Distribution of Redline Stealer Disguised as Software Crack - ASEC

By ATCP

Published: 2022-12-28 · Archived: 2026-04-05 13:14:03 UTC

In the previous blog post, the AhnLab ASEC analysis team has mentioned malware that is searched through keywords such as cracks and serials of commercial software, urging users to take caution.

While investigating a recent breach case of the internal network of a certain company, the team has discovered that the company was infected with Redline Stealer disguised as a crack for commercial software and had its VPN website and account credentials leaked.

The company where the damage occurred provided VPN service to employees who were working from home to give access to the company's internal network, and the employees connected to the VPN on the provided laptops or their PCs. The targeted employee used the password management feature provided by the web browser to save and use the account and password for the VPN website on the web browser. While doing so, the PC was infected with malware targeting account credentials, leaking accounts and passwords of various websites, which also included the VPN account of the company.

The system that had the account credentials leaked is the employee's PC, which is also used by the employee's family members for other purposes. One of the family members searched for SoundShifter, a pitch-shifting

program from Waves, with the keywords free and crack. The user then downloaded waves_60e87ffe7200b.zip file, which had a malicious file included, then executed the malicious and system was infected.

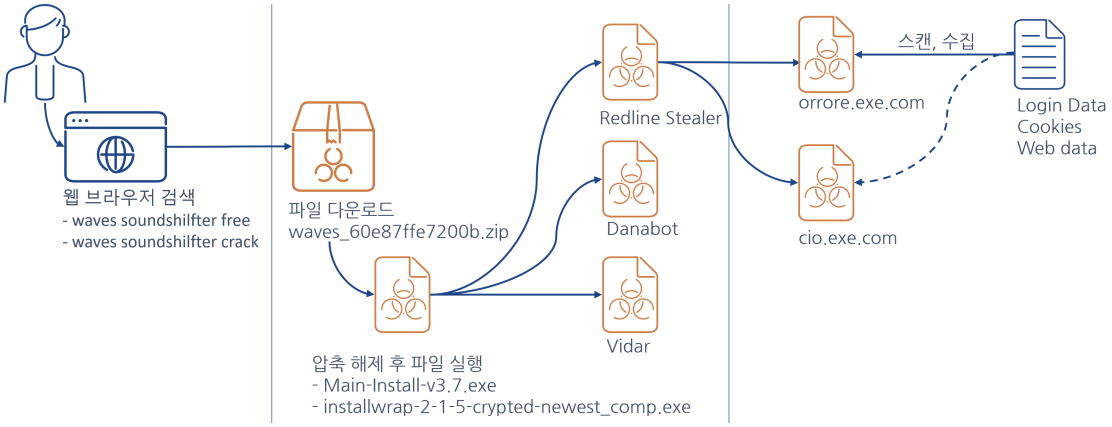

Figure 1. Infection process of malicious file

The team has discovered the search history of the keywords waves soundshifter free and waves soundshifter crack from the web browser history.

항목	날짜 및 시간	유형
https://poshukach.com/search?q=waves+soundshifter+free&fr=ps&gp=496721&altserp=1		잠재적 브라우저 활동
https://poshukach.com/search?q=waves+soundshifter+free&fr=ps&gp=496721&altserp=1p		잠재적 브라우저 활동
https://www.google.co.kr/search?q=waves+soundshifter+crack&ei=UH_oYIHhKtichwODgImoCQ&oq=waves+soundshifter+crack&gs...	2021/07/10 01:57:06	WebKit 브라우저 웹 기록 (카빙)

Figure 2. Traces of searching illegal software in web browser

Searching the keywords on Google shows various download websites on the search results.

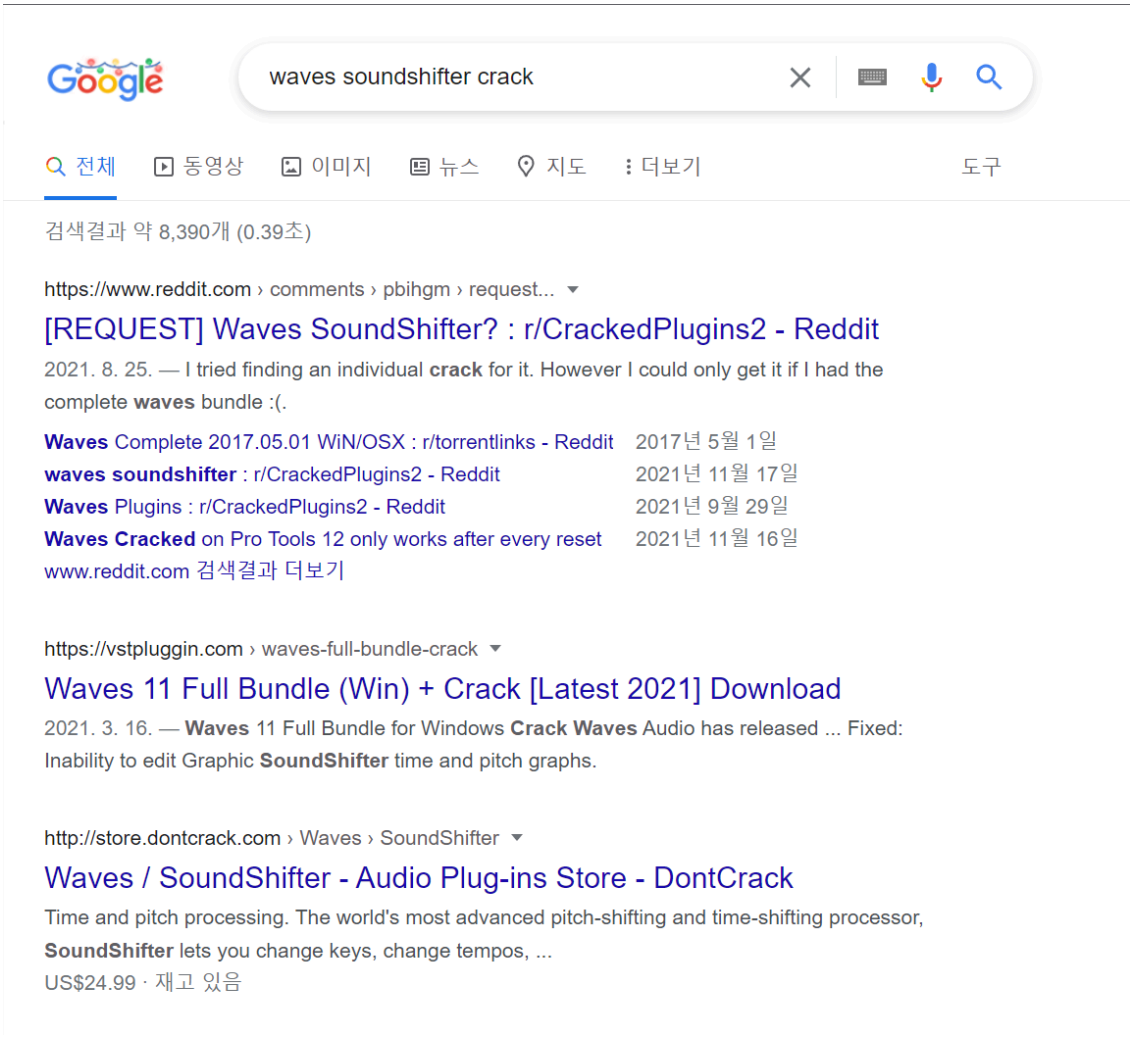

Figure 3. Google search results for waves soundshifter crack

It seems that the user visited multiple pages shown on the search result.

호스트	이름	액세스한...	생성한 날짜/...	만료 날짜/시간
store.dontcrack.com	__atuvc	2021/07/10 01:55:45	2021/07/10 01:55:45	2022/08/10 01:55:45
www.waves.com	waves_abtest_server	2021/07/10 02:00:54	2021/07/10 01:54:48	
.lf-recrenew-soundshifterpitchvstdownload.peatix.com	_ga	2021/07/10 02:01:49	2021/07/10 01:54:14	2023/07/10 01:54:14

Figure 4. Browsing history of websites shown on Google search results

There was also a trace of file download. As the process for visiting the download page was not confirmed, it appears that the user manually accessed the malicious page shown on the search results. However, current search result does not show whether it is possible to do so.

