ADVISORY FOR ICM SECTOR

# Weaver Ant Targeting Telecom Providers in Asia

Original report published on: March 24, 2025[1]

## Executive Summary

Sygnia uncovered a cyber espionage campaign by *Weaver Ant*, a threat actor, targeting a major telecommunications provider in Asia. The group maintained persistent access for over four years using web shells, including *China Chopper* and the memory-resident *INMemory*, to evade detection. They leveraged a proxy infrastructure of compromised Zyxel routers—forming an *Operational Relay Box (ORB)* network—for stealth and lateral movement. The operation focused on intelligence gathering and credential theft, aligning with strategic cyber interests, and highlights the need for proactive detection and rapid incident response.

## Background

Sygnia investigated a cyber espionage by *Weaver Ant*, a threat actor targeting a major, undisclosed telecommunications provider in Asia. The objective was to maintain long-term access for intelligence gathering, employing web shells and tunnelling techniques to achieve persistence and enable lateral movement. Target selection was aligned with strategic cyber interests, focusing on specific sectors and geographic regions.

Weaver Ant leveraged an *Operational Relay Box (ORB)* network—primarily composed of compromised Zyxel CPE routers (notably with firmware version VMG3625-T20A)—to proxy traffic and obscure its infrastructure. Through this ORB network, the actor was able to pivot from one telecom provider's compromised device to another across organisations.

The discovery was triggered when a previously deactivated privileged login account was re-activated. Weaver Ant had maintained persistent access to an internal server for four years using the *China Chopper* web shell and a newly identified, memory-resident web shell named '*INMemory*', which supports in-memory execution to evade detection. The actor's motivation focuses on cyber espionage, credential harvesting, and network intelligence gathering.

## Detection and Mitigation

IMDA recommends organisations to perform continual testing and validation of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques (Annex B) in this advisory:
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.

- Monitor for web page creation and command execution originating from web server processes (i.e. w3wp.exe, tomcat6.exe)
- Monitor the activation of privileged accounts and managed it through Privileged Access Management solutions.
- Enable PowerShell transcript logging to capture and analyse suspicious activity.
- Restrict web-service accounts to the least privileges required.
- Ensure IIS logging is enabled and ingested into the SIEM, with X-Forwarded-For (XFF) headers configured. Monitor any disruptions or stoppages in log ingestion.
- Monitor incoming HTTP requests with unusually large payloads in the request's body and unexpected parameter names or values in incoming HTTP requests.
- Validate and add malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR).

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

## Annex A - Indicators of Compromise

| Malware Hash – SHA1 | Remark |
|---|---|
| 23c4049121a9649682b3b901eaac0cc52c308756 | ASPX Encrypted ChinaChopper Web shell |
| 9022f78087e1679035e09160d59d679dc3ac345d | |
| be52275b0c2086735dac478dc4f09fd16031669a | |
| c879a8eb6630b0cd7537b068f4e9af2c9ca08a62 | |
| 25a593b9517d6c325598eab46833003c40f9491a | |
| a9bbea73504139ce91a0ec20fef303c68a131cd4 | |
| 334a88e288ae18c6e3fd7fb2d1ad9548497d52ce | |
| 4aeeae023766153a91b83d02b1b24da20c0dd135 | |
| 3cac6ff7cddcb8f82409c79c85d976300fc60861 | |
| 55eeaa904bc6518a2715cc77648e6c5187416a46 | |
| ff7b2c3938306261881c42e78d0df51d9bcdd574 | PHP Encrypted ChinaChopper Web shell |
| 089439168d3c75b4da94ab801f1c46ad6b9e1fdc | |
| a5c36b8022751cfeb4a88a21153847df3870c7c0 | VB Encrypted ChinaChopper Web shell |
| ad3dbec2b621807fa9a2f1b2f575d7077e494626 | ASPX China ChopperWeb shell |
| 4dc0ebfa52adf9b9eb4fa8f0a359c21a14e183fb | |
| d102a34b3f0efb57f1d9f04eff26b256875a3aa1 | ASPX Web shell |
| 2b9b740fb5fe0549810500476f567002683df71d | |
| 4fa2b2ab3e24ee9d130cfeda63c7ae1ccbc393dc | "ReGeorg" |
| 495a4b4757f3b1eec7fdaa9d0b2930071565f2b1 | ASPX Custom Webshell |
| f31920d636224356e8c7a182c2b9b37e42a09181 | |
| 9dc3d272652851428f5cc44f2fd9458bff1d6a78 | INMemory module Webshell |
| 4dd22a08a5b103e1f2238aed7f7ce66c5a542533 | |

| | |
|---|---|
| 02065bbdb3209e0522db3225600b8e79f8a10293 | |
| 81622512757f897206a84b29ee866fb933fa3d48 | |
| 151dc47b213aaec3751ffd1427737c65757ab410 | |
| 492cbe143f795888d8e5006ac595f65f4565ed6e | |
| 0e282dc84d6cfd447fece7d3ecc622523b143aa8 | OWA Backdoor DLL |
| 49cd96df4c85cdd7461701340c0bb4d05a5049d8 | |
| 207b7cf5db59d70d4789cb91194c732bcd1cfb4b | |

## Annex B - MITRE ATT&CK Tactics and Techniques

| Tactic | Technique ID | Technique Title |
|---|---|---|
| Initial Access | T1190 | Exploit Public-Facing Application |
| Execution | T1059.001 | Command and Scripting Interpreter: PowerShell |
| | T1059.003 | Command and Scripting Interpreter: Windows Command Shell |
| | T1059.005 | Command and Scripting Interpreter: Visual Basic |
| | T1059.007 | Command and Scripting Interpreter: JavaScript |
| Persistence | T1078.002 | Valid Accounts: Domain Accounts |
| | T1078.003 | Valid Accounts: Local Accounts |
| | T1505.003 | Server Software Component: Web Shell |
| Privilege Escalation | T1078.002 | Valid Accounts: Domain Accounts |
| | T1134.001 | Access Token Manipulation: Token Impersonation/Theft |
| Defence Evasion | T1055 | Process Injection |
| | T1134.001 | Access Token Manipulation: Token Impersonation/Theft |
| Credential Access | T1003.002 | OS Credential Dumping: Security Account Manager |
| | T1552.001 | Unsecured Credentials: Credentials In Files |
| Discovery | T1016 | System Network Configuration Discovery |
| | T1018 | Remote System Discovery |
| | T1082 | System Information Discovery |
| | T1083 | File and Directory Discovery |
| | T1087.002 | Account Discovery: Domain Account |
| | T1135 | Network Share Discover |
| Lateral Movement | T1021.001 | Remote Services: SMB/Windows Admin Shares |
| | T1570 | Lateral Tool Transfer |
| Collection | T1071.001 | Data Staged: Local Data Staging |
| | T1560.001 | Archive Collected Data: Archive Via Utility |
| Command and Control | T1071.001 | Application Layer Protocol: Web Protocols |
| | T1090.001 | Proxy: Internal Proxy |
| | T1572 | Protocol Tunnelling |
| Exfiltration | T1048 | Exfiltration Over Alternative Protocol |

## References


1. ^ “Tracking a China-Nexus Cyber Espionage Operation”