XFiles Stealer Campaign Abusing Follina

By Shmuel Gihon

Published: 2022-07-03 · Archived: 2026-04-06 00:21:17 UTC

Research

Executive Summary

As many threat actors and groups seek to utilize recently discovered vulnerabilities, the Cyberint Research Team found several XFiles stealer campaigns, in which Follina vulnerability was exploited as part of the delivery phase.

Follina is one of the most widespread vulnerabilities discovered throughout 2022. The vulnerability allows a threat actor to perform a remote code execution (RCE) through malicious Word documents.

XFiles stealer is a vastly used info stealer that took off during the end of 2021. The group that sells the stealer is Russia-region based and is currently looking to expand.

Recent evidence suggests that worldwide threat actors' campaigns abuse the Follina vulnerability in order to deliver the XFiles info stealer, which has become popular even among veterans.

Figure 1: XFiles Reborn stealer ad on an underground forum

Purchasing

This campaign consists of two major components. The delivery module includes the Follina exploits and the XFiles info stealer sample.

Follina Exploits

As expected, once the Follina vulnerability was published, its use became widespread, due to its simple exploitation and massive effect when successful. Many exploit developers and underground vulnerability researchers offered exploits abusing Follina, for sale or even for free (Figure 2, 3).

Figure 2: Threat actor publishing fully undetected exploit builder for 3.5K USD.

Figure 3: Exploit being advertised in a Telegram channel for free

Most sellers offer malicious documents exploiting this vulnerability to fulfill the buyer's end goal. The prices vary, depending on the developer's reputation and level of detection.

XFiles Reborn Information Stealer

XFiles developers currently operate several Telegram channels and bots to fully support their customers. They have a news channel, updates channel, and shopping bot along with a direct chat with the seller and overall chat for customers.

The subscription plans they currently offer are 5, 10, or 20 USD per week, month, or six months, respectively.

XFiles Reborn Panel

Although the XFiles Reborn group recommends using Telegram as a panel for the information gathering from the stealers, they also provide the ability to create a “classic” panel on a given C2 by the seller (Figure 4, 5).

Figure 4: XFiles Reborn stealer’s panel login page

XFiles Reborn Group

The XFiles Reborn group started its operations in March 2021.

The group reminds us of another fairly new, yet ambitious group, Jester [1], as they put many efforts into publicity. Additionally, they do the “extra mile” to make themselves unique compared to other info stealer operators. Simplicity and efficiency is the name of the game.

Before they had a respectable amount of subscribers to their Telegram channels, the XFiles Reborn group used to advertise themselves on the notorious underground forum, “Lolz.Guru” (Figure 6).

Figure 6: XFiles Reborn group’s first post on lolz.guru

Threat Actors Recruitment

As for expanding their operation, it seems that they are constantly looking to recruit new members, mostly ones that already have experience with info stealers.

During the past year, a threat actor created a new info stealer named Whisper Project. The campaign went on for a couple of months and started to get subscribers.

Whisper Project was short-lived but looked very professional and seemed to have the potential to become quite popular. As XFiles Reborn was looking to expand, they made some efforts to recruit the individual responsible for Whisper Project. Once they were successful, the Whisper Project died with an announcement by the creator that he had joined the XFiles Reborn team (Figure 7).

Figure 7: Whisper Project creator announces shutting down the operation and joining XFiles Reborn

Punisher Miner

This ambitious group is not only expanding its personnel but also adding new products to their shelves. Earlier this year, they introduced the Punisher Miner (Figure 8).

Figure 8: Punisher Miner’s advertisement on an underground forum

This miner seems to be fairly sophisticated, as it supports mining Monero, Toncoin and Ravecoin. The miner is also packed with evasion techniques, such as hiding itself from the Task Manager, delaying execution on startup, and more. The purchasing and building process is all done via a dedicated Telegram bot that provides a built executable once the payment is done. The price of the Punisher Miner is 500 rubles, which is around 10 USD.

XFiles Info Stealer

Although they added the miner recently, the group's flagship is still the info stealer. The stealer targets all Chromium-based browsers, Opera, and Firefox browsers, including history, cookies, passwords and credit card information.

Also, the stealer seeks to obtain FTP, Telegram and Discord credentials. In addition, it targets predefined file types that are located on the victim's Desktop along with a screenshot. Other clients, such as Steam and crypto-wallets, are also targeted in the process.

Technical Analysis

Initial Infection

Recent campaigns suggest that the infection process consists of `malicious .docx` files containing an OLE object pointing to the C2 server's `LoadingUpdate.html` file (Figure 9).

Figure 10: JavaScript code that exploits Follina

First Stage

The HTML file contains a JavaScript code (Figure 10) that will exploit the Follina vulnerability in order to download the second infection stage from the C2, `ChimLacUpdate.exe`.

Figure 10: JavaScript code that exploits Follina

The JavaScript code includes an encoded base64 string that, once decoded, reveals a PowerShell command that will create persistence within the startup directory for the newly-downloaded file (Figure 11) and execute it.

Figure 11: PowerShell command decoded

Second Stage

The second stage is a crucial part of the infection process. The `ChimLacUpdate.exe` file includes a shellcode runner module. This module contains hardcoded encrypted shell code and an AES decryption key.

Once the shellcode is decrypted, it is executed within the same process via the `VirtualProtect` API call (Figure 12) and loaded into an unprotected section within the running process.

Figure 12: Shellcode extraction and execution decompiled function

As mentioned, this method is not new and is considered one of the simpler techniques to identify although it is enough for this particular stage.

The shellcode itself is another downloader from the same C2 that will load and execute the XFiles Reborn stealer sample.

Post Infection

This part is pretty similar in most info stealers and XFiles is no different. It pursues Discord and Telegram credentials, browsing information, such as cookies, passwords and history, FTP clients credentials and, of course, crypto wallets.

In addition, the XFiles stealer looks for something less common: credit card information stored in browsing applications.

Finally, in some cases, the stealer looks for particular files such as `.txt` and `.pdf` and gathers screenshots of the victim's machine.

Working Directory

XFiles Reborn creates its working directory in the same path in which it is running, which in our case is the `%APPDATA%` directory. The working directory consists of two directories:

- **Grabber** – Contains all files stolen and crypto-wallets.
- **Browsers** – Contains all browsing information divided into browser directories.

The `PCInfo.txt` file, which contains the system information of the victim's machine (Figure 14), is also created within the working directory along with the captured screenshot.

Figure 14: XFiles Reborn working directory

Data Exfiltration

The Data exfiltration stage is done via Telegram.

Telegram has become very popular among the new info stealers introduced this year. XFiles Reborn abuses the simplicity and efficiency of Telegram to get a free, highly anonymous C2 infrastructure.

At this stage, once the stealer has gathered all the necessary information, it dynamically creates a zip file (does not save it locally) as a stream and sends it to the threat actor's preconfigured Telegram bot (Figure 15).

Figure 15: C2 Telegram bot presenting new logs notification

Conclusions

The discovery of the Follina vulnerability provided threat actors with a new tool to weaponize their delivery process. It is inevitable and obvious that these techniques will be seen in ongoing campaigns, especially when we

observe the info stealers industry.

Over the past six months, the Cyberint Research Team has witnessed massive numbers of new info stealers introduced to the market.

The trend of deploying C2 infrastructure using Telegram, which requires minimal effort on the part of the operators and developers, is taking over and lowering the level of skill that used to be required by threat actors in order to establish their own info stealer brand.

Cyberint Research Team is convinced that this trend will lead to many more threat actors and info stealers brands in the marketplaces, as other types of malware, such as RATs or even ransomware, follow the trend.

References

[1] https://cyberint.com/blog/research/jester-stealer/
