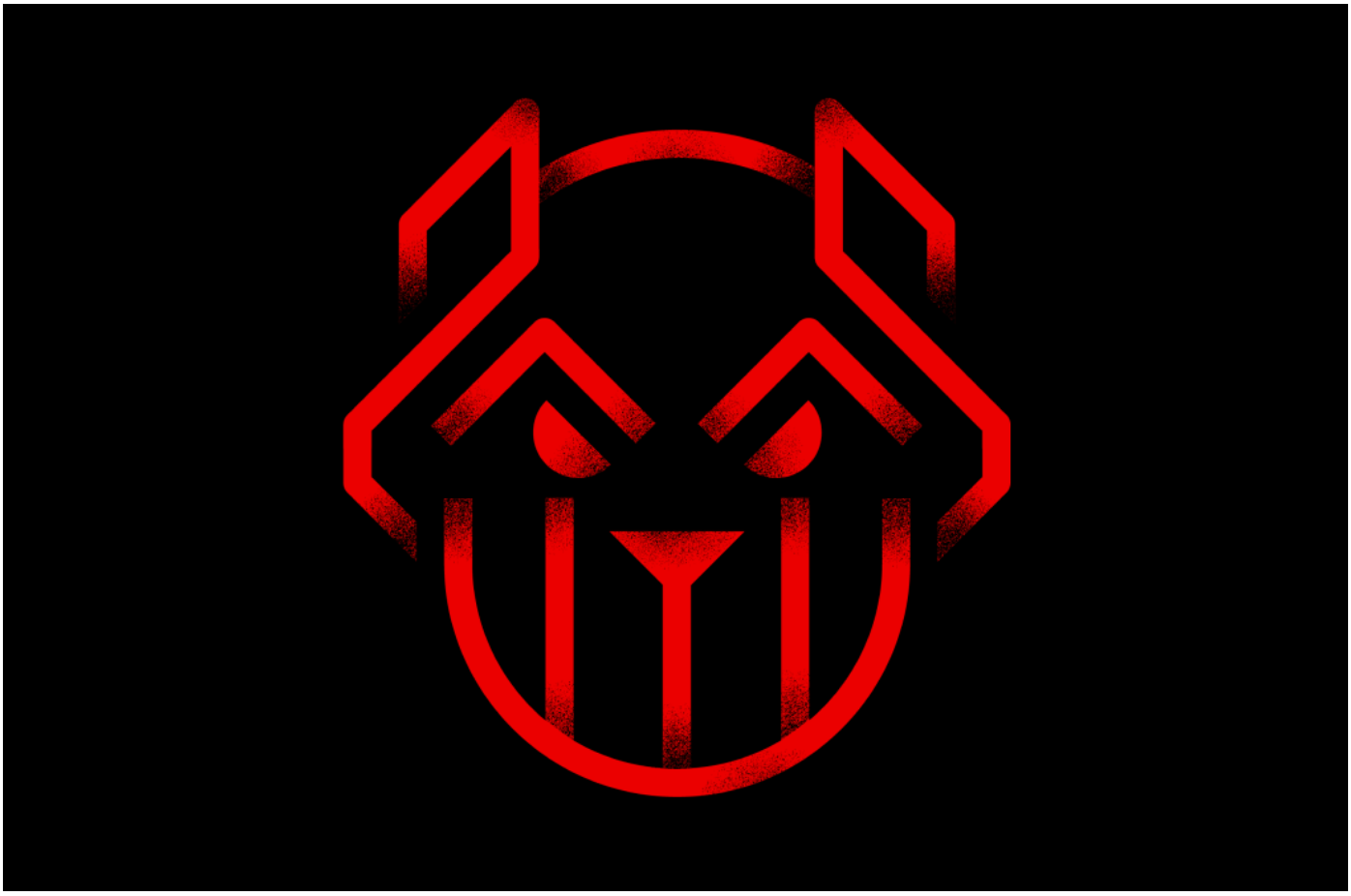
Unveiling WARP PANDA: A New Sophisticated China-Nexus Adversary

