

Instantly share code, notes, and snippets.



roycewilliams / badrabbit-info.txt

Last active 2 years ago

☆ Star 24

🍴 Fork 1

<> Code

🔄 Revisions

96

☆ Stars

23

🍴 Forks

1

Embed ▾

<script src="https://



Download ZIP

badrabbit-info.txt

<> badrabbit-info.txt

Raw

```
1  Rough summary of developing BadRabbit info
2  -----
3
4  BadRabbit is locally-self-propagating ransomware (ransom: 0.05 BTC), spreading via SMB once inside.
5  Requires user interaction.
6  Mostly targeting Russia and Ukraine so far, with a few others (Germany, Turkey, Bulgaria, Montenegro ...)
7  Not globally self-propagating, but could be inflicted on selected targets on purpose.
8  May be part of same group targeting Ukraine generally (BACKSWING) (per FireEye)
9  Confirmed to use ETERNALROMANCE exploit, and same source code and build chain as NotPetya (per Talos)
10 Mitigations are similar to Petya/NotPetya resistance. An inoculation is also available (see below).
11 Supporting infrastructure shut down a few hours after starting (per Beaumont, Motherboard)
12 Very cool diagram of infection flow at Endgame by @malwareunicorn:
13     https://www.endgame.com/blog/technical-blog/badrabbit-technical-analysis
14
15 Initial infection:
16
17     Watering-hole attack, sourced from compromised media/news sites in selected regions.
18     Poses as fake Flash update.
19         https://twitter.com/jiriativirlab/status/922835700873158661/photo/1
20         https://twitter.com/darienhuss/status/922847966767042561
21     Watering-hole-style / drive-by likely, but may also be selectively targeted.
22     Beaumont (GossiTheDog) suspects supply-chain tampering or injection (it appears to be self-limiting w/shutdown, etc.)
23
24 Targets/victims
25
26     Mostly affecting .ru/.ua so far. Media outlets, transportation, gov may have been early targets.
27     Watering holes in Germany, Turkey, Bulgaria, Montenegro.
28     Avast says also Poland and South Korea?
29     Good summray thread of country coverage from @Steve3D and contributors (no US *infections* known)
30         https://twitter.com/SteveD3/status/923186304963284992
31     Avast says some US have been detected (as @Steve3D notes, detected != infected)
32     McAfee says no US detected yet
33         https://twitter.com/avast_antivirus/status/922941896439291904
34         https://twitter.com/SteveD3/status/922964771967848449
35     Check Point says some US detections
36         https://twitter.com/Bing_Chris/status/923204408539844609
37     Map (indirectly sourced from Avast PR?)
38         https://twitter.com/Bing_Chris/status/922932810725326848
39     Better source, later in the timeline:
40         https://blog.avast.com/its-rabbit-season-badrabbit-ransomware-infects-airports-and-subways
41
42 List of targeted file extensions:
43     Image Tweet: https://twitter.com/craiu/status/922877184494260227
44     Text: https://pastebin.com/CwZfyY2F
45
46 Components and methods:
47
48     Using legit signed DiskCryptor binary to encrypt.
49     Encrypts using AES-128-CBC (per Kaspersky article)
50     Creates scheduled task to reboot the target system.
51     May be using EternalBlue (or at least triggers controls that are watching for its use?), Unit 42 sees no sign of this
52     Incorporates stripped-down Mimikatz to discover credentials for propagation.
53         https://twitter.com/gentilkiwi/status/922945304172875778
54     Named "rabbitlib.dll"
55         https://twitter.com/cherepanov74/status/923207933332283392
56     Overwrites MBR to deliver ransom message.
```

```
57 Ransom message directs users to Tor-based (.onion) site
58 Gives a "please turn off antivirus" user message in some circumstances.
59
60 Also spreads via SMB and WebDAV - locally self-propagating
61 https://twitter.com/GossiTheDog/status/922875805033730048
62
63 Also uses this hard-coded list of creds:
64 https://pastebin.com/01C05L0C
65 https://twitter.com/MaartenVDantzig/status/922854232176422912
66
67 C:\WINDOWS\cscc.dat == DiskCryptor (block execution to inoculate?)
68 https://www.virustotal.com/#/file/682adcb55fe4649f7b22505a54a9dbc454b4090fc2bb84af7db5b0908f3b7806/details
69
70 C:\Windows\infpub.dat == #BADRABBIT pushed laterally (block execution to inoculate?)
71 Creating a read-only version of this file may halt infection; more below
72 https://twitter.com/0xAmit/status/922886907796819968
73
74 Analysis of flash_install.php component
75 https://www.hybrid-analysis.com/sample/630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da?environmentId=100
76
77 Video of action:
78 https://twitter.com/GossiTheDog/status/922858264534142976
79
80 Apparently clears Windows logs and the filesystem journal, per ESET and Carbon Black
81 Uses wevtutil cmdline
82
83 Appears to be McAfee-aware:
84 https://twitter.com/ValthekOn/status/923143946796183552
85
86 May incorporate copy-and-pasted Microsoft cert/signing?
87 https://twitter.com/gN3mes1s/status/922907460842721281
88 @mattifestation PS script to search for other use:
89 https://gist.github.com/mattifestation/f76c64e87daa40f0d740cb037e575e96
90 https://gist.github.com/mattifestation/225c9b4e38b5d11a488bf5c1ccda99cb
91
92 Also installs a keylogger? [source?]
93 (The Register mentions this third-hand)
94
95 Wipes boot sector and puts kernel at the end of the drive?
96
97 C&C and payload domains were set up well in advance:
98 https://twitter.com/mrjohnkelly73/status/922899328636735488
99 https://twitter.com/craiu/status/922911496497238021
100
101 Unlike NotPetya, confirmed to be decrypt-ready:
102 https://twitter.com/antonivanovm/status/922944062935707648 (Kaspersky)
103
104 13% code reuse of notpeyta
105 https://analyze.intezer.com/#/analyses/d41e8a98-a106-4b4f-9b7c-fd9e2c80ca7d
106
107 Good analysis from @bartblaze of similarities between NotPetya and BadRabbit:
108 https://bartblaze.blogspot.com/2017/10/comparing-eternalpetya-and-badrabbit.html
109
110 May be a variant of Diskcoder, per ESET
111
112 LIVE SAMPLE (see tweet for password, use at your own risk):
113 https://twitter.com/gentilkiwi/status/922944766161154053
114
115 Still contains link to external debugging symbols file (.pdb) [can this be manipulated?] (@malwareunicorn):
116 https://twitter.com/malwareunicorn/status/923009391770533888
117
118 Shut down a few hours after starting:
119 https://twitter.com/GossiTheDog/status/923300443962335232
120
121 Pop-culture references contained:
122 Game of Thrones dragons (Drogon, Rhaegal)
123 Hackers movie (bottom of list of hard-coded passwords)
124
125 Detection:
126 Yara rule (from a McAfee lead engineer)
127 https://pastebin.com/Y7pJv3tK
128 Another Yara, including Mimikatz:
129 https://github.com/Neo23x0/signature-base/blob/master/yara/crime_badrabbit.yar
130
```

```
131     IOCs (via ESET)
132
133     79116fe99f2b421c52ef64097f0f39b815b20907      infopub.dat      Win32/Diskcoder.D      Diskcoder
134     afeee8b4acff87bc469a6f0364a81ae5d60a2add      dispci.exe      Win32/Diskcoder.D      Lockscreen
135     413eba3973a15c1a6429d9f170f3e8287f98c21c      Win32/RiskWare.Mimikatz.X      Mimikatz (32-bits)
136     16605a4a29a101208457c47ebfde788487be788d      Win64/Riskware.Mimikatz.X      Mimikatz (64-bits)
137     de5c8d858e6e41da715dca1c019df0bfb92d32c0      install_flash_player.exe      Win32/Diskcoder.D      Dropper
138     4f61e154230a64902ae035434690bf2b96b4e018      page-main.js      JS/Agent.NWC      JavaScript on compromised s
139
140     fbbdc39af1139aebba4da004475e8839
141     b14d8faf7f0cbcfad051cefe5f39645f
142     caforssztxqzf2nm[.]onion
143     1dnscontrol[.]com/flash_install.php
144     1dnscontrol[.]com/install_flash_player.exe
145     630325cac09ac3fab908f903e3b00d0dadadd5fdaa0875ed8496fcbb97a558d0da
146
147     Defense
148     (via @GossitheDog):
149     * block inbound SMB
150     * use Credential Guard in Windows
151     * control # of admins
152     * monitor scheduled tasks and service creation
153
154     Vaccination: https://twitter.com/0xAmit/status/922911491694694401
155     ** Create the following files c:\windows\infpub.dat && c:\windows\cscd.dat
156     ** remove ALL PERMISSIONS (inheritance) and you are now vaccinated. :)
157
158     Carbon Black:
159     * Patch for MS17-010
160     * Use GPO to disable access to admin shares.
161     https://social.technet.microsoft.com/Forums/windows/en-US/251f0f40-ffbf-4441-ba35-3dd1acd7a445/how-can-we-disable-the-autom
162
163     Other ideas:
164     * Disable WMI where feasible
165
166     Money trail
167     Bitcoin addresses (h/t: @Steve3D)
168     https://blockchain.info/address/1GxXGMoz7HAVvRDZd7ezkKipY4DHLUqzmM
