Chinese Threat Actor BrickStorm Targeting VMware vSphere

TL;DR

Chinese state-linked operators (known as BrickStorm/Warp Panda / UNC522) have been gaining access to VMware vSphere environments and deploying a Golang backdoor called BrickStorm.

Once inside, they create hidden VMs, steal VM snapshots, harvest Active Directory data, and use the access to reach cloud apps like Azure, Microsoft 365, OneDrive, and SharePoint.

This campaign has hit U.S. technology, legal, and manufacturing firms throughout 2024-2025.

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), The National Security Agency (NSA), and the Canadian Cyber Centre released a joint malware analysis confirming that Chinese state-sponsored operators are gaining access to VMware vSphere servers using a toolset known as BrickStorm. CISA reviewed eight BrickStorm samples from intrusions where attackers used vCenter and ESXi to build rogue VMs and pull sensitive data while keeping their activity buried in normal traffic.

Affected Products

- VMware vSphere (vCenter, ESXi hosts)
- Windows servers inside vSphere environments
- Azure / Microsoft 365 accounts reachable after on-prem compromise

BrickStorm is written in Go and acts as a stealthy backdoor across VMware and Windows systems. It gives the operator remote control inside vCenter, along with the ability to move traffic through SOCKS tunnels and send commands over encrypted channels. BrickStorm also watches itself and comes back if defenders try to stop it.

The intrusion dates back to April 2024, starting with a DMZ web server and eventually reaching vCenter and the organization's identity systems. Once inside, the attackers gathered the keys and access needed to stay in place. Aspire's security partner, CrowdStrike, has since linked this activity, including BrickStorm and two related implants, to Warp Panda across legal, tech, and manufacturing firms.

BrickStorm hides well inside VMware systems and can put your cloud access at risk. If you use vSphere, vCenter, ESXi, or rely on Azure or Microsoft 365, look over your environment as soon as possible.

Aspire Protects

- Patch - Broadcom has released patched vCenter Server versions to address the exploited vulnerabilities, and the full advisory with fixed builds is available in Broadcom's security bulletin.
- Scan all vCenter, ESXi hosts, and DMZ servers using CISA's YARA/Sigma rules.
- Review VMware logs for unexpected VM creation and snapshot activity.
- Segment vCenter away from DMZ systems and enforce strict firewall rules.
- Block unauthorized DNS-over-HTTPS providers.
- Rotate service accounts, ADFS certificates, and review MFA registration logs.
- Audit Microsoft 365 and Azure logs for unusual directory queries or downloads.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may have exploited vulnerable edge devices and VMware vCenter flaws to gain a foothold.

- Valid Accounts [T1078] – The attacker may have used stolen service accounts or cloud tokens to authenticate into VMware or Microsoft 365 environments.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may have executed commands through BrickStorm's shell access on vCenter or Windows hosts.

Persistence

- Create or Modify System Process, [T1543] – The attacker may have used BrickStorm's self-monitoring routine to restart the backdoor if removed.

  Account Manipulation [T1098] – The attacker may have registered new MFA devices or altered service accounts to maintain long-term access.

IoCs

File Names and Patch

- /usr/lib/vmware/vmware-vsockd
- /usr/lib/vmware/vmware-vmxd
- /usr/lib/vmware/vmware-guestd
- /usr/lib/vmware/vmware-vmxstats

- /usr/lib/vmware/vmware-networkd
- /usr/lib/vmware/vmmetrics
- /tmp/vm*
- /var/log/vmware/*

Processes and Services

- vmware-vsockd
- vmware-vmxd
- vmware-networkd
- vmguestd
- vmguestconduit
- guestconduit
- junction

Domains and URLS

- hxxps://api[.]github[.]com (used in sample traffic)
- hxxps://raw[.]githubusercontent[.]com
- hxxps://dns[.]google[.]com/dns-query (DoH)
- hxxps://cloudflare-dns[.]com/dns-query
- hxxps://mozilla[.]cloudflaredns[.]com/dns-query

IP Addresses

- 104[.]21[.]47[.]113
- 172[.]67[.]215[.]15
- 104[.]16[.]248[.]249
- 104[.]16[.]249[.]249

Hashes

- 3bb8b5f0c7a7c0af6cdaa9fce20bb1bd47c4c18c533e80cd4c7fba9968432e9b
- 7d469fde4b8e9445da32cbae24bafc39a50ee1cd8cdb3b0f5cd542c6da137c31
- dbc767e9f7fa1e59a1c93e6ecfdd8cb557484d45bb8ed6af2c1e573d52f1b5e6
- 01f7c0b07c80e81251e21560de330f94ed1aa267e4cd13ca9cdd9998235a8a3b
- e0a2042cd6ef4b67bfe8074c9187507ff65f63222505cb48eddf72ffc132eaf0
- c7fa8c87bb659b29c33fd89a1d9924fd8e601ccaa71b916328fdd5621e0a701d
- 8611e4a830a60b711d0fd351e5c8a06d84701e7f9ee6aeedc8a0d00913419cbc

- 5a2077c689bcf9c4fbd5b4f3524e636dd7af1e8051573b18e2db7fc1f0ebfd16

Targeted Industries

This campaign targets VMware vSphere and vCenter environments across U.S.-based organizations with long-term access goals.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance
- Technology
- Legal
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will

ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

BRICKSTORM Backdoor | CISA

MALWARE-ANALYSIS-REPORT-BRICKSTORM-BACKDOOR.PDF

cisa.gov/sites/default/files/2025-12/MAR-251165.c1.v1.CLEAR_stix2.json