FBI FLASH
ACTIONABLE CYBER INTELLIGENCE
16 NOVEMBER 2026
FLASH Number
CC-111626-MW

Gootloader Malware Using SEO Poisoning and Compromised Websites to Gain Initial Access

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate identified tactics, techniques, and procedures (TTPs) related to Gootloader malware. Gootloader is an initial access framework that uses a JavaScript malware loader, compromised websites, and search engine optimization (SEO) techniques to infect organizations. Cyber actors used Gootloader as a ransomware precursor to attack victims across a wide variety of sectors. As of October 2026, the FBI identified over 1000 infected WordPress sites and 216 domains controlled by the Gootloader administrator, which led to over $28 million in ransomware payments. The FBI encourages organizations to contact the FBI if they have been compromised, and to implement the actions in the recommendations section to reduce the likelihood and impact of a compromise by Gootloader.

Threat

Between 2020 and 2026, the FBI observed cyber threat actors using Gootloader to obtain initial access to organizations through selected search phrases with low-ranking competition[1], such as a jurisdiction-specific contract clause[2]. Using SEO, threat actor-controlled pages would appear next to legitimate resources. The Gootloader administrator scanned WordPress sites looking for xlmrpc.php[3]. The administrator then later used compromised credentials to breach systems. Gootloader used a traffic distribution system (TDS) to filter content by country, referrer, cookie, or IP address.

Gootloader compromised WordPress sites, which then acted as lure pages, redirectors, traffic filters, or relay infrastructure. Hidden keyword links and arranged backlinks were used to increase lure visibility. The Gootloader administrator used stolen credentials to access vulnerable plugins and themes, injected posts, XML-RPC, REST routes, and modified JavaScript.

Gootloader SEO search terms consisted of targeting practicing attorneys, in-house counsel, law firm partners, litigation and privacy teams, legal operations professionals, general counsel, and legal technology decision makers inside law firms or legal departments.

[1] Search phrases that have a low search volume allowing for specific keywords targeted.
[2] Search phrases and results driven by jurisdiction-specific legal language.
[3] XML-RPC is a standard WordPress API endpoint frequently targeted by attackers for brute-forcing credentials.

FBI FLASH
ACTIONABLE CYBER INTELLIGENCE

Technical Details

Evolution of Gootloader

2020 to 2021	SEO-poisoned document searches; simulated forum pages; ZIP-delivered JavaScript; Windows Script Host execution.
2022 to 2024	Trojanized JavaScript libraries; AppData staging; use of PowerShell, scheduled tasks, and registry-resident payloads; continued use of SEO-poisoned searches.
2025 to 2026	Abuse of WordPress comment paths; geofencing and traffic distribution services; primary focus described as U.S. legal professionals and legal technology decision makers.

Related Threat Actors Abusing WordPress

Table 1. Related threat actors abusing WordPress and their outcome

Campaign	Scale and dates	How the site is used	Outcome for visitors
SocGholish (TA569), TA2726, Parrot TDS and other traffic brokers	Operation Endgame took down 106 servers and cleaned 14,971 WordPress sites (Jun 2026). From April to July 2026, there were 1,509 sites still active.	Injected JavaScript; fake plugin (platformist-quadendpointer) with a REST route /wp-json/<words>-<hex>/v1/<hex>; domain shadowing via hijacked DNS accounts	Fake browser update; follow-on loaders, RATs and ransomware (Evil Corp, LockBit, RansomHub)
StopAndProtect	Thousands of sites; found mid-May 2026	Hidden must-use plugins in wp-content/mu-plugins; concealed REST API upload endpoint with hard-coded credentials	ClickFix; SilentEncryptor ransomware, stealers, SMB/USB worms
"DoubleDonut" stealer operation	250+ sites in 12 countries	Remote script, inline script, or /wp-admin/admin-ajax[.]php?action=ajjs_run; skips visitors with admin cookies	ClickFix; Donut loader, then Vidar, Impure Stealer or VodkaStealer