169     https://blockchain.info/address/17GhezAiRhgB8DGArcZXBkrZBFTGCC9SQ2Z
170
171     Only a few transactions (@ChristiaanBeek):
172     https://twitter.com/ChristiaanBeek/status/923264222699585536
173
174     Coverage and news
175
176     ESET (very good tech coverage):
177     https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back-improved-ransomware/
178
179     The Register (good tech summary):
180     https://www.theregister.co.uk/2017/10/24/badrabbit_ransomware/
181
182     Steve Ragan article (excellent, being updated rapidly)
183     https://www.csoonline.com/article/3234691/security/badrabbit-ransomware-attacks-multiple-media-outlets.html
184
185     Watch @GossiTheDog on Twitter for updates.
186     https://twitter.com/GossiTheDog
187
188     Palo Alto analysis (Unit 42):
189     https://researchcenter.paloaltonetworks.com/2017/10/threat-brief-information-bad-rabbit-ransomware-attacks/
190     ... and Palo Alto protections:
191     https://researchcenter.paloaltonetworks.com/2017/10/palo-alto-networks-protections-bad-rabbit-ransomware-attacks/
192
193     Group-IB (first to alert/discover):
194     https://www.group-ib.com/blog/badrabbit
195
196     Microsoft malware entry
197     https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Tibbar.A
198
199     Kaspersky:
200     https://www.kaspersky.com/blog/bad-rabbit-ransomware/19887/
201     https://securelist.com/bad-rabbit-ransomware/82851
202
203     Avast:
204     https://blog.avast.com/its-rabbit-season-badrabbit-ransomware-infects-airports-and-subways
```

```
205
206 McAfee:
207     https://securingtomorrow.mcafee.com/mcafee-labs/badrabbit-ransomware-burrows-russia-ukraine/
208
209 Cisco/Talos:
210     http://blog.talosintelligence.com/2017/10/bad-rabbit.html
211
212 Carbon Black:
213     https://www.carbonblack.com/2017/10/24/threat-advisory-analysis-bad-rabbit-ransomware/
214
215 Motherboard articles:
216     https://motherboard.vice.com/en_us/article/59yb4q/bad-rabbit-petya-ransomware-russia-ukraine
217     https://motherboard.vice.com/en_us/article/d3dp5q/infrastructure-for-the-bad-rabbit-ransomware-appears-to-have-shut-down
218
219 Symantec:
220     https://www.symantec.com/connect/blogs/badrabbit-new-strain-ransomware-hits-russia-and-ukraine
221
222 BleepingComputer article:
223     https://www.bleepingcomputer.com/news/security/bad-rabbit-ransomware-outbreak-hits-eastern-europe/
224
225 AlienVault matrix:
226     https://otx.alienvault.com/pulse/59ef5e053db003162704fcb2/
227
228 US-CERT notice:
229     https://www.us-cert.gov/ncas/current-activity/2017/10/24/Multiple-Ransomware-Infections-Reported
230
231 Threatpost:
232     https://threatpost.com/badrabbit-ransomware-attacks-hitting-russia-ukraine/128593/
233
234 The Hacker News:
235     https://thehackernews.com/2017/10/bad-rabbit-ransomware-attack.html
236
237 FireEye:
238     https://www.fireeye.com/blog/threat-research/2017/10/backswing-pulling-a-badrabbit-out-of-a-hat.html
239
240 Cylance:
241     https://www.cylance.com/en_us/blog/threat-spotlight-bad-rabbit-ransomware.html
242
243 PC Magazine:
244     https://www.pcmag.com/news/356977/badrabbit-ransomware-targets-systems-in-russia-ukraine
245
246 Cybereason (vaccine approach):
247     https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomware
248
249 MIT Technology Review:
250     https://www.technologyreview.com/the-download/609206/a-new-strain-of-ransomware-is-hitting-eastern-europe/
251
252 Malwarebytes (@hasherezade):
253     https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/
254
255 RiskIQ:
256     https://www.riskiq.com/blog/labs/badrabbit/
257
258 Endgame analysis (@malwareunicorn):
259     https://www.endgame.com/blog/technical-blog/badrabbit-technical-analysis
260
261 Qualys:
262     https://threatprotect.qualys.com/2017/10/24/bad-rabbit-ransomware/
263     https://blog.qualys.com/news/2017/10/24/bad-rabbit-ransomware
264
265 Intezer (code reuse analysis):
266     http://www.intezer.com/notpetya-returns-bad-rabbit/
267
268 cert.ro (larger list of sites):
269     https://cert.ro/citeste/bad-rabbit-o-noua-campanie-ransomware
270
271 Hackplayers (Spanish - in fact, it looks like they translated an earlier version of my document!)
272     http://www.hackplayers.com/2017/10/badrabbit-que-es-lo-que-hay-que-saber-de-momento.html
```



