ADVISORY FOR ICM SECTOR

PHP-CGI Exploited for Cyber Espionage Against Infocommunication and Media Sectors (ICM)

Original report published on: March 6, 2025[1]

Executive Summary

Cisco Talos identified a campaign primarily targeting organisations in Japan including those in the telecommunications and media sectors. Initial access was attained by exploiting a remote code execution vulnerability in the PHP-CGI implementation of PHP on Windows (CVE-2024-4577). The attackers used Cobalt Strike "TaoWu" and other tools for post-exploitation, privilege escalation, persistence, credential theft and lateral movement. Publicly available tools like Blue-lotus, BeEF, and Viper C2 were leveraged to maintain persistence within the victim's environment.

Background

Cisco Talos released a report on a remote code execution vulnerability in the PHP-CGI implementation of PHP on Windows (CVE-2024-4577) to attain initial access into a victim's environment. This was used by a threat actor targeting ICM sectors in Japan.

Once initial access is attained, the threat actor executed a PowerShell script to run Cobalt Strike reverse HTTP shellcode to ensure remote access to the victim's machine and utilised plugins of publicly available Cobalt Strike kit "TaoWu" for post exploitation, and credential theft. The threat actor conducted other activities such as reconnaissance, privilege escalation through customised tools like JuicyPotato, RottenPotato, and SweetPotato, maintaining persistence by modifying registry keys and scheduling tasks, evading detection by clearing Windows Event logs, lateral movement, and data exfiltration using Mimikatz.

Talos discovered that tools and payloads were hosted on Alibaba Cloud infrastructure including scripts to install a suite of offensive tools – including Blue-Lotus, BeEF, and Viper C2 – via docker containers.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention 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.
- Validate and add malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and Network Detection and Response (NDR) for Cobalt Strike activities.

- Monitor unauthorised modification of registry and scheduled task/job as well as the use of `wevtutil.exe` to remove Windows event logs.
- Work with your vendor to patch affected products to mitigate against remote execution vulnerability in PHP-CGI implementation of PHP on Windows (CVE-2024-4577).

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 – MD5	Remark
e10adc3949ba59abbe56e057f20f883e	MD5 hash in the response indicating a successful exploitation

IP Address	Remark
38[.]14[.]255[.]23	Suspected C2
118[.]31[.]18[.]77	

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique
Initial Access	T1190	Exploit Public Facing Application
Persistence	T1112	Modify Registry
	T1053	Scheduled Task/Job
	T1543	Create or Modify System Process
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defence Evasion	T1070.001	Indicator Removal on Host: Clear Windows Event Logs
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory
Discovery	T1033	System Owner/User Discovery
Lateral Movement	T1570	Lateral Tool Transfer
Exfiltration	T1041	Exfiltration over C2 Channel

References

1. ^ “Unmasking the new persistent attacks on Japan”