

The 7 Habits of Highly-Effective Hackers

(and what we can learn from them)

Ryan Kazanciyan
Chief Security Architect, Tanium



whoami



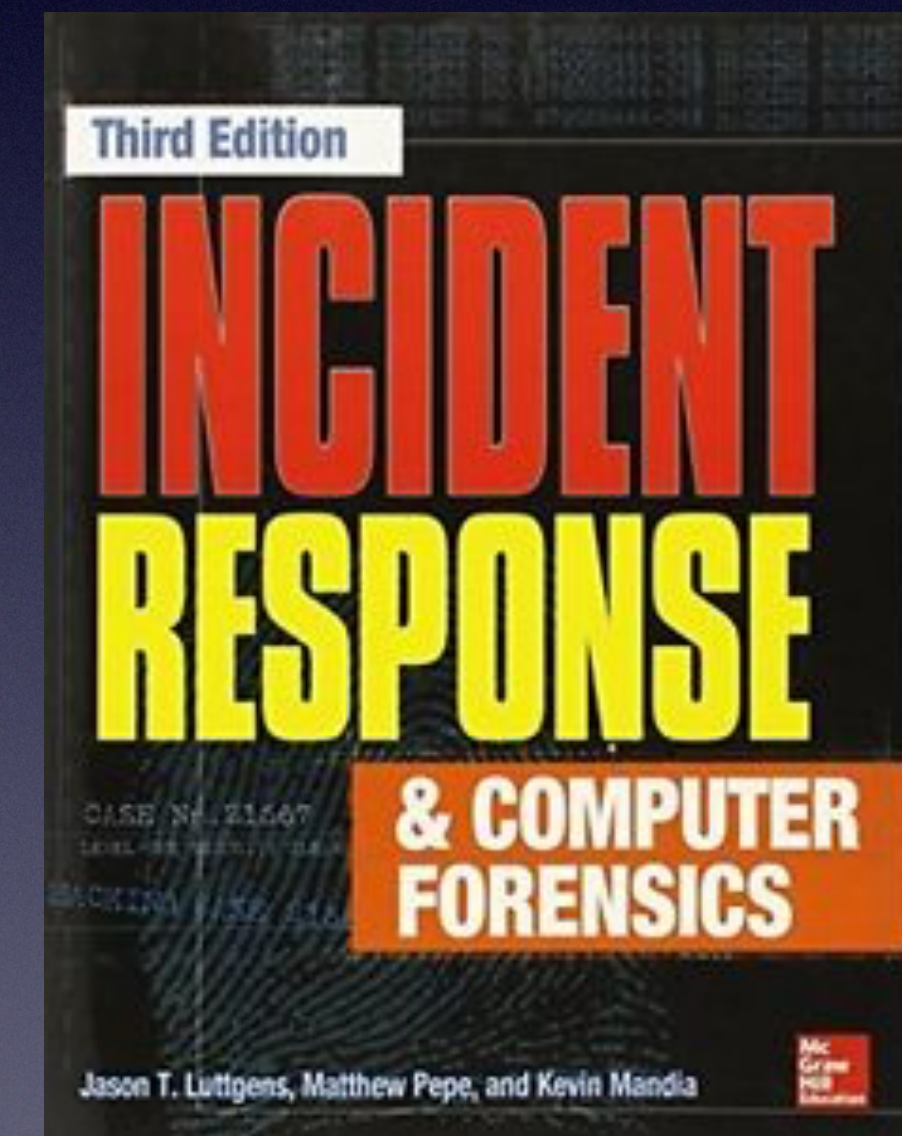
2004 - 2009



2009 - 2015



2015 - Present



Contributing
Author (2014)

MR. ROBOT

Technical Consultant
(S2 & S3)

```
Thu Aug 7, 12:41 AM

US Mobile - Law En...
View Go Bookmarks Help
Next Fit
207 Maine
208 Idaho
209 California
210 Texas
212 New York
213 California
214 Texas
215 Pennsylvania
216 Ohio
217 Illinois
218 Minnesota
219 Indiana
220 Tennessee

File Edit Search
NYPD Main Fax Line

root@kalibox:~
root@kalibox:~# scanimage --format=tiff > scannedexigentform.tif
root@kalibox:~# sendfax -f "US Mobile Law Enforcement" -r "Exigent Circumstance form" -X "NYPD" -x "US Mobile" -d 2125550117 -h ttyIAX@localhost scannedexigentform.tif
request id is 1 (group id 1) for host localhost (1 file)
root@kalibox:~# faxstat -s
HylaFAX scheduler on kalibox: Running
Modem ttyIAX (1.212.555.0126): Sending job 1
JID Pri S Owner Number Pages Dials TTS Status
1 1 R root 2125550117 0:1 0:12
root@kalibox:~#
```

```
File Edit View Search Terminal Help
root@kali:~/tools# radare2 -s 0x32C24 -w apc_hw05_aos_640.bin
WARNING: bin_strings buffer is too big (0x002d6300)
[0x00032c24]> pd 16
0x00032c24 bfe9b90a00 mov edi, 0xab9ef
.-> 0x00032c29 8bc1 mov eax, ecx
| 0x00032c2b 49 dec ecx
| 0x00032c2c 0bc0 or eax, eax
|=< 0x00032c2e 75f9 jne 0x32c29
0x00032c30 f6460640 test byte [esi + 6], 0x40 ; [0x40:1]=5 ; '@'
.==> 0x00032c34 7409 je 0x32c3f
| 0x00032c36 ba7affed80 mov edx, 0x80edff7a
| 0x00032c3b cc int3
| 0x00032c3c 80eb07 sub bl, 7
|--< 0x00032c3f ba7affed80 mov edx, 0x80edff7a
0x00032c44 e47f7f in al, 0x7f
0x00032c46 ba7affef90 mov edx, 0x90efff7a
0x00032c4b 90 nop
0x00032c4c 90 nop
0x00032c4d 90 nop
[0x00032c24]> s 0x00032c34
```


The 7 5 Habits of Highly-Effective Hackers (and what we can learn from them)

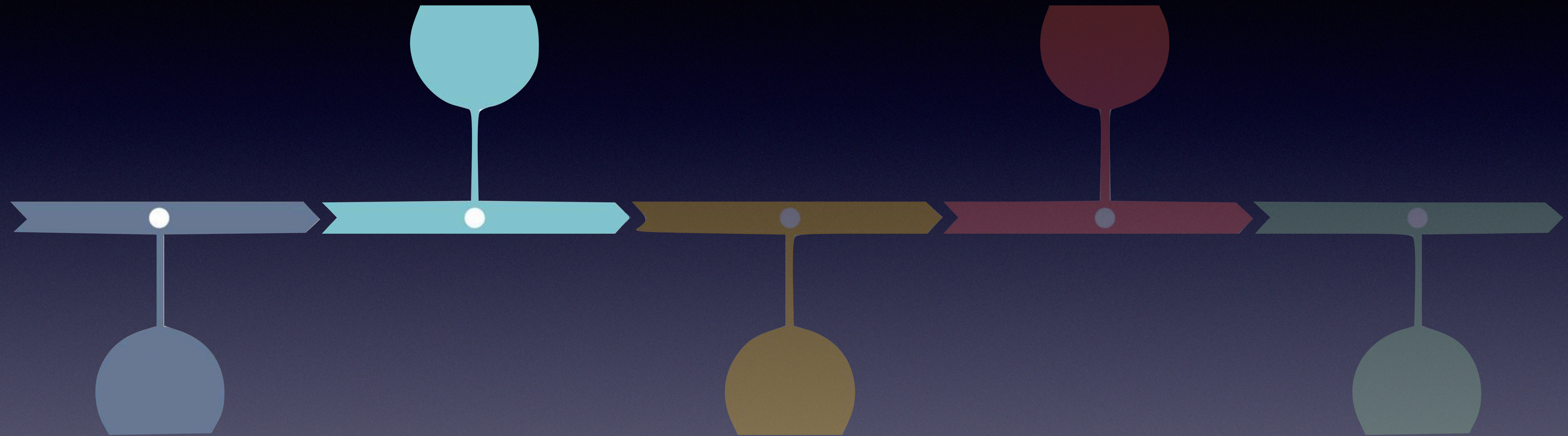
Ryan Kazanciyan
Chief Security Architect, Tanium



A hand holding a camera lens against a blurred background of a house and trees. The text "Knowing your environment" is overlaid in white.

