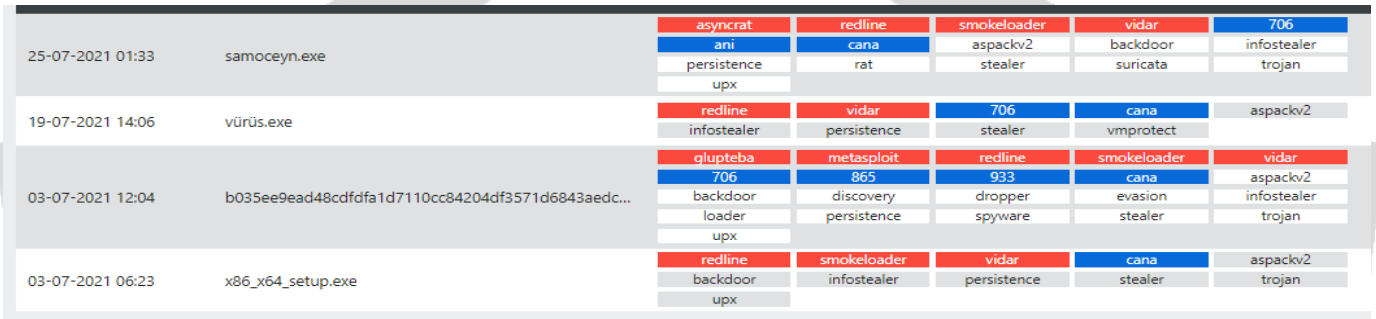
DİAMONDFOX

Technical Analysis Report

Contents

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 L!NK. 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: 9e285901af26b01bafe9afb312620887

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

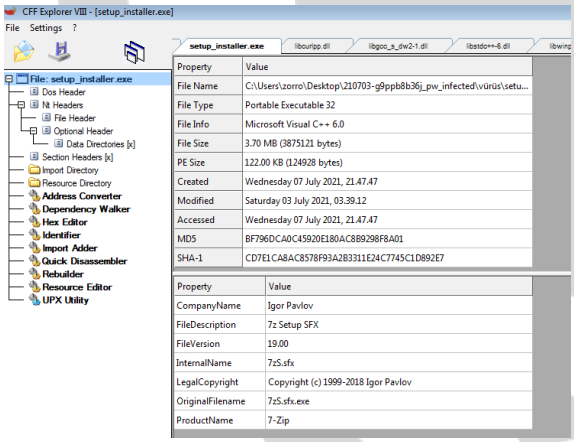
SHA256: 3e70e230daee66f33db3fdba03d3b7a9832088fe88b0b4435d719e185ae8a330

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.

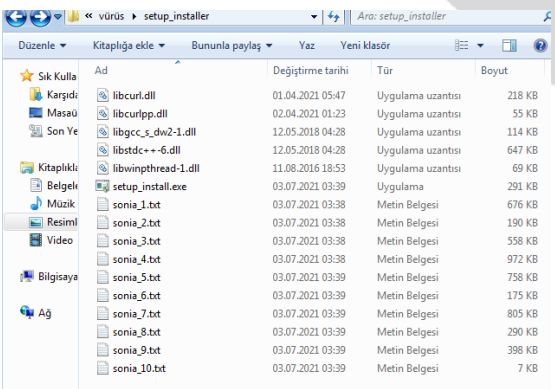
When we open archives sequentially, we see that the exeler, folder and dlls appear in the following order.

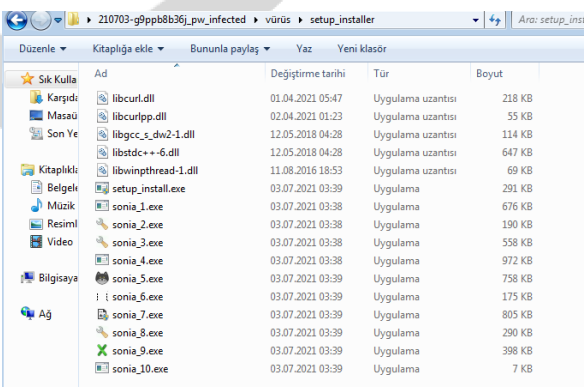
Setup_installer.exe is a setup file configured as 7z setup sfx, as we can see here, and this file contains the files that need to be run directly in it.



