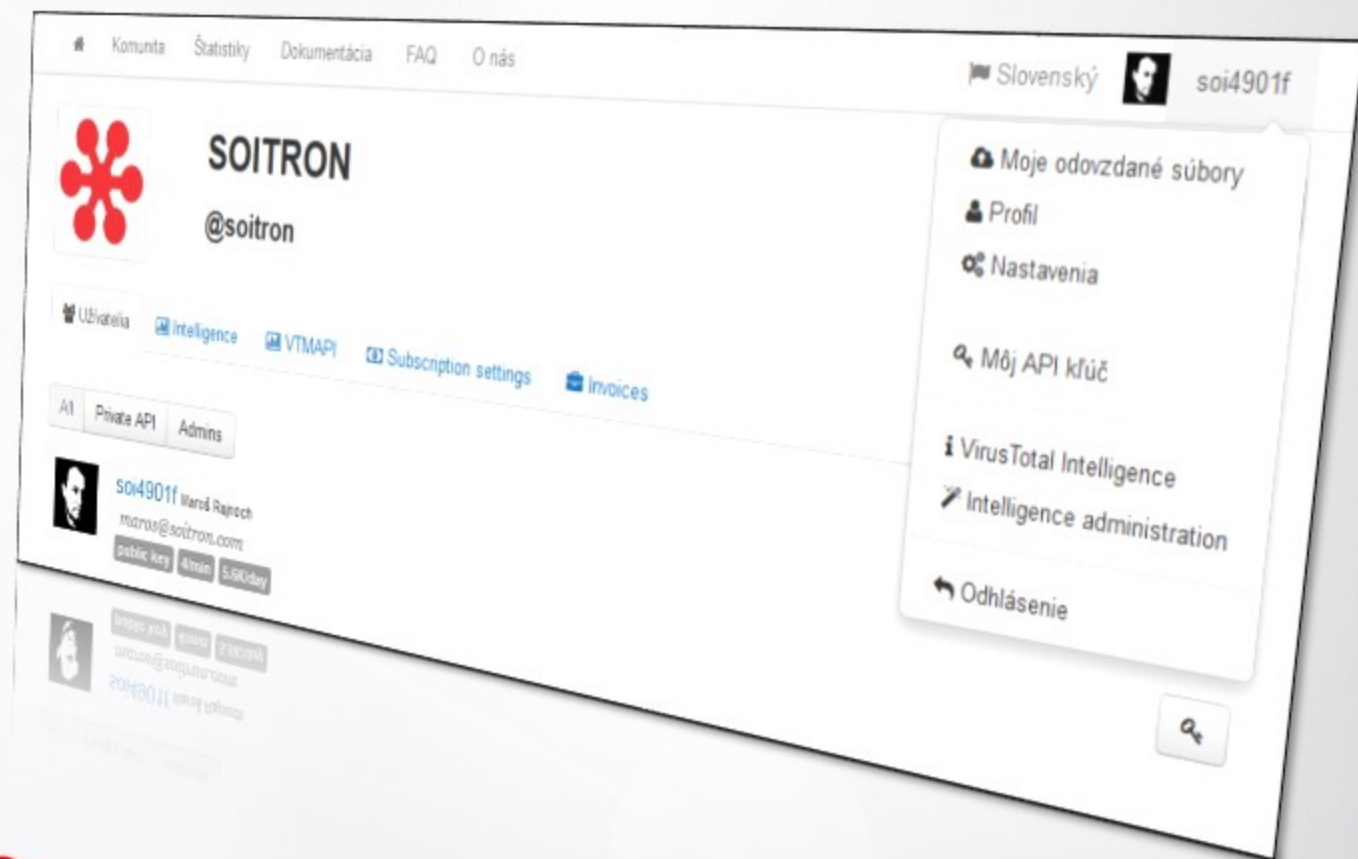
[Can't access your account?](#)



AVCaesar

<http://malwaredb.malekal.com/>

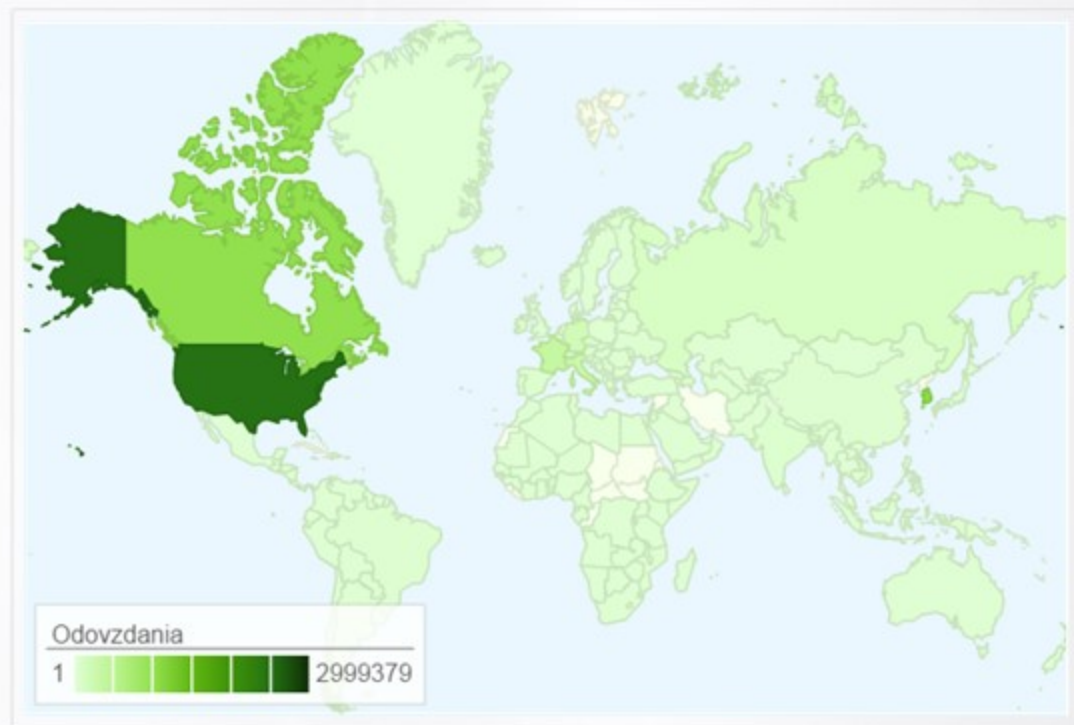
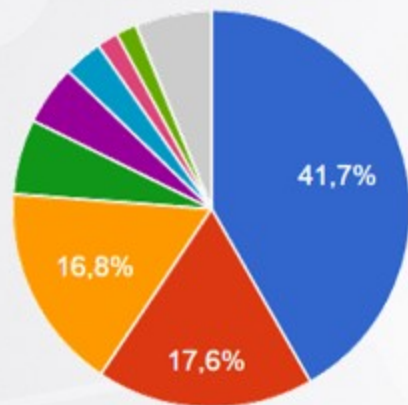
<https://github.com/krmawell/maltrieve>