Fake Cloudflare lure	Active since Dec 2025	Injected fake Cloudflare popup	In-memory shellcode; credential and crypto-wallet theft
ClearFake	Active Sep 2026	Base64 <script> tag on index pages; payload pulled from blockchain smart contracts (EtherHiding), so it changes without re-touching the site	ClickFix for Windows and macOS
DollyWay	20,000+ sites since 2016; 10,000+ active Feb 2025	Malicious and fake mu-plugins, WPCode snippets; hidden admin users with random hex names; reinfects on every page load	Redirects to scam pages

Windows Utility Tools

Table 2. Windows utility tools leveraged by Gootloader

Source	Event	Purpose
PowerShell	4103 and 4104; transcription where policy permits	Reveal Script Block creation, Invoke-Expression, AMSI patch strings, Assembly.Load, encoded loaders, and remote commands.
Windows Security	4624, 4648, 4688, 4697, 4769, 5140, 5145	Correlate network logons, explicit credentials, process creation, service creation, ticket requests, and admin share access.
System	7045	Detect transient remote service installation.
WMI Activity	5857 through 5861	Identify remote WMI providers, filters, and suspicious consumer or process behavior.
WinRM	Operational logs	Identify remote shell establishment and source or destination relationships.
Sysmon	1, 3, 7, 8, 10, 11, 13, 22	Process, network, image load, remote thread, process access, file, registry, and DNS visibility.
EDR	Memory, API, script, process lineage, network attribution	Detect hollowing, AMSI impairment, cross process writes, and in memory managed loads.

WordPress Technical Protection

Table 3. Windows technical protections and their implementations

Control	Implementation
Patching	Automatically update WordPress core and trusted plugins or themes where feasible; use virtual patching for emergency exposure.
Reduce attack surface	Remove unused plugins, themes, accounts, staging sites, and default components. Maintain a complete software inventory.
Protect administration	Require phishing-resistant Mulit-Factor Authentication (MFA) or strong MFA for administrators and hosting access; use SSO or VPN restrictions where practical.
Restrict XML-RPC	Disable xmlrpc.php if unused. If required, rate-limit and allow only necessary methods or trusted integrations; monitor authentication and POST volume.
Constrain PHP	Run PHP as a non-privileged account, make core files read-only where practical, and deny PHP execution under wp-content/uploads.
Use least privilege	Separate hosting accounts and sites, limit database permissions, protect wp-config.php, and prevent one site from writing another site's files.
Deploy WAF controls	Use managed rules, bot protection, login throttling, file-upload controls, and alerts for new REST endpoints or unusual admin-ajax actions.
Monitor integrity	Compare core files with official checksums and alert on unexpected plugin, theme, mu-plugin, JavaScript, .htaccess, and index-file changes.
Monitor search abuse	Review Search Console and webmaster tools for unrelated legal or business queries, sudden indexed pages, manual actions, and security warnings.
Centralize evidence	Retain web access, WAF, authentication, control-panel, SFTP or SSH, database, DNS, and outbound connection logs outside the web server.

Example of Hidden Keyword Links and Backlinks Used by Gootloader

String

**id=”aaeetce”>
<a href=”2022/12/13/zoning-government-definition/index.html”**

FBI FLASH
ACTIONABLE CYBER INTELLIGENCE

Keywords

- Zoning Government Definition
- York Region Police Requirements
- Wyoming Bule Sky Laws
- World No 1 Business Magazine
- Word Definition Solitude
- With Armour Legal
- Will Uk Abolish Inheritance Tax
- Why Should Legal Drinking Age Be 21
- Why is It agasint the Law to Drive without Shoes
- Why Can't the Cell Theory Become a Law
- Who Pays for legal Fees Election
- Who Is a Justice of the Supreme Court
- Who Branch Implements Laws
- Which Parent Will Get the Child Tax Credit
- Which of the Following Best Describes the Concept of Legal Jurisdiciton
- Which Command Is Used to change th eDefinition of a Table in Sql
- Where is My legal Point of Discharge
- Where can I Llegally Bet on the Super Bowl
- When Was Divorce Legalized in Korea
- When did Sports Betting Become Legal in Virginia

