New Gootloader Variant “GootBot” Changes the Game in Malware Tactics

socradar.io/new-gootloader-variant-gootbot-changes-the-game-in-malware-tactics/

November 7, 2023

Researchers recently identified a fresh Gootloader malware variant known as “GootBot,” used in SEO poisoning attacks. This variant introduces features that enable threat actors to move laterally within infected systems, and make it challenging for organizations to detect or block.

Gootloader has predominantly served as an initial access provider, with certain infections leading to ransomware incidents. The evolution of Gootloader malware, aimed at enhancing stealth and evading detection, coupled with the potential for ransomware attacks, raises significant concerns.

GootBot’s emergence signifies a significant shift in the malware’s **post-infection** tactics, and in this context, comprehending their evolving tactics and tools is imperative for mitigating the risks associated with post-exploitation activities.

How Does GootBot Enhance the Capabilities of Gootloader?

The Gootloader group, also known as **UNC2565 or Hive0127**, has historically employed techniques like SEO poisoning and compromised WordPress websites. Although active since 2014, the group expanded its tactics in 2022 by disseminating new secondary payloads such as Cobalt Strike, IcedID, and SystemBC in their attacks.

With the latest development, Gootloader introduces GootBot, which provides efficient means to infiltrate networks and deploy additional payloads. This approach aims to elude detection by steering clear of commonly identified off-the-shelf tools like CobaltStrike or RDP for Command and Control (C2).

Researchers identified the new variant in campaigns employing **SEO poisoning attacks**. These campaigns exploit search engine algorithms using keywords related to contracts, legal forms, and business documents, luring victims to seemingly legitimate websites where they unwittingly download the initial payload.

After infection, GootBot implants are disseminated widely throughout the corporate network. Each implant connects to a distinct hardcoded C2 server, often hosted on compromised WordPress sites, rendering detection and blocking more challenging. Furthermore, researchers note that GootBot currently maintains an undetected status on VirusTotal.

How Does a Gootloader Infection Work? How Does It Employ GootBot?

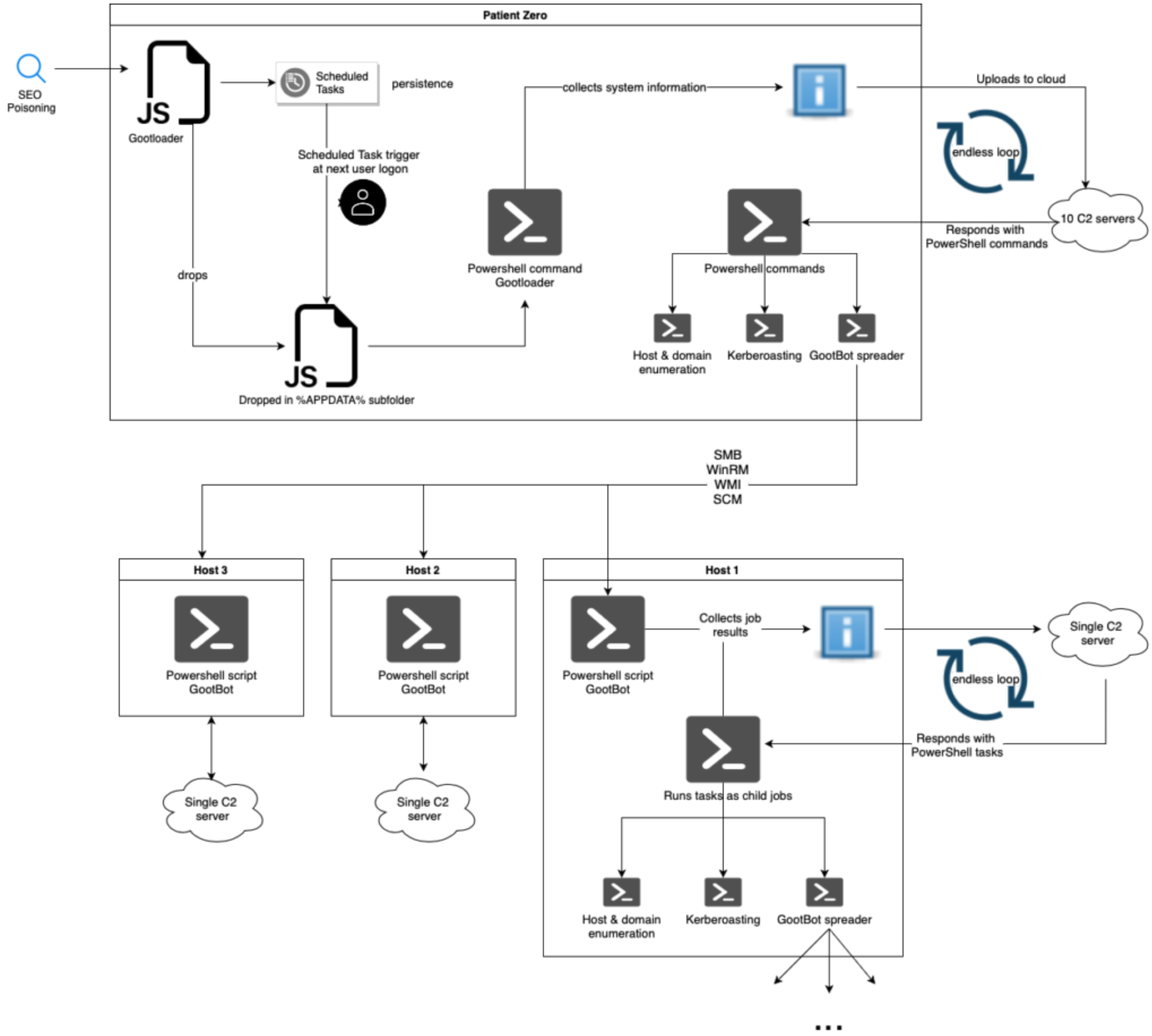
IBM’s X-Force has examined the stages of Gootloader malware infection and its latest variant, GootBot. Here is an overview of the researchers’ findings:

Gootloader Infections

Gootloader initiates infections when a user downloads an infected archive, containing a heavily obfuscated JavaScript file, which is Gootloader’s first stage. This JavaScript file drops another file in a selected subfolder under the %AppData% folder with an inconspicuous English filename.

Rather than running the second stage directly, Gootloader triggers a scheduled task for execution and persistence. When the second stage JavaScript runs, it executes a PowerShell script and the third stage, which collects system information and uploads it to one of its 10 hardcoded C2 servers. Gootloader uses hacked WordPress sites for its C2 servers, leading to URLs ending with **“/xmlrpc.php”**.

The User-Agent remains consistent, as does the presumed malware ID, **3B47772CE3**. The malware anticipates the C2’s response to contain a PowerShell script for execution. The third stage PowerShell script runs in an endless loop, enabling the actor to receive various PowerShell payloads from the C2.



How does Gootloader employ GootBot? (Source: IBM)

Introduction to GootBot

The GootBot payload is the new Gootloader variant that functions as a lightweight PowerShell script. GootBot only contains a single C2 server address, and features strings that are slightly obfuscated using a replacement key.

Similar to Gootloader, GootBot sends a GET request to its C2 server, requesting PowerShell tasks. In response, it expects a string with a Base64-encoded payload, with the task name encoded in the last 8 characters. GootBot decodes the payload, injects it into a simple scriptblock, and runs it in a background job using the “Start-Job” Cmdlet. This asynchronous execution reduces EDR detections, as there is no generated child processes.

GootBot beacons out every 60 seconds, with settings changeable through specific strings. The working directory path can also be modified with a signal string. After receiving tasks from the C2, GootBot queries task results and returns completed job results or specific strings for jobs that are not completed ("E1" or "E2").

Post-Infection

GootBot's lateral movement capabilities allow it to spread within the environment. Infected hosts receive scripts that enumerate the host and domain, with various techniques used to distribute the GootBot payload to other hosts. GootBots' C2 infrastructure rapidly generates various GootBot payloads, each with distinct C2 contact addresses. Lateral-movement scripts automate their deployment, potentially resulting in **host reinfections**.

Lateral-movement scripts employ WinRM in PowerShell. Other examples include copying payloads via SMB, and using WinAPI calls for creating remote services and scheduled tasks. In some cases, GootBot uses exfiltrated credentials for spreading.

