RansomHub: New Ransomware has Origins in Older Knight

symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware

Threat Hunter TeamSymantec

RansomHub, a new Ransomware-as-a-Service (RaaS) that has rapidly become one of the largest ransomware groups currently operating, is very likely an updated and rebranded version of the older Knight ransomware.

Analysis of the RansomHub payload by Symantec, part of Broadcom, revealed a high degree of similarity between the two threats, suggesting that Knight was the starting point for RansomHub.

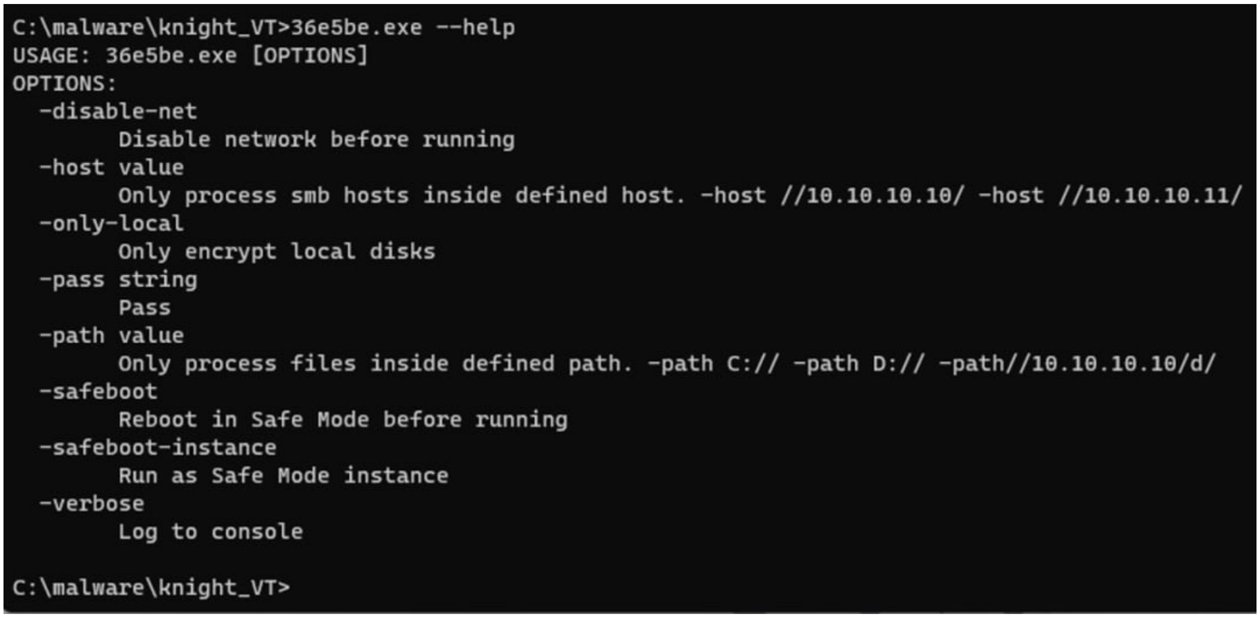
Despite shared origins, it is unlikely that Knight's creators are now operating RansomHub. Source code for Knight (originally known as Cyclops) was offered for sale on underground forums in February 2024 after Knight's developers decided to shut down their operation. It is possible that other actors bought the Knight source code and updated it before launching RansomHub.

RansomHub and Knight compared

Both payloads are written in Go and most variants of each family are obfuscated with Gobfuscate. Only some early versions of Knight are not obfuscated.

The degree of code overlap between the two families is significant, making it very difficult to differentiate between them. In many cases, a determination could only be confirmed by checking the embedded link to the data leak site.

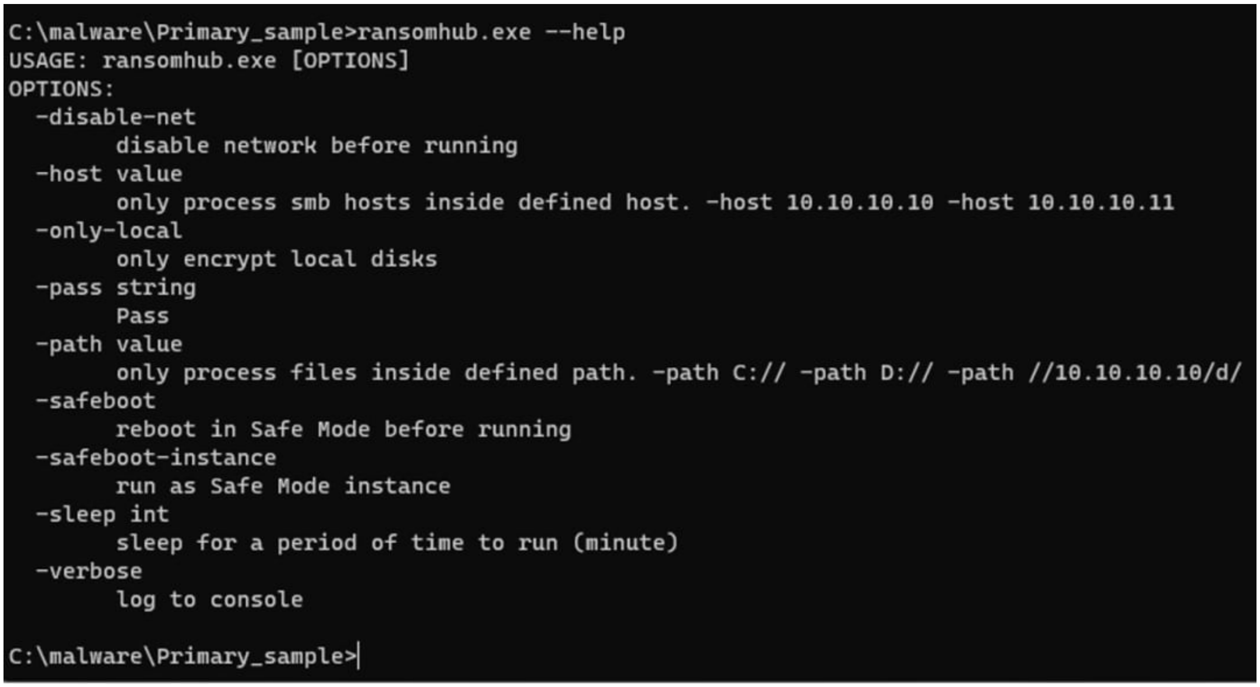
The two families have virtually identical help menus available on the command line. The sole difference is the addition of a sleep command in RansomHub.



```
C:\malware\knight_VT>36e5be.exe --help
USAGE: 36e5be.exe [OPTIONS]
OPTIONS:
  -disable-net
        Disable network before running
  -host value
        Only process smb hosts inside defined host. -host //10.10.10.10/ -host //10.10.10.11/
  -only-local
        Only encrypt local disks
  -pass string
        Pass
  -path value
        Only process files inside defined path. -path C:// -path D:// -path//10.10.10.10/d/
  -safeboot
        Reboot in Safe Mode before running
  -safeboot-instance
        Run as Safe Mode instance
  -verbose
        Log to console

C:\malware\knight_VT>
```

Figure 1. Knight command-line help menu.

