# LokiBot Malware | CISA

Published: 2020-10-24 · Archived: 2026-04-05 13:19:16 UTC

## Summary

*This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise frameworks for all referenced threat actor techniques.*

This product was written by the Cybersecurity and Infrastructure Security Agency (CISA) with contributions by the Multi-State Information Sharing & Analysis Center (MS-ISAC) .

CISA has observed a notable increase in the use of LokiBot malware by malicious cyber actors since July 2020. Throughout this period, CISA's EINSTEIN Intrusion Detection System, which protects federal, civilian executive branch networks, has detected persistent malicious LokiBot activity. LokiBot uses a credential- and information-stealing malware, often sent as a malicious attachment and known for being simple, yet effective, making it an attractive tool for a broad range of cyber actors across a wide variety of data compromise use cases.

## Technical Details

LokiBot—also known as Lokibot, Loki PWS, and Loki-bot—employs Trojan malware to steal sensitive information such as usernames, passwords, cryptocurrency wallets, and other credentials.

- The malware steals credentials through the use of a keylogger to monitor browser and desktop activity (*Credentials from Password Stores* [T1555 ]).
  - (*Credentials from Password Stores: Credentials from Web Browsers* [T1555.003 ])
  - (*Input Capture: Keylogging* [T1056.001 ])
- LokiBot can also create a backdoor into infected systems to allow an attacker to install additional payloads (*Event Triggered Execution: Accessibility Features* [T1546.008 ]).
- Malicious cyber actors typically use LokiBot to target Windows and Android operating systems and distribute the malware via email, malicious websites, text, and other private messages (*User Execution: Malicious File* [T1204.002 ]). See figure 1 for enterprise techniques used by LokiBot.

*Figure 1: MITRE ATT&CK enterprise techniques used by LokiBot*

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

- **February 2020:** Trend Micro identified cyber actors using LokiBot to impersonate a launcher for Fortnite—a popular video game.[1 ]
- **August 2019:** FortiGuard SE researchers discovered a malspam campaign distributing LokiBot information-stealing payloads in spearphishing attack on a U.S. manufacturing company.[2 ]

- **August 2019:** Trend Micro researchers reported LokiBot malware source code being hidden in image files spread as attachments in phishing emails.[3 ]
- **June 2019:** Netskope uncovered LokiBot being distributed in a malspam campaign using ISO image file attachments.[4 ]
- **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.[5 ]
- **February 2018:** Trend Micro discovered CVE-2017-11882 being exploited in an attack using Windows Installer service to deliver LokiBot malware.[6 ]
- **October 2017:** SfyLabs identified cyber actors using LokiBot as an Android banking trojan that turns into ransomware.[7 ]
- **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.[8 ]
- **March 2017:** Check Point discovered LokiBot malware found pre-installed on Android devices.[9 ]
- **December 2016:** Dr.Web researchers identified a new LokiBot variant targeting Android core libraries.[10 ]
- **February 2016:** Researchers discovered the LokiBot Android Trojan infecting the core Android operating system processes.[11]

## MITRE ATT&CK Techniques

According to MITRE, LokiBot uses the ATT&CK techniques listed in table 1.

*Table 1: LokiBot ATT&CK techniques*

| Technique | Use |
|---|---|
| *System Network Configuration Discovery* [T1016 ] | LokiBot has the ability to 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 has the ability to discover the username on the infected host. |
| *Exfiltration Over C2 Channel* [T1041 ] | LokiBot has the ability to 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 has the ability to capture input on the compromised host via keylogging. |

| Technique | Use |
| --- | --- |
| *Application Layer Protocol: Web Protocols* [T1071.001 ] | LokiBot has used Hypertext Transfer Protocol for command and control. |
| *System Information Discovery* [T1082 ] | LokiBot has the ability to 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 has the ability to copy itself to a hidden file and directory. |

## Detection

### Signatures

CISA developed the following Snort signature for use in detecting network activity associated with LokiBot activity.

alert tcp any 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,)

## Mitigations

CISA and MS-ISAC recommend that federal, state, local, tribal, territorial government, private sector users, and network administrators consider applying the following best practices to strengthen the security posture of their organization's systems. System owners and administrators should review any configuration changes prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines. See Protecting Against Malicious Code.
- Keep operating system patches up to date. See Understanding Patches and Software Updates.

- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Enforce multi-factor authentication. See Supplementing Passwords for more information.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators' group unless required.
- Enforce a strong password policy. See Choosing and Protecting Passwords.
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known. See Using Caution with Email Attachments.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.
- Visit the MITRE ATT&CK Techniques pages (linked in table 1 above) for additional mitigation and detection strategies.

For additional information on malware incident prevention and handling, see the National Institute of Standards and Technology Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

## Resources

Center for Internet Security Security Event Primer – Malware: https://www.cisecurity.org/white-papers/security-event-primer-malware/
MITRE ATT&CK – LokiBot: https://attack.mitre.org/software/S0447/
MITRE ATT&CK for Enterprise: https://attack.mitre.org/matrices/enterprise/

## References

[1] Trend Micro: LokiBot Impersonates Popular Game Launcher and Drops Compiled C# Code File

[2] Fortinet: Newly Discovered Infostealer Attack Uses LokiBot

[3] ZDNet: LokiBot Malware Now Hides its Source Code in Image Files

[4] SecurityWeek: LokiBot and NanoCore Malware Distributed in ISO Image Files

[5] Netskope: LokiBot & NanoCore being distributed via ISO disk image files

[6] Trend Micro: Attack Using Windows Installer Leads to LokiBot

[7] BleepingComputer: LokiBot Android Banking Trojan Turns Into Ransomware When You Try to Remove It

[8] Fortinet: New Loki Variant Being Spread via PDF File

[9] Check Point: Preinstalled Malware Targeting Mobile Users

[10] BleepingComputer: Loki Trojan Infects Android Libraries and System Process to Get Root Privileges

[11] New Jersey Cybersecurity & Communications Integration Cell: LokiBot

## Revisions

September 22, 2020: Initial Version|September 23, 2020: Added hyperlink to MS-ISAC

---