Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

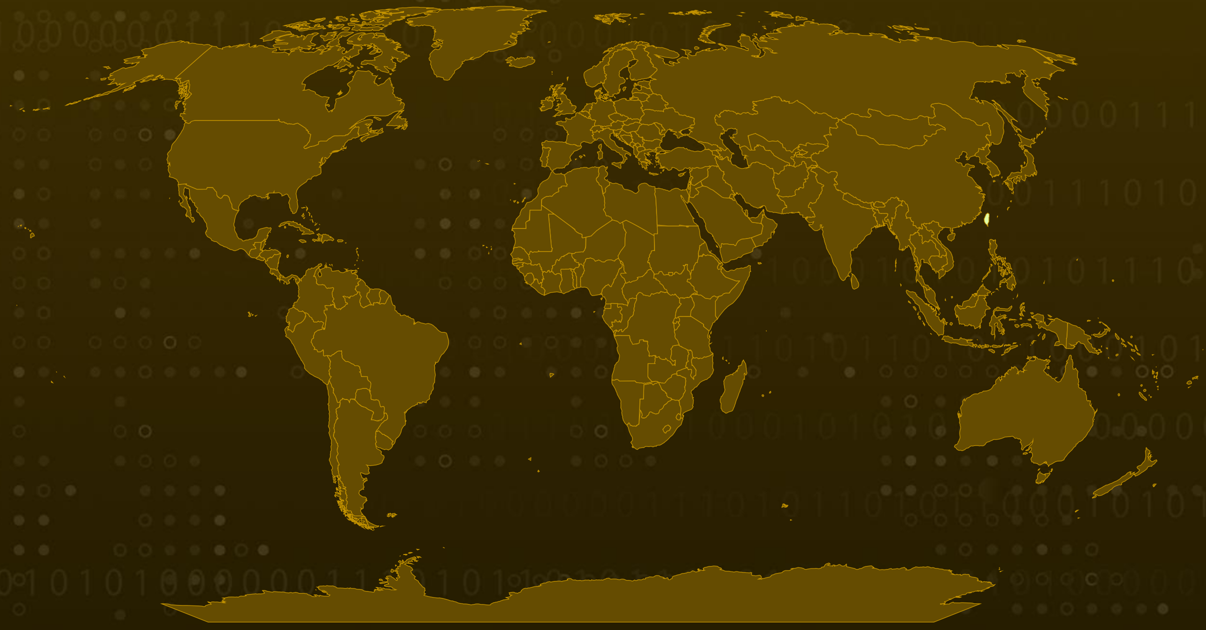
Msupedge Backdoor Haunts Taiwan Institution

Date of Publication	Admiralty Code	TA Number
August 21, 2024	A1	TA2024321

Summary

First Seen: July 2024
Malware: Msupedge Backdoor
Targeted Country: Taiwan
Targeted Industry: Education
Attack: The newly discovered "Msupedge" backdoor has been deployed in a recent cyberattack targeting a university in Taiwan. This advanced malware is notable for its use of DNS traffic to establish communication with its command-and-control (C&C) server. The attack likely exploited a critical PHP vulnerability, enabling remote code execution.

Attack Regions



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

CVE

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

Attack Details

#1 A newly identified backdoor, dubbed "Msupedge," has been utilized in a recent cyberattack targeting a university in Taiwan. A key feature of the Msupedge backdoor is its ability to communicate with a command-and-control (C&C) server using DNS traffic.

#2 The initial method of access that facilitated the deployment of Msupedge likely involved exploiting a critical vulnerability in PHP, known as CVE-2024-4577. This flaw, which was disclosed recently, could be exploited to achieve remote code execution.

#3 Msupedge functions as a dynamic link library (DLL) and uses DNS tunneling to interact with the C&C server. The DNS tunneling mechanism is based on the open-source dnscat2 tool. The backdoor receives its commands by resolving DNS queries.

#4 Interestingly, Msupedge not only obtains instructions via DNS traffic but also interprets the resolved IP address of the C&C server as part of the command structure. Specifically, the third octet of the resolved IP address acts as a switch case. By subtracting seven and converting it to hexadecimal, determines its behavior and triggers the appropriate actions.

Recommendations

Patch Critical Vulnerabilities: Ensure that all systems, especially those running PHP, are updated to address critical vulnerabilities such as CVE-2024-4577. Regularly check for and apply security patches and updates to mitigate potential exploitation.

Utilize Application Control: Implement application whitelisting to ensure that only approved applications can run on your systems, preventing unauthorized or malicious executables, such as backdoors, from executing. Additionally, deploy application control solutions that analyze application behavior to detect and block any unusual or unauthorized activities.

Network Traffic Analysis: Use deep packet inspection (DPI) to examine the contents of network traffic and detect hidden or encrypted data channels that malware might use for command-and-control communication. Additionally, implement anomaly-based detection systems to identify unusual network traffic patterns that could indicate backdoor activity.

Adopt Zero Trust Architecture: Embrace a Zero Trust security model that verifies and validates every access attempt, regardless of whether it originates from inside or outside the network perimeter, reducing the attack surface and thwarting unauthorized access attempts by sophisticated adversaries.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**TA0042** Resource Development
T1071 Application Layer Protocol	**T1543** Create or Modify System Process	**T1046** Network Service Discovery	**T1071.004** DNS
T1190 Exploit Public-Facing Application	**T1033** System Owner/User Discovery	**T1548** Abuse Elevation Control Mechanism	**T1105** Ingress Tool Transfer
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1083** File and Directory Discovery
T1505.003 Web Shell	**T1070.004** File Deletion		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e08dc1c3987d17451a3e86c04ed322a9424582e2f2cb6352c892b7e0645eda, f5937d38353ed431dc8a5eb32c119ab575114a10c24567f0c864cb2ef47f9f, a89ebe7d1af3513d146a831b6fa4a465c8edeafea5d7980eb5448a94a4e344
File Path	csidl_drive_fixed\xampp\wuplog.dll, csidl_system\wbem\wmiclnt.dll

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

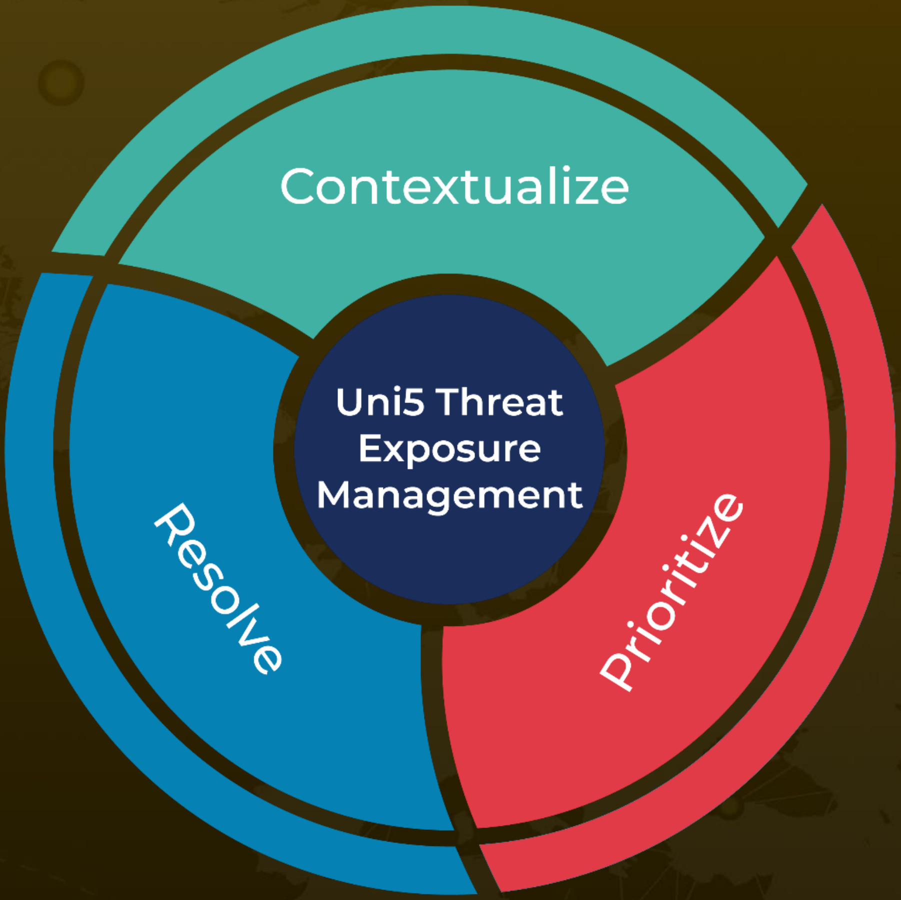
https://symantec-enterprise-blogs.security.com/threat-intelligence/taiwan-malware-dns

https://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

August 21, 2024 • 5:00 AM

More at www.hivepro.com