# Trojan:W32/Lokibot | F-Secure

Archived: 2026-04-05 18:39:04 UTC

## Classification

Aliases:

Trojan.TR/AD.LokiBot, Fareit

## Summary

Lokibot is a password/info-stealing malware, delivered through malware spam (malspam) campaigns, and notably known for the wide range of applications that it targets.

## Removal

### Automatic action

Based on the settings of your F-Secure security product, it will either move the file to the **quarantine** where it cannot spread or cause harm, or **remove** it.

A False Positive is when a file is incorrectly detected as harmful, usually because its code or behavior resembles known harmful programs. A False Positive will usually be fixed in a subsequent database update without any action needed on your part. If you wish, you may also:

- **Check for the latest database updates**

  First, check if your F-Secure security program is using the latest updates, then try scanning the file again.

- **Submit a sample**

  After checking, if you still believe the file is incorrectly detected, you can submit a sample of it for re-analysis.

  *Note:* If the file was moved to **quarantine**, you need to collect the file from quarantine before you can submit it.

- **Exclude a file from further scanning**

  If you are certain that the file is safe and want to continue using it, you can exclude it from further scanning by the F-Secure security product.

  *Note:* You need administrative rights to change the settings.

## Technical Details

## Infection vector

Lokibot is commonly delivered through malicious spam (malspam) campaigns. There are numerous ways that the payload has been seen to be delivered through these spam mails:

Lokibot has been witnessed to exploit certain vulnerabilities in some of these attachment file formats, notably CVE-2017-11882, CVE-2018-0802, and CVE-2018-20250.

Files & Mutexes

Lokibot ensures that only a single instance of the malware is running on an infected system by creating a mutex. The mutex string is computed as the MD5 hash of the MachineGUID (obtained through registry).

Additionally, Lokibot creates a folder which contains multiple files. The folder path is %AppData%/<MD5_MACHINEGUID>[7:12]/.

The folder contains:

Data Stealing

This malware is notably known for stealing credentials from browsers, mail clients, file sharing programs, remote connection programs, and more. It also contains a keylogger component, which can be utilized by the malefactor.

Lokibot is capable of stealing data from the following applications:

- 1Password
- 32BitFtp
- 360Browser
- AbleFTP
- Automize7
- BitKinex
- Bitvise
- BlazeFTP
- Catalina Group Citrio
- CheckMail
- Chromium
- Cá»‘c Cá»‘c
- Comodo Chromodo
- Comodo Dragon
- Comodo IceDragon
- Coowon
- Cyberduck
- Cyberfox
- DeluxeFTP
- EasyFTP
- EnPass

- Epic Privacy Browser
- Estsoft ALFTP
- ExpanDrive
- FAR Manager
- Fasteam NETFile
- FileZilla
- FlashFXP
- FossaMail
- Foxmail
- FreshFTP
- FTP Navigator
- FTP Now
- FTPBox
- FTPGetter
- FtpInfo
- FTPShell
- FullSync
- Ghisler Total Commander
- GmailNotifierPro
- GoFTP
- Google Chrome
- Google Chrome SxS
- IncrediMail
- Internet Explorer
- Ipswitch
- Iridium
- JaSFTP
- KeePass
- KiTTY
- K-Meleon
- LinasFTP
- Lunascape
- Maple
- Maple Studio ChromePlus
- MikroTik Winbox
- Mozilla Flock
- Mozilla SeaMonkey
- mSecure
- Mustang Browser
- NCH ClassicFTP
- NCH Fling
- NetDrive

- NETGATE BlackHawk
- NetSarang XFTP
- NexusFile
- Nichrome
- NoteFly
- Notezilla
- NovaFTP
- NppFTP
- Odin Secure FTP Expert
- Opera
- Opera Mail
- Opera Next
- Orbitum
- Outlook
- oZone3D MyFTP
- Pale Moon
- Pidgin
- Pocomail
- Postbox
- PuTTY
- QtWeb
- QupZilla
- RealVNC
- RoboForm
- Rockmelt
- Safari
- SecureFX
- SftpNetDrive
- sherrod FTP
- Sleipnir
- SmartFTP
- Spark
- Staff-FTP
- Steed
- stickies
- StickyNotes
- Superbird
- SuperPutty
- Syncovery
- Titan
- To-Do DeskList
- Torch

- Trojit
- TrulyMail
- UltraFXP
- Vivaldi
- Waterfox
- WinChips
- WinFtp Client
- WinSCP
- WS_FTP
- Yandex Browser
- yMail

Network Activity

The payload initiates a communication with the C&C server to exfiltrate the stolen data and receive commands. Besides the stolen data, it sends the Windows product name and version, username, computer name, and domain name to the C&C server.

Lokibot is most commonly seen to send a POST request to <DOMAIN>/subdir/subdir1/../fre[.]php, although other less-common patterns have also been observed in the wild (e.g. <DOMAIN>/subdir/subdir1/cat[.]php).

User-Agent: Mozilla/4.08 (Charon; Inferno)

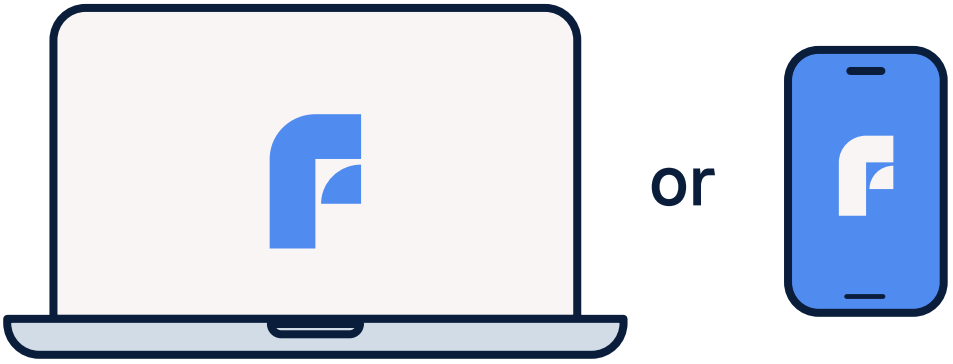
Analysis on file: 55589f10cbf2e9efa809a09c9d75bd8ff6aacd16

## Protect your devices from malware with F-Secure Total

Protecting your devices from malicious software is essential for maintaining online security. F-Secure Total makes this easy, helping you to secure your devices in a brilliantly simple way.

- Award-winning antivirus and malware protection
- Online browsing, banking, and shopping protection
- 24/7 online identity and data breach monitoring
- Unlimited VPN service to safeguard your privacy
- Password manager with private data protection

Choose how many devices you want to protect to get started.




- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €69.99.

- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €89.99.

- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €99.99.

## More Support

**Contact Support**

Chat with with or call an agent.