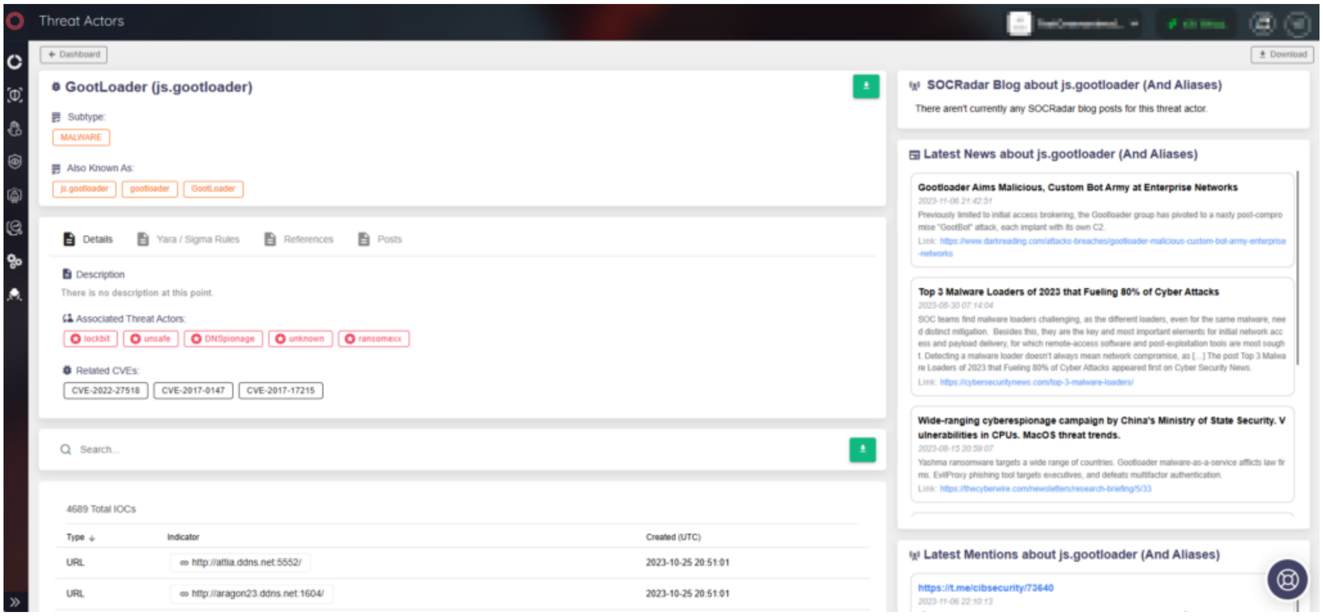
Additionally, GootBot employs environment variables to store encrypted strings, reducing script size. It may also use a technique to spoof PowerShell process arguments by creating a new process before writing the malicious script to the process's standard input.

GootBot conducts a reconnaissance script as one of its initial tasks, which includes the unique GootBot ID for the host. It collects domain user names, OS information, architecture details, domain controller information, running processes, SIDs, local IP addresses, hostnames, and formats the data with the specified ID.

Stay Ahead of Threat Actors with SOCRadar XTI

SOCRadar XTI leverages automated data collection, classification, and AI-driven analysis across a wide spectrum of sources spanning the surface, deep, and dark web. This comprehensive approach ensures that our Threat Actor & Malware panel remains continuously updated, providing you with the most current information regarding threat actors and malware.

The SOCRadar platform offers extensive details on GootLoader, including threat actors who have utilized its services, related vulnerabilities, and indicators of compromise (IoCs). These details are continuously refreshed and kept up to date.



GootLoader (js.gootloader)

Subtype:
MALWARE

Also Known As:
js.gootloader | gootloader | GootLoader

Description
There is no description at this point.

Associated Threat Actors:
lockbit | unsafe | DNSpionage | unknown | ransomexx

Related CVEs:
CVE-2022-27518 | CVE-2017-0147 | CVE-2017-17215

4689 Total IOCs

Type	Indicator	Created (UTC)
URL	http://attia.ddns.net:5552/	2023-10-25 20:51:01
URL	http://aragon23.ddns.net:1604/	2023-10-25 20:51:01

SOCRadar Blog about js.gootloader (And Aliases)
There aren't currently any SOCRadar blog posts for this threat actor.

Latest News about js.gootloader (And Aliases)

Gootloader Aims Malicious, Custom Bot Army at Enterprise Networks
2023-11-06 21:42:51
Previously limited to initial access brokering, the Gootloader group has pivoted to a nasty post-compromise "GootBot" attack, each implant with its own C2.
Link: https://www.darkreading.com/attacks-breaches/gootloader-malicious-custom-bot-army-enterprise-networks

Top 3 Malware Loaders of 2023 that Fueling 80% of Cyber Attacks
2023-08-30 07:14:04
SOC teams find malware loaders challenging, as the different loaders, even for the same malware, need distinct mitigation. Besides this, they are the key and most important elements for initial network access and payload delivery, for which remote-access software and post-exploitation tools are most sought. Detecting a malware loader doesn't always mean network compromise, as […] The post Top 3 Malware Loaders of 2023 that Fueling 80% of Cyber Attacks appeared first on Cyber Security News.
Link: https://cybersecuritynews.com/top-3-malware-loaders/

