SECUINFRA Falcon Team • 07.02.2023 | Incident Response | Vulnerabilities

Hide your Hypervisor: Analysis of ESXiArgs Ransomware

Inhalt

In this blog post we will be analyzing the recent "ESXiArgs" Ransomware variant, which spread to a large number of outdated, internet-exposed ESXi Servers around the world.

Attack Vectors

In the past Ransomware targeting ESXi Hypervisors was largely human-operated as a later stage of general Ransomware attack, where other Assets (Clients, Servers) are encrypted first. Accessing these virtualization systems usually involves acquiring credentials first and changing configuration options to allow for remote access to the Hypervisor, where the ransomware is executed by the attacker through a **"hands-on-keyboard" attack**.

This changed in late 2022 when Juniper Threat Labs first **discovered a novel Backdoor** targeting ESXi Hypervisors. A few weeks later this Backdoor script would be the first post-exploitation component of an automated Ransomware campaign named "ESXiArgs" (after the targeted systems and the file extension .args). The spread of ESXiArgs Ransomware surged starting on February 2nd 2023 when automated exploitation of the Vulnerability **CVE-2021-21974** hit many internet-facing ESXi deployments hosted with e.g. **OVH**, Hetzner and other Hosters around the world. The OpenSLP (Service Location Protocol) on Port 427/tcp is exploited through a Heap-Overflow leading to Remote Code Execution on the ESXi system. **Public exploitation tools** have been available since June 2021. According to the warning issued by **CERT-FR** the vulnerability affects unpatched systems running the following ESXi versions:

- ESXi versions 7.x before ESXi70U1c-17325551
- ESXi versions 6.7.x before ESXi670-202102401-SG
- ESXi versions 6.5.x before ESXi650-202102101-SG

Figure 1: Censys Search for ESXiArg victims

Analysis of ESXiArgs Ransomware

Figure 2: Ransomnote displayed on the ESXi Webinterface of a compromised system

After the initial exploitation of CVE-2021-21974 the threat actors persist the “vmtools.py” Backdoor script that was previously analyzed by Juniper Threat Labs. The Web Shell consists of a HTTP Server on Port 8008 that accepts post requests with a specified command structure. Requests with the action “local” run commands on the Hypervisor system and output to the web shell. Using the “remote” action the attackers can open a reverse shell to the specified host IP and port.

Figure 3: vmtools.py Script – used for a Web Shell

Once persistence on the Hypervisor is achieved the threat actors transfer the Ransomware components to the system through an archive file called “archieve.zip”, which contains the Ransomnotes for the Web Interface and SSH Message of the Day as well as a Bash script and an ELF binary for the file encryption.

ESXiArgs Ransomware is implemented in the Bash script while the supplied ELF binary is only used for the encryption process. Let’s look at the script first:

First ESXiArgs collects a list of disk and swap files for the configured VMs on the Hypervisor and renames them. In contrast to many other ESXi Ransomware implementations ESXiArgs does not use utilities like “esxcli”, “vmware-cmd” or “vim-cmd”

Figure 4: Information Gathering and killing vmx

When encrypting VM data ESXiArgs iterates through a list of volumes and tries to encrypt VM storage and configuration files using intermitted encryption blocks. The information which file to encrypt is passed as arguments to the “encrypt” binary which we will analyze shortly.

Figure 5: File Encryption Routine

After encrypting the VM files the Ransomware drops two Ransomnotes: The first one will overwrite the vSphere Web Interface (see Figure 2) and the second one will overwrite the SSH Message of the Day to be displayed on Login.
To cover their tracks and make following investigations more difficult ESXiArgs deletes Log-Files from the system.

Figure 6: Dropping the Ransomnote and deleting Log files

Lastly ESXiArgs will remove it’s persistence (e.g. via /etc/rc.local.d/local.sh) and delete all artifacts used for the encryption process to act as an Anti-Analysis measure.

Figure 7: Deletion of artifacts and persistence

The ESXiArgs “encrypt” binary is a 64bit LSB ELF file with the debug information still intact. Still it only handles the actual file encryption it is relatively small with a file size of

Figure 8: Information on the “encrypt” binary

The binary features a usage dialog and requires the RSA Public Key, the file path and values for the intermitted encryption to be passed as arguments.