crowdstrike.com/en-us/blog/warp-panda-cloud-threats

Counter Adversary Operations



Throughout 2025, CrowdStrike has identified multiple intrusions targeting VMware vCenter environments at U.S.-based entities, in which newly identified China-nexus adversary WARP PANDA deployed *BRICKSTORM* malware. WARP PANDA exhibits a high level of technical sophistication, advanced operations security (OPSEC) skills, and extensive knowledge of cloud and virtual machine (VM) environments. In addition to *BRICKSTORM*, WARP PANDA has also deployed JSP web shells and two new implants for ESXi environments — now named *Junction* and *GuestConduit* — during their operations.

WARP PANDA demonstrates a high level of stealth and almost certainly focuses on maintaining persistent, long-term, covert access to compromised networks. Their operations are likely motivated by intelligence-collection requirements aligned with the strategic interests of the People's Republic of China (PRC).

Details

During the summer of 2025, CrowdStrike identified multiple instances in which the adversary now tracked as WARP PANDA targeted VMware vCenter environments at U.S.-based legal, technology, and manufacturing entities.

WARP PANDA maintained long-term, persistent access to the compromised networks; in one of the intrusions, gaining initial access in late 2023. In addition to deploying JSP web shells and *BRICKSTORM* on VMware vCenter servers, the adversary also deployed two previously unobserved Golang-based implants — *Junction* and *GuestConduit* — on ESXi hosts and guest VMs, respectively.

WARP PANDA frequently gains initial access by exploiting internet-facing edge devices and subsequently pivots to vCenter environments, using valid credentials or exploiting vCenter vulnerabilities. To move laterally within the compromised networks, the adversary uses SSH and the privileged vCenter management account `vpxuser`.[1] In some instances, CrowdStrike identified them using the Secure File Transfer Protocol (SFTP) to move data between hosts.

Using tradecraft focused on stealth and OPSEC, WARP PANDA leverages TTPs that include log clearing and file timestomping, as well as creating malicious VMs[2] — unregistered in the vCenter server — and shutting them down after use. Similarly, in an attempt to blend in with legitimate network traffic, the adversary has used *BRICKSTORM* to tunnel traffic through vCenter servers, ESXi hosts, and guest VMs. *BRICKSTORM* implants masquerade as legitimate vCenter processes and have persistence mechanisms that allow the implants to survive after file deletion and system reboots.

On numerous occasions, CrowdStrike observed WARP PANDA staging data for exfiltration. The adversary used an ESXi-compatible version of 7-Zip to extract and stage data from thin-provisioned snapshots of live ESXi guest VMs. Separately, WARP PANDA leveraged 7-Zip to extract data from VM disks hosted on a non-ESXi Linux-based hypervisor. CrowdStrike Services also found evidence that the adversary used their access to vCenter servers to clone domain controller VMs, likely in an attempt to collect sensitive data such as the Active Directory Domain Services database.

WARP PANDA likely used their access to one of the compromised networks to engage in rudimentary reconnaissance against an Asia Pacific government entity. They also connected to various cybersecurity blogs and a Mandarin-language GitHub repository. Further, during at least one intrusion, the adversary specifically accessed email accounts of employees who work on topics that align with Chinese government interests.

Malware

BRICKSTORM

BRICKSTORM is a backdoor written in Golang that frequently masquerades as legitimate vCenter processes, such as `updatemgr` or `vami-http`.[3] The implant has tunneling and file management capabilities allowing users to browse file systems and download or upload files.

