ASPXSpy (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:58:21 UTC

php.aspxspy (Back to overview)

ASPXSpy

Actor(s): APT39, APT41, HAFNIUM

ASPXSpy is an open-source web shell written in C# that allows a threat actor to accomplish various post-exploitation tasks, including file access and command execution.

References

2023-02-13 · AhnLab · kingkimgim
Dalbit (m00nlight): Chinese Hacker Group’s APT Attack Campaign
Godzilla Webshell ASPXSpy BlueShell CHINACHOPPER Cobalt Strike Ladon MimiKatz Dalbit

2022-10-03 · Kaspersky Labs · GReAT
DeftTorero: tactics, techniques and procedures of intrusions revealed
Nightrunner Tunna ASPXSpy LaZagne ExplosiveRAT reGeorg Volatile Cedar

2021-12-14 · Recorded Future · Insikt Group
Full Spectrum Detections for 5 Popular Web Shells: Alfa, SharPyShell, Krypton, ASPXSpy, and TWOFACE
TwoFace ASPXSpy SharPyShell

2019-09-23 · MITRE · MITRE ATT&CK
APT41
Derusbi MESSAGETAP Winnti ASPXSpy BLACKCOFFEE CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT MimiKatz NjRAT PlugX ShadowPad Winnti ZXShell APT41

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/php.aspxspy