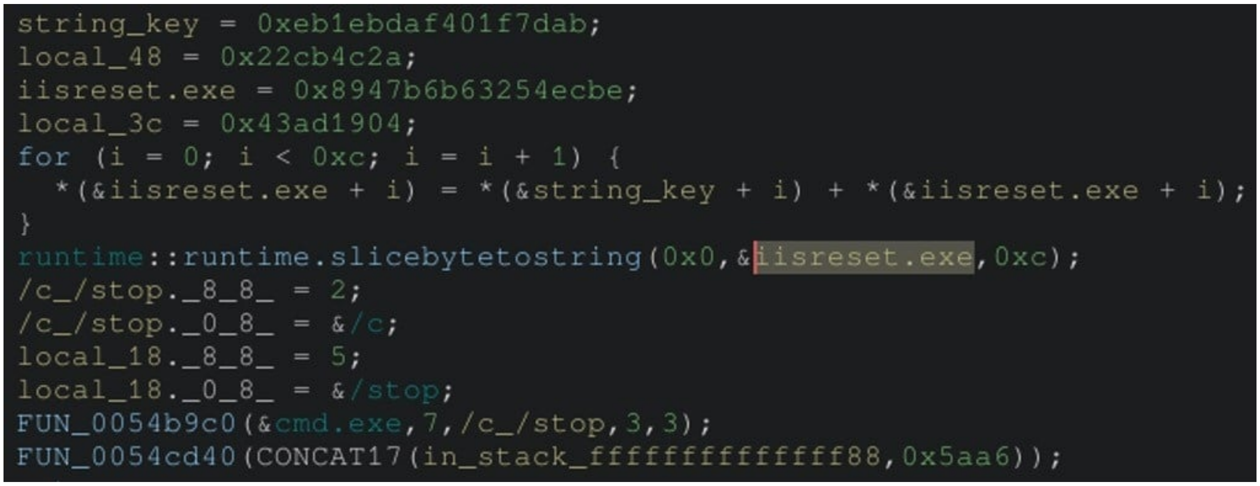


```
C:\malware\Primary_sample>ransomhub.exe --help
USAGE: ransomhub.exe [OPTIONS]
OPTIONS:
  -disable-net
        disable network before running
  -host value
        only process smb hosts inside defined host. -host 10.10.10.10 -host 10.10.10.11
  -only-local
        only encrypt local disks
  -pass string
        Pass
  -path value
        only process files inside defined path. -path C:// -path D:// -path //10.10.10.10/d/
  -safeboot
        reboot in Safe Mode before running
  -safeboot-instance
        run as Safe Mode instance
  -sleep int
        sleep for a period of time to run (minute)
  -verbose
        log to console

C:\malware\Primary_sample>
```

Figure 2. RansomHub command-line help menu.

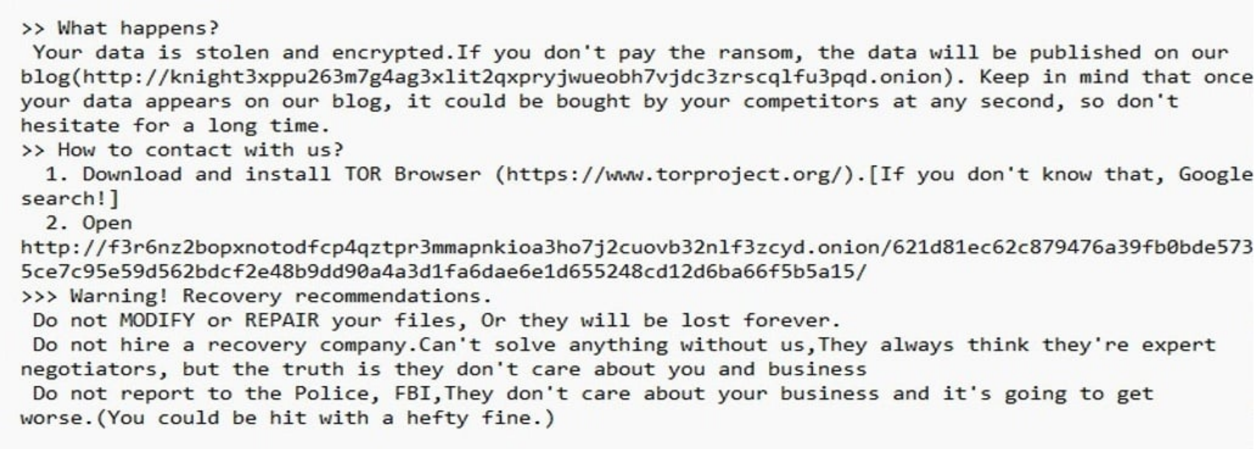
Both threats employ a unique obfuscation technique, where important strings are each encoded with a unique key and decoded at runtime. For example, in the command “cmd.exe /c iisreset.exe /stop”, only the iisrest.exe string is encrypted with a unique key.



```
string_key = 0xeb1ebdaf401f7dab;
local_48 = 0x22cb4c2a;
iisreset.exe = 0x8947b6b63254ecbe;
local_3c = 0x43ad1904;
for (i = 0; i < 0xc; i = i + 1) {
  *(&iisreset.exe + i) = *(&string_key + i) + *(&iisreset.exe + i);
}
runtime::runtime.slicebytetostring(0x0,&iisreset.exe,0xc);
/c_/stop._8_8_ = 2;
/c_/stop._0_8_ = &/c;
local_18._8_8_ = 5;
local_18._0_8_ = &/stop;
FUN_0054b9c0(&cmd.exe,7,/c_/stop,3,3);
FUN_0054cd40(CONCAT17(in_stack_ffffffffffffff88,0x5aa6));
```