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





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 vürüs.401389
C2 0400         ret 4
68 F8AD4000     push vürüs.40ADF8                    40ADF8:L"runas C:\\Users\\zorro\\AppData\\Local\\Temp\\setup_installer.exe"
FF7424 08       push dword ptr ss:[esp+8]
E8 73410000     call vürüs.4055A4
C2 0400         ret 4
55              push ebp
8BEC            mov ebp,esp
```

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.

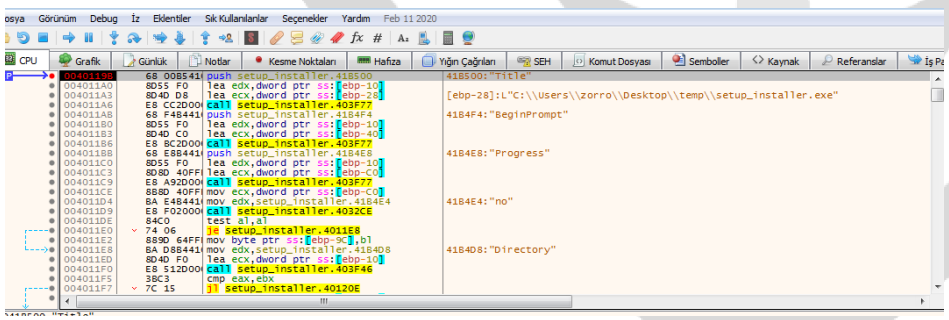
1. Windows Gezgini'ni kullanarak c:\Install'a gidin
2. sağ tıklayın ve "Yeni Metin Dosyası"nı seçin ve config.txt olarak adlandırın
3. sağ tıklayın ve "NotePad++ ile Düzenle'yi seçin
4. "Kodlama Menüsü"ne tıklayın ve "UTF-8'de Kodla"yı seçin
5. Bunun gibi bir şey girin:

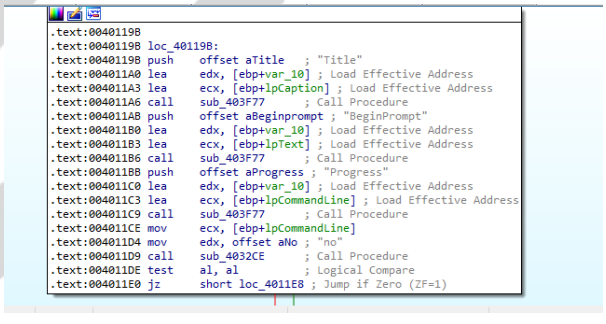
```
;!@Yükle@!UTF-8!
Title="YAZILIM v1.0.0.0"
BeginPrompt="YAZILIM v1.0.0.0 yüklemek istiyor musunuz?"
RunProgram="setup.exe"
;!@InstallEnd@!
```

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@!
```

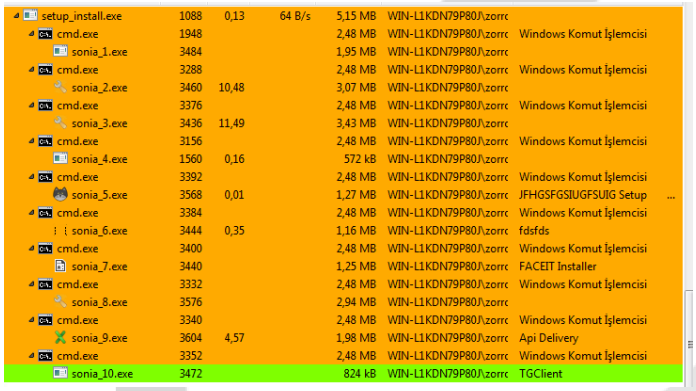
setup_installer.exe is configured with the configuration shown in the picture.