Knowing your environment

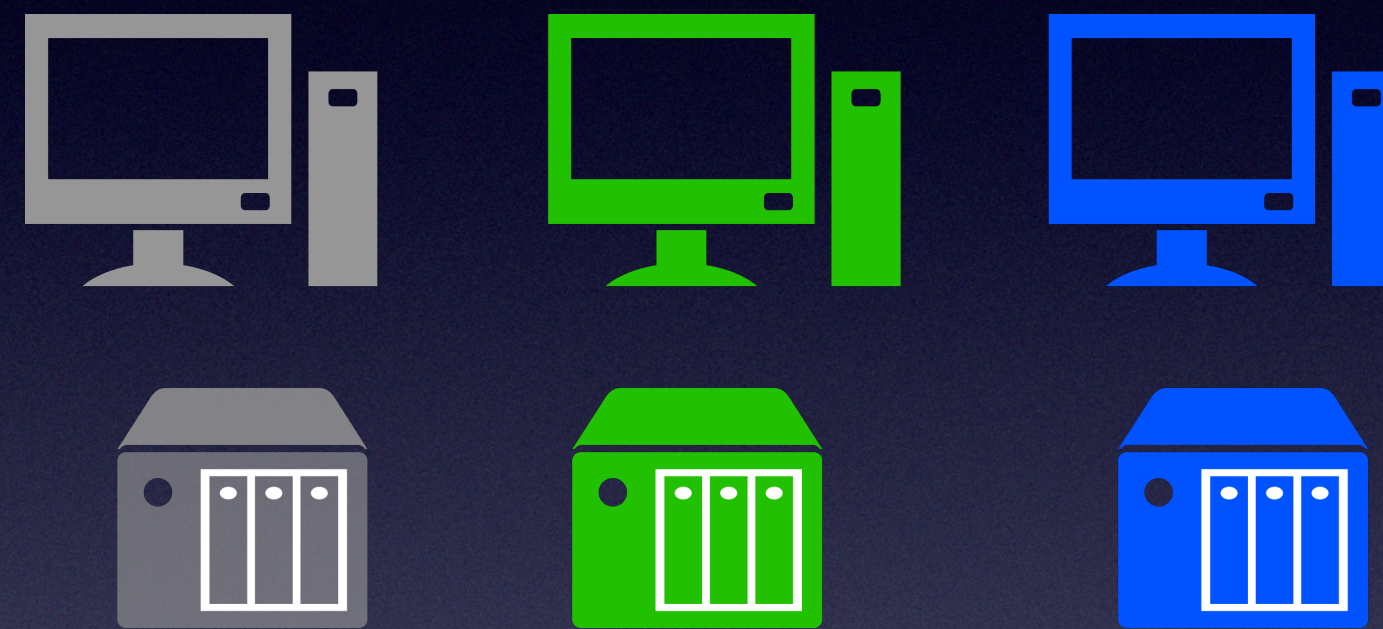
Reconnaissance



Initial Infection



Users



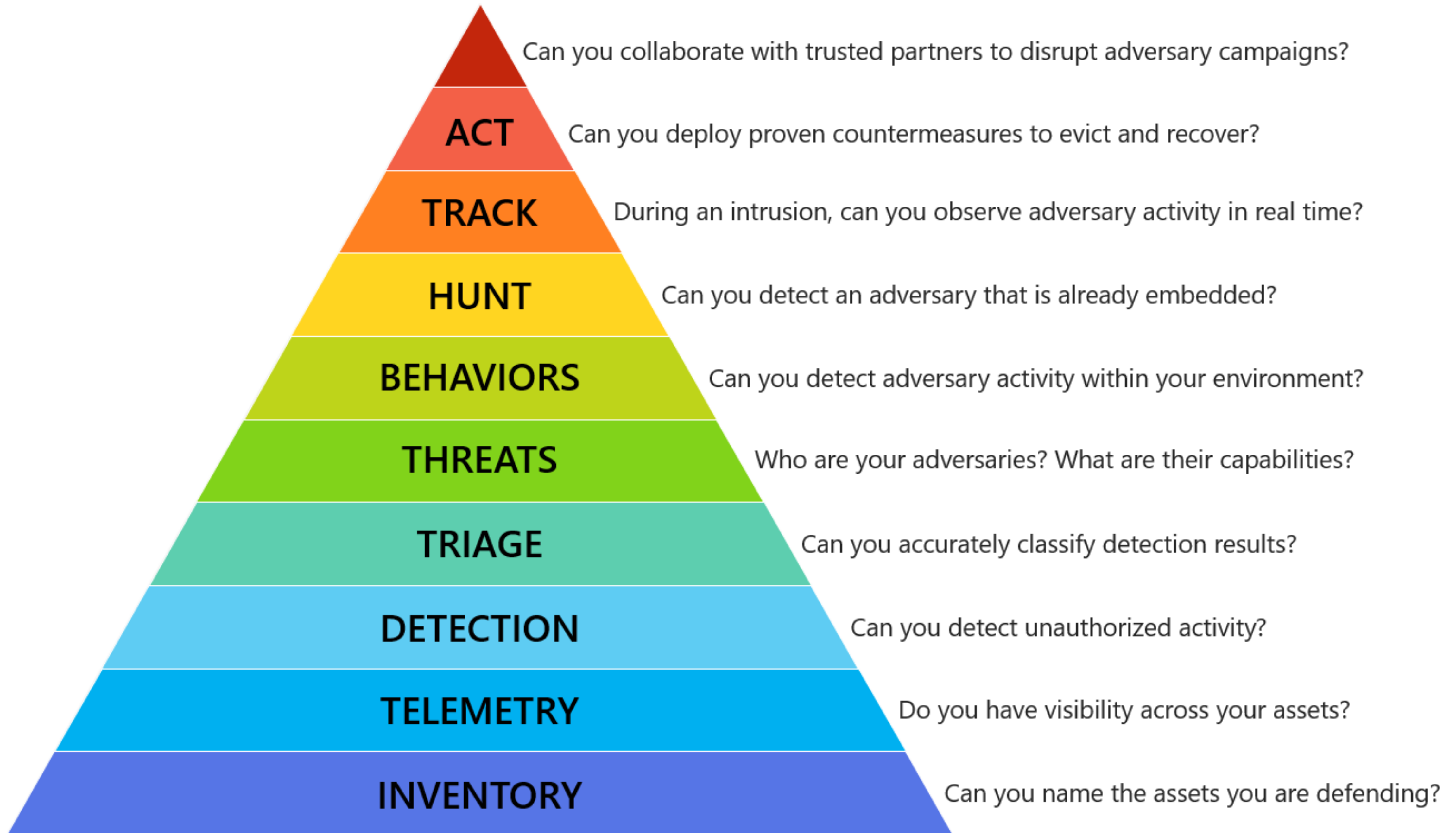
Systems



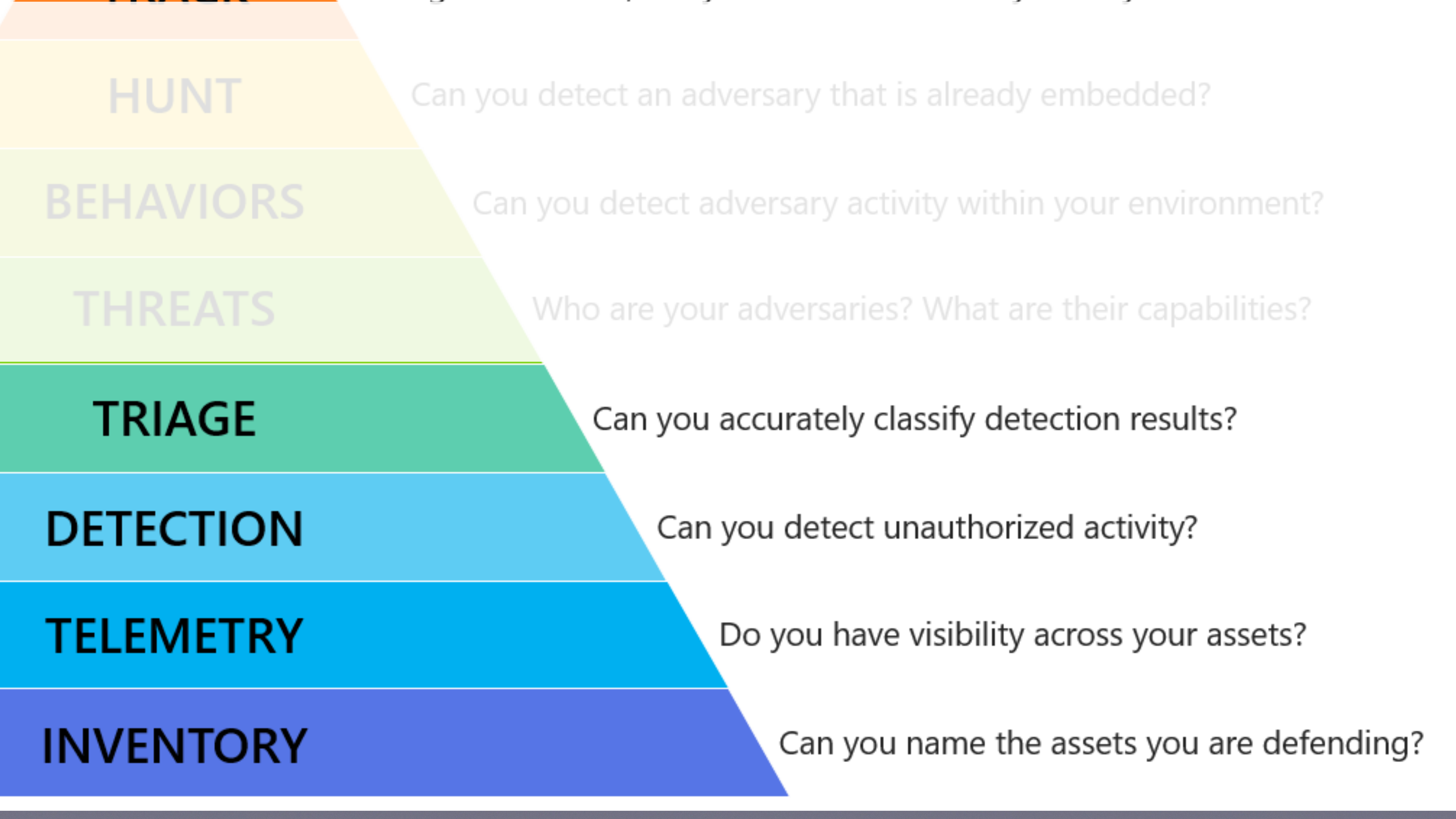
Data

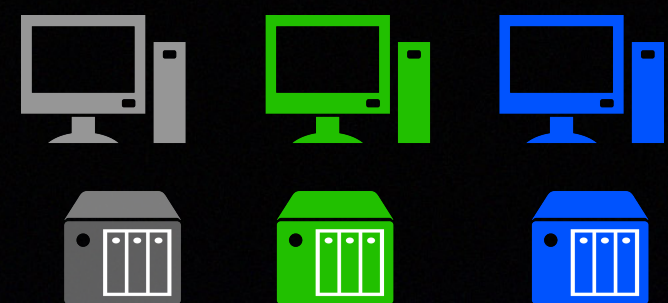
~20%

unmanaged endpoints typically identified by Tanium
in production networks

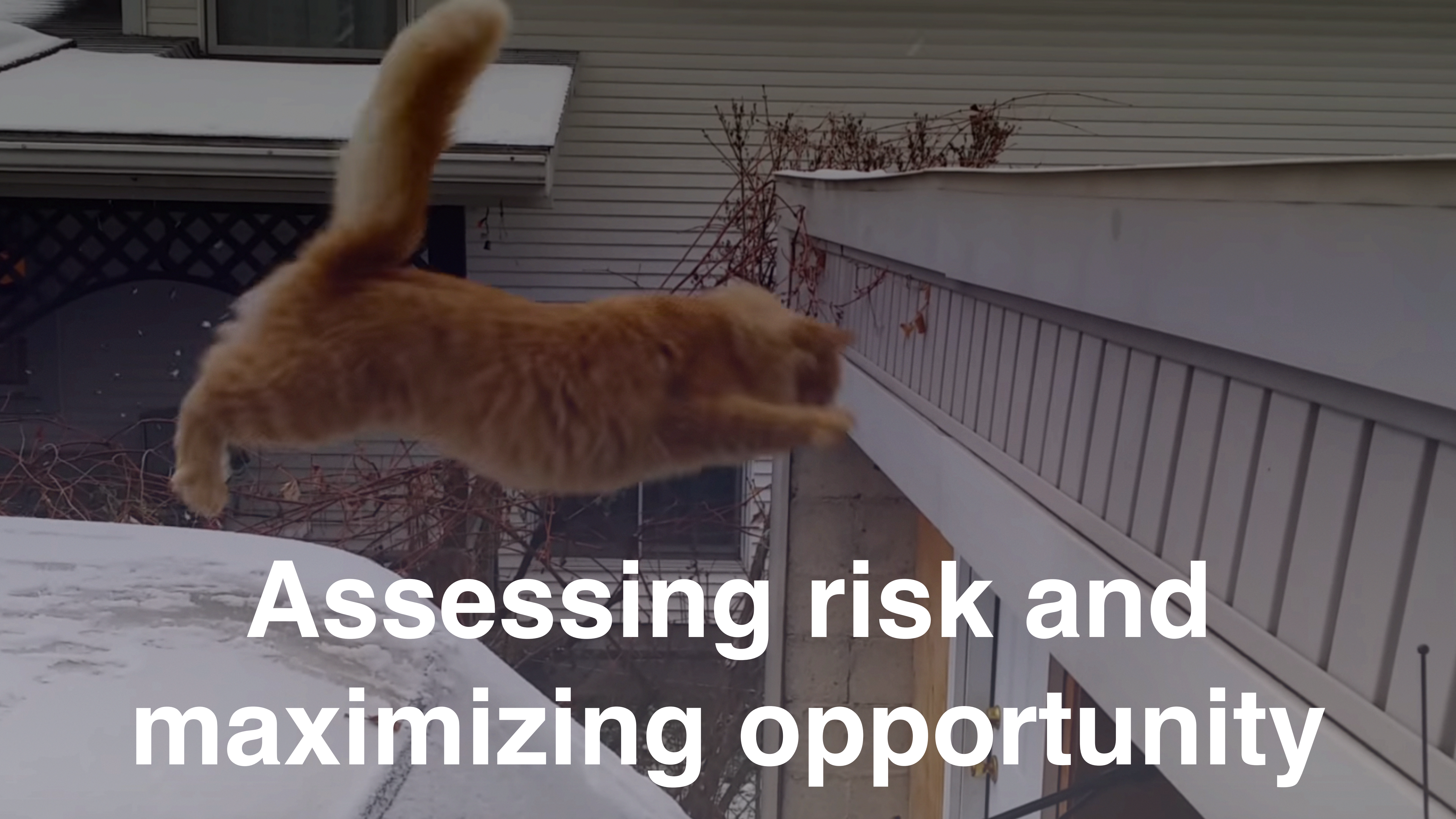


Source: Matt Swann @ <https://github.com/swannman/ircapabilities>





- Hostname
- Hardware
- Geolocation
- Custodian
- User role / function
- Current logged-in users
- Recent logged-in users
- Common logon sources
- Common logon destinations
- Installed applications
- Application usage metrics
- Missing patches
- Compliance status
