Linux Variant of REvil Ransomware Targets VMware's ESXi, NAS Devices

By Tom Spring

Published: 2021-07-01 · Archived: 2026-04-05 13:55:27 UTC

Criminals behind the potent REvil ransomware have ported the malware to Linux for targeted attacks.

UPDATE

Cybercriminals behind a string of high-profile ransomware attacks, including one extorting $11 million from JBS Foods last month, have ported their malware code to the Linux operating system. The unusual move is an attempt to target VMware's ESXi virtual machine management software and network attached storage (NAS) devices that run on the Linux operating system (OS).

Researchers at AT&T Cybersecurity said they have confirmed four Linux samples of the REvil malware in the wild.

Ofer Caspi, security researcher at Alien Labs, a division of AT&T Cybersecurity, wrote in a Thursday blog that after receiving a tip from MalwareHuntingTeam it identified the four samples.

"REvil ransomware authors have expanded their arsenal to include Linux ransomware, which allows them to target ESXi and NAS devices," Caspi wrote.

In a nod to research by AdvIntel in early May 2021, which reported REvil's intent to port its Windows-based ransomware to Linux, Caspi confirmed the Linux variant was spotted in May "affecting *nix systems and ESXi."

"The samples are ELF-64 executables, with similarities to the Windows REvil executable, being the most noticeable among the configuration options," he wrote.

Executable and Linkable Format (or ELF-64) is a standard file format for executable files within Linux and UNIX-like operating systems, according to a technical breakdown.

Linux Ransomware: Rare, but Real

What makes Alien Labs' discovery of the Linux REvil variant unique is that the Linux, Unix and other Unix-like computer operating systems, are not typically targeted by adversaries. Microsoft Windows computer systems generally deliver the biggest return for an attacker's effort because of the ubiquity of the OS. Furthermore, instances of Linux are generally well-protected against vulnerabilities, thanks to a tightknit user-base delivering fast security updates.

Past examples of Linux malware over the past several years have included Tycoon, Lilocked (or Lilu) and QNAPCrypt. In November, Kaspersky identified a Linux sample of RansomEXX. Researchers noted that criminals based its Linux variant on "WinAPI (functions specific to Windows OS)" and used a similar mechanism to manipulate targeted Linux MBED TLS libraries.

MBED TLS is an implementation of the TLS and SSL protocols distributed under the Apache License.

"The Apache license itself has nothing to do with web servers, other than it being one of the more widely used pieces of software that uses the license, among hundreds of thousands of other open source projects," said Kenneth White, director of the Open Crypto Audit Project.

In May, researchers noted criminals behind the DarkSide ransomware also released a Linux variant. Attackers also targeted, "virtual machine-related files on VMware ESXI servers." Researchers said the malware "parses its embedded configuration, kills virtual machines, encrypts files on the infected machine, collects system information, and sends it to the remote server."

Targeted Attacks: Linux in the Crosshairs

VMware ESXi, formerly known as ESX, is a bare metal hypervisor that installs easily on to your server and partitions it into multiple virtual machines (VM).

"The hypervisor ESXi allows multiple virtual machines to share the same hard drive storage. However, this also enables attackers to encrypt the centralized virtual hard drives used to store data from across VMs, potentially causing disruptions to companies," Alien Labs reported. "[I]n addition to targeting ESXi, REvil is also targeting NAS devices as another storage platform with the potential to highly impact the affected companies."

Researchers said the Linux version of REvil share similar attributes to the Windows OS variant. "The [executable's] configuration file format is very similar to the one observed for REvil Windows samples, but with fewer fields," Caspi wrote.

Similarities also include:

- Base64-encoded value containing the attacker's public key used to encrypt files.
- Ransomware-as-a-service (RaaS) affiliate identifier (7987) is shared between both operating systems.
- The ransom note's body content is encoded in base64.
- The encrypted extensions, which appears to be five random character, both are: .rhkrc, .qoxaq, .naixq, and .7rspj.

"The threat actors behind REvil RaaS have rapidly developed a Linux version to compete against the recently released Linux version of DarkSide. It is hard to clarify if these two RaaS are competing against each other or collaborating team members, as stated by other security researchers," researchers wrote.

(This article was updated 7/6 at 12:40 p.m. ET to reflect a clarification on the nature of the Apache software license in the context of MBED TLS.)

Check out our free upcoming live and on-demand webinar events – unique, dynamic discussions with cybersecurity experts and the Threatpost community.
