REvil ransomware's new Linux encryptor targets ESXi virtual machines

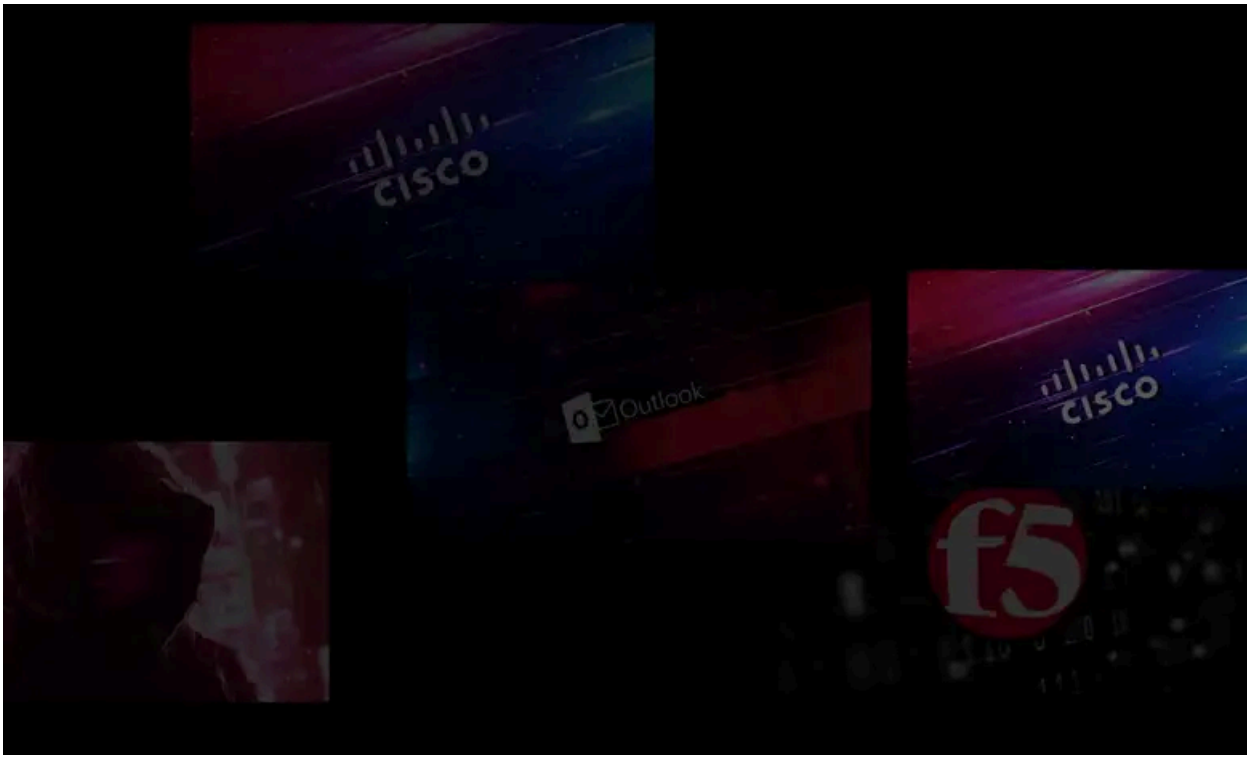
By Lawrence Abrams

Published: 2021-06-28 · Archived: 2026-04-02 12:30:32 UTC

The REvil ransomware operation is now using a Linux encryptor that targets and encrypts Vmware ESXi virtual machines.

With the enterprise moving to virtual machines for easier backups, device management, and efficient use of resources, ransomware gangs increasingly create their own tools to mass encrypt storage used by VMs.

In May, Advanced Intel's Yelisey Boguslavskiy shared a forum post from the REvil operation where they confirmed that they had released a Linux version of their encryptor that could also work on NAS devices.


cisco
Outlook
cisco
f5

> #REvil just directly confirmed that they had added an operating Linux version portable for NAS as well.
> pic.twitter.com/Fc6p2H62vf
>
> — Yelisey Boguslavskiy (@y_advintel) May 9, 2021

Today, security researcher MalwareHunterTeam found a Linux version of the REvil ransomware (aka Sodinokibi) that also appears to target ESXi servers.

Advanced Intel's Vitali Kremez, who analyzed the new REvil Linux variant, told BleepingComputer it is an ELF64 executable and includes the same configuration options utilized by the more common Windows executable.

Kremez states that this is the first known time the Linux variant has been publicly available since it was released.

When executed on a server, a threat actor can specify the path to encrypt and enable a silent mode, as shown by the usage instructions below.

```
 Usage example: elf.exe --path /vmfs/ --threads 5
 without --path encrypts current dir
--silent (-s) use for not stoping VMs mode
!!!BY DEFAULT THIS SOFTWARE USES 50 THREADS!!!
```

When executed on ESXi servers, it will run the esxcli command line tool to list all running ESXi virtual machines and terminate them.

```
esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list | awk -F ""*,"*" '{system("esxcli vm
```

This command is used to close the virtual machine disk (VMDK) files stored in the /vmfs/ folder so that the REvil ransomware malware can encrypt the files without them being locked by ESXi.

If a virtual machine is not correctly closed before encrypting its file, it could lead to data corruption, as explained by Emsisoft CTO Fabian Wosar.

By targeting virtual machines this way, REvil can encrypt many servers at once with a single command.

Wosar told BleepingComputer that other ransomware operations, such as Babuk, RansomExx/Defray, Mespinoza, GoGoogle, DarkSide, and Hellokitty have also created Linux encryptors to target ESXi virtual machines.

"The reason why most ransomware groups implemented a Linux-based version of their ransomware is to target ESXi specifically," said Wosar.

File hashes associated with the REvil Linux encryptor have been collected by security researcher Jaime Blasco and shared on Alienvault's Open Threat Exchange.