- Processes and libraries
- Autostart programs
- Network traffic profile
- New binaries
- Script activity
- ...



**Assessing risk and
maximizing opportunity**

**Network
team**

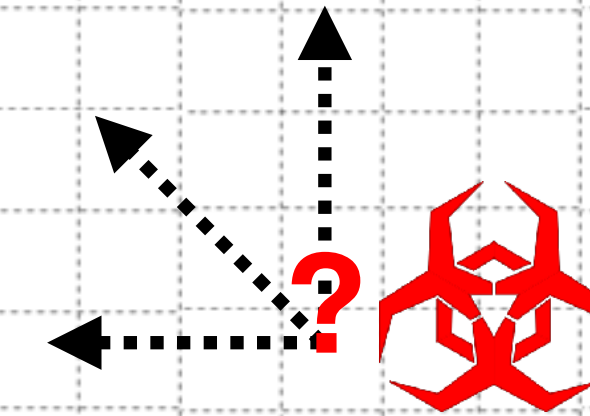
**Executive
team**

**Endpoint
admins**

Finance team

**Database
servers**

**Remote access
servers**



**Employee
desktops**

SOC analysts

**Security
servers**

**E-mail
servers**

Web servers

PoS terminals

Legal team

**Engineering
team**

**Domain
controllers**

**Helpdesk
team**



John Lambert

@JohnLaTwC

Following



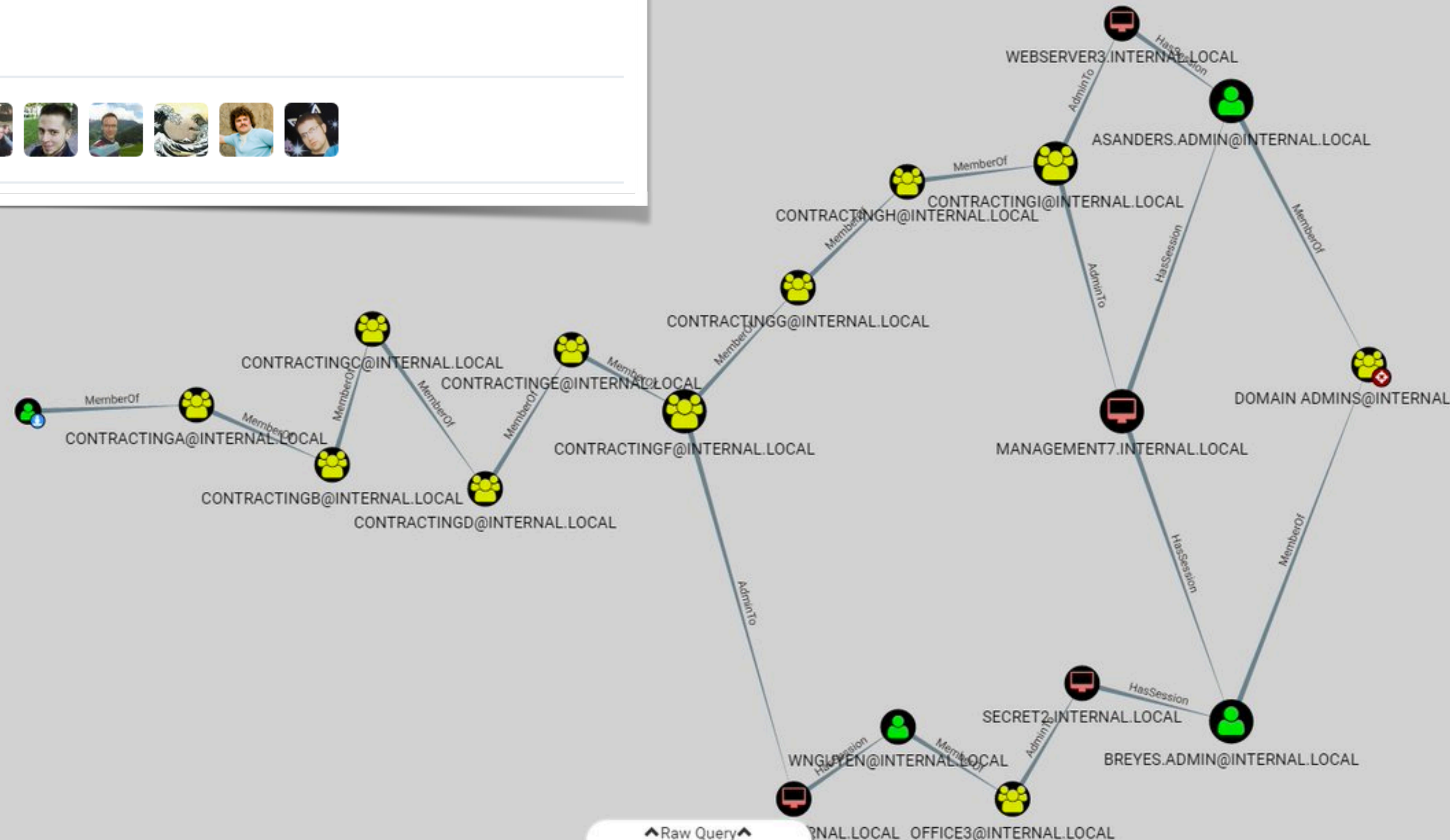
3. Your network is a directed graph of credentials. Hacking is graph traversal. See the graph or all you'll see is exfil.

RETWEETS

116

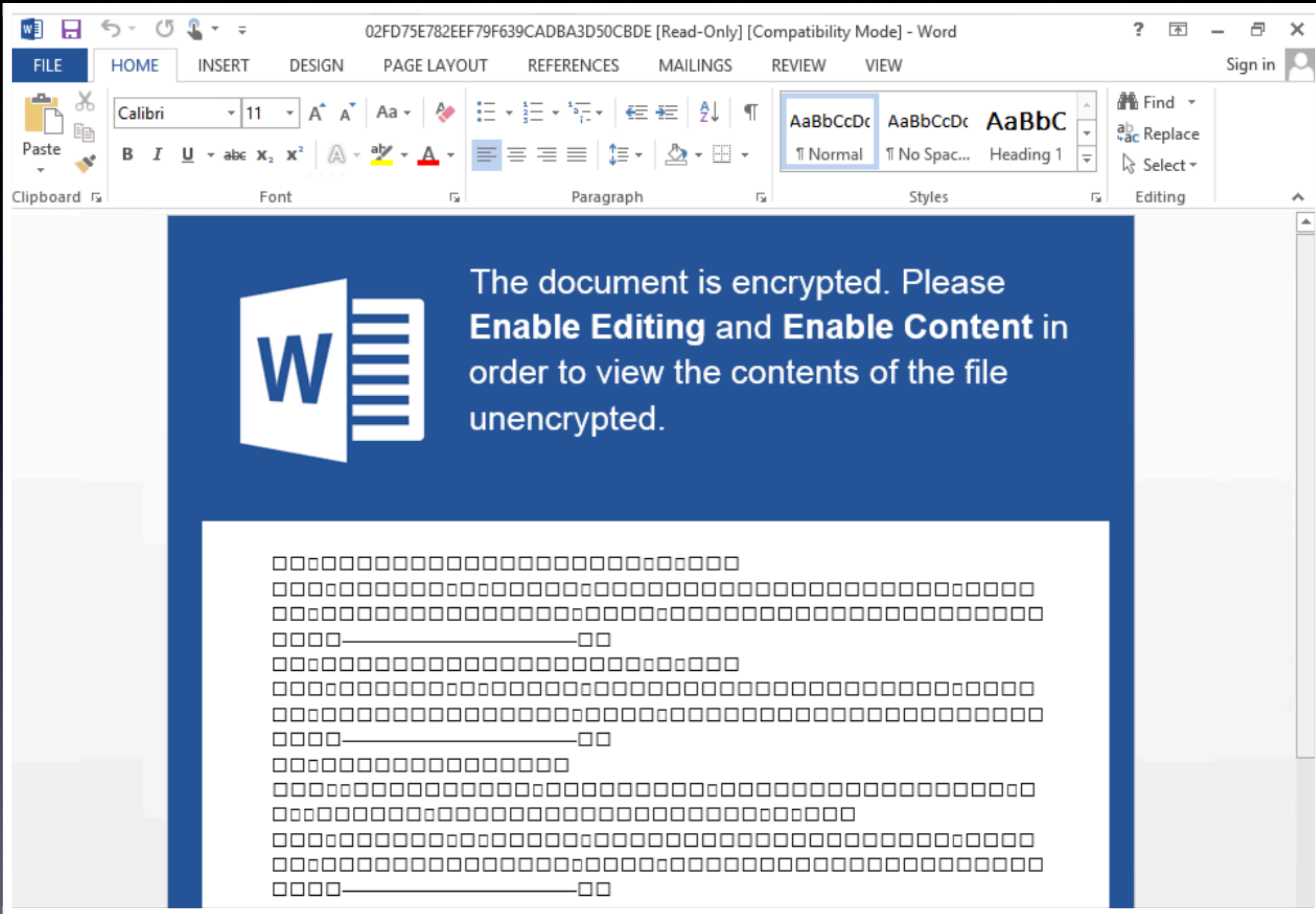
LIKES

166



38.5%

of malicious files detected by Microsoft Office365 in
2016 were Word documents



86%

said the greatest rise in potential IT security risk came from mobile devices, such as smartphones

0.03%

percentage of mobile devices infected with “truly
malicious” (non-adware) malware

Massive Android DDoS Botnet Derailed

WireX appears to have first surfaced on August 2 and remained unnoticed till August 15th when researchers from multiple security companies began observing it being used in prolonged DDoS attacks, some involving a minimum of 70,000 IP addresses. An analysis of the DDoS attack data



BUSINESS

CULTURE

DESIGN

GEAR

SCIENCE

SECURITY

TRANSPORTATION

LILY HAY NEWMAN SECURITY 09.29.16 6:00 PM

SHARE

SHARE
430

TWEET

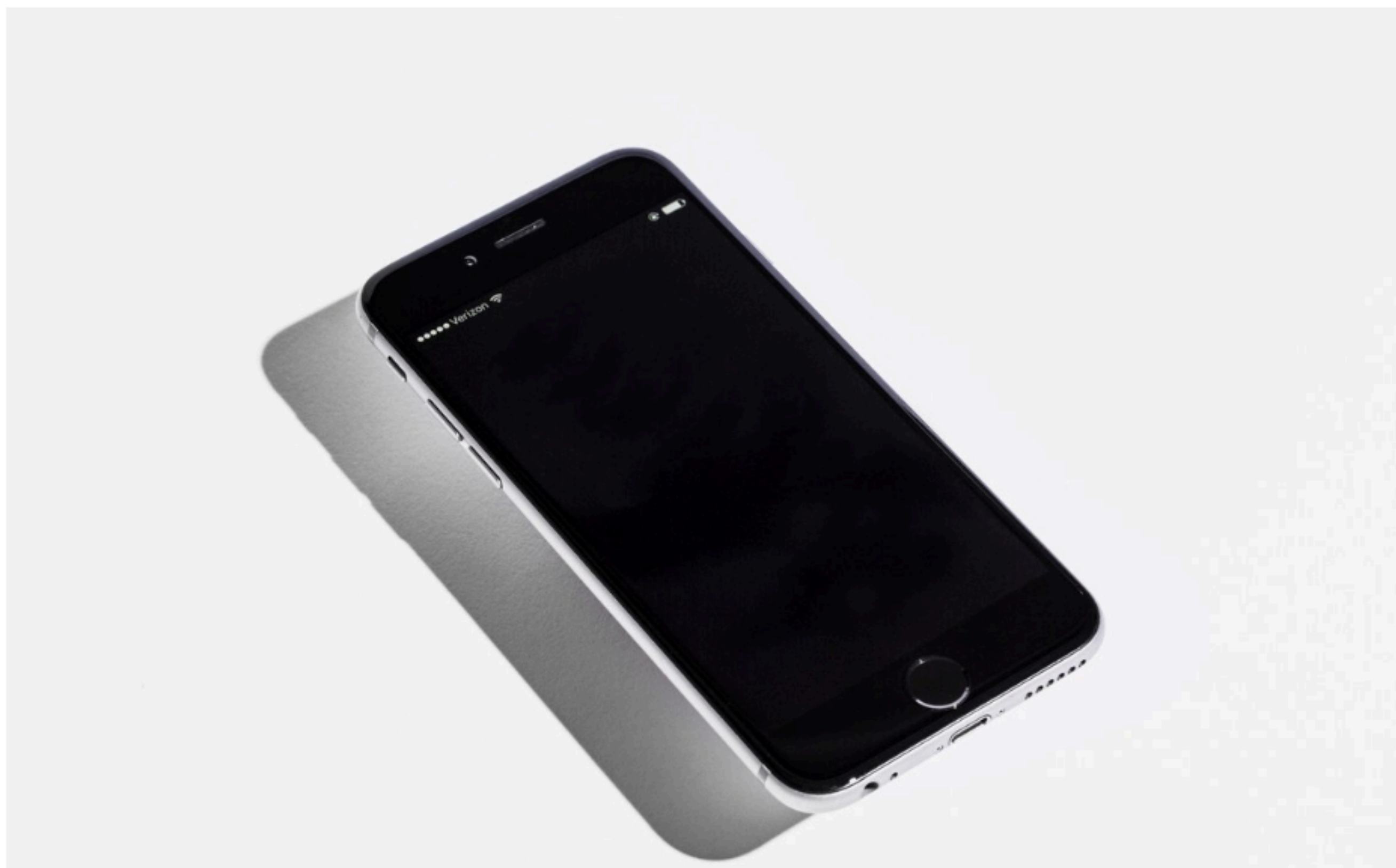


COMMENT



EMAIL

A TOP-SHELF IPHONE HACK NOW GOES FOR \$1.5 MILLION



MOST POPULAR



WHOA

A Stunning Video of Mars
That Took Three Months to
Stitch Together—by Hand
LIZ STINSON



BOOK EXCERPT

Humans Made the Banana
Perfect—But Soon, It'll Be
Gone
ROB DUNN



SECURITY

The FBI Has Been
Investigating Trump's
Russia Ties Since July
ANDY GREENBERG



MORE STORIES

71%

said that zero day attacks do the most harm

Exploiting vulnerabilities has become increasingly difficult

Exploitation used to be simple

Circa 2003; exploit steps for CVE-2003-0344

- ✓ Trigger stack buffer overrun
- ✓ Overwrite return address with ~~predictable address of a "JMP ESP"~~
- ✓ ~~Execute shellcode from the stack~~
- ✓ Arbitrary native code execution ☹

Windows Vista
enables ASLR

**Kills (most)
predictable images**

Internet Explorer 8
enables DEP

**Kills heap
spraying of code**

Exploits start relying
on ~~non-ASLR DLLs~~ to
bypass ASLR and ROP
to bypass DEP

*The Info leak era of
software exploitation*

Fermin Serna, Black Hat 2012

Exploits start relying
on address space
information
disclosures

Windows 8 adds
Force ASLR; IE10
enables it

**Kills all predictable
images**

Now, it is much more involved

- ✓ Place array length at a predictable location (via heap spray/massage)
- ✓ Modify array length via memory corruption, enabling arbitrary read/write
- ✓ Use arbitrary read/write to discover DLL base address
- ✓ Construct ROP payload by searching for code sequences in the DLL
- ✓ Corrupt C++ virtual table pointer and trigger virtual method call to first gadget
- ✓ Execute ROP payload (typically to make shellcode executable)
- ✓ Execute arbitrary native code
- ✓ Escape the sandbox (or operate inside it)

2006

2007

2008

2009

2010

2011

2012

2013

2014

2015

2016

Code heap spraying era

Non-ASLR DLL era

Arbitrary read/write era

**But...what about Shadow Brokers and
EternalBlue and and WannaCry and
NotPetya and...**

April 2015



Jose Barreto's Blog

A blog by Jose Barreto, a member of the OneDrive team at Microsoft.

The Deprecation of SMB1 – You should be planning to get rid of this old SMB dialect

Rate this article ★★★★★



[JoseBarreto](#) April 21, 2015

September 2016

Stop using SMB1



September 16, 2016 by [NedPyle \[MSFT\]](#) // [149 Comments](#)

 Share 795

 810

 706

Hi folks, [Ned](#) here again and today's topic is short and sweet:

Stop using SMB1. *Stop using SMB1. **STOP USING SMB1!***

Earlier this week we released [MS16-114](#), a security update that prevents denial of service and remote code execution. If you need this security patch, you already have a much bigger problem: you are still running SMB1.

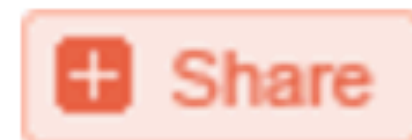
The original SMB1 protocol is nearly [30 years old](#), and like much of the software made in

January 2017



SMB Security Best Practices

Original release date: January 16, 2017 | Last revised: March 16, 2017



In response to public reporting of a potential Server Message Block (SMB) vulnerability, US-CERT is providing known best practices related to SMB. This service is universally available for Windows systems, and legacy versions of SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

US-CERT recommends that users and administrators consider:

- disabling SMBv1 and
- blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports

March 2017

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.

On this page

[Executive Summary](#)

[Affected Software and
Vulnerability Severity Ratings](#)



Ooops, your files have been encrypted!

English

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:58:59

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:58:59

[About bitcoin](#)[How to buy bitcoins?](#)[Contact Us](#)

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

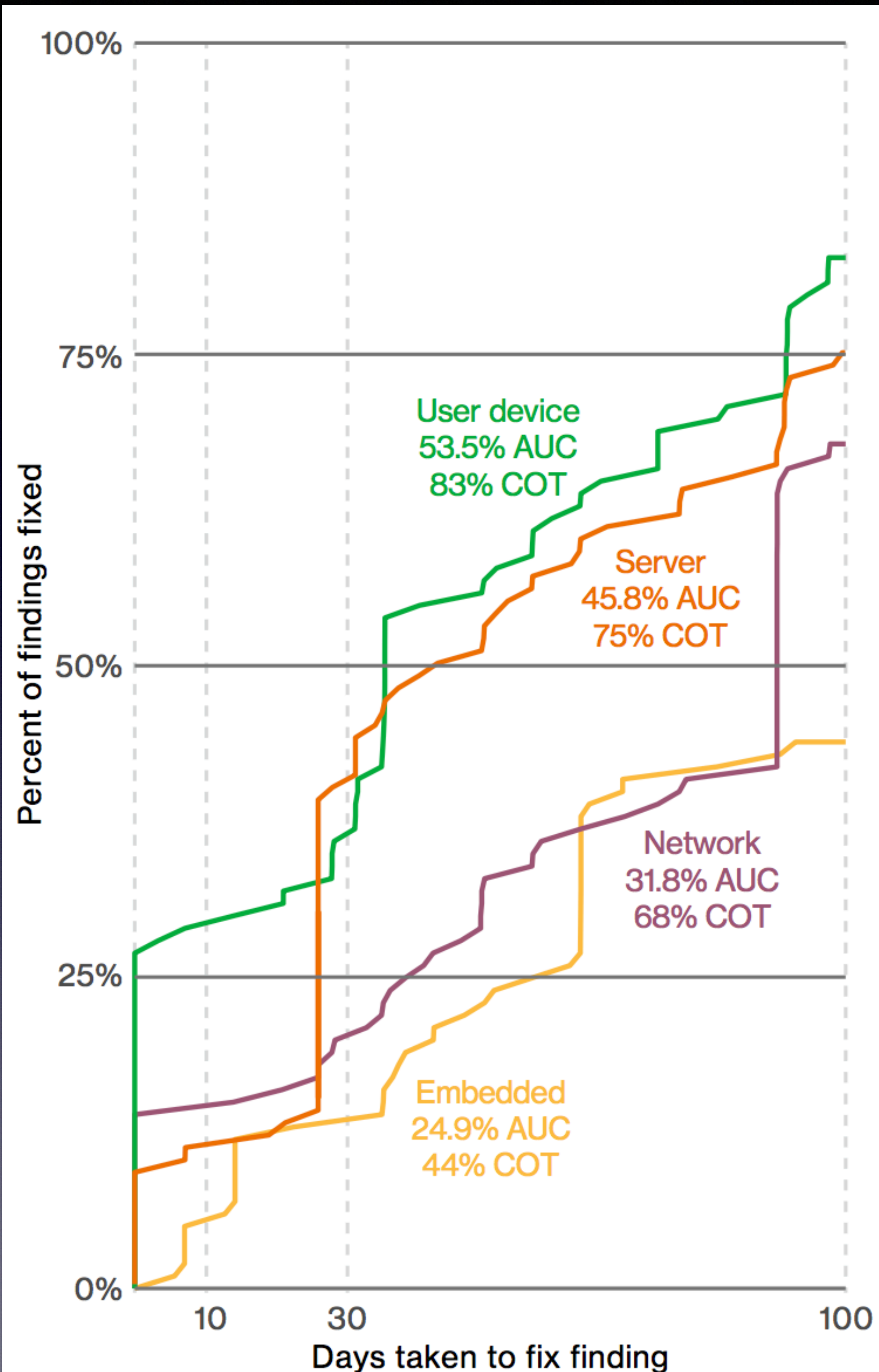
CMT from Mondays to Fridays



Send \$300 worth of bitcoin to this address:

115p7UMMngo1pMvkcPHjcRdfJNXj6LrLn

[Copy](#)[Check Payment](#)[Decrypt](#)



“We found 12 weeks was where most organizations had completed their patch process”

‘on time’ may be seven days for [critical] findings, where a quarterly patch cycle may be the “norm” for the rest.’

-Verizon DBIR 2017


```

uu$$$$$$$$$$$$uu
uu$$$$$$$$$$$$$$$$uu
u$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$*$$$$$*$$$$$u
*$$$$$*u$u$$$$$*
$$$u$u$u$$$
$$$u$u$u$$$
*$$$$$uu$$$$$$$$uu$$$$$*
*$$$$$$$$$*$$$$$$$$$*
u$$$$$$$$$u$$$$$$$$$u
u$*$*$*$*$*$*$*$u
$$$u$ $ $ $ $u$$$
$$$$$u$u$u$$$
$$$$$uu$$$$$*
u$$$$$$$$$$$$$$$$uu*****uuuu$$$$$$$$$$$$
$$$$$***$$$$$$$$$$$$$$$$uuuuuu$$$$$$$$$$$$$$$$$$$$$*
*****$$$$$$$$$$$$$$$$$uu**$***
uuuu**$$$$$$$$$$$$$$$$$uuuu
u$$$$$uuu$$$$$$$$$$$$$uu**$$$$$$$$$$$$$$$$$uuuu$$$
$$$$$$$$$$$$$$$$$*****$$$$$$$$$$$$$$$$$$$$$*
*$$$$$*$$$$$*
$$$*PRESS ANY KEY!$$$$$*

```


NCCIC observed multiple methods used by NotPetya to propagate across a network. The first and—in most cases—most effective method, uses a modified version of the Mimikatz tool to steal the user's Windows credentials. The cyber threat actor can then use the stolen credentials, along with the native Windows Management Instrumentation Command Line (WMIC) tool or the Microsoft SysInternals utility, psexec.exe, to access other systems on the network. Another method for propagation uses the EternalBlue exploit tool to target unpatched systems running a vulnerable version of SMBv1. In this case, the malware attempts to identify other hosts on the

<https://www.us-cert.gov/ncas/alerts/TA17-181A>

NCCIC observed multiple methods used by NotPetya to propagate across a network. The first and—in most cases—most effective method, uses a modified version of the Mimikatz tool to steal the user's Windows credentials. The cyber threat actor can then use the stolen credentials, along with the native Windows Management Instrumentation Command Line (WMIC) tool or the Microsoft SysInternals utility, psexec.exe, to access other systems on the network. Another method for propagation uses the EternalBlue exploit tool to target unpatched systems running a vulnerable version of SMBv1. In this case, the malware attempts to identify other hosts on the

<https://www.us-cert.gov/ncas/alerts/TA17-181A>

Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques

Mitigating the risk of lateral movement and privilege escalation

Copyright © 2012 Microsoft Corporation. All rights reserved.



scriptjunkie

@scriptjunkie1

 Follow



If infosec was an NBA defense it would spend 100% of practice time stopping half-court shots, 0% on everything else

Josh Abraham @Jabra

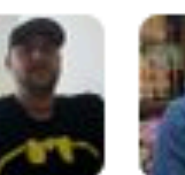
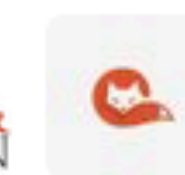
"In sports, great coaches study the opposition's favorite strategies and build in defensive strategies to take them off the table."

