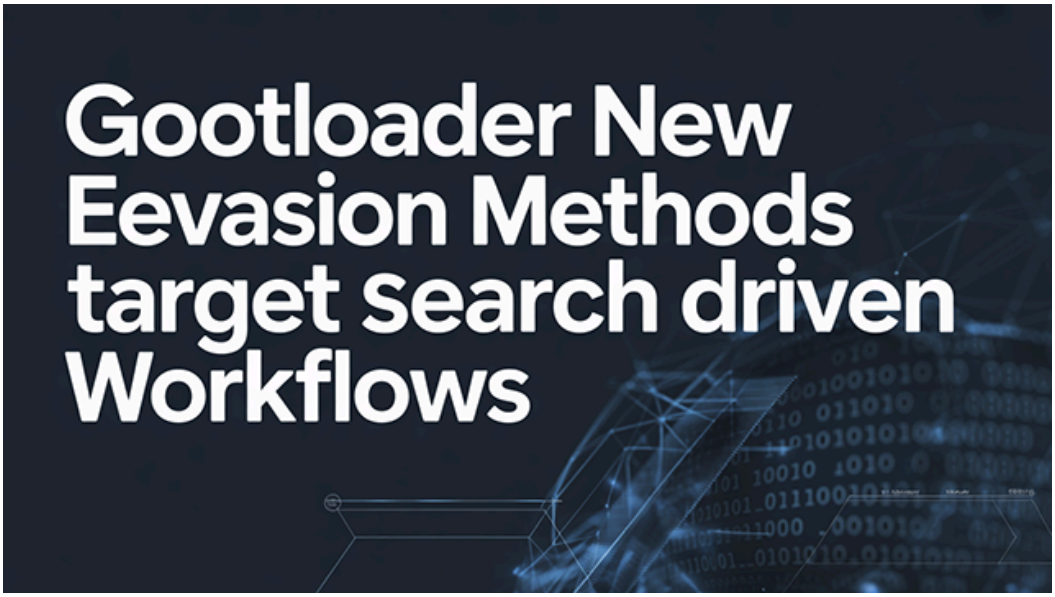
GootLoader New Evasion Methods Target Search Driven Workflows

cybersecsentinel.com/gootloader-new-evasion-methods-target-search-driven-workflows

Cybersec Sentinel November 6, 2025



Threat Group – UNC2565 (also tracked as Storm-0494)
Threat Type – Malware Loader and Initial Access Platform
Exploited Vulnerabilities – No specific CVE confirmed. Campaign relies on SEO poisoning, compromised WordPress sites, archive format inconsistencies, Windows Script Host execution, and legacy filename behaviour.
Malware Used – GootLoader, GootBot, secondary payloads such as Cobalt Strike Beacon, Gootkit, Osiris, SNOWCONE, and ransomware families associated with affiliates including Vanilla Tempest (DEV-0832) such as Rhysida, BlackCat, Zeppelin, and Quantum Locker.
Threat Score – 5.9 🟠 Elevated – justified by a novel ZIP evasion technique that delays detection, rapid post-execution reconnaissance, and monetisation through Access-as-a-Service affiliate sales.
Last Threat Observation – 6 November 2025

Overview

This advisory confirms a renewed and technically advanced resurgence in **GootLoader** operations throughout 2025. The threat actor **UNC2565 (Storm-0494)** continues to run a mature Access-as-a-Service (AaaS) platform, providing compromised systems to ransomware affiliates such as **Vanilla Tempest**.

The 2025 campaign introduces a **dual-personality ZIP archive** evasion mechanism that shows benign files to analysis tools while extracting a malicious **JScript payload** when opened in Windows Explorer. This technique enables the actor to evade detection and establish persistence within enterprise environments before defences can respond.

Key Details

Delivery Method

- SEO poisoning of legitimate WordPress websites to lure victims searching for business document templates.
- Download of a dual-personality ZIP archive designed to display harmless contents to sandboxes but extract a `.js` file to human users.
- User double-clicks the JScript file, launching **WScript.exe** or **CScript.exe** which executes an obfuscated JScript loader that spawns a PowerShell stage and retrieves the next payload.

Target

- Professional and business service sectors, including legal, accounting, and financial firms.
- Broader exposure across corporate users seeking contract or agreement templates online.
- Microsoft Windows environments connected to Active Directory domains.

Functions

- Executes via **Windows Script Host (WSH)**.
- Performs environment and analysis checks to evade sandboxes.
- Deploys payloads such as **Cobalt Strike**, **Gootkit**, or **custom implants** like **GootBot**.
- Establishes persistence using the **Startup folder** (replacing scheduled tasks).
- Enables rapid reconnaissance, lateral movement, and credential theft.

Obfuscation

- ZIP structure conflict between **Local File Header** and **Central Directory Record**, leading to alternate extraction results.
- Encoded and XOR-obfuscated PowerShell chains.
- Use of **WOFF2 font glyph substitution** and **Windows 8.3 short filenames** to disguise artifacts.
- Decentralised **WordPress-based C2** to resist bulk blocking.

High Level Findings and Campaign Validation

This campaign verifies the active development of **UNC2565** and its affiliates. The threat actor maintains a consistent financial motive through Access-as-a-Service.

The **dual-personality ZIP** evasion technique manipulates metadata so that Windows Explorer extracts a malicious `.js`, while common tools like 7-Zip or Python's `zipfile` extract a harmless decoy. The resulting discrepancy effectively **delays detection** long enough for the actor to achieve persistence and initiate reconnaissance.

Blocking **Windows Script Host execution** at the organisational level prevents this evasion from succeeding, making WSH controls the most critical defensive measure.

Time Criticality of the Threat

GootLoader operates on a compressed timeline. Once the malicious JScript executes:

Stage	Observed Timing
Initial Execution to Reconnaissance	Within 20 minutes
Lateral Movement Toward Domain Controller	Within 1 hour
Full Domain Controller Compromise	As fast as 17 hours

This rapid execution window underscores why **post-event file analysis is inadequate**. Automated containment and behavioural controls must activate within minutes to prevent network compromise.

Deep Dive – Infection Chain and Evasion Tactics

Technical Analysis of the Dual-Personality ZIP Evasion

The GootLoader archive embeds a conflict between ZIP metadata components:

Metadata Component	Function	Manipulation Purpose
Local File Header (LFH)	Defines file offset and compressed size	Set to valid values for malicious JScript extraction
Central Directory Record (CDR)	Global archive index	Set to conflicting benign values for sandbox evasion

Windows Explorer relies on LFH and extracts the `.js` payload.
Analysis tools typically rely on CDR and extract decoy files.

This asymmetry is deliberate and specifically targets automated security scanning.

Initial Execution via Windows Script Host

When the user double-clicks the `.js` payload:

```
WScript.exe "C:\Users\<user>\AppData\Local\Temp\Temp1_<filename>.zip\<document name>.js"
```

The JScript invokes **PowerShell** with encoded parameters, typically spawning secondary payloads such as **FONELAUNCH** or **Cobalt Strike**.

Detection choke points include:

- **WSH spawning PowerShell with -enc or -e flags**.
- **PowerShell network activity immediately post-execution**.
- **File creation in user Startup folders shortly after script launch**.

Ancillary Evasion

- **WOFF2 fonts** obscure filenames through glyph substitution.
- **8.3 short filenames** hinder forensic string-based analysis.

Post-Exploitation TTPs and Malware Stages

Persistence Mechanism Update (2025)
UNC2565 now favours the **user Startup folder** rather than scheduled tasks:
`%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\<shortname>.lnk`
This low-noise persistence method is less likely to trigger EDR telemetry.

GootBot Implant Analysis and Lateral Movement
GootBot is a lightweight PowerShell-based implant introduced to replace common tools like Cobalt Strike. It communicates through decentralised C2 channels hosted on compromised **WordPress xmlrpc.php endpoints**, often with unique SSL certificates.

Each implant communicates with a different endpoint, ensuring the campaign persists even if several domains are blocked. Commands are delivered as encrypted PowerShell scripts, executed using `Start-Job` for stealth.

GootBot performs:

- **Active Directory enumeration and Kerberoasting**.
- **Lateral movement via WinRM**.
- **Privilege escalation leading to domain dominance**.

