Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

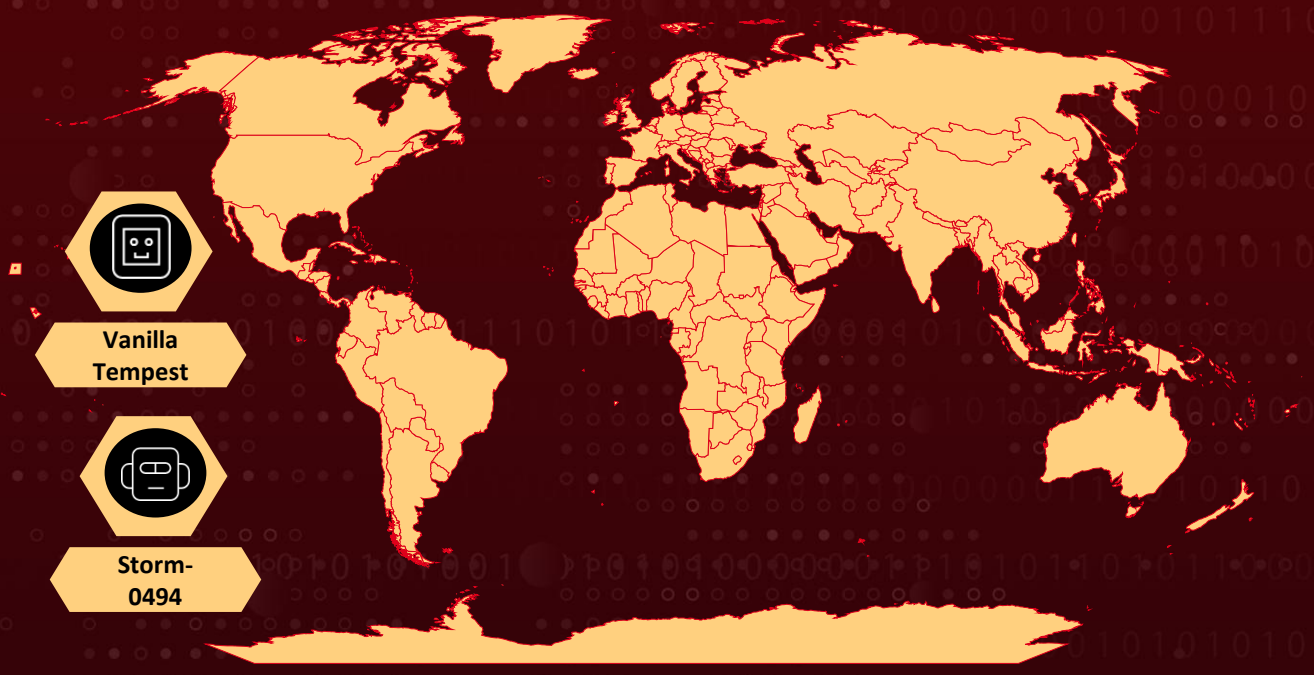
Return of Gootloader: Blending Technical Evasion with Operational Discipline

Date of Publication	Admiralty Code	TA Number
November 7, 2025	A1	TA2025340

Summary

Attack Commenced: October 27, 2025
Targeted Countries: Worldwide
Targeted Platforms: Windows
Threat Actor: Storm-0494, Vanilla Tempest (DEV-0832, Vice Society)
Malware: Gootloader, Supper backdoor, Rhysida ransomware
Attack: Gootloader re-emerged in late October 2025 with renewed activity, leading to rapid domain controller compromises within hours of infection. The campaign features advanced evasion using custom WOFF2 fonts for filename obfuscation and continues leveraging SEO poisoning and compromised WordPress sites for initial access. It now uses XOR-encrypted payloads and Startup-folder shortcuts with Windows 8.3 filenames for persistence. The operation reflects collaboration between Storm-0494 and the Rhysida ransomware group, demonstrating a fast, organized, and technically sophisticated threat chain.

