ESXi-Targeting Ransomware: The Threats That Are After Your Virtual Machines (Part 1)

By Giovanni Vigna, Oleg Boyarchuk

Published: 2022-09-28 · Archived: 2026-04-05 16:28:27 UTC

Introduction

In recent months, we have observed in our telemetry an increase in ransomware that targets ESXi servers.

Since virtualization is the foundation of any large-scale deployment of computing and storage resources, it is not surprising that ransomware actors have now expanded their targets to include virtualization servers: with a single attack it is possible to shut down entire data centers and affect virtualized storage that is shared among workloads, with devastating effects.

In the following, we provide a comprehensive overview of the families of ransomware that target ESXi servers.

Babuk

The ransomware called Babuk appeared in the beginning of 2021. Babuk's builder, which leaked to the public later that year, was used to generate Windows and Linux executables, and it included the VMware ESXi encryptor. The full source code of this ransomware was published by the author on one of the hacker forums later that year.

The only parameter the ESXi encryptor expects during execution is the path to the target directory. It scans the directory for the presence of files with .log, .vmdk, .vmem, .vswp and .vmsn extensions. Once it finds them, it encrypts them with the stream cipher Sosemanuk.

Babuk drops a text file "How To Restore Your Files.txt" with a ransom note in every folder containing encrypted files. Interestingly, Babuk does not shut down the ESXi virtual machines before encrypting their files. This may cause file corruption or lead to the inability to decrypt files.

IOCs:
4fa565cc2ebfe97b996786facdb454e4328a28792e27e80e8b46fe24b44781af (Builder)
Dc90560d7198bf824b65ba2cfbe403d84d38113f41a1aa2f37f8d827fd9e0ceb (ESXi encryptor)

AvosLocker

AvosLocker, specifically targeting Windows machines, was discovered in 2021. One year later, in the beginning of 2022, its Linux variant, targeting VMware ESXi instances, was discovered. As for many other ransomware families, AvosLocker's selling model is Ransomware-as-a-Service (RaaS).

If the target directory for the ESXi encryptor is /vmfs/volumes, then the tool searches only for files with .log, .vmdk, .vmem, .vswp, .vmsn extensions. Otherwise, it recursively encrypts all files in the given directory. Before

the file encryption starts, AvosLocker shuts down the ESXi virtual machines using the esxcli command-line utility.

AvosLocker uses a combination of the stream cipher Salsa20 and RSA. When the encryption is completed, it appends the .avoslinux or .avos2 extension to the filename. At the end, it drops a text file "README_FOR_RESTORE", which contains a ransom note.

IOCs:
0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6

BlackCat

BlackCat, also known as ALPHV is the first widely known ransomware written in the Rust programming language. Its appearance in late 2021 was highlighted by the ability to target many platforms, including VMware ESXi. BlackCat operates under the Ransomware-as-a-Service (RaaS) model.

Like many other ransomware families, for encryption BlackCat has chosen a combination of the stream cipher Salsa20 and RSA. Before starting the encryption, BlackCat shuts down the virtual machines with the esxcli command-line utility.

The tool targets files with all extensions. The extension that the ransomware adds to the names of the encrypted files looks like a random combination of alphabetic characters and digits and it is always specific to the system. Examples of the extensions are .dkrpx75 , .kh1ftzx, and .wpzlbji. After encryption, the tool drops a text file "RECOVER- XXXXXXX -FILES.txt" with a ransom note ("XXXXXXX" is the extension added to encrypted files).

IOCs:
3a08e3bfec2db5dbece359ac9662e65361a8625a0122e68b56cd5ef3aedf8ce1

Hive

The Hive ransomware group, working under the RaaS model, was discovered in June 2021. Four months later, in October 2021, the first variant targeting VMware ESXi, written in Golang, was observed. According to ESET, the sample couldn't run properly. Following the BlackCat's trend, around March 2022, the authors of Hive ported their product to the Rust programming language.

IOCs:
6a0449a0b92dc1b17da219492487de824e86a25284f21e6e3af056fe3f4c4ec0
2e52494e776be6433c89d5853f02b536f7da56e94bbe86ae4cc782f85bed2c4b

Luna

The Luna ransomware appeared in July 2022. Unlike its competitors, this threat targeted VMware ESXi instances from the day it started operating. The Luna threat actors chose the cross-platform programming language Rust to develop its ransomware components. Similar to other ransomware threats, Luna operates as RaaS.

The ESXi encryptor targets all folders and files except for the set of those that can be found only on Windows: OpenServer, Windows, Program Files, Recycle.Bin, ProgramData, AppData, All Users; .ini, .dll, .exe, .lnk. For file encryption the ransomware uses a combination of X25519 and AES. Unlike most of the competitors, Luna does not shut down the virtual machines, which may lead to file corruption or inability to decrypt the encrypted files.

When the file is encrypted, Luna appends the .Luna extension to the file's name and then creates a text file "readme-Luna.txt" with a ransom note.

IOCs:
1cbbf108f44c8f4babde546d26425ca5340dccf878d306b90eb0fbec2f83ab51

REvil

REvil (aka Sodinokibi) is one of the most notorious ransomware gangs. It was formed in 2019 and since then operated following the RaaS model. In June 2021 the ransomware started targeting VMware ESXi instances. The alleged authors were arrested by the Russian authorities in January 2022, but as of today (September 2022) the gang is still believed to be active.
REvil's ESXi encryptor can be executed without parameters. It will then immediately start encrypting all files in the current directory. Before encrypting the files, the tool tries to shut down the virtual machines with the esxcli command-line utility. When the files are encrypted, it appends a specific extension to the file's name, e.g., .rhkrc, .qoxaq, .naixq. In the folder, where the encrypted files are locates, it also drops the "XXXXX-readme.txt" file with a ransom note (the XXXX string is replaced with the chosen random extension).

IOCs:
ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4

HelloKitty

The HelloKitty ransomware emerged in late 2020. Unlike most families, which operate under the Ransomware as a Service (RaaS) model, HelloKitty is used exclusively by the gang ViceSociety, who targets companies using human-operated double-extortion campaigns. In July 2021 an encryptor that targeted explicitly VMware ESXi systems was discovered.

The target path must be given to the ESXi encryptor as a parameter during execution. Before the file encryption starts, the tool tries to shut down the virtual machines with the esxcli command-line utility.

For file encryption the tool uses a combination of the symmetric key encryption cipher AES and the public key encryption cipher RSA. After the file is encrypted, HelloKitty appends the .crypt extension to the file's name and then drops a "<file_name>.tmp.README_TO_RESTORE" with a ransom note in the same folder where the file resides.

IOCs:
8f3db63f70fad912a3d5994e80ad9a6d1db6c38d119b38bc04890dfba4c4a2b2

Black Basta

The first samples of the Black Basta ransomware date back to February 2022. Five months later, in June 2022, the gang released a new encryptor targeting VMware ESXi. The ransomware operates following the RaaS model.

Being executed without parameters, the ESXi encryptor starts encrypting all files in the /vmfs/volumes folder, where the files of the ESXi virtual machines reside.

The encryptor uses a combination of the stream cipher ChaCha20 and RSA. After encryption, the tool adds the .basta extension to the encrypted file and then drops a "readme.txt" text file with a ransom note. Unlike most of the ESXi encryptors, Black Basta does not shut down the virtual machines prior to encryption, which may lead to file corruption and inability to decrypt the encrypted files.

IOCs:
0d6c3de5aebbbe85939d7588150edf7b7bdc712fceb6a83d79e65b6f79bfc2ef

DarkSide/BlackMatter

The actors behind DarkSide initially distributed REvil ransomware but grew tired of sharing the profits with the REvil ransomware-as-a-service (RaaS) operator, so decided to create their own ransomware. The DarkSide ransomware has been used to target a wide variety of organizations across North America and Europe.

Most famously, the U.S. fuel distribution company, Colonial Pipeline, was held ransom by DarkSide, dramatically affecting gasoline distribution on the East Coast. DarkSide initially targeted Windows hosts but quickly evolved to include Linux targets— and in particular, those running on ESXi servers. These servers are usually targeted after the threat actors gain access to a VMware vCenter deployment, often by means of stolen credentials.

The DarkSide ransomware uses the ChaCha20 and RSA cyphers for encryption, and adds a ".darkside" extension to the files, eventually dropping a ransom note named "darkside_readme.txt".

BlackMatter is considered an evolution of the DarkSide ransomware.34 Interestingly, the actors behind BlackMatter made sure to publicly announce that they were not targeting specific verticals, such as healthcare, oil and gas, government, and critical infrastructure companies— possibly following the backlash that the Colonial Pipeline attack created, and the unwanted attention that the DarkSide operators received.

IOCs:
984ce69083f2865ce90b48569291982e786980aeef83345953276adfcbbeece8
9cc3c217e3790f3247a0c0d3d18d6917701571a8526159e942d0fffb848acffb
c93e6237abf041bc2530ccb510dd016ef1cc6847d43bf023351dce2a96fdc33b
da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5

Defray777/RansomEXX

Defray777 is a Linux-based, command-line driven ransomware that employs traditional methods for enumerating folders and files on a system and then encrypts them using hardcoded encryption keys. Typically, this malware

requires a set of command line arguments that specify the folder in which the ransomware should start its encryption.

The malware then enumerates through all folders and files in the specified directory, targeting files names that do not contain the encrypted extension nor file names that match the ransom note filename. Finally, the ransom note is created and written on the filesystem.

