Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

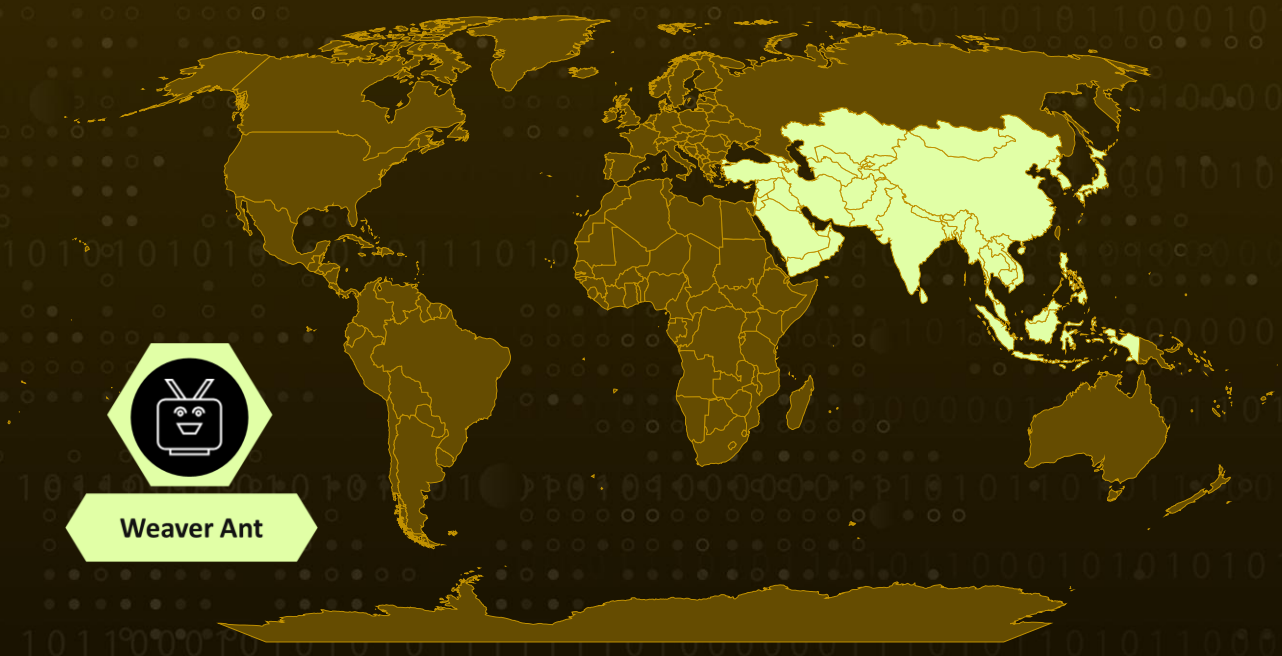
Web Shell Warfare: Weaver Ant's Covert Cyber Espionage Campaign

Date of Publication	Admiralty Code	TA Number
March 25, 2025	A1	TA2025093

Summary

Attack Discovered: 2025
Targeted Countries: Asia
Targeted Industry: Telecommunication
Affected Platform: Windows
Malware: China Chopper, INMemory
Actor: Weaver Ant
Attack: A stealthy and highly persistent China-linked threat actor, tracked as Weaver Ant, has infiltrated a major telecommunication provider in Asia. The group's objective was long-term access, enabling cyber espionage through the collection of sensitive data. Their tactics, emphasizing their reliance on web shells and web shell tunneling to maintain persistence and move laterally within the network. The incident underscores the urgency of strengthening defenses against state-sponsored threats.

Attack Regions



Attack Details

#1 For over four years, Weaver Ant, a China-linked threat group, remained hidden within a telecommunications provider's network, using compromised Zyxel CPE routers to evade detection. This anomaly led to the discovery of a China Chopper web shell variant, embedded deep within an internal server a stealthy backdoor that had remained undetected for years. Upon further investigation a widespread campaign was uncovered built entirely around web shells, providing persistent access, remote code execution, and tunneling capabilities.

#2 Weaver Ant used two distinct web shells to maintain control over the network. The first was an encrypted variant of China Chopper, a lightweight yet powerful tool commonly used by Chinese threat actors for remote access, command execution, and data exfiltration. Placed on externally facing ASPX and PHP servers, this variant leveraged encryption to evade detection while ensuring continuous access. The second was an advanced and previously undocumented web shell called 'INMemory', designed for in-memory execution.

