CRYPTBOT

Teknik Analiz Raporu

İÇİNDEKİLER

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 ağımıza 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

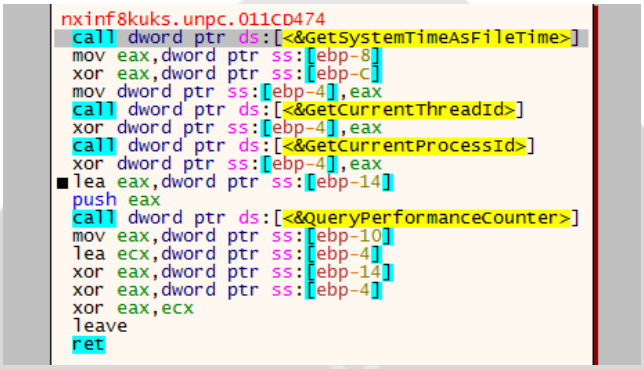
İncelenen bu versiyondaki CryptBot zararlısı 2021-06-27 tarihinde ortaya çıkmıştır. Lisanssız uygulamalarla birlikte inerek yayılmayı sürdürmüştür. İlk olarak zararlının uzantısı .exe olup bu uzantı ile bulaşmaktadır.Ana exe çalıştıktan kısa bir süre sonra 2 alt process açıp kendini bulunduğu konumdan 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 decyrpt 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

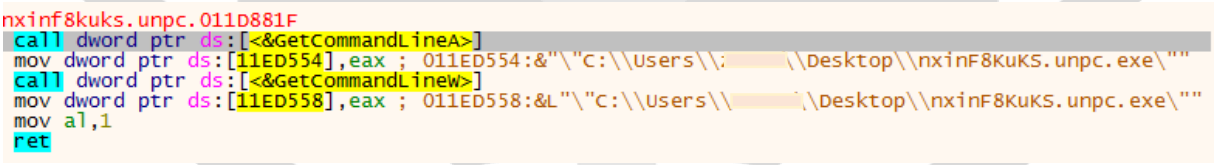
DOSYA ADI	nxinf8kuks.exe
MD5	663FDF847D6B11308415FF86EBFFC275
SHA1	6167FDF3CD9A585A44F24EB15D414281EDAD2485

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

İlk olarak sistem ile ilgili bilgileri almaktadır.

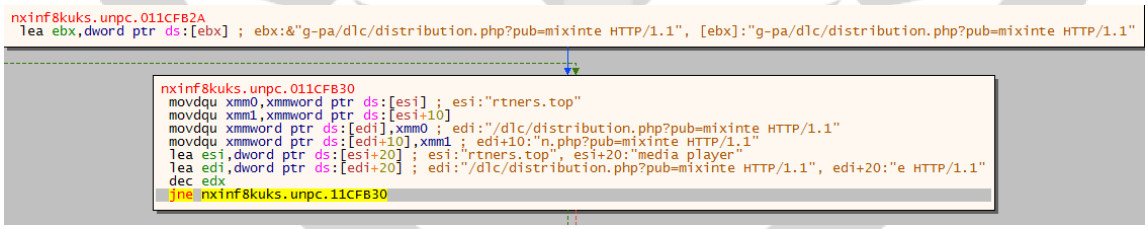


GetCommandLineA ile process oluşturmak için ve değişiklikler yapmak için komut satırı dizinini almaktadır.