Analysis of the code within the Defray777 malware suggests that it is an evolution of the RansomEXX ransomware threat. This is based partially on the similarities of hardcoded data but also very similar programming styles.

IOCs:
cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849

GwisinLocker

GwisinLocker, a ransomware targeting companies exclusively in South Korea, was discovered in July 2022. It supports both Windows and Linux systems. The latter variant is targeting also the VMware ESXi systems. Being executed without parameters, the ESXi encryptor starts encrypting all files in the system. It has the ability to shut down the virtual machines. This feature is not active by default.

GwisinLocker combines the symmetric cipher AES and RSA. After the file is encrypted, it adds the extension, which consists out of random characters, to the file's name and then creates another file with the same name and "0" (zero character) appended, where it stores the encrypted AES key for the encrypted file. Afterwards, it creates the "!!!_HOW_TO_UNLOCK_XXXXX_FILES_!!!.TXT" text file with a ransom note, where XXXXX is the appended extension.

IOCs:
7594bf1d87d35b489545e283ef1785bb2e04637cc1ff1aca9b666dde70528e2b

Cheerscrypt

The Cheerscrypt ransomware was discovered in May 2022. The code of Cheerscrypt showed many similarities with the code of Babuk, specifically its ESXi encryptor. It's no surprise that the authors of Cheerscrypt took the Babuk's C code as the basis for their project.

One of the key differences from Babuk is that, prior to file encryption, Cheerscrypt shuts down the virtual machines with help of the esxcli command-line utility.

For file encryption, Cheerscrypt uses a combination of the stream cipher Sosemanuk and ECDH, similar to what Babuk does. After encryption, the tool appends the .Cheers extension to the file's name and then drops the text file "How To Restore Your Files.txt" with a ransom note.

IOCs:
Unavailable at the time of writing.

RedAlert

The RedAlert ransomware, targeting VMware ESXi, was discovered in July 2022. Unlike its competitors, it can be configured using a number of parameters. For example, -w parameter can be used to stop all running virtual machines with the help of the esxcli command-line utility while -r can be used to enable the recursive encryption mode.

One interesting feature of the encryptor, which differentiates it from the other ransomware samples, is that it requires root privileges. Before any encryption attempt it tries to drop a configuration file to the root directory and fails to do so when running under the privileges of a normal user.

The encryptor is targeting files with .log, .vmdk, .vmem, .vswp, .vmsn extensions only. For encryption, it uses a combination of AES and, the public key cryptosystem NTRUEncrypt, which is unusual. After the file is encrypted, it adds the .crypt[number] extension to the file's name and then drops the "HOW_TO_RESTORE" text file with a ransom note.

IOCs:
039e1765de1cdec65ad5e49266ab794f8e5642adb0bdeb78d8c0b77e8b34ae09

Lockbit

Lockbit became one of the most prolific ransomware families known today. Discovered in 2019, it operates under the RaaS model. Its VMware ESXi encryptor component is one of the oldest, and was discovered back in October 2021.

The tool is able to shut down virtual machines by executing the esxcli command-line utility, and it uses a combination of AES and ECC (Curve25519) for encryption. This ransomware tool appends the .lockbit extension to the file's name and then drops a text file with a ransom note.

IOCs:
f3a1576837ed56bcf79ff486aadf36e78d624853e9409ec1823a6f46fd0143ea

Conti

The Conti ransomware appeared in December 2019. Like many other ransomware families, it operates following the RaaS model. In March 2022, the source code of the Windows version of the ransomware and the builder, as well as the gang members' chats were leaked, exposing their conversation about plans to build an ESXi encryptor. One month later, in April 2022, the ESXi encryptor was discovered.

The ESXi encryptor requires the target directory to be specified. All files in that directory will be encrypted. The tool is also able shut down virtual machines prior encryption with help of the esxcli command-line utility.

For file encryption the tool uses a combination of the stream cipher Salsa20 and RSA. After encryption, it appends the .conti extension to the filenames and then drops the text file readme.txt with a ransom note.

IOCs:
95776f31cbcac08eb3f3e9235d07513a6d7a6bf9f1b7f3d400b2cf0afdb088a7

Conclusions

Ransomware can be a devastating threat. ESXi-targeting ransomware can cause infrastructure-level damage that require substantial resources for recovery and mitigation. Therefore, it is important to understand this type of threat, and create countermeasure to prevent the compromise of ESXi hosts.

VMware provides a collection of resources to protect your infrastructure against ransomware.

In addition, VMware's NSX Advanced Threat Protection delivers the broadest set of threat detection capabilities that span network IDS/IPS and behavior-based network traffic analysis.

This also includes VMware NSX Sandbox, a network sandbox offering based on a full-system emulation technology that has visibility into every malware action. VMware NSX is purpose-built to protect data center traffic with the industry's highest fidelity insights into advanced threats.
