

Linux version of Abyss Locker ransomware targets VMware ESXi servers

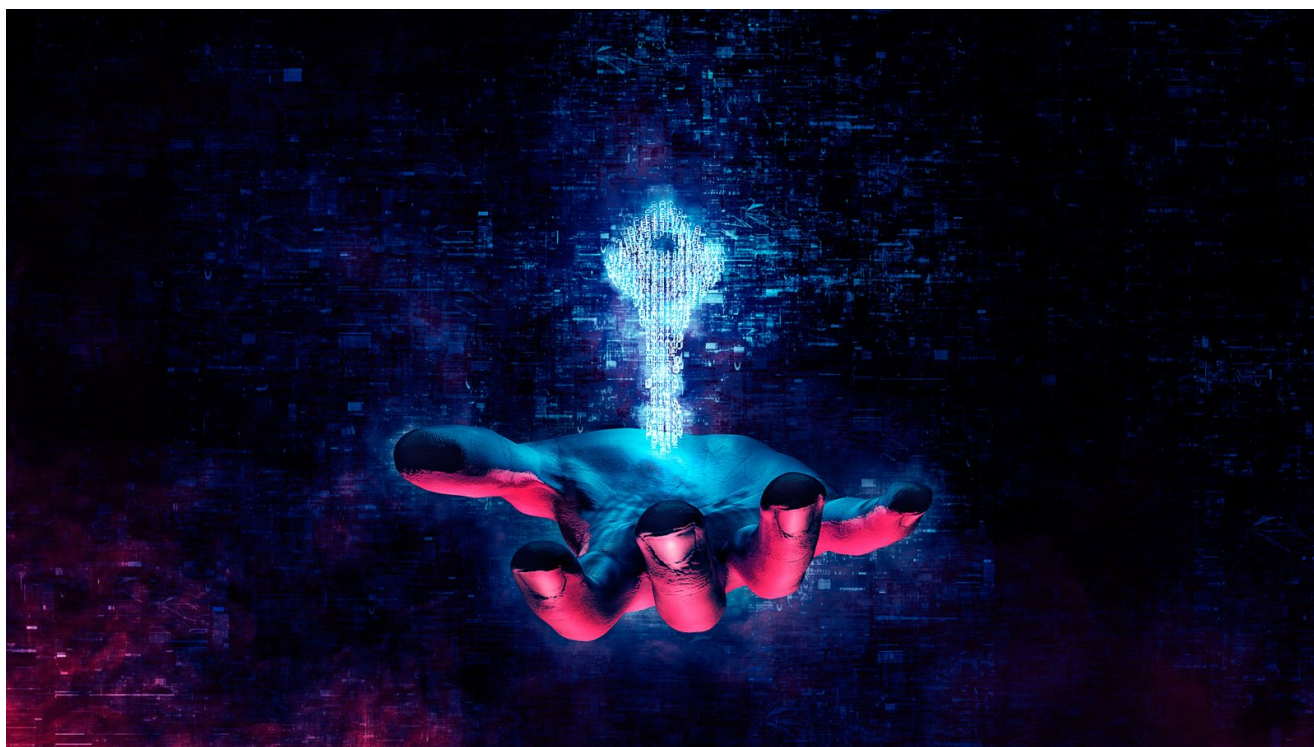
bleepingcomputer.com/news/security/linux-version-of-abyss-locker-ransomware-targets-vmware-esxi-servers/

Lawrence Abrams

By

[Lawrence Abrams](#)

- July 29, 2023
- 11:17 AM
- [0](#)



The Abyss Locker operation is the latest to develop a Linux encryptor to target VMware's ESXi virtual machines platform in attacks on the enterprise.

As the enterprise shifts from individual servers to virtual machines for better resource management, performance, and disaster recovery, ransomware gangs create encryptors focused on targeting the platform.

With VMware ESXi being one of the most popular virtual machine platforms, almost every ransomware gang has begun to release Linux encryptors to encrypt all virtual servers on a device.

