

Linux version of BlackMatter ransomware targets VMware ESXi servers

By Lawrence Abrams

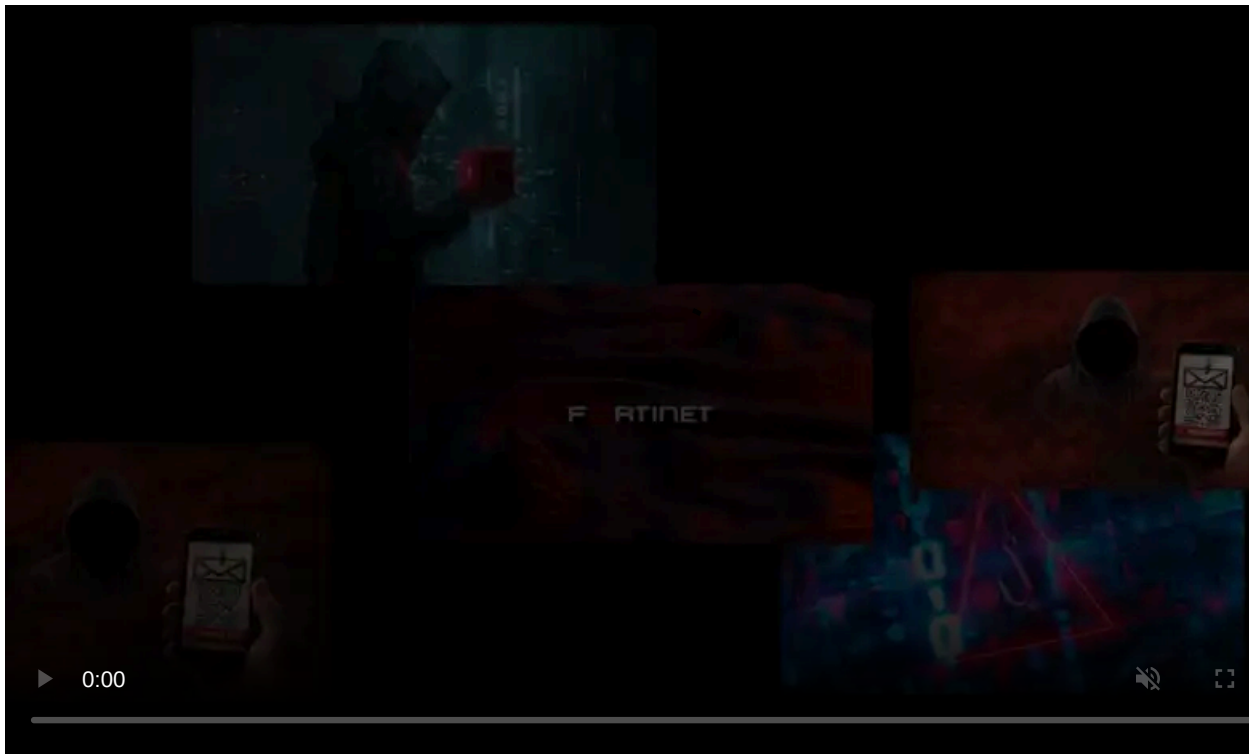
Published: 2021-08-05 · Archived: 2026-04-05 20:29:01 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

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 >8)
bool app::esxi_utils::get_running_vms(std::vector >8)
bool app::esxi_utils::get_process_list(std::vector >8)
bool app::esxi_utils::get_os_version(std::vector >8)
bool app::esxi_utils::get_storage_list(std::vector >8)
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.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/linux-version-of-blackmatter-ransomware-targets-vmware-esxi-servers/>