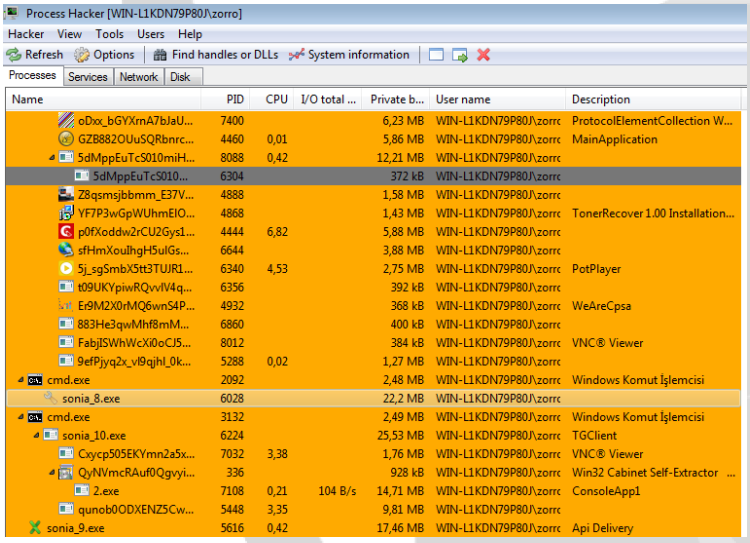




Runtime

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.



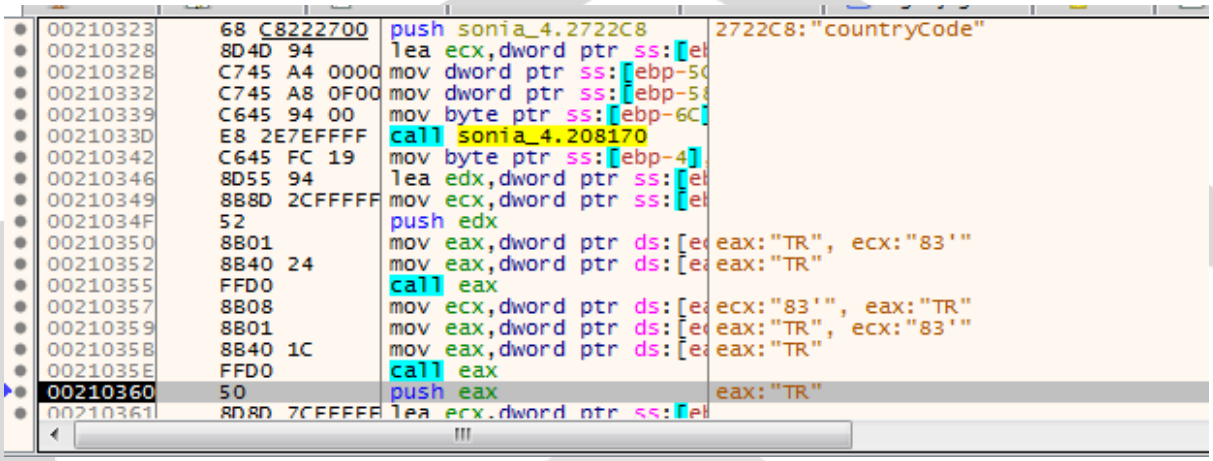


Language Check

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

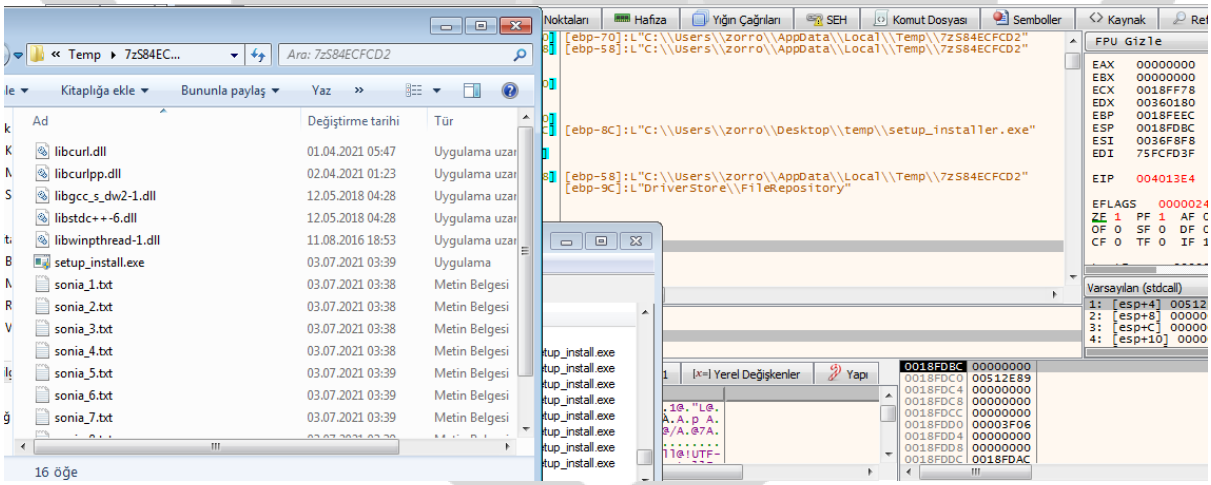
Country Check

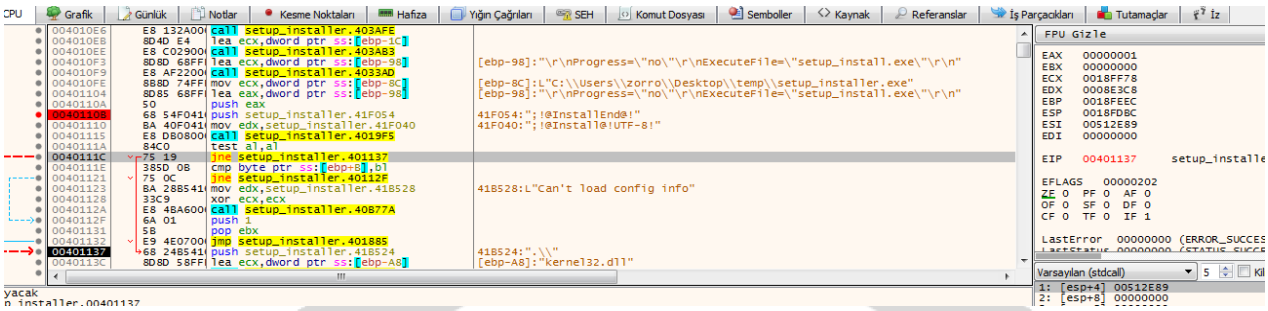
Gets the country code.



setup_installer.exe

The setup_installer.exe, which is the sfx file, creates the 7zS84ecfcd2 file temporarily in temp and extracts itself to that folder. Runs the setup_install.exe file in the 7zS84ecfcd2 folder and makes the extension of the txts to exe and runs it with cmd and the processes begin. It also downloads utf-8.





