What you need to know about

MITRE ATT&CK v17

New TTPs for ESXi are addressing critical gaps in hypervisor security

For the first time ever, MITRE has included Tactics, Techniques, and Procedures (TTPs) focused on ESXi threats in response to ransomware groups actively targeting the hypervisor layer in virtualized environments.

Overview

The ESXi framework builds off of the existing Linux framework since ESXi is Linux-based with 30 unadapted TTPs, 34 adapted TTPs and 4 new TTPs unique to ESXi. These are fitted into 12 categories focused on the different steps that may be taken during an attack chain: Initial access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command & Control, Exfiltration, and Impact.

How will this impact compliance?

While MITRE ATT&CK isn't a compliance standard, many organizations use the MITRE ATT&CK framework to help align their departments and map their operations to compliance standards like ISO, HIPAA ,and NIST. With the new addition of an ESXi framework, now not securing the hypervisor layer could translate into an auditable gap in security that companies could be liable for. The addition of ESXi to the MITRE ATT&CK framework validates the attack risk many ESXi users have faced and the need for runtime ESXi security.

Highlighting the 4 new ESXi TTPs

- **T1675: ESXi Administration Control:**
  Abusing ESXi administration services
  Resolved with ZeroLock: SSH-MFA & Lockdown Rules
- **T1059.12: Command and Scripting Interpreter: Hypervisor CLI**
  Using hypervisor CLIs for commands
  Resolved with ZeroLock: Lockdown Rules & Application Filtering
- **T1505.006: Server Software Component: vSphere Installation Bundles**
  Abusing VIBs to establish persistent access to ESXi hypervisors
  Resolved with ZeroLock: Application Filtering
- **T1673: Virtual Machine Discovery**
  Enumerating running VMs after gaining access to a host or hypervisor
  Resolved with ZeroLock: Lockdown Rules & AI-behavioral Detection

What can you do to address these new TTPs?

To make sure you are proactively addressing all of the TTPs outlined in MITRE ATT&CK v17, you need a comprehensive approach to your hypervisor security. Vali Cyber's ZeroLock® takes a multilayered approach to hypervisor defense, providing runtime protection at the hypervisor level, featuring SSH-MFA, virtual patching, application filtering, AI detection, automated remediation, and more.

ZeroLock for hypervisors features:

- SSH-MFA
- Lockdown Rules & Virtual Patching
- Application Filtering
- Real-time Threat Detection
- Automated Remediation
- Much more!

Schedule your demo today! info@valicyber.com

valicyber®

ZeroLock®

ZeroLock Endpoint Agent Requirements for Hypervisors

OS	• ESXi, 6.7+ (Older versions supported upon request.) • Nutanix, AHV-2017+ • XenServer, 6.5+ • Citrix Hypervisor, 8.0+ • Proxmox, 3.0+ • Red Hat Enterprise Virtualization (RHEV), 3.6+ • KVM, Kernel 3.5+
Processor	x86-64, ARM-64 (coming soon)
Memory	50MB
Disk Space	100MB
Kernel Mods	No kernel modification or modules required
Installation Methods	• One-line, web-based deployment (Wget) • File-based deployment (Tar.gz or Bash) • ESXi: Signed VIB and deployable via vCenter

ZeroLock Server Requirements (Only required for on-prem deployment.)

RAM	16GB
Disk Space	128GB (Dependent on number of endpoints and data retention period.)
CPU Cores	6 or more recommended
Installation Reqs.	• Self-deployment: Latest version of Docker installed • OVA-deployment: ESXi 7.0 or later

ZeroLock Bidirectional API-First Architecture

Documentation	Visit api.zerolock.com for a full API
Existing Integrations	• SIEM: Splunk, Sumo Logic, Elastic • SOAR: Swimlane • Incident API: Veeam

About Vali Cyber

Vali Cyber, Inc. was founded in 2020 with the mission of addressing the specific security needs of Linux and its derivatives. By focusing on creating a Linux-first security solution with increased efficacy and reduced Total Cost of Ownership (TCO), we created the ZeroLock platform. Our approach puts clients in control of their hypervisor & Linux security by reducing analyst and computational overhead, while simultaneously ensuring uptime with state-of-the-art AI behavioral techniques to stop attacks and automated file rollback to restore your most critical data in milliseconds. Imagine detecting and fully remediating a ransomware attack on your hypervisor in real-time...that dream has become reality.

MADE IN THE U.S.A.

valicyber®