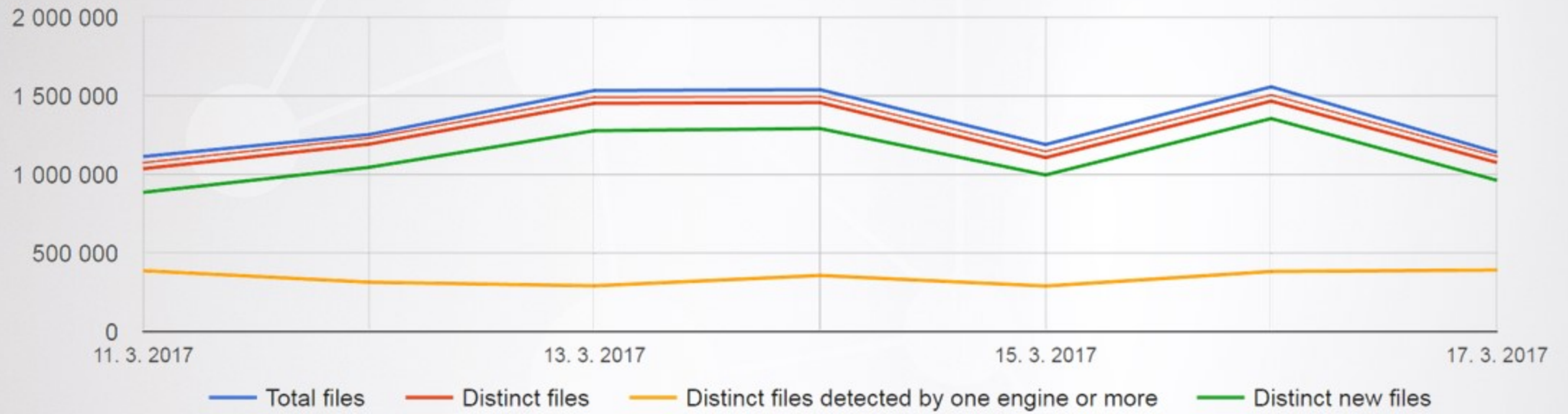
Štatistiky súboru počas posledných 7 dní

Odozvané súbory podľa krajín

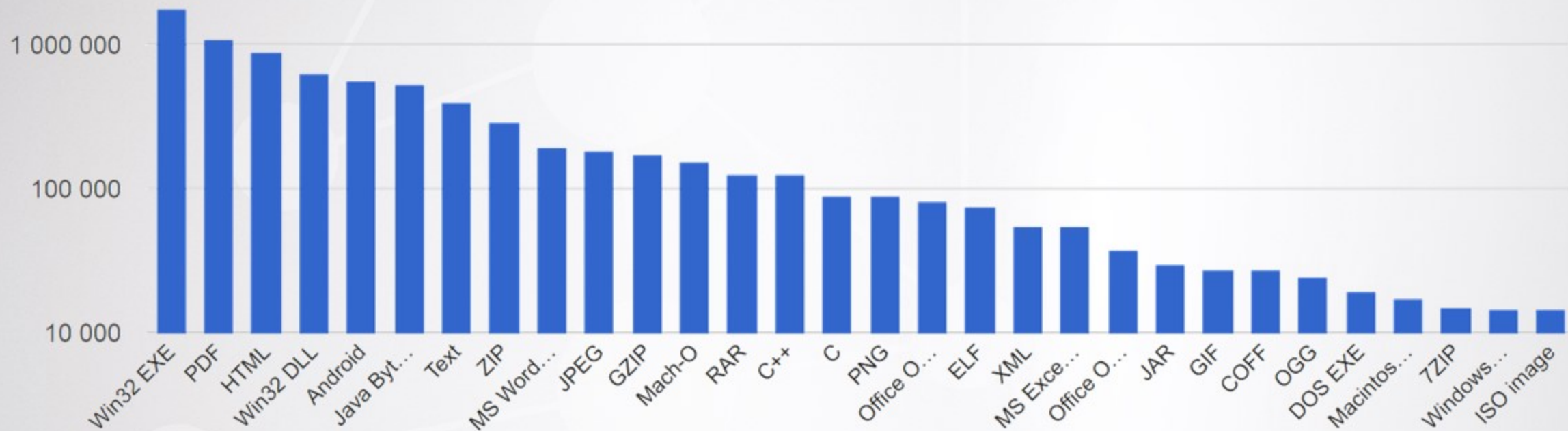
- United States of...
- Korea
- Canada
- France
- Italy
- Germany
- Russian Federation
- Czech Republic
- Iné



Odovzdana



Typy súborov



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 identify threats on your PC. These definitions are updated automatically, but you can also click on them to update them manually.

Status - Symantec Endpoint Protection

Status

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**

Scan for Threats
 Change Settings
 View Quarantine
 View Logs
 LiveUpdate...

