Linux version of HelloKitty ransomware targets VMware ESXi servers

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

Lawrence Abrams

By
Lawrence Abrams

- July 15, 2021
- 11:13 AM
- 3

The ransomware gang behind the highly publicized attack on CD Projekt Red uses a Linux variant that targets VMware's ESXi virtual machine platform for maximum damage.

As the enterprise increasingly moves to virtual machines for easier backup and resource management, ransomware gangs are evolving their tactics to create Linux encryptors that target these servers.

VMware ESXi is one of the most popular enterprise virtual machine platforms. Over the past year, there has been an increasing number of ransomware gangs releasing Linux encryptors targeting this platform.

While ESXi is not strictly Linux as it uses its own customer kernel, it does share many similar characteristics, including the ability to run ELF64 Linux executables.

HelloKitty moves to ESXi

Yesterday, security researcher MalwareHunterTeam found numerous Linux ELF64 versions of the HelloKitty ransomware targeting ESXi servers and the virtual machines running on them.

It has been known that HelloKitty utilizes a Linux encryptor, but this is the first sample that researchers have publicly spotted.

> Seems no one mentioned yet, so let me do it: the Linux version of HelloKitty ransomware was already using esxcli at least in early March for stopping VMs...@VK_Intel @demonslay335 pic.twitter.com/atSv0OO7YL
>
> — MalwareHunterTeam (@malwrhunterteam) July 14, 2021

MalwareHunterTeam shared samples of the ransomware with BleepingComputer, and you can clearly see strings referencing ESXi and the ransomware's attempts to shut down running virtual machines.

```
First try kill  VM:%ld  ID:%d   %s
esxcli vm process kill -t=soft -w=%d
Check kill      VM:%ld  ID:%d
esxcli vm process kill -t=hard -w=%d
Unable to find
Killed          VM:%ld  ID:%d
still running VM:%ld    ID:%d try force
esxcli vm process kill -t=force -w=%d
Check   VM:%ld  ID:     %d manual !!!
.README_TO_RESTORE
Find ESXi:%s
esxcli vm process list
World ID:
Process ID:
Running VM:%ld  ID:%d   %s
Total VM run on host:   %ld
```

From the debug messages, we can see that the ransomware uses ESXi's `esxcli` command-line management tool to list the running virtual machines on the server and then shut them down.

Ransomware gangs targeting ESXi servers will shut down virtual machines before encrypting files to prevent the files from being locked and to avoid data corruption.

> Some Darkside affiliates have a tendency to forget to stop all the ESXi daemons before kicking off the encryption. The result is that sometimes encrypted data can be interlaced with unencrypted data or that the footer containing the file key is partially overwritten. Same result.
>
> — Fabian Wosar (@fwosar) April 14, 2021

When shutting down the virtual machines, the ransomware will first try a graceful shutdown using the 'soft' command:

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

If there are still VMs running, it will try an immediate shutdown of virtual machines using the 'hard' command:

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

Finally, if virtual machines are still running, the malware will use the 'force' command to shut down any running VMs forcefully.

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

After the virtual machines are shut down, the ransomware will begin encrypting **.vmdk** (virtual hard disk), **.vmsd** (metadata and snapshot information), and **.vmsn** (contains the active state of the VM) files.

This method is very efficient as it allows a ransomware gang to encrypt many virtual machines with a single command.

Last month, MalwareHunterTeam also found a Linux version of the REvil ransomware that targets ESXi servers and used the esxcli command as part of the encryption process.

Emsisoft CTO Fabian Wosar told BleepingComputer at the time that other ransomware operations, such as Babuk, RansomExx/Defray, Mespinoza, GoGoogle, and the now-defunct DarkSide, 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.

A bit about HelloKitty

HelloKity has been in operation since November 2020, when a victim first posted about the ransomware in our forums.

Since then, the threat actors have not been particular actively compared to other human-operated ransomware operations.

Their most well-known attack has been against CD Projekt Red, where the threat actors encrypted devices and claim to have stolen source code for Cyberpunk 2077, Witcher 3, Gwent, and more.

The threat actors later claimed that someone had purchased the files stolen from CD Projekt Red.

This ransomware, or its variants, has been used under different names such as DeathRansom and Fivehands.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Hive ransomware ports its Linux VMware ESXi encryptor to Rust

Shutterfly services disrupted by Conti ransomware attack

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

- FiveHands
- HelloKitty
- 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

Comments

-

  RealityBites - 10 months ago

  Hacking is terrorism, simply start posting rewards for hackers heads.

- sylokdefiled Photo
  sylokdefiled - 10 months ago
    -
    -

  https://twitter.com/fr0gger_/status/1417015272679030784
  Decryptor available.

-
  kimikoa2 - 10 months ago
    -
    -

  <p>Can Lawrence Abrams, or whomever edits these posts, do a simple grammar check and proof-read before posting... &quot;... it uses its own customer kernel.&quot; - as in, a kernel that a customer paid for? but you meant &#39;custom&#39; right? &quot;... not been particular actively compared to other human-operated ransomware operations.&quot; - actively compared to, vs &quot;active, compared to&quot; And I&#39;m sure there&#39;s others, but it makes it hard to read when you see errors like this. Come on... Jesus</p>

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: