Hive Pro

Threat Level

Red

✓ CISA: AR25-338A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

BRICKSTORM Breaks In: China's Quiet Grip on US Virtual Stack

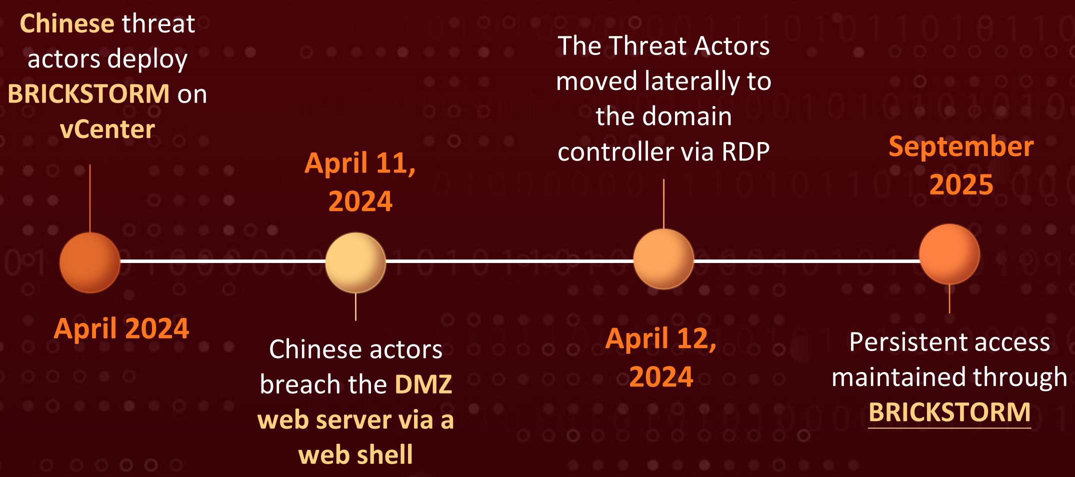
Date of Publication	Admiralty Code	TA Number
December 12, 2025	A1	TA2025378

Summary

Attack Commenced: April 2024
Malware: BRICKSTORM Backdoor
Threat Actor: WARP PANDA
Targeted Country: United States
Targeted Industries: Government, IT, Legal, Technology, Manufacturing

Attack: China-linked operators are deploying BRICKSTORM, a Go-based ELF backdoor built for stealth, durability, and deep system control. In 2025, the WARP PANDA threat group used BRICKSTORM during intrusions targeting U.S. VMware vCenter environments. BRICKSTORM implants tunneled traffic through vCenter servers, ESXi hosts, and guest VMs while masquerading as legitimate processes, maintaining persistence even after file deletion and reboots.

