Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

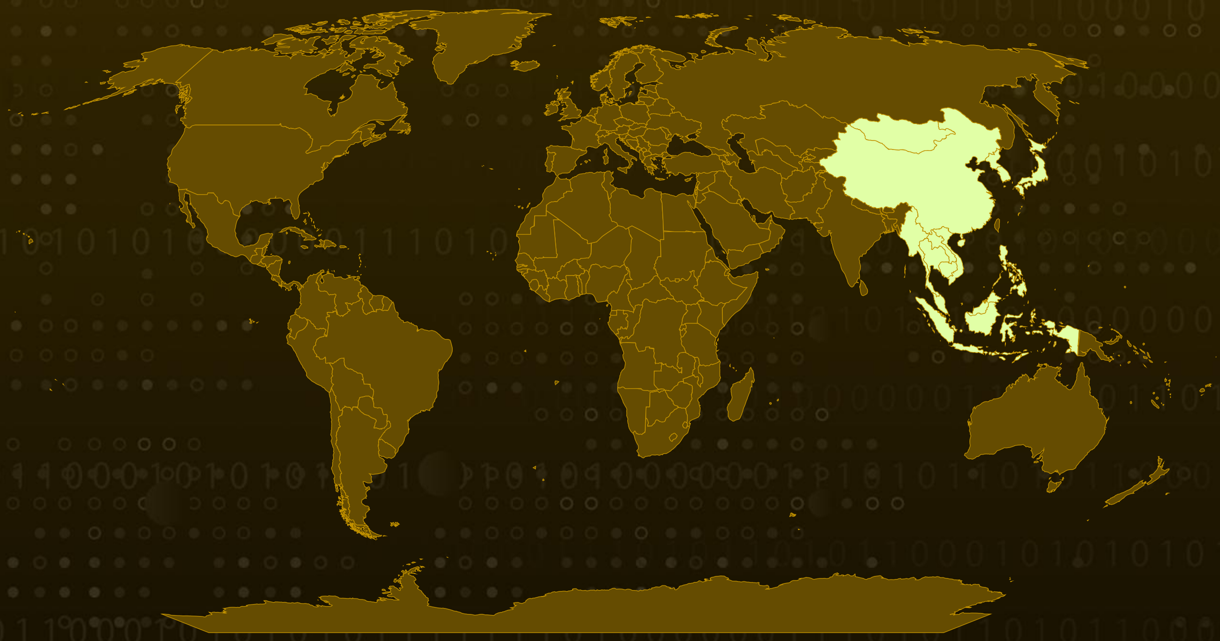
Operation Rewrite: How BadIIS Rewired the Web for SEO Poisoning

Date of Publication	Admiralty Code	TA Number
September 24, 2025	A1	TA2025294

Summary

Attack Discovered: March 2025
Targeted Countries: East and Southeast Asia
Cluster: CL-UNK-1037
Malware: BadIIS
Campaign: Operation Rewrite
Attack: Operation Rewrite is a stealthy campaign where Chinese-speaking hackers turned search engines into traps, using a malicious IIS module called BadIIS to secretly rewrite web traffic. Instead of building their own websites, they hijacked legitimate ones, stuffing them with keywords to climb search rankings and lure unsuspecting users. When victims clicked what looked like a normal search result, they were silently redirected to scam pages controlled by the attackers. With a tailored focus on East and Southeast Asia, especially Vietnam, and multiple variants of their toolkit, the operation shows how attackers can twist the very tools we trust to find information into powerful weapons of deception.

Attack Regions



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

Attack Details

#1

In March 2025, a Chinese-speaking threat actor was uncovered running a sophisticated search engine optimization (SEO) poisoning campaign dubbed “Operation Rewrite.” At the heart of the operation is BadIIS, a malicious native IIS module designed to intercept and tamper with web traffic on compromised servers. The campaign shows a clear geographic focus on East and Southeast Asia, especially Vietnam, with tailored logic for local search engines. Beyond BadIIS, the threat actors deploy a wider toolkit that includes ASP.NET handlers, managed .NET IIS modules, and standalone PHP scripts.

