Linux version of Qilin ransomware focuses on VMware ESXi

bleepingcomputer.com/news/security/linux-version-of-qilin-ransomware-focuses-on-vmware-esxi/

Lawrence Abrams

By
Lawrence Abrams

- December 3, 2023
- 04:07 PM
- 0

A sample of the Qilin ransomware gang's VMware ESXi encryptor has been found and it could be one of the most advanced and customizable Linux encryptors seen to date.

The enterprise is increasingly moving to virtual machines to host their servers, as they allow for better usage of available CPU, memory, and storage resources.

Due to this adoption, almost all ransomware gangs have created dedicated VMware ESXi encryptors to target these servers.

While many ransomware operations utilize the leaked Babuk source code to create their encryptors, a few, such as Qilin, create their own encryptors to target Linux servers.

Qilin targets VMware ESXi

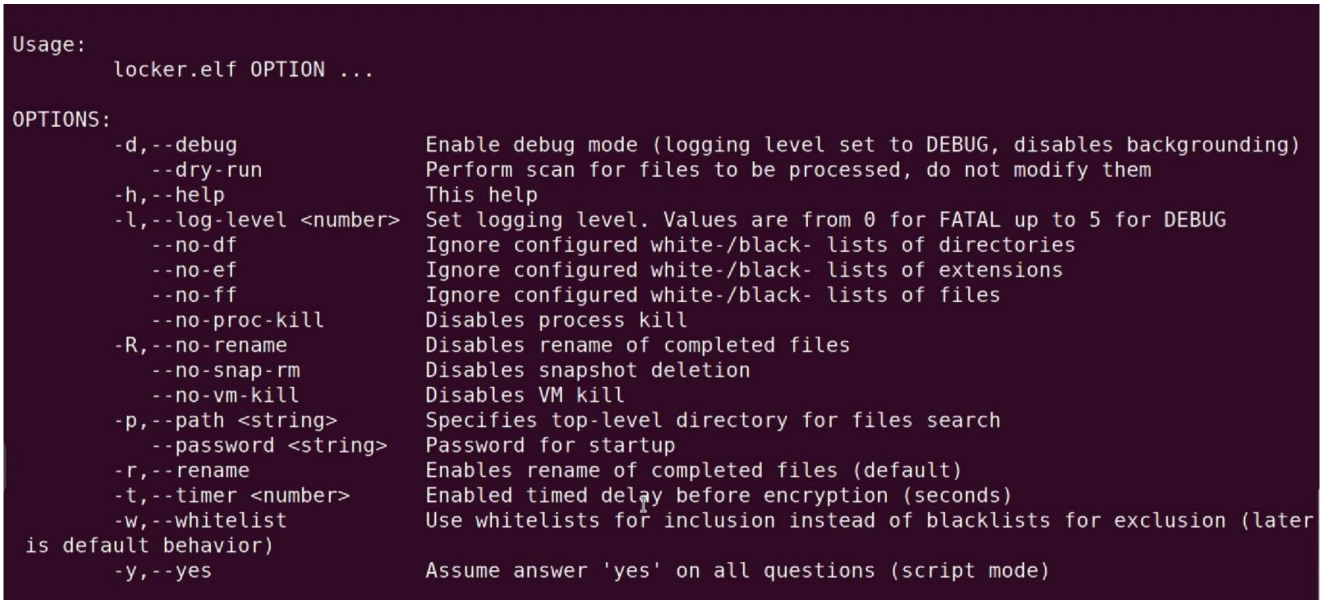
Last month, security researcher MalwareHunterTeam found a Linux ELF64 encryptor for the Qilin ransomware gang and shared it with BleepingComputer to analyze.

While the encryptor can be used on Linux, FreeBSD, and VMware ESXi servers, it heavily focuses on encrypting virtual machines and deleting their snapshots.

Qilin's encryptor is built with an embedded configuration specifying the extension for encrypted files, the processes to terminate, the files to encrypt or exclude, and the folders to encrypt or exclude.

However, it also includes numerous command-line arguments allowing extensive customization of these configuration options and how files are encrypted on a server.

