ADVISORY FOR ICM SECTOR

WARP PANDA deployed BRICKSTORM backdoor via VMware vCenter and ESXi

Original report published on: December 4, 2025

Executive Summary

CrowdStrike published a report on WARP PANDA (also known as UNC5221), a threat actor that has been actively targeting the information technology, legal, and manufacturing sectors since 2022.
WARP PANDA has been observed deploying BRICKSTORM, a backdoor malware specifically designed for VMware environments, including VMware vCenter servers and VMware ESXi hypervisors. These systems are widely across various sectors. The threat actor's toolkit also includes JSP web shells and two Golang-based implants—Junction and GuestConduit—tailored for ESXi environments. The adversary avoids detection and is assessed to prioritise maintaining persistent, long-term covert access consistent with intelligence-collection operations to be espionage-oriented, with no immediate indication of intent to disrupt services or operations.

Background

CrowdStrike observed WARP PANDA frequently gaining initial access by exploiting internet-facing systems, subsequently pivoting into vCenter environments using either valid credentials or by exploiting known vCenter vulnerabilities, including CVE-2024-38812, CVE-2021-22005, and CVE-2023-34048.

Following initial access, the threat actor deployed BRICKSTORM backdoor on compromised VMware management servers. BRICKSTORM maintains persistent and covert access, allowing the threat actor to maintain control of the environment whilst blending malicious activities with legitimate administrative operations. JSP web shells and additional malware implants (GuestConduit and Junction) are used to ensure continued access to compromised systems. CrowdStrike has observed the threat actor utilising privileged management accounts (such as vpxuser) and SSH protocols to facilitate lateral movement between compromised networks.

To evade detection and prolong dwell time within victim environments, WARP PANDA has implemented several operational security measures, including:

- Log clearing and manipulation
- File timestamp modification
- Creation of temporary and unauthorised virtual machines

Detection and Mitigation

IMDA recommends that organisations perform continual testing and validation of existing security controls to ensure effective detection and prevention of BRICKSTORM-related activities and other malware implants identified in this advisory:

- Scan for Indicators of Compromise (Annex A) across VMware vCenter, VMware ESXi, management jump hosts and administrative workstations.
- Refer to the MITRE ATT&CK techniques documented in this advisory (Annex B) to:
    - Create, test, and validate detection rules against identified threat behaviours
    - Validate and deny or disable processes, ports, and protocols that have no legitimate business requirement
- Review VMware vCenter and ESXi logs for anomalous administrative activity and unauthorised configuration changes. Hunt for behaviours consistent with:

    - Credential access from virtual machine snapshots
    - Suspicious vCenter tasks and operations
    - Creation of unregistered or rogue virtual machines
    - Anomalous outbound encrypted tunnels originating from management planes
- Monitor for unauthorised or short-lived virtual machine creation and deletion.
- Apply IP whitelist to virtual machine.
- Apply security patches to VMware products and internet-facing systems by prioritising critical and high risk vulnerabilities.
- Restrict access to virtualised management interfaces to trusted networks only, implementing network segmentation where appropriate.
- Review daily the use of privileged and service accounts, including default management accounts such as **vpxuser**.

Annex A – Indicators of Compromise (IOC)

SHA256 Hash	**Description**
0db68331cb52dd3ffa0698144d1e6919779ff432e2e80c058e41f7b93cec042	GuestConduit
88db1d63dbd18469136bf9980858eb5fc0d4e41902bf3e4a8e08d7b6896654ed	Junction
9a0e1b7a5f7793a8a5a62748b7aa4786d35fc38de607fb3bb8583ea2f7974806	Junction
40992f53effc60f5e7edea632c48736ded9a2ca59fb4924eb6af0a078b74d557	Brickstorm
aaf5569c8e349c15028bc3fac09eb982efb06eabac955b705a6d447263658e38	Brickstorm
013211c56caaa697914b5b5871e4998d0298902e336e373ebb27b7db30917eaf	Brickstorm
57bd98dbb5a00e54f07ffacda1fea91451a0c0b532cd7d570e98ce2ff741c21d	Brickstorm
b3b6a992540da96375e4781afd3052118ad97cfe60ccf004d732f76678f6820a	Brickstorm
22c15a32b69116a46eb5d0f2b228cc37cd1b5915a91ec8f38df79d3eed1da26b	Brickstorm
f7cda90174b806a34381d5043e89b23ba826abcc89f7abd520060a64475ed506	Brickstorm
39b3d8a8aedffc1b40820f205f6a4dc041cd37262880e5030b008175c45b0c46	Brickstorm
73fe8b8fb4bd7776362fd356fdc189c93cf5d9f6724f6237d829024c10263fe5	Brickstorm
77b49c854afd6746fee393711b48979376fb910b34105c0e18a3fdc24ea31d5c	Brickstorm
6a67a9769a55ec889a5dd4199b2fc08965d39d737838836853bc13c81c56a800	Brickstorm
ed907d39efd5750236b075ca9fbb1f090d7bf578578c38faab24210d298a60ae	Brickstorm

IP Address	**Description**
208.83.233[.]14	C2 IP Address
149.28.120[.]31	C2 IP Address

Annex B – MITRE ATT&CK Techniques

Tactic	**Technique ID**	**Technique Name**
Resource Development	T1583.001	Acquire Infrastructure: Domains
	T1583.003	Acquire Infrastructure: Virtual Private Server
	T1583.007	Acquire Infrastructure: Serverless
	T1584.008	Compromise Infrastructure: Network Devices

	T1588.001	Obtain Capabilities: Malware
	T1608.003	Stage Capabilities: Install Digital Certificate
Initial Access	T1078.004	Valid Accounts: Cloud Accounts
	T1190	Exploit Public-Facing Application
Persistence	T1078.001	Valid Accounts: Default Accounts
	T1098.001	Account Manipulation: Additional Cloud Credentials
	T1505.003	Server Software Component: Web Shell
Defensive Evasion	T1036.004	Masquerading: Masquerade Task or Service
	T1070.004	Indicator Removal: File Deletion
	T1070.006	Indicator Removal: Timestomp
	T1564.006	Hide Artifacts: Run Virtual Instance
Discover	T1083	File and Directory Discovery
Lateral Movement	T1021.004	Remote Services: SSH
	T1550.001	Use Alternate Authentication Material: Application Access Token
Collection	T1114.002	Email Collection: Remote Email Collection
	T1213	Data from Information Repositories
	T1213.002	Data from Information Repositories: SharePoint
	T1530	Data from Cloud Storage
	T1560.001	Archive Collected Data: Archive via Utility
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
	T1071.004	Application Layer Protocol: DNS
	T1090	Proxy
	T1090.003	Proxy: Multi-hop Proxy
	T1095	Non-Application Layer Protocol
	T1572	Protocol Tunneling
	T1573.002	Encrypted Channel: Asymmetric Cryptography
Exfiltration	T1041	Exfiltration Over C2 Channel

References

[1] CrowdStrike Blog Report
[2] BRICKSTORM Backdoor | CISA