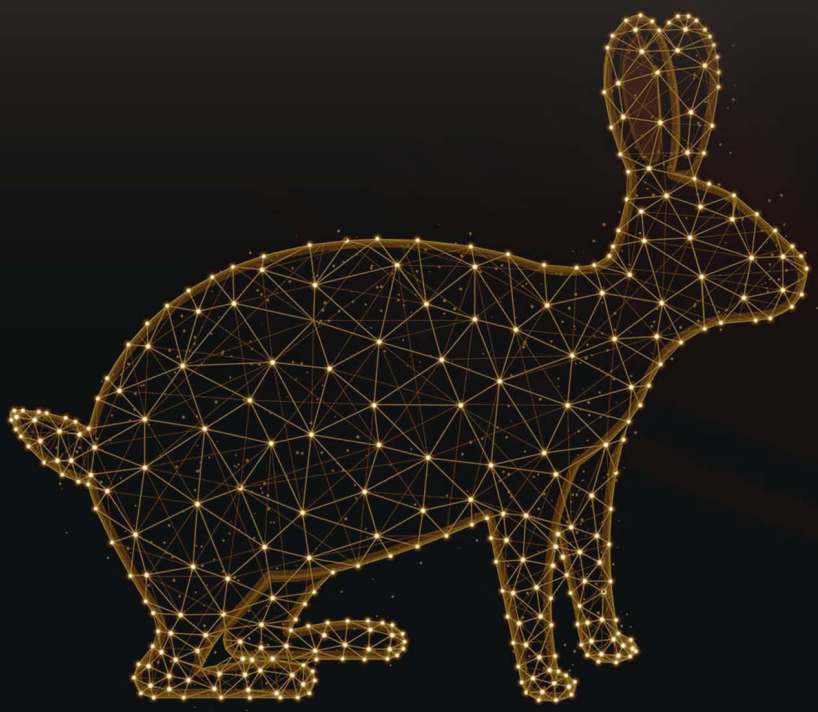
Lodestone

White Rabbit Ransomware and the F5 Backdoor



THE WHITE RABBIT RANSOMWARE AND THE F5

On December 14, 2021, the Lodestone Forensic Investigations team responded to a client whose environment was affected by what appeared to be a new strain of ransomware: White Rabbit. Lodestone identified via open-source intelligence (OSINT) that White Rabbit was first publicly disclosed on Twitter on the same date by security researcher Michael Gillespie (@demonslay355).

Based on tactics, techniques, and procedures (TTPs) observed in ongoing investigations and further research, Lodestone has determined that the White Rabbit group may be affiliated with known threat actor group FIN8. FIN8 is a financially motivated group active since 2016 that has targeted retail, restaurant, and financial institutions using social engineering and spear-phishing attacks. Additionally, FIN8 has been linked to backdoor malware PUNCHBUGGY and BADHATCH, and the memory scraping malware PUNCHTRACK. The White Rabbit ransomware group appears to have leveraged a previously unseen version of BADHATCH which, based on characteristics of the malware sample acquired, Lodestone has named F5.

Lodestone has made preliminary observations of White Rabbit behavior that are described in the text and screen captures below.

```
                  HELLO Client_Name

If you are reading this message, means that:
      - your network infrastructures have been compromised,
      - critical data has leaked,
      - files are encrypted

            â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”“
            â”ƒ         Welcome to the Ransom House          â”ƒ
            â”ƒ              You are locked by               â”ƒ
            â”ƒ           W H I T E   R A B B I T            â”ƒ
            â”ƒ      Knock, Knock. Follow the White Rabbit... â”ƒ
            â”ƒ                                              â”ƒ
            â”ƒ                   (\(\                       â”ƒ
            â”ƒ                   (-.-)                      â”ƒ
            â”ƒ                   (")(")                     â”ƒ
            â”ƒ                                              â”ƒ
            â”—â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”â”›

            The best and only thing you can do is to contact us
              to settle the matter before any losses occurs.

--------------------------------------------------------------------------

                                1. THE FOLLOWING IS STRICTLY FORBIDDEN

1.1 DELETION THIS NOTE.
                            Each note carries the encryption key
                            needed to decrypt the data,
                            don't lose it

1.2 EDITING FILES OR HDD.
                            Renaming, copying or moving any files
                            could DAMAGE the cypher and
                            decryption will be impossible.

1.3 USING THIRD-PARTY SOFTWARE.
                            Trying to recover with any software
                            can also break the cipher and
                            file recovery will become a problem.

1.4 SHUTDOWN OR RESTART THE PC.
                            Boot and recovery errors can also damage the cipher.
                            Sorry about that, but doing so is entirely at your own risk.

1.5 HIRING THE FBI AND OTHERS
                            Cooperating with the FBI|CIA and so on
                            and involving their officers in negotiations
                            will end our communication with you
                            and we will share all the leaked data for free.
```

