Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

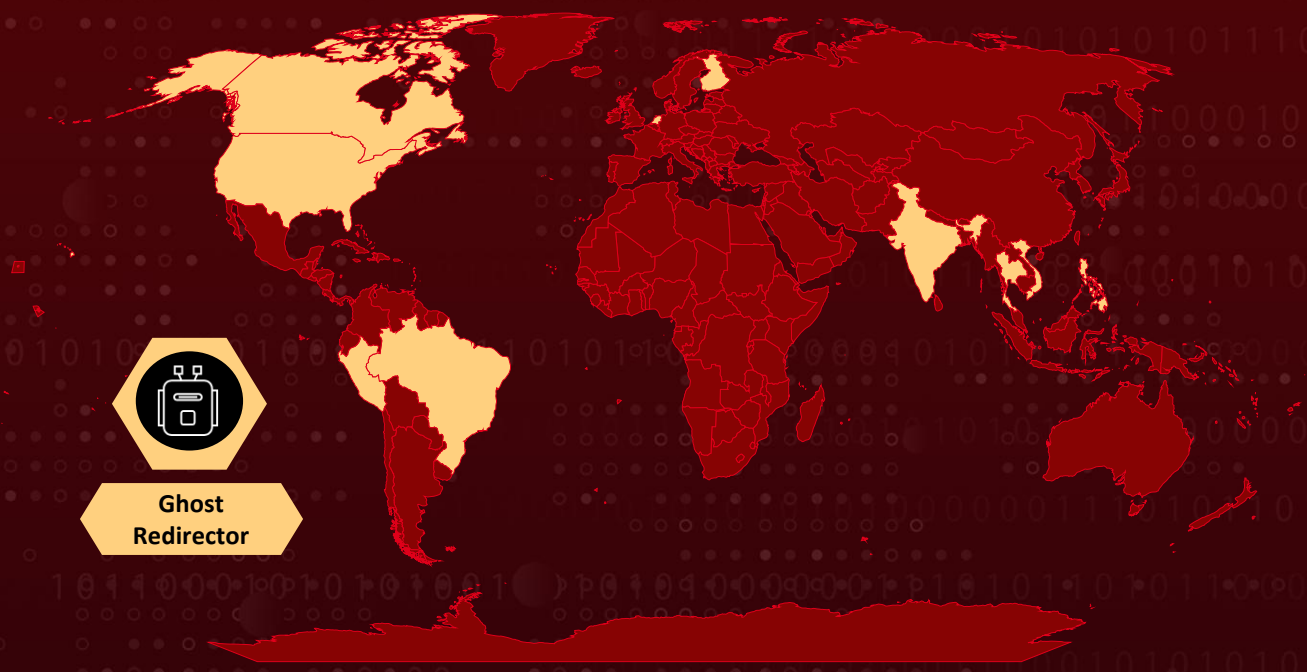
GhostRedirector Targets Windows Servers Globally for SEO Fraud

Date of Publication	Admiralty Code	TA Number
September 5, 2025	A1	TA2025269

Summary

First Seen: August 2024
Targeted Countries: Brazil, Peru, Thailand, Vietnam, United States, Canada, Finland, India, Netherlands, Philippines, Singapore
Targeted Platforms: Windows
Threat Actor: GhostRedirector
Targeted Industries: Education, Healthcare, Insurance, Transportation, Technology, Retail
Malware: Rungan, Gamshen
Attack: GhostRedirector is a newly discovered China-aligned threat actor targeting Windows servers worldwide since 2024, compromising at least 65 servers by mid-2025. The group gains access through SQL injection flaws, escalates privileges using public exploits, and deploys a backdoor (Rungan) along with an IIS trojan (Gamshen). While Rungan enables covert command execution, Gamshen manipulates Google search crawlers to inject backlinks, boosting illicit sites, often tied to gambling. Supported by tools like Zunput and misused remote utilities, the campaign is financially motivated, resilient, and opportunistic, demonstrating a modular approach to monetizing compromised infrastructure at scale.

Attack Regions



Attack Details

#1 GhostRedirector is a newly identified threat actor targeting Windows servers, active since at least August 2024 and detected on 65 servers by June 2025. While the campaign has a global reach, most victims are in Brazil, Thailand, and Vietnam. Initial access is likely gained through SQL injection flaws, with attackers using built-in tools like PowerShell and CertUtil to pull malicious payloads from their infrastructure.

