HC3: Analyst Note

September 29, 2023 TLP:CLEAR Report: 202309291200

Analyst Note: LokiBot Malware

Executive Summary

Active since 2015 and among the most prevalent and persistent strains of malware families since 2018, LokiBot has matured over time to target multi-sector industries. Despite its apolitical targeting of critical infrastructure, the malware's adverse effect on the Healthcare and Public Health (HPH) sector shows its reach. In March 2020, a multi-threat actor spearphishing campaign to spread LokiBot malware with a false World Health Organization trademark image solidified its threat to the HPH sector. In addition to other malware analyses, HC3 reported on this specific cyberattack in a 2020 HC3 Sector Note on LokiBot. The malware has been widely used for years, and because of behavior changes, it takes a lot of effort to monitor. However, there are some best practices for protecting against LokiBot and managing its impact. What follows is an update to the previous HC3 analysis of LokiBot, a timeline of multi-sector targeted applications, detection strategies, sample MITRE ATT&CK techniques, indicators of compromise, and recommended defenses and mitigations against the malware.

Overview

LokiBot was first observed in 2015 for sale on cybercrime forums by the cyber alias "lokistov," with a sale price of $540 USD for both a stealer and a loader. Named for the Norse mythological shapeshifting god, it became a popular malware choice for threat actors due to its low price and ease of use. After its version 1 source code leaked in 2018, lokistov developed version 2 of the malware, which has better evasion capabilities, as well as expanded keylogger and remote access trojan functionality. As of September 2023, the malware version sells for a mere $80 USD.

Figure 1: Artist Image of LokiBot *(Source: Webroot)*

Primarily targeting Windows devices and Android phones, its capabilities include logging keystrokes, capturing screenshots, and stealing everything from email credentials, payment card data and cryptocurrency wallet passwords, to the cookies and system data needed to bypass multi-factor authentication. These functionalities, combined with continually updating their initial access methods, have made it easier and more efficient for threat actors to use the malware to spread and infect systems

across all critical infrastructure sectors.

Since LokiBot is an infostealer, its primary purpose is to steal user credentials from infected machines. According to researchers, LokiBot is capable of stealing credentials from over 100 different clients. The impact of the theft of these credentials depends on their purpose. Successful credential theft could allow an attacker to steal sensitive data, gain access to other systems within an organization's network, or achieve other purposes.

In addition to this core infostealing functionality, LokiBot also incorporates modules that can be used for other purposes. For example, the backdoor functionality built into LokiBot could allow an attacker to remotely control an infected system and use it to download additional malware. After using LokiBot to gain initial access to a system, an attacker could download ransomware or other malware to expand their capabilities and the impact of their attack.

Target Industries

LokiBot is a widely used malware variant, especially after its source code was leaked. This means that many cybercrime groups incorporate it and variants of it into their attacks. With so many groups using it and LokiBot's wide range of capabilities, it is not targeted at any specific industry or geographic location.

Timeline of Known LokiBot Targeted Applications

Since LokiBot was first reported in 2015, cyber actors have used it across a range of targeted applications, including the following:

Date	Targeted Application
March 2020	FortiGuard Labs discovered a new COVID-19-themed spearphishing email with LokiBot malware that used the World Health Organization trademark.
February 2020	Trend Micro identified cyber actors using LokiBot to impersonate a launcher for Fortnite—a popular video game.
August 2019	FortiGuard SE researchers discovered a malware spam campaign distributing LokiBot information-stealing payloads in a spearphishing attack on a U.S. manufacturing company.
August 2019	Trend Micro researchers reported LokiBot malware source code being hidden in image files spread as attachments in phishing emails.
June 2019	Netskope uncovered LokiBot being distributed in a malware spam campaign using ISO image file attachments.
April 2019	Netskope uncovered a phishing campaign using malicious email attachments with LokiBot malware to create backdoors onto infected Windows systems and steal sensitive information.
February 2018	Trend Micro discovered CVE-2017-11882 being exploited in an attack using a Windows Installer service to deliver LokiBot malware.
October 2017	SfyLabs identified cyber actors using LokiBot as an Android banking trojan that turns into ransomware.
May 2017	Fortinet reported malicious actors using a PDF file to spread a new LokiBot variant capable of stealing credentials from more than 100 different software tools.
March 2017	Check Point discovered LokiBot malware found pre-installed on Android devices.
December 2016	Dr.Web researchers identified a new LokiBot variant targeting Android core libraries.
February 2016	Researchers discovered the LokiBot Android trojan infecting the core Android operating system processes.

