RecordBreaker Stealer Distributed via Hacked YouTube Accounts

asec.ahnlab.com/en/52072/

By Sanseo May 3, 2023

RecordBreaker is a new Infostealer that appeared in 2022 and is known as the new version of Raccoon Stealer. Similar to other Infostealers, such as CryptBot, RedLine, and Vidar, it is a major malware type that usually disguises itself as a software crack or installer. AhnLab Security Emergency response Center (ASEC) has confirmed the distribution of RecordBreaker through a YouTube account that is assumed to have been recently hacked.

1. Previous Distribution Cases

Search engines are one of the major attack vectors used for malware distribution. ASEC has published the following blog post that covers the distribution cases of RecordBreaker through search engines.

> New Info-stealer Disguised as Crack Being Distributed

Users who search for the cracks, serial keygens, and installers of commercial software on search engines are led to fake distribution pages where they are tricked into downloading malware.

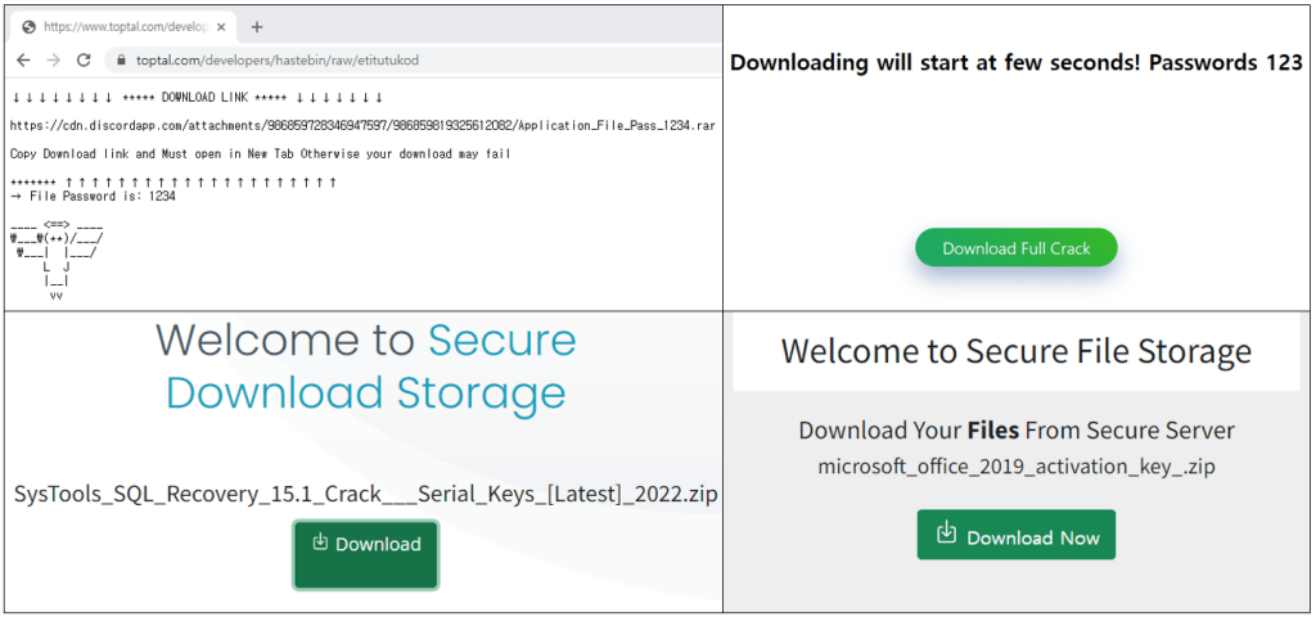

Figure 1. Webpages distributing the malware

There have been many recent cases of malware being distributed through YouTube and not just search engines. For example, a threat actor who distributed the RedLine Infostealer in the past had uploaded a tutorial video on how to install a crack program along with a link disguised as a download page to install the crack. **[1]** There is also another case where BlackGuard Infostealer was distributed as a hack for the game Valorant. **[2] [3]**

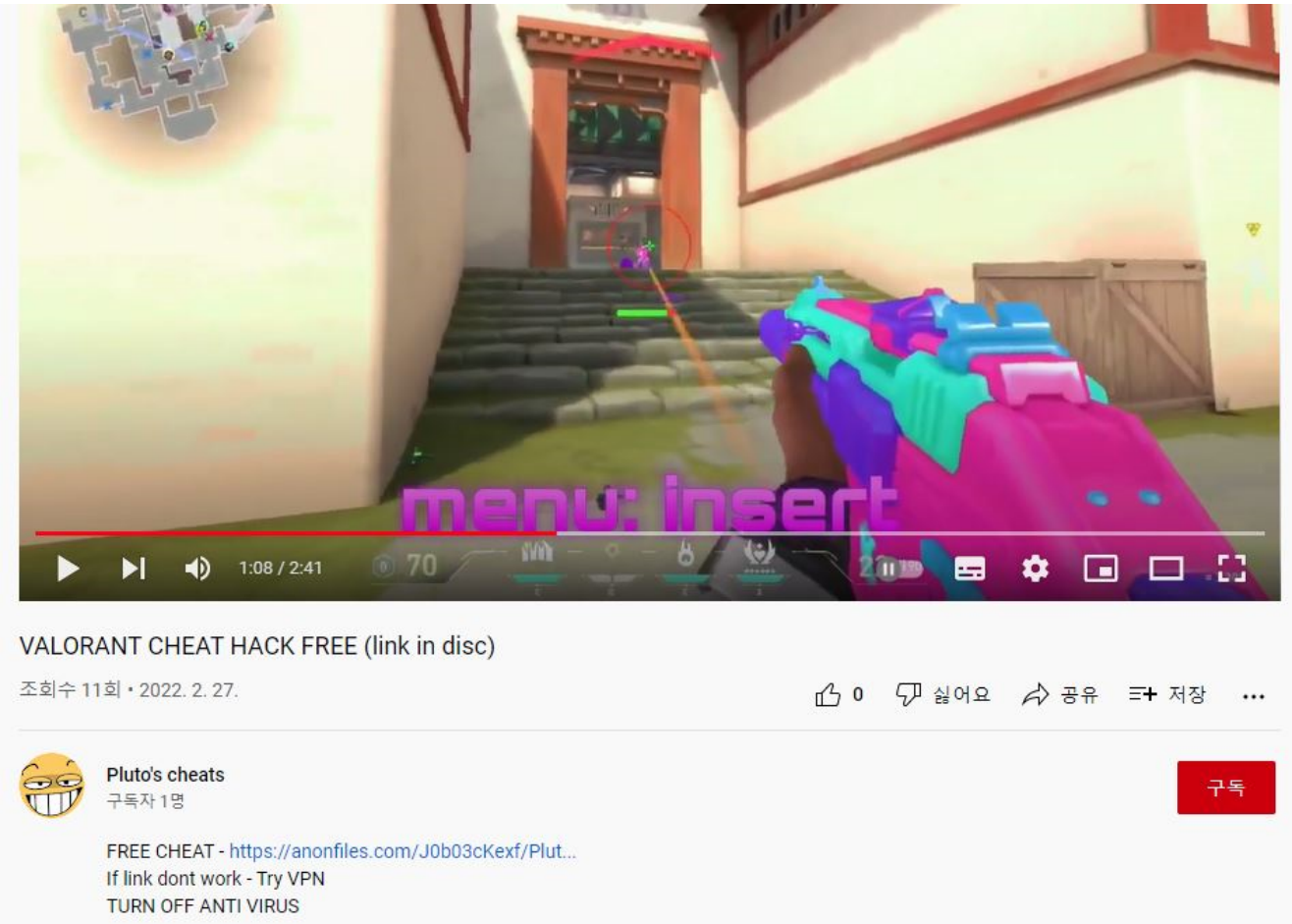

Figure 2. Video distributing BlackGuard disguised as a game hack for Valorant.

2. Case of RecordBreaker Distribution via YouTube

While monitoring malware strains that are being distributed via YouTube, ASEC has confirmed the distribution of the RecordBreaker Infostealer through an account that is assumed to have been hacked. The post below was uploaded by the threat actor, and it contains the download link to an Adobe Photoshop crack along with a link to a tutorial in both the video description and the comment section.

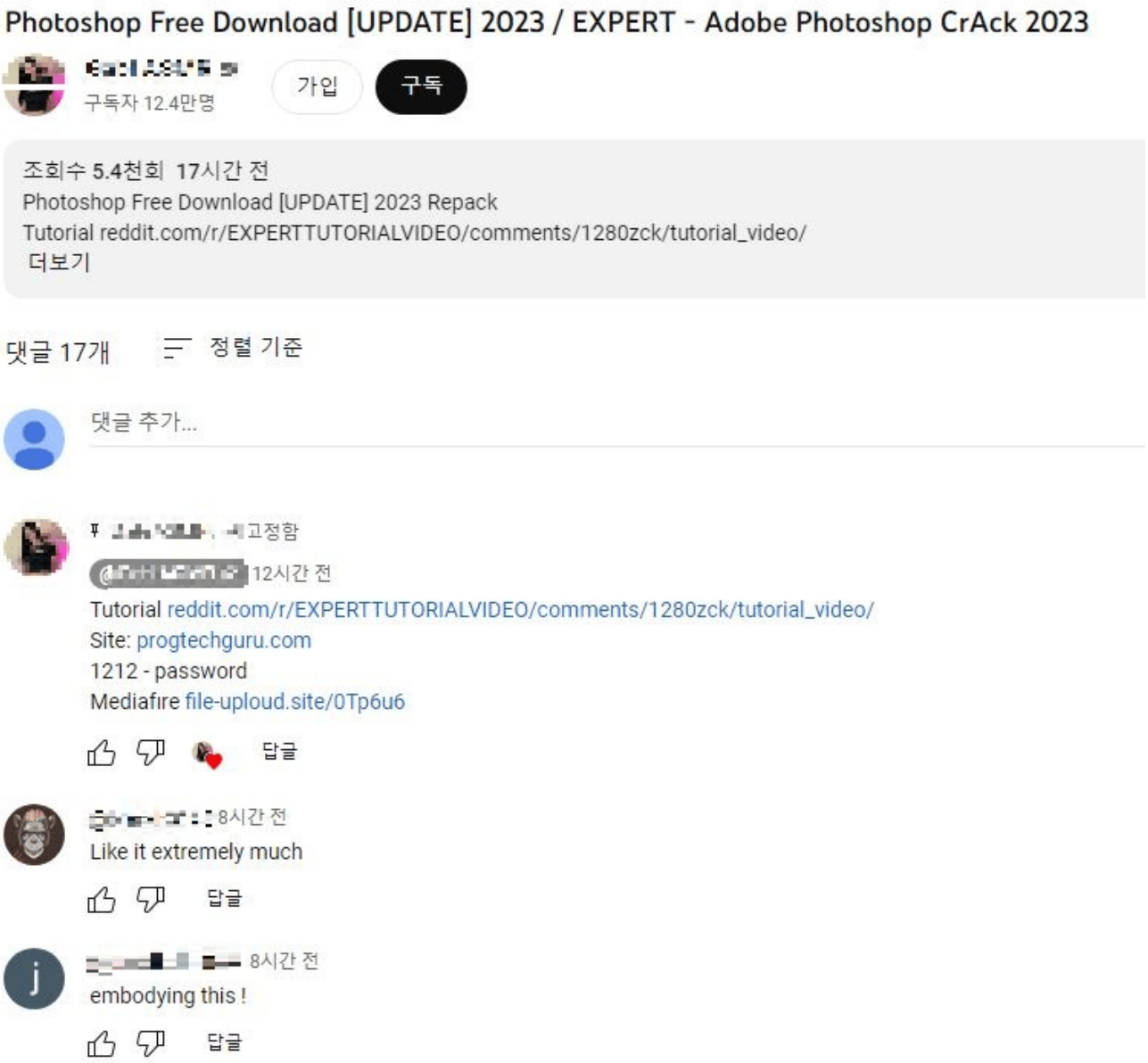

Figure 3. Malware download link uploaded by the threat actor with the YouTube video

The distribution of malware through YouTube is a common method, and most threat actors create new accounts to upload malware links. However, this account currently has more than 120,000 subscribers. Additionally, considering that the original owner had been uploading videos regularly just a few days before the malware distribution videos were uploaded, it is assumed that the threat actor had stolen the YouTuber's account before using it to upload malware.

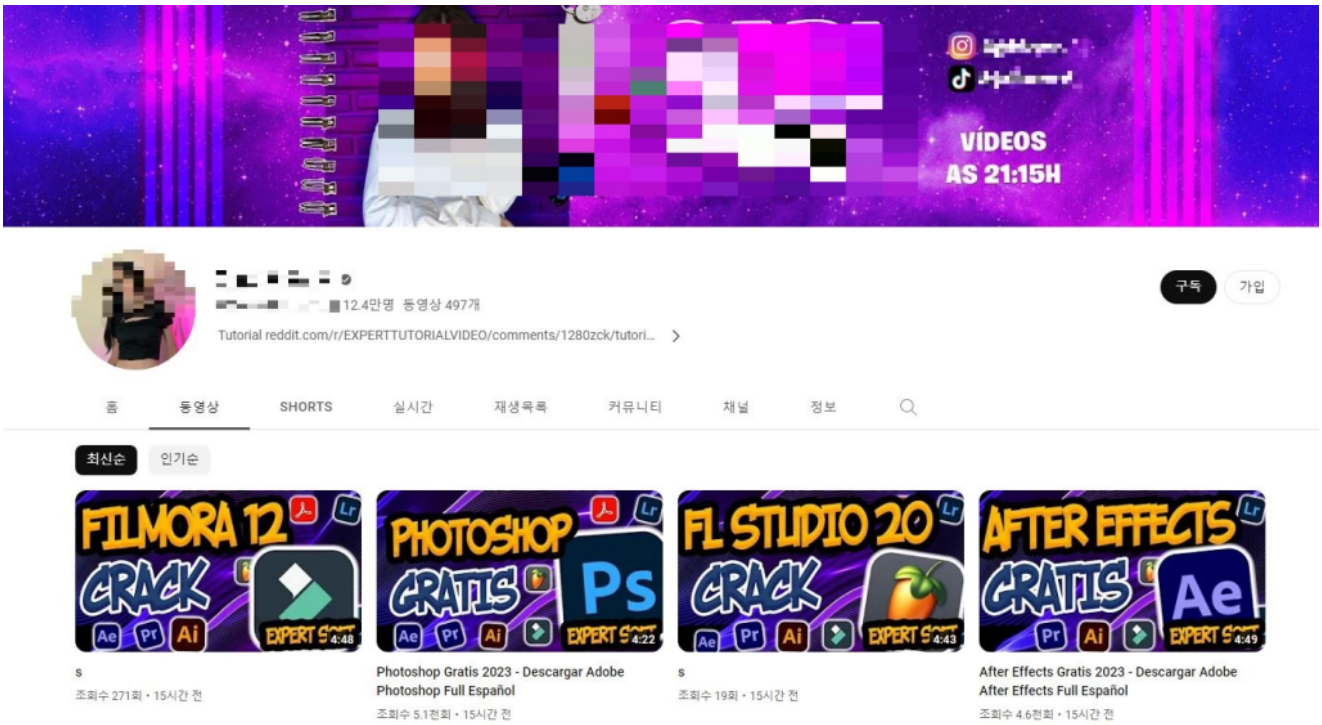

Figure 4. Account used to distribute malware.

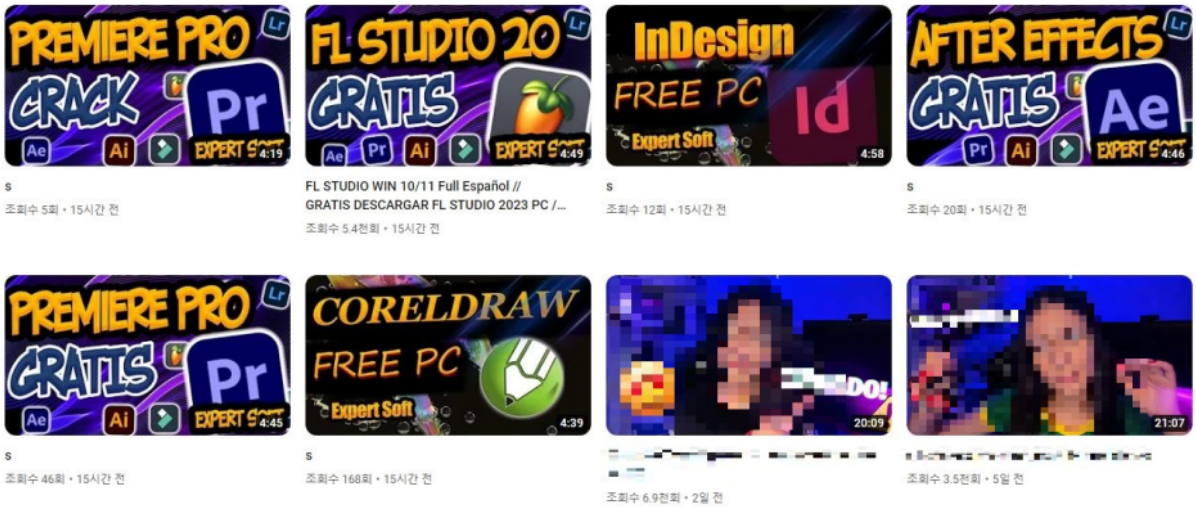

Figure 5. Videos uploaded by the threat actor along with the videos from the original owner

Clicking on the links in the YouTube videos lead to a MediaFire download page, where users can download a compressed file that has malware inside of it. Similar to previous cases, the downloaded compressed file is encrypted with a password.