#2 Once inside, the group escalates privileges with public exploits such as EfsPotato and BadPotato, some signed with legitimate Chinese-issued certificates. This allows them to create administrator accounts, alter user credentials, and establish persistence across compromised servers.

#3 The campaign mainly using two custom tools, Rungan, a passive C++ backdoor, and a Gamshen IIS trojan. Rungan, deployed as a disguised DLL, passively listens for crafted HTTP requests to execute commands or maintain control. Gamshen manipulates Googlebot traffic by injecting backlinks to gambling websites, enabling stealthy SEO fraud while remaining invisible to regular users.

#4 The attackers reinforce their operations with tools like Zunput, which drops webshells into dynamic directories, and legitimate but misused utilities such as GoToHTTP for remote access. This layered toolkit provides resilience, ensuring persistence even if some components are removed. Targets span industries from healthcare to retail, showing opportunistic rather than sector-specific targeting.

#5 Clues such as Chinese-language strings, a Chinese code-signing certificate, and embedded credentials suggest GhostRedirector is China-aligned. However, the campaign appears financially motivated, using privilege escalation, hidden backdoors, and SEO manipulation to monetize compromised infrastructure at scale.

Recommendations

Prevent Initial Access: Regularly patch web applications and databases to close vulnerabilities like SQL injection, the most likely entry point. Enforce web application firewalls (WAFs) and input validation to block injection attempts. Monitor PowerShell, CertUtil, and other Living-off-the-Land (LOLBins) tools for suspicious use, especially when reaching out to unknown domains.

Detect and Contain Privilege Escalation: Audit the creation or modification of administrator accounts and changes to user credentials. Deploy endpoint detection tools capable of spotting privilege escalation exploits like EfsPotato and BadPotato. Revoke or block binaries signed with suspicious or misused certificates, even if they appear legitimate.

Identify and Remove Persistence Mechanisms: Inspect IIS servers for unauthorized DLLs or modules, especially ones like miniscreen.dll. Monitor for webshells in dynamic directories (PHP, ASPX, etc.) using both signature-based and heuristic scanning. Review scheduled tasks, services, and autoruns for abnormal entries that may ensure attacker persistence.

Harden SEO Manipulation Vectors: Periodically review IIS configurations for unknown modules. Compare web content served to crawlers (Googlebot) vs. normal users to detect cloaking or hidden injection. Monitor outbound traffic for signs of communication with attacker-controlled C2 domains.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0006 Credential Access	TA0040 Impact	TA0011 Command and Control

TA0003 Persistence	TA0004 Privilege Escalation	T1112 Modify Registry	T1027.009 Embedded Payloads
T1059.003 Windows Command Shell	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation
T1008 Fallback Channels	T1565 Data Manipulation	T1588.002 Tool	T1588 Obtain Capabilities
T1083 File and Directory Discovery	T1219 Remote Access Software	T1071.001 Web Protocols	T1071 Application Layer Protocol
T1587 Develop Capabilities	T1587.001 Malware	T1608.006 SEO Poisoning	T1608 Stage Capabilities
T1583 Acquire Infrastructure	T1583.001 Domains	T1583.004 Server	T1134 Access Token Manipulation
T1608.001 Upload Malware	T1608.002 Upload Tool	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information
T1588.003 Code Signing Certificates	T1190 Exploit Public-Facing Application	T1106 Native API	T1559 Inter-Process Communication
T1546 Event Triggered Execution			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	EE22BA5453ED577F8664CA390EB311D067E47786, 677B3F9D780BE184528DE5967936693584D9769A, 5D4D7C96A9E302053BDFAF2449F9A2AB3C806E63, 28140A5A29EBA098BC6215DDAC8E56EACBB29B69,

TYPE	VALUE
SHA1	371818BDC20669DF3CA44BE758200872D583A3B8, 9DD282184DDFA796204C1D90A46CAA117F46C8E1, 87F354EAA1A6ED5AE51C4B1A1A801B6CF818DAFC, 5A01981D3F31AF47614E51E6C216BED70D921D60, 6EBD7498FC3B744CED371C379BA537077DD97036, 0EE926E29874324E52DE816B74B12069529BB556, 373BD3CED51E19E88876B80225ECA65A5C01413F, 5CFFC4B3B96256A45FB45056AE0A9DC76329C25A, B017CEE02D74C92B2C65517101DC72AFA7D18F16, A8EE056799BFEB709C08D0E41D9511CED5B1F19D, C4681F768622BD613CBF46B218CDA06F87559825, E69E4E5822A81F68107B933B7653C487D055C51B, A3A55E4C1373E8287E4E4D5D3350AC665E1411A7, E6E4634CE5AFDA0688E73A2C21A2ECDABD5E155D, 5DFC2D0858DD7E811CD19938B8C28468BE494CB6, 08AB5CC8618FA593D2DF91900067DB464DC72B3E, 871A4DF66A8BAC3E640B2D1C0AFC075BB3761954, 049C343A9DAAF3A93756562ED73375082192F5A8
Filename	SitePut.exe, EfsNetAutoUser.exe, NetAutoUser.exe, miniscreen.dll, auto.exe, auto_sign.exe, EfsNetAutoUser.exe, DotNet4.5.exe, NetAUtoUser_sign .exe, link.exe, ManagedEngine32 _v2.dll, ManagedEngine64 _v2.dll
IPv4	104[.]233[.]192[.]1, 104[.]233[.]210[.]229, 43[.]228[.]126[.]4, 103[.]251[.]112[.]11
Domains	xzs[.]868id[.]com, xz[.]868id[.]com, q[.]822th[.]com www[.]881vn[.]com, gobr[.]868id[.]com, brproxy[.]868id[.]com, www[.]cs01[.]shop

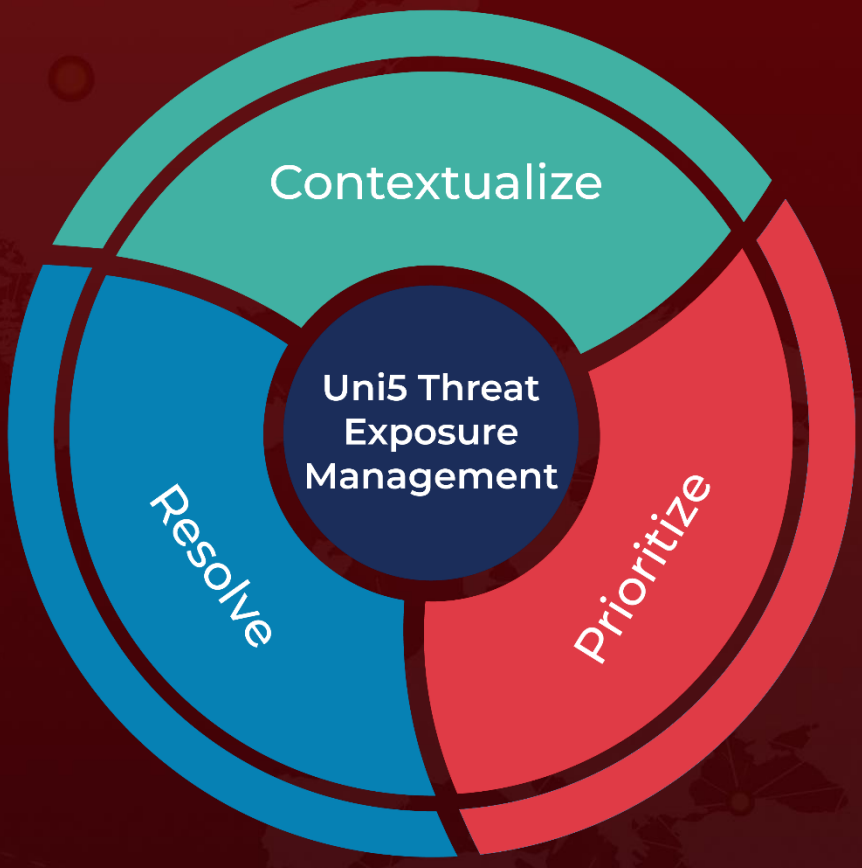
References

https://www.welivesecurity.com/en/eset-research/ghostredirector-poisons-windows-servers-backdoors-side-potatoes/

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 5, 2025 • 4:30 AM

More at www.hivepro.com