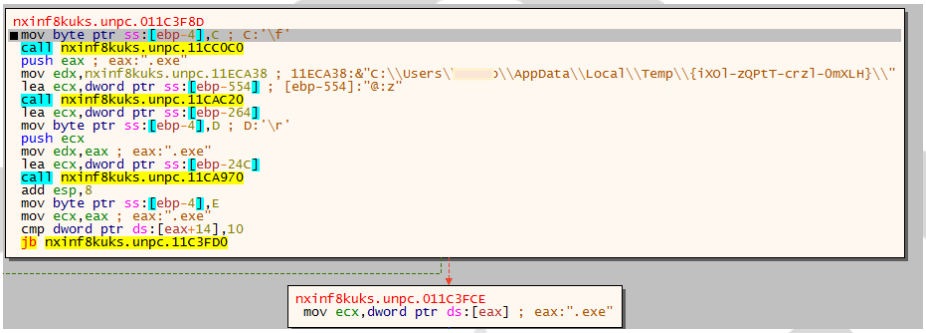


Api-ms-win-core-synch-l1-2-0.dll dosyası, dinamik bağlantı kitaplığı dosyaları gibi yürütülebilir (exe) dosyaları için bilgileri ve talimatları kaydetmektedir.

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

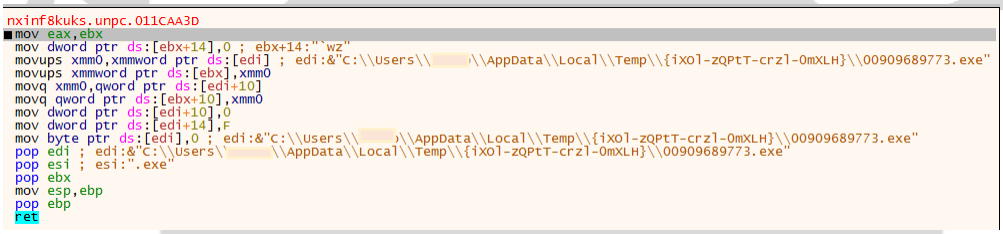


Zararlı hafıza adresini uzak sunucudan aldığı EXE dosyasında tutmakta ve C:\Users\name\AppData\Local\Temp\{{iXOl-zQPtT-crzl-0mXLH}}\ dizininin altına bir exe dosyası oluşturmaktadır.



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

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



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

Dosya Adı	79331032056.exe
MD5	2081D43A914A66D1CB5C54FD3802DFB1
SHA1	8958C6E1E2FF8112C31846B706C52FF25028E182

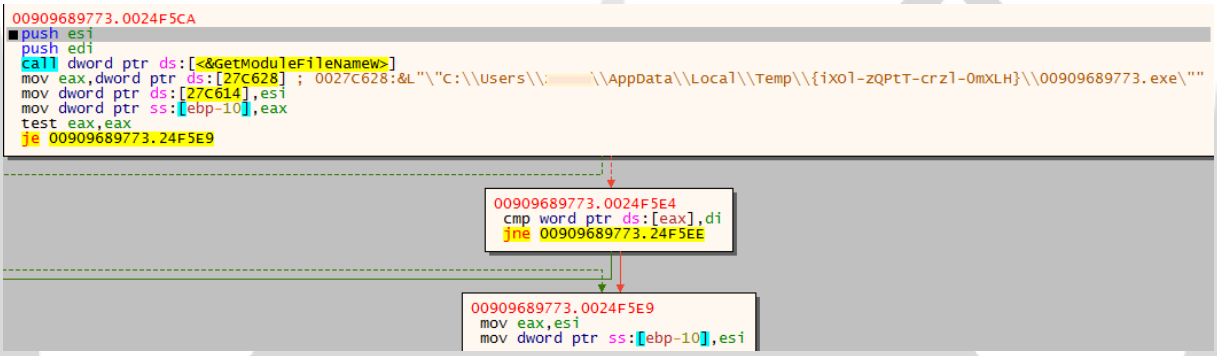
Dosyaları oluşturduktan sonra kendisini silip alt processinde zararlı işlemlerine devam etmektedir.

00909689773.exe Analizi

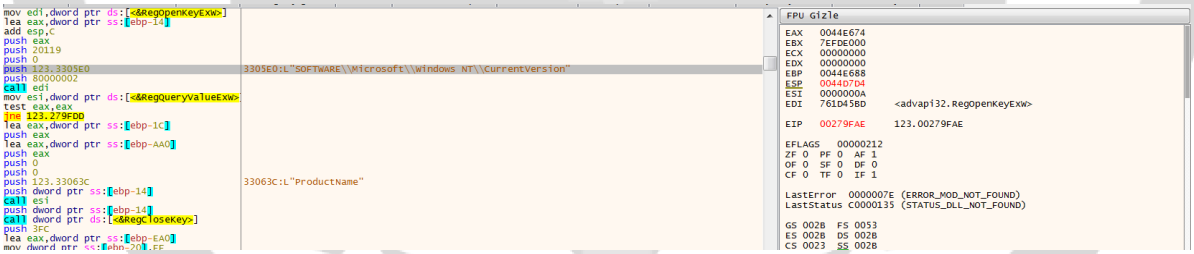
DOSYA	00909689773.exe
MD5	610FE925494BD7F87858672C17F7D917
SHA1	CA63E707905182D88DF434BC83E6094F91AA4D61

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.

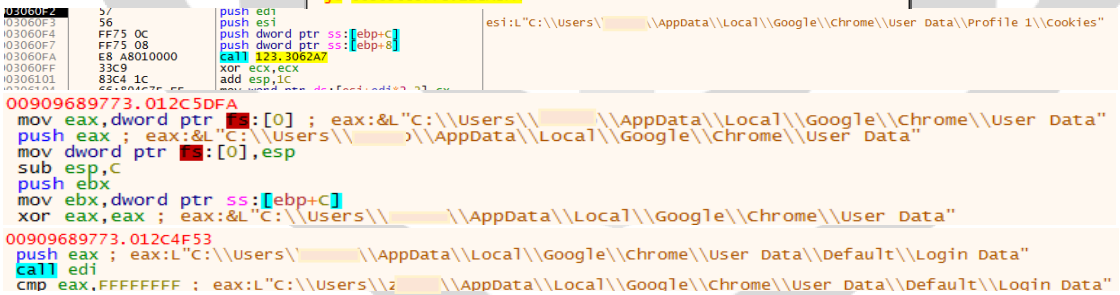


Sistem üzerinde kalıcılık elde etmek için kendisini CurrentVersiona kayıt etmektedir.

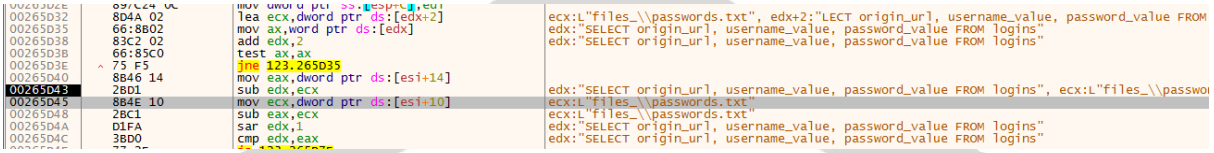


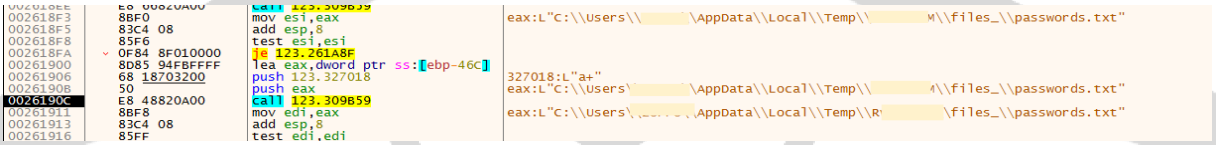
CreateDirectoryW API kullanarak bir temp dizinini alıp bu dizinin handle ının altında rastgele adlandırılmış LYOJYcHurFyK isimli bir dosya oluşturmaktadır.