These command line arguments include options to enable a debug mode, perform a dry run without encrypting any files, or customize how virtual machines and their snapshots are encrypted.



```
Usage:
        locker.elf OPTION ...

OPTIONS:
        -d,--debug              Enable debug mode (logging level set to DEBUG, disables backgrounding)
           --dry-run            Perform scan for files to be processed, do not modify them
        -h,--help               This help
        -l,--log-level <number> Set logging level. Values are from 0 for FATAL up to 5 for DEBUG
           --no-df              Ignore configured white-/black- lists of directories
           --no-ef              Ignore configured white-/black- lists of extensions
           --no-ff              Ignore configured white-/black- lists of files
           --no-proc-kill       Disables process kill
        -R,--no-rename          Disables rename of completed files
           --no-snap-rm         Disables snapshot deletion
           --no-vm-kill         Disables VM kill
        -p,--path <string>      Specifies top-level directory for files search
           --password <string>  Password for startup
        -r,--rename             Enables rename of completed files (default)
        -t,--timer <number>     Enabled timed delay before encryption (seconds)
        -w,--whitelist          Use whitelists for inclusion instead of blacklists for exclusion (later
 is default behavior)
        -y,--yes                Assume answer 'yes' on all questions (script mode)
```

Qilin Linux encryptor
Source: BleepingComputer
The full list of command line options are listed below:

```
OPTIONS:
-d,--debug               Enable debug mode (logging level set to DEBUG, disables
backgrounding)
   --dry-run             Perform scan for files to be processed, do not modify them
-h,--help                This help
-l,--log-level <number>  Set logging level. Values are from 0 for FATAL up to 5 for
DEBUG
   --no-df               Ignore configured white-/black- lists of directories
   --no-ef               Ignore configured white-/black- lists of extensions
   --no-ff               Ignore configured white-/black- lists of files
   --no-proc-kill        Disables process kill
-R,--no-rename           Disables rename of completed files
   --no-snap-rm          Disables snapshot deletion
   --no-vm-kill          Disables VM kill
-p,--path <string>       Specifies top-level directory for files search
   --password <string>   Password for startup
-r,--rename              Enables rename of completed files (default)
-t,--timer <number>      Enabled timed delay before encryption (seconds)
-w,--whitelist           Use whitelists for inclusion instead of blacklists for
exclusion (later is default behavior)
-y,--yes                 Assume answer 'yes' on all questions (script mode)
```

In the sample analyzed by BleepingComputer.com, the encryptor is configured by default with the following exclusions and targeting criteria:

Processes to not terminate:

```
"kvm", "qemu", "xen"
```

Directories to exclude from encryption:

```
"/boot/", "/proc/", "/sys/", "/run/", "/dev/", "/lib/", "/etc/", "/bin/", "/mbr/",
"/lib64/", "/vmware/lifecycle/", "/vdtc/", "/healthd/"
```

Files to exclude from encryption:

```
"initrd", "vmlinuz", "basemisc.tgz", "boot.cfg", "bootpart.gz", "features.gz",
"imgdb.tgz", "jumpstrt.gz", "onetime.tgz", "state.tgz", "useropts.gz"
```

File extensions to exclude from encryption:

```
"v00", "v01", "v02", "v03", "v04", "v05", "v06", "v07", "v08", "v09", "b00", "b01",
"b02", "b03", "b04", "b05", "b06", "b07", "b08", "b09", "t00", "t01", "t02", "t03",
"t04", "t05", "t06", "t07", "t08", "t09"
```

Directories to target for encryption:

```
"/home", "/usr/home", "/tmp", "/var/www", "/usr/local/www", "/mnt", "/media", "/srv",
"/data", "/backup", "/var/lib/mysql", "/var/mail", "/var/spool/mail", "/var/vm",
"/var/lib/vmware", "/opt/virtualbox", "/var/lib/xen", "/var/opt/xen", "/kvm",
"/var/lib/docker", "/var/lib/libvirt", "/var/run/sr-mount", "/var/lib/postgresql",
"/var/lib/redis", "/var/lib/mongodb", "/var/lib/couchdb", "/var/lib/neo4j",
"/var/lib/cassandra", "/var/lib/riak", "/var/lib/influxdb", "/var/lib/elasticsearch"
```

