Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

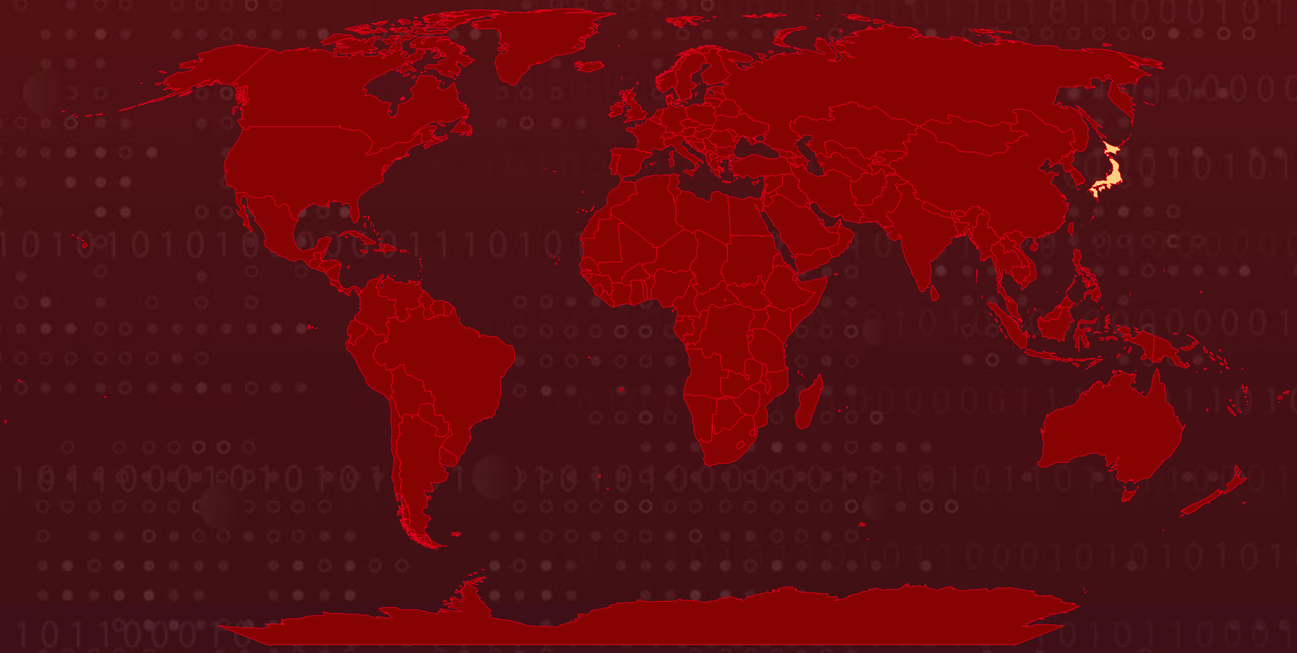
Hackers Weaponize CVE-2024-4577 to Deploy Cobalt Strike and Compromise Systems

Date of Publication	Admiralty Code	TA Number
March 10, 2025	A1	TA2025070

Summary

Attack Discovered: January 2025
Targeted Country: Japan
Affected Industries: Technology, Telecommunication, Entertainment, Education and Research Institute, E-commerce
Affected Platform: Windows
Attack: Since January 2025, an unidentified threat actor has been targeting organizations in Japan by exploiting CVE-2024-4577, a remote code execution (RCE) flaw in the PHP-CGI implementation on Windows, to gain initial access. Once inside, they execute PowerShell scripts to deploy a Cobalt Strike reverse HTTP shellcode payload, establishing persistent remote access. For post-exploitation, they leverage TaoWu, a set of publicly available Cobalt Strike plugins, enabling further control over compromised systems and facilitating lateral movement within the network.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-4577	PHP-CGI OS Command Injection Vulnerability	PHP version: 5 - 8.3.7	✗	✓	✓

Attack Details

#1 Since January 2025, an unidentified threat actor has been targeting organizations in Japan, leveraging CVE-2024-4577, a vulnerability in the PHP-CGI implementation on Windows. By exploiting this flaw, the attacker gains initial access and executes a PowerShell script to establish remote control over victim machines. They then gather system details, assess user privileges, and escalate their access by running privilege escalation exploits. To maintain persistence, they modify registry keys, create malicious services, and use scheduled tasks.