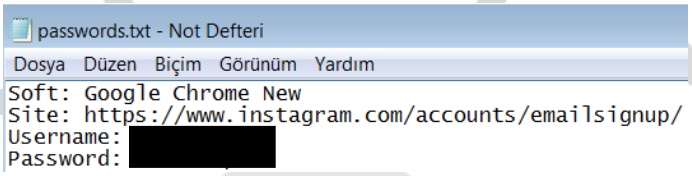
Zararlı sistem üzerindeki tarayıcıların (Chrome,Mozilla Firefox,Internet Explorer) cookie bilgilerini, tarayıcı geçmişini, kaydettiği şifreleri ve e-posta adreslerini almaktadır.



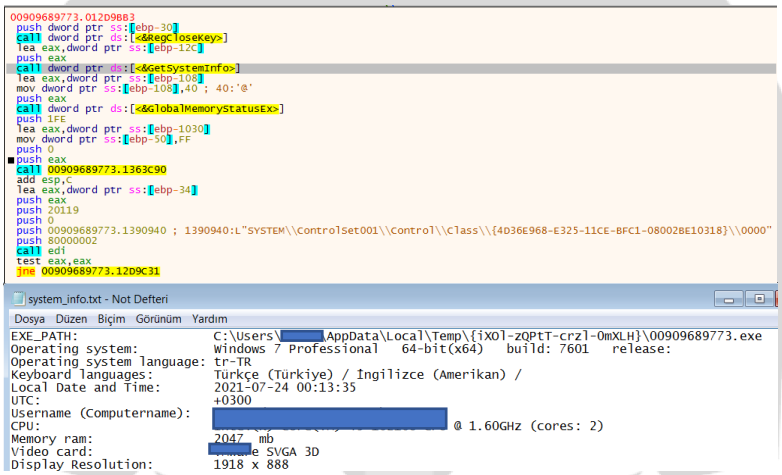
Logins tablosunda bulunan verileri sql sorgusuyla çekmektedir. Kullanıcıya ait kayıtlı şifreler, kullanıcı adları ve url bilgisi hedeflenmektedir. Password_value encrypted şekilde tutulurken zararlı sistem üzerinde decrypt ederek password.txt dosyasına yazmaktadır.



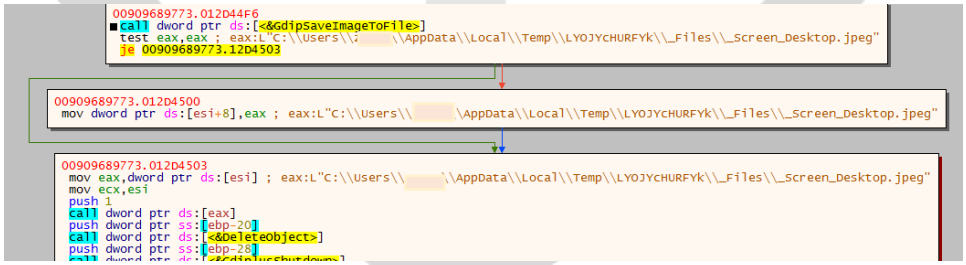




Zararlı sistem bilgilerini (username,computer name,cpu bilgisi,saat ve tarih,kullanılan dil) GetSystemInfo ile alarak oluşturduğu _Information.txt adlı dosyaya yazdırmaktadır.



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



Web Data-Login Data bilgilerini alarak google_chrome_new.txt dosyası oluşturarak içine yazdırmaktır.

```
309AD8    66:391E         cmp word ptr ds:[esi],bx        esi:L"C:\\Users\\:    \\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
```