Symantec

Cisco AMP for Endpoints

Scan Now
 History
 Settings

Status: Connected
 Scanned: 3/22/2017 10:37:07 AM
 Policy: Protect Policy

CISCO

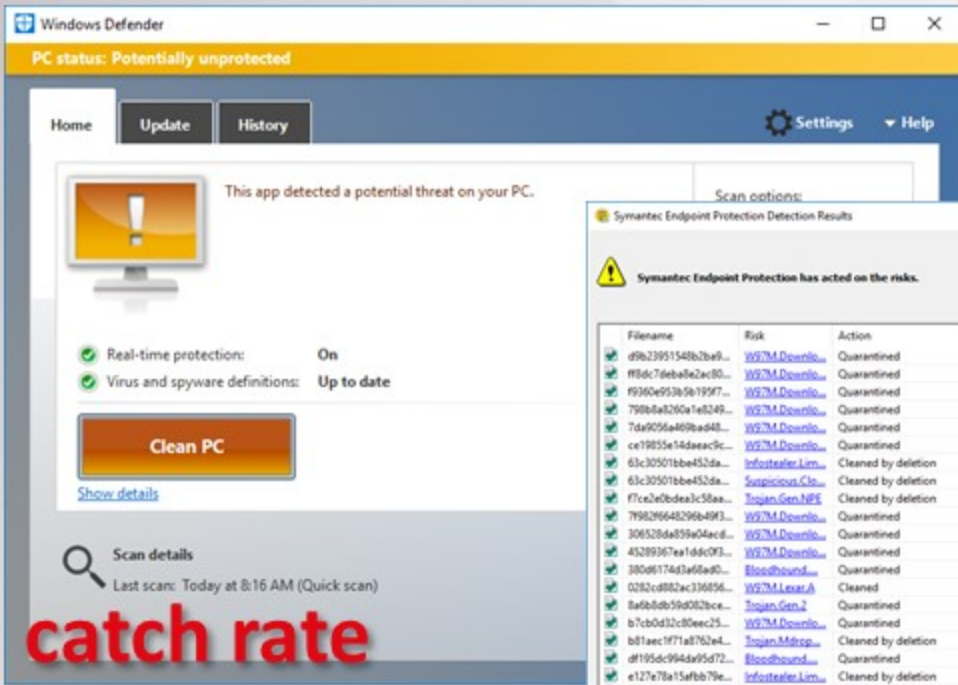
About





And the winner

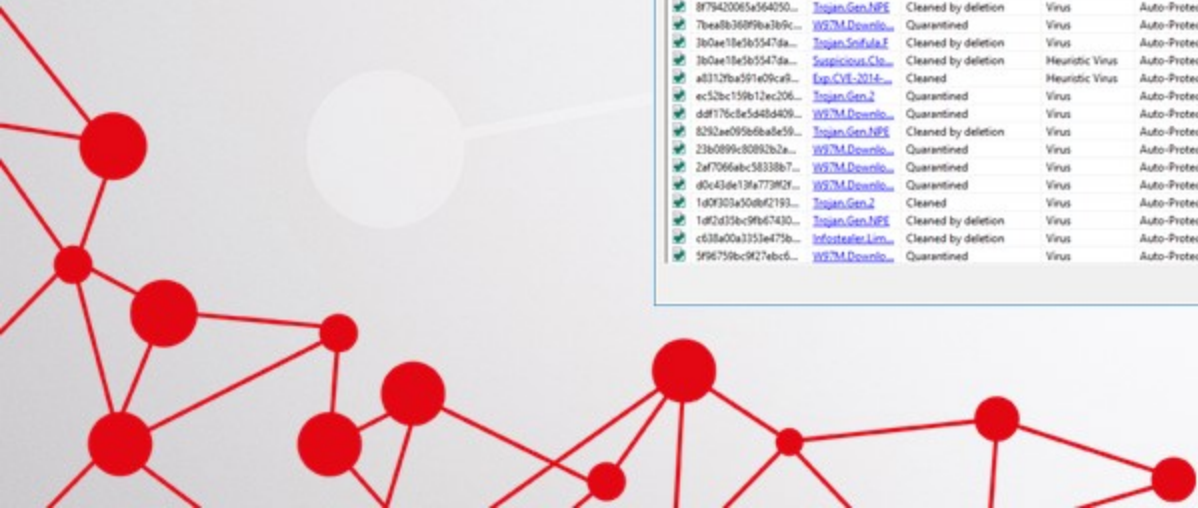
is...



catch rate
57%

Filename	Risk	Action	Risk Type	Logged By	Original Location	Computer	User	Status	Current Location	Primary Action	Secondar...	Action Description	Date and Time
d9623951548b2ba9...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:57:00 AM
f86c74eb4e2ac80...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:57:15 AM
f936c493b3e19597...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:57:28 AM
798ba226ca1e0249...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:57:43 AM
7da9056a499e4d8...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:57:59 AM
ca1985e14daac3c...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:58:26 AM
63c30501bbe452da...	InfoStealer.Lin...	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 11:57:28 AM
63c30501bbe452da...	Suspicious.Cl...	Cleaned by deletion	Heuristic Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 11:57:28 AM
f7ca2e0bde3c58aa...	W97M.Describ...	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 11:57:28 AM
798286482966493...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:58:38 AM
3065284859404ac...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:58:50 AM
45289367ea1d4a09...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:58:12 AM
38046174d3a66da...	Bloodhound...	Quarantined	Heuristic Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:59:11 AM
0282cd82ac336856...	W97M.Least A	Cleaned	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Cleaned	C:\Users\zochova\Desktop\infected...	Clean security risk	Quarantine	The file was repaired successfully.	3/22/2017 11:58:26 AM
8a6b8bb594022cc...	Injran.Gen.2	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:59:24 AM
b7c0d32c0dec25...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:59:37 AM
b81aac1f71a8762a...	Injran.Malvar...	Cleaned by deletion	Heuristic Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 11:58:50 AM
d195dc9944a95d72...	W97M.Describ...	Quarantined	Heuristic Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 11:59:47 AM
e127e78a15afbb79...	InfoStealer.Lin...	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 11:59:11 AM
e127e78a15afbb79...	W97M.Describ...	Cleaned by deletion	Heuristic Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 11:59:12 AM
d2c6045c5209955a...	Injran.Dropper	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 11:59:12 AM
5716374355384814b...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:00:09 PM
d9993304c279485...	Security.Risk.g...	Quarantined	Security Risk	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	SYSTEM	Infected	Quarantine	Quarantine	Leave al...	The file was quarantined success...	3/22/2017 11:58:59 AM
abf21bb789e3a677c...	Injran.Gen.2	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:00:19 PM
29049fed98e030c1...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:00:28 PM
424e06722a27a2ced...	Injran.Gen.NPE	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 11:59:47 AM
9788922a176c3e62...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:00:37 PM
1e7f455171543aed3...	W97M.Than.gen	Cleaned	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Cleaned	C:\Users\zochova\Desktop\infected...	Clean security risk	Quarantine	The file was repaired successfully.	3/22/2017 12:00:09 PM
79c3358b8a95651...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:00:55 PM
8f9420065a564050...	Injran.Gen.NPE	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 12:00:19 PM
7bea8e38999e3b9c...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:01:04 PM
380ae18e585547da...	Injran.SofJua.F	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 12:00:28 PM
380ae18e585547da...	Suspicious.Cl...	Cleaned by deletion	Heuristic Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 12:00:28 PM
a8112ba591e09ca9...	Exp.CVE-2014...	Cleaned	Heuristic Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Cleaned	C:\Users\zochova\Desktop\infected...	Clean security risk	Quarantine	The file was repaired successfully.	3/22/2017 12:00:29 PM
ec52bc159e12ec206...	Injran.Gen.2	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:01:14 PM
da8176c6e548b4d09...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:01:23 PM
8292ae095868a659...	Injran.Gen.NPE	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 12:00:55 PM
236089cc80892b2a...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:01:33 PM
2af7066abc58338b7...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:01:42 PM
d0c43d413fa77802...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:01:52 PM
1a9f03a050842193...	Injran.Gen.2	Cleaned	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Cleaned	C:\Users\zochova\Desktop\infected...	Clean security risk	Quarantine	The file was repaired successfully.	3/22/2017 12:01:23 PM
1a9f03a050842193...	Injran.Gen.NPE	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 12:01:24 PM
e638a00a3351e475b...	InfoStealer.Lin...	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Deleted	Deleted	Clean security risk	Quarantine	The file was deleted successfully.	3/22/2017 12:01:24 PM
596759c927abc6...	W97M.Describ...	Quarantined	Virus	Auto-Protect s...	C:\Users\zochova\Desktop\infec...	DESKTOP-48P...	zochova	Infected	Quarantine	Clean security risk	Quarantine	The file was quarantined success...	3/22/2017 12:02:01 PM

catch rate
70%



SHA256: d0c43de13fa773ff2f383777f5e4e76588fc5f704222f884e93915e56bacf8a

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	✓	Sophos ✓
Kingsoft	✓	SUPERAntiSpyware ✓
Malwarebytes	✓	TheHacker ✓
McAfee	✓	TotalDefense ✓
McAfee-GW-Edition	✓	TrendMicro ✓
Microsoft	✓	TrendMicro-HouseCall ✓
NANO-Antivirus	✓	Trustlook ⚡
nProtect	✓	VBA32 ✓
Panda	✓	VIPRE ✓
Sophos	✓	ViRobot ✓
SUPERAntiSpyware	✓	Webroot ✓
TheHacker	✓	WhiteArmor ✓
TotalDefense	✓	Yandex ✓
		Zillya ✓
		Zoner ✓

Cisco AMP

Warning!

Threat Quarantined

93ce15e3dc46a1ced370062b494a880526fce99627a0ef8c2
as W32.D982395154-95.SBX.TG.
:ccessful.

1 of 240

catch rate
96 %



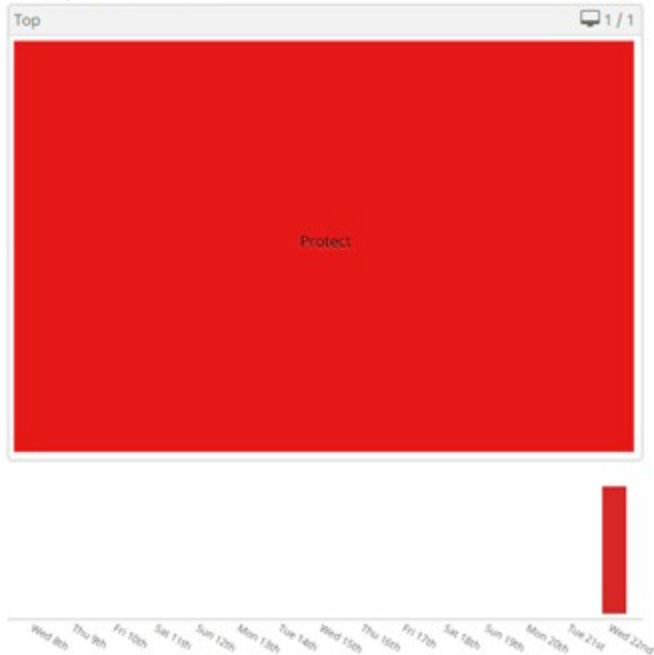
Dashboard

Dashboard | [Inbox](#) | [Overview](#) | [Events](#) | [Heat Map](#)

Time Period 14 days

100% compromised

Compromises



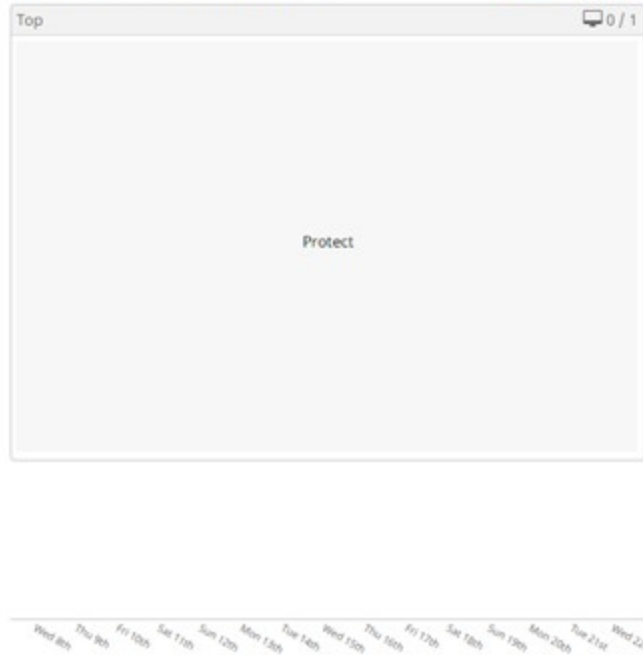
Significant Compromise Artifacts

SHA	1bd54bdc...c9500f0a	1
SHA	0aca34a7...130749ed	1
SHA	fa4b116f...77bf5383	1
SHA	ec52bc15...c6710763	1
SHA	dcccfee6...7b991689	1

Inbox Status

1 Requires Attention | 0 In Progress | 0 Resolved

Quarantined Detections



Compromise Event Types

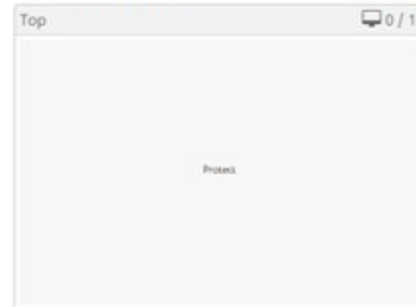
Threat Quarantined	1
Threat Detected	1
Quarantine Failure	1

Cognitive Threat Analytics

unresolved threats

0

Vulnerabilities



AMP Threat Grid Analysis

0 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

0 Files Scanned
0 Network Connections Logged

Connectors

1 Connectors
2 Installs
0 Install Failures

Quick Start

- Set Up Windows Connector
- Set Up Mac Connector
- Set Up Linux Connector

Dashboard

Dashboard [Inbox](#) [Overview](#) [Events](#) [Heat Map](#)

0 Cognitive Incidents [🔗](#)

Filter: (New) [🔗](#)

Select a Filter

Event Type

Group

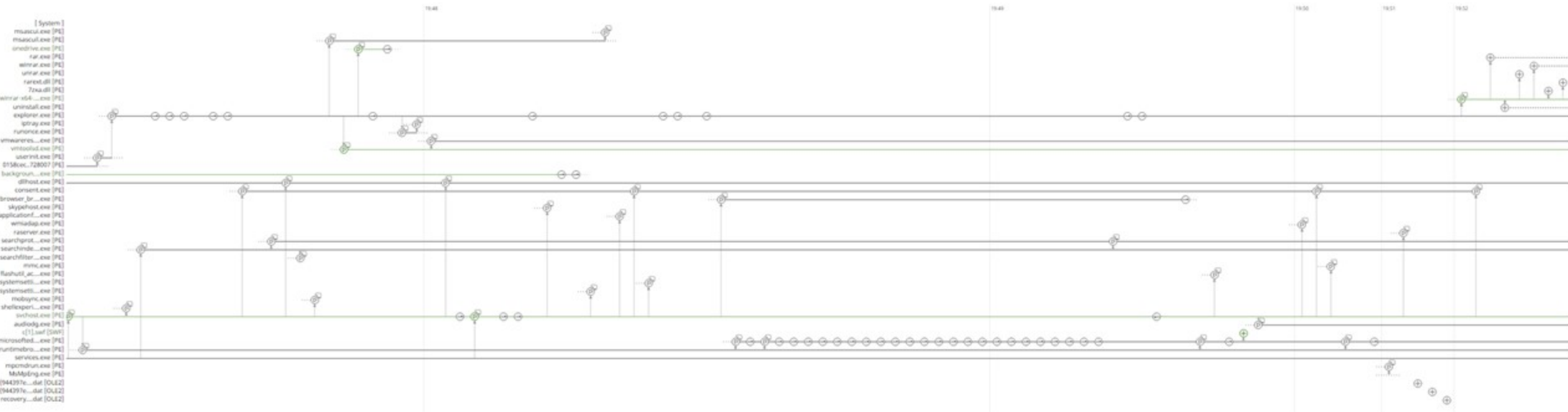
Filters Add filters by clicking on the **T** icon in the event details

Time Range

Sort

Not Subscribed

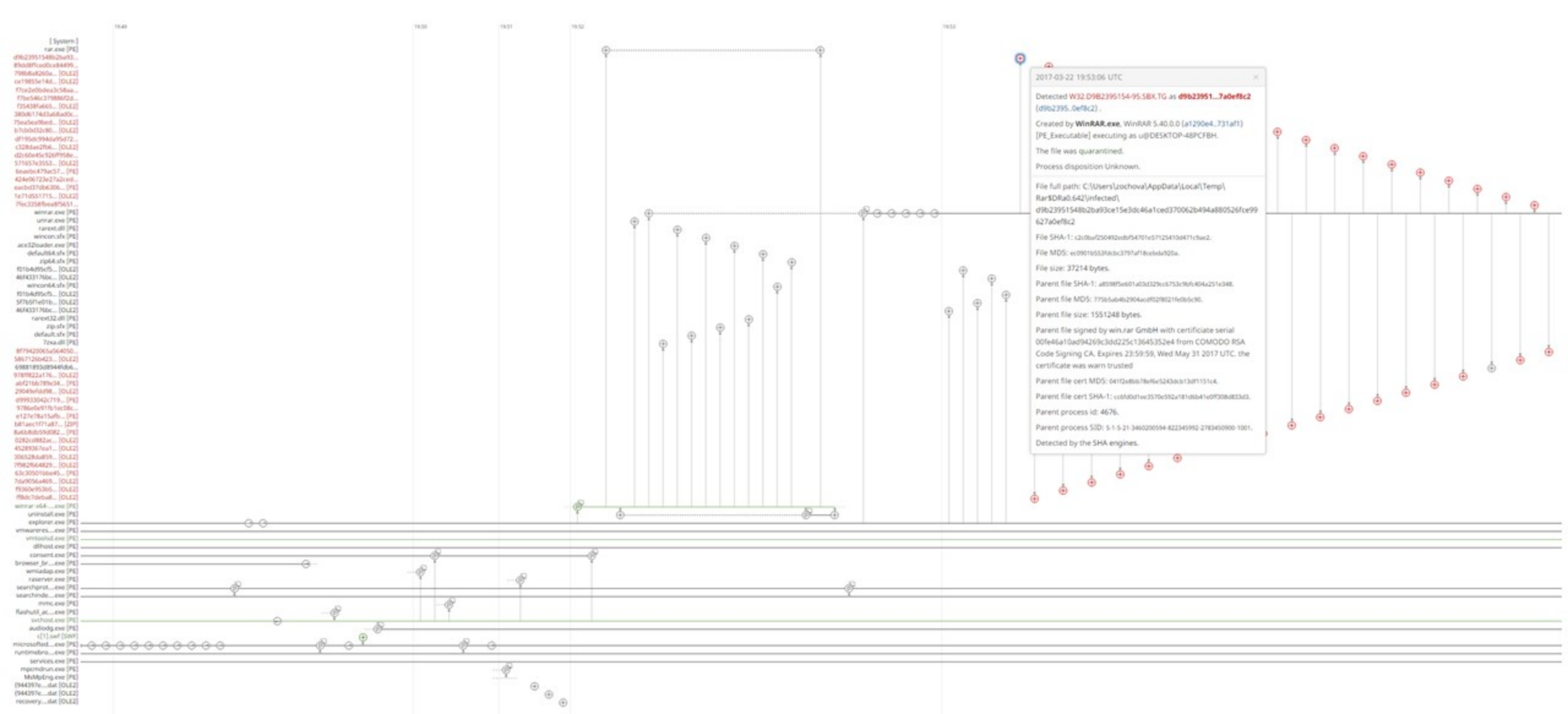
DESKTOP-48PCFBH detected c5d9c52583ef003728ba877bf217259e26a4435e9433b87dc82b77b695edd as W32.Gen:Trojan.20eu.1201	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 374eae096a5ed7ca07dfe0a8cda900b7cb19737b4720321f0f149c3d045e as DOC.26145D87E4.malicious.tht.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 3294896114b71457b418d385796a29b2024b74cbdc2549099e7b0773a0f0e53 as W32.3294896114-95.SBX.TG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 018a39e1884691106824a07285265ead67837e6f92d477c0e39bebee1abc23d as W32.3294896114-95.SBX.TG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected c5c67a2652edcc7c0c997e26f9a606b9d5623922deb59fe38f5236b5da906 as W32.Auto.c5c67a.MASH.SR.SBX.VIOC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 50c386d8ad900208670041d0591eae303aa80f15b1b4c74fe01987594f16158 as W32.Agent.Gen.20ep.1201	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected dc4bf16fb3aa8ca9630142934387e0c7f34528708baba65b7e0980c15f110 as W32.Auto:dc4bf1.in03.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected e64057b32cee22e5c34a71b6b86419e1bbd422f8216ced9ad023810afb3bdf0e as Auto.E64057_201562.in02	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 09771c70b7c1f625acf6f2f3f0923d668b12c7c4f324a7e6c70302919989333 as DOC.09771C70B7.malicious.tht.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 572953d2cbb83f747d924a159ff83980b1aaf8fce3455f2747d5082c9eedc1 as W32.572953D2CB-95.SBX.TG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 674e05351b475f1144b4d58acf24cd303fe3aa99961aaaa57b176053972df as W32.Auto:674e05.in03.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 4c87b2d48565ad8566c43ae421d69d1ab0795c8c79d4a3c5ef785e872e48492 as DOC.12B521826A.malicious.tht.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected ea0ef4de7c62ad794edf1c2d023e2bc3a926917a0bf21eea127cbf5fae8a0ca as DOC.EA0EF4DE7C.malicious.tht.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 445397b277985132d8327e594014c7e3ec2707242999d8e63bc210160360e15 as DOC.445397B277.ExecsPowerShell.hunt.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected ae3965065b6e4e1db3b92d52f7ca0335dc3f764ec275973e9853c03b4c6632fe as W32.AE3965065B-95.SBX.TG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected f81a3165bf232f3440fd36c85dfb8ac74a359b3a6aebc7451c8e00614e71c66 as W32.Auto:f81a31.in03.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 9a6ed973aff4dfbbaeeb6cc5520c15aaf31b884877cdf4d3a0b2d3f847a8a8 as W32.9A6ED973A-100.SBX.TG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 2d60ae951197c83a7807319a999d729e3d169550e129b8ad9782f79fa9e04 as XLS.2D60AE9511.ExecsPowerShell.hunt.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected 6bc48fe5e1f3efefc6e51c3f1cc988da3000552cbda271000f46019010833f9 as DOC.6BC48FE5E1.malicious.tht.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC
DESKTOP-48PCFBH detected d6f6e470483887e222e2192bb4a70c4c82a4dbb321c1e5e1cfc58912d3a244 as W32.Auto:d6f6e4.in03.Talos	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quarantine: Failed	2017-03-22 19:53:14 UTC



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

EVENT TYPE	<input checked="" type="checkbox"/> create	<input checked="" type="checkbox"/> copy	<input checked="" type="checkbox"/> move	<input checked="" type="checkbox"/> execute	<input checked="" type="checkbox"/> open	<input checked="" type="checkbox"/> connection	<input checked="" type="checkbox"/> scan detection	<input checked="" type="checkbox"/> exec block	<input checked="" type="checkbox"/> compromised?
	<input checked="" type="checkbox"/> restore	<input checked="" type="checkbox"/> reboot	<input checked="" type="checkbox"/> scan	<input checked="" type="checkbox"/> defs update	<input checked="" type="checkbox"/> policy update	<input checked="" type="checkbox"/> connector update	<input checked="" type="checkbox"/> scan schedule	<input checked="" type="checkbox"/> uninstall	
EVENT DISPOSITION	<input checked="" type="checkbox"/> benign	<input checked="" type="checkbox"/> malicious	<input checked="" type="checkbox"/> unknown	EVENT FLAGS			<input checked="" type="checkbox"/> warning	<input checked="" type="checkbox"/> audit only	<input checked="" type="checkbox"/> command line
FILE TYPE	<input checked="" type="checkbox"/> executable	<input checked="" type="checkbox"/> ms office (ole2)	<input checked="" type="checkbox"/> pdf	<input checked="" type="checkbox"/> ms cabinet	<input checked="" type="checkbox"/> flash	<input checked="" type="checkbox"/> zip archive	<input checked="" type="checkbox"/> other	<input checked="" type="checkbox"/> unknown	

Search Uncheck All Check All



2017-03-22 19:53:06 UTC

Detected W32.D9B2395154-95.5BX.TG as **d9b23951...7a0ef8c2** (d9b2395...0ef8c2).

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\lochova\AppData\Local\Temp\RarSDRa0.642\infected\d9b23951548b2ba93ce15e3dc46a1ced370062b494a880526fce99627a0ef8c2

File SHA-1: c20ba250492ed8f54701e57125410d471c9e2.

File MD5: ec9016553f8bc3791af18e6bd9320a.

File size: 37214 bytes.

Parent file SHA-1: a83885e01a03d329cc753c96f404a251c348.

Parent file MD5: 77965a4b2904aaf928021f6b5c90.

Parent file size: 1551248 bytes.

Parent file signed by win.rar GmbH with certificate 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: 0412d8bb78f8e5243ab313d7151c4.

Parent file cert SHA-1: c6fab3f6c3570e92a181d6b41e0f908d833d3.

Parent process id: 4676.

Parent process SID: S-1-5-21-346020094-82234992-278345090-1001.

Detected by the SHA engines.