다운로드 소스	파일 이름	시작 시간 날짜/시간	종료 시간 날짜/시간
http://18.188.253.6/0f00f1c348c012f0a73892100e67...	waves_60e87ffe7200b.zip	2021/07/10 01:57:38	2021/07/10 01:57:43

Figure 5. Trace of downloading illegal software

The downloaded file is a compressed file that contains an encrypted compressed file and a TXT file that has the password for decompression. Such a method is used by attackers to bypass anti-malware detection that is run when the file is downloaded.

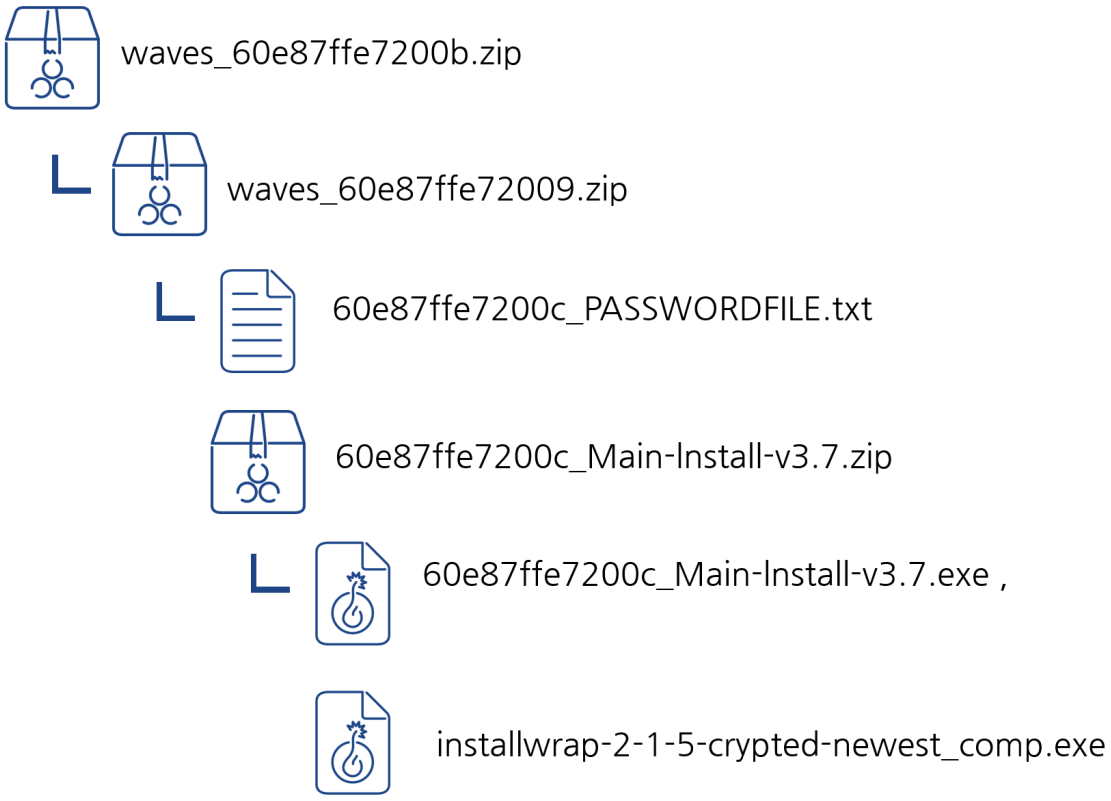

Figure 6. Internal structure of downloaded compressed file (waves_60e87ffe7200b.zip)

As the user downloaded the file to install the software, the user would have read and followed the description written on TXT file, decompressing the encrypted file and executing the malicious file disguised as an installer. The decompressed installer has multiple malicious files inside. When it is installed, malicious files such as Danabot, Redline Stealer, and Vidar are created in the system. Analyzing the malicious files found in the system and related artifacts such as file path and file name showed that there were other nearly identical files distributed during a similar period.

Such cases also had malicious files disguised as installers of illegal software such as cracks or keygens that were distributed by being uploaded on file-sharing websites. Among similar malicious files we found, the analysis result and many behaviors (folder path of a malicious file created in the personal PC, folder name, naming rules of a malicious file, file creation order, etc.) of the malicious file distributed in the Keygen sharing website (topkeygen.com) on June 2021 match those of the file discussed in this post.

The following figure shows a similarity of the location that the file is created.

Figure 7. Similarity in file created location between malicious file in breached personal PC and malicious file distributed in topkeygen

After the malicious file was executed, the breached personal PC had traces of suspicious files being run such as cio.exe.com, orrore.exe.com, and certe.exe.com. But they could not be secured as they were deleted after being run. Considering that the traces discovered in the system are similar to those of the system infected with Redline Stealer type, it seems that the malicious files all fall into the same category.

Traces of possible Redline Stealer infection confirmed in the system

- Using findstr.exe
- Using 7Zip SFX compressed file (path: %Temp%\7ZipSfx.000\)
- Name of malicious file (cio.exe.com)
- Using double file extensions (.exe.com)
- Scanning and collecting web browser credentials (Chrome, Login Data of Edge browser, Cookies, and Web Data)

As for scanning web browser credentials, Microsoft Windows Defender's log file MPLog detected a trace of the Login Data file recorded with account names and password of the web browser being scanned by Orrore.exe.com on July 10th.

```
2021-07-10T10:30:43.941Z ProcessImageName: Orrore.exe.com, Pid: 14764, TotalTime: 60,
Count: 15, MaxTime: 15, MaxTimeFile: \Device\Mup\localhost\c$\Users\[redacted]\AppData\
Local\Google\Chrome\User Data\Default\Login Data, EstimatedImpact: 18%
```

Figure 8. Trace of Orrore.exe.com accessing Login Data (MPLog-20210710-015710.log)

The account credentials saved on the website were leaked by Redline Stealer, and the list of accounts that were leaked includes the VPN website of the company and account & password credentials.

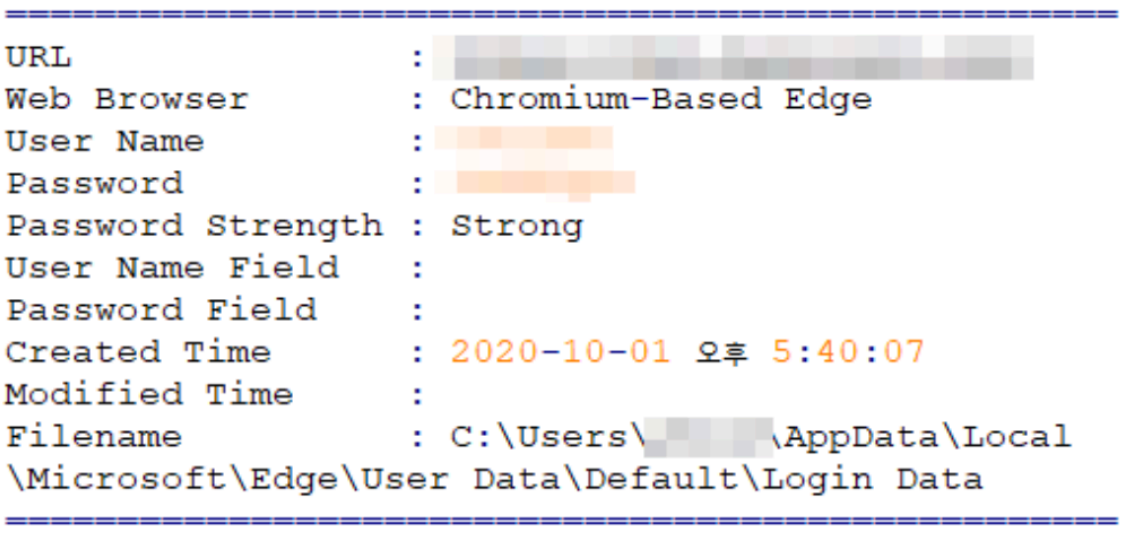

Figure 9. VPN website and account and password credentials saved in Login Data

The leaked account was used to breach the internal network of the company several months later.

FQDN

certe[.]exe[.]com

cio[.]exe[.]com

orrore[.]exe[.]com

Additional IOCs are available on AhnLab TIP.

IP

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/30445/