_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
 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"
```

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.

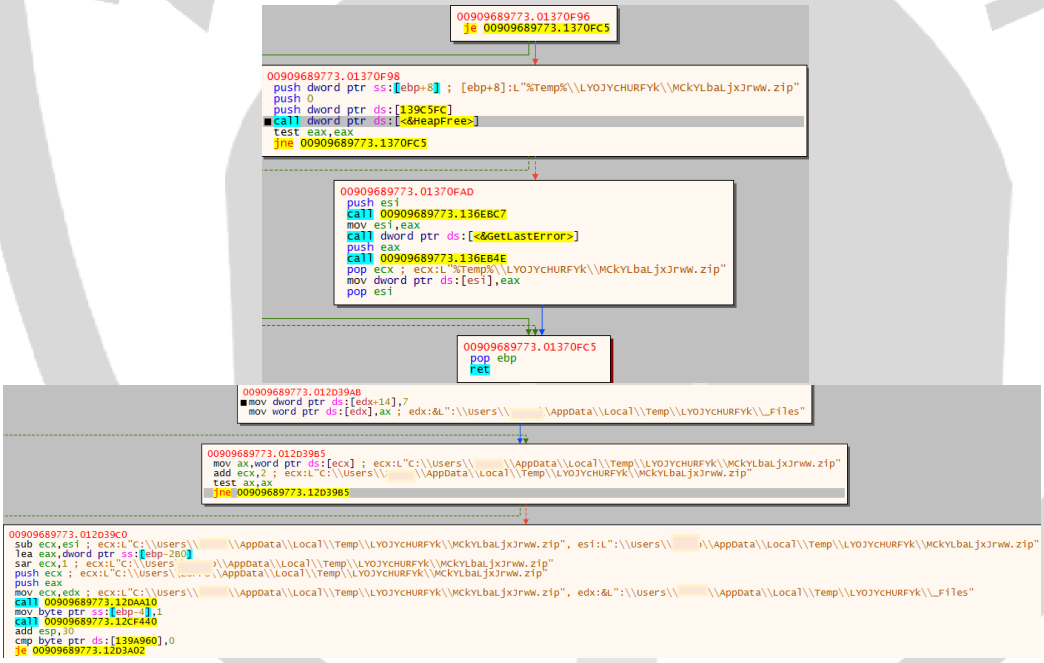
-Tarayıcılarda kayıtlı bulunan tüm şifreleri kullanıcı ismi ve url bilgisiyle birlikte password.txt ve AllPassword.txt dosyalarına kaydetmektedir.

-Tüm e-posta ve kullanıcı isimlerini doğrulama kodları ile birlikte forms.txt ve AllForms_list.txt adlı dosyalara kaydetmektedir.

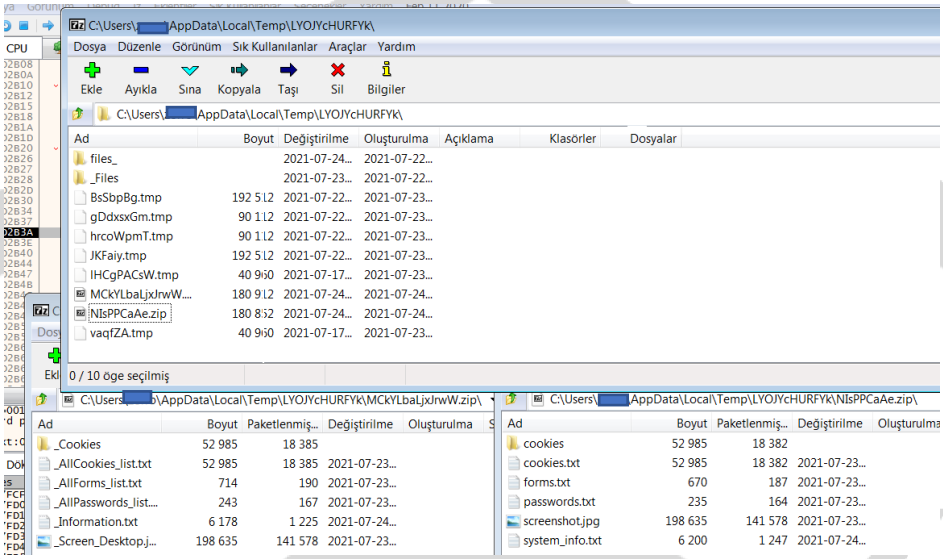
Zararlının oluşturduğu dosyalar aşağıdaki tabloda verildiği gibidir.

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

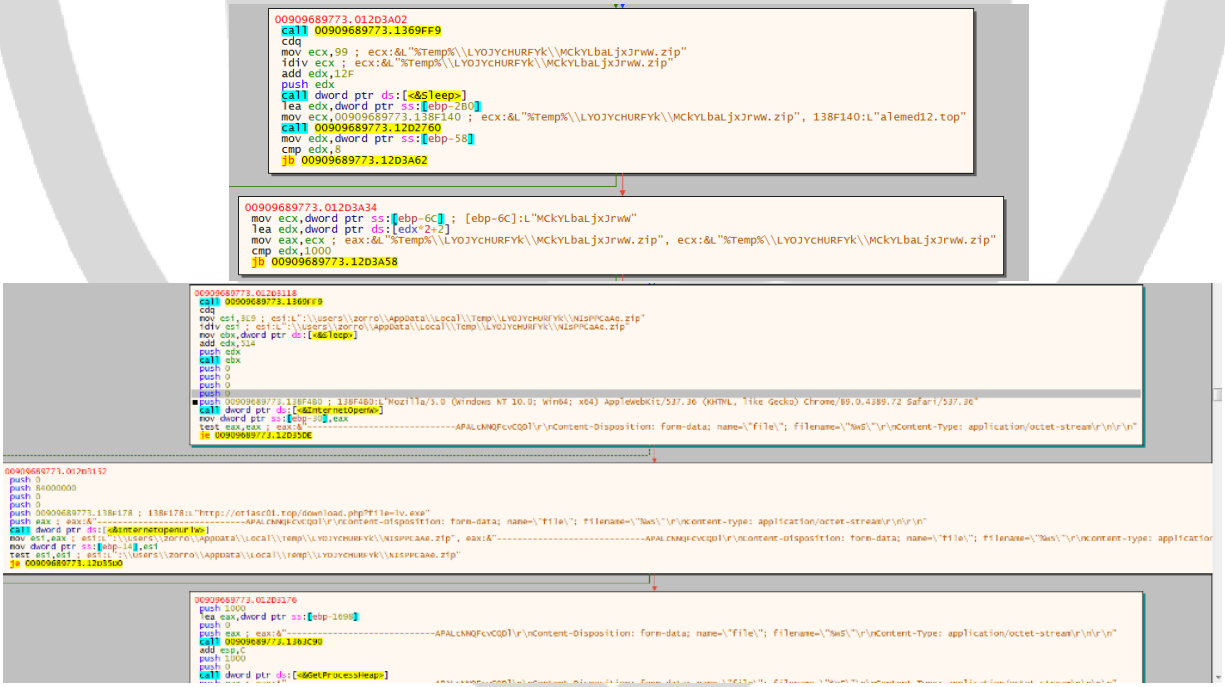
Files_ dosyasında kaydettiği bilgileri MckYLbaLjxJrwWzip adlı dosyasının içine yazdırmaktadır.



MckYLbaLjxJrwW.zip adlı zip dosyasını oluşturduktan sonra _files a kaydettiği bilgilere ait olan NIsPPCaAe isimli bir zip dosyası daha oluşturmaktadır.

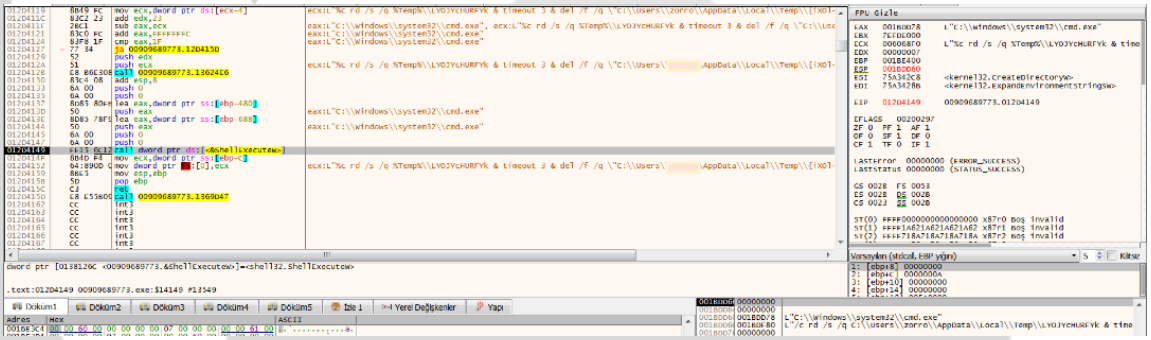


http://alemed12[.]top ile bağlantı kurarak oluşturduğu zip dosyalarını bu adrese göndermektedir.



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

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



lv.exe

Dosya Adı	lv.exe
MD5	1CA90B66B79DF8576C3D35BFAD0F33FA
SHA1	17291F5B80496EFC656A489C340D8856EEC27EE3

lv.exe nin alıştırdığı 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.

Zararlının içerisinde bulunan kripto adresleri aşağıdaki gibidir;

“0x9876A5bc27ff511bF5dA8f58c8F93281E5BD1f21”

“bc1qgvs5jxqqzd68f9u0y5g3xekyeuppnzc8ws5xht”,

“19rxWcjug44Xft1T1Ai11ptDZr94wEdRTz”,

“3J4u4wbwseKXExKC8EdvABkLwXn1gmFdfs”

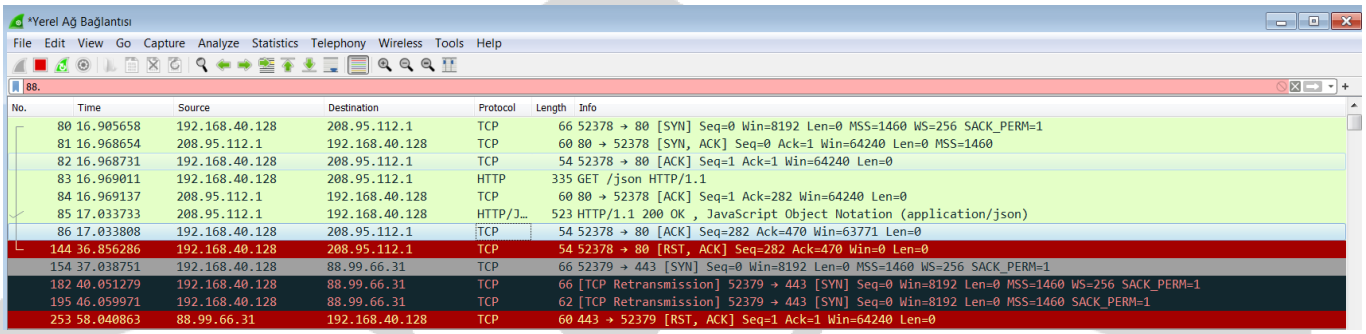
“rHnvqST17xvqhuFkhF1XAL8DMg2EwU5yP7”

“LcW5MfbLwHayuHRL2jJeQN8AXGWC4Bv6Xk”

“43LKVsDuqiDVhxkWwkkyCW2K4J2DrbmH55Rk8qj44JmBTkExo2qRGNceNtMUpnLSZhcKRWHTyNXKjGSPBXRigki35UCYPFP”

“t1Uczn845Pvs36iKUc3BZ4qY7oMc2nRoW2Z”

Network Analizi



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/stats/remember[.]php?pub=mixinte&user

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

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

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

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

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
}
```

KERİME GENÇAY

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