Attack Timeline



April 2024

Chinese threat actors deploy **BRICKSTORM** on **vCenter**

April 11, 2024

Chinese actors breach the **DMZ web server via a web shell**

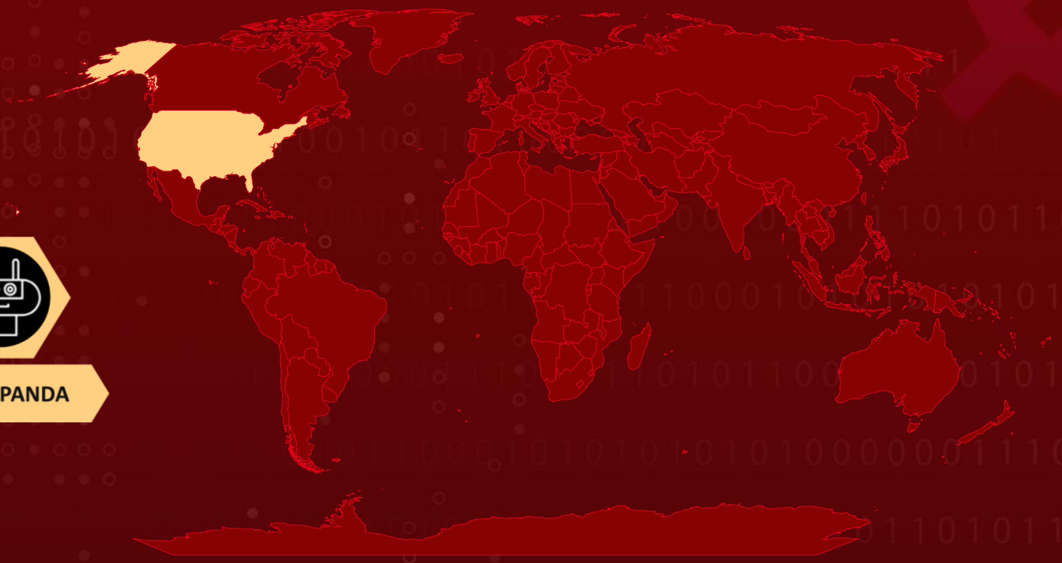
April 12, 2024

The Threat Actors moved laterally to the domain controller via RDP

September 2025

Persistent access maintained through **BRICKSTORM**

Attack Regions



WARP PANDA

Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-38812	VMware vCenter Server Heap-Overflow Vulnerability	VMware vCenter Server, VMware Cloud Foundation	✗	✓	✓
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration Utility	✗	✓	✓
CVE-2023-34048	VMware vCenter Server Out-of-Bounds Write Vulnerability	VMware vCenter Server	✓	✓	✓
CVE-2021-22005	VMware vCenter Server File Upload Vulnerability	VMware vCenter Server	✗	✓	✓

Note: WARP PANDA exploited the vulnerabilities listed above.

Attack Details

#1

The People's Republic of China is deploying a Go-based ELF backdoor known as BRICKSTORM to secure long-term, covert access to targeted systems. The malware is built for persistence, stealth, and reliable command-and-control. BRICKSTORM begins by running integrity and environment checks, then anchors itself with a self-monitoring mechanism that automatically reinstalls or restarts if interrupted. It configures environment variables to match the compromised host, enabling stable operation.

#2

Once active, BRICKSTORM establishes an encrypted link to its command-and-control server, layering multiple forms of encryption and using DNS-over-HTTPS to obscure traffic. It can mimic legitimate web server behavior, blending its communication into normal network activity.

#3

After the connection is established, operators gain full remote control, including interactive shell access and the ability to browse, manipulate, or transfer files. Certain variants also function as a SOCKS proxy, enabling tunneling and lateral movement across internal systems.

#4

In 2025, the China-nexus group WARP PANDA used BRICKSTORM during intrusions targeting VMware vCenter environments at U.S. organizations. The group demonstrates advanced technical skill, strong operational security, and deep knowledge of cloud and virtualization platforms. Their operations often begin with exploiting internet-facing edge devices, followed by pivoting into vCenter environments through stolen credentials or vCenter vulnerabilities.

#5

WARP PANDA has exploited multiple flaws in edge appliances and vCenter systems. Their tradecraft includes clearing logs, altering file timestamps, and creating unregistered malicious virtual machines that are powered down after use. They use BRICKSTORM to tunnel traffic through vCenter servers, ESXi hosts, and guest VMs, allowing activity to blend with legitimate operations. The implants disguise themselves as authentic vCenter processes and retain persistence even after attempts at file removal or system reboot.

Recommendations

Prioritize Patching and Vulnerability Management: Patch known exploited vulnerabilities immediately, prioritizing edge devices. Address critical CVEs highlighted in this advisory: CVE-2024-21887, CVE-2023-46805, CVE-2024-38812, CVE-2023-46747, CVE-2023-34048, and CVE-2021-22005. Upgrade unsupported devices to vendor-supported models with security updates.

Hardening Virtual Infrastructure: Keep all VMware vSphere, vCenter, and ESXi hosts fully updated. Apply security patches on release, remove unsupported versions, and validate that all management interfaces use hardened configurations.

Securing Edge Devices: Maintain an authoritative inventory of every internet-facing and internal edge device. Monitor these devices for configuration drift, unexpected services, and outbound traffic that deviates from baseline behavior.

Controlling Service Account Exposure: Limit service-account permissions to the minimum required operations. Audit usage patterns, enforce MFA where supported, and alert on interactive logins or privilege escalation events tied to these accounts.

Network Segmentation and Egress Control: Isolate ESXi management interfaces behind strict segmentation and firewall rules. Block outbound internet access from both ESXi and vCenter systems. Monitor and restrict the use of nonstandard or optional ports, including port 8090.

Validating Access Pathways: Audit all remote-access channels. Remove dormant accounts, rotate credentials exposed to edge systems, and enforce strict authentication controls on systems that manage virtual infrastructure.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0008 Lateral Movement	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control
T1037 Boot or Logon Initialization Scripts	T1574 Hijack Execution Flow	T1574.007 Path Interception by PATH Environment Variable	T1505 Server Software Component
T1505.003 Web Shell	T1548 Abuse Elevation Control Mechanism	T1548.003 Sudo and Sudo Caching	T1036 Masquerading
T1078 Valid Accounts	T1083 File and Directory Discovery	T1003 OS Credential Dumping	T1003.003 NTDS
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1105 Ingress Tool Transfer	T1090 Proxy
T1090.001 Internal Proxy	T1041 Exfiltration Over C2 Channel	T1583 Acquire Infrastructure	T1583.001 Domains
T1583.003 Virtual Private Server	T1583.007 Serverless	T1584 Compromise Infrastructure	T1584.008 Network Devices
T1588 Obtain Capabilities	T1588.001 Malware	T1608 Stage Capabilities	T1608.003 Install Digital Certificate
T1190 Exploit Public-Facing Application	T1078.004 Cloud Accounts	T1078.001 Default Accounts	T1098.001 Additional Cloud Credentials

T1036.004 Masquerade Task or Service	**T1070.004** File Deletion	**T1070.006** Timestomp	**T1564.006** Run Virtual Instance
T1021.004 SSH	**T1550.001** Application Access Token	**T1114.002** Remote Email Collection	**T1213** Data from Information Repositories
T1213.002 Sharepoint	**T1530** Data from Cloud Storage	**T1560.001** Archive via Utility	**T1071.004** DNS
T1090.003 Multi-hop Proxy	**T1095** Non-Application Layer Protocol	**T1572** Protocol Tunneling	**T1573.002** Asymmetric Cryptography
T1098 Account Manipulation	**T1573** Encrypted Channel	**T1560** Archive Collected Data	**T1114** Email Collection
T1550 Use Alternate Authentication Material	**T1021** Remote Services	**T1564** Hide Artifacts	**T1070** Indicator Removal

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	208[.]83[.]233[.]14, 149[.]28[.]120[.]31
MD5	8e4c88d00b6eb46229a1ed7001451320, 39111508bfde89ce6e0fe6abe0365552, dbca28ad420408850a94d5c325183b28, 0a4fa52803a389311a9ddc49b7b19138, 82bf31e7d768e6d4d3bc7c8c8ef2b358, 18f895e24fe1181bb559215ff9cf6ce3, a52e36a70b5e0307cbcaa5fd7c97882c, a02469742f7b0bc9a8ab5e26822b3fa8
SHA1	9bf4c786ebd68c0181cfe3eb85d2fd202ed12c54, f639d9404c03af86ce452db5c5e0c528b81dc0d7, fb11c6caa4ea844942fe97f46d7eb42bc76911ab,

TYPE	VALUE
SHA1	97001baaa379bcd83677dca7bc5b8048fdfaaddc, de28546ec356c566cd8bca205101a733e9a4a22d, c3549d4e5e39a11f609fc6fbf5cc1f2c0ec272b4, 44a3d3f15ef75d9294345462e1b82272b0d11985, 10d811029f6e5f58cd06143d6353d3b05bc06d0f
SHA256	aaf5569c8e349c15028bc3fac09eb982efb06eabac955b705a6d447263658e38, 013211c56caaa697914b5b5871e4998d0298902e336e373ebb27b7db30917eaf, 57bd98dbb5a00e54f07ffacda1fea91451a0c0b532cd7d570e98ce2ff741c21d, b3b6a992540da96375e4781afd3052118ad97cfe60ccf004d732f76678f6820a, 22c15a32b69116a46eb5d0f2b228cc37cd1b5915a91ec8f38df79d3eed1da26b, f7cda90174b806a34381d5043e89b23ba826abcc89f7abd520060a64475ed506, 39b3d8a8aedffc1b40820f205f6a4dc041cd37262880e5030b008175c45b0c46, 73fe8b8fb4bd7776362fd356fdc189c93cf5d9f6724f6237d829024c10263fe5, 40db68331cb52dd3ffa0698144d1e6919779ff432e2e80c058e41f7b93cec042, 88db1d63dbd18469136bf9980858eb5fc0d4e41902bf3e4a8e08d7b6896654ed, 9a0e1b7a5f7793a8a5a62748b7aa4786d35fc38de607fb3bb8583ea2f7974806, 40992f53effc60f5e7edea632c48736ded9a2ca59fb4924eb6af0a078b74d557, 320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759, dfac2542a0ee65c474b91d3b352540a24f4e223f1b808b741cfe680263f0ee44, b91881cb1aa861138f2063ec130b2b01a8aaf0e3f04921e5cbfc61b09024bf12, bfb3ffd46b21b2281374cd60bc756fe2dcc32486dcc156c9bd98f24101145454
SHA512	5e654776e9c419e11e6f93a452415a601bd9a2079710f1074608570e498a9af37b81bb57c98cb8bb626c5ee4b3e35757d3ae8c1c3717f28d9f3fe7a4cebe0608, 74b4c6f7c7cae07c6f8edf3f2fb1e9206d4f1f9734e8e4784b15d192eec8cd8a4f59078fc0c56dc4ad0856cdd792337b5c92ffd3d2240c8a287a776df4363bba,

TYPE	VALUE
SHA512	659205fa2cfa85e484c091cc2e85a7ec4e332b196e423b1f39bafdc8fca33e3db712bbe07afcc091ff26d9b4f641fa9a73f2a66dce9a0ced54ebeb8c2be82a7f, 65ebf5dfafb8972ffead44271436ec842517cfaaf3d1f1f1237a32d66e1d280943bd3a69f1d539a1b7aca6152e96b29bc822e1047e2243f6aec8959595560147, 4c52caf2e5f114103ed5f60c6add3aa26c741b07869bb66e3c25a1dc290d4a8bf87c42c336e8ac8ebf82d9a9b23eaa18c31f7051a5970a8fe1125a2da890340f, 79276523a6a507e3fa1b12b96e09b10a01c783a53d58b9ae7f5780a379431639a80165e81154522649b8e2098e86d1a310efffebe32faafc7b3bc093eec60a64, bbe18d32bef66ccfa931468511e8ba55b32943e47a1df1e68bb5c8f8ae97a5bf991201858ae9632fa24df5f6c674b6cb260297a1c11889ca61bda68513f440ce, 8e29aeb3603ffe307b2d60f7401bd9978bebe8883235eb88052ebf6b9e04ce6bf35667480cedea5712c1e13e8c6dcfb34d5fde0ddca6ca31328de0152509bf8f
URLs	hxxps[:]//1[.]0[.]0[.]1/dns-query, hxxps[:]//1[.]1[.]1[.]1/dns-query, hxxps[:]//8[.]8[.]4[.]4/dns-query, hxxps[:]//8[.]8[.]8[.]8/dns-query, hxxps[:]//9[.]9[.]9[.]9/dns-query, hxxps[:]//149[.]112[.]112[.]11/dns-query, hxxps[:]//45[.]90[.]28[.]160/dns-query, hxxps[:]//9[.]9[.]9[.]11/dns-query

Patch Details

CVE-2024-21887 & CVE-2023-46805:
https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE-2024-38812:
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968

CVE-2023-46747:
https://my.f5.com/manage/s/article/K000137353

CVE-2023-34048:
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23677

CVE-2021-22005:
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23611

References

https://www.cisa.gov/news-events/analysis-reports/ar25-338a

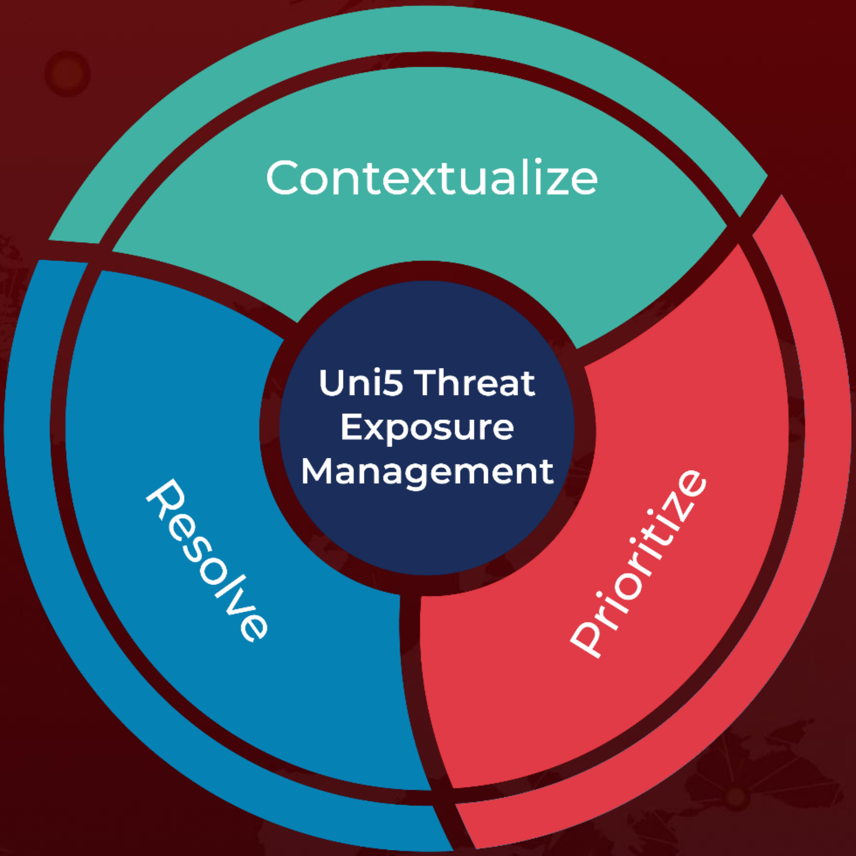
https://www.crowdstrike.com/en-us/blog/warp-panda-cloud-threats/

https://hivepro.com/threat-advisory/brickstorm-malware-quietly-builds-the-perfect-hideout-in-us-networks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 12, 2025 • 9:30 AM

More at www.hivepro.com