Hive ransomware ports its Linux VMware ESXi encryptor to Rust

bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/

Lawrence Abrams

By
Lawrence Abrams

- March 27, 2022
- 03:18 PM
- 0

The Hive ransomware operation has converted their VMware ESXi Linux encryptor to the Rust programming language and added new features to make it harder for security researchers to snoop on victim's ransom negotiations.

As the enterprise becomes increasingly reliant on virtual machines to save computer resources, consolidate servers, and for easier backups, ransomware gangs are creating dedicated encryptors that focus on these services.

Ransomware gang's Linux encryptors typically target the VMware ESXI virtualization platforms as they are the most commonly used in the enterprise.

While Hive has been using a Linux encryptor to target VMware ESXi servers for some time, a recent sample shows that they updated their encryptor with features first introduced by the BlackCat/ALPHV ransomware operation.

Hive borrows features from BlackCat

When ransomware operations attack a victim, they try to conduct their negotiations in private, telling victims if a ransom is not paid their data will be published and they will suffer a reputational hit.

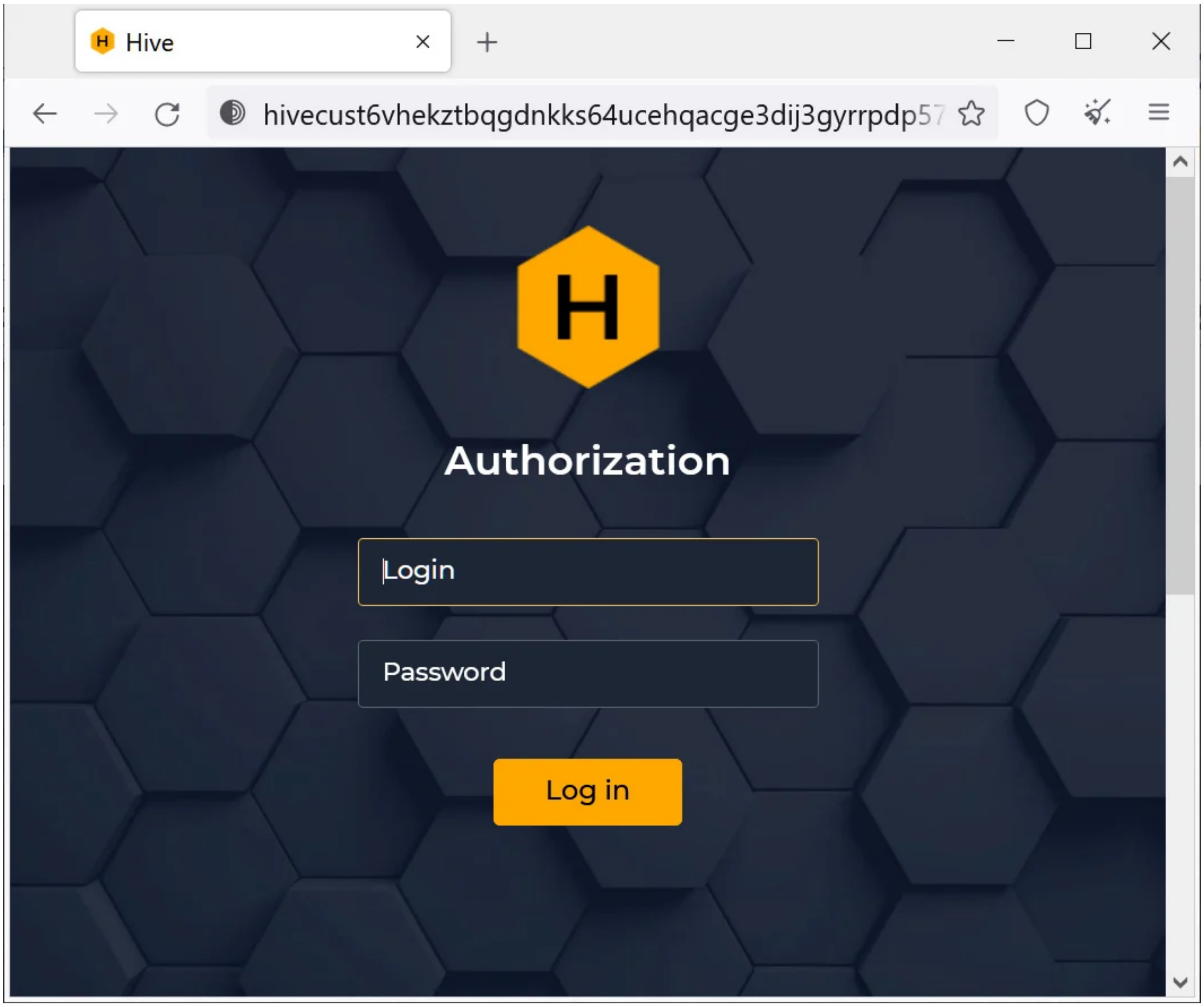
However, when ransomware samples are uploaded to public malware analysis services, they are commonly found by security researchers who can extract the ransom note and snoop on negotiations.

In many cases, these negotiations are then publicized on Twitter and elsewhere, causing negotiations to fail.

The BlackCat ransomware gang removed Tor negotiation URLs from their encryptor to prevent this from happening. Instead, it required the URL to be passed as a command-line argument when the encryptor is executed.

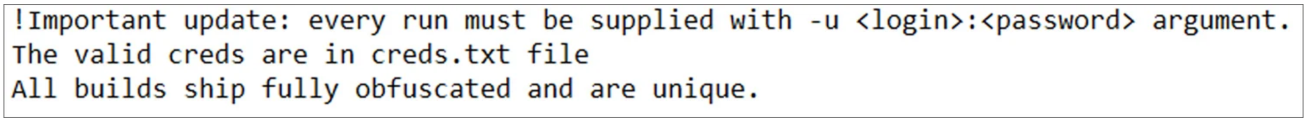
This feature prevents researchers who find the sample from retrieving the URL as it's not included in the executable and only passed to the executable at run time.

While the Hive Ransomware already requires a login name and password to access a victim's Tor negotiation page, these credentials were previously stored in encryptor executable, making them easy to retrieve.



Hive Tor ransom negotiation site

In a new Hive Linux encryptor found by Group-IB security researcher rivitna, the Hive operation now requires the attacker to supply the user name and login password as a command-line argument when launching the malware.



```
!Important update: every run must be supplied with -u <login>:<password> argument.
The valid creds are in creds.txt file
All builds ship fully obfuscated and are unique.
```

Instructions to Hive ransomware affiliates

Source: rivitna

By copying BlackCat's tactics, the Hive ransomware operation has made it impossible to retrieve negotiation login credentials from Linux malware samples, with the credentials now only available in ransom notes created during the attack.

Ransomware expert Michael Gillespie told BleepingComputer that the Windows executables were also modified to require the credentials be passed as a command-line argument during encryption.

Rivitna also told BleepingComputer that Hive continued to copy BlackCat by porting their Linux encryptor from Golang to the Rust programming language to make the ransomware samples more efficient and harder to reverse engineer.

"Rust allows to get safer, fast, and efficient code, while code optimization complicates analysis of Rust program," rivitna told BleepingComputer in a chat on Twitter.

With the encryption of VMware ESXi virtual machines a critical part of a successful attack, ransomware operations are constantly evolving their code to not only be more efficient, but to keep the operations and negotiations secret.

As more businesses move to virtualization for their servers, we will continue to see ransomware developers not only focus on Windows devices, but also create dedicated Linux encryptors targeting ESXi.

Due to this, all security professionals and network admins need to pay close attention to their Linux servers to detect signs of attacks.

Update 3/30/22: Added information about changes to Windows encryptors.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

National bank hit by ransomware trolls hackers with dick pics

Beware: Onyx ransomware destroys files instead of encrypting them

The Week in Ransomware - April 1st 2022 - 'I can fight with a keyboard'

Shutterfly services disrupted by Conti ransomware attack

- Encryptor
- Hive
- Linux
- Ransomware
- Virtual Machine
- Vmware ESXi

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.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: