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In this blog post we will be analyzing the recent "ESXiArgs" Ransomware variant, which spread to a large number of outdated, internet-exposed ESXi Servers around the world.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

"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

At the time of writing there are nearly 2500 ESXi systems exposed to the Internet that are affected by ESXiArgs Ransomware (Figure 1 shows the results of a Censys search filtered for the Ransomnote being present on the ESXi Web Interface).

Figure 1: Censys Search for ESXiArg victims

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

Figure 3: vmtools by 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 p[illegible]cript first:

First ESXiArgs collects a list of disk and swap files for the configured VMs on the Hypervisor and renames them. [illegible] many other ESXi Ransomware implementations ESXiArgs [illegible] “vmware-cmd” or “vim-cmd” to power down running VMs to be able to encrypt them, but rather it just terminates the vmx process. This action could potentially lead to errors or corruption of VM data.

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 [illegible] 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 encrypt[illegible] 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 48KB.

Figure 8: Information on the "encrypt" binary

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

Before any recovery of virtual machines in attempted the ESXi Hypervisor should be secured and backed up. In some cases, the encryption may have failed to encrypt the VM data correctly and therefore some can be recovered. Enes Sonmez & Ahmet Aykac 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.

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**.

6 – **Review user authentication**: User authentication should not be done through Active Directory to prevent Lateral Movement to the Hypervisor in case of a Domain Controller compromise. Local user accounts should be restricted to a Password Policy, limited authentication attempts and temporary lockouts if they fail to authenticate.

Yara rules

We provide the Yara rules, Bodies and Binary of the utility by ESXiArgs that we have found in our GitHub repository.

Indicators of Compromise

Samples

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

11b1b2375d9d840912cfd1f0d0d04d93ed0cddb9ae4ddb559e5b62cd044d6b66 encrypt

encrypt.sh

773d147a031d8ef06ee8ec20b614a4fd9733668efeb2b05aa03e36baaf082878 vmtools.py

Filenames

vmtools.py

encrypt

/tmp/tmpy_8th_nb

nohup.out

public.pem

archieve.zip

motd

MITRE ATT&CK Mapping

Tactic	Technique	Description	Observable
Reconnaissance	Active Scanning: Vulnerability Scanning (T1595.002)	Threat Actors behind ESXiArgs are actively scanning for vulnerable ESXi Servers	CVE-2021-21974 artifacts

	Application (T1190)		
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 python	HTTP Post Server on Port 8008
Command and Control	Non-Standard Port (T1571)	Reverse Shell implemented in python	Reverse Shell via specified port, default fallback: 427
Execution	Command and Scripting Interpreter: Unix Shell (T1059.004)	Ransomware functionality is implemented in Bash	encrypt.sh
Impact	Data Encrypted for Impact (T1486)	Data is encrypted with 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 of the SSH MOTD	Overwriting motd with the Ransomnote
Defense Evasion	Indicator Removal:	Log file deletion	Deleting all .log files

	Logs (T1070.002)		

SECUINFRA Falcon Team • Autor
Digital Forensics & Incident Response experts

In addition to the activities that are the responsibility of customer orders, the Falcon team takes care of the operation, further development and research of various projects and topics in the DF/IR area.

> all articles