GitHub Gist Search... All gists Back to GitHub Sign in Sign up

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 : Download ZIP

badrabbit-info.txt

badrabbit-info.txt Raw

```
Rough summary of developing BadRabbit info
------------------------------------------


BadRabbit is locally-self-propagating ransomware (ransom: 0.05 BTC), spreading via SMB once inside.
Requires user interaction.
Mostly targeting Russia and Ukraine so far, with a few others (Germany, Turkey, Bulgaria, Montenegro ..
Not globally self-propagating, but could be inflicted on selected targets on purpose.
May be part of same group targeting Ukraine generally (BACKSWING) (per FireEye)
Confirmed to use ETERNALROMANCE exploit, and same source code and build chain as NotPetya (per Talos)
Mitigations are similar to Petya/NotPetya resistance. An inoculation is also available (see below).
Supporting infrastructure shut down a few hours after starting (per Beaumont, Motherboard)
Very cool diagram of infection flow at Endgame by @malwareunicorn:
    https://www.endgame.com/blog/technical-blog/badrabbit-technical-analysis

Initial infection:

    Watering-hole attack, sourced from compromised media/news sites in selected regions.
    Poses as fake Flash update.
        https://twitter.com/jiriatvirlab/status/922835700873158661/photo/1
        https://twitter.com/darienhuss/status/922847966767042561
    Watering-hole-style / drive-by likely, but may also be selectively targeted.
    Beaumont (GossiTheDog) suspects supply-chain tampering or injection (it appears to be self-limiting

Targets/victims

    Mostly affecting .ru/.ua so far. Media outlets, transportation, gov may have been early targets.
    Watering holes in Germany, Turkey, Bulgaria, Montenegro.
    Avast says also Poland and South Korea?
    Good summray thread of country coverage from @Steve3D and contributors (no US *infections* known)
        https://twitter.com/SteveD3/status/923186304963284992
    Avast says some US have been detected (as @Steve3D notes, detected != infected)
        McAfee says no US detected yet
        https://twitter.com/avast_antivirus/status/922941896439291904
        https://twitter.com/SteveD3/status/922964771967848449
        Check Point says some US detections
                https://twitter.com/Bing_Chris/status/923204408539844609
    Map (indirectly sourced from Avast PR?)
        https://twitter.com/Bing_Chris/status/922932810725326848
        Better source, later in the timeline:
            https://blog.avast.com/its-rabbit-season-badrabbit-ransomware-infects-airports-and-subways

List of targeted file extensions:
        Image Tweet: https://twitter.com/craiu/status/922877184494260227
        Text: https://pastebin.com/CwZfyY2F

Components and methods:

    Using legit signed DiskCryptor binary to encrypt.
    Encrypts using AES-128-CBC (per Kaspersky article)
    Creates scheduled task to reboot the target system.
    May be using EternalBlue (or at least triggers controls that are watching for its use?), Unit 42 se
    Incorporates stripped-down Mimikatz to discover credentials for propagation.
        https://twitter.com/gentilkiwi/status/922945304172875778
        Named "rabbitlib.dll"
            https://twitter.com/cherepanov74/status/923207933332283392
    Overwrites MBR to deliver ransom message.
    Ransom message directs users to Tor-based (.onion) site
    Gives a "please turn off antivirus" user message in some circumstances.

    Also spreads via SMB and WebDAV - locally self-propagating
        https://twitter.com/GossiTheDog/status/922875805033730048

    Also uses this hard-coded list of creds:
        https://pastebin.com/01C05L0C
        https://twitter.com/MaartenVDantzig/status/922854232176422912

    C:\WINDOWS\cscc.dat == DiskCryptor (block execution to inoculate?)
        https://www.virustotal.com/#/file/682adcb55fe4649f7b22505a54a9dbc454b4090fc2bb84af7db5b0908f3b7

    C:\Windows\infpub.dat == #BADRABBIT pushed laterally (block execution to inoculate?)