Figure 9: Help menu for the “encrypt” binary

The file encryption is done through a combination of asymmetric RSA and symmetric Sosemanuk algorithms. Sosemanuk is part of the eSTREAM portfolio and a relatively rare sight in Ransomware. From the debug information contained in the binary we suspect that the threat actors may have based their implementation on this **Github repository**.

Figure 10: Sosemanuk and RSA encryption routines

Recovery Options

from YoreGroup Tech Team have documented a recovery workflow **here**, which might help victims to restore their VMs in a timely manner. It seems that this process only applies to VM with "thin provisioned" storage though.
Update (2023-02-08): CISA released a recovery script for affected Hypervisors, you can find it on **GitHub**.

Steps to protect your Hypervisor

1 – **Keep your Hypervisor up-to-date**: Affected ESXi versions should be upgraded to the latest patch immediately. Versions that reached the End-of-Life in terms of vendor support should be decommissioned and migrated to a more recent version.

2 – **Do not expose your Hypervisor to the public Internet**: This includes all management interfaces (LAN, IPMI) but also protocols and features such as SSH, OpenSLP, SNMP and vSphere (which should all be disabled by default). Network access to the Hypervisor should be restricted through a firewall.

3 – **Back up your Hypervisor**: As with any other system affected by Ransomware, keeping Backups is a key step in restoring the service in a timely manner. This includes Virtual Harddisk files as well as VMware configuration data for the VMs.

4 – **Use Syslog to retain Logs**: ESXiArgs and many other Hypervisor-specific Ransomware target Log files on the system for deletion to prevent further investigation, so it is important to export and store these logs safely.

5 – **Disable the execution of unsigned software**: The configuration option *execInstalledOnly* restricts the ESXi to only execute so-called vSphere Installable Bundles (VIB) which refers to ESXi software components or VMware-approved third party applications. Any unsigned Ransomware binaries could therefore not be run on the system. It is important to understand that this configuration option should be persisted through UEFI SecureBoot (which requires a supported Hardware TPM) to defend against human-operated Ransomware. More information about this feature can be found **here**.

authentication attempts and temporary lockouts if they fail to authenticate.

Yara rules

Yara rules for the Python, Bash and Binary files utilized by ESXiArgs Ransomware can be found in our **Github repository**.

Indicators of Compromise

Samples

The Ransomware samples were procured through an **affected victim on the BleepingComputer Forum**.

11b1b2375d9d840912cfd1f0d0d04d93ed0cddb0ae4ddb550a5b62cd044d6b66 encrypt

10c3b6b03a9bf105d264a8e7f30dcab0a6c59a414529b0af0a6bd9f1d2984459 encrypt.sh

773d147a031d8ef06ee8ec20b614a4fd9733668efeb2b05aa03e36baaf082878 vmtools.py

Filenames

vmtools.py
encrypt
/tmp/tmpy_8th_nb
nohup.out
public.pem
archieve.zip
motd

MITRE ATT&CK Mapping

Reconnaissance	Active Scanning: Vulnerability Scanning (T1595.002)	Threat Actors behind ESXiArgs are actively scanning for vulnerable ESXi Servers	CVE-2021-21974 artifacts
Initial Access	Exploit Public-Facing Application (T1190)	Explotation of OpenSLP	CVE-2021-21974 artifacts
Execution	Command and Scripting Interpreter: Python (T1059.006)	Backdoor/Web Shell implemented in Python	vmtools.py
Persistence	Boot or Logon Initialization Scripts: RC Scripts (T1037.004)	Persisting the Python backdoor	/etc/rc.local.d/local.sh
Command and Control	Non-Standard Port (T1571)	Web Shell implemented in vmtools.py	HTTP Post Server on Port 8008

Execution	Command and Unix Shell (T1059.004)	Ransomware functionality is	encrypt.sh
Impact	Data Encrypted for Impact (T1486)	VM data is encrypted via RSA+Sosemanuk	encrypt binary
Impact	Service Stop (T1489)	Ending a process to power down VMs	Killing the vmx process in encrypt.sh
Impact	Defacement: External Defacement (T1491.002)	Defacement of the vSphere Web Interface	Overwriting index.html with the Ransomnote
Impact	Defacement: Internal Defacement (T1491.001)	Defacement of the SSH MOTD	Overwriting motd with the Ransomnote
Defense Evasion	Indicator Removal: Clear Linux or Mac	Log file deletion	Deleting all .log files