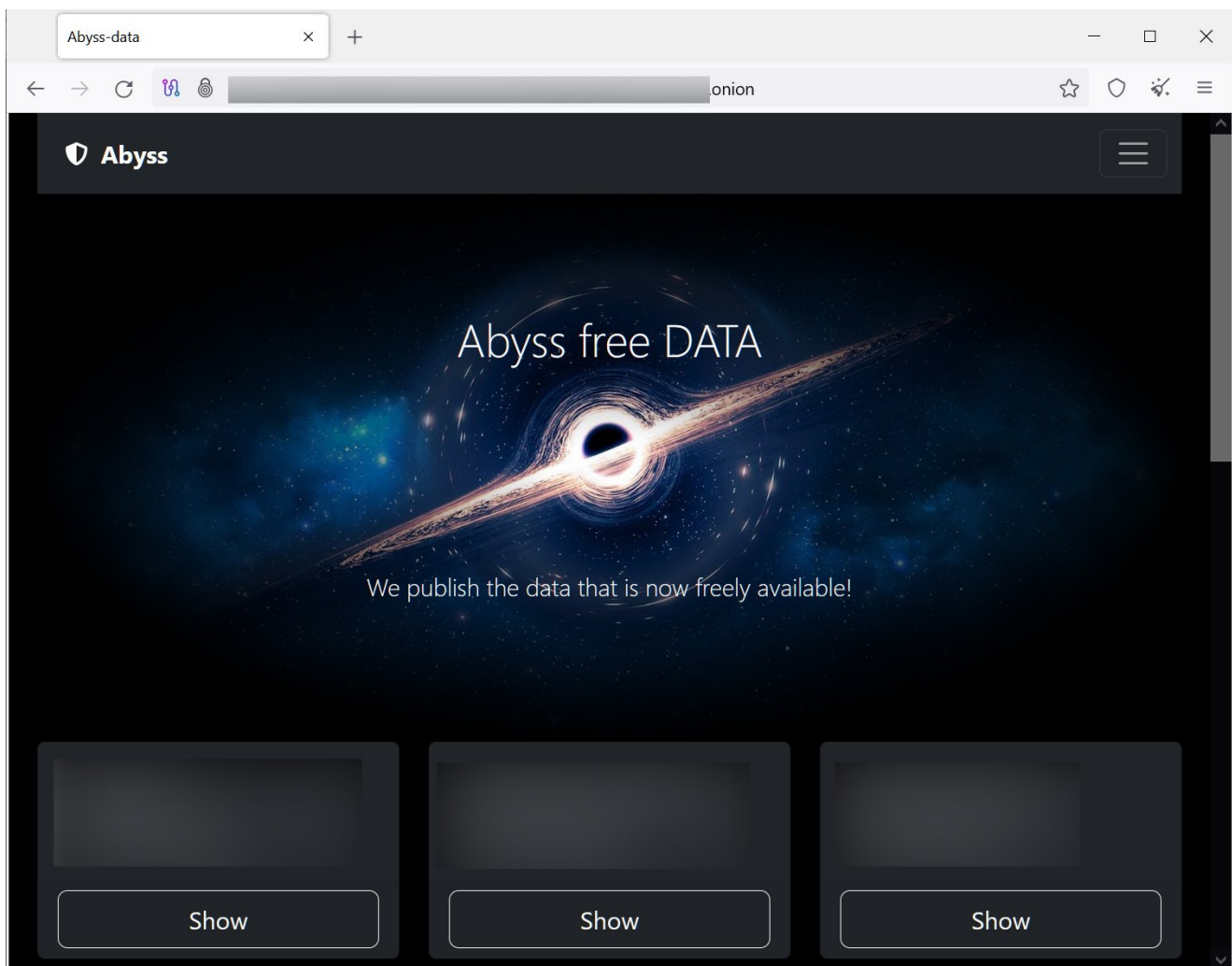
Other ransomware operations that utilize Linux ransomware encryptors, with most targeting VMware ESXi, include [Akira](#), [Royal](#), [Black Basta](#), [LockBit](#), [BlackMatter](#), [AvosLocker](#), [REvil](#), [HelloKitty](#), [RansomEXX](#), and [Hive](#).

The Abyss Locker

Abyss Locker is a relatively new ransomware operation that is believed to have [launched in March 2023](#), when it began to target companies in attacks.

Like other ransomware operations, the Abyss Locker threat actors will breach corporate networks, steal data for double-extortion, and encrypt devices on the network.

The stolen data is then used as leverage by threatening to leak files if a ransom is not paid. To leak the stolen files, the threat actors created a Tor data leak site named 'Abyss-data' that currently lists fourteen victims.



Abyss Locker data leak site

Source: [BleepingComputer](#)

The threat actors claim to have stolen anywhere between 35 GB of data from one company to as high as 700 GB at another.

Targeting VMware ESXi servers

This week, security researcher [MalwareHunterTeam](#) found a Linux ELF encryptor for the Abyss Locker operation and shared it with BleepingComputer for analysis.

After looking at the strings in the executable, it is clear that the encryptor specifically targets VMware ESXi servers.

As you can see from the commands below, the encryptor utilizes the 'esxcli' command-line VMware ESXi management tool to first list all available virtual machines and then terminate them.