        Creating a read-only version of this file may halt infection; more below
        https://twitter.com/0xAmit/status/922886907796819968
```

```

Analysis of flash_install.php component
    https://www.hybrid-analysis.com/sample/630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97

Video of action:
    https://twitter.com/GossiTheDog/status/922858264534142976

Apparently clears Windows logs and the filesystem journal, per ESET and Carbon Black
    Uses wevtutil cmdline

Appears to be McAfee-aware:
    https://twitter.com/ValthekOn/status/923143946796183552

May incorporate copy-and-pasted Microsoft cert/signing?
    https://twitter.com/gN3mes1s/status/922907460842721281
    @mattifestation PS script to search for other use:
        https://gist.github.com/mattifestation/f76c64e87daa40f0d740cb037e575e96
    https://gist.github.com/mattifestation/225c9b4e38b5d11a488bf5c1ccda99cb

Also installs a keylogger? [source?]
    (The Register mentions this third-hand)

Wipes boot sector and puts kernel at the end of the drive?

C&C and payload domains were set up well in advance:
    https://twitter.com/mrjohnkelly73/status/922899328636735488
    https://twitter.com/craiu/status/922911496497238021

Unlike NotPetya, confirmed to be decrypt-ready:
    https://twitter.com/antonivanovm/status/922944062935707648 (Kaspersky)

13% code reuse of notpeyta
    https://analyze.intezer.com/#/analyses/d41e8a98-a106-4b4f-9b7c-fd9e2c80ca7d

Good analysis from @bartblaze of similarities between NotPetya and BadRabbit:
    https://bartblaze.blogspot.com/2017/10/comparing-eternalpetya-and-badrabbit.html

May be a variant of Diskcoder, per ESET

LIVE SAMPLE (see tweet for password, use at your own risk):
    https://twitter.com/gentilkiwi/status/922944766161154053

Still contains link to external debugging symbols file (.pdb) [can this be manipulated?] (@malwareu
    https://twitter.com/malwareunicorn/status/923009391770533888

    Shut down a few hours after starting:
        https://twitter.com/GossiTheDog/status/923300443962335232

    Pop-culture references contained:
        Game of Thrones dragons (Drogon, Rhaegal)
        Hackers movie (bottom of list of hard-coded passwords)

Detection:
    Yara rule (from a McAfee lead engineer)
        https://pastebin.com/Y7pJv3tK
    Another Yara, including Mimikatz:
        https://github.com/Neo23x0/signature-base/blob/master/yara/crime_badrabbit.yar

    IOCs (via ESET)

    79116fe99f2b421c52ef64097f0f39b815b20907    infopub.dat                     Win32/Diskcoder.D
    afeee8b4acff87bc469a6f0364a81ae5d60a2add    dispci.exe                      Win32/Diskcoder.D
    413eba3973a15c1a6429d9f170f3e8287f98c21c    Win32/RiskWare.Mimikatz.X       Mimikatz (32-bits)
    16605a4a29a101208457c47ebfde788487be788d    Win64/Riskware.Mimikatz.X       Mimikatz (64-bits)
    de5c8d858e6e41da715dca1c019df0bfb92d32c0    install_flash_player.exe        Win32/Diskcoder.D
    4f61e154230a64902ae035434690bf2b96b4e018    page-main.js                    JS/Agent.NWC

        fbbdc39af1139aebba4da004475e8839
        b14d8faf7f0cbcfad051cefe5f39645f
        caforssztxqzf2nm[.]onion
        1dnscontrol[.]com/flash_install.php
        1dnscontrol[.]com/install_flash_player.exe
        630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da

Defense
    (via @GossitheDog):
    * block inbound SMB
    * use Credential Guard in Windows
    * control # of admins
    * monitor scheduled tasks and service creation

    Vaccination: https://twitter.com/0xAmit/status/922911491694694401
    ** Create the following files c:\windows\infpub.dat && c:\windows\cscc.dat
    ** remove ALL PERMISSIONS (inheritance) and you are now vaccinated. :)

    Carbon Black:
    * Patch for MS17-010
    * Use GPO to disable access to admin shares.