BRICKSTORM uses WebSockets to communicate with command-and-control (C2) infrastructure over TLS and uses multiple methods to obfuscate C2 communications and circumvent network-monitoring measures. These methods include using DNS-over-HTTPS (DoH) to resolve C2 domains, creating multiple nested TLS channels for C2 sessions, and leveraging public cloud services such as Cloudflare Workers and Heroku for C2 infrastructure.[4]

Junction

Junction is a Golang-based implant for VMware ESXi servers that masquerades as a legitimate ESXi service by listening on port `8090`, which is also used by the legitimate VMware service `vvold`. The implant acts as an HTTP server, listening for incoming requests, and has extensive capabilities that include executing commands, proxying network traffic, and communicating with guest VMs through VM sockets (VSOCK).

GuestConduit

GuestConduit is a Golang-based network traffic–tunneling implant that runs within a guest VM and establishes a VSOCK listener on port `5555`. This implant facilitates communication between guest VMs and hypervisors. *GuestConduit* also parses JSON-formatted client requests to mirror or forward network traffic and likely is intended to work with *Junction*'s tunnelling commands.

Vulnerability Exploitation

WARP PANDA has exploited multiple vulnerabilities in edge devices and VMware vCenter environments during their operations (Table 1).

Vulnerability	Description
CVE-2024-21887 and CVE-2023-46805	Vulnerabilities affecting Ivanti Connect Secure VPN appliances and Ivanti Policy Secure gateways; this exploit chain bypasses authentication, enabling arbitrary remote command execution
CVE-2024-38812	Heap-overflow vCenter vulnerability in the DCERPC protocol's implementation
CVE-2023-46747	Authentication-bypass vulnerability affecting select F5 BIG-IP devices
CVE-2023-34048	Out-of-bounds (OOB) write vCenter vulnerability in the DCERPC protocol's implementation; can lead to remote code execution (RCE)

CVE-2021-22005	Critical-severity vulnerability affecting vCenter servers

Table 1. Vulnerabilities exploited by WARP PANDA

Cloud Activity

WARP PANDA is a cloud-conscious adversary capable of moving laterally, accessing sensitive data, and establishing persistence in cloud environments.

In late summer 2025, the adversary exploited access to multiple entities' Microsoft Azure environments, primarily to access Microsoft 365 data stored in OneDrive, SharePoint, and Exchange. In one instance, the adversary obtained user session tokens — likely by exfiltrating user browser files — and tunneled traffic through *BRICKSTORM* implants to access Microsoft 365 services via session replay. The adversary further accessed and downloaded sensitive SharePoint files related to an entity's network engineering and incident response teams.

In at least one case, to establish persistence, the adversary registered a new multifactor authentication (MFA) device via an Authenticator app code after initially logging into a user account. In another intrusion, the adversary used the Microsoft Graph API to enumerate service principles, applications, users, directory roles, and emails.

Conclusion

Active since at least 2022, WARP PANDA is a cloud-conscious targeted intrusion adversary that exhibits advanced technical skills and distinct malware use. To date, WARP PANDA is the only adversary that CrowdStrike Intelligence has observed leveraging *BRICKSTORM*, *GuestConduit*, and *Junction*; however, industry reporting has noted that BRICKSTORM is possibly leveraged by multiple adjacent China-nexus actors.[5]

The adversary primarily targets entities in North America and consistently maintains persistent, covert access to compromised networks, likely to support intelligence-collection efforts aligned with PRC strategic interests.

WARP PANDA will likely maintain their intelligence-collection operations in the near to long term. This assessment is made with moderate confidence based on the adversary's significant technical capabilities and focus on long-term access operations, which suggest they are associated with a well-resourced organization that has heavily invested in cyberespionage capabilities.

