11 December 2025

TLP: WHITE

INTEL471

EMERGING THREATS

Gootloader Malware - Update

UPDATE 12/08/2025: In October 2025, Gootloader resurfaced with enhanced capabilities, building on the multi-stage loader malware first seen in 2020. These capabilities include methods of initial access incorporating SEO (Search Engine Optimization) poisoning via law related decoys, and modified ZIP archive extraction methods to conceal itself. Additionally, newer persistence techniques and deployment of more unique malicious tooling has been observed by researchers as well.

THREAT SUMMARY

UPDATE 12/08/2025: In October 2025, Gootloader resurfaced with enhanced capabilities, building on the multi-stage loader malware first seen in 2020. These capabilities include methods of initial access incorporating SEO (Search Engine Optimization) poisoning via law related decoys, and modified ZIP archive extraction methods to conceal itself. Additionally, newer persistence techniques and deployment of more unique malicious tooling has been observed by researchers as well.

The GootLoader malware variant is identified as a downloader, and is used to facilitate the pathway to the next stage(s) of infection. Seen in the wild since late 2020, the variant is known to infect victims' systems via SEO (Search Engine Optimization) poisoning - which is a type of malicious advertising technique that threat actors use to put malicious websites near the top of search results. As referenced in the extensive analysis done by researchers at Intel 471, this technique can be used to target specific individuals as well, with the threat actors knowing information about who they are targeting and crafting the results accordingly. GootLoader is known as a delivery mechanism for other second stage malware variants such as Gootkit and tools such as SystemBC and SharpHound. Due to GootLoader's stealthiness, effectiveness and its exploitation in the wild by a number of ransomware campaigns, it is important that teams assess and prepare for this loader's capabilities.

TITAN References:

- Titan Malware Campaign Report: https://titan.intel471.com/report/fintel/48f86795369858d923a6fa26c9ea4ef9
- Titan Malware Report: https://titan.intel471.com/report/malrep/7a662b69267fefda9f77e90bcd7147c9
- Titan Malware Profile: https://titan.intel471.com/malware/1195d06fcea9e1f026fb5332871556ef
- Titan Malware Campaign Report: Gootloader malware returns with updates: https://titan.intel471.com/report/fintel/0d349e091f9985c1c97a21fb807e653a

SYNOPSIS

In late 2020, the GootLoader malware variant was observed in the wild and seen to drop the information stealing malware dubbed “GootKit” - however, since then the malware has evolved and has been utilized with a larger diversity of malicious payloads. Utilizing Intel 471's reliable and timely threat intelligence it has been observed to be associated with infection chains containing tools such as Cobalt Strike, SystemBC, and SharpHound; initiating multi-phased infections that can lead to serious threats like Ransomware. At the outset, GootLoader employs compromised WordPress websites as malware landing pages - often utilizing SEO (Search Engine Optimization) poisoning techniques in order to direct potential victims to these compromised websites and ultimately downloading a zip file containing the first-stage JavaScript and PowerShell script file(s) leading to infection.

After initial access is achieved and the .zip file is unzipped and executed, a script attempts to reach out and connect to Command and Control domains utilizing obfuscated PowerShell scripts. Prior to this phase, it is worthy to note that GootLoader has been observed to create scheduled tasks and registry keys for persistence. Once the connection to the C2 is successful and validated by the server as well, the server transmits the necessary component that allows the attacker(s) to load the next stage of infection - such as tools for lateral movement or privilege escalation (Cobalt Strike), reconnaissance (Bloodhound), or even ransomware payloads.

GOOTLOADER MALWARE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('9cb6b330-c7e8-4b1f-8b2e-7750c1c07390'),touched:!t)

RELATED HUNT PACKAGES

Suspicious Scheduled Task Created - Execution Details Contains Scripting Reference

https://hunter.cyborgsecurity.io/research/hunt-package/9a4fa42f-57dd-4449-b0c0-a1dd0976b17a

JS and LNK File Written in Short Period in Same Folder - Potential Malware Installation

https://hunter.cyborgsecurity.io/research/hunt-package/44D88C4F-6F06-4D2C-918F-073A30029912

LNK File Created in Startup Folder - Potential Indirect Malware Execution

https://hunter.cyborgsecurity.io/research/hunt-package/abe99d8c-522c-4fe0-8377-07a51313c063

Rundll32 Run Without Arguments

https://hunter.cyborgsecurity.io/research/hunt-package/f4e1ba57-3c1f-44ce-a320-f3e61a7ed389

Suspicious Scheduled Task Create/Update - Unusual Task Command and Arguments

https://hunter.cyborgsecurity.io/research/hunt-package/b858f30e-a0a4-4cf0-9b85-f9b9a2ed0eef

LNK Created in Startup Folder by Script Interpreter - Potential Script Loader Persistence

https://hunter.cyborgsecurity.io/research/hunt-package/F9745B88-F707-4512-91A6-B24B621D2F81

File Created In Startup Folder

https://hunter.cyborgsecurity.io/research/hunt-package/8fedb48c-396b-4cd5-9483-69d7fc3eecee

Scheduled Task Executing from Abnormal Location

https://hunter.cyborgsecurity.io/research/hunt-package/09a380b3-45e5-408c-b14c-3787fa48d783

WScript Executing File From Zip - Potential Loader Execution

https://hunter.cyborgsecurity.io/research/hunt-package/c669b475-5fa4-4c9d-a3a9-6b8afc4f12f1

Wscript Spawning Suspicious Processes - Potential Script Loaders

https://hunter.cyborgsecurity.io/research/hunt-package/95DA5101-3589-4B54-A484-1B2F99336CEF

MITRE CONTEXT

- MITRE Tactic Names:
  - Defense Evasion
  - Persistence
  - Execution
  - Privilege Escalation
- MITRE Technique Names:
  - Scheduled Task
  - Registry Run Keys / Startup Folder
  - Visual Basic
  - System Binary Proxy Execution
  - Windows Command Shell
  - JavaScript
  - Shortcut Modification
  - Malicious File
  - Rundll32
  - PowerShell
- MITRE Technique IDs:
  - T1218
  - T1059.003
  - T1218.011
  - T1059.007,
  - T1059.001
  - T1547.001
  - T1053.005
  - T1059.005
  - T1547.009
  - T1204.002
- Exploitation Vulnerabilities:
  - CVE-2021-1675
  - CVE-2021-34527

REFERENCES

1. https://redcanary.com/threat-detection-report/threats/gootloader/
2. https://www.attackiq.com/2024/01/17/gootloader-unloaded/
3. https://www.huntress.com/blog/gootloader-threat-detection-woff2-obfuscation