White Rabbit Ransom Note

```
                                2. EXPLANATION OF THE SITUATION
2.1 HOW DID THIS HAPPEN

The security of your IT perimeter has been compromised (it's not perfect at all).
We encrypted your workstations and servers to make the fact of the intrusion visible and to prevent you from hiding critical data leaks.
We spent a lot of time for researching and finding out the most important directories of your business, your weak points.
We have already downloaded a huge amount of critical data and analyzed it. Now it's fate is up to you, it will either be deleted or sold, or shared with the media.

2.2 VALUABLE DATA WE USUALLY STEAL:
                            - Databases, legal documents, billings, clients personal information, SSN...
                            - Audit reports
                            - Any financial documents (Statements, invoices, accounting, transfers etc.)
                            - work files and corporate correspondence
                            - Any backups

2.3 TO DO LIST (best practies)
                            - Contact us as soon as possible
                            - Contact us only in our chat, otherwise you can run into scammers.
                            - Purchase our decryption tool and decrypt your files. There is no other way to do this.
                            - Realize that dealing with us is the shortest way to the success and secrecy.
                            - Give up the idea of using decryption help programs, otherwise you will destroy the system permanently
                            - Avoid any third-party negotiators and recovery groups. They can allow the event to leak.
```

White Rabbit Ransom Note (cont.)

```
--------------------------------------------------------------------------------------------------------------

                                        4. EVIDENCE OF THE LEAKAGE
4.1 SCREENSHOTS:
                    https://paste.pics/
                    https://paste.pics/
                    https://paste.pics/
                    https://paste.pics/
                    https://paste.pics/

4.2 DB sample:      https://file.io/
                    https://file.io/
                    Password:
--------------------------------------------------------------------------------------------------------------
```

Evidence Uploaded to Paste[.]pics and File[.]io (Redacted)

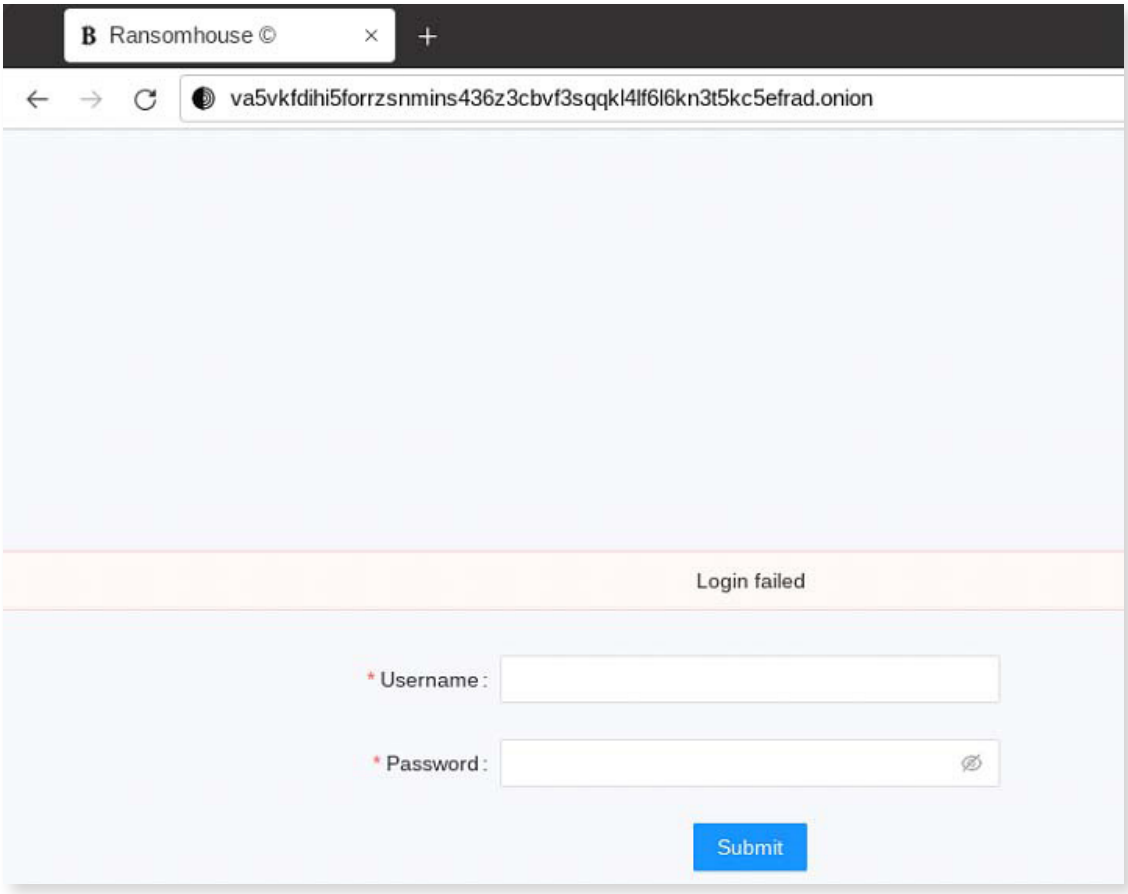
```
--------------------------------------------------------------------------------------------------------------

                                        5. HOW TO CONTACT US

5.1 Download and install TOR Browser https://torproject.org
5.2 Open our live-chat website at http://va5vkfdihi5forrzsnmins436z3cbvf3sqqkl4lf6l6kn3t5kc5efrad.onion
5.3 To review leaked data at temporarily server get the ftp access in our live chat
5.4 If the TOR Browser is restricted in your area then use VPN services
5.5 All your Data will be published in 4 Days in the case of silence on your side
5.6 Your Decryption keys will be permanently destroyed synchronous 5.5
5.7 Your Data will be published if you will hire third-party negotiators to contact us

--------------------------------------------------------------------------------------------------------------
```