#2 To evade detection, the attacker clears event logs, conducts network reconnaissance, and abuses Group Policy Objects (GPOs) using SharpGPOAbuse.exe. They deploy Mimikatz to extract and exfiltrate credentials, including passwords and NTLM hashes. Their attack chain begins with a publicly available Python exploit script, which determines if a target URL is vulnerable by sending a crafted POST request containing PHP code. If successful, the response includes a predefined MD5 hash, confirming exploitation. The attacker then executes arbitrary PHP commands remotely.

#3 Once executed, this shellcode injects itself into memory and connects to a command-and-control (C2) server over HTTP, granting remote access. With control established, the attacker issues commands from a Cobalt Strike team server equipped with plugins from the TaoWu toolkit. Using Ladon.exe, they bypass user access controls, while other TaoWu.NET plugins modify registry keys and create scheduled tasks for persistence.

#4 The attacker further strengthens persistence by deploying SharpTask.exe to schedule tasks, SharpHide.exe to create hidden registry keys, and SharpStay.exe to establish a malicious Windows service. To cover their tracks, they leverage wevtutil.exe, a living-off-the-land binary (LoLBin), to wipe event logs. Network reconnaissance and lateral movement are conducted using fscan.exe and Seatbelt, tools that enumerate security-relevant system configurations. Additionally, SharpGPOAbuse.exe is used to manipulate GPOs for further privilege escalation.

#5 Their infrastructure includes two C2 servers hosted on Alibaba Cloud and running the Cobalt Strike team server. One is an exposed root directory, revealing stored PowerShell scripts, Cobalt Strike beacons, and exploit programs. The attacker also downloaded and executed a shell script from Gitee's repository, linked to a Chinese cybersecurity training service, possibly repurposed for malicious intent.

#6 While threat actors frequently rely on Cobalt Strike, Metasploit, ARL, Vulfocus, and PowerShell Empire, some tools in this attack - Blue-Lotus, BeEF, and Viper C2 are less commonly seen in malicious operations. These tools have been documented in threat intelligence reports to highlight their offensive capabilities and potential for abuse in targeted intrusions. Meanwhile, CVE-2024-4577 has been exploited by various ransomware strains and malware over the past year.

Recommendations

Apply Patch: Immediately update PHP installations to a patched version that addresses CVE-2024-4577. Ensure that Windows-based PHP environments using CGI configurations are secured with the latest security updates.

Strengthen System Security: Limit administrative access by following the principle of least privilege (PoLP), ensuring that users and applications only have the permissions they absolutely need. Regularly review and audit registry changes and scheduled tasks to detect any unauthorized modifications. Restrict PowerShell execution to prevent abuse and closely monitor script activity to identify suspicious behavior before it becomes a threat.

Strengthen Network Security and Monitoring: Set up intrusion detection and prevention systems (IDS/IPS) to identify and block any attempts to exploit vulnerabilities. Keep a close watch on outbound network traffic to spot unusual connections, especially those linking to unknown command-and-control (C2) servers, which could indicate an ongoing attack.

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.

Improve Log and Event Monitoring: Enable and actively monitor Windows event logs, focusing on PowerShell activity and scheduled tasks to detect potential threats. Regularly review logs for any signs of tampering, such as unexpected log clearing, which could indicate an attacker attempting to cover their tracks.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0043 Reconnaissance	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0008 Lateral Movement	TA0010 Exfiltration	T1033 System Owner/User Discovery	T1068 Exploitation for Privilege Escalation
T1112 Modify Registry	T1053 Scheduled Task/Job	T1543 Create or Modify System Process	T1070 Indicator Removal
T1070.001 Clear Windows Event Logs	T1570 Lateral Tool Transfer	T1003 OS Credential Dumping	T1003.001 LSASS Memory
T1041 Exfiltration Over C2 Channel	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.006 Python	T1592 Gather Victim Host Information	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	38[.]14[.]255[.]23, 118[.]31[.]18[.]77
URLs	hxxp[://]38[.]14[.]255[.]23[:]8077/6Qeq, hxxp[://]38[.]14[.]255[.]23[:]8077/jANd
SHA256	a2f493769c0cd1cb3518571678f071588d683703ed368830f15405c1eb4028b2, 73d908725a08dcfebf300ef187dab1c5ba1c3cba8343c678df49335ba7e89e47, 83290b2f6e7b3fb1bcfa90ed1e550acaeb85c7dc0cb4476b35818436af9395d2, cec655cc4c6bfcbc336d3afc4e5537e619bcf58329d291a51f39b3d3a250e962, ccedc244ad5933537231139e24b4cad0df3e44d3b2944ef3b28dea5973396185, f7396835d69675b138d0e2bee9b4ceb0a048bf705cb2f1012f1eee51e406d6e6, 6b5a75dcc505ac1c065844be27ee6d4693ac51abfc04aaf9bbfc1a06e69a19fd, ad5f610e8fb4f0d74d5d761532c8c8b2b9e01a2a402ba89389794d15ecca8337, 07d8a505492566daeb6174c312a4f7114dc60efcd1d17fef12ca0b8d6303fb2b, 8015b6036ecbae1f9e850af6bdf361d7598201cd4d4c55ae334ed72cf17ba94d, 0ff87724012499381266e5eb8481117ed4549f44fa88be2c517afee899c2179f, 829c5a07b065b15969ea8c519705d64fc4c1c39c05e898fc9abfbdb289c484d5, 3c6511b15e3b0e8c378a549347fa0f0745fd371aaa86206cb03528fdc0a23b29