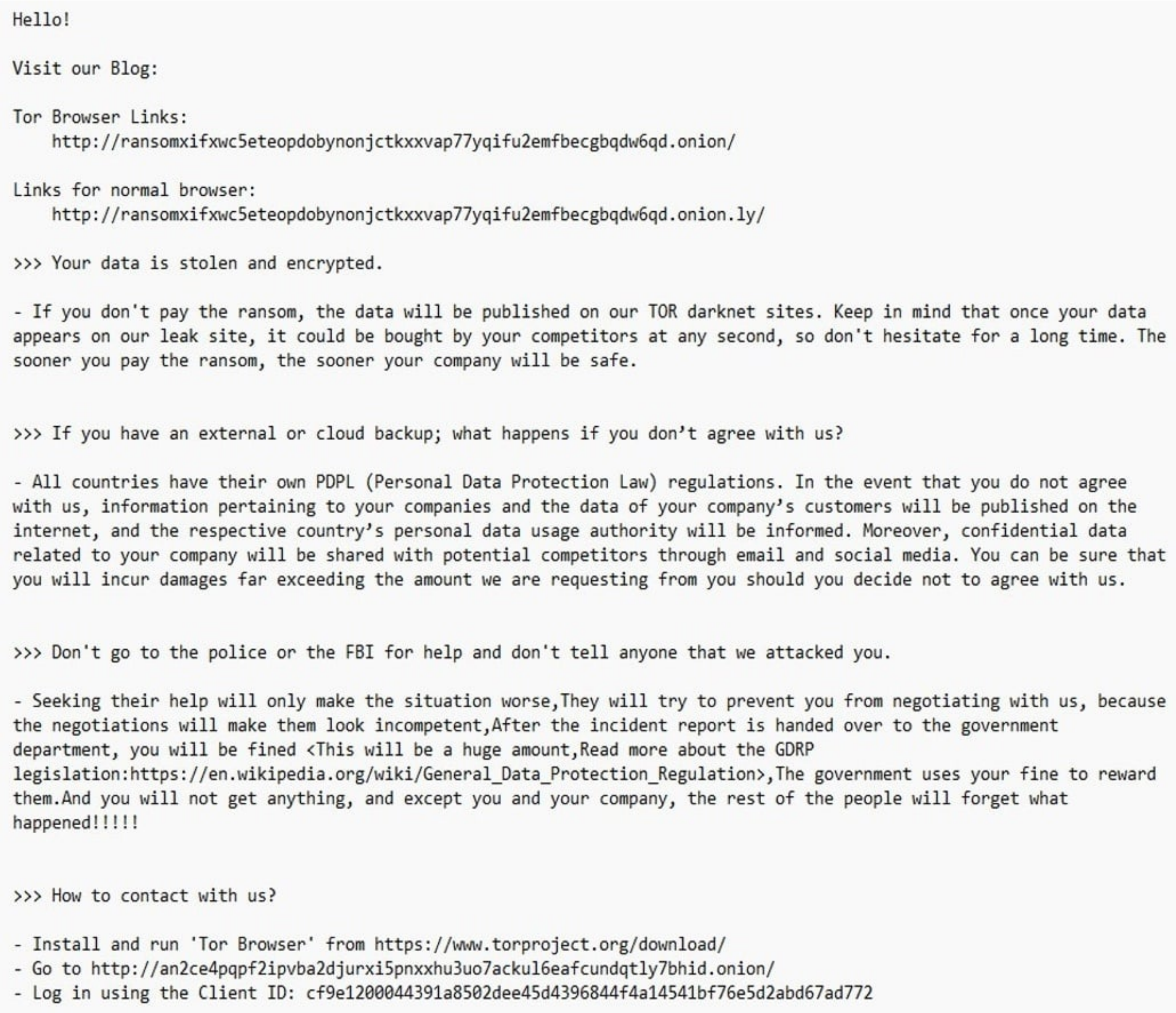
Figure 3. RansomHub string encoding. Only the iisrest.exe string is encrypted with a unique key.

There are significant similarities between the ransom notes left by both payloads, with many phrases used by Knight appearing verbatim in the RansomHub note, suggesting that the developers simply edited and updated the original note.



```
>> What happens?
 Your data is stolen and encrypted.If you don't pay the ransom, the data will be published on our
blog(http://knight3xppu263m7g4ag3xlit2qxpryjwueobh7vjdc3zrscqlfu3pqd.onion). Keep in mind that once
your data appears on our blog, it could be bought by your competitors at any second, so don't
hesitate for a long time.
>> How to contact with us?
  1. Download and install TOR Browser (https://www.torproject.org/).[If you don't know that, Google
search!]
  2. Open
http://f3r6nz2bopxnotodfcp4qztpr3mmapnkioa3ho7j2cuovb32nlf3zcyd.onion/621d81ec62c879476a39fb0bde573
5ce7c95e59d562bdcf2e48b9dd90a4a3d1fa6dae6e1d655248cd12d6ba66f5b5a15/
>>> Warning! Recovery recommendations.
 Do not MODIFY or REPAIR your files, Or they will be lost forever.
 Do not hire a recovery company.Can't solve anything without us,They always think they're expert
negotiators, but the truth is they don't care about you and business
 Do not report to the Police, FBI,They don't care about your business and it's going to get
worse.(You could be hit with a hefty fine.)
```

Figure 4. Knight ransom note.



```
Hello!

Visit our Blog:

Tor Browser Links:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Links for normal browser:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data
appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The
sooner you pay the ransom, the sooner your company will be safe.


>>> If you have an external or cloud backup; what happens if you don’t agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree
with us, information pertaining to your companies and the data of your company’s customers will be published on the
internet, and the respective country’s personal data usage authority will be informed. Moreover, confidential data
related to your company will be shared with potential competitors through email and social media. You can be sure that
you will incur damages far exceeding the amount we are requesting from you should you decide not to agree with us.


>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because
the negotiations will make them look incompetent,After the incident report is handed over to the government
department, you will be fined <This will be a huge amount,Read more about the GDRP
legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward
them.And you will not get anything, and except you and your company, the rest of the people will forget what
happened!!!!!


>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://an2ce4pqpf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtly7bhid.onion/
- Log in using the Client ID: cf9e1200044391a8502dee45d4396844f4a14541bf76e5d2abd67ad772
```

Figure 5. RansomHub ransom note.

One of the main differences between the two ransomware families is the commands run through cmd.exe. These commands may be configured when the payload is built or during configuration. Although the commands themselves are different, the way and order in which they are called relative to other operations is the same.

A unique feature present in both Knight and RansomHub is the ability to restart an endpoint in safe mode before starting encryption. This technique was previously employed by Snatch ransomware in 2019 and allows encryption to progress unhindered by operating system or other security processes. Snatch is also written in Go and has many similar features, suggesting it could be another fork of the same original source code used to develop Knight and RansomHub. However, Snatch contains significant differences, including an apparent lack of configurable commands or any sort of obfuscation.

Another ransomware family that restarts the affected computer in safe mode before encryption is Noberus Interestingly, the encryptor stores its configuration in a JSON where keywords match what was observed in RansomHub.

RansomHub attacks

In recent RansomHub attacks investigated by Symantec, the attackers gained initial access by exploiting the Zerologon vulnerability (CVE-2020-1472), which can allow an attacker to gain domain administrator privileges and take control of the entire domain.

The attackers used several dual-use tools before deploying the ransomware. Atera and Splashtop were used to facilitate remote access, while NetScan was used to likely discover and retrieve information about network devices. The RansomHub payload leveraged the iisreset.exe and iisrstas.exe command-line tools to stop all Internet Information Services (IIS) services.

Rapid growth

Despite only first appearing in February 2024, RansomHub has managed to grow very quickly and, over the past three months, was the fourth most prolific ransomware operator in terms of numbers of attacks publicly claimed. The group last week claimed responsibility for an attack on UK auction house Christies.

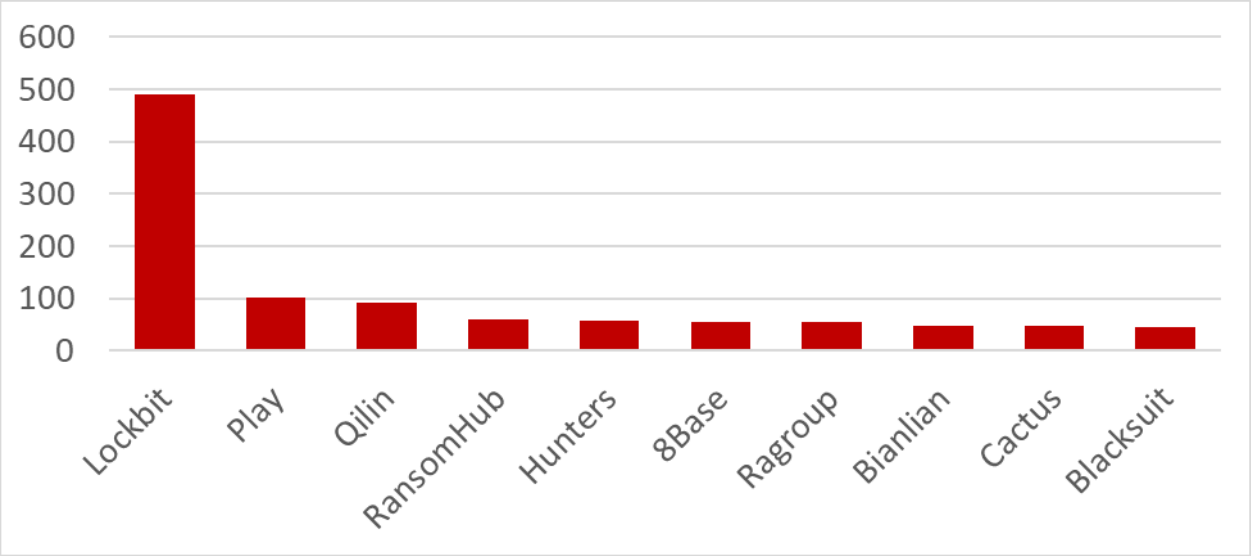


Figure 6. Most prolific ransomware operations by claimed attacks, March-May 2023.

One factor contributing to RansomHub's growth may be the group's success in attracting some large former affiliates of the Noberus (aka ALPHV, Blackcat) ransomware group, which closed earlier this year. One former Noberus affiliate known as Notchy is now reportedly working with RansomHub. In addition to this, tools previously associated with another Noberus affiliate known as Scattered Spider, were used in a recent RansomHub attack.

The speed at which RansomHub has established its business suggests that the group may consist of veteran operators with experience and contacts in the cyber underground.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

SHA-256 hash	Description
02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292	RansomHub
34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087	RansomHub
7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a	RansomHub
8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7	RansomHub
ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00	RansomHub
104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2	Knight

SHA-256 hash	Description
2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad	Knight
36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e	Knight
595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb	Knight
7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2	Knight
e654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23	Knight
fb9f9734d7966d6bc15cce5150abb63aadd4223924800f0b90dc07a311fb0a7e	NetScan
f1a6e08a5fd013f96facc4bb0d8dfb6940683f5bdfc161bd3a1de8189dea26d3	Splashtop
a96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2	Atera

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?