Known Indicators of Compromise (IoCs)

Indicator Type	Indicator / Pattern	Description / Context	Confidence
File Path	`%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\<shortname>.lnk`	Persistence file using 8.3 short naming convention; replaces older scheduled tasks method	High
File Path	`%TEMP%\Temp1_*.zip\*.js`	Extracted JScript payload path after dual-personality ZIP extraction via Windows Explorer	High
Process	`wscript.exe` or `cscript.exe` spawning `powershell.exe` with `-enc` or `-e` flags	Core execution pattern for loader activity	High
Command Line	`cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "<path>"`	Self-deletion sequence used to erase temporary payloads	Medium-High
Network URL	`*/xmlrpc.php`	Common endpoint used by GootBot C2 infrastructure on compromised WordPress sites	High
Network Domain	Compromised or hijacked WordPress sites with legitimate SSL certificates	Decentralised and constantly rotated	High
Network Behaviour	Slow beaconing every 300–900 seconds with small encrypted HTTPS payloads	GootBot communication pattern	High
PowerShell Artefact	`Start-Job` usage in encrypted PowerShell sessions originating from WSH-spawned processes	Post-exploitation C2 execution	Medium-High
Historical Hash Reference	SHA256: `a79eaf53a4b42e80d9ecdb8b139e9dc812cedf063153da3f8a2b7a49bc7b81d4`	Known GootLoader JScript dropper variant (late 2024)	Medium

URLs

- hxxps://espressonisten[.]de
- hxxps://r34porn[.]net
- hxxps://www[.]lovestu[.]com
- hxxps://www[.]pathfindertravels[.]se/tickets/
- hxxps://www[.]smithcoinc[.]biz
- hxxps://www[.]supremesovietoflove[.]com/wp/
- hxxps://xxxmorritas[.]com
- hxxp://cookcountyjudges[.]org/
- hxxps://allreleases[.]ru
- hxxps://apprater[.]net
- hxxps://aradax[.]ir
- hxxps://blossomthemesdemo[.]com
- hxxps://bluehamham[.]com
- hxxps://buildacampervan[.]com
- hxxps://campfosterymca[.]com
- hxxps://cargoboard[.]de
- hxxps://cloudy[.]pk
- hxxps://cortinaspraga[.]com
- hxxps://dailykhabrain[.]com[.]pk
- hxxps://egyptelite[.]com
- hxxps://eliskavaea[.]cz
- hxxps://filmcrewnepal[.]com
- hxxps://fotbalovavidea[.]cz
- hxxps://gravityforms[.]ir
- hxxps://headedforspace[.]com
- hxxps://hotporntv[.]net
- hxxps://idmpakistan[.]pk
- hxxps://influenceimmo[.]com
- hxxps://jungutah[.]com
- hxxps://kollabmi[.]se
- hxxps://latimp[.]eu
- hxxps://leadoo[.]com
- hxxps://lepolice[.]com
- hxxps://medicit-y[.]ch
- hxxps://michaelcheney[.]com
- hxxps://motoz[.]com[.]au
- hxxps://myanimals[.]com
- hxxps://onsk[.]dk
- hxxps://ostmarketing[.]com
- hxxps://patriotillumination[.]com
- hxxps://redronic[.]com
- hxxps://restaurantchezhenri[.]ca
- hxxps://solidegypt[.]net
- hxxps://spirits-station[.]fr
- hxxps://studentspoint[.]org
- hxxps://sugarbeecrafts[.]com
- hxxps://themasterscraft[.]com
- hxxps://thetripschool[.]com
- hxxps://tiresdoc[.]com

- hxxps://unica[.]md
- hxxps://usma[.]ru
- hxxps://villasaze[.]ir
- hxxps://vps3nter[.]ir
- hxxps://wessper[.]com
- hxxps://whiskymuseum[.]at
- hxxps://www[.]claritycontentservices[.]com/wp/
- hxxps://www[.]ferienhausdehaanmieten[.]de
- hxxps://www[.]minklinkaps[.]com
- hxxps://www[.]us[.]registration[.]fcaministers[.]com
- hxxps://www[.]wagenbaugrabs[.]ch
- hxxps://www[.]worldwealthbuilders[.]com
- hxxps://www1[.]zonewebmaster[.]eu/news/
- hxxps://www2[.]pelisyseries[.]net
- hxxps://x[.]fybw[.]org
- hxxps://yoga-penzberg[.]de
- hxxps://yourboxspring[.]nl