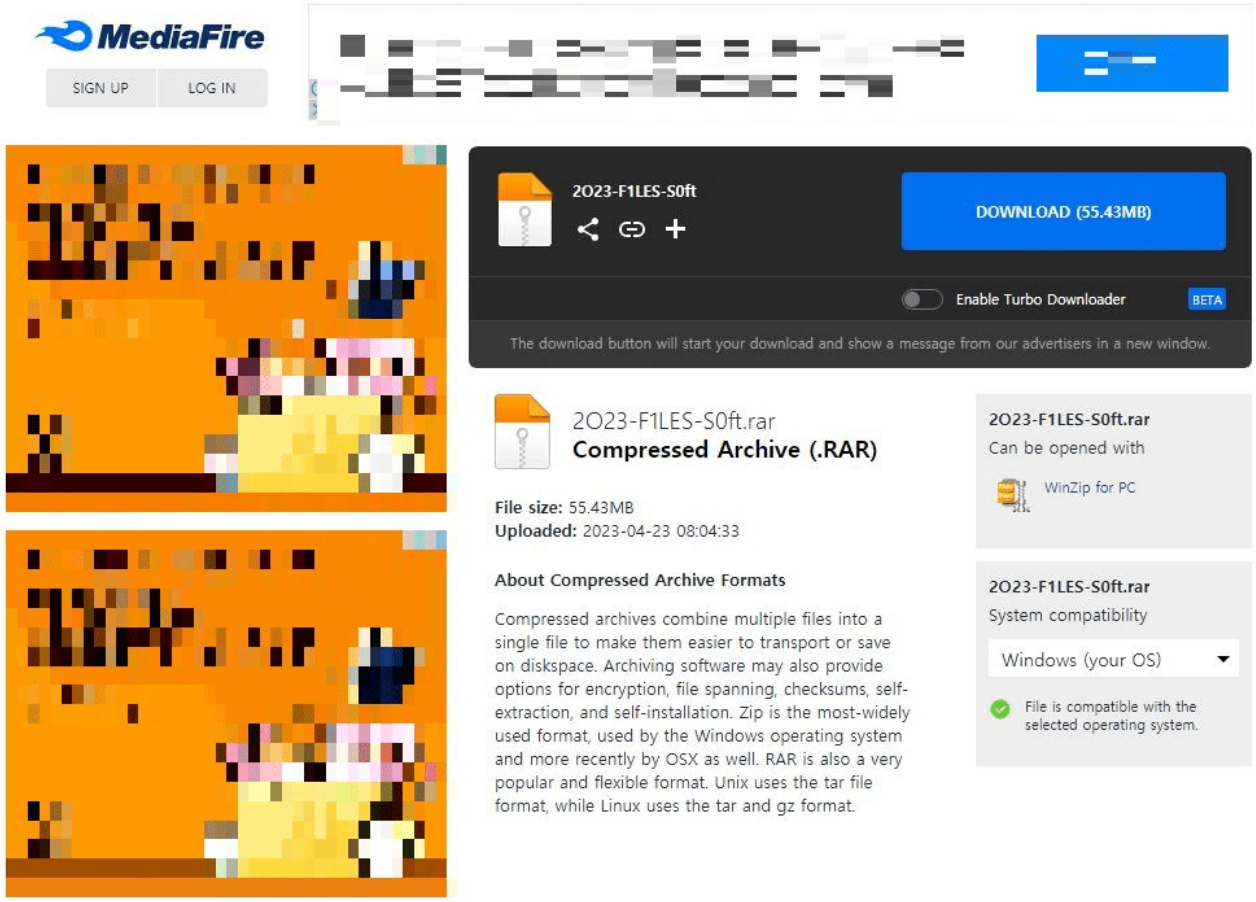

Figure 6. MediaFire download page

3. RecordBreaker Analysis

Just like in the prior cases, decompressing the compressed file creates an executable that is more than 700 MB called “Launcher_S0FT-2O23.exe”. The threat actor had deliberately padded this file immensely to make it appear bigger. It is assumed that this is to evade being collected and detected by security products.

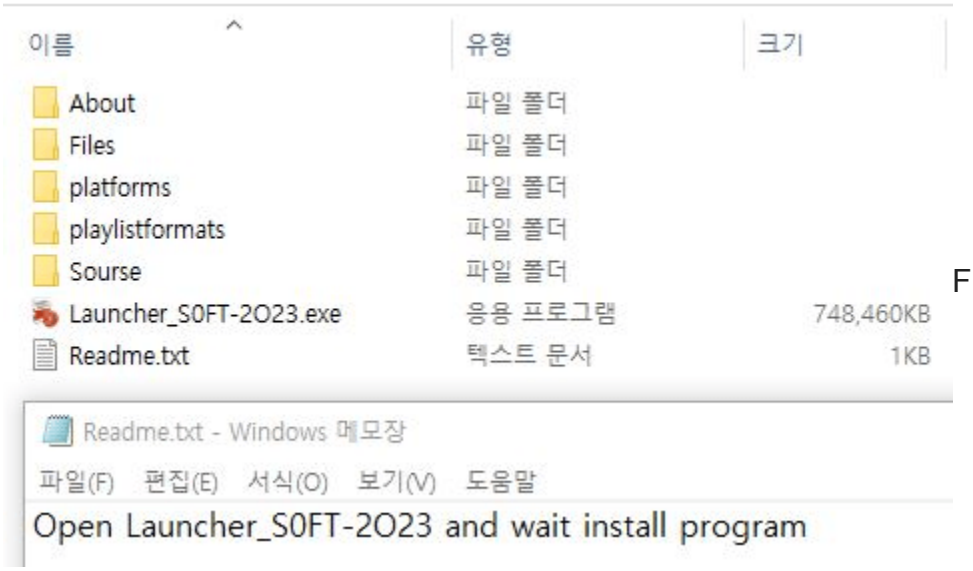

Figure 7. Malware created after decompression

"Launcher_S0FT-2O23.exe" is the RecordBreaker Infostealer malware that accesses the C&C server upon execution to download the DLL files required for configuration and information theft.

Result	Protocol	Host	URL	Body	Content-Type	Comments
200	HTTP	212.113.119.153	/	7,581	text/html; charset=utf-8	Get Config
200	HTTP	212.113.119.153	/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll	2,042,296	application/octet-stream	Download DLL (nss3.dll)
200	HTTP	212.113.119.153	/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll	449,280	application/octet-stream	Download DLL (msvcp140.dll)
200	HTTP	212.113.119.153	/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll	80,128	application/octet-stream	Download DLL (vcruntime140.dll)
200	HTTP	212.113.119.153	/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll	627,128	application/octet-stream	Download DLL (mozglue.dll)
200	HTTP	212.113.119.153	/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll	684,984	application/octet-stream	Download DLL (freebl3.dll)
200	HTTP	212.113.119.153	/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll	254,392	application/octet-stream	Download DLL (softokn3.dll)
200	HTTP	212.113.119.153	/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll	1,099,223	application/octet-stream	Download DLL (sqlite3.dll)
200	HTTP	212.113.119.153	/5006502f0954e90dd25e67b048931fcb	8	text/html; charset=utf-8	Send collected data #1
200	HTTP	212.113.119.153	/5006502f0954e90dd25e67b048931fcb	8	text/html; charset=utf-8	Send collected data #2
200	HTTP	212.113.119.153	/5006502f0954e90dd25e67b048931fcb	8	text/html; charset=utf-8	Send collected data #3
200	HTTP	212.113.119.153	/5006502f0954e90dd25e67b048931fcb	8	text/html; charset=utf-8	Send collected data #4
302	HTTPS	github.com	/jesus061031r/mooliik/releases/download/mooliik/vfdcs.exe	0	text/html; charset=utf-8	Download Payload #1
200	HTTPS	objects.githubusercontent.com	/github-production-release-asset-2e65be/630157753/f3e269b...	316,240	application/octet-stream	Download Payload #1 - CoinMiner
302	HTTPS	github.com	/jesus061031r/mooliik/releases/download/mooliik/GUI_MODER...	0	text/html; charset=utf-8	Download Payload #2
200	HTTPS	objects.githubusercontent.com	/github-production-release-asset-2e65be/630157753/d00390b...	49,152	application/octet-stream	Download Payload #2 - Crack

Figure 8. Network behavior of RecordBreaker

When RecordBreaker is executed, it obtains the "machineId" and sends the "configId" value that is hard-coded into the malware to the C&C server. Afterward, the C&C server sends back the following configuration data. The data received includes URLs that will be used to download specific DLL files that are necessary for stealing information, along with the path for the files that are going to be stolen.

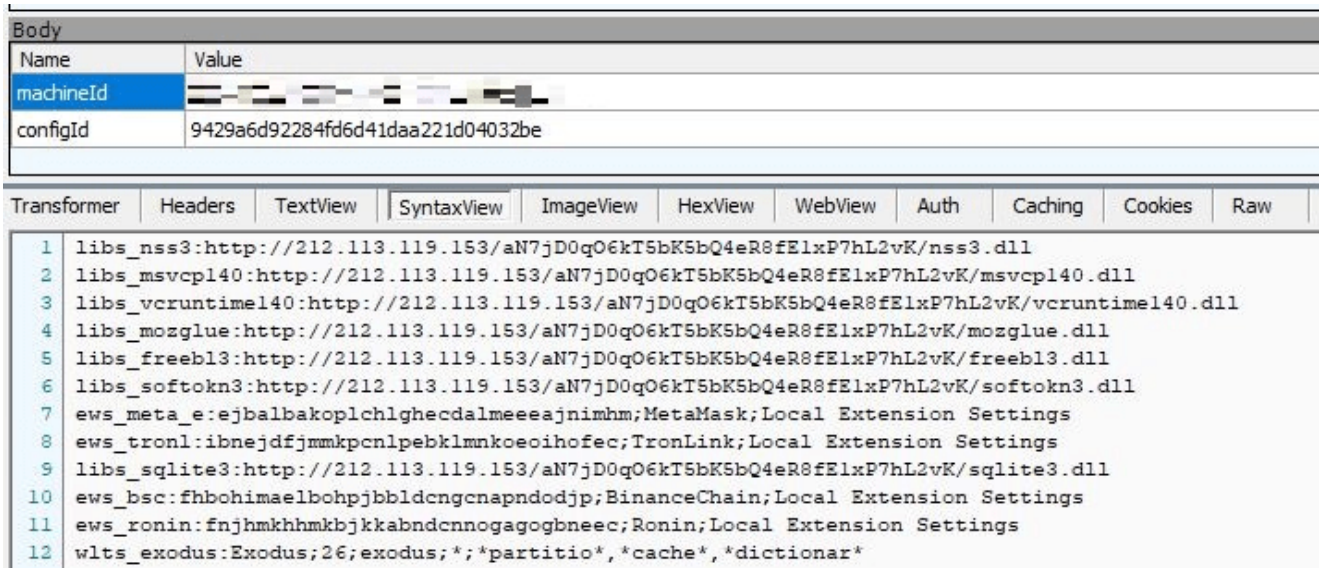

Figure 9. Configuration data received from the C&C server

RecordBreaker collects and steals various information saved on a system, such as basic system information, a list of installed programs, screenshots, account credentials saved on a browser, etc., and it is also capable of downloading and installing additional payloads at the end. The below Fiddler log shows two payloads, which have been uploaded to GitHub, being downloaded and executed.

```
tlgrm_Telegram:Telegram Desktop\tdata|*|*emoji*,*user_data*,*tdummy*,*dumps*
dscrd_Discord:discord\Local Storage\leveldb|*.log,*.ldb|-
grbr_Desktop:%USERPROFILE%\Desktop\|*.txt|*recycle*,*windows*|10|1|1|files
grbr_Documents:%USERPROFILE%\Documents\|*.txt|*recycle*,*windows*|10|1|1|files
ldr_1:https://github.com/jesus061031r/mooliik/releases/download/mooliik/vfdcs.exe|%APPDATA%\|exe
ldr_1:https://github.com/jesus061031r/mooliik/releases/download/mooliik/GUI_MODERNISTA.exe|%TEMP%\|exe
token:5006502f0954e90dd25e67b048931fcb
```

Figure 10. Path for files to be stolen and URLs for additional payloads to be downloaded

Among the downloaded files, “GUI_Modernista.exe” is a program that provides the ability to download various crack files. This causes users to believe that they have downloaded a normal crack program, making it difficult for them to notice the installation of malware.

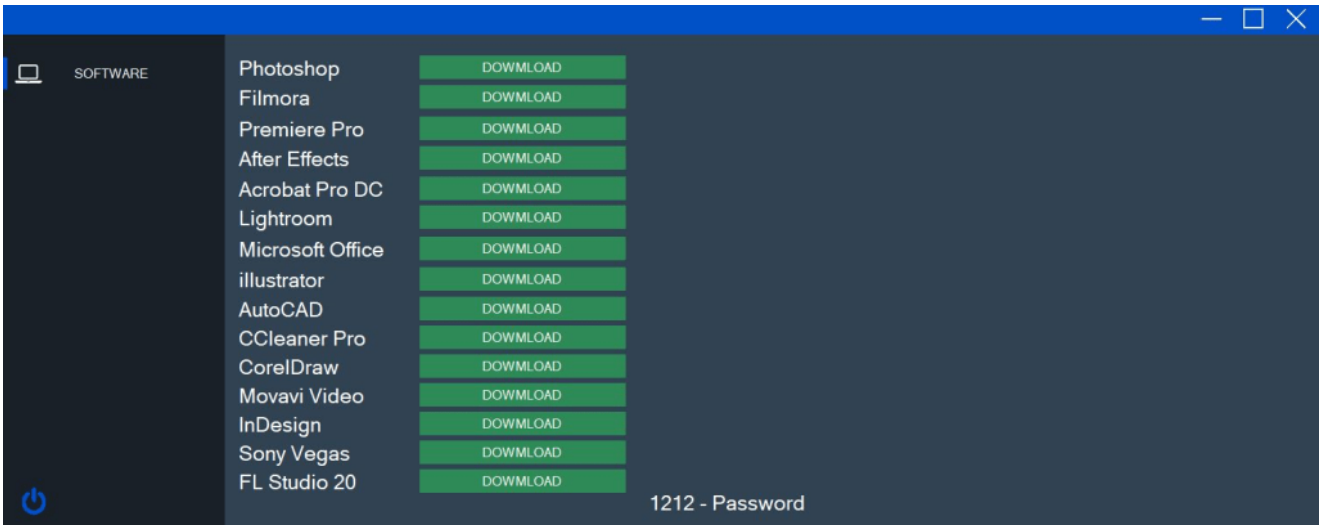

Figure 11. Downloaded and executed crack programs

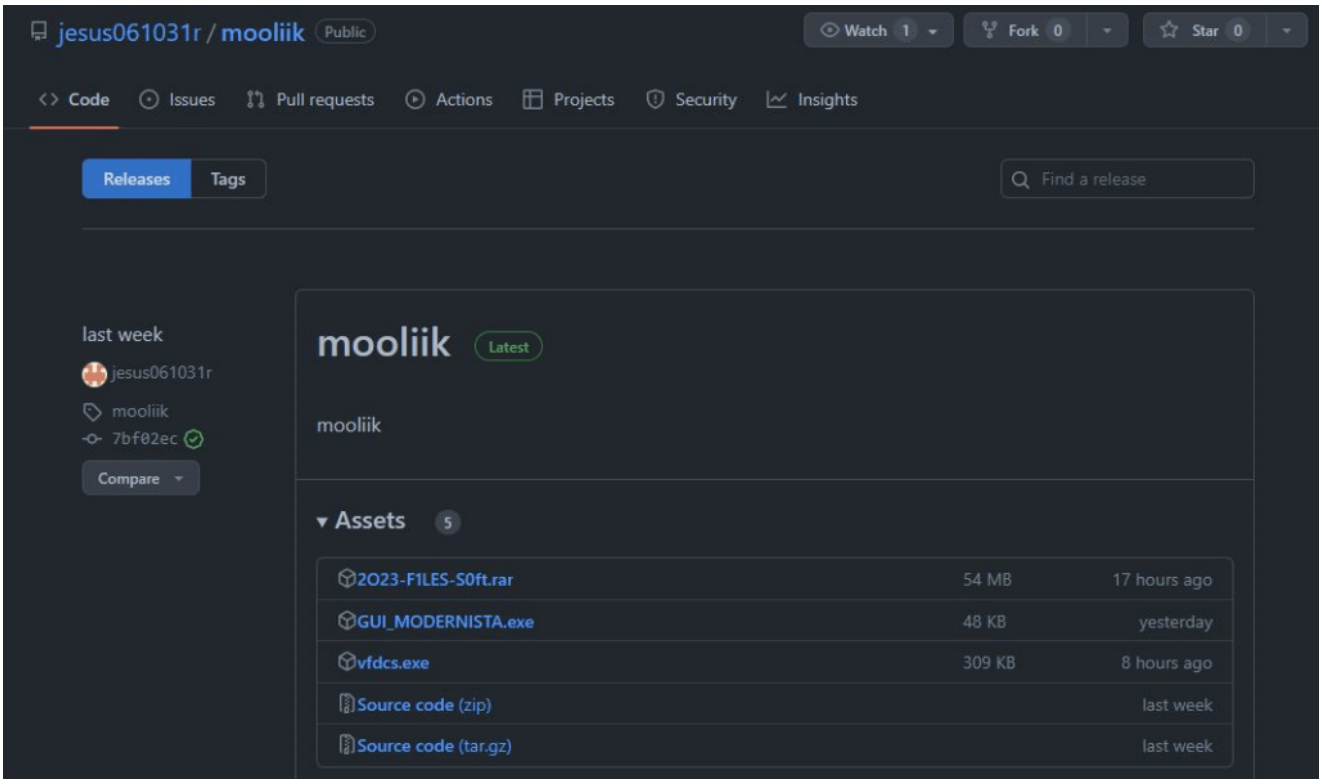

Figure 12. Malware uploaded to GitHub

After collecting information from the infected system, the threat actor installs a CoinMiner using a malware file named “vdcs.exe” and uses the system’s resources to mine cryptocurrency.

4. Conclusion

A case has been confirmed recently of RecordBreaker being distributed via YouTube. RecordBreaker is an Infostealer that collects and steals various user information saved inside infected systems. It can also download and install additional malware.

RecordBreaker was distributed through an account that has over 100,000 subscribers. Based on the account’s activity prior to the distribution, it is believed that it was hacked by a threat actor. The threat actor used RecordBreaker to collect information from infected systems and installed CoinMiner to mine for cryptocurrency on the infected systems afterward.

As explained in this post, malware can be installed through various platforms, therefore, users should refrain from downloading illegal programs and using suspicious websites or P2P and use genuine software at all times. Also, V3 should be updated to the latest version so that malware infection can be prevented.

ASEC selects malware with the highest distribution rate each week through the Live C&C information of AhnLab TIP, and provides the C&C information that have been confirmed through an automatic analysis system. The URL and IP information assumed to be C&C

servers can be used to assist with malware analysis and response.

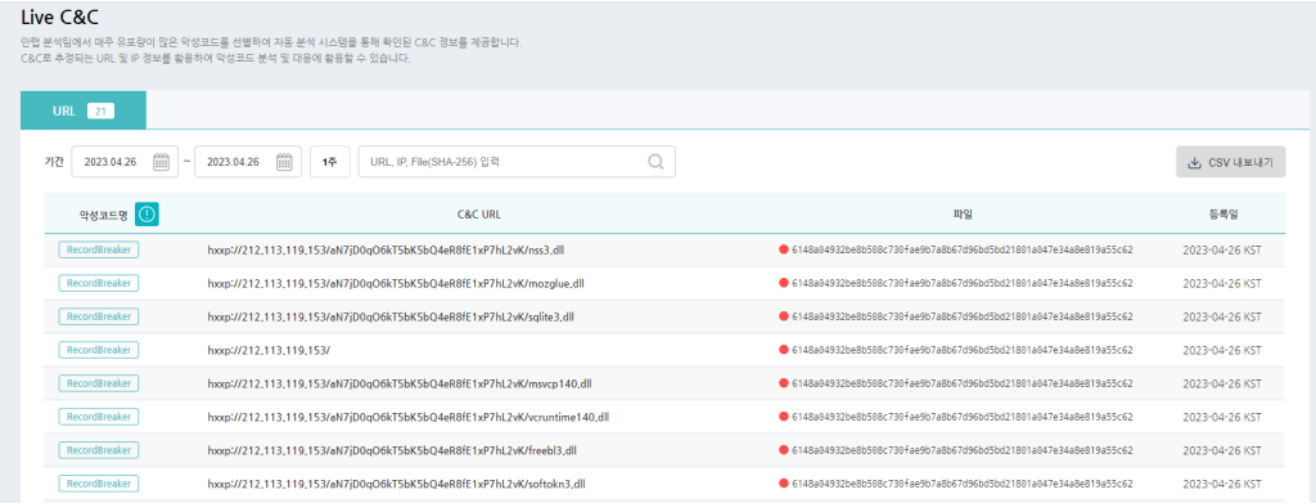

Figure 13. RecordStealer C&C URLs as seen in the AhnLab TIP Service's Live C&C

File Detection

– Infostealer/Win.RecordStealer.C5410598 (2023.04.13.02)
– Trojan/Win.Generic.C5403811 (2023.04.01.03)
– Trojan/Win.MSILKrypt.C5418981 (2023.04.27.03)

IOC

MD5

– 1cc87e637e55a2e6a88c745855423045 – RecordBreaker (Launcher_S0FT-2O23.exe)
– 116857ca1574a5a36da3bb0ddff32eac – Crack Downloader (GUI_MODERNISTA.exe)
– 803a1f3e984a9eaa56ac74a203096959 – CoinMiner (vdsds.exe)

Download URLs

– hxxps://www.mediafire[.]com/file/0u0tldiluood47v/2O23-F1LES-S0ft.rar – Compressed File
– hxxp://212.113.119[.]153/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll – Normal DLL used for information collection
– hxxp://212.113.119[.]153/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll – Normal DLL used for information collection
– hxxp://212.113.119[.]153/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll – Normal DLL used for information collection
– hxxp://212.113.119[.]153/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll – Normal DLL used for information collection
– hxxp://212.113.119[.]153/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll – Normal DLL used for information collection
– hxxp://212.113.119[.]153/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll – Normal DLL used for information collection
– hxxp://212.113.119[.]153/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll – Normal DLL used for information collection
– hxxps://github[.]com/jesus061031r/mooliik/releases/download/mooliik/vdsds.exe –

CoinMiner
–
hxxps://github[.]com/jesus061031r/mooliik/releases/download/mooliik/GUI_MODERNISTA.exe
– Crack Downloader

C&C URL
– hxxp://212.113.119[.]153/ – RecordBreaker

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:recordbreaker,Youtube