Files to target for encryption:

```
"3ds", "3g2", "3gp", "7z", "aac", "abw", "ac3", "accdb", "ai", "aif", "aiff", "amr",
"apk", "app", "asf", "asx", "atom", "avi", "bak", "bat", "bmp", "bup", "bz2", "cab",
"cbr", "cbz", "cda", "cdr", "chm", "class", "cmd", "conf", "cow", "cpp", "cr2",
"crdownload", "cs", "csv", "cue", "cur", "dat", "db", "dbf", "dds", "deb", "der",
"desktop", "dmg", "dng", "doc", "docm", "dot", "dotm", "dotx", "dpx", "drv", "dtd",
"dvi", "dwg", "dxf", "eml", "eps", "epub", "f4v", "fnt", "fon", "gam", "ged", "gif",
"gpx", "gz", "h264", "hdr", "hpp", "hqx", "htm", "html", "ibooks", "ico", "ics",
"iff", "image", "img", "indd", "iso", "jar", "java", "jfif", "jpe", "jpeg", "jpf",
"jpg", "js", "json", "jsp", "key", "kml", "kmz", "log", "m4a", "m4b", "m4p", "m4v",
"mcd", "mdbx", "mht", "mid", "mkv", "ml", "mobi", "mov", "mp3", "mp4", "mpa", "mpeg",
"mpg", "msg", "nes", "numbers", "odp", "ods", "odt", "ogg", "ogv", "otf", "ova",
"ovf", "pages", "parallels", "pcast", "pct", "pdb", "pdf", "pds", "pef", "php",
"pkg", "pl", "plist", "png", "pptm", "prproj", "ps", "psd", "ptx", "py", "qcow",
"qcow2", "qed", "qt", "r3d", "ra", "rar", "rm", "rmvb", "rtf", "rv", "rw2", "sh",
"shtml", "sit", "sitx", "sketch", "spx", "sql", "srt", "svg", "swf", "tar", "tga",
"tgz", "thmx", "tif", "tiff", "torrent", "ttf", "txt", "url", "vdi", "vhd", "vhdx",
"vmdk", "vmem", "vob", "vswp", "vvfat", "wav", "wbmp", "webm", "webp", "wm", "wma",
"wmv", "wpd", "wps", "xhtml", "xlsm", "xml", "xspf", "xvid", "yaml", "yml", "zip",
"zipx"
```

Configuring a list of virtual machines that should not be encrypted is also possible.

When executing the encryptor, a threat actor must specify the starting directory for encryption and a specific password tied to the encryptor.

When executed, the ransomware will determine if it is running in Linux, FreeBSD, or VMware ESXi server.

If it detects VMware ESXi, it will run the following *esxcli* and *esxcfg-advcfg* commands, which we have not seen in other ESXi encryptors in the past.

```
for I in $(esxcli storage filesystem list |grep 'VMFS-5' |awk '{print $1}'); do
vmkfstools -c 10M -d eagerzeroedthick $I/eztDisk > /dev/null; vmkfstools -U
$I/eztDisk > /dev/null; done
for I in $(esxcli storage filesystem list |grep 'VMFS-5' |awk '{print $1}'); do
vmkfstools -c 10M -d eagerzeroedthick $I/eztDisk; vmkfstools -U $I/eztDisk; done
for I in $(esxcli storage filesystem list |grep 'VMFS-6' |awk '{print $1}'); do
vmkfstools -c 10M -d eagerzeroedthick $I/eztDisk > /dev/null; vmkfstools -U
$I/eztDisk > /dev/null; done
for I in $(esxcli storage filesystem list |grep 'VMFS-6' |awk '{print $1}'); do
vmkfstools -c 10M -d eagerzeroedthick $I/eztDisk; vmkfstools -U $I/eztDisk; done
esxcfg-advcfg -s 32768 /BufferCache/MaxCapacity
esxcfg-advcfg -s 20000 /BufferCache/FlushInterval
```