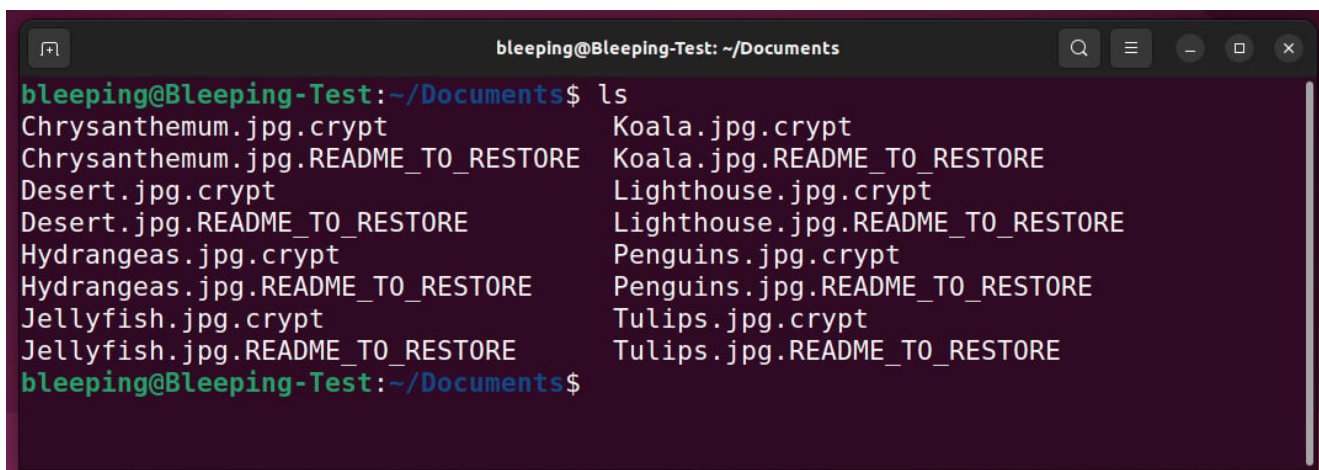
```
esxcli vm process list
esxcli vm process kill -t=soft -w=%d
esxcli vm process kill -t=hard -w=%d
esxcli vm process kill -t=force -w=%d
```

When shutting down the virtual machines, Abyss Locker will use the 'vm process kill' command and one of the soft, hard, or forced options.

The *soft* option performs a graceful shutdown, the *hard* option terminates a VM immediately, and *force* is used as a last resort.

The encryptor terminates all virtual machines to allow the associated virtual disks, snapshots, and metadata to be properly encrypted by encrypting all files with the following extensions: .vmdk (virtual disks), .vmsd (metadata), and .vmsn (snapshots).

In addition to targeting virtual machines, the ransomware will also encrypt all other files on the device and append the **.crypt** extension to their filenames, as shown below.

A terminal window titled 'bleeping@Bleeping-Test: ~/Documents' showing the output of the 'ls' command. The output lists various files with their original names and extensions, followed by their encrypted versions. For example, 'Chrysanthemum.jpg.crypt' and 'Chrysanthemum.jpg.README_TO_RESTORE'. The files are listed in two columns.

```
bleeping@Bleeping-Test:~/Documents$ ls
Chrysanthemum.jpg.crypt          Koala.jpg.crypt
Chrysanthemum.jpg.README_TO_RESTORE Koala.jpg.README_TO_RESTORE
Desert.jpg.crypt                Lighthouse.jpg.crypt
Desert.jpg.README_TO_RESTORE    Lighthouse.jpg.README_TO_RESTORE
Hydrangeas.jpg.crypt           Penguins.jpg.crypt
Hydrangeas.jpg.README_TO_RESTORE Penguins.jpg.README_TO_RESTORE
Jellyfish.jpg.crypt            Tulips.jpg.crypt
Jellyfish.jpg.README_TO_RESTORE Tulips.jpg.README_TO_RESTORE
bleeping@Bleeping-Test:~/Documents$
```

Encrypted files and ransom notes

Source: *BleepingComputer*

For each file, the encryptor will also create a file with a **.README_TO_RESTORE** extension, which acts as the ransom note.

This ransom note contains information on what happened to the files and a unique link to the threat actor's Tor negotiation site. This site is barebones, only having a chat panel that can be used to negotiate with the ransomware gang.



```
bleeping@Bleeping-Test: ~/Documents
We are the Abyss Locker V2, professionals in all aspects we perform.

Your company Servers are locked and Data has been taken to our servers. This is serious.

Good news:
- 100% of your Server system and Data will be restored by our Decryption Tool;
- for now, your data is secured and safely stored on our server;
- nobody in the world is aware about the data leak from your company except you and Abyss Locker team.

FAQs:

Want to go to authorities for protection?
- they will do their job properly, but you will not get any win points out of it, only headaches; they will never make decryption for data or servers, they just can't.
  Also, they will take all of your IT infrastructure as a part of their procedure; but still they will not help you at all.

Think you can handle it without us by decrypting your servers and data using some IT Solution from third-party non-hackers or specialists?
```

Abyss Locker ransom note

Source: *BleepingComputer*

Ransomware expert [Michael Gillespie](#) said that the Abyss Locker Linux encryptor is based on Hello Kitty, using ChaCha encryption instead.

However, it is not known if this is a rebrand of the HelloKitty operation or if another ransomware operation gained access to the encryptor's source code, as we [saw with Vice Society](#).

Unfortunately, HelloKitty has historically been a secure ransomware, preventing the recovery of files for free.

Related Articles:

[Monti ransomware targets VMware ESXi servers with new Linux locker](#)

[The Week in Ransomware - August 4th 2023 - Targeting VMware ESXi](#)

[LockBit ransomware builder leaked online by "angry developer"](#)

[The Week in Ransomware - August 18th 2023 - LockBit on Thin Ice](#)

Microsoft: BlackCat's Sphynx ransomware embeds Impacket, RemCom

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.