DavidBuchanan314 commented on Oct 25, 2017 • edited by roycewilliams ▾



ransom: \$0.05 BTC

Is that BTC or USD?

[Royce: heh - BTC; good catch, fixed!]



xl-tech commented on Oct 25, 2017 • edited by roycewilliams ▾

...

Great, because of this I can't boot to my encrypted partition, Windows Defender deleted DiskCryptor bootloader. And now legit DiskCryptor detected as trojan...

[Royce: yikes, that's terrible. Could you post something independently (not in this thread) that demonstrates this problem, so that I can link to it? If verifiable, this is important for people to know.]



snakems commented on Oct 25, 2017 • edited by roycewilliams ▾

...

Unlike NetPetya, confirmed to be decrypt-ready:

May be NotPetya ?

[Royce: indeed, good catch - fixed!]



xl-tech commented on Oct 26, 2017

...

Post about deleted bootloader (in russian, with translate) https://translate.google.com/translate?sl=auto&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=https%3A%2F%2Fhabrahabr.ru%2Fpost%2F340940%2F&edit-text=



ralf44 commented on Oct 26, 2017 • edited ▾

...

@roycewilliams Win 7 HP 64 SP1 with DiskCryptor - system rebooted yesterday (25th) and could not login to Windows again. Managed to launch in Safe Mode and checked to find the DiskCryptor Bootloader had been damaged or wiped from my Boot Drive MBR. Reinstalled a bootloader using DiskCryptor and rebooted.

Thanks to the comment above and your detailed resources on how to spot real BadRabbit, I found that Microsoft Security Essentials absolutely does have the wrong detection heuristics.

The two telltale files in C:Windows that BadRabbit drops were never there. MSE current version identifies legit DiskCryptor bootloaders as "Ransom:DOS/Tibbar.A" and removes them.

Evidence: <https://imgur.com/a/idMuk>

Since I am on Win7 and first report above is about a slightly different MS antivirus product, this is a major SNAFU which can render computers unusable. If my C: drive had been encrypted as well as my data drives, I don't think I could even have got as far as Safe Mode so the threat level of this hasty action by MS is severe.

Advise anyone using DiskCryptor to make a bootable CD or USB loader as backup and if you know how to contact anyone at MS Security directly or Tweet at the right folks, please do so!

PS - line 27 "summary".

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