Wide-ranging cyberespionage campaign by China's Ministry of State Security. Vulnerabilities in CPUs. MacOS threat trends.
2023-08-15 20:59:07
Yashma ransomware targets a wide range of countries. Gootloader malware-as-a-service afflicts law firms. EvilProxy phishing tool targets executives, and defeats multifactor authentication.
Link: https://thecyberwire.com/newsletters/research-briefing/5/33

Latest Mentions about js.gootloader (And Aliases)

https://t.me/cibsecurity/73640
2023-11-06 22:10:13

Details of Gootloader (SOCRadar)

Equipped with the insights available on the SOCRadar platform, you can craft more effective use cases for the detection and prevention of malicious activities. This proactive approach empowers you to safeguard your organization against potential threats.

Recommendations to Avoid/Detect Gootloader Infections

Researchers advise security teams to enable script block logging within their environments and maintain vigilant monitoring of relevant Windows event logs, scheduled tasks, and network traffic to identify any signs of compromise.

Further recommendations are listed below:

- Closely scrutinize the execution of JavaScript files within downloaded ZIP archives to detect potential threats.
- Thoroughly examine network traffic for any suspicious HTTP requests, particularly those ending with **“xmlrpc.php”**.
- Keep an eye out for unusual cookie values (**<BOT_ID>=<If user is admin: 0/1>**) and content formats (**<BOT_ID>=[sX<<random_int>><packet_seq_number>]<data>**).
- Proactively monitor and identify lateral movement within your environment, utilizing various techniques like WinRM, WMI, or SCM.
- Assess the usage of the “Start-Job” Cmdlet and consider disabling or monitoring it to prevent malicious activities.

Indicators of Compromise (IoCs) Related to Gootloader

Mandiant has previously published a blog post outlining Gootloader’s operations, which included a set of Indicators of Compromise (IoCs). See them below:

ZIP File:

- 1011b2cbe016d86c7849592a76b72853
- 80a79d0c9cbc3c5188b7a247907e7264
- bee08c4481babb4c0ac6b6bb1d03658e

JS File:

- 82607b68e061abb1d94f33a2e06b0d20
- 961cd55b17485bfc8b17881d4a643ad8
- af9b021a1e339841cfdf65596408862d
- d3787939a5681cb6d6ac7c42cd9250b5
- ea2271179e75b652cafd8648b698c6f9
- ab1171752af289e9f85a918845859848

Registry Payload 1:

- FONELAUNCH.FAX
  d6220ca85c44e2012f76193b38881185
- FONELAUNCH.PHONE
  - 35238d2a4626e7a1b89b13042f9390e9
  - 53c213b090784a0d413cb00c27af6100
  - 7352c70b2f427ef4ff58128a428871d3
  - a0b7da124962b334f6c788c27beb46e3
  - a4ee41bd81dc3b842ddb2952d01f14ed
  - d401dc350aff1e3fd4cc483238208b43
  - ec17564ac3e10530f11a455a475f9763
  - f9365bf8d4b021a873eb206ec98453d9
  - aec78c1ef489f3f4b621037113cbdf81
- FONELAUNCH.DIALTONE
  - 08fa99c70e90282d6bead3bb25c358dc
  - aef6d31b3249218d24a7f3682a00aa10

Registry Payload 2:

- Cobalt Strike BEACON
  - 04746416d5767197f6ce02e894affcc7
  - 2eede45eb1fe65a95aefa45811904824
  - 3d768691d5cb4ae8943d8e57ea83cac1
  - 84f313426047112bce498aad97778d38
  - 92a271eb76a0db06c94688940bc4442b
- SNOWCONE
  - 328b032c5b1d8ad5cf57538a04fb02f2
  - 7a1369922cfb6d00df5f8dd33ffb9991

Network Indicators:

- jonathanbartz[.]com
- jp[.]imonitorsoft[.]com
- junk-bros[.]com
- kakiosk[.]adsparkdev[.]com
- kepw[.]org
- kristinee[.]com
- lakeside-fishandchips[.]com

Cobalt Strike Beacon Backdoor:

- hxxps://108.61.242[.]65/dot.gif
- hxxps://108.61.242[.]65/submit.php
- hxxps://146.70.78[.]43/fwlink
- hxxps://146.70.78[.]43/submit.php
- hxxps://87.120.254[.]39/ga.js
- hxxps://87.120.254[.]39/submit.php
- hxxps://45.150.108[.]213/ptj
- hxxps://45.150.108[.]213/submit.php
- hxxps://92.204.160[.]240/load
- hxxps://92.204.160[.]240/submit.php