#2

BadIIS was first profiled in 2021. The implant is capable of injecting malicious JavaScript, hijacking 404 errors, issuing silent redirects, tunneling traffic, and even harvesting sensitive information. Its strategy is twofold: first, trick search engines into indexing poisoned content, and then lure real users who click those links. By feeding search engine crawlers keyword-stuffed HTML, the attackers ensure that compromised websites appear to rank for trending or popular search terms. Once a victim clicks a manipulated result, BadIIS silently redirects their browser to attacker-controlled pages, completing the trap.

#3

The attackers gained an initial foothold by breaching web servers, escalating privileges, and spreading laterally to other high-value hosts. They planted multiple web shells, created new user accounts, and compressed sensitive application directories for exfiltration. The implants were registered as IIS modules, enabling them to alter web responses before a user ever sees them. By injecting links for popular terms, the campaign hijacked local search relevance to maximize visibility.

#4

The malware’s origin traces back to a C++ class name, chongxiede (“rewrite” in Pinyin), which inspired the campaign’s title. Linguistic clues, simplified Chinese code comments, and overlapping infrastructure linked the activity to the Chinese-speaking cluster CL-UNK-1037. Researchers attribute it with moderate confidence to Group 9 and lower confidence to DragonRank, supported by overlaps in C2 domains, URL patterns, and shared technical elements like the RegisterModule function.

#5

BadIIS has since evolved into three variants: an ASP.NET handler that cloaks malicious activity, a managed IIS module that hijacks 404 errors and injects content, and a PHP-based script for quick deployment that even fabricates XML sitemaps for Googlebot. These updates highlight Operation Rewrite’s growth into a flexible, multi-pronged campaign designed to exploit trust in search engines across the region.

Recommendations

Keep your servers patched and monitored: Attackers often exploit outdated software to infiltrate systems. Make sure your IIS servers and related web applications are regularly updated and keep an eye on unusual activities like unknown DLLs or suspicious user accounts.

Watch for strange traffic patterns: SEO poisoning thrives on redirecting users. Monitor for odd referral traffic or spikes in visits from unexpected keywords, these could be signs your site has been compromised.

Harden your web infrastructure: Use strong access controls, disable unused modules, and limit who can upload or register IIS modules. If an attacker can't plant their implant, they can't hijack your traffic.

Inspect your site content regularly: Look for injected links, hidden keywords, or unexpected scripts on your webpages. Even if the site looks fine to you, attackers often cloak content to only show poisoned results to search engines.

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.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0010** Exfiltration	**TA0011** Command and Control	**T1608** Stage Capabilities
T1608.006 SEO Poisoning	**T1505** Server Software Component	**T1505.004** IIS Components	**T1505.003** Web Shell
T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1078** Valid Accounts	**T1053** Scheduled Task/Job

T1041 Exfiltration Over C2 Channel	**T1071** Application Layer Protocol	**T1204** User Execution	**T1036** Masquerading
T1189 Drive-by Compromise			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	01a616e25f1ac661a7a9c244fd31736188ceb5fce8c1a5738e807fdbef70fd60, bc3bba91572379e81919b9e4d2cbe3b0aa658a97af116e2385b99b610c22c08c, 5aa684e90dd0b85f41383efe89dddb2d43ecbdaf9c1d52c40a2fdf037fb40138, c5455c43f6a295392cf7db66c68f8c725029f88e089ed01e3de858a114f0764f, 82096c2716a4de687b3a09b638e39cc7c12959bf380610d5f8f9ac9cddab64d7, ed68c5a8c937cd55406c152ae4a2780bf39647f8724029f04e1dce136eb358ea, 6d79b32927bac8020d25aa326ddf44e7d78600714beacd473238cc0d9b5d1ccf, b95a1619d1ca37d652599b0b0a6188174c71147e9dc7fb4253959bd64c4c1e9f, 8078fa156f5ab8be073ad3f616a2302f719713aac0f62599916c5084dd326060, a73c7f833a83025936c52a8f217c9793072d91346bb321552f3214efdeef59eb, 6d044b27cd3418bf949b3db131286c8f877a56d08c3bbb0924baf862a6d13b27, 78ef67ec600045b7deb8b8ac747845119262bea1d51b2332469b1f769fb0b67d, 78ef67ec600045b7deb8b8ac747845119262bea1d51b2332469b1f769fb0b67d, 88de33754e96cfa883d737aea7231666c4e6d058e591ef3b566f5c13a88c0b56, a393b62df62f10c5c16dd98248ee14ca92982e7ac54cb3e1c83124c3623c8c43, 40a0d0ee76b72202b63301a64c948acb3a4da8bac4671c7b7014a6f1e7841bd2, 40a0d0ee76b72202b63301a64c948acb3a4da8bac4671c7b7014a6f1e7841bd2,

TYPE	VALUE
SHA256	1c870ee30042b1f6387cda8527c2a9cf6791195e63c5126d786f807239bd0ddc, 271c1ddfdfb6ba82c133d1e0aac3981b2c399f16578fcf706f5e332703864656, 22a9e1675bd8b8d64516bd4be1f07754c8f4ad6c59a965d0e009cbeaca6147a7, e2e00fd57d177e4c90c1e6a973cae488782f73378224f54cf1284d69a88b6805, 23aa7c29d1370d31f2631abd7df4c260b85227a433ab3c7d77e8f2d87589948f, ab0b548931e3e07d466ae8598ca9cd8b10409ab23d471a7124e2e67706a314e8, 22a4f8aead6aef38b0dc26461813499c19c6d9165d375f85fb872cd7d9eba5f9, de570369194da3808ab3c3de8fb7ba2aac1cc67680ebdc75348b309e9a290d37, d8a7320e2056daf3ef4d479ff1bb5ce4facda67dfc705e8729aeca78d6f9ca84, d6a0763f6ef19def8a248c875fd4a5ea914737e3914641ef343fe1e51b04f858, c6622e2900b8112e8157f923e9fcbd48889717adfe1104e07eb253f2e90d2c6a, 6cff06789bf27407aa420e73123d4892a8f15cae9885ff88749fd21aa6d0e8ad, b056197f093cd036fa509609d80ece307864806f52ab962901939b45718c18a8, 2af61e5acc4ca390d3bd43bc649ab30951ed7b4e36d58a05f5003d92fde5e9a7, 36bf18c3edd773072d412f4681fb25b1512d0d8a00aac36514cd6c48d80be71b
URLs	hxxp[:]//103[.]6[.]235[.]26/xvn[.]html, hxxp[:]//x404[.]008php[.]com/zz/u[.]php, hxxp[:]//103[.]6[.]235[.]78/vn[.]html, hxxp[:]//x404[.]008php[.]com/index[.]php, hxxp[:]//103[.]6[.]235[.]78/index[.]php, hxxp[:]//103[.]6[.]235[.]78/zz/u[.]php, hxxp[:]//cs[.]pyhycy[.]com/index[.]php, hxxp[:]//cs[.]pyhycy[.]com/zz/u[.]php, hxxps[:]//sl[.]008php[.]com/kt[.]html, hxxp[:]//160[.]30[.]173[.]87/zz/u[.]php, hxxp[:]//404[.]pyhycy[.]com/index[.]php, hxxp[:]//404[.]pyhycy[.]com/zz/u[.]php, hxxp[:]//404[.]hao563[.]com/index[.]php, hxxp[:]//404[.]300bt[.]com/zz/u[.]php, hxxp[:]//404[.]yyphw[.]com/index[.]php, hxxp[:]//103[.]6[.]235[.]26/kt[.]html,

TYPE	VALUE
URLs	hxxp[:]//404[.]yyphw[.]com/zz/u[.]php, hxxp[:]//404[.]hzyzn[.]com/index[.]php, hxxp[:]//404[.]hzyzn[.]com/zz/u[.]php, hxxp[:]//404[.]300bt[.]com/index[.]php, hxxp[:]//103[.]248[.]20[.]197/index[.]php, hxxp[:]//103[.]248[.]20[.]197/zz/u[.]php, hxxps[:]//fb88s[.]icu/uu/tt[.]js, hxxp[:]//404[.]hao563[.]com/zz/u[.]php, hxxp[:]//www[.]massnetworks[.]org, hxxp[:]//vn404[.]008php[.]com/index[.]php, hxxp[:]//vn404[.]008php[.]com/zz/u[.]php, hxxp[:]//404[.]008php[.]com/zz/u[.]php

References

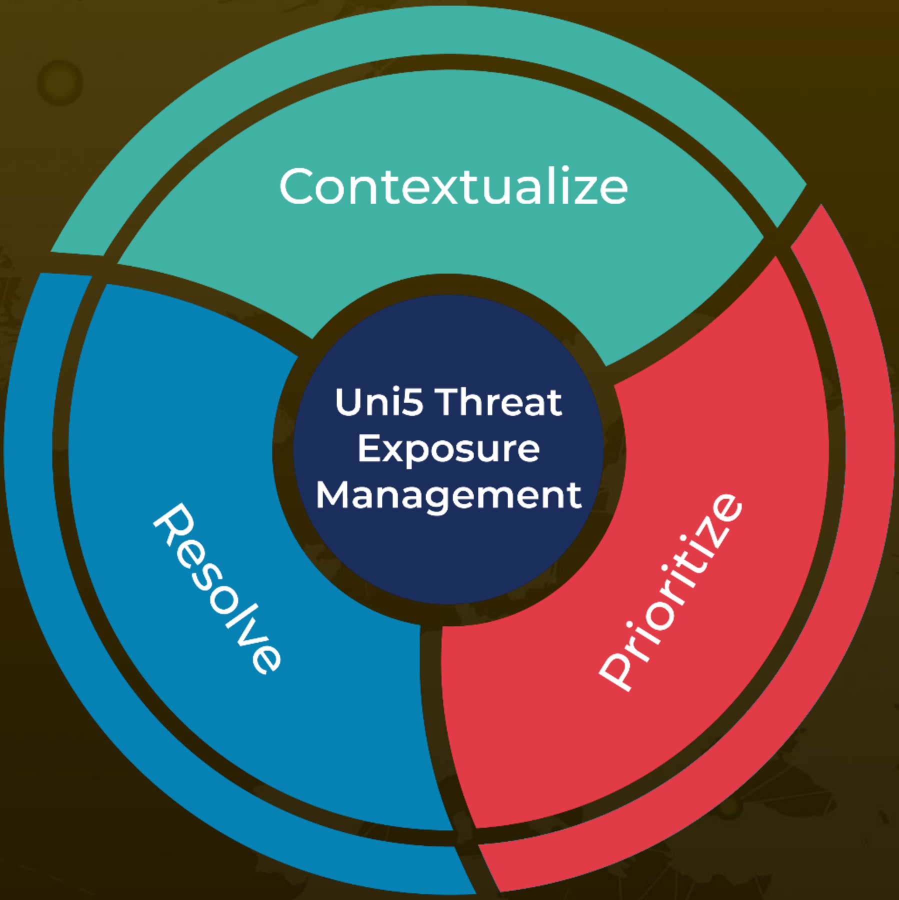
https://unit42.paloaltonetworks.com/operation-rewrite-seo-poisoning-campaign/

https://hivepro.com/threat-advisory/dragonrank-the-seo-hackers-manipulating-search-results/

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

September 24, 2025 • 9:30 AM

More at www.hivepro.com