#3 Weaver Ant also leveraged web shell tunneling to create stealthy communication channels. They converted compromised servers into proxy nodes, rerouting HTTP traffic to execute payloads across various internal systems. This allowed them to interact with isolated, non-internet-facing servers, bypassing traditional security controls. To further obscure their presence, the attackers encrypted tunneling traffic and used port mirroring to capture packets without detection. Their approach resembled a 'Matryoshka' doll, layering multiple obfuscation techniques to conceal their true activities until the final stage of execution.

#4 To evade detection, Weaver Ant disabled security monitoring mechanisms, bypassed AMSI protections, and suppressed event logs. They avoided triggering security tools by using System.Management.Automation.dll instead of PowerShell.exe, executing commands invisibly. For lateral movement, they leveraged stolen high-privilege credentials to deploy additional web shells, extract IIS logs and configuration files, and map out the Active Directory environment.

#5 Despite multiple remediation efforts, Weaver Ant continuously adapted, regaining access through compromised Zyxel routers and leveraging a non-provisioned Operational Relay Box (ORB) network to anonymize their operations. Their persistent reliance on web shells as a primary attack vector, coupled with sophisticated evasion techniques, highlights the evolving nature of state-sponsored cyber espionage.

Recommendations

- **Strengthen Identity and Access Security:** Regularly audit privileged accounts and disable unused ones. Enforce Multi-Factor Authentication (MFA) for admin and remote access. Continuously monitor for unusual activity, such as reactivated accounts or unexpected privilege escalations.
- **Detect and Remove Web Shells:** Regularly monitor file integrity on externally facing servers to spot unauthorized changes. Use behavioral detection to flag unusual web requests or execution patterns. Block suspicious ASPX, PHP, and other web shell execution paths on critical systems.
- **Secure Network Edge and Third-Party Devices:** Keep Zyxel CPE routers and other edge devices updated to prevent exploitation. Monitor traffic from these devices for unusual proxy behavior. Disable unused services and enforce strict remote management policies to reduce risks.
- **Strengthen Credential and Web Security:** Implement LAPS, gMSA, or a PIM solution to regularly rotate credentials and prevent misuse. Enhance web security by tuning WAF and logging systems to detect obfuscated code signatures and behavioral patterns associated with China Chopper and INMemory web shells.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**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
T1190 Exploit Public-Facing Application	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1590** Gather Victim Network Information

T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell	**T1059.005** Visual Basic
T1059.007 JavaScript	**T1078** Valid Accounts	**T1078.002** Domain Accounts	**T1078.003** Local Accounts
T1505 Server Software Component	**T1505.003** Web Shell	**T1134** Access Token Manipulation	**T1134.001** Token Impersonation/Theft
T1055 Process Injection	**T1552** Unsecured Credentials	**T1552.001** Credentials In Files	**T1003** OS Credential Dumping
T1003.002 Security Account Manager	**T1087** Account Discovery	**T1087.002** Domain Account	**T1083** File and Directory Discovery
T1135 Network Share Discovery	**T1018** Remote System Discovery	**T1082** System Information Discovery	**T1016** System Network Configuration Discovery
T1021 Remote Services	**T1021.002** SMB/Windows Admin Shares	**T1570** Lateral Tool Transfer	**T1560** Archive Collected Data
T1560.001 Archive via Utility	**T1074** Data Staged	**T1074.001** Local Data Staging	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1572** Protocol Tunneling	**T1090** Proxy	**T1090.001** Internal Proxy
T1048 Exfiltration Over Alternative Protocol			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	23c4049121a9649682b3b901eaac0cc52c308756, 9022f78087e1679035e09160d59d679dc3ac345d, be52275b0c2086735dac478dc4f09fd16031669a, c879a8eb6630b0cd7537b068f4e9af2c9ca08a62, 25a593b9517d6c325598eab46833003c40f9491a,

