Linux version of BlackMatter ransomware targets VMware ESXi servers

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

Lawrence Abrams

By
Lawrence Abrams

- August 5, 2021
- 05:32 PM
- 0

The BlackMatter gang has joined the ranks of ransomware operations to develop a Linux encryptor that targets VMware's ESXi virtual machine platform.

The enterprise is increasingly moving to virtual machines for their servers for better resource management and disaster recovery.

With VMware ESXi being the most popular virtual machine platform, almost every enterprise-targeting ransomware operation has begun to release encryptors that specifically target its virtual machines.

BlackMatter targets VMware ESXi

Yesterday, security researcher MalwareHunterTeam found a Linux ELF64 encryptor [VirusTotal] for the BlackMatter ransomware gang that specifically targets VMware ESXi servers based on its functionality.

BlackMatter is a relatively new ransomware operation that started last month and is believed to be a rebrand of DarkSide. After researchers found samples, it was determined that the encryption routines used by the ransomware were the same custom and unique ones used by DarkSide.

DarkSide shut down after attacking and shutting down Colonial Pipeline and then feeling the total pressure of international enforcement and the US government.

From the sample BlackMatter's Linux encryptor shared with BleepingComputer, it is clear that it was designed solely to target VMWare ESXi servers.

Advanced Intel's Vitali Kremez reverse engineered the sample and told BleepingComputer that the threat actors created an 'esxi_utils' library that is used to perform various operations on VMware ESXi servers

```
/sbin/esxcli
bool app::esxi_utils::get_domain_name(std::vector >&)
bool app::esxi_utils::get_running_vms(std::vector >&)
bool app::esxi_utils::get_process_list(std::vector >&)
bool app::esxi_utils::get_os_version(std::vector >&)
bool app::esxi_utils::get_storage_list(std::vector >&)
std::string app::esxi_utils::get_machine_uuid()
bool app::esxi_utils::stop_firewall()
bool app::esxi_utils::stop_vm(const string&)
```

Kremez told us that each function would execute a different command using the esxcli command-line management tool, such as listing VMs, stopping the firewall, stopping a VM, and more.

For example, stop_firewall() function will execute the following command:

```
esxcli network firewall  set --enabled false
```

While the stop_vm() will execute the following esxcli command:

```
esxcli vm process kill --type=force --world-id [ID]
```

All ransomware that targets ESXi servers attempts to shut down virtual machines before encrypting the drives. This is done to prevent data from being corrupted while it is encrypted.

Once all the VMs are shut down, it will encrypt files that match specific file extensions based on the configuration included with the ransomware.

Targeting ESXi servers is very efficient when conducting ransomware attacks, as it allows the threat actors to encrypt numerous servers at once with a single command.

As more businesses move to this type of platform for their servers, we will continue to see ransomware developers focus primarily on Windows machines but also create a dedicated Linux encrypted targeting ESXi.

Emsisoft CTO Fabian Wosar told BleepingComputer that other ransomware operations, such as REvil, HelloKitty, Babuk, RansomExx/Defray, Mespinoza, GoGoogle, have also created Linux encryptors for this purpose.

Related Articles:

Hive ransomware ports its Linux VMware ESXi encryptor to Rust

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Beware: Onyx ransomware destroys files instead of encrypting them

Karakurt revealed as data extortion arm of Conti cybercrime syndicate

Shutterfly services disrupted by Conti ransomware attack

- BlackMatter
- DarkSide
- Encryptor
- Linux
- Ransomware
- Server
- 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: