RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO1-T09

Disrupting Adversarial Success— Giving the Bad Guys No Sleep

Christiaan Beek

ATR Lead – Office of the CTO
Intel Security

Raj Samani

VP, CTO for EMEA
Intel Security

#RSAC

Agenda

- Introduction
- When the power shuts down….
- Using botnets for insider trading
- Giving the bad guys no sleep
- What’s next?

Christiaan Beek

Director Strategic Intelligence & Operations
Intel Security – Office of the CTO

Raj Samani

CTO for Europe, Middle East, and Africa
Intel Security

When the power shuts down

- Ukrainian Power Grid attack

When the power shuts down….

- **Dec 23, 2015**: Two Ukrainian power-companies, Prykarpattyaoblenergo and Kyivoblenergo were hit by a coordinated cyber-attack.

- As a result of this attack, eight provinces of the Ivan-Frakivk region were impacted, resulting in a power-outage for approximately **six hours** affecting **over 80,000 customers**.

- The affected company reported to be operating in "manual' mode, an indicator that their network was impacted.

- At the same time a DDoS attack was launched against assets of the energy company.

Stage 1 of the attack: Flow of events

Cbeek-2016

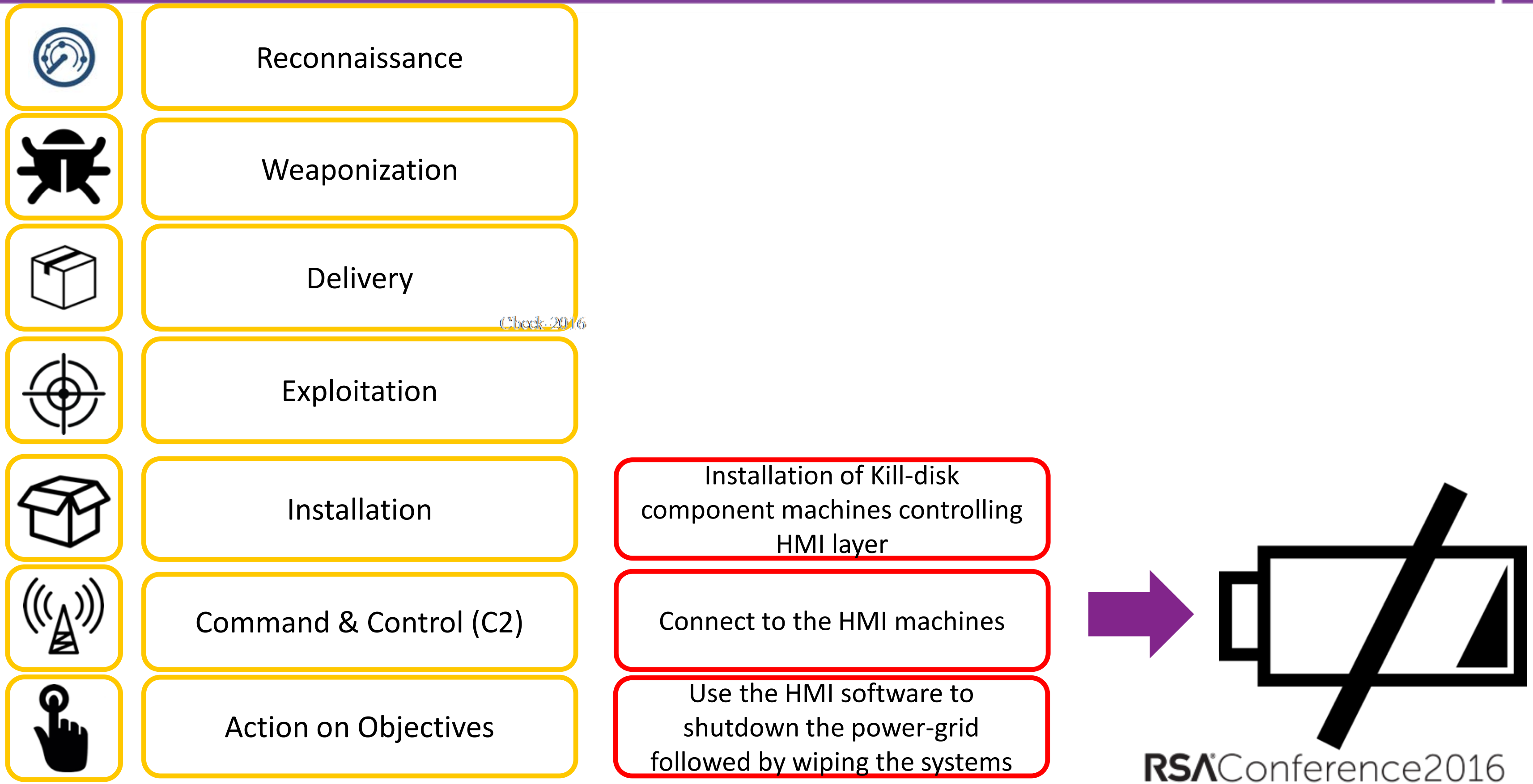
Reconnaissance	
Weaponization	Excel/Word exploits – hidden dropper in Macro
Delivery	Spear-phishing email in Ukrainian language with weaponized attachment
Exploitation	Execution of macro
Installation	Installation of dropper
Command & Control (C2)	Connect to C2 and download stage 2 malware
Action on Objectives	Gather intel of landing point in the target's network

Stage 2 of the attack: Establish control

Cbeek-2016

Reconnaissance	
Weaponization	
Delivery	Using backdoor created by malware to upload tooling
Exploitation	
Installation	Installation of SSH backdoor or Shells
Command & Control (C2)	Connect to Attacker(s)
Action on Objectives	Lateral movement to find machines controlling the HMI layer

Stage 3 of the attack: Execution time



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control (C2)

Action on Objectives

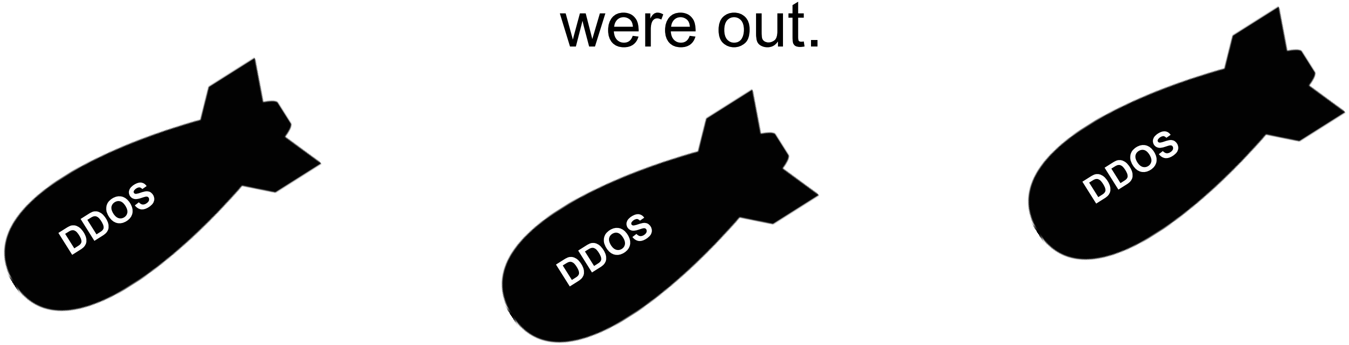
Installation of Kill-disk component machines controlling HMI layer

Connect to the HMI machines

Use the HMI software to shutdown the power-grid followed by wiping the systems

At the same time…

- While the attackers were shutting down the services, a coordinated DDoS attack was launched against the phone systems so that operators didn't know that remote sites were out.



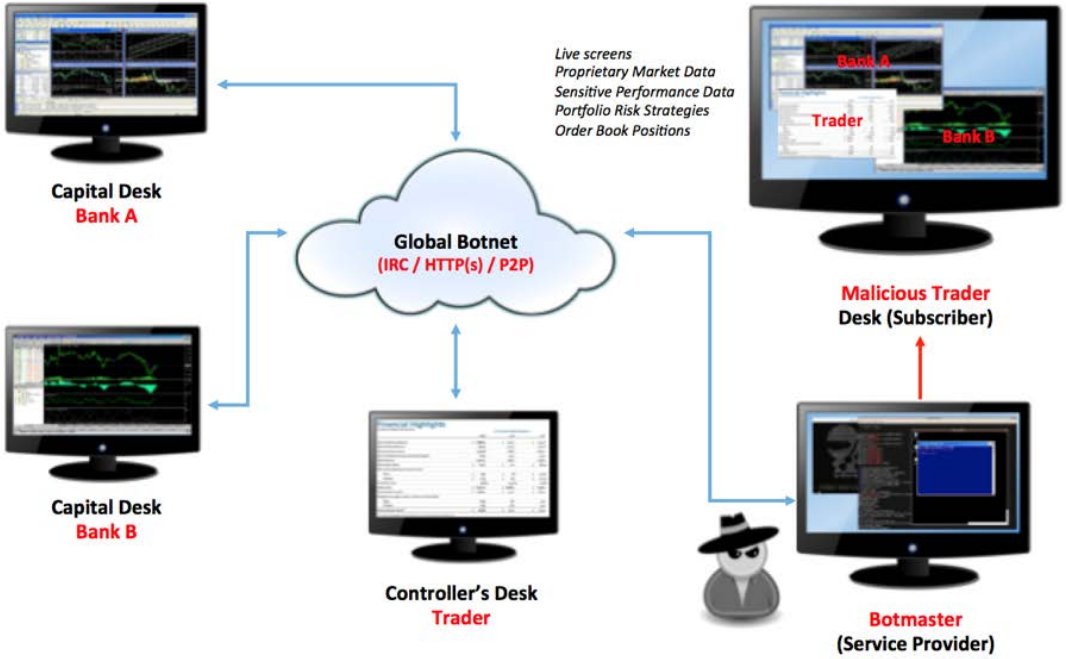
- To be continued……

Using botnets for insider trading

Botnets

- Traditionally: Remote control, Denial of Service, Pii theft
- Today a managed service with:
- Anonymous communications
- Access management to subscribed networks/systems
- Help desk Services
- Payment Services

Botnets used for insider trading



- https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet/
- https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet-part-2/

Giving the bad guys no sleep

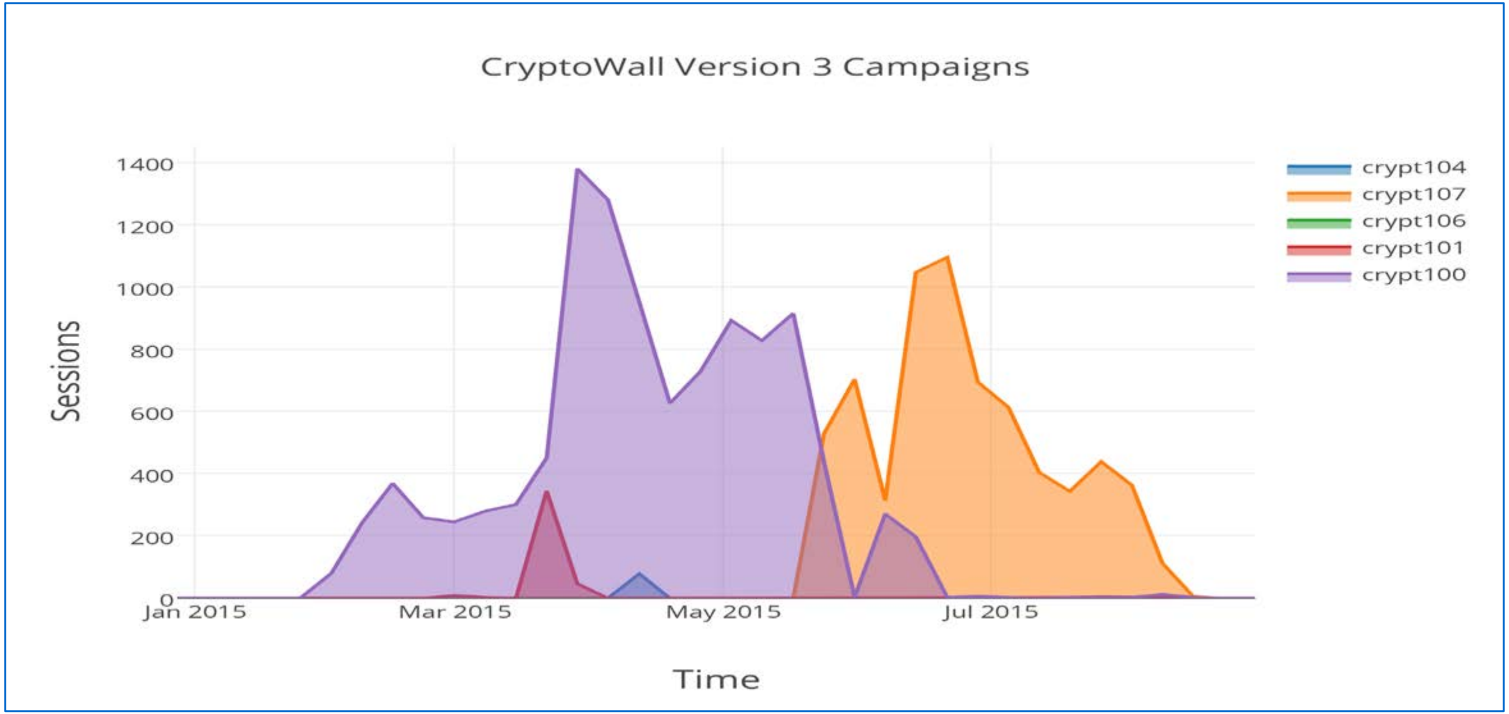
Where to Hit Them?

- The six Ds of Cyber Defense
  - Delay
  - Degrade
  - Disrupt
  - Deny
  - Destroy
  - Defeat

Examples of recent Operations

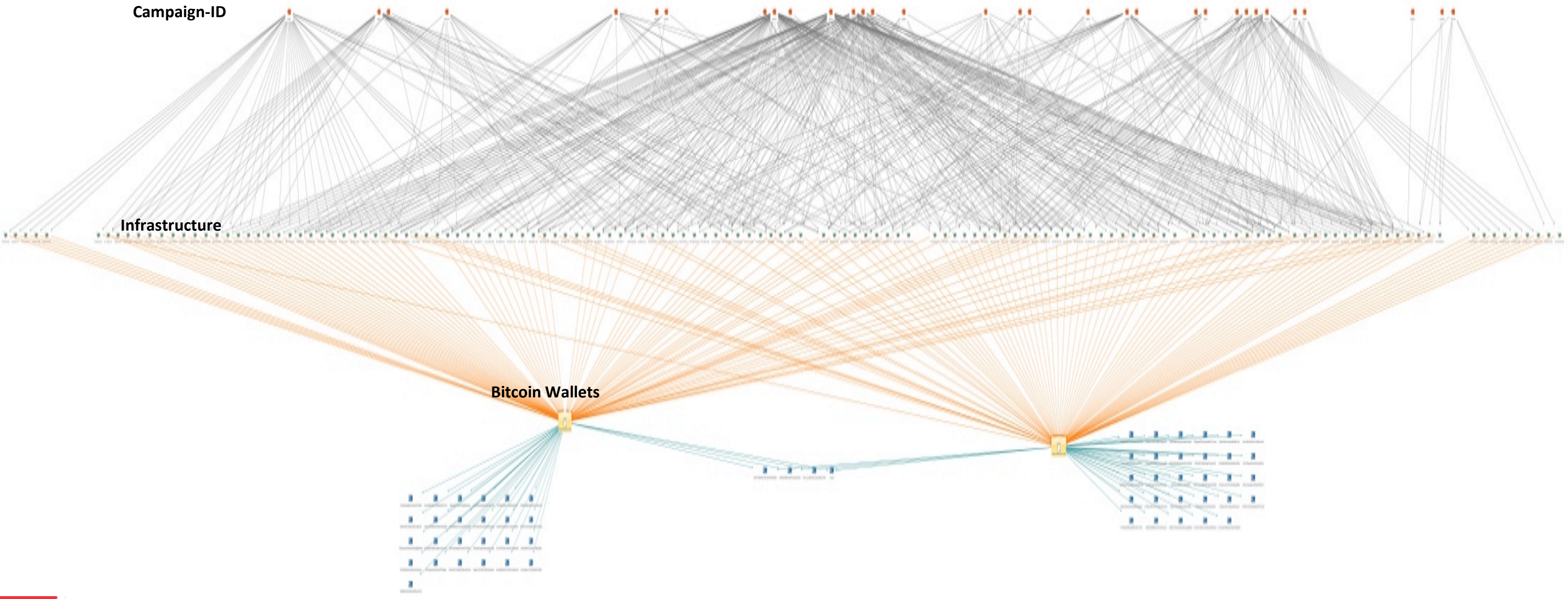
- CryptoWall v3.0
- Beebone

#CryptoWall 3.0

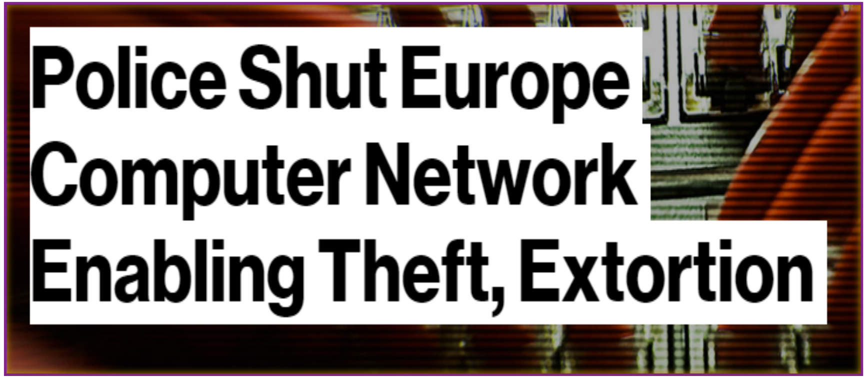


Source: CTA Report CryptoWall 3 operation

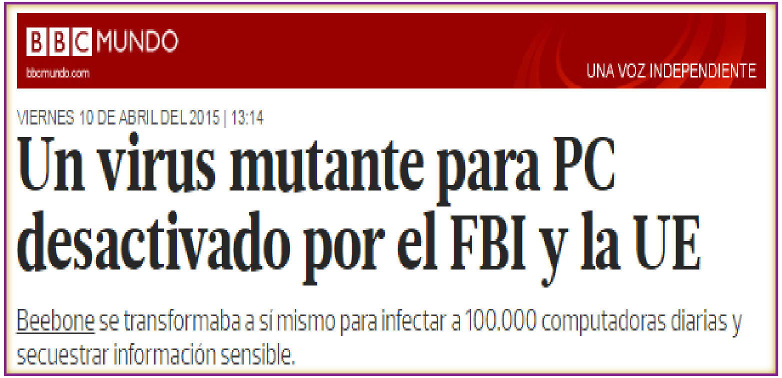
#CryptoWall 3.0



#OpBeebone



Police Shut Europe Computer Network Enabling Theft, Extortion



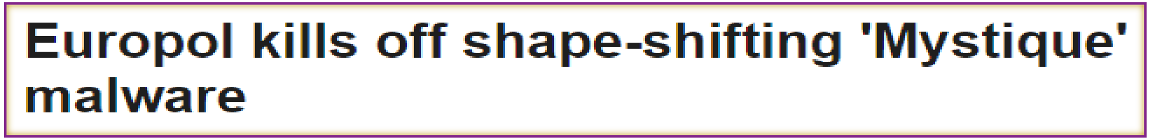
BBC MUNDO
bbcmundo.com
UNA VOZ INDEPENDIENTE

VIERNES 10 DE ABRIL DEL 2015 | 13:14

Un virus mutante para PC desactivado por el FBI y la UE