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
      lea ecx,dword ptr ss:[ebp-10]
00    call setup_installer.40E83C
      lea edx,dword ptr ss:[ebp-10]
FFFF  lea ecx,dword ptr ss:[ebp-98]    [ebp-98]:"\r\nProgress=\"no\"\r\nExecuteFile=\"setup_install.exe\"\r\n"
00    call setup_installer.403C57
      test al,al
      jne setup_installer.40119B
      cmp byte ptr ss:[ebp+B],bl
      jne setup_installer.401193
00    mov edx,setup_installer.41B508   41B508:L"Config failed"
      xor ecx,ecx
00    call setup_installer.40B77A
      push 1
```

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\7zS84ecfcd2

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 b7v49ezmfyjY8yPUl728VzS6.exe

DVRrv75N3d0cq9kr9v1nybhD.exe jdw6amdvloiFhGwIbHrF9bId.exe

jXKnQe3TxYFteWy6j3yegXVO.exe ksn2FwIHkR6rBdWC4wPt3JNr.exe

MWfsWcm042byzXi5l9sNEvpV.exe pVewZJtyml5fXqzzLBi4BYUA.exe

QiLxAKnbZiFVrIaHVYrVaCor.exe tXlH2r9moz62hZPcvIryh0o3.exe

vqd7AT7ae6Trme1GYn3mYmhh.exe xvakguFf42t2cm80ddcmFdSW.exe

YDQgBKZPYWCdWgcUNzdp3XSu.exe xmNWhWqAFpLCfekZ83BQg4bT.exe

_O6dRJaKSVIsmYSHDNe2HP2J.exe _O6dRJaKSVIsmYSHDNe2HP2J.exe

2M3NhGrvxSqWKxfUZaLIV6T3.exe 3EaucCSGZDQ6kBhOhGL6GzIs.exe

4YuMZqpIHmQunPxfoSr8reVN.exe 5EZopq09PuytQxgh7s3mcjdM.exe

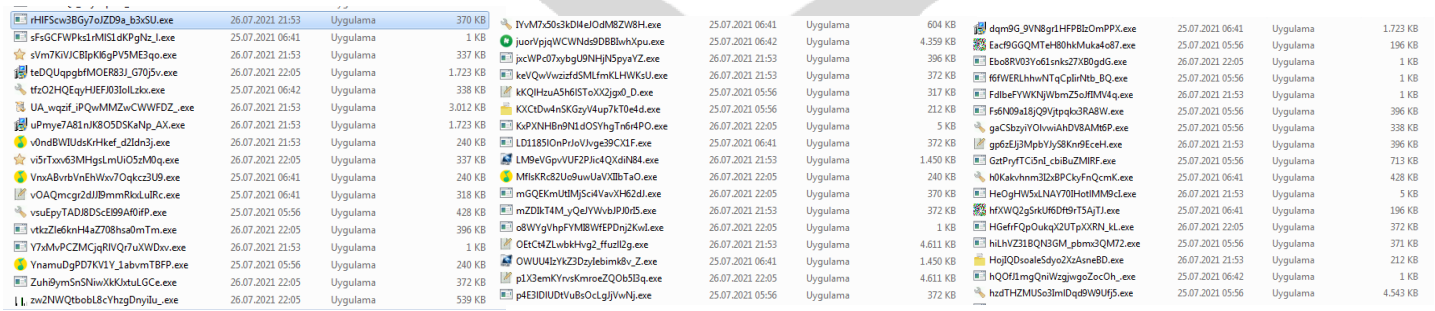
7_6ykZv7EvdCcqo5NVamsE5Z.exe 9kEtX2IGRqLKvOoj8lHVD5nN.exe

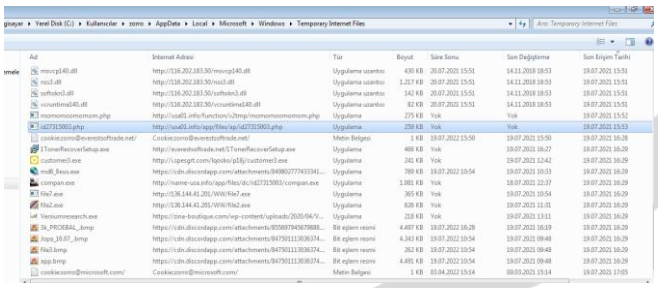
a0b6FbwlMTk4Pu1B7S6kg54S.exe a2oOWdAaiKKhVMBVvYfzoevb.exe

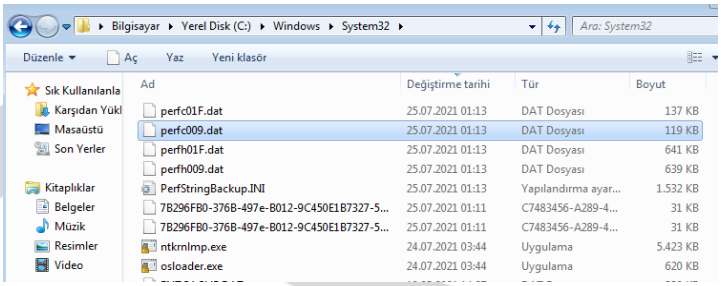
b9m753ZLMwrPudU1Z8oLgpRu.exe bk7ZfU2gLdOfP4WvGCutiJ9y.exe

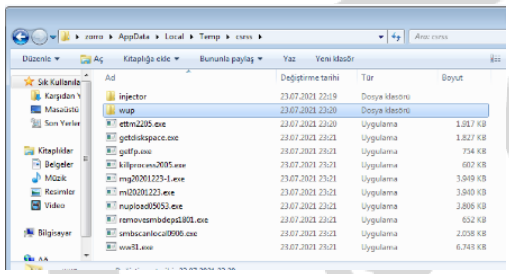
patch.exe narbux.exe injector.exe ww31.exe

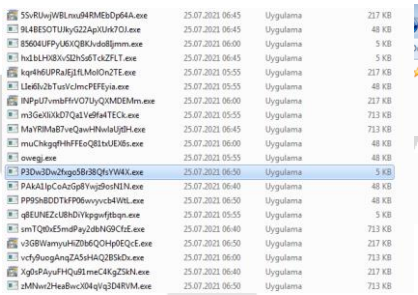
These are just some of the dropped files, downloading some files and deleting them directly.

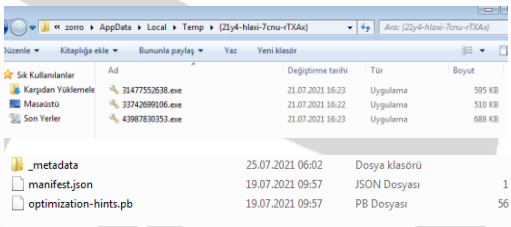