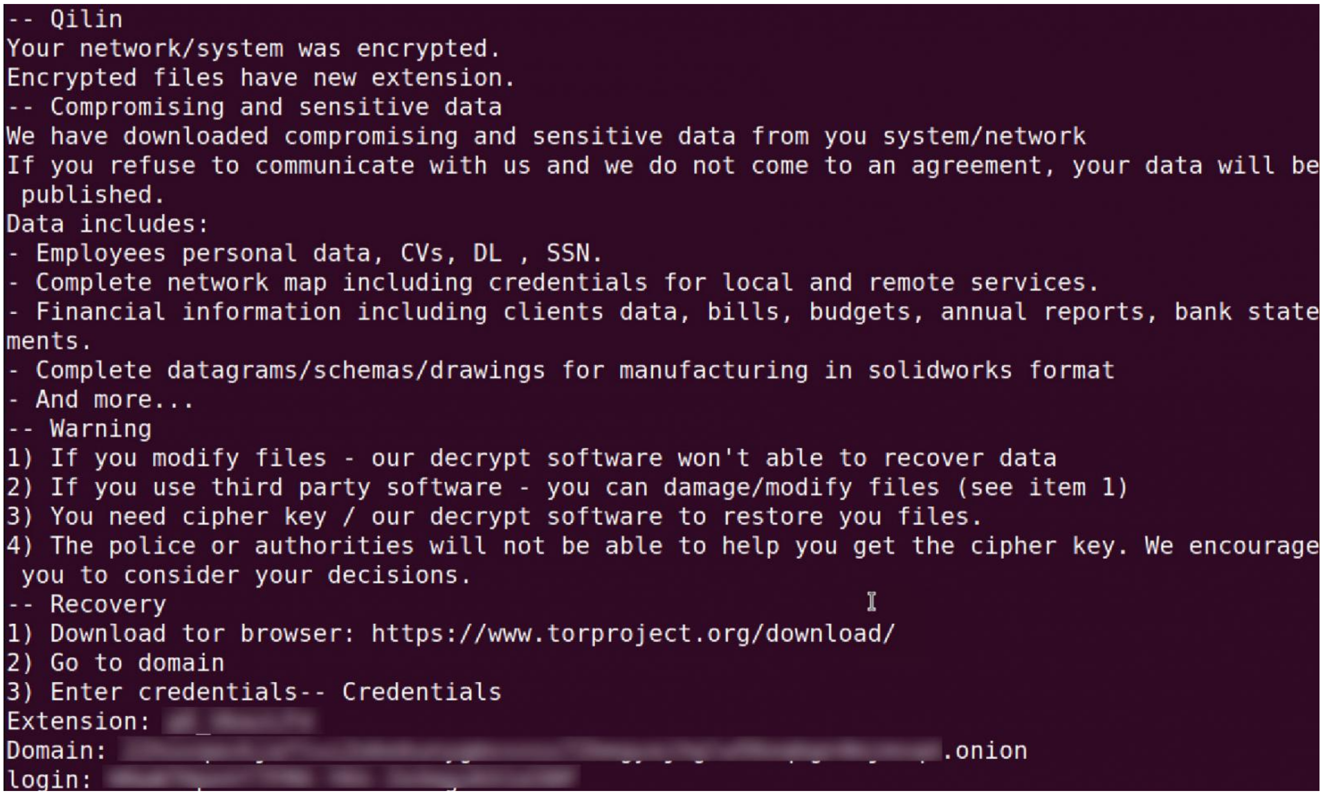
VMware expert Melissa Palmer told BleepingComputer that these commands were likely copied from VMware support bulletins to resolve a known VMware memory heap exhaustion bug and increase performance when executing ESXi commands on the server.

Before encrypting any detected virtual machines, the ransomware will first terminate all VMs and delete their snapshots using the following commands:

```
esxcli vm process list
vim-cmd vmsvc/getallvms
esxcli vm process kill -t force -w %llu
vim-cmd vmsvc/snapshot.removeall %llu > /dev/null 2>&1
```

All targeted files will then be encrypted and have the configured extension appended to the file name.

In each folder, a ransom note named [extension]_RECOVER.txt will be created that contains links to the ransomware gang's Tor negotiation site and the login credentials required to access the victim's chat page.



```
-- Qilin
Your network/system was encrypted.
Encrypted files have new extension.
-- Compromising and sensitive data
We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreement, your data will be
 published.
Data includes:
- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank state
ments.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...
-- Warning
1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key. We encourage
 you to consider your decisions.
-- Recovery
1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
3) Enter credentials-- Credentials
Extension: [redacted]
Domain: [redacted].onion
login: [redacted]
```

Qilin ransom note

Source: BleepingComputer

BleepingComputer has seen ransom demands ranging from $25,000 to millions of dollars.

The Qilin ransomware operation

The Qilin ransomware operation was initially launched as "Agenda" in August 2022. However, by September, it had rebranded under the name Qilin, which it continues to operate as to this day.

Like other enterprise-targeting ransomware operations, Qilin will breach a company's networks and steal data as they spread laterally to other systems.

When done collecting data and gaining server administrator credentials, the threat actors deploy the ransomware to encrypt all devices on the network.

The stolen data and the encrypted files are then used as leverage in double-extortion attacks to coerce a company into paying a ransom demand.

Since its launch, the ransomware operation has had a steady stream of victims but has seen increased activity towards the end of 2023.

A recent attack by Qilin was on the auto-parts giant Yanfeng.

Related Articles:

Microsoft fixes Windows Server VMs broken by October updates

MGM casino's ESXi servers allegedly encrypted in ransomware attack

Victoria court recordings exposed in reported ransomware attack

Qilin ransomware claims attack on automotive giant Yanfeng

VX-Underground malware collective framed by Phobos ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.