TOR URL for Communication with White Rabbit (Redacted)



Login Page for White Rabbit Communication Channel

At the time of writing, the earliest evidence of compromise Lodestone has observed in its investigations was a PowerShell script that executed on July 10, 2021. An analysis of PowerShell script artifacts revealed script blocks that matched those described in a July 27, 2021, Bitdefender article on FIN8. Additional White Rabbit activity Lodestone observed occurred on December 11, 2021; while the PowerShell artifacts from this most recent event were similar to those associated with activity from August 30, 2021, these were not an exact match.

Lodestone's analysis of a White Rabbit sample from August 30, 2021, suggested that it was an updated version of FIN8's BADHATCH malware, also known as SARDONIC, that contains the following PDB path:

> "C:\Users\dev_win10_00\ Documents\Sardonic\SardonicUtility\ LoaderAssembly\obj\x86\Release\MSDAC.pdb".

The December 11, 2021, sample, however, contains the PDB path below:

> "C:\Users\dev_win10_00\Documents\f5\F5Utility\LoaderAssembly\obj\x86\Release\Default.pdb".

property	value
md5	0708B2C2F1A5F8EC8D64DB761CAF2205
sha1	C1115C834764974B131B82F8DD0DD6692AD9FD7F
sha256	F487F02E5E3F1F66DF190771DB1EF6F03BA25B9280FA27EA4AB9DF6E39C5A49C
age	1
size	122 (bytes)
format	RSDS
debugger-stamp	0xF9554826 (Sun Jul 23 16:36:54 2102 | UTC)
path	C:\Users\dev_win10_00\Documents\Sardonic\SardonicUtility\LoaderAssembly\obj\x86\Release\MSDAC.pdb
Guid	40715AA7-7E0F-474B-AAF-D12A70A3BFCE

property	value
md5	08E5F8D1EB574AF8EA81B00D859868B8
sha1	04427CE15C8AFF60C66144C68A739DC0866ED488
sha256	D96A44F8A06A1082CE94F66A21299126C568298BF76CFB1361100BDD0065DD57
age	1
size	112 (bytes)
format	RSDS
debugger-stamp	0x903DE08C (Fri Sep 07 23:04:44 2046 | UTC)
path	C:\Users\dev_win10_00\Documents\f5\F5Utility\LoaderAssembly\obj\x86\Release\Default.pdb
Guid	6174A428-40E-41EA-832-A68EB54A610

DLL Debug Information from August and December PowerShell Event Logs

The exact relationship between the White Rabbit group and FIN8 is currently unknown. However, Lodestone identified a number of TTPs suggesting that White Rabbit, if operating independently of FIN8, has a close relationship with the more established threat group or is mimicking them.

Lodestone will continue to provide updates with additional findings on this emerging threat.

INDICATORS OF COMPROMISE

IP Addresses

- 170.130.55[.]120
- 104.168.138[.]128

Domains

- 104-168.132[.]128.nip[.]io

URLs

- https://104-168-132-128.nip[.]io/51b16c
- http://va5vkfdihi5forrzsnmins436z3cbvf3sqqkl4lf6l6kn3t5kc5efrad[.]onion

Filenames

- “default.dll”

Hash Values

- 655c3c304a2fe76d178f7878d6748439 (“default.dll”)
- 6ffa106ac8d923ca32bc6162374f488b (Sardonic PowerShell script)
- fb3de0512d1ee5f615edee5ef3206a95 (Sardonic x86 DLL)
- 4a03238e31e3e90b38870ffc0a3ceb3b (Sardonic x64 DLL)
- Beffdd959b1f7e11e1c2b31af2804a07 (F5 PowerShell script)
- d9f5a846726f11ae2f785f55842c630f (F5 x86 DLL)
- 087f82581b65e3d4af6f74c8400be00e (F5 x64 DLL)

ADDITIONAL INFORMATION RESOURCES

- Michael Gillespie’s White Rabbit announcement on Twitter:

  https://twitter.com/demonslay335/status/1470823608725475334

- Bitdefender on FIN8:

  https://businessinsights.bitdefender.com/deep-dive-into-a-fin8-attack-a-forensic-investigation

  https://www.bitdefender.com/files/News/CaseStudies/study/394/Bitdefender-PR-Whitepaper-BADHATCH-creat5237-en-EN.pdf

- MITRE profile on FIN8

  https://attack.mitre.org/groups/G0061/

- PUNCHBUGGY and PUNCHTRACK

  https://www.mandiant.com/resources/windows-zero-day-payment-cards
  https://blog.morphisec.com/security-alert-fin8-is-back

www.lodestone.com
320 E. Main Street
Lewisville, TX 75057