Patch Details

Upgrade to the latest patched PHP versions 8.3.8, 8.2.20, and 8.1.29 is highly recommended.

Link: https://www.php.net/downloads

References

https://blog.talosintelligence.com/new-persistent-attacks-japan/

https://www.hivepro.com/threat-advisory/php-rce-flaw-opens-a-gateway-for-tellyouthepass-ransomware/

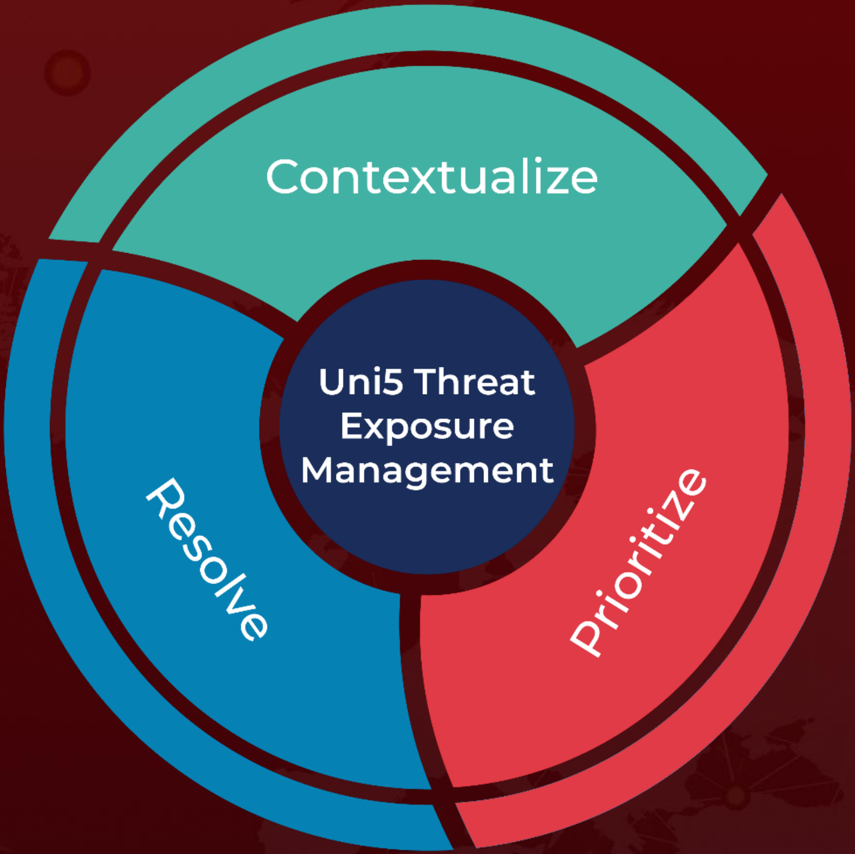
https://hivepro.com/threat-advisory/msupedge-backdoor-haunts-taiwan-institution/

https://www.hivepro.com/threat-advisory/php-rce-flaw-opens-a-gateway-for-tellyouthepass-ransomware/

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 10, 2025 • 5:30 AM

More at www.hivepro.com