Recommendations

These recommendations can be implemented to help protect against the activity described in this blog post:

- Monitor for the creation of unsanctioned VMs; CrowdStrike Services offers a tool to identify unregistered VMware VMs[6]
- Retain and monitor ESXi and vCenter `syslog` via CrowdStrike Falcon® Next-Gen SIEM
- Audit unsanctioned outbound connections to `unexpected network destinations` and known command-and-control (C2) infrastructure associated with BRICKSTORM
- Consider disabling SSH access to VMware ESXi hosts
- Monitor for SSH authentications, specifically authentications as `root` and `vpxuser`
- Forward vSphere `syslog` to an external platform
- For daily administration, leverage local accounts using the principle of least privilege
- Enable ESXi's `execInstalledOnly` enforcement setting
- For ESXi versions 8.0 or later, deactivate shell access for the `vpxuser` account on ESXi hosts
- Restrict outbound internet access from ESXi and vCenter
- Implement strict network segmentation and firewall rules for ESXi management interfaces
- Monitor and restrict nonstandard port usage on ESXi servers, particularly the use of port `8090` and other optional service ports
- Access vCenter only via an identity federation provider that mandates MFA
- Ensure EDR solutions are installed on guest VMs to detect potential tunneling activities
- Install security patches for vSphere infrastructure
- Enforce password policies and regular password rotation
- Regularly rotate administrative credentials and API keys

Appendix

Falcon LogScale Query

This CrowdStrike Falcon® LogScale query detects the activity described in this blog post. Network matches from VMware vSphere infrastructure should be investigated as a priority.

```
// Hunting rule for indicators

case { in("SHA256HashData",
values=["40db68331cb52dd3ffa0698144d1e6919779ff432e2e80c058e41f7b93cec042",
"88db1d63dbd18469136bf9980858eb5fc0d4e41902bf3e4a8e08d7b6896654ed",
"9a0e1b7a5f7793a8a5a62748b7aa4786d35fc38de607fb3bb8583ea2f7974806",
"40992f53effc60f5e7edea632c48736ded9a2ca59fb4924eb6af0a078b74d557"]);
in("RemoteAddressIP4", values=["149.28.120.31", "208.83.233.14"]) } | table([cid, aid,
#event_simpleName, ComputerName])
```

Indicators of Compromise

This table details the IOCs related to the information provided in this blog post.

IOC	Description

40db68331cb52dd3ffa0698144d1e6919779ff432e2e80c058e41f7b93cec042	*GuestConduit* SHA256 hash
88db1d63dbd18469136bf9980858eb5fc0d4e41902bf3e4a8e08d7b6896654ed	*Junction* SHA256 hash
9a0e1b7a5f7793a8a5a62748b7aa4786d35fc38de607fb3bb8583ea2f7974806	*Junction* SHA256 hash
40992f53effc60f5e7edea632c48736ded9a2ca59fb4924eb6af0a078b74d557	*BRICKSTORM* SHA256 hash
208.83.233[.]14	IP address leveraged by WARP PANDA
149.28.120[.]31	IP address leveraged by WARP PANDA

MITRE ATT&CK

This table details the tactics and techniques described in this blog post.

Tactic	Technique	Observable
Resource Development	T1583.001 - Acquire Infrastructure: Domains	WARP PANDA uses Cloudflare DNS services to register C2 domains
	T1583.003 - Acquire Infrastructure: Virtual Private Server	WARP PANDA uses VPS hosting providers
	T1583.007 - Acquire Infrastructure: Serverless	*BRICKSTORM* uses infrastructure hosted behind Cloudflare and has used Cloudflare Workers and Heroku for C2 communications
	T1584.008 - Compromise Infrastructure: Network Devices	WARP PANDA targets internet-facing edge devices
	T1588.001 - Obtain Capabilities: Malware	WARP PANDA has access to *BRICKSTORM*, *Junction*, and *GuestConduit*
	T1608.003 - Stage Capabilities: Install Digital Certificate	WARP PANDA uses TLS certificates on C2 infrastructure

