ADVISORY FOR ICM SECTOR

Espionage campaign delivers VSOCKpuppet malware to Telco in Southeast Asia

Original report published on: March 06, 2026

Executive Summary

In February 2026, CrowdStrike observed several VMware ESXi vulnerabilities being exploited on a web server hosted in a Southeast Asian telecommunications provider. The threat actor (TA) gained initial access to a virtual machine (VM)-hosted web server, deployed web shells for command execution, and conducted reconnaissance to expand their foothold within the environment.

TA used an exploit tool (Hardline) to target VMware ESXi vulnerabilities (likely CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226) which enable VM-to-hypervisor escape and the deployment of VSOCKpuppet malware on the ESXi host. This allowed the actor to compromise the underlying hypervisor and establish persistent access across the virtualised environment.

Background

In February 2026, TA likely exploited a file upload vulnerability on an Apache web server hosted on a VM. After gaining access, the actor deployed web shells, a Stowaway backdoor and malware. This malware accepted inbound TCP network connections via port 7475. The malware enabled TA to perform reconnaissance to map the environment, create a new shell process, and expand their foothold through additional hands-on-keyboard (HOK) activity.

Subsequently, TA used the Hardline tool as part of an exploit chain targeting VMware ESXi vulnerabilities enabling escape from the virtual machine and compromise of the underlying hypervisor. This resulted in elevated privileges, system-level modifications, and the deployment of the VSOCKpuppet malware on the ESXi host. TA also executed the PwnKit exploit, likely to obtain root privileges and run additional commands.

VSOCKpuppet malware supports command execution and file transfer, and uses a simplified C2 protocol that does not require an initial handshake. It accepts connections via the VSOCK interface (including port 6667) or from any context between the virtual machine and the hypervisor, enabling persistent control of the compromised environment.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the VSOCKpuppet activity identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Apply vendor patches for CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226 across all vulnerable VMware ESXi environments.
- Enforce strict network segmentation between virtual machines and ESXi management interfaces.
- Restrict administrative access to ESXi hosts and monitor usage.

- Deploy EDR/XDR coverage across all virtual machines and supporting infrastructure to improve visibility into post-compromise tooling, reconnaissance, and lateral movement.
- Monitor ESXi host file systems for suspicious activity, including changes to service configurations such as inetd and other critical system files.
- Monitor ESXi hosts for abnormal system-level modifications, including changes to services, configuration files, and unexpected process execution at the hypervisor layer.
- Monitor ESXi hosts for newly created virtual machines and verify whether they are legitimate or potentially created by a threat actor.
- Conduct regular vulnerability assessments and penetration testing, prioritising internet-facing applications and services exposed to external access.
- Implement application allow listing and integrity controls on ESXi hosts to prevent execution of unauthorised binaries and payloads.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

SHA256 Hash	Description
de0f24485c5cbfe0990d108610361f5b8e9351d48cd137c80791b800a4439961	Malicious Python script (m.py) used to execute shell commands and store command output
a4a29791066858dc95065ce480239c74024d33ee01c5917d3f6376fe834b84f8	Executable (cv) containing VMware ESXi exploit implementations (likely for CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226) and an embedded VSOCKpuppet payload
3567ecf3e17e70af7321c5e736faeec712fcd5bea37a7469e09ad9c54a56e833	Stowaway executable used to connect to IP address 207.254.184[.]247 on port 443
0abb9ba45351da733a189ebffad4ae9b0b32dbd0b1fb725f967c2c3c9655d4ab	PwnKit executable named pwnkit.so
2677dced829b06bab9157266bf4cbea991ba785ddc0a6963c2dcceb2a4e2b4e8	executable named getroot
824ebc51b80953f97bf9ddf2fad3105aff2c5913de6524f0b03f5a49b2169785	web shell named shell.php
6aab0317ce0679ea31ca1c4f86f4d75de2125f015f8b2c7c97301b8204d1a5a0	Web shell named either work_by_del.php or 3.php
7f12f61b2735434a4e13c7861de7d55155782203cae723958f63065b4a2b0bbf	web shell named 3.html
dde3faba655b5c46bcca18a2a95593a829abf7195873fb80586b0d70f24fa09a	web shell named 2.php
21bf235aadab8d618f3ec3f1c95678f2dc471c5d9fe9afebeef2426a84ad12c7	VSOCKpuppet executable

IP Address	Description
207.254.184[.]247	Stowaway C2

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
	T1059.006	Command and Scripting Interpreter: Python
Persistence	T1505.003	Server Software Component: Web Shell
Privilege Escalation	T1068	Exploitation for Privilege Escalation
	T1611	Escape to Host
Defence Evasion	T1562.001	Impair Defenses: Disable or Modify Tools
Discovery	T1082	System Information Discovery
	T1497.001	Virtualization/Sandbox Evasion: System Checks
Collection	T1005	Data from Local System
Command and Control	T1095	Non-Application Layer Protocol
	T1105	Ingress Tool Transfer
	T1571	Non-Standard Port
Exfiltration	T1041	Exfiltration Over C2 Channel

References

1. ESXi Exploitation in the Wild | Huntress