TYPE	VALUE
SHA1	a9bbea73504139ce91a0ec20fef303c68a131cd4, 334a88e288ae18c6e3fd7fb2d1ad9548497d52ce, 4aeeae023766153a91b83d02b1b24da20c0dd135, 3cac6ff7cddcb8f82409c79c85d976300fc60861, 55eeaa904bc6518a2715cc77648e6c5187416a46, ff7b2c3938306261881c42e78d0df51d9bcdd574, 089439168d3c75b4da94ab801f1c46ad6b9e1fdc, a5c36b8022751cfeb4a88a21153847df3870c7c0, ad3dbec2b621807fa9a2f1b2f575d7077e494626, 4dc0ebfa52adf9b9eb4fa8f0a359c21a14e183fb, d102a34b3f0efb57f1d9f04eff26b256875a3aa1, 2b9b740fb5fe0549810500476f567002683df71d, 4fa2b2ab3e24ee9d130cfeda63c7ae1ccbc393dc, 495a4b4757f3b1eec7fdaa9d0b2930071565f2b1, f31920d636224356e8c7a182c2b9b37e42a09181, 9dc3d272652851428f5cc44f2fd9458bff1d6a78, 4dd22a08a5b103e1f2238aed7f7ce66c5a542533, 02065bbdb3209e0522db3225600b8e79f8a10293, 81622512757f897206a84b29ee866fb933fa3d48, 151dc47b213aaec3751ffd1427737c65757ab410, 492cbe143f795888d8e5006ac595f65f4565ed6e, 0e282dc84d6cfd447fece7d3ecc622523b143aa8, 49cd96df4c85cdd7461701340c0bb4d05a5049d8, 207b7cf5db59d70d4789cb91194c732bcd1cfb4b

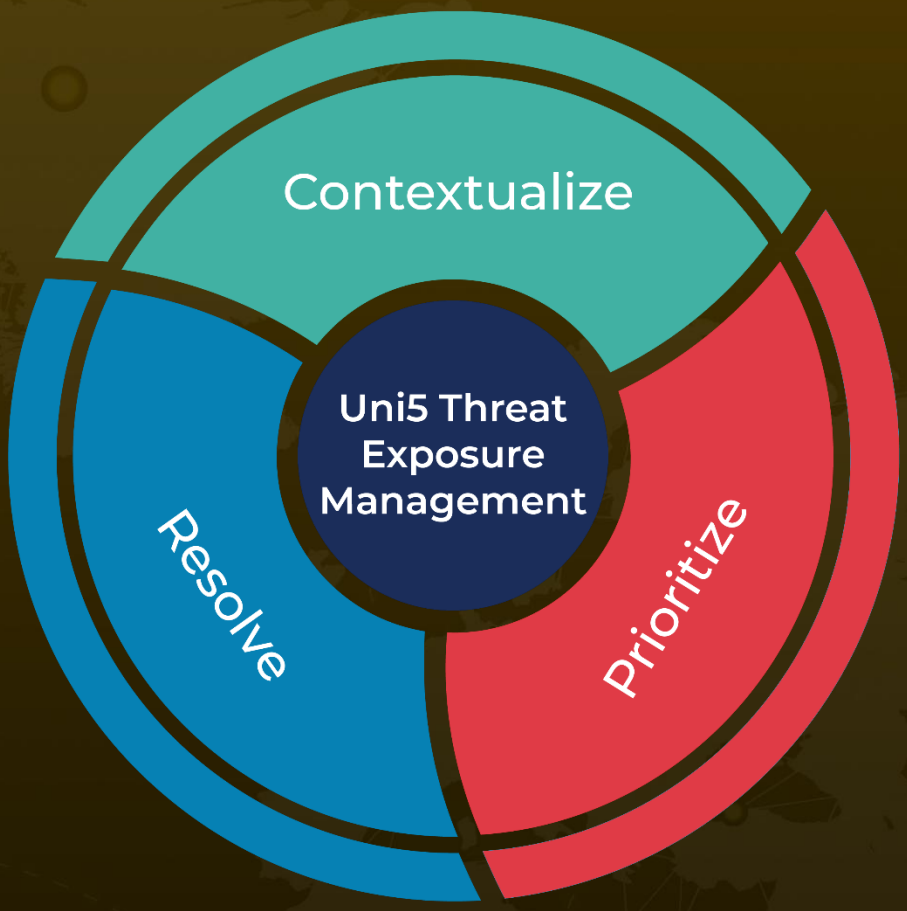
References

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

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

March 25, 2025 • 5:50 AM

More at www.hivepro.com