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

EVENT TYPE	<input checked="" type="checkbox"/> create	<input checked="" type="checkbox"/> copy	<input checked="" type="checkbox"/> move	<input checked="" type="checkbox"/> execute	<input checked="" type="checkbox"/> open	<input checked="" type="checkbox"/> connection	<input checked="" type="checkbox"/> scan detection	<input checked="" type="checkbox"/> exec block	<input checked="" type="checkbox"/> compromised?
	<input checked="" type="checkbox"/> restore	<input checked="" type="checkbox"/> reboot	<input checked="" type="checkbox"/> scan	<input checked="" type="checkbox"/> defs update	<input checked="" type="checkbox"/> policy update	<input checked="" type="checkbox"/> connector update	<input checked="" type="checkbox"/> scan schedule	<input checked="" type="checkbox"/> uninstall	
EVENT DISPOSITION	<input checked="" type="checkbox"/> benign	<input checked="" type="checkbox"/> malicious	<input checked="" type="checkbox"/> unknown				<input checked="" type="checkbox"/> warning	<input checked="" type="checkbox"/> audit only	<input checked="" type="checkbox"/> command line
FILE TYPE	<input checked="" type="checkbox"/> executable	<input checked="" type="checkbox"/> ms office (ole2)	<input checked="" type="checkbox"/> pdf	<input checked="" type="checkbox"/> ms cabinet	<input checked="" type="checkbox"/> flash	<input checked="" type="checkbox"/> zip archive	<input checked="" type="checkbox"/> other	<input checked="" type="checkbox"/> unknown	

Search

System

- 01715a6c114861... [PE]
- 09623951548b2ba92... [PE]
- 89a88f1ed0ca84499... [PE]
- 798ba8260a... [OLE2]
- ce1995e14d... [OLE2]
- f7e2d0e6a3c58a... [OLE2]
- f7e2d0e6a3c58a... [OLE2]
- 05438f665... [OLE2]
- 380a1343a66a80c... [OLE2]
- 75a5ea9b6c... [OLE2]
- b71b043d89... [OLE2]
- af195a394a2a572... [OLE2]
- c328a6206... [OLE2]
- d215a45c526f996a... [OLE2]
- 371451c3553... [OLE2]
- 6e4ebc473a57... [PE]
- 424e06723c27a3e... [OLE2]
- ea-bd3784306... [PE]
- 7c71d551715... [OLE2]
- 75c3358f6ea89651... [OLE2]
- 7baeb3689... [OLE2]
- 44660b3740f260b... [OLE2]
- 16e118676ba... [OLE2]
- d8f178e9da... [OLE2]
- 239-0999408... [OLE2]
- 00434e13fa773f2f... [OLE2]
- 54c1aaa1e50... [OLE2]
- c338a0a3333e... [PE]
- 596759c92786c6d... [OLE2]
- e42c5a00928964c1... [OLE2]
- 77e49582755... [OLE2]
- 39811791566a6e40... [OLE2]
- 12294bd814944fb... [OLE2]
- 379615ac119... [OLE2]
- 19254092a6a6428... [OLE2]
- 20ca794e48... [OLE2]
- d3842ac106a0... [ZIP]
- 62c0776337899999c... [OLE2]
- 06ce8766ac... [OLE2]
- 750e9474ca917e4... [OLE2]
- 696e8f6a16... [OLE2]
- 2e4c090838f8e11... [OLE2]
- 54b1156a7d380083... [OLE2]
- 81d678458a... [OLE2]
- aba33ad80ba94e... [OLE2]
- d4f92314773972b... [OLE2]
- 90588ba743ca8051... [OLE2]
- 8c2a6f840c... [OLE2]
- 93079a3765736352... [OLE2]
- bee3c90b31f614f3... [OLE2]
- 9db3d78a4d33d7... [OLE2]
- winrar.exe [PE]
- 46433176ac... [OLE2]
- 87b0a95c... [OLE2]
- 5f76f1e01b... [OLE2]
- 75494a862599785e... [OLE2]
- 016624a007959e... [OLE2]
- 5b056c3a23... [OLE2]
- 1d75b020643b... [PE]
- bea79b0944... [OLE2]
- 61e42916c3985... [PE]
- 056248b968... [OLE2]
- 918505891762... [PE]
- 478963114bd... [PE]
- 3c017ba8f92... [OLE2]
- 846465f6d3731... [PE]
- 6676956669... [OLE2]
- 7ca41877e887486b3... [OLE2]
- 569964a0a067ed32... [OLE2]
- ab0d0c82bd... [OLE2]
- e03bc7b198a68... [PE]
- 3232eaf854... [OLE2]
- 58b9803ad299d771... [OLE2]
- f03d5714878a6e0... [PE]
- 04073256b7803... [PE]
- 874e209ea... [OLE2]
- 315879324483374a... [PE]
- 1bd46bc3e5a9... [PE]
- 100303a508f2... [PE]
- 1d24336c9b67439f... [OLE2]
- 2af7066abc3838b7... [OLE2]
- 8292ae09564ba6e9... [OLE2]
- ec52bc139b72e... [PE]
- a8312ba591... [OLE2]
- 310e15e5554... [PE]
- af79a79a3a3a3a3a

2017-03-22 19:53:07 UTC

Detected DOC.7BEA8B368F.ExecsPowerShell.hunt.Talos as **7bea8b36...2393c59d** (7bea8b36...2393c59d)[MS OLE2 CF].

Created by WinRAR.exe, WinRAR 5.40.0.0 (x1290e4_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\7bea8b368f9ba3b9ca8cf5e0636d148aae6317e8194ec72504340dd2393c59d

File SHA-1: 120eabdf1857575793b0783e6f78f9e845d.

File MD5: d6ca30ba1f65b3c317087b08934fc23.

File size: 128512 bytes.

Parent file SHA-1: a85985e601e03d326c5753b6f404a251e348.

Parent file MD5: 775e5ab4b2904ac0928021f066c90.

Parent file size: 1551248 bytes.

Parent file signed by win.rar GmbH with certificate 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: 04102abb78f6e5243ab13d01151c4.

Parent file cert.SHA-1: ccbf80d1ec3570e992a18186b41e0f080833d3.

Parent process id: 4676.

Parent process SID: S-1-5-21-346020594-822345992-278340900-1001.

Detected by the SHA engines.

Timeline view showing various system events and file operations. The timeline is represented by a series of vertical lines with circular markers at the top and bottom, indicating the duration of each event. The events are color-coded and labeled with their type and flags.

19h Mar 22, 2017, 20:43

Mar 22, 2017, 21:46

EVENT TYPE	<input checked="" type="checkbox"/> create	<input checked="" type="checkbox"/> copy	<input checked="" type="checkbox"/> move	<input checked="" type="checkbox"/> execute	<input checked="" type="checkbox"/> open	<input checked="" type="checkbox"/> connection	<input checked="" type="checkbox"/> scan detection	<input checked="" type="checkbox"/> exec block	<input checked="" type="checkbox"/> compromised?
	<input checked="" type="checkbox"/> restore	<input checked="" type="checkbox"/> reboot	<input checked="" type="checkbox"/> scan	<input checked="" type="checkbox"/> defs update	<input checked="" type="checkbox"/> policy update	<input checked="" type="checkbox"/> connector update	<input checked="" type="checkbox"/> scan schedule	<input checked="" type="checkbox"/> uninstall	
EVENT DISPOSITION	<input checked="" type="checkbox"/> benign	<input checked="" type="checkbox"/> malicious	<input checked="" type="checkbox"/> unknown				<input checked="" type="checkbox"/> warning	<input checked="" type="checkbox"/> audit only	<input checked="" type="checkbox"/> command-line
FILE TYPE	<input checked="" type="checkbox"/> executable	<input checked="" type="checkbox"/> ms office (ole2)	<input checked="" type="checkbox"/> pdf	<input checked="" type="checkbox"/> ms cabinet	<input checked="" type="checkbox"/> flash	<input checked="" type="checkbox"/> zip archive	<input checked="" type="checkbox"/> other	<input checked="" type="checkbox"/> 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_SFicar](#) • 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 7.6	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
--	---------------------	---	---------------------------	-------------------------	-------------------

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 <u>100</u> 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 <u>100</u> 1		2017-03-22 08:10:59 UTC
Tinba.exe was only executed on Demo_Tinba	Report <u>95</u> 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 <u>100</u> 1		2017-03-22 08:07:42 UTC
jwenjktgenwrger234231.exe was only executed on Demo_Dyre	Report <u>100</u> 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 <u>100</u> 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



Endpoint IOC - Installed Endpoint IOCs

[View All Changes](#)

Categories Groups Keywords

Search by description



Showing



Actions

<input type="checkbox"/> Zeus 6d2a1b03-b216-4cd8-9a9e-8827af6ebf93.ioc	Uploaded: 2017-03-22 16:35:42 UTC	Active	<input type="button" value="View"/> <input type="button" value="Edit"/> <input type="button" value=""/>	<input type="button" value="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-b216-4cd8-1-1">
  <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="fe11706-9ebe-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>
      </Indicator operator="OR" id="67505775-6577-43b2-bccd-74603223180a">
    </Indicator operator="AND" id="0781258f-6960-4da5-97a0-ec35fb403cac">
  </Indicator operator="OR" id="9c8df971-32a8-4ede-8a3a-c5cb2c1439c6">

```

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

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_

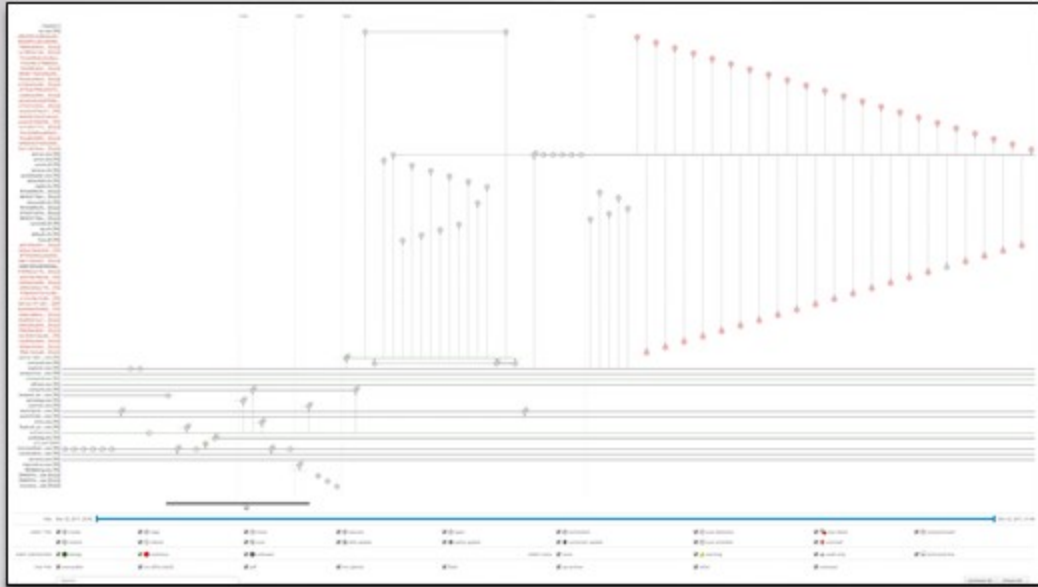
Loaded IOCs: 1

Save



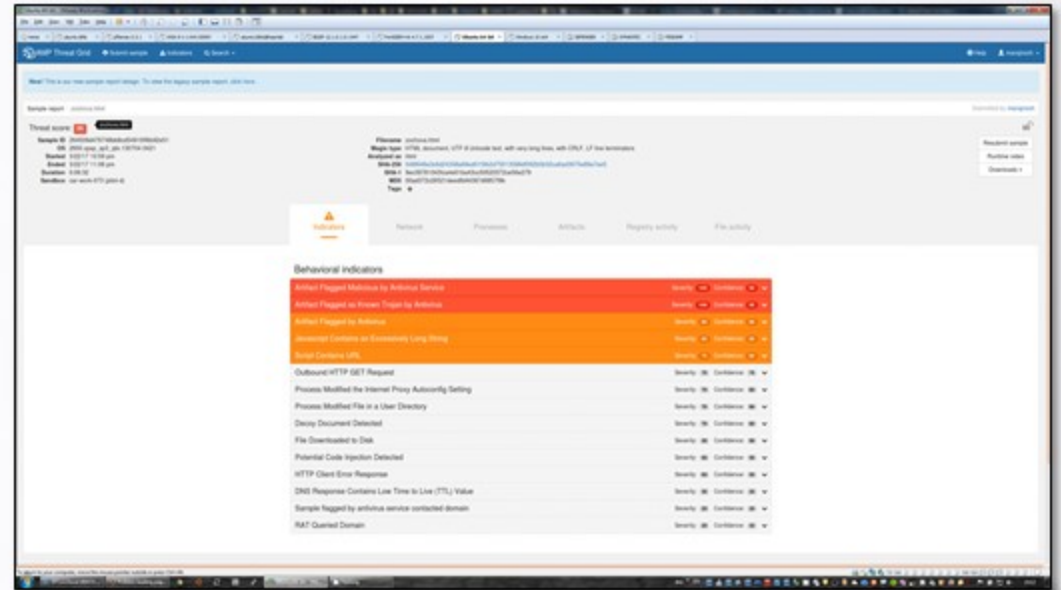
SOITRON*
INSPIRUJEME K NÁROČNOSTI

Cisco FireAMP trajectory



https://youtu.be/F_b25WJ8Q7U

Cisco Threatgrid sandboxing



<https://youtu.be/wctsekRoUJY>