New White Rabbit ransomware linked to FIN8 hacking group

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** January 18, 2022 11:56 AM **0**

A new ransomware family called 'White Rabbit' appeared in the wild recently, and according to recent research findings, could be a side-operation of the FIN8 hacking group.

FIN8 is a financially motivated actor who has been spotted targeting financial organizations for several years, primarily by deploying POS malware (https://www.bleepingcomputer.com/news/security/visa-warns-of-ongoing-cyber-attacks-on-gas-pump-pos-systems/) that can steal credit card details.

A simple tool to deliver double-extortion

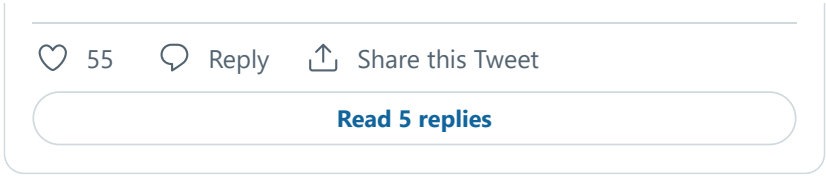
The first public mention of the White Rabbit ransomware was in a tweet by ransomware expert Michael Gillespie, seeking a sample of the malware.

Michael Gillespie
@demonslay335

🔒 #Ransomware Hunt: "White Rabbit" with extension ".scrypt", drops note for each encrypted file with "<filename>.scrypt.txt" with victim-specific information: pastebin.com/waLqSHCh
"Follow the White Rabbit..." 🐰🤔

2:30 AM · Dec 15, 2021

Read the full conversation on Twitter



In a new report by Trend Micro, researchers analyze a sample of the White Rabbit ransomware obtained during an attack on a US bank in December 2021.

The ransomware executable is a small payload, weighing in at 100 KB file, and requires a password to be entered on command line execution to decrypt the malicious payload.

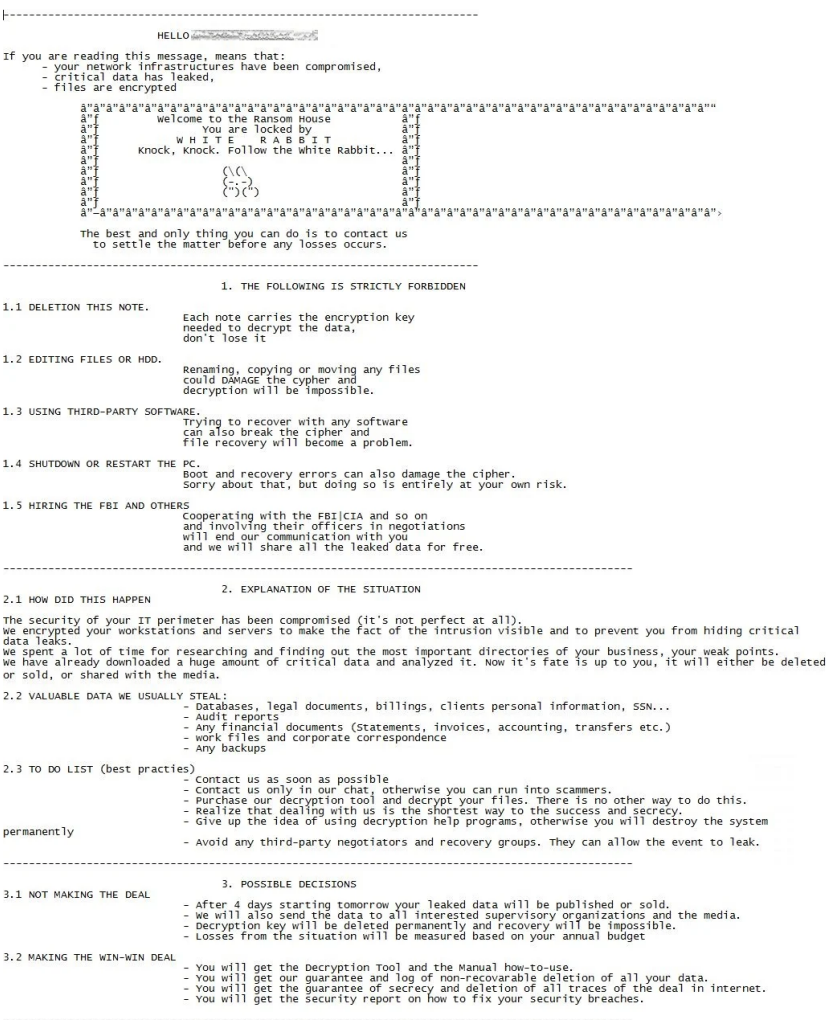
A password to execute the malicious payload has been used previously by other ransomware operations, including Egregor, MegaCortex, and SamSam (https://www.bleepingcomputer.com/news/security/new-samsam-variant-requires-special-password-before-infection/).

Once executed with the correct password, the ransomware will scan all folders on the device and encrypt targeted files, creating ransom notes for each file it encrypts.

For example, a file named test.txt would be encrypted as **test.txt.scrypt**, and a ransom note would be created named **test.txt.scrypt.txt**.

While encrypting a device, removable and network drives are also targeted, with Windows system folders excluded from encryption to prevent rendering the operating system unusable.