Domains

- allreleases[.]ru
- apprater[.]net
- aradax[.]ir
- blossomthemesdemo[.]com
- bluehamham[.]com
- buildacampervan[.]com
- campfosterymca[.]com
- cargoboard[.]de
- cookcountyjudges[.]org
- cortinaspraga[.]com
- egyptelite[.]com
- eliskavaea[.]cz
- espressonisten[.]de
- filmcrewnepal[.]com
- fotbalovavidea[.]cz
- gravityforms[.]ir
- headedforspace[.]com
- hotporntv[.]net
- jungutah[.]com
- kollabmi[.]se
- medicit-y[.]ch
- michaelcheney[.]com
- motoz[.]com[.]au
- onsk[.]dk
- ostmarketing[.]com
- patriotillumination[.]com
- redronic[.]com
- restaurantchezhenri[.]ca
- solidegypt[.]net
- spirits-station[.]fr
- studentspoint[.]org

- themasterscraft[.]com
- thetripschool[.]com
- tiresdoc[.]com
- unica[.]md
- villasaze[.]ir
- vps3nter[.]ir
- whiskymuseum[.]at
- xxxmorritas[.]com
- yoga-penzberg[.]de
- yourboxspring[.]nl

Hostnames

- www[.]claritycontentservices[.]com
- www[.]ferienhausdehaanmieten[.]de
- www[.]lovestu[.]com
- www[.]minklinkaps[.]com
- www[.]pathfindertravels[.]se
- www[.]smithcoinc[.]biz
- www[.]supremesovietoflove[.]com
- www[.]us[.]registration[.]fcaministers[.]com
- www[.]wagenbaugrabs[.]ch
- www[.]worldwealthbuilders[.]com
- www1[.]zonewebmaster[.]eu
- www2[.]pelisyseries[.]net
- x[.]fybw[.]org

IPv4 Addresses

- 103[.]253[.]42[.]91
- 146[.]19[.]49[.]177
- 178[.]32[.]224[.]219
- 193[.]104[.]58[.]64
- 213[.]232[.]236[.]138
- 37[.]59[.]205[.]2
- 91[.]236[.]230[.]134

File Hashes (SHA256)

- 2f056ce0657542da3e7e43fb815a8973c354624043f19ef134dff271db1741b3
- 5ec9e926d4fb4237cf297d0d920cf0e9a5409f0226ee555bd8c89b97a659f4b0
- 7557d5fed880ee1e292aba464ffdc12021f9acbe0ee3a2313519ecd7f94ec5c4
- 87cbe9a5e9da0dba04dbd8046b90dbd8ee531e99fd6b351eae1ae5df5aa67439
- ad88076fd75d80e963d07f03d7ae35d4e55bd49634baf92743eece19ec901e94
- b9a61652dffd2ab3ec3b7e95829759fc43665c27e9642d4b2d4d2f7287254034
- c2326db8acae0cf9c5fc734e01d6f6c1cd78473b27044955c5761ec7fd479964
- c2b9782c55f75bb1797cb4fbae0290b44d0fcad51bf4f2c11c52ebbe3526d2ac
- cf44aa11a17b3dad61cae715f4ea27c0cbf80732a1a7a1c530a5c9d3d183482a

Mitigation and Prevention

Mitigation Checklist (for Gap Analysis)

Control Area	Recommended Actions
Windows Script Host Control	Disable WSH via Group Policy or Registry, or redirect script extensions (.js, .vbs, etc.) to Notepad to prevent execution.
Attack Surface Reduction (ASR)	Enforce ASR rule GUID `d3e037e1-3eb8-44c8-a917-57927947596d` in Block mode to stop WSH-spawned scripts from launching executables.
PowerShell Hardening	Enable Constrained Language Mode for users, enable Script Block Logging, and alert on `Start-Job` misuse.
Endpoint Detection and Response	Detect and alert on WSH spawning PowerShell, PowerShell executing encoded commands, and Startup folder modifications.
Network Defence	Monitor for HTTP(S) to `xmlrpc.php` on uncommon WordPress domains; block or sandbox suspicious traffic.
User Awareness	Educate users about the risk of downloading document templates from search results; enforce policy to source templates internally.

Risk Assessment

The GootLoader 2025 campaign is rated **Elevated (5.9)**. While it requires user execution and does not exploit zero-day vulnerabilities, its effectiveness comes from:

- Advanced **metadata-based evasion**,
- Rapid post-execution activity (minutes to compromise),
- Integration into ransomware affiliate ecosystems, and
- Adoption of custom tools like **GootBot**.

Organisations relying on legacy antivirus or delayed manual analysis are most at risk. Enterprises enforcing **WSH and ASR hardening** and maintaining **rapid containment playbooks** will mitigate the threat effectively.

Conclusion

The 2025 **GootLoader** resurgence highlights an actor capable of bypassing traditional scanning and analysis through engineered evasion. By exploiting ZIP metadata conflicts, GootLoader gains crucial operational time to establish persistence and deploy **GootBot**, facilitating decentralised C2 and stealthy post-exploitation.

Key Recommendations:

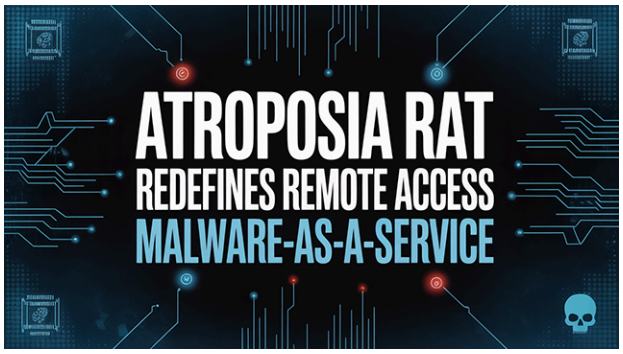
- **Disable or restrict WSH** execution through policy or file association controls.
- **Deploy ASR rules** to block script-based execution chains.
- **Implement high-fidelity behavioural detections** for WSH → PowerShell → Startup persistence.
- **Automate incident response** to achieve host isolation and credential rotation within minutes.

Failure to act within the 17-hour compromise window leaves organisations exposed to ransomware or data theft initiated via purchased access.

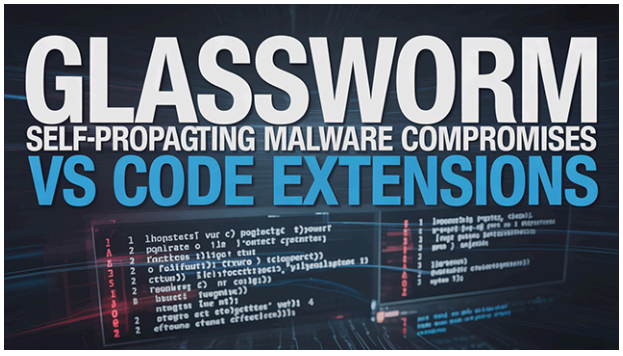
Sources

- **Mandiant | Google Cloud Blog** – *Tracking the Evolution of GootLoader Operations* – https://cloud.google.com/blog/topics/threat-intelligence/tracking-evolution-gootloader-operations
- **Red Canary** – *The Goot Cause Detecting GootLoader and Its Follow-On Activity* – https://redcanary.com/blog/threat-intelligence/gootloader

- **Darktrace** – *Detecting and Containing GootLoader Malware* – https://www.darktrace.com/blog/gootloader-malware-detecting-and-containing-multi-functional-threats-with-darktrace
- **IBM X-Force** – *GootBot GootLoader's New Approach to Post-Exploitation* – https://www.ibm.com/think/x-force/gootbot-gootloaders-new-approach-to-post-exploitation
- **GBHackers** – *Hackers Use SEO Techniques to Push GootLoader Malware via Google* – https://gbhackers.com/gootloader-malware-via-google
- OTX AlienVault - Indicators of Compromise - https://otx.alienvault.com/pulse/690cadc6a4a3c3370cc2e697



Threat Group – Unknown actor likely a financially motivated Malware as a Service operator Threat Type – Remote Access Trojan and Malware as a Service Exploited Vulnerabilities – No specific CVEs publicly linked at time of writing. Built in UAC bypass and a Local Vulnerability Scanner enable dynamic post infection exploitation Malware Used



Threat Group – Unknown (no confirmed attribution) Threat Type – Self-propagating software supply chain malware targeting VS Code and OpenVSX ecosystems Exploited Vulnerabilities – Abuse of trusted publisher credentials and the automated extension update pipeline; no CVE assigned for the platform itself Malware Used – GlassWorm loader and final-stage ZOMBI module (RAT with SOCKS

Threat Group – Highly sophisticated nation state actor Threat Type – Data breach and supply chain compromise Exploited Vulnerabilities – Initial access vector undisclosed. CVE 2025 54500 is a separate HTTP2 data plane denial of service flaw, not the entry point for the breach. Malware Used – Not publicly disclosed Threat Score – 🔴 7.5