Attack Regions



Attack Details

#1

Gootloader has resurfaced after a period of reduced activity, returning in late October 2025 with renewed and aggressive operations. It's been observed multiple infections beginning October 27, two of which escalated into hands-on-keyboard intrusions that achieved domain controller compromise within just 17 hours of initial infection. This demonstrates the attackers' operational efficiency and their ability to progress rapidly from initial access through reconnaissance, privilege escalation, and lateral movement.

#2

The campaigns follow a consistent pattern that includes Active Directory enumeration through Kerberoasting, SPN scanning, and WinRM-based lateral movement, ultimately leading to privileged account creation and preparatory actions for ransomware deployment. A key technical evolution in these campaigns is the use of custom WOFF2 web fonts with glyph substitution to obfuscate filenames within the malicious JavaScript payloads. This method hides readable text in the source code, revealing it only when rendered by the browser, thereby evading static detection mechanisms.

#3

The loader continues to abuse WordPress comment submission endpoints (/wp-comments-post.php) to deliver XOR-encrypted ZIP archives, each uniquely keyed by its obfuscated filename. The infection chain also reflects the group's continued reliance on Search Engine Optimization (SEO) poisoning, which lures victims searching for business-related documents to compromised WordPress sites. For persistence, Gootloader has shifted from scheduled tasks to Startup-folder shortcuts using Windows 8.3 short filenames to obscure true file paths and hinder analysis.

#4

Following initial compromise, the attackers deploy the "Supper" SOCKS5 backdoor, which employs heavy obfuscation techniques including API hashing, runtime shellcode injection, API hammering, and custom LZMA compression. Despite its simple functionality, providing SOCKS proxying and remote shell access, the backdoor's encryption and rotating C2 infrastructure ensure reliable, covert access. This operation highlights the collaboration between Storm-0494 (Gootloader operators) and Vanilla Tempest/Rhysida ransomware actors, where the former handles infection and initial access, and the latter conducts rapid reconnaissance and domain controller compromise within hours.

Recommendations

Early Detection and Monitoring: Implement behavioral monitoring in EDR and SIEM platforms to detect suspicious PowerShell, WScript, or CScript activity, especially processes launched from unusual locations such as %AppData%. Hunt for Startup-folder .lnk shortcuts referencing JavaScript files or using Windows 8.3 short filenames.

Network Defense and Blocking: Block or sinkhole the identified C2 IP addresses and domains linked to recent Gootloader activity. Closely monitor outbound network connections over TCP/443 that do not conform to standard TLS handshakes, as the “Supper” backdoor uses encrypted but non-TLS communication over that port.

Hunting and Forensics: Review proxy and web logs for POST requests to */wp-comments-post.php, especially those followed by small ZIP downloads, which may indicate Gootloader payload delivery. Collect forensic artifacts from compromised systems, including Startup folder contents, %AppData% directories, registry Run keys, and memory dumps for evidence of persistence or lateral movement.

Credential Security: Assume potential credential theft on affected hosts. Enforce password resets for privileged and service accounts, enable MFA where possible, and monitor for new account creations or privilege escalations following an infection event.

User Awareness and Access Controls: Educate users about SEO-poisoning lures that promise business-related documents or templates from unfamiliar websites. Restrict execution of JavaScript files via Windows Script Host where not required, and apply least privilege principles to limit lateral movement opportunities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0007 Discovery
TA0005 Defense Evasion	TA0040 Impact	TA0010 Exfiltration	TA0009 Collection
TA0006 Credential Access	TA0008 Lateral Movement	TA0011 Command and Control	TA0043 Reconnaissance
T1490 Inhibit System Recovery	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1027.013 Encrypted/Encoded File
T1105 Ingress Tool Transfer	T1090 Proxy	T1021.006 Windows Remote Management	T1584 Compromise Infrastructure
T1190 Exploit Public-Facing Application	T1204 User Execution	T1027 Obfuscated Files or Information	T1059.001 PowerShell
T1021 Remote Services	T1113 Screen Capture	T1608 Stage Capabilities	T1608.006 SEO Poisoning
T1189 Drive-by Compromise	T1059.007 JavaScript	T1547.001 Registry Run Keys / Startup Folder	T1068 Exploitation for Privilege Escalation
T1547 Boot or Logon Autostart Execution	T1059 Command and Scripting Interpreter	T1140 Deobfuscate/Decode Files or Information	T1555 Credentials from Password Stores
T1036 Masquerading	T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1055 Process Injection
T1584.001 Domains	T1552 Unsecured Credentials	T1558.003 Kerberoasting	T1558 Steal or Forge Kerberos Tickets
T1095 Non-Application Layer Protocol			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2f056ce0657542da3e7e43fb815a8973c354624043f19ef134dff271db1741b3, b9a61652dffd2ab3ec3b7e95829759fc43665c27e9642d4b2d4d2f7287254034, cf44aa11a17b3dad61cae715f4ea27c0cbf80732a1a7a1c530a5c9d3d183482a, 39d980851be1e111c035e4db2589fa3d5f59a5bef7b7b3e36bff5435c78f7049, c2326db8acae0cf9c5fc734e01d6f6c1cd78473b27044955c5761ec7fd479964, ad88076fd75d80e963d07f03d7ae35d4e55bd49634baf92743eece19ec901e94, 7557d5fed880ee1e292aba464ffdc12021f9acbe0ee3a2313519ecd7f94ec5c4, 5ec9e926d4fb4237cf297d0d920cf0e9a5409f0226ee555bd8c89b97a659f4b0, 87cbe9a5e9da0dba04dbd8046b90dbd8ee531e99fd6b351eae1ae5df5aa67439
File Path	C:\Users\username\AppData\Roaming\ISIS Drivers\, C:\Users\username\AppData\Roaming\Nuance\ , C:\Users\username\AppData\Roaming\PFU\, C:\Users\username\AppData\Local\Oardwior\ , C:\Users\username\AppData\Roaming\myHUD, C:\Users\username\AppData\Roaming\Canon U.S.A.
IPv4	178[.]32[.]224[.]219 , 37[.]59[.]205[.]2 , 193[.]104[.]58[.]64, 103[.]253[.]42[.]91 , 91[.]236[.]230[.]134 , 213[.]232[.]236[.]138 , 146[.]19[.]49[.]177
URLs	hxxps[:]//spirits-station.fr/, hxxps[:]//www.us.registration.fcaministers.com/, hxxps[:]//motoz.com.au/, hxxps[:]//routinelynomadic.com/, hxxps[:]//www.wagenbaugrabs.ch/, hxxps[:]//studentspoint.org/, hxxps[:]//dailykhabrain.com.pk/,

TYPE	VALUE
URLs	hxxps[:]//myanimals.com/, hxxps[:]//www2.pelisyseries.net/, hxxps[:]//www.claritycontentservices.com/wp/ , hxxps[:]//patriotillumination.com/ , hxxps[:]//michaelcheney.com/ , hxxps[:]//allreleases.ru/ , hxxps[:]//cloudy.pk/ , hxxps[:]//eliskavaea.cz/ , hxxps[:]//r34porn.net/ , hxxps[:]//leadoo.com/ , hxxps[:]//ostmarketing.com/, hxxps[:]//egyptelite.com/ , hxxps[:]//restaurantchezhenri.ca/ , hxxps[:]//www1.zonewebmaster.eu/news/ , hxxps[:]//campfosterymca.com/ , hxxps[:]//idmpakistan.pk/ , hxxps[:]//themasterscraft.com/ , hxxps[:]//unica.md/ , hxxps[:]//cargoboard.de/ , hxxps[:]//www.supremesovietoflove.com/wp/ , hxxps[:]//buildacampervan.com/, hxxps[:]//www.minklinkaps.com/ , hxxps[:]//aradax.ir/ , hxxps[:]//medicit-y.ch/ , hxxps[:]//redronic.com/ , hxxps[:]//www.ferienhausdehaanmieten.de/ , hxxps[:]//gravityforms.ir/ , hxxps[:]//apprater.net/ , hxxps[:]//fotbalovavidea.cz/ , hxxps[:]//usma.ru/ , hxxps[:]//thetripschool.com/ , hxxps[:]//cortinaspraga.com/ , hxxp[:]//cookcountyjudges.org/ , hxxps[:]//x.fybw.org/ , hxxps[:]//jungutah.com/ , hxxps[:]//influenceimmo.com/ , hxxps[:]//tokyocheapo.com/ , hxxps[:]//espressonisten.de/ , hxxps[:]//tiresdoc.com/ , hxxps[:]//hotporntv.net/ , hxxps[:]//yourboxspring.nl/, hxxps[:]//filmcrewnepal.com/ ,

TYPE	VALUE
URLs	hxxps[:]//yoga-penzberg.de/ , hxxps[:]//sugarbeecrafts.com/ , hxxps[:]//www.worldwealthbuilders.com/ , hxxps[:]//lepolice.com/ , hxxps[:]//www.lovestu.com/ , hxxps[:]//bluehamham.com/ , hxxps[:]//vps3nter.ir/ , hxxps[:]//whiskymuseum.at/ , hxxps[:]//latimp.eu/, hxxps[:]//solidegypt.net/ , hxxps[:]//wessper.com/ , hxxps[:]//www.pathfindertravels.se/tickets/ , hxxps[:]//www.smithcoinc.biz/ , hxxps[:]//kollabmi.se/ , hxxps[:]//xxxmorritas.com/ , hxxps[:]//onsk.dk/ , hxxps[:]//villasaze.ir/ , hxxps[:]//blossomthemesdemo.com/ , hxxps[:]//headedforspace.com/

References

https://www.huntress.com/blog/gootloader-threat-detection-woff2-obfuscation

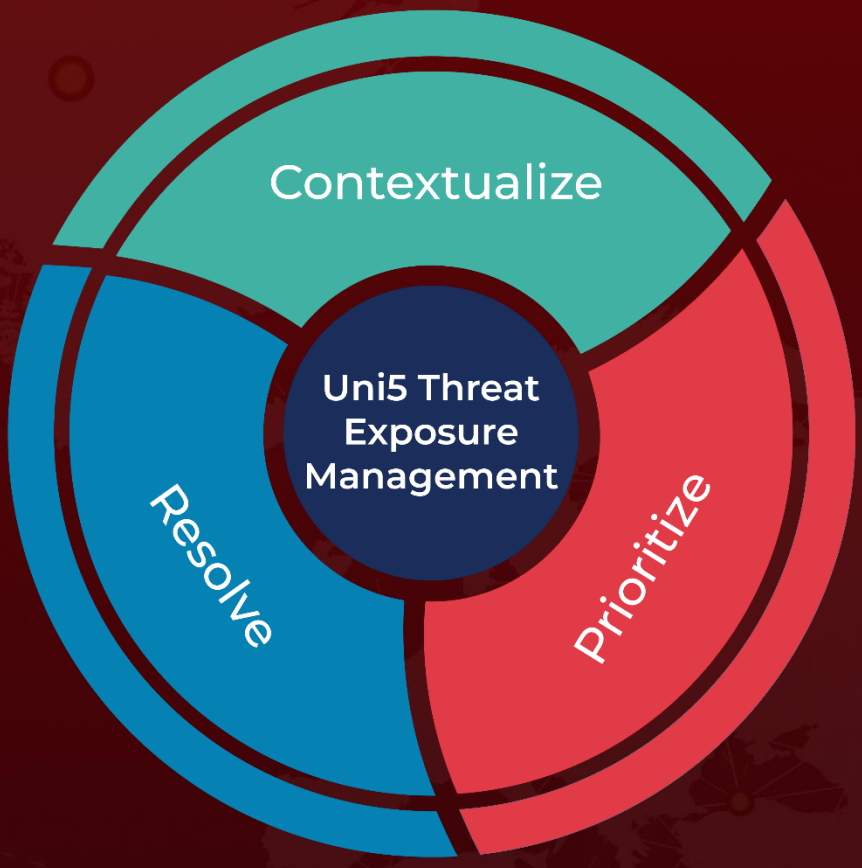
https://hivepro.com/threat-advisory/gootloaders-evolution-from-seo-poisoning-to-persistent-network-intrusions/

https://hivepro.com/threat-advisory/vanilla-tempest-targets-healthcare-with-inc-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

November 7, 2025 • 8:30 AM

More at www.hivepro.com