The ransom note informs the victim that their files had been exfiltrated and threatens to publish and/or sell the stolen data if the demands are not met.



```
                    HELLO

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

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

            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.

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

                              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.

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

                              3. POSSIBLE DECISIONS
3.1 NOT MAKING THE DEAL
                              - After 4 days starting tomorrow your leaked data will be published or sold.
                              - We will also send the data to all interested supervisory organizations and the media.
                              - Decryption key will be deleted permanently and recovery will be impossible.
                              - Losses from the situation will be measured based on your annual budget

3.2 MAKING THE WIN-WIN DEAL
                              - You will get the Decryption Tool and the Manual how-to-use.
                              - You will get our guarantee and log of non-recovarable deletion of all your data.
                              - You will get the guarantee of secrecy and deletion of all traces of the deal in internet.
                              - You will get the security report on how to fix your security breaches.

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

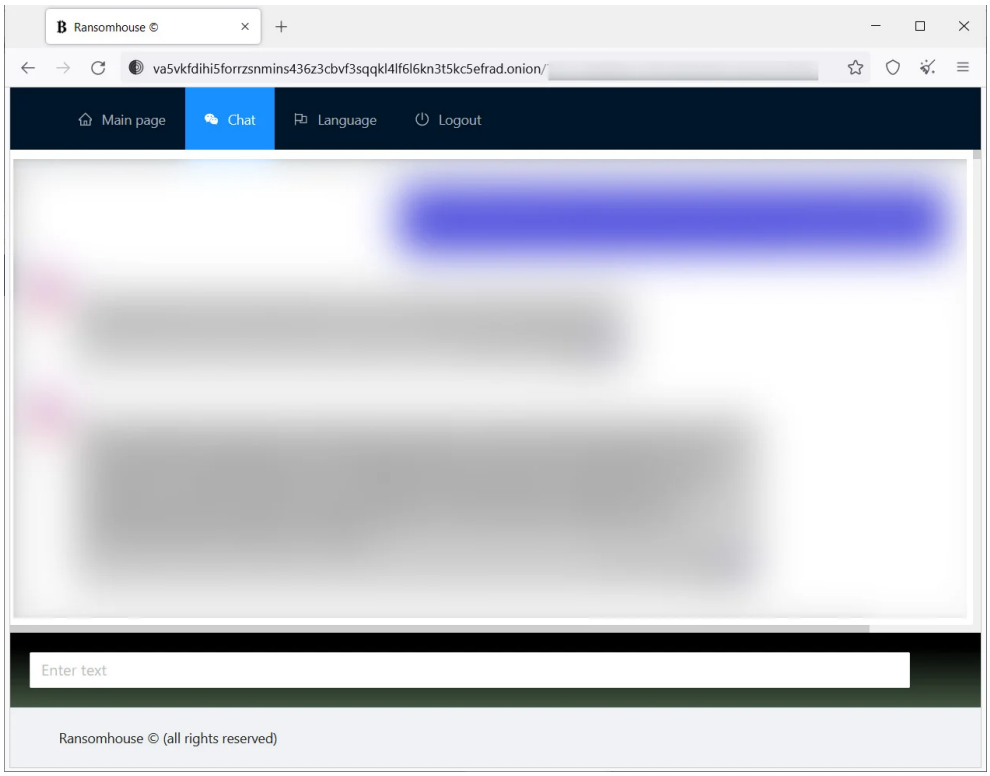
White Rabbit ransom note

Source: Trend Micro

The deadline for the victim to pay a ransom is set to four days, after which the actors threaten to send the stolen data to data protection authorities, leading to data breach GDPR penalties.

The evidence of the stolen files is uploaded to services such as 'paste[.]com' and 'file[.]io,' while the victim is offered a live chat communication channel with the actors on a Tor negotiation site.

The Tor site includes a 'Main page,' used to display proof of stolen data, and a Chat section where the victim can communicate with the threat actors and negotiate a ransom demand, as shown below.



White Rabbit's private Tor site

Links to FIN8

As noted in the Trend Micro report (https://www.trendmicro.com/en_us/research/22/a/new-ransomware-spotted-white-rabbit-and-its-evasion-tactics.html), evidence that connects FIN8 and 'White Rabbit' is found in the ransomware's deployment stage.

More specifically, the novel ransomware uses a never-before-seen version of Badhatch (aka "Sardonic (https://www.bleepingcomputer.com/news/security/fin8-cybercrime-gang-backdoors-us-orgs-with-new-sardonic-malware/)"), a backdoor associated with FIN8.

Typically, these actors keep their custom backdoors to themselves and continue to develop them privately.

This finding is also confirmed by a different report on the same ransomware family undertaken by Lodestone researchers.

They too found Badhatch in 'White Rabbit' attacks, while they also noticed PowerShell artifacts similar to FIN8-associated activity from last summer.

As the Lodestone report (https://lodestone.com/insight/white-rabbit-ransomware-and-the-f5-backdoor/) concludes: "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."

For now, White Rabbit has limited itself to only targeting a few entities but is considered an emerging threat that could turn into a severe menace to companies in the future.

At this point, it can be contained by taking standard anti-ransomware measures like the following:

- Deploy cross-layered detection and response solutions.
- Create an incident response playbook for attack prevention and recovery.
- Conduct ransomware attack simulations to identify gaps and evaluate performance.
- Perform backups, test backups, verify backups, and keep offline backups.

Related Articles:

Fashion giant Moncler confirms data breach after ransomware attack (https://www.bleepingcomputer.com/news/security/fashion-giant-moncler-confirms-data-breach-after-ransomware-attack/)

Cyber espionage campaign targets renewable energy companies (https://www.bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies/)

Microsoft: Fake ransomware targets Ukraine in data-wiping attacks (https://www.bleepingcomputer.com/news/security/microsoft-fake-ransomware-targets-ukraine-in-data-wiping-attacks/)

Russia charges 8 suspected REvil ransomware gang members (https://www.bleepingcomputer.com/news/security/russia-charges-8-suspected-revil-ransomware-gang-members/)

Qlocker ransomware returns to target QNAP NAS devices worldwide (https://www.bleepingcomputer.com/news/security/qlocker-ransomware-returns-to-target-qnap-nas-devices-worldwide/)