HC3: Analyst Note

September 29, 2023 TLP:CLEAR Report: 202309291200

Technical Details

LokiBot, also known as Lokibot, Loki PWS, and Loki-bot, employs trojan malware to steal sensitive informaiton such as usernames, passwords, cryptocurrency wallets, and other credentials. According to one security researcher, in two-thirds of attack attempts, the LokiBot malware arrives in the form of an email attachment. Most of the other attack attempts use a delivery mechanism that, in 82% of cases, involves targeting a 23-year-old memory coruption flaw in Microsoft Office that first came to light six years ago.

Designated CVE-2017-11882, the flaw exists in Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1 and Microsoft Office 2016. Owing to continued use of these products, rather than still-supported and patched versions, many attempts to exploit this vulnerability remain successful. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has continued to feature this flaw on its list of the most "routinely exploited vulnerabilities," owing to their continued exploitation by nation-state hacking teams as well as criminals.

LokiBot-wielding attackers continue to test fresh strategies for infecting targets. In 2020, CISA warned that the operators behind the malware had been using malicious websites to hide the malware from victims, as well as to send phishing links through SMS and other private messages that contain LokiBot.

This summer, researchers warned they had been seeing an increase in attacks that used malicious Microsoft Office documents to drop LokiBot. Each of the attacks tended to target one of these two flaws:

- CVE-2021-40444: A Microsoft Office MSHTML remote code execution vulnerability.
- CVE-2022-30190: A Microsoft Office Support Diagnostic Tool, or MSDT, remote code execution vulnerability.

The malware steals credentials using a keylogger to monitor browser and desktop activity.	
MITRE ATT&CK ID	T1555
Sub-techniques	T1555.001, T1555.002, T1555.003
Tactic	Credential Access
Platforms	Linux, Windows, macOS
Permissions Required	Administrator
Data Sources	API monitoring, File monitoring, PowerShell logs, Process monitoring, System Calls
Version	1.0
Created	February 11, 2020
Last Modified	March 25, 2020

LokiBot can also create a backdoor into infected systems to allow an attacker to install additional payloads. (Event Triggered Execution: Accessibility Features)	
MITRE ATT&CK ID	T1546.008
Sub-technique of	T1546
Tactics	Privilege Escalation, Persistence
Platforms	Windows
Permissions Required	Administrator
Effective Permissions	SYSTEM
Data Sources	File monitoring, Process command-line parameters, Process monitoring, Windows Registry
CAPEC ID	CAPEC-558

HC3: Analyst Note

September 29, 2023 TLP:CLEAR Report: 202309291200

Version	1.0
Created	January 24, 2020
Last Modified	May 13, 2020

Malicious cyber actors typically use LokiBot to target Windows and Android operating systems and to distribute the malware via email, malicious websites, text, and other private messages.	
MITRE ATT&CK ID	T1204.002
Sub-technique of	T1204
Tactic	Execution
Platforms	Linux, Windows, macOS
Permissions Required	User
Data Sources	Anti-virus, Process command-line parameters, Process monitoring
Version	1.0
Created	March 11, 2020
Last Modified	March 11, 2020

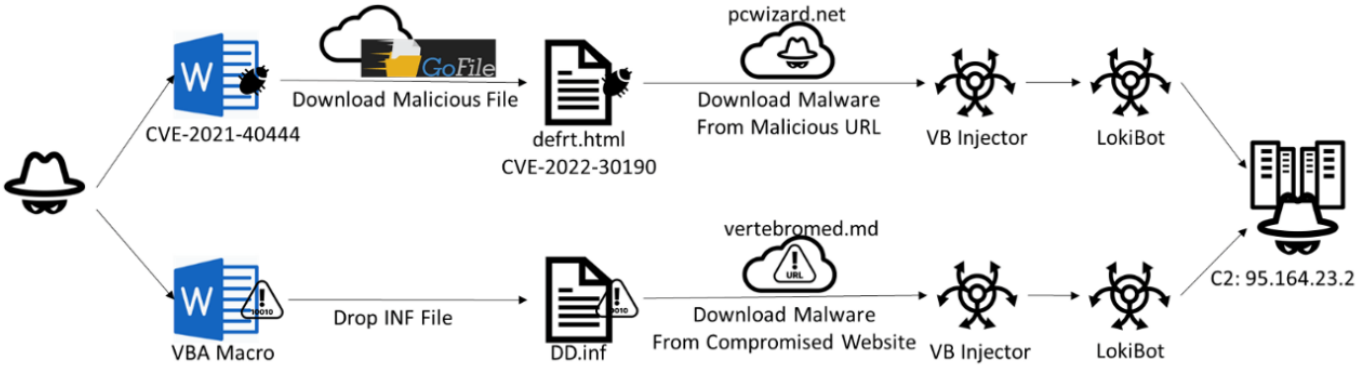

Figure 2: LokiBot Attack Chain *(Source: Fortinet)*

MITRE ATT&CK Techniques

According to MITRE, LokiBot uses the ATT&CK techniques listed in the table below:

Technique	ID	Use
System Network Configuration Discovery	T1016	LokiBot can discover the domain name of the infected host.
Obfuscated Files or Information	T1027	LokiBot has obfuscated strings with base64 encoding.
Obfuscated Files or Information: Software Packing	T1027.002	LokiBot has used several packing methods for obfuscation.
System Owner/User Discovery	T1033	LokiBot can discover the username on the infected host.
Exfiltration Over C2 Channel	T1041	LokiBot can initiate contact with command and control to exfiltrate stolen data.
Process Injection: Process Hollowing	T1055.012	LokiBot has used process hollowing to inject into legitimate Windows process vbc.exe.
Input Capture: Keylogging	T1056.001	LokiBot can capture input on the compromised host via keylogging.
Application Layer Protocol: Web Protocols	T1071.001	LokiBot has used Hypertext Transfer Protocol for command and control.
System Information Discovery	T1082	LokiBot can discover the computer name and Windows product

		name/version.
User Execution: Malicious File	T1204.002	LokiBot has been executed through malicious documents contained in spearphishing emails.
Credentials from Password Stores	T1555	LokiBot has stolen credentials from multiple applications and data sources, including Windows operating system credentials, email clients, File Transfer Protocol, and Secure File Transfer Protocol clients.
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	LokiBot has demonstrated the ability to steal credentials from multiple applications and data sources, including Safari and Chromium and Mozilla Firefox-based web browsers.
Hide Artifacts: Hidden Files and Directories	T1564.001	LokiBot can copy itself to a hidden file and directory.

Detection

The Cybersecurity & Infrastructure Security Agency (CISA) developed the following Snort signature for use in detecting network activity associated with LokiBot activity:

alert tcp any -> any $HTTP_PORTS (msg:"Lokibot:HTTP URI POST contains '/*/fre.php' post-infection"; flow:established,to_server; flowbits:isnotset,.tagged; content:"/fre.php"; http_uri; fast_pattern:only; urilen:<50,norm; content:"POST"; nocase; http_method; pcre:"/\/(?:alien|loky\d|donep|jemp|lokey|new2|loki|Charles|sev7n|dbwork|scroll\/NW|wrk|job|five\d?|donemy|animation\dkc|love|Masky|v\d|lifetn|Ben)\/fre\.php$/iU"; flowbits:set,.tagged;classtype:http-uri; metadata:service http; metadata:pattern HTTP-P001,)

Indicators of Compromise

One security researcher noted that LokiBot activity has a relatively small number of indicators of compromise (IOC). However, during the end of 2022, the number of occurrences peaked in the last three days of December. Threat actors often increase their attack efforts during U.S. or other targeted nations' holidays. During this time, cyberattacks are often more effective as security and other personnel take this time off.

Palo Alto Unit 42 Indicators of Compromise	
Type	IOC
ZIP file	4edd01345f58b9cc04a88ca15d6b82895f44f5b9cb51ad63b809de09029670ac
ISO	8a5a024272361bb1ae12860c033bb52685d7b0ea3bce5fac46439f3f3ad36a84
Loader	1b574a66c84924886daec4841e1b107258e019aaf6f336329ae8fae7cbd52a34

Fortinet Indicators of Compromise	
Type	IOC
C2	95[.]164[.]23[.]2
File	17d95ec93678b0a73e984354f55312dda9e6ae4b57a54e6d57eb59bcbbe3c382
File	23982d2d2501cfe1eb931aa83a4d8dfe922bce06e9c327a9936a54a2c6d409ae
File	9eaf7231579ab0cb65794043affb10ae8e4ad8f79ec108b5302da2f363b77c93
File	da18e6dcefe5e3dac076517ac2ba3fd449b6a768d9ce120fe5fc8d6050e09c55
File	2e3e5642106ffbde1596a2335eda84e1c48de0bf4a5872f94ae5ee4f7bffda39
File	80f4803c1ae286005a64ad790ae2d9f7e8294c6e436b7c686bd91257efbaa1e5
File	21675edce1fdabfee96407ac2683bcad0064c3117ef14a4333e564be6adf0539

File	4a23054c2241e20aec97c9b0937a37f63c30e321be01398977e13228fa980f29

Cyware Indicators of Compromise	
Type	IOC
Filename	COVID_19-WORLD HEALTH ORGANIZATION CDC_DOC[.]zip[.]arj
Filename	COVID_19-WORLD HEALTH ORGANIZATION CDC_DOC[.]pdf[.]exe
SHA256	9e17f5e70c30ead347b68841fa137015d713269add98f0257fb30cc6afdea4fe
SHA256	f8e041bed93783bbd5966bfba6273fe7183464035ea54fe1d59ff85a679b3e3e
C2	hxxp://bslines[.]xyz/copy/five/fre[.]php
Spam Relay	159[.]69[.]16[.]177

Defense and Mitigations

LokiBot malware has been used by attackers for many years, and there have been multiple versions of this threat. It takes a lot of effort for any security team to constantly monitor the behavior changes in the malware and add the necessary protections. However, some best practices for protecting against LokiBot and managing the impact of LokiBot infections include:

- **Anti-Phising Protection:** LokiBot is a trojan that is often distributed as an attachment to phishing emails and other messages. Anti-phishing solutions that can identify and block malicious content in attachments from reaching the user can protect against infections by LokiBot.

- **Endpoint Security Solutions:** LokiBot is a well-known malware variant, and most endpoint security solutions have a signature for it and are familiar with its activities. Deploying an endpoint security solution on all devices and keeping them up-to-date should help to reduce the risk of infections. Additionally, endpoint security solutions may be able to prevent the download and execution of second-stage malware delivered via LokiBot.

- **Multi-Factor Authentication (MFA):** LokiBot's primary purpose is to identify and steal employees' login credentials from infected machines. By deploying MFA across the organization, a company can limit the utility of these compromised credentials to an attacker.

- **Zero-Trust Security:** A zero trust security strategy limits the access and permissions of user accounts to the minimum required for their role. By implementing and enforcing zero trust principles, an organization can limit the damage that can be done with an account compromised via credentials stolen by LokiBot.

- **Cybersecurity Awareness Training:** LokiBot malware is commonly spread via phishing attacks and malicious websites. Cybersecurity training can help employees to identify and properly respond to these threats, limiting the risk of infections.

- **Network Traffic Monitoring:** LokiBot can be used as a remote access trojan (RAT), allowing an attacker to remotely control an infected computer to steal data or install malware. Unusual network traffic associated with LokiBot's use as a RAT can be detected via network traffic analysis.

Way Forward

LokiBot is probably not going to be the last to use the COVID-19 epidemic as a lure for unsuspecting companies and organizations. Info stealers such as LokiBot do not work in a vacuum. The information this type of malware steals from a system is known as a "bot," and bots are then packaged up into "logs" that get sold on dedicated cybercrime markets. LokiBot's relative simplicity makes it easy to spot, since almost everything it does will involve command-and-control communications. The primary way to prevent LokiBot from being installed on a system is to not allow unknown downloads from suspicious emails. As such, most anti-virus software should detect and block the malware or find it, if it is set to reguarly scan systems.

In addition to the aforementioned defense and mitigation strategies, HC3 recommends that HPH organizations utilize resources from CISA Stop Ransomware, HHS 405(d), and the H-ISAC to proactively and reactively aid healthcare organizations with cybersecurity awareness and guidance.

The probability of cyber threat actors targeting any industry remains high, but especially so for the Healthcare and Public Health sector. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent a cyberattack remains the best way forward for healthcare organizations.

Relevant HHS Reports

HC3: Sector Note – LokiBot Malware Threat to Healthcare (June 16, 2020)

References

"ATT&CK ID: T1204.002." MITRE ATT&CK. Accessed September 27, 2023. https://attack.mitre.org/versions/v7/techniques/T1204/002/

"ATT&CK ID: T1546.008." MITRE ATT&CK. Accessed September 27, 2023. https://attack.mitre.org/versions/v7/techniques/T1546/008/

"ATT&CK ID: T1555." MITRE ATT&CK. Accessed September 27, 2023. https://attack.mitre.org/versions/v7/techniques/T1555/

"COVID-19 Themed Spearphishing Campaign Now Dropping LokiBot Infostealer." Cyware. April 10, 2020. https://cyware.com/blog/covid-19-themed-spearphishing-campaign-now-dropping-lokibot-infostealer-5a12

"Cybercriminals Exploit Microsoft Word Vulnerabilities to Deploy LokiBot Malware." The Hacker News. July 17, 2023. https://thehackernews.com/2023/07/cybercriminals-exploit-microsoft-word.html

"CVE-2021-40444 Detail." National Vulnerability Database. Accessed September 27, 2023. https://nvd.nist.gov/vuln/detail/CVE-2021-40444

"CVE-2022-30190 Detail." National Vulnerability Database. Accessed September 27, 2023. https://nvd.nist.gov/vuln/detail/cve-2022-30190

Lin, Cara. "LokiBot Campaign Targets Microsoft Office Document Using Vulnerabilities and Macros." Fortinet. July 12, 2023. https://www.fortinet.com/blog/threat-research/lokibot-targets-microsoft-office-document-using-vulnerabilities-and-macros#:~:text=LokiBot%2C%20also%20known%20as%20Loki,sensitive%20information%20from%20infe

cted%20machines.

"Lokibot Malware." Check Point. Accessed September 27, 2023. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/lokibot-malware/

"LokiBot Malware." Cybersecurity & Infrastructure Security Agency. October 24, 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-266a

Naprys, Ernestas. "LokiBot malware going for a song at $80." Cybernews. September 14, 2023. https://cybernews.com/security/lokibot-malware-going-for-a-song-at-80/

Navarrete, Chris, Edouard Bochin, Durgesh Sangvikar, Lei Xu, and Yu Fu. "Spike in LokiBot Activity During Final Week of 2022." Unit 42. March 3, 2023. https://unit42.paloaltonetworks.com/lokibot-spike-analysis/#post-127127-_ru696q1s5tpr

Schwartz, Mathew J. "LokiBot Information Stealer Packs Fresh Infection Strategies." Bank Info Security. September 14, 2023. https://www.bankinfosecurity.com/lokibot-information-stealer-packs-fresh-infection-strategies-a-23079

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback