THREAT ALERT: GootLoader - SEO Poisoning and Large Payloads Leading to Compromise

By Cybereason Incident Response Team

Archived: 2026-04-05 15:14:11 UTC

Cybereason issues Threat Alerts to inform customers of emerging impacting threats. The Cybereason Incident Response (IR) team documented such critical attack scenarios, which started from a GootLoader infection to ultimately deploy more capabilities. Cybereason Threat Alerts summarize these threats and provide practical recommendations for protecting against them.

KEY DETAILS

- **GootLoader has security evasion in mind:** Cybereason IR team observed payloads with large sizes (40MB and more) and masquerading with legitimate JavaScript code to evade security mechanisms.
- **Aggressive threat actor**: The threat actor displayed fast-moving behaviors, quickly heading to control the network it infected and getting elevated privileges in less than 4 hours.
- **Deployment of additional C2 frameworks**: Cybereason IR team observed post-infection frameworks being deployed: Cobalt Strike and SystemBC, which is usually leveraged for data exfiltration.
- **SEO Poisoning techniques used:** Cybereason's IR team discovered SEO Poisoning techniques used to spread malware. It works when the threat actors create fraudulent websites. Threat actors optimize fraudulent websites to appear higher in search engine results. The higher the search engine results, the more likely victims will click the links.
- **Post-exploitation activities detected by Cybereason**: Cybereason Defense Platform generates detections upon these infections and post-exploitation actions.
- **Severe Threat:** Cybereason's IR team assesses the threat level as SEVERE given the potential of the attacks.
- **Targeting English-Speaking Countries:** GootLoader targets companies in English-speaking countries, primarily including the United States, United Kingdom, and Australia.
- **Target Industries Including Healthcare and Finance:** Targeted attacks have been more prominent against healthcare and finance organizations.

WHAT'S HAPPENING?

In December 2022, the Cybereason Incident Response (IR) team investigated an incident that involved new deployment methods of GootLoader, observed recently in other cases.

The following observation was made regarding the infection methods used:

- Hosting of the infection payload on a compromised WordPress website, acting as a water hole and leveraging Search Engine Optimization (SEO) (MITRE Stage Capabilities: SEO Poisoning) poisoning

techniques to lure victims into downloading the malicious payloads
    - SEO Poisoning and Google service abuse, in general, has been documented a lot recently, which indicates this infection vector is becoming common for threat actors
- Cybereason IR team observed the deployment of GootLoader through heavily-obfuscated JavaScript files with large file sizes (over 40 Megabytes)

On top of the new techniques utilized to load GootLoader, the post-infection methods that the threat actor carried out stand out:

- Cybereason first observed Cobalt Strike deployment, which leveraged DLL Hijacking, on top of a VLC MediaPlayer executable.
    - Cobalt Strike is an adversary simulation framework with the primary use case of assisting red team operations, nowadays being leveraged by threat actors for post-infection activities.
- Cybereason then identified SystemBC being leveraged by the threat actor
    - SystemBC is a proxy malware leveraging SOCKS5 and often utilized during the exfiltration phase of the attack.

Gootkit / GootLoader

Gootkit initially started as a banking Trojan in 2014. It was only in 2021 when the actors behind this piece of malware *moonlighted* and switched from a banker Trojan to a malware loader, leading to the **GootLoader** name. Security firm Mandiant named the threat actor operating GootLoader "UNC2565".

The Sophos researchers were the first to name this malware family Gootloader.

GootLoader generally relies on JavaScript for its infections. It also uses SEO poisoning techniques to place its infected pages in internet browser search results. That way, it will change how potential victims see them by presenting different websites whenever your link is clicked.

SEO Poisoning and malicious Google Ads explained with an example

SEO Poisoning and Google service abuse like Google Ads is becoming a trend amongst malware operators to distribute their payloads.

As explained above, threat actors create websites or populate web forums or similar websites with specific keywords and links, leading to a website hosting the infected file.

Search engine Ads are also leveraged to provide a link to the infected piece of malware (fake software for instance) on top of the search engine.

When searching for Rufus Pro, a USB boot disk creator tool, we provided an example on the search engine DuckDuckGo. The first result is the legitimate Rufus software page, and the second is the SEO Poisoning phishing domain.

This page seems to be taken down, but another related page is still up, https://ruflus[.]xyz. It appears to be a clone of the official Rufus page:

However the download links to a malicious payload:

- https://transfer[.]sh/get/7i8rkw/Rufus_Pro_signed.exe (VT link provided)
- This appears to be a sample of Lumma Stealer

Detection of SEO Poisoning and similar delivery methods such as Fake Google Ads

We are fully aware of this ongoing trend as well as threats actors taking advantage of google ads to get initial access to their malware.

As for now, all the threats and malware that are known to use these tactics (for example Redline, Vidar, IcedID, Gozi, Rhadamanthys and of course GootLoader) are covered in Cybereason.

Relation with Wordpress-enabled websites

Most of the domains configured in the GootLoader PowerShell stage #2 script had one commonality : they displayed a "*/xmlrpc.php* " relation in VirusTotal.

Intelligence teams have continuously observed GootLoader leveraging compromised Wordpress websites to use as C2 servers.

Post-infection Activities

Following the GootLoader infection, the Cybereason IR team observed hands-on keyboard activities which led to further deployment of attack frameworks, Cobalt Strike and SystemBC.

The threat actor leveraged these frameworks following the infection phase and during the lateral movement phase.

Download the Full Threat Alert

This blog post is a summary of a full 36-page Threat Alert, which can be downloaded here.

CYBEREASON RECOMMENDATIONS

The Cybereason Defense Platform can detect and prevent GootLoader, Cobalt Strike, or SystemBC post-exploitations. Cybereason recommends the following actions:

- **Enhance Cybereason sensor policies :** Set the Cybereason Anti-Ransomware protection mode to Prevent. More information for Cybereason customers can be found here.
- **Enable Variant Payload Protection in your Cybereason sensor policy**: Upgrade to a version that has VPP and enable VPP, as this will completely prevent the ransomware execution. VPP is supported in version 21.2.100 and above (Beta, and disabled by default) and 22.1.183 and above (GA, and enabled by default). More information can be found on The NEST.
- **Compromised user blocking** : Block users involved in the attack, in order to stop or at least slow down attacker propagation over the network.
- **Identify and block malicious network connections**: Identify network flows toward malicious IP/domains identified in the reports and block connections to stop the attacker from controlling the compromises

machines.

- **Reset Active Directory access**: If Domain controllers were accessed by the attacker and potentially all accounts have been stolen, it is recommended that, when rebuilding the network, all AD accesses are reset. Important note : krbtgt account needs to be reset twice and in a timely fashion.
- **Engage Incident Response**: It is important to investigate thoroughly the actions of the attacker to be sure not to miss any activity and patch what is needed to patch.

Compromised machine cleansing: Isolate and re-image all infected machines, to limit the risk of a second compromise or the attacker still getting access to the network afterward.

ABOUT THE RESEARCHERS

Loïc Castel, IR Investigator, Cybereason IR Team

Loïc Castel is a Security Analyst with the Cybereason IR team. Loïc analyses and researches critical incidents and cybercriminals in order to better detect compromises. In his career, Loïc worked as a security auditor in well-known organizations such as ANSSI (French National Agency for the Security of Information Systems) and as Lead Digital Forensics & Incident Response at Atos. Loïc loves digital forensics and incident response but is also interested in offensive aspects such as vulnerability research.

Jakes Jansen, IR Investigator Cybereason IR Team

Jakes is an Incident Response consultant and has been with Cybereason for a total of 3 years specializing in IR, Reverse Engineering, and Threat Hunting. With more than 16 years of Infosec experience, Jakes was, among other roles, responsible for building and leading DFIR teams that have handled large-scale investigations for government and multinational private entities, including financial institutions, manufacturing, and telecommunications. Jakes also has experience in internal threat investigations, mobile phone analysis, syndicate cases, and data analysis expected with eDiscovery during corporate acquisitions.

Nitin Grover, IR Investigator, Cybereason IR Team

Cyber Security Specialist with over 5 years of multi-geographical experience in protecting organizations from various cyber security attacks. Reducing security risks by 70-80% for the clients by providing them with optimal Vulnerability Assessments, Detailed Log Analysis, Security Strategies, Risk Management Solutions, Credential Risk Assessments, SIEM Solutions that include continuous threat monitoring and malicious activity detection capabilities. Performing Incident Response Analysis and Digital Forensic investigations for clients on a security incident to ensure immediate containment, recovery, and no business disruption.

About the Author

Cybereason Incident Response Team