MITRE ATT&CK Mappings

Table 4. MITRE ATT&CK Mappings

ID	Technique	Tactic	Local evidence
T1059.001	PowerShell	Execution	Most payloads are PowerShell templates or commands.
T1027	Obfuscated Files or Information	Defense Evasion	Randomized names, string substitution, compressed or encoded payloads.
T1140	De-obfuscate or Decode Files or Information	Defense Evasion	Base64, gzip, raw deflate, and runtime reconstruction.
T1620	Reflective Code Loading	Defense Evasion	Assembly.Load executes managed payloads without a normal on disk assembly load.

T1562.001	Impair Defenses	Defense Evasion	Patches AmsiScanBuffer.
T1055	Process Injection	Defense Evasion	Writes into another process and creates a remote thread.
T1055.012	Process Hollowing	Defense Evasion	Replaces a suspended process image.
T1548.002	Bypass User Account Control	Privilege Escalation	Use a mock trusted directory and auto elevated executable.
T1574.002	DLL Side Loading	Persistence or Privilege Escalation	Dll is placed next to copied easinvoker.exe.
T1036.005 or T1036.006	Masquerading path or space	Defense Evasion	Mock C:\Windows trailing space path.
T1047	Windows Management Instrumentation	Execution	WMI process creation and access testing.
T1021.006	Windows Remote Management	Lateral Movement	Invoke-Command and TCP 5985 discovery.
T1021.002	SMB Windows Admin Shares	Lateral Movement	C$ staging and low-level SMB authentication.
T1569.002	Service Execution	Execution	Starts, and deletes remote services.
T1078	Valid Accounts	Defense Evasion or Lateral Movement	Supplied credentials are used with WinRM, WMI, and SMB.
T1550.002	Pass the Hash	Lateral Movement	NTLM hash is used directly for SMB authentication.
T1558.003	Kerberoasting	Credential Access	SPN discovery and service ticket extraction to $krb5tgs$ format.
T1003.002	Security Account Manager	Credential Access	Reg save of HKLM SAM and SYSTEM.
T1003.004	LSA Secrets	Credential Access	SECURITY hive is export.
T1087.002	Domain Account Discovery	Discovery	AD account and SPN enumeration.

T1069.002	Domain Groups Discovery	Discovery	Group and SID collection.
T1482	Domain Trust Discovery	Discovery	SharpHound
T1018	Remote System Discovery	Discovery	AD computer enumeration.
T1046	Network Service Discovery	Discovery	Tests 445 and 5985 across discovered computers.
T1057	Process Discovery	Discovery	Enumerate processes and owners.
T1082	System Information Discovery	Discovery	OS, product, architecture, and hostname collection.
T1016	System Network Configuration Discovery	Discovery	IP address and interface context.
T1033	System Owner User Discovery	Discovery	Current identity and process owner checks.
T1090.001	Internal Proxy	Command and control	Reverse multiplexed proxy provides pivoting.
T1071.001	Web Protocols	Command and control	HTTP and HTTPS GET and POST tasking.
T1573	Encrypted Channel	Command and control	Custom RC4 like and XOR proxy channel; web traffic may use TLS.
T1105	Ingress Tool Transfer	Command and control	Task content and bot code are transferred to endpoints.
T1041	Exfiltration Over C2 Channel	Exfiltration	Can send selected data through a configured transfer path.
T1567.002	Exfiltration to Cloud Storage	Exfiltration	Alternate upload uses bashupload.com.
T1106	Native API	Execution	Windows memory, thread, process, and section APIs are invoked.



T1070.004	File Deletion	Defense Evasion	Temporary scripts, services, and UAC artifacts are removed.
T1587.001	Develop Capabilities Malware	Resource Development	PHP builders generate customized implants. Applies to operator side capability.

Recommendations

The FBI recommends organizations take the steps below to improve their security posture in response to the evolving entities targeted in this scheme. FBI recommends organizations also establish and maintain strong liaison relationships with the FBI Field Office in their region. Through these partnerships, the FBI can assist with identifying vulnerabilities and mitigating potential threat activity. The FBI further recommends organizations review and, if needed, update incident response and communication plans that list actions an organization will take if impacted by a cyber incident.

The FBI recommends network defenders apply the following actions to mitigate initial unauthorized access and harden security against future malicious attempts and compromises:

Windows Detection and Response

If a suspicious archive was downloaded but not opened

- Do not extract or preview its contents. In an organization, submit the file through the approved internal security process.
- Record the download URL, search query, browser history time, filename.
- Delete the file only after the security team confirms evidence preservation is complete.
- If the JavaScript file was opened disconnect network access. Do not power off unless your incident-response procedure requires it.
- Use a separate known-clean device to change credentials after the security team scopes credential exposure. Do not change passwords from the suspected computer.
- Have responders collect endpoint memory when appropriate, process trees, scheduled tasks, autoruns, browser history, DNS, proxy records, and PowerShell logs.
- Reimage the endpoint when follow-on malware, credential theft, or persistence is confirmed. Removing only the downloaded file does not restore trust.

If the JavaScript file was opened

- Disconnect network access. Do not power off unless your incident-response procedure requires it.
- Use a separate known-clean device to change credentials after the security team scopes credential exposure. Do not change passwords from the suspected computer.

- Have responders collect endpoint memory when appropriate, process trees, scheduled tasks, autoruns, browser history, DNS, proxy records, and PowerShell logs.
- Reimage the endpoint when follow-on malware, credential theft, or persistence is confirmed. Removing only the downloaded file does not restore trust.

Windows prevention priorities

- Disable Windows Script Host where business applications do not require it, or control script execution with WDAC or AppLocker.
- Block unapproved scripts and executables from user-writable locations. Keep Microsoft Defender, SmartScreen, cloud protection, AMSI, and tamper protection enabled.
- Use standard user accounts, protected administrator workflows, browser download controls, attachment scanning, DNS filtering, and authenticated web proxy logging.
- Centralize PowerShell, Security, Sysmon or EDR, DNS, proxy, and firewall telemetry with enough retention to investigate delayed follow-on activity.

WordPress Response

Immediate response when compromise is suspected

- Place the site in a controlled maintenance state or restrict public access while preserving a forensic copy of files, database, logs, and hosting configuration.
- Reset hosting panel, SSH, SFTP, WordPress administrator, database, API, and CDN credentials from a clean system. Revoke active sessions and application passwords.
- Identify the initial access path. Restore from a known-clean backup only after removing the vulnerability or stolen credential that allowed entry.

Reporting Notice

The FBI encourages any suspected Gootloader intrusions to be reported to their local FBI field office at www.fbi.gov/contact-us/field-offices or 1-800-CALL-FBI (225-5324) or to the FBI Internet Crime Complaint Center at www.ic3.gov.

When available, each report should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Retain all information regarding the incident, including affected package names and versions, network logs, credentials or secrets potentially exposed, and any extortion communications or ransom demands.

When available, include the date and time the compromise was discovered, estimated date of initial infection, type of activity observed, systems and environments affected, name of the submitting company or organization, and designated point of contact.

Your organization has no obligation to provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, it must do so consistently with applicable state and federal law.

Administrative Note

The information in this document is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber actors. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by the FBI.

This FLASH was coordinated with DHS/CISA and is marked **TLP: CLEAR**.