RETWEETS

95

LIKES

151



8:57 PM - 31 Jul 2016



9



95



151



Building on platforms

COZYCAR

SEADUKE

ZEROACCESS

DRIDEX

GH0ST

X-AGENT

KAZUAR

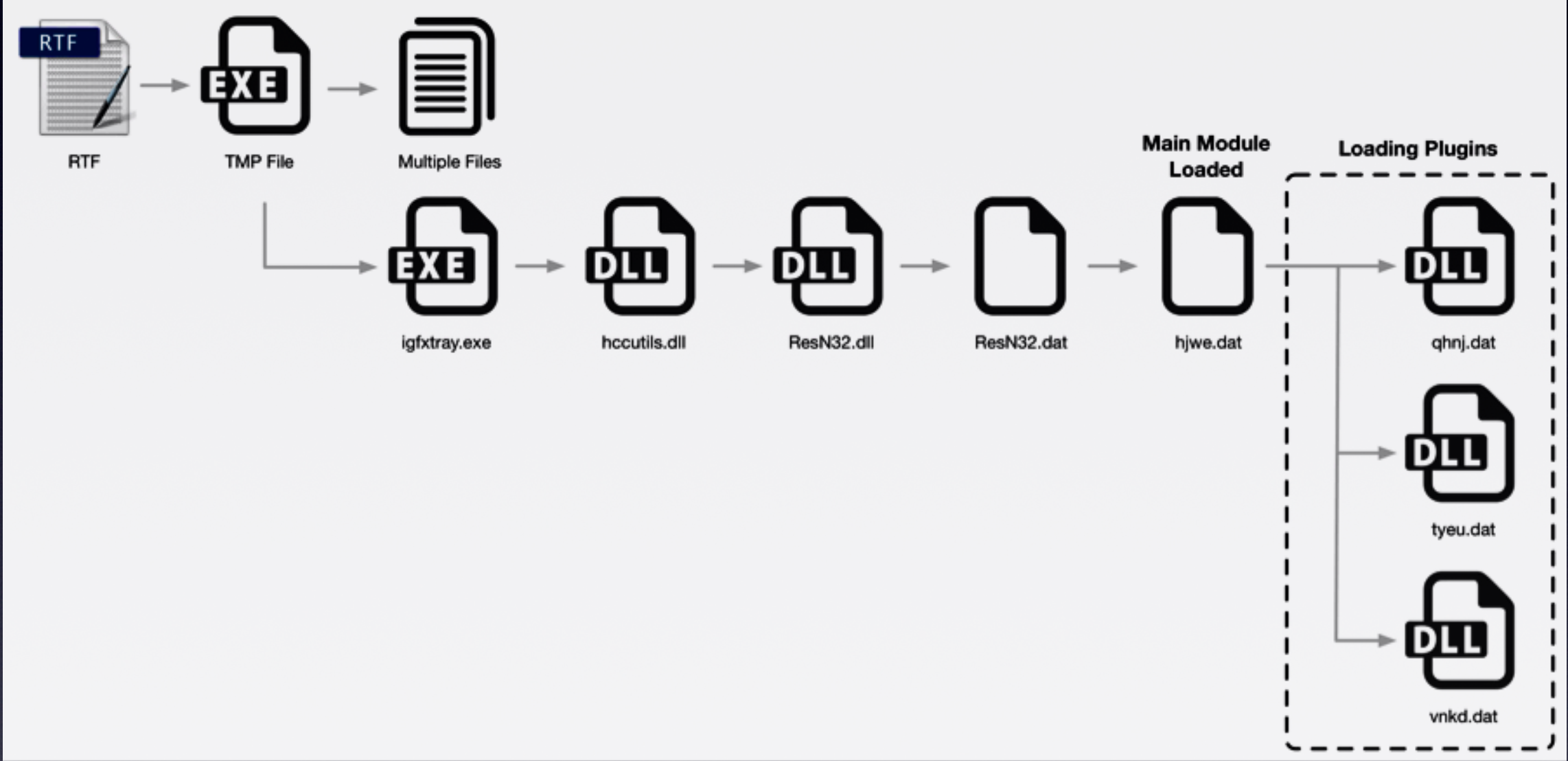
FLAME

REGIN

BLACKENERGY

DUQU

NECURS



Source: Palo Alto

- Extensibility & flexibility
- Operator consistency
- Development efficiencies
- Endpoint footprint

34% - 6-10

15% - 10+

Average # of endpoint agents









Jessica Payne

@jepayneMSFT

Following



Sometimes to enhance security and reduce attack surface of a system the answer is not to add more technology, but to take away technology.

RETWEETS

166

LIKES

361



2:06 PM - 1 Dec 2016

16

166

361

Managing your software supply chain

Sustainable and responsible



Artisanal
Malware

A locally-sourced guide

O RLY?

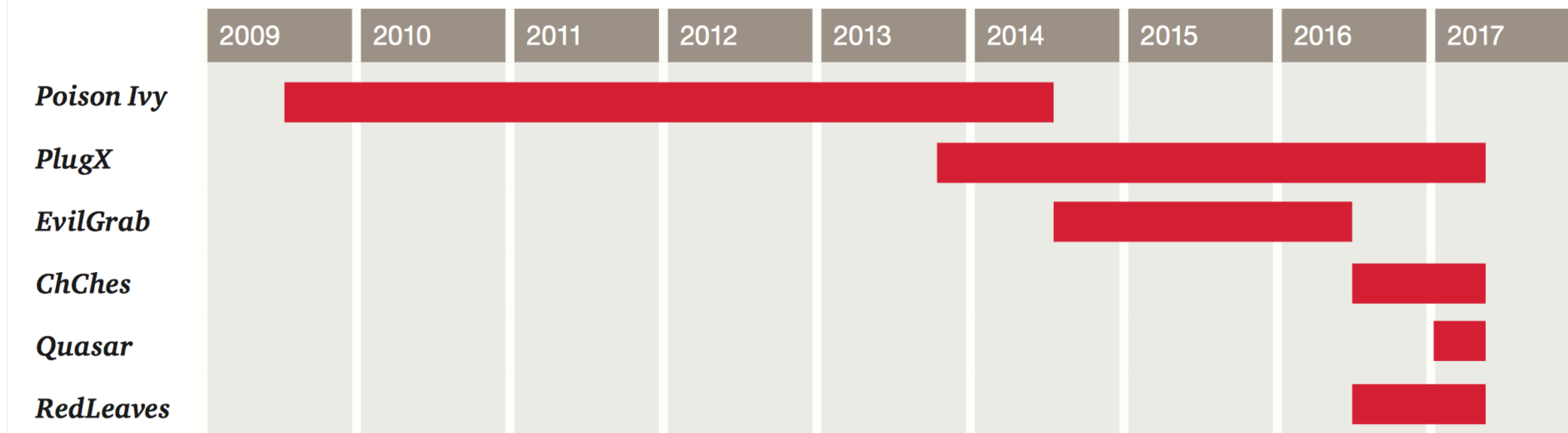
Your Favorite APT

What software do organized
attack groups trust?

APT10

Timeline

Figure 17: Timeline of APT10 malware use

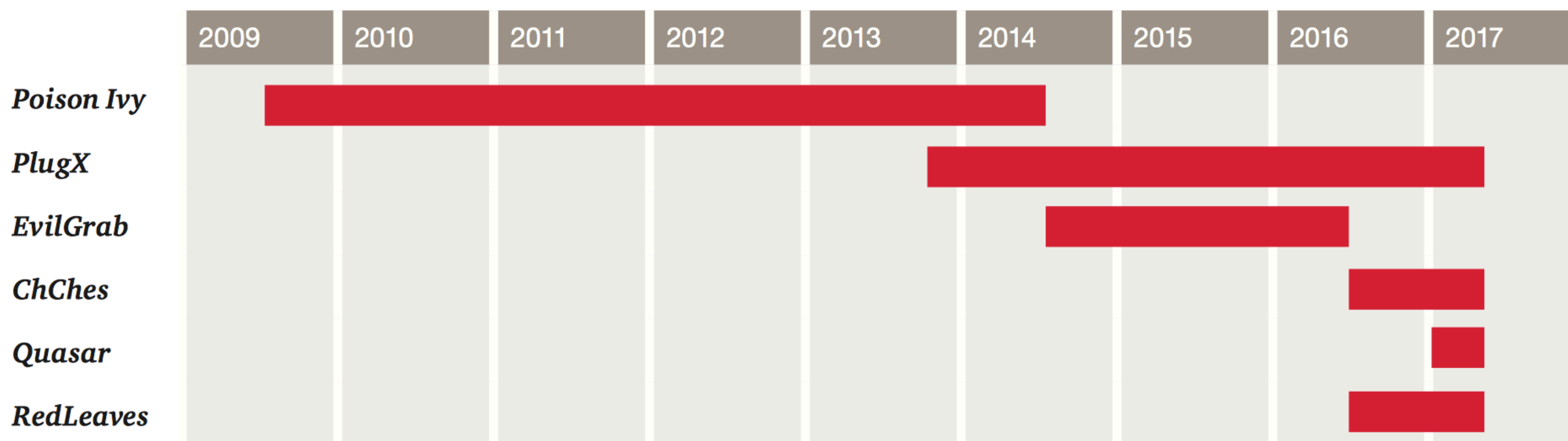


<https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf>

APT10

Timeline

Figure 17: Timeline of APT10 malware use



<https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf>

FIN10

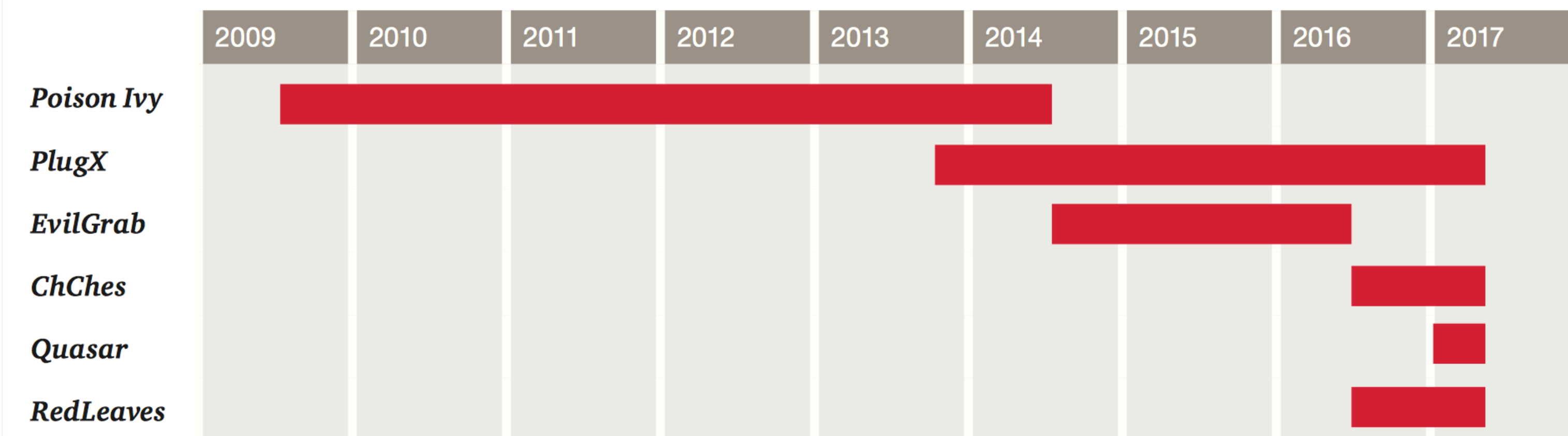
Meterpreter, an advanced payload included in the Metasploit Framework, is the primary strategy the group used to gain admission into corporate networks, although FireEye also detected the group using Splinter Remote Access Trojan (SplinterRAT). The group also was found to be using PowerShell Empire, a pen-testing tool, for elevated persistence.

<https://www.scmagazine.com/fin10-extorting-companies-in-cyber-schemes-fireeye/article/669244/>

APT10

Timeline

Figure 17: Timeline of APT10 malware use



<https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf>

FIN10

Meterpreter, an advanced payload included in the Metasploit Framework, is the primary strategy the group used to gain admission into corporate networks, although FireEye also detected the group using Splinter Remote Access Trojan (SplinterRAT). The group also was found to be using PowerShell Empire, a pen-testing tool, for elevated persistence.

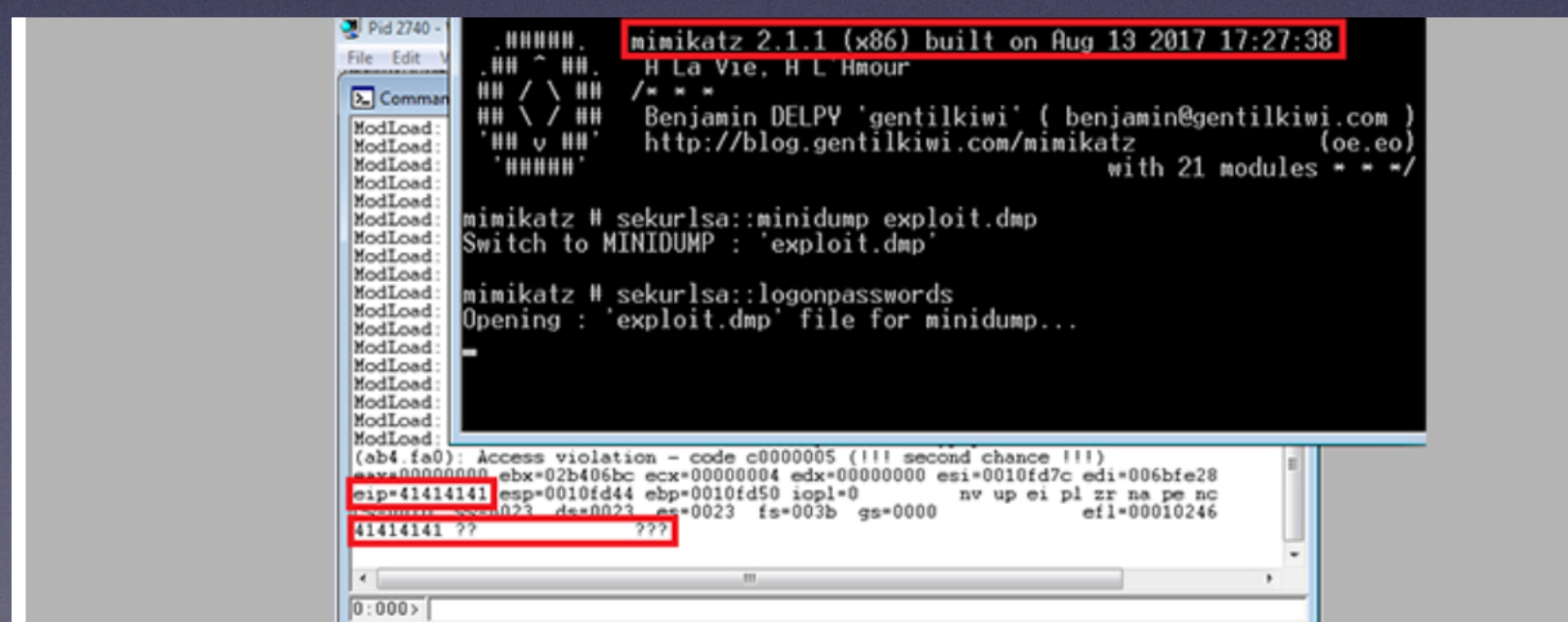
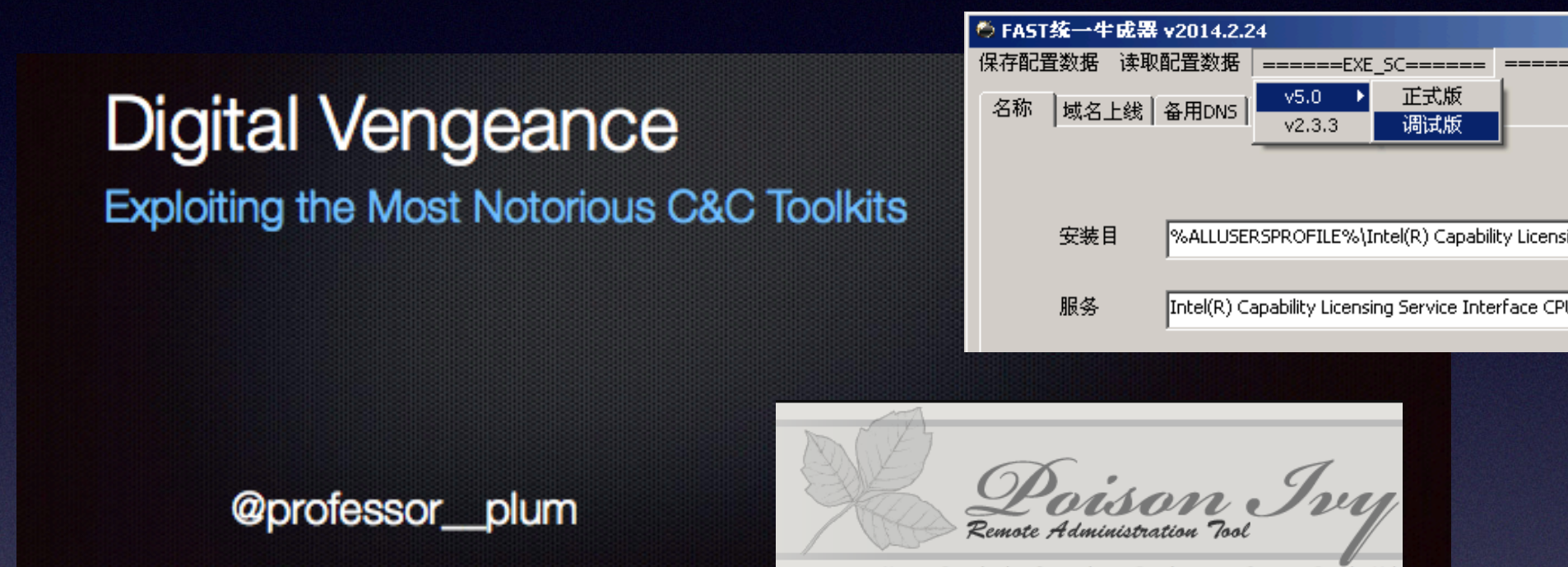
<https://www.scmagazine.com/fin10-extorting-companies-in-cyber-schemes-fireeye/article/669244/>

APT28

APT28 is increasing reliance on public code repositories, such as Carberp, PowerShell Empire, P.A.S. webshell, Metasploit modules, and others in a likely effort to accelerate their development cycle and provide plausible deniability.

<https://www.scmagazineuk.com/fireeye-report-hacking-group-apt28-and-their-tradecraft/article/631133/>

Hacking tools are not immune to exploitable bugs!



HACK THE HACKER – FUZZING MIMIKATZ ON WINDOWS WITH WINAFL & HEATMAPS (0DAY)

They're Coming for Your Tools!

Exploiting Design Flaws for Active Intrusion Prevention



What do the best attackers worry about?

(as learned from certain leaks)

- Identifiers and exposure from re-used code
- Standardized vs. homegrown protocols and crypto
- Development rigor → stability and reliability
- Forensic footprint
- Code security

What end-user applications do you “trust” in your environment?



SHA256: 2fd2863d711a1f18eeee5c7c82f2349c5d4e00465de9789da837fcdca4d00277

File name: ZvitPublishedObjects.dll

Detection ratio: 1 / 62

Analysis date: 2017-07-04 12:40:11 UTC (2 days, 2 hours ago) [View latest](#)



- Analysis
- File detail
- Relationships
- Additional information
- Comments 1
- Votes

Antivirus	Result	Update
ESET-NOD32	a variant of MSIL/TeleDoor.A	20170704
Ad-Aware	✓	20170704
AegisLab		
AhnLab-V3		
Alibaba		
ALYac		
Antiy-AVL		
Arcabit		
Avast		
AVG		
Avira (no cloud)		
AVware	✓	20170704
Baidu	✓	20170704
BitDefender	✓	20170704
Bkav	✓	20170704
CAT-QuickHeal	✓	20170704
ClamAV	✓	20170704
CMC	✓	20170701
Comodo	✓	20170704
CrowdStrike Falcon (ML)	✓	20170420

File name: ZvitPublishedObjects.dll

Detection ratio: 1 / 62



1 / 64

One engine detected this file

SHA-256	6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9
File name	ccleaner
File size	7.32 MB
Last analysis	2017-09-14 14:26:20 UTC
Community score	+34

Detection

Details

Relations

Behavior

Community

2

ClamAV

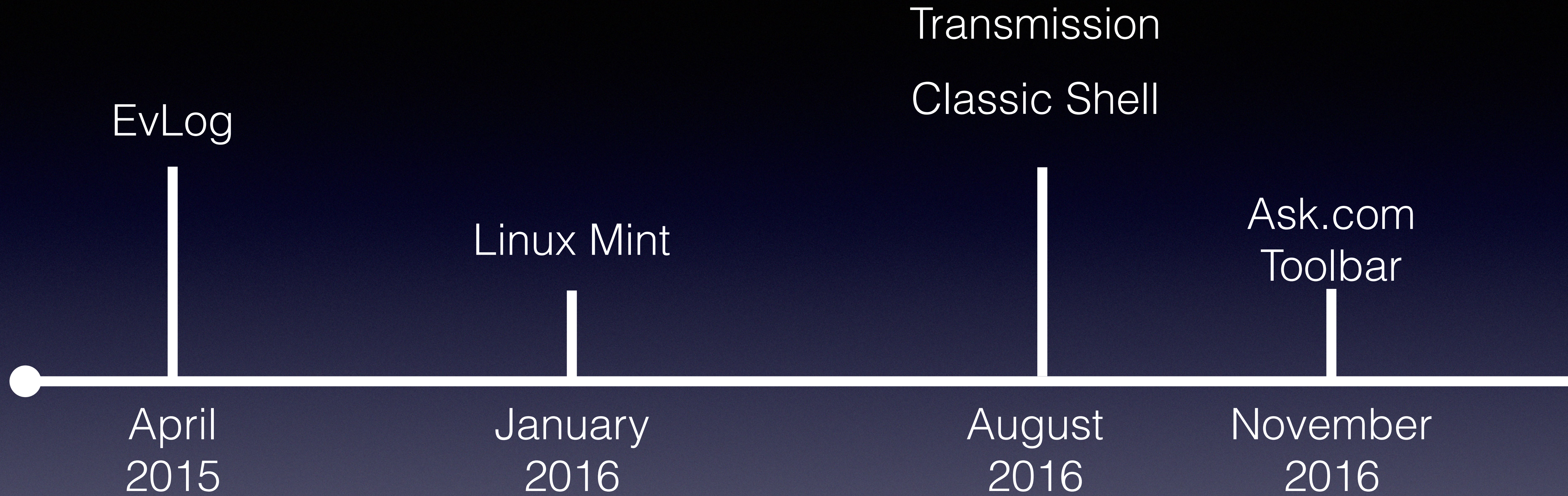


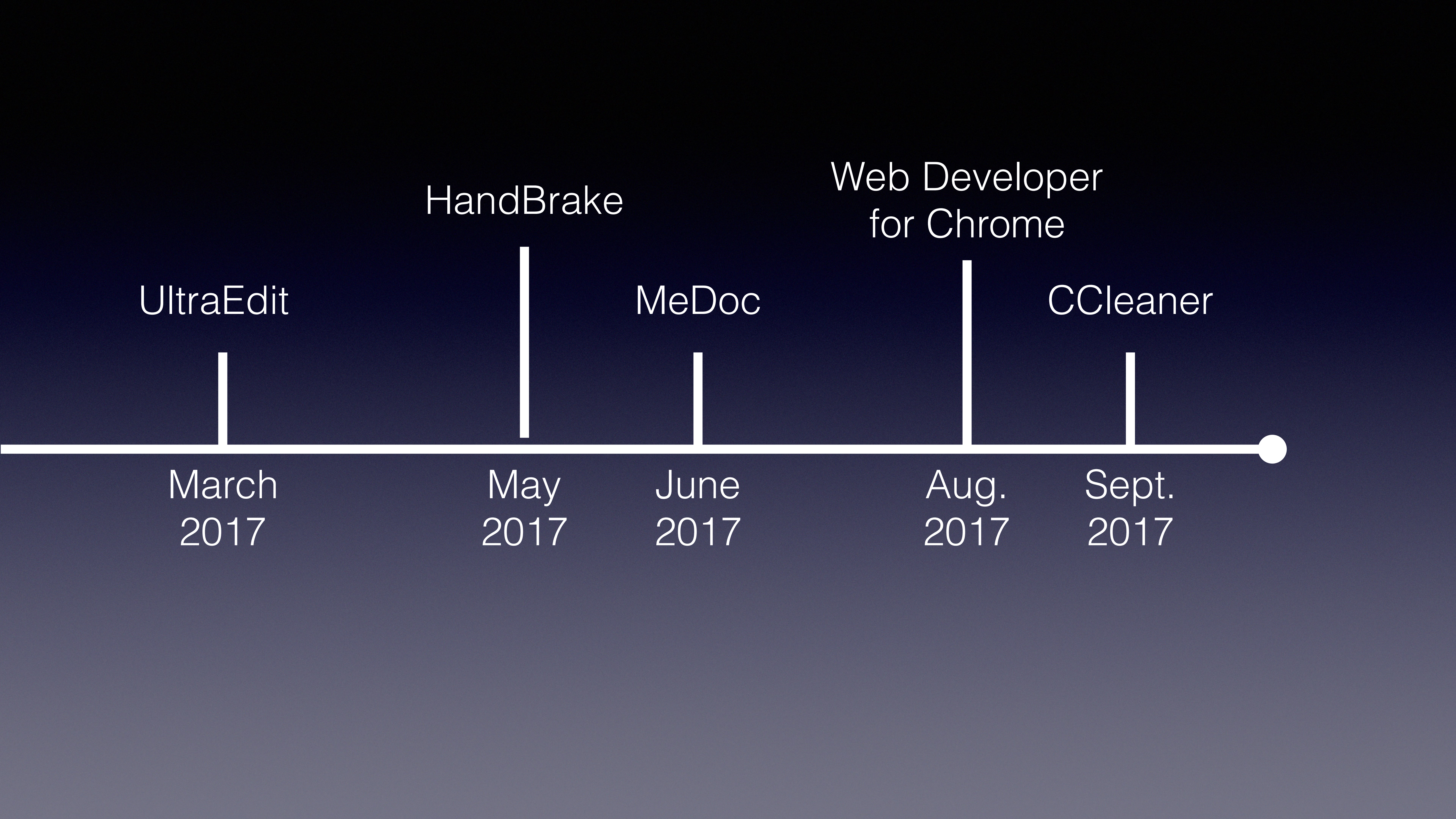
Win.Trojan.Floxif-6336251-0

Ad-Aware



Clean





UltraEdit

HandBrake

MeDoc

Web Developer
for Chrome

CCleaner

March
2017

May
2017

June
2017

Aug.
2017

Sept.
2017

Managing what you trust

- Review completeness and accuracy of application inventory
- Assess where controls implicitly trust end-user software
- Table-top supply-chain attack scenarios
- Baseline trusted application behaviors
- Manage and restrict software sources



Engineering for resilience

99 days

median dwell time from compromise
to detection in 2016

- Software failure
- Operator error
- Automated detection
- Human detection
- Hardware replacement



NCCIC



Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: This report is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction. For more information on the Traffic Light Protocol, see <https://www.us-cert.gov/tlp>.

Reference Number: JAR-16-20296A

December 29, 2016

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

TODAY'S TOP STORIES

Inside the Russian hack of Yahoo: How they did it

A single click was all it took to launch one of the biggest data breaches ever



By **Martyn Williams**

Senior U.S. Correspondent, [IDG News Service](#) | MAR 16, 2017 4:29 AM PT



Sam Quigley

@emerose

 Follow



The goal of security infrastructure should be to make the safe thing easy. Sometimes, making the unsafe thing impossible is the best path

Diogo Mónica ★ @diogomonica

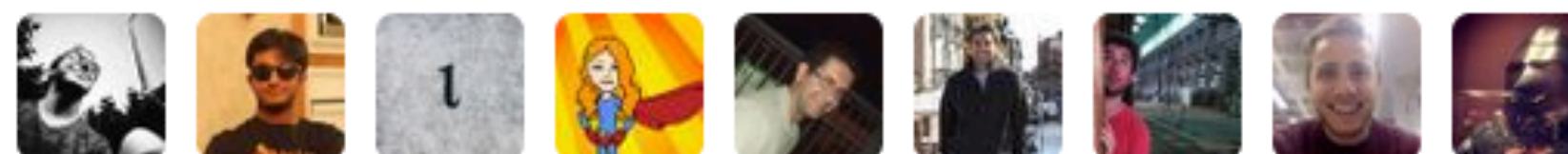
Taking away the option of deploying something without TLS forces your own developers to do it constantly, increasing empathy for the user.

RETWEETS

12

LIKES

29



8:02 PM - 26 Mar 2017



12



29



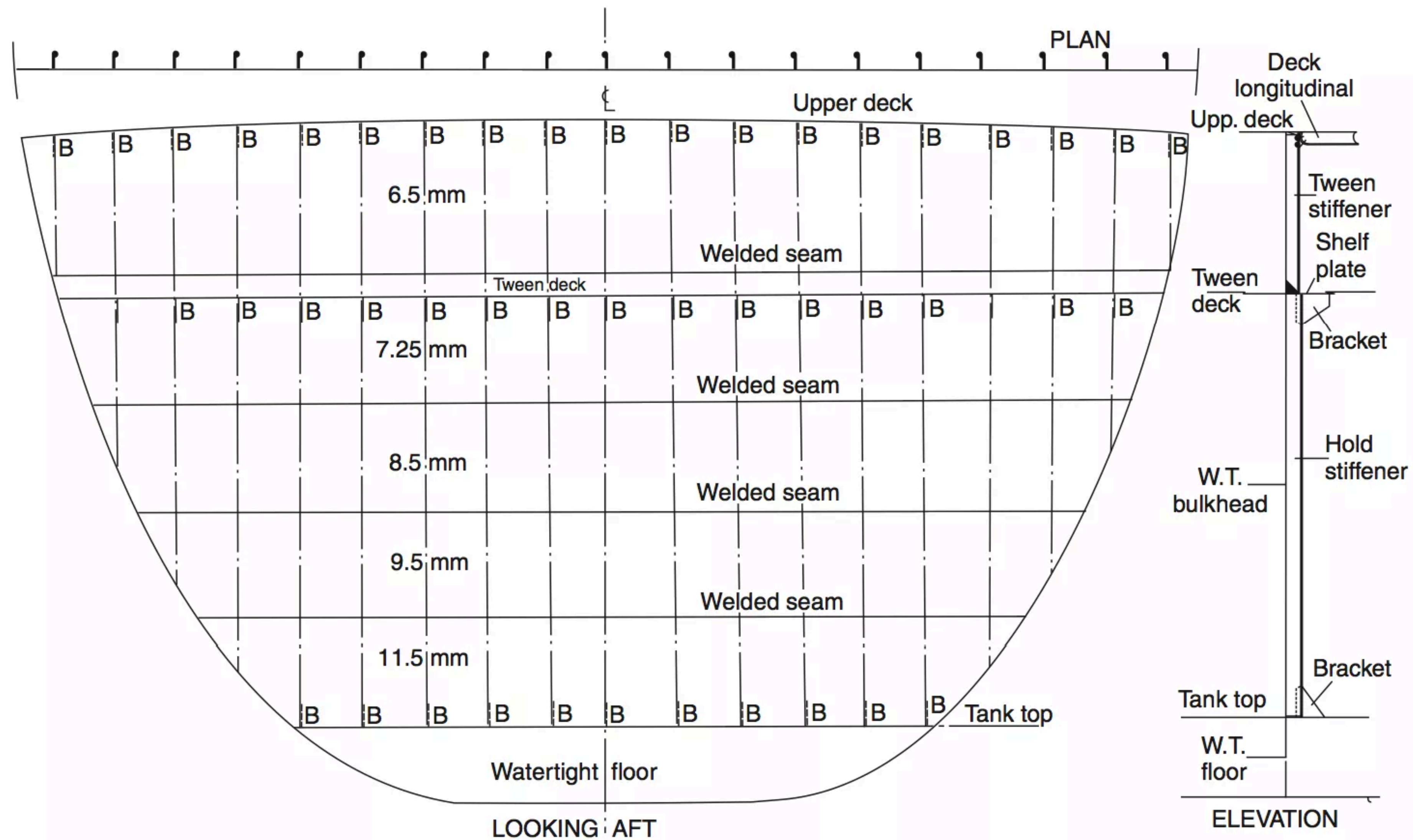


FIGURE 18.1 Plain watertight bulkhead

Thank you!

@ryankaz42