HUNTER

EMERGING THREATS

GOOTLOADER MALWARE

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. 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**â€™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 loaderâ€™s capabilities.

THREAT SUMMARY

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. 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**â€™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 loaderâ€™s capabilities.

SYNOPSIS

In late 2020, the **GootLoader** malware variant was observed in the wild and seen to drop the information stealing malware dubbed â€œGootKitâ€ - however, since then the malware has evolved and has been utilized with a larger diversity of malicious payloads. Utilizing [Intel 471](https://intel471.com/)'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.

HUNT PACKAGES

SUSPICIOUS SCHEDULED TASK CREATED – EXECUTION DETAILS CONTAINS SCRIPTING REFERENCE
https://hunter.cyborgsecurity.io/research/hunt-package/9a4fa42f-57dd-4449-b0c0-a1dd0976b17a

SUSPICIOUS SCHEDULED TASK CREATE/UPDATE – UNUSUAL TASK COMMAND AND ARGUMENTS
https://hunter.cyborgsecurity.io/research/hunt-package/b858f30e-a0a4-4cf0-9b85-f9b9a2ed0eef

SCHEDULED TASK WITH ABNORMAL LOCATION IN DETAILS
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

RELATED LINKS
Sign up for free HUNTER access
GootLoader Malware Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Execution
  - Persistence
- Technique Names:
  - Scheduled Task
  - Malicious File
- Threat Names:
  - GootLoader

REFERENCES

1. https://redcanary.com/threat-detection-report/threats/gootloader/
2. https://www.attackiq.com/2024/01/17/gootloader-unloaded/
3. https://titan.intel471.com/malware/1195d06fcea9e1f026fb5332871556ef
4. https://titan.intel471.com/report/fintel/48f86795369858d923a6fa26c9ea4ef9