        https://social.technet.microsoft.com/Forums/windows/en-US/251f0f40-ffbf-4441-ba35-3dd1acd7a445/
    Other ideas:
    * Disable WMI where feasible

Money trail
    Bitcoin addresses (h/t: @Steve3D)
    https://blockchain.info/address/1GxXGMoz7HAVwRDZd7ezkKipY4DHLUqzmM
    https://blockchain.info/address/17GhezAiRhgB8DGArZXBkrZBFTGCC9SQ2Z

    Only a few transactions (@ChristiaanBeek):
        https://twitter.com/ChristiaanBeek/status/923264222699585536

Coverage and news

    ESET (very good tech coverage):
        https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back-improved-ransomware/

    The Register (good tech summary):
        https://www.theregister.co.uk/2017/10/24/badrabbit_ransomware/

    Steve Ragan article (excellent, being updated rapidly)
        https://www.csoonline.com/article/3234691/security/badrabbit-ransomware-attacks-multiple-media-

    Watch @GossiTheDog on Twitter for updates.
        https://twitter.com/GossiTheDog

    Palo Alto analysis (Unit 42):
        https://researchcenter.paloaltonetworks.com/2017/10/threat-brief-information-bad-rabbit-ransomwa
    ... and Palo Alto protections:
        https://researchcenter.paloaltonetworks.com/2017/10/palo-alto-networks-protections-bad-rabbit-r

    Group-IB (first to alert/discover):
        https://www.group-ib.com/blog/badrabbit

    Microsoft malware entry
        https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32

    Kaspersky:
        https://www.kaspersky.com/blog/bad-rabbit-ransomware/19887/
        https://securelist.com/bad-rabbit-ransomware/82851

    Avast:
        https://blog.avast.com/its-rabbit-season-badrabbit-ransomware-infects-airports-and-subways

    McAfee:
        https://securingtomorrow.mcafee.com/mcafee-labs/badrabbit-ransomware-burrows-russia-ukraine/

    Cisco/Talos:
        http://blog.talosintelligence.com/2017/10/bad-rabbit.html

    Carbon Black:
        https://www.carbonblack.com/2017/10/24/threat-advisory-analysis-bad-rabbit-ransomware/

    Motherboard articles:
        https://motherboard.vice.com/en_us/article/59yb4q/bad-rabbit-petya-ransomware-russia-ukraine
        https://motherboard.vice.com/en_us/article/d3dp5q/infrastructure-for-the-bad-rabbit-ransomware-

    Symantec:
        https://www.symantec.com/connect/blogs/badrabbit-new-strain-ransomware-hits-russia-and-ukraine

    BleepingComputer article:
        https://www.bleepingcomputer.com/news/security/bad-rabbit-ransomware-outbreak-hits-eastern-euro

    AlienVault matrix:
        https://otx.alienvault.com/pulse/59ef5e053db003162704fcb2/

    US-CERT notice:
        https://www.us-cert.gov/ncas/current-activity/2017/10/24/Multiple-Ransomware-Infections-Reporte

    Threatpost:
        https://threatpost.com/badrabbit-ransomware-attacks-hitting-russia-ukraine/128593/

    The Hacker News:
        https://thehackernews.com/2017/10/bad-rabbit-ransomware-attack.html

    FireEye:
        https://www.fireeye.com/blog/threat-research/2017/10/backswing-pulling-a-badrabbit-out-of-a-hat

    Cylance:
        https://www.cylance.com/en_us/blog/threat-spotlight-bad-rabbit-ransomware.html

    PC Magazine:
        https://www.pcmag.com/news/356977/badrabbit-ransomware-targets-systems-in-russia-ukraine

    Cybereason (vaccine approach):
        https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomwar

    MIT Technology Review:
        https://www.technologyreview.com/the-download/609206/a-new-strain-of-ransomware-is-hitting-east

    Malwarebytes (@hasherezade):
        https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyano

    RiskIQ:
        https://www.riskiq.com/blog/labs/badrabbit/

    Endgame analysis (@malwareunicorn):
        https://www.endgame.com/blog/technical-blog/badrabbit-technical-analysis

    Qualys:
        https://threatprotect.qualys.com/2017/10/24/bad-rabbit-ransomware/
        https://blog.qualys.com/news/2017/10/24/bad-rabbit-ransomware

    Intezer (code reuse analysis):
        http://www.intezer.com/notpetya-returns-bad-rabbit/

    cert.ro (larger list of sites):
        https://cert.ro/citeste/bad-rabbit-o-noua-campanie-ransomware

    Hackplayers (Spanish - in fact, it looks like they translated an earlier version of my document!)
        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".