Hive Pro

THREAT ADVISORY

FIN8 Hacker group using new 'White Rabbit' Ransomware against U.S. Banks

TA2022014

Threat Level AMBER

Publish Date – Jan 20, 2022

White Rabbit is a ransomware family that has only recently been discovered. It could be a subsidiary project of the FIN8 hacking gang. A ransomware expert seeking for a sample of the malware made the first public disclosure of the White Rabbit ransomware in a tweet. The ransomware strain was recently deployed against a local bank in the U.S. in December 2021.

The ransomware exe is a short payload (100 KB file) that requires a password to decode the malicious payload when run from the command line. The ransomware scans all folders on the device and encrypts data, leaving ransom notes for each file it encrypts once it has been launched. A file named test[.]txt, for example, will be encrypted as test[.]txt[.]scrypt, and a ransom note called test[.]txt[.]script[.]txt will be produced.

During encrypting a device, network and removable drives are targeted as well, with Windows system directories left unencrypted to prevent the OS from becoming unusable. The ransom note informs the victim that their files or data have been stolen, and that if the demands are not met, the stolen data will be leaked or sold.

Actor Detail

Name	Target Locations	Target sectors
FIN8	United States of America	Retail, Restaurant, hospitality industries and financial institutions

Indicators of Compromises(IoCs)

Type	Value
MD5	fb3de0512d1ee5f615edee5ef3206a95, d9f5a846726f11ae2f785f55842c630f, beffdd959b1f7e11e1c2b31af2804a07, 6ffa106ac8d923ca32bc6162374f488b, 655c3c304a2fe76d178f7878d6748439, 4a03238e31e3e90b38870ffc0a3ceb3b, 087f82581b65e3d4af6f74c8400be00e,
Ipv4	170.130.55.120
SHA-256	b0844458aaa2eaf3e0d70a5ce41fc2540b7e46bdc402c798dbdfe12b59ab32c3
hostname	104-168-132-128.nip.io, 104-168.132.128.nip.io
Domain	va5vkfdihi5forrzsnmins436z3cbvf3sqqkl4lf6l6kn3t5kc5efrad.onion

References

https://www.trendmicro.com/en_nl/research/22/a/new-ransomware-spotted-white-rabbit-and-its-evasion-tactics.html
https://lodestone.com/insight/white-rabbit-ransomware-and-the-f5-backdoor/
https://thehackernews.com/2022/01/fin8-hackers-spotted-using-new-white.html
https://otx.alienvault.com/pulse/61e7f74a936eea5d44026b8e