BREAKING: THE STATE-SPONSORED CHINESE HACKERS WEAVER ANT BREACH ASIAN TELECOM REMAIN UNDETECTED FOR YEARS

Vairav Security News Report

Date: March 26, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A Chinese state-sponsored hacking group, tracked as **Weaver Ant**, has breached an undisclosed Asian telecommunications provider and remained undetected for over four years, according to a new Sygnia report. The attackers leveraged web shells, tunneling techniques, and custom malware to maintain persistence and facilitate cyber espionage. Notably, they deployed China Chopper and an undocumented tool, INMemory, designed to execute malicious payloads in memory, leaving minimal forensic traces. The campaign also utilized Zyxel routers for traffic proxying and leveraged an Outlook-based backdoor linked to Emissary Panda.

DETAILED EXPLANATION

Weaver Ant's attack began with exploiting a public-facing application to implant two web shells, an encrypted variant of China Chopper and a previously unseen INMemory web shell. INMemory allowed attackers to execute Base64-encoded payloads in memory, avoiding detection. The web shells facilitated the deployment of recursive HTTP tunneling tools, enabling lateral movement over SMB, a method previously used by Elephant Beetle.

The attackers performed post-exploitation actions, including:

- Bypassing security defenses by patching Event Tracing for Windows (ETW) and Antimalware Scan Interface (AMSI).
- Executing PowerShell commands without launching PowerShell.exe, using System.Management.Automation.dll.
- Reconnaissance against Active Directory (AD) to identify high-privilege accounts and critical servers.

Weaver Ant is a threat actor exhibiting characteristics commonly associated with a China-linked targeted threat group. These attributes include:

- **Target Selection**: Focused on industries and geographic regions that align with China's cyber objectives.
- **Operational Strategy**: Well-defined goals guided by their attack campaigns.
- **Web Shell Deployment**: Extensive use of China Chopper web shell variants.
- **Attack Timing**: Operations were primarily conducted within the GMT +8 time zone, mainly on regular working days while avoiding weekends and holidays.

- **Use of Operational Relay Box (ORB) Networks**: Relied on a non-provisioned ORB network to proxy traffic and obfuscate their infrastructure. This network comprised compromised Zyxel CPE routers (mostly running firmware version VMG3625-T20A) operated by Southeast Asian telecom providers. By leveraging this ORB network, the attackers pivoted from one compromised telecom device to another.
- **Malicious DLL Injection**: Used various techniques to load trojanized DLLs for system infection.
- **Backdoor Deployment**: Utilized a backdoor previously attributed to Chinese APT groups.

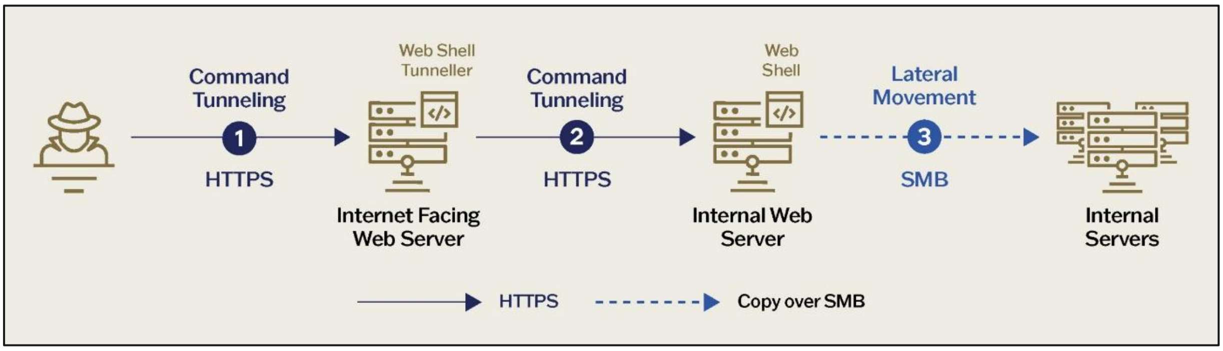

Figure 1: Web Shell tunneling flow

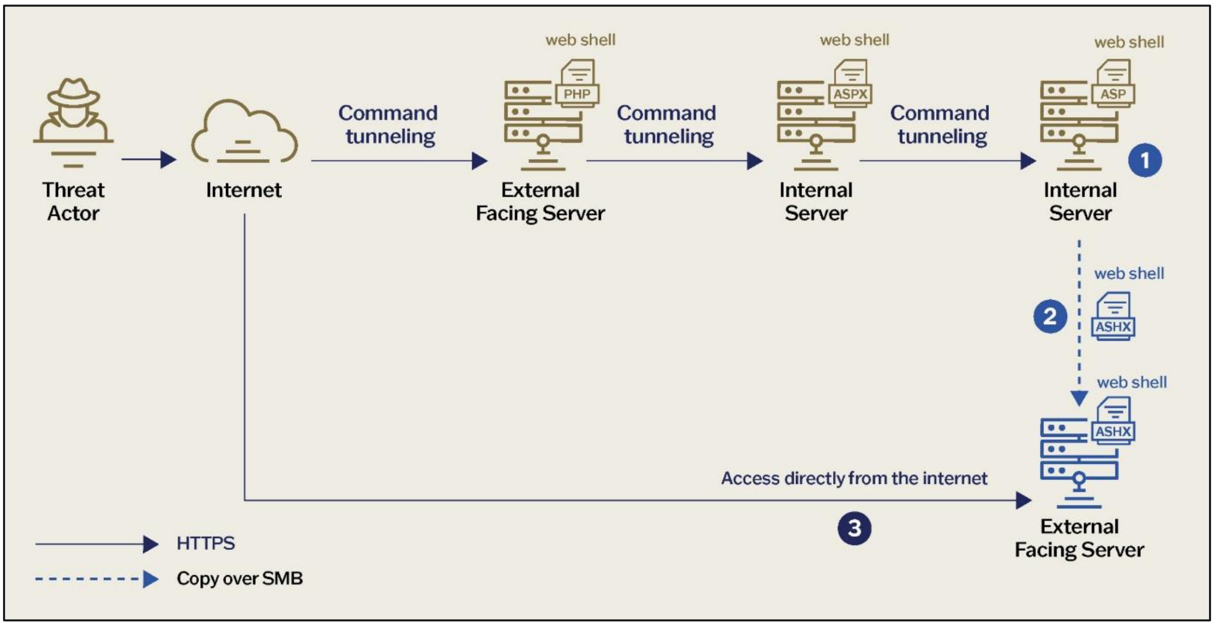

Figure 2: Web Shell deployment chain

Related Developments

In a parallel cybersecurity development, China's Ministry of State Security (MSS) accused four Taiwanese individuals linked to Taiwan's Information, Communications, and

Electronic Force Command (ICEFCOM) of conducting cyberattacks against China. These alleged activities include:

- Phishing campaigns targeting Chinese government and military agencies.
- Disinformation campaigns leveraging social media.
- Use of open-source tools like AntSword, IceScorpion, Metasploit, and Quasar RAT.

Chinese cybersecurity firms QiAnXin and Antiy further linked APT-Q-20 (aka GreenSpot, Poison Cloud Vine, and White Dolphin) to spear-phishing attacks deploying C++ trojans and C2 frameworks like Cobalt Strike and Sliver. The group also exploited N-day vulnerabilities and weak IoT credentials to gain unauthorized access.

MITRE ATT&CK TECHNIQUES

Tactics	Techniques (ID)
Initial Access	Exploit Public-Facing Application (T1190)
Execution	Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Visual Basic (T1059.005) • JavaScript (T1059.007)
Persistence	Valid Accounts (T1078) • Domain Accounts (T1078.002) • Local Accounts (T1078.003) Server Software Component (T1505) • Web Shell (T1505.003)
Privilege Escalation	Valid Accounts (T1078) • Domain Accounts (T1078.002) Access Token Manipulation (T1134) • Token Impersonation/Theft (T1134.001)
Defense Evasion	Process Injection (T1055) Access Token Manipulation (T1134) • Token Impersonation/Theft (T1134.001)

Credential Access	Unsecured Credentials (T1552) • Credentials In Files (T1552.001) OS Credential Dumping (T1003) • Security Account Manager (T1003.002)
Discovery	Account Discovery (T1087) • Domain Account (T1087.002) File and Directory Discovery (T1083) Network Share Discovery (T1135) Remote System Discovery (T1018) System Information Discovery (T1082) System Network Configuration Discovery (T1016)
Lateral Movement	Remote Services (T1021) • SMB/Windows Admin Shares (T1021.001) Lateral Tool Transfer (T1570)
Collection	Archive Collected Data (T1560) • Archive via Utility (T1560.001) Data Staged (T1074) • Local Data Staging (T1074.001)
Command and Control	Application Layer Protocol (T1071) • Web Protocols (T1071.001) Protocol Tunneling (T1572) Proxy (T1090) • Internal Proxy (T1090.001)
Exfiltration	Exfiltration Over Alternative Protocol (T1048)

INDICATORS OF COMPROMISE (IOCs)

23c4049121a9649682b3b901eaac0cc52c308756

9022f78087e1679035e09160d59d679dc3ac345d

be52275b0c2086735dac478dc4f09fd16031669a

c879a8eb6630b0cd7537b068f4e9af2c9ca08a62

25a593b9517d6c325598eab46833003c40f9491a

a9bbea73504139ce91a0ec20fef303c68a131cd4

334a88e288ae18c6e3fd7fb2d1ad9548497d52ce

4aeeae023766153a91b83d02b1b24da20c0dd135

3cac6ff7cddcb8f82409c79c85d976300fc60861

55eeaa904bc6518a2715cc77648e6c5187416a46

ff7b2c3938306261881c42e78d0df51d9bcdd574

089439168d3c75b4da94ab801f1c46ad6b9e1fdc

a5c36b8022751cfeb4a88a21153847df3870c7c0

ad3dbec2b621807fa9a2f1b2f575d7077e494626

4dc0ebfa52adf9b9eb4fa8f0a359c21a14e183fb

d102a34b3f0efb57f1d9f04eff26b256875a3aa1

2b9b740fb5fe0549810500476f567002683df71d

4fa2b2ab3e24ee9d130cfeda63c7ae1ccbc393dc

495a4b4757f3b1eec7fdaa9d0b2930071565f2b1

f31920d636224356e8c7a182c2b9b37e42a09181

9dc3d272652851428f5cc44f2fd9458bff1d6a78

4dd22a08a5b103e1f2238aed7f7ce66c5a542533

02065bbdb3209e0522db3225600b8e79f8a10293

81622512757f897206a84b29ee866fb933fa3d48

151dc47b213aaec3751ffd1427737c65757ab410

492cbe143f795888d8e5006ac595f65f4565ed6e

0e282dc84d6cfd447fece7d3ecc622523b143aa8

49cd96df4c85cdd7461701340c0bb4d05a5049d8

207b7cf5db59d70d4789cb91194c732bcd1cfb4b

RECOMMENDATIONS

Organizations should implement the following security measures:

- Monitor for Indicators of Compromise (IoCs) associated with Weaver Ant and APT-Q-20.
- Secure public-facing applications to prevent web shell deployment.
- Implement EDR solutions to detect memory-only malware like INMemory.
- Restrict PowerShell execution and monitor suspicious script activities.
- Harden SMB and Active Directory security to mitigate lateral movement risks.
- Conduct routine security audits to detect unauthorized backdoors and tunneling activity.

The long-term undetected presence of Weaver Ant within a critical telecom provider underscores the importance of continuous threat hunting and proactive cybersecurity defenses. Organizations, especially in telecommunications and critical infrastructure, must adopt advanced detection strategies to counter persistent cyber espionage threats.

ADDITIONAL RESOURCES

https://thehackernews.com/2025/03/chinese-hackers-breach-asian-telecom.html

https://www.sygnia.co/threat-reports-and-advisories/weaver-ant-tracking-a-china-nexus-cyber-espionage-operation/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com