Beebone se transformaba a sí mismo para infectar a 100.000 computadoras diarias y secuestrar información sensible.

US And European Cyber Squads Take Down International Beebone Botnet



Europol kills off shape-shifting 'Mystique' malware

Evasion Capabilities

W32/Worm-AAEH behaviors:

Executes
at system startup.

Copies
itself on all removable drives.

Disables
Windows Task Manager's ability to terminate applications.

Detects and evades
virtual machines and antivirus software.

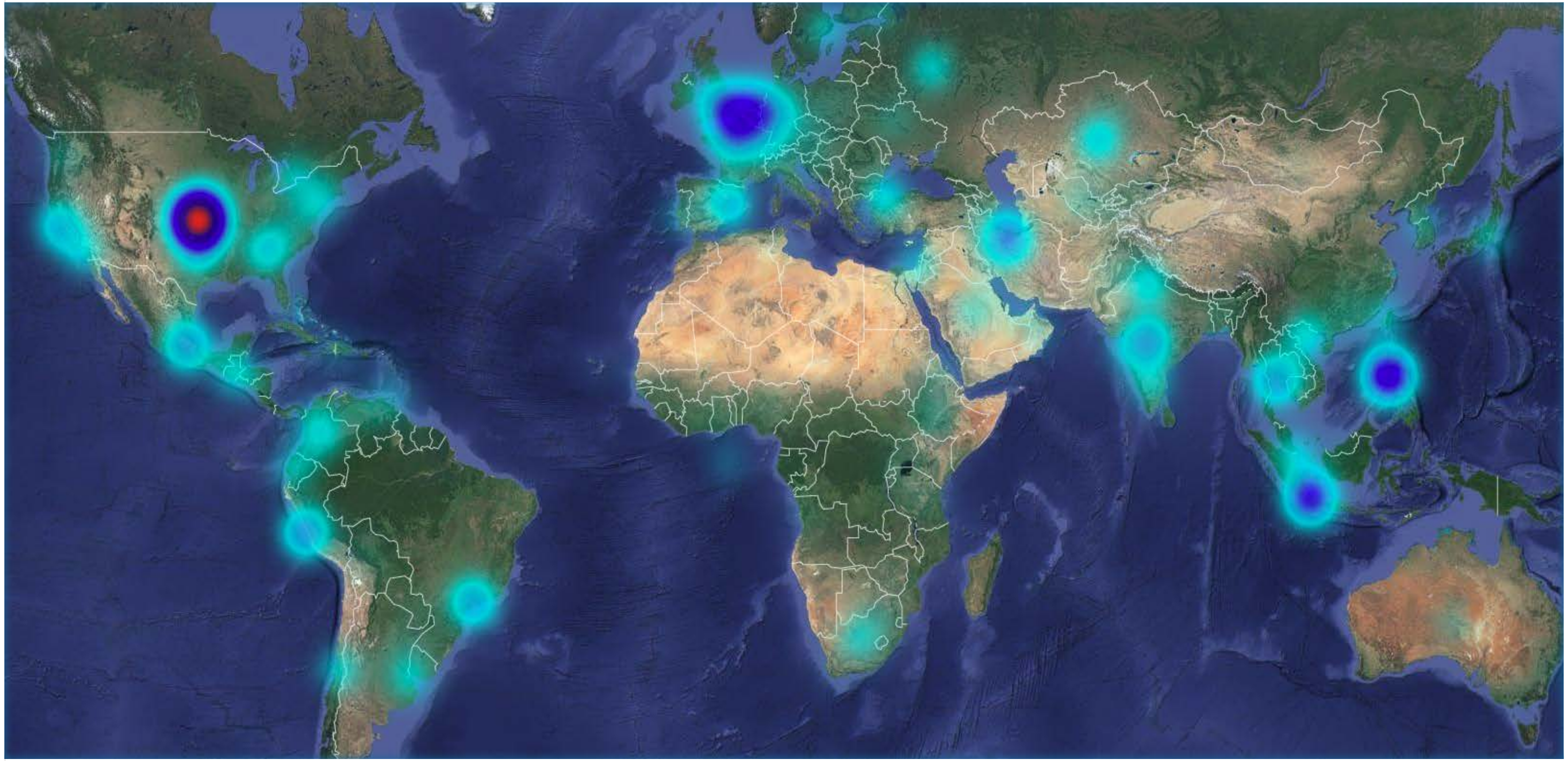
Injects malware
- Password stealers
- Ransomware
- Rootkits
- And more

What Does This Mean?