Initial Access	T1078.004 - Valid Accounts: Cloud Accounts	WARP PANDA has gained access to Microsoft Azure environments, specifically targeting Office365 resources
	T1190 - Exploit Public-Facing Application	WARP PANDA has exploited vulnerabilities in internet-facing edge devices to gain initial network access
Persistence	T1078.001 - Valid Accounts: Default Accounts	WARP PANDA has leveraged the legitimate `vpxuser` account for privileged access to vCenter servers
	T1098.001 - Account Manipulation: Additional Cloud Credentials	WARP PANDA has registered a new MFA device using an Authenticator app code
	T1505.003 - Server Software Component: Web Shell	WARP PANDA has used web shells to maintain persistence
Defense Evasion	T1036.004 - Masquerading: Masquerade Task or Service	*BRICKSTORM* and *Junction* masquerade as legitimate VMware processes and services
	T1070.004 - Indicator Removal: File Deletion	WARP PANDA has deleted files to avoid detection
	T1070.006 - Indicator Removal: Timestomp	WARP PANDA has modified file timestamps to avoid detection and blend in with legitimate files
	T1564.006 - Hide Artifacts: Run Virtual Instance	WARP PANDA has created malicious VMs within the VMware environment
Discovery	T1083 - File and Directory Discovery	*Junction* allows a connected client to browse and download files from the host machine
Lateral Movement	T1021.004 - Remote Services: SSH	WARP PANDA has used SSH to move between vCenter servers and ESXi hosts
	T1550.001 - Use Alternate Authentication Material: Application Access Token	WARP PANDA has moved laterally between different cloud services within the Azure environment

Collection	T1114.002 - Email Collection: Remote Email Collection	WARP PANDA has gained access to mailboxes
	T1213 - Data from Information Repositories	WARP PANDA has gained access to sensitive files
	T1213.002 - Data from Information Repositories: SharePoint	WARP PANDA has used *BRICKSTORM* to access and download sensitive SharePoint files
	T1530 - Data from Cloud Storage	WARP PANDA has accessed cloud environments to collect sensitive information
	T1560.001 - Archive Collected Data: Archive via Utility	WARP PANDA has used 7-Zip to compress data before exfiltration
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols	*BRICKSTORM* uses WebSockets to communicate with C2 infrastructure over TLS
	T1071.004 - Application Layer Protocol: DNS	*BRICKSTORM* uses DNS-over-HTTPS to resolve C2 domains
	T1090 - Proxy	*Junction* allows a connected client to start a TCP or UDP proxy; *GuestConduit* allows traffic proxying from a host hypervisor to a different endpoint address
	T1090.003 - Proxy: Multi-hop Proxy	WARP PANDA has used commercial VPN services
	T1095 - Non-Application Layer Protocol	*Junction* and *GuestConduit* can both communicate using VSOCK network connections
	T1572 - Protocol Tunneling	*Junction* can forward network traffic over a VSOCK connection to a listening virtual machine (VM)
	T1573.002 - Encrypted Channel: Asymmetric Cryptography	*BRICKSTORM* can communicate with C2 infrastructure via TLS
Exfiltration	T1041 - Exfiltration Over C2 Channel	WARP PANDA has exfiltrated archived data to C2 infrastructure

[1] The `vpxuser` account is native to vCenter-managed ESXi hosts. The account's password is random, managed by vCenter, and unique for each ESXi host. Automatically changed on a regular basis, the password is stored in an encrypted form on the vCenter server. The account should

only be used by vCenter to manage ESXi. Any evidence of SSH activity using this account should be thoroughly investigated, as such activity is likely malicious.

[2] https[:]//github[.]com/CrowdStrike/VirtualGHOST

[3] https[:]//cloud[.]google[.]com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

[4] https[:]//www[.]nviso[.]eu/blog/nviso-analyzes-brickstorm-espionage-backdoor

[5] https[:]//cloud[.]google[.]com/blog/topics/threat-intelligence/brickstorm-espionage-campaign

[6] https[:]//github[.]com/CrowdStrike/VirtualGHOST

CrowdStrike 2025 Threat Hunting Report

Adversaries weaponize and target AI at scale.

Download report