The McAfee Labs zoo contains more than five million unique W32/Worm-AAEH samples. It infected over 23,000 systems in 2014.

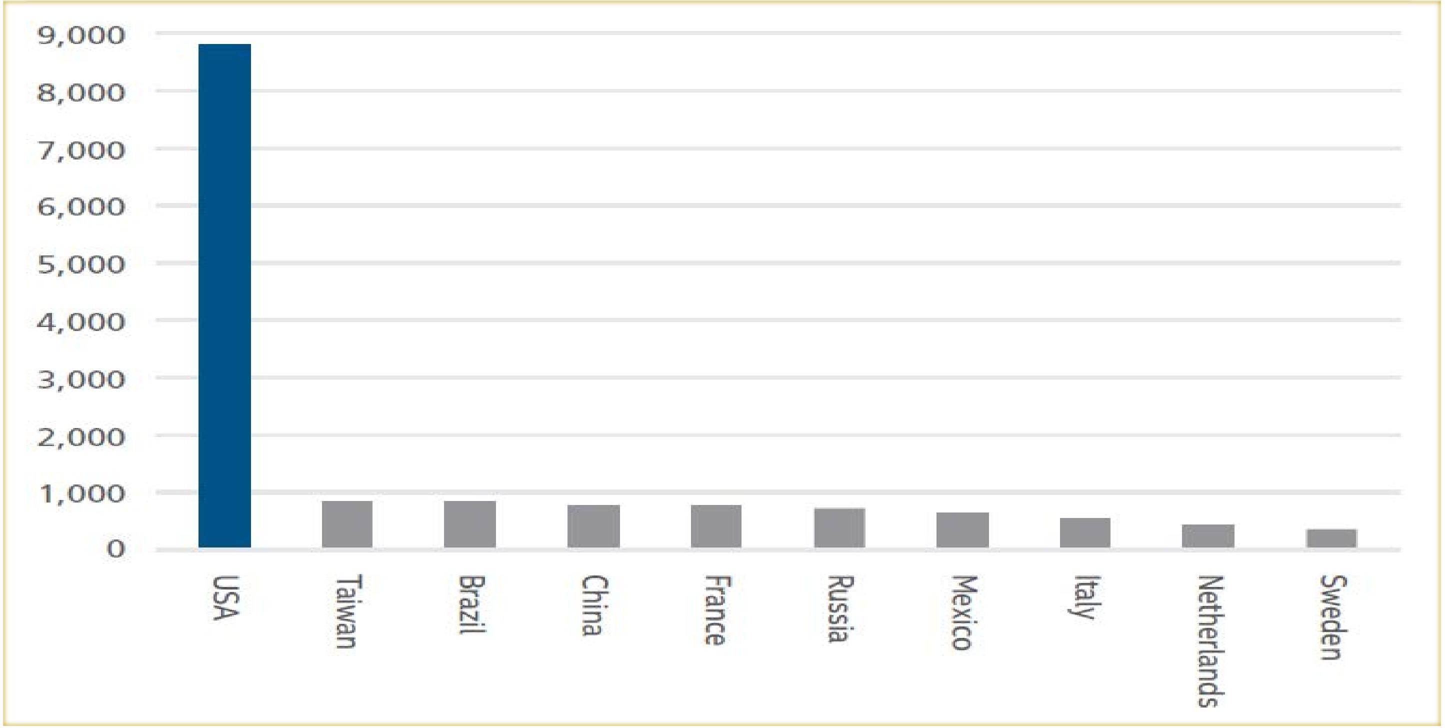
In April 2015, a global law enforcement action took down the control servers for this botnet.

What Does This Mean?



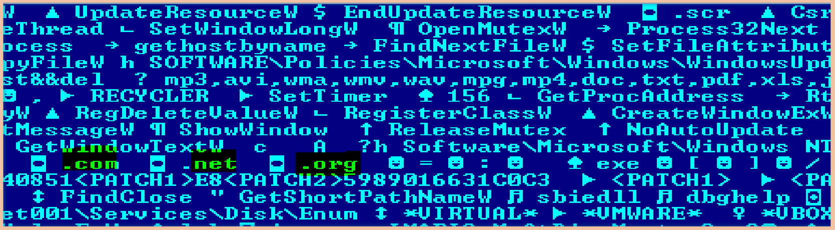
Telemetry Analysis

Total systems infected by W32/Worm-AAEH in 2013-2014

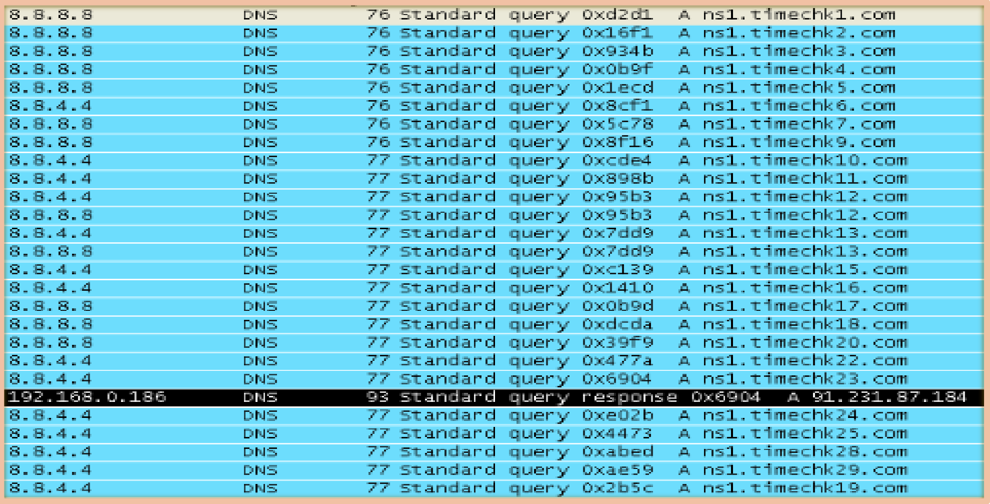


Cracking the Code

First DGA: 6 TopLevelDomains

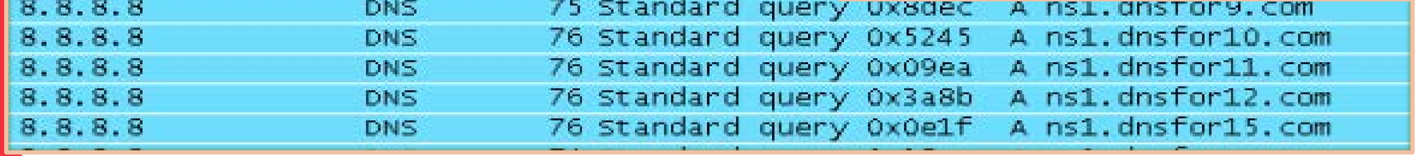


```
W  ▲ UpdateResourceW $ EndUpdateResourceW  ◘ .scr  ▲ Csr
eThread ∟ SetWindowLongW  ¶ OpenMutexW  → Process32Next
ocess  → gethostbyname → FindNextFileW $ SetFileAttribut
pyFileW h SOFTWARE\Policies\Microsoft\Windows\WindowsUpd
st&&del  ? mp3,avi,wma,wmv,wav,mpg,mp4,doc,txt,pdf,xls,j
☻ , ► RECYCLER  ► SetTimer  ♠ 156 ∟ GetProcAddress  → Rt
yW ▲ RegDeleteValueW ∟ RegisterClassW  ▲ CreateWindowExW
tMessageW ¶ ShowWindow  ↑ ReleaseMutex  ↑ NoAutoUpdate
 GetWindowTextW  c   A  ?h Software\Microsoft\Windows NT
  ◘ .com  ◘ .net  ◘ .org  ☻ = ☻ : ☻   ♠ exe ☻ [ ☻ ] ☻ /
40851<PATCH1>E8<PATCH2>5989016631C0C3  ► <PATCH1>  ► <PA
 ↕ FindClose " GetShortPathNameW ♫ sbiedll ♫ dbghelp ⊡
et001\Services\Disk\Enum ↕ *VIRTUAL* ► *VMWARE*  ♀ *VBOX
```



```
8.8.8.8          DNS   76 Standard query 0xd2d1   A ns1.timechk1.com
8.8.8.8          DNS   76 Standard query 0x16f1   A ns1.timechk2.com
8.8.8.8          DNS   76 Standard query 0x934b   A ns1.timechk3.com
8.8.8.8          DNS   76 Standard query 0x0b9f   A ns1.timechk4.com
8.8.8.8          DNS   76 Standard query 0x1ecd   A ns1.timechk5.com
8.8.4.4          DNS   76 Standard query 0x8cf1   A ns1.timechk6.com
8.8.8.8          DNS   76 Standard query 0x5c78   A ns1.timechk7.com
8.8.8.8          DNS   76 Standard query 0x8f16   A ns1.timechk9.com
8.8.4.4          DNS   77 Standard query 0xcde4   A ns1.timechk10.com
8.8.4.4          DNS   77 Standard query 0x898b   A ns1.timechk11.com
8.8.4.4          DNS   77 Standard query 0x95b3   A ns1.timechk12.com
8.8.8.8          DNS   77 Standard query 0x95b3   A ns1.timechk12.com
8.8.4.4          DNS   77 Standard query 0x7dd9   A ns1.timechk13.com
8.8.8.8          DNS   77 Standard query 0x7dd9   A ns1.timechk13.com
8.8.4.4          DNS   77 Standard query 0xc139   A ns1.timechk15.com
8.8.4.4          DNS   77 Standard query 0x1410   A ns1.timechk16.com
8.8.8.8          DNS   77 Standard query 0x0b9d   A ns1.timechk17.com
8.8.8.8          DNS   77 Standard query 0xdcda   A ns1.timechk18.com
8.8.8.8          DNS   77 Standard query 0x39f9   A ns1.timechk20.com
8.8.4.4          DNS   77 Standard query 0x477a   A ns1.timechk22.com
8.8.4.4          DNS   77 Standard query 0x6904   A ns1.timechk23.com
192.168.0.186    DNS   93 Standard query response 0x6904  A 91.231.87.184
8.8.4.4          DNS   77 Standard query 0xe02b   A ns1.timechk24.com
8.8.4.4          DNS   77 Standard query 0x4473   A ns1.timechk25.com
8.8.4.4          DNS   77 Standard query 0xabed   A ns1.timechk28.com
8.8.4.4          DNS   77 Standard query 0xae59   A ns1.timechk29.com
8.8.4.4          DNS   77 Standard query 0x2b5c   A ns1.timechk19.com
```

Then to 3 TLDs



```
Destination      Protocol  Length  Info
8.8.8.8          DNS       74 Standard query
8.8.8.8          DNS       75 Standard query
8.8.8.8          DNS       75 Standard query 0x8dec  A ns1.dnsfor9.com
8.8.8.8          DNS       76 Standard query 0x5245  A ns1.dnsfor10.com
8.8.8.8          DNS       76 Standard query 0x09ea  A ns1.dnsfor11.com
8.8.8.8          DNS       76 Standard query 0x3a8b  A ns1.dnsfor12.com
8.8.8.8          DNS       76 Standard query 0x0e1f  A ns1.dnsfor15.com
```

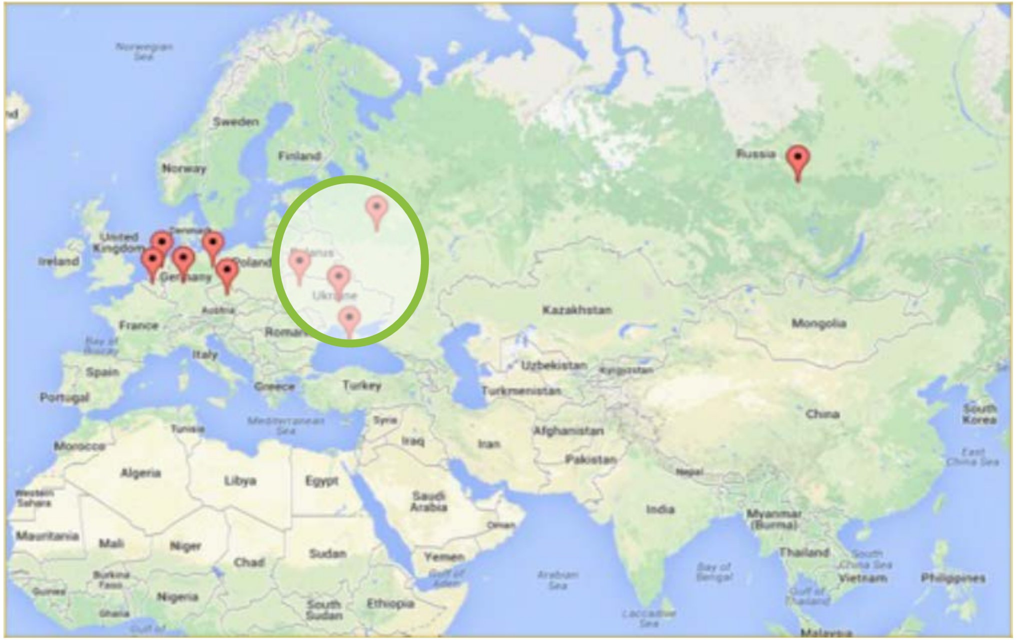
The Plan

DGA Elements	Previous DGA (dnsfor)	Older DGAs	Current DGA (timecheck)
Number Suffix Start range	0 (numbers optional) dnsfor.net is acceptable domain in DGA	Numbers optional	1 (must have number in domain)
Number Suffix End Range	Sample-dependent. does not exceed 29. Most samples 15.	None/99	29
TLDs	net/com/org	net/com/org/info/biz	com/net/org bug in code prevents checking net/org Samples may exist that check all 3
Active Period	2013-Sep 2014	2009-2013	Oct 2014-present

Identify the Command and Control Servers

- Sinkholing operation

- All of the worm's control servers detected by McAfee Labs between March 14, 2014, and September 14, 2014, were based in Europe



Source: McAfee Labs

Sinkhole

A botnet sinkhole is a target machine used by researchers to gather information about a particular botnet.

Sinkholing is the redirection of traffic from its original destination to one specified by the sinkhole owners.

The altered destination is known as the sinkhole. The name is a reference to a physical sinkhole, into which items apparently disappear.

Sinkhole

Regular Expression for DGA prior to September 22 2014:

^ns1.dnsfor[0-9]{1,2}\.(com|org|net)$

Numbers after “ns1.dnsfor” range from 1 to 30

Examples:
ns1.dnsfor9.com
ns1.dnsfor27.net
ns1.dnsfor1.org

The last known IP for this DGA is 188.127.249.119 at ns1.dnsfor9.com

Regular Expression for DGA after September 22 2014:

^ns1.timechk[0-9]{1,2}\.(com|org|net)$

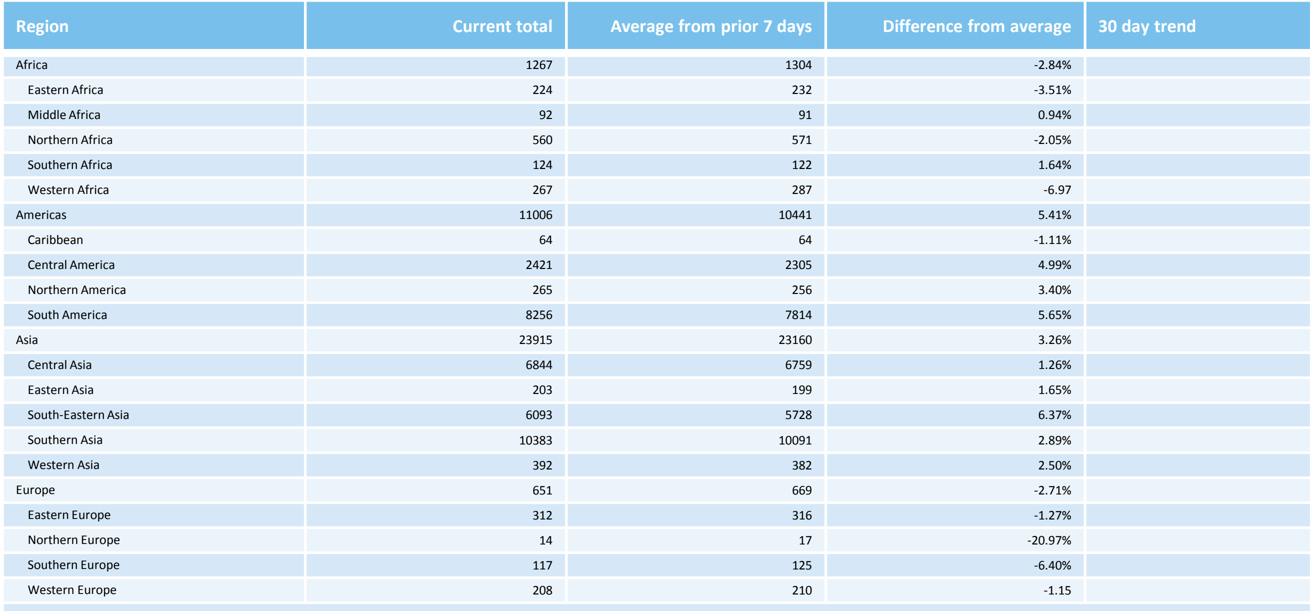
Numbers after “ns1.timechk” range from 1 to 30

Examples:
ns1.timechk7.org
ns1.timechk3.com
ns1.timechk19.net

The last known IP for this DGA is 91.231.87.184 at ns1.timechk23.com

The Results

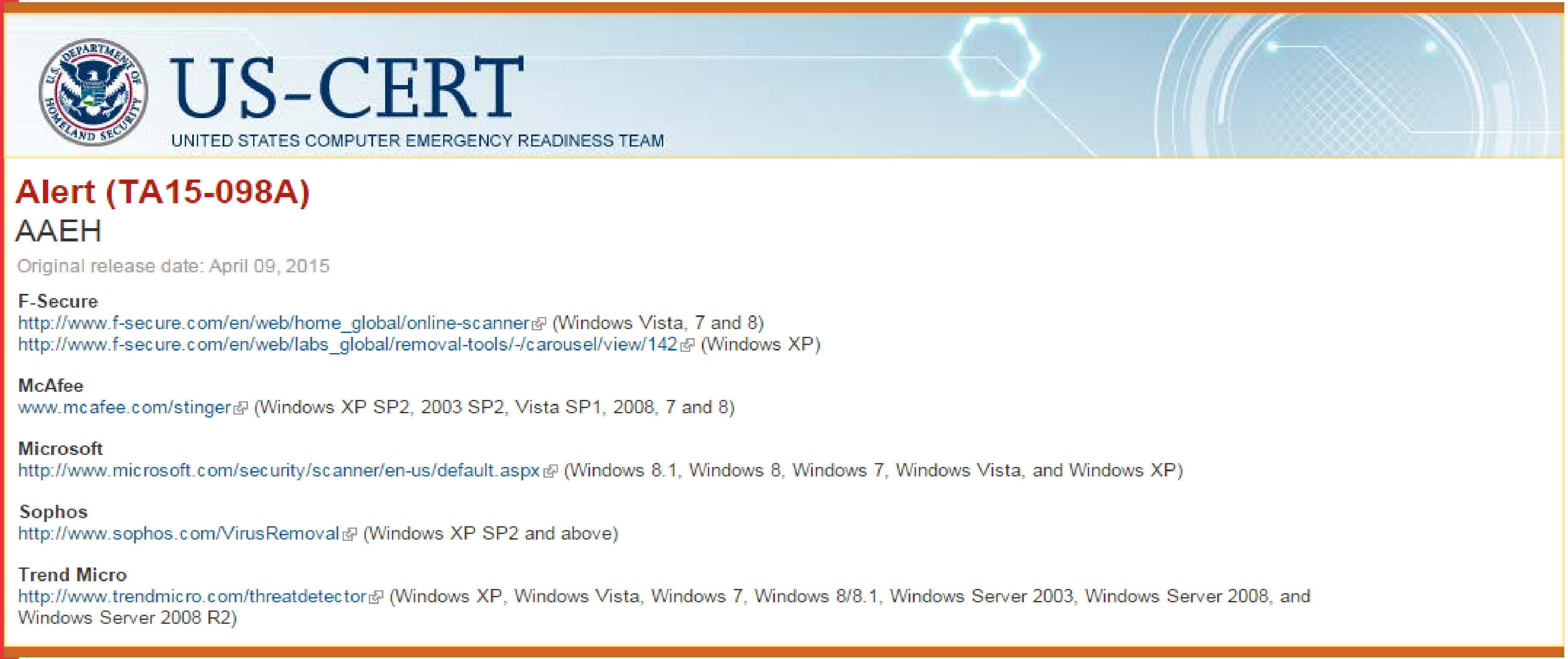
Country	Total
Iran, Islamic Republic of	8,403
Peru	6,548
Kazakhstan	3,212
Uzbekistan	2,947
Indonesia	2,051
Vietnam	1,838
Guatemala	1,643
India	1,533
Thailand	1,218
Philippines	879
Mexico	685
Ecuador	677
Bolivia	518
Kyrgyzstan	375
Afghanistan	354
Tajikistan	306
United States	250
Algeria	204
Russian Federation	170
Sudan	168



Region	Current total	Average from prior 7 days	Difference from average	30 day trend
Africa	1267	1304	-2.84%	
Eastern Africa	224	232	-3.51%	
Middle Africa	92	91	0.94%	
Northern Africa	560	571	-2.05%	
Southern Africa	124	122	1.64%	
Western Africa	267	287	-6.97	
Americas	11006	10441	5.41%	
Caribbean	64	64	-1.11%	
Central America	2421	2305	4.99%	
Northern America	265	256	3.40%	
South America	8256	7814	5.65%	
Asia	23915	23160	3.26%	
Central Asia	6844	6759	1.26%	
Eastern Asia	203	199	1.65%	
South-Eastern Asia	6093	5728	6.37%	
Southern Asia	10383	10091	2.89%	
Western Asia	392	382	2.50%	
Europe	651	669	-2.71%	
Eastern Europe	312	316	-1.27%	
Northern Europe	14	17	-20.97%	
Southern Europe	117	125	-6.40%	
Western Europe	208	210	-1.15	

Source: McAfee Labs

Remediation



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Alert (TA15-098A)

AAEH

Original release date: April 09, 2015

F-Secure
http://www.f-secure.com/en/web/home_global/online-scanner (Windows Vista, 7 and 8)
http://www.f-secure.com/en/web/labs_global/removal-tools/-/carousel/view/142 (Windows XP)

McAfee
www.mcafee.com/stinger (Windows XP SP2, 2003 SP2, Vista SP1, 2008, 7 and 8)

Microsoft
http://www.microsoft.com/security/scanner/en-us/default.aspx (Windows 8.1, Windows 8, Windows 7, Windows Vista, and Windows XP)

Sophos
http://www.sophos.com/VirusRemoval (Windows XP SP2 and above)

Trend Micro
http://www.trendmicro.com/threatdetector (Windows XP, Windows Vista, Windows 7, Windows 8/8.1, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2)

https://www.us-cert.gov/ncas/alerts/TA15-098A

Final thoughts…

Summary

- Intel Security is actively participating in operations against malware, botnets and actors cooperating with Law Enforcement around the globe and peers.

- We respect our customer's privacy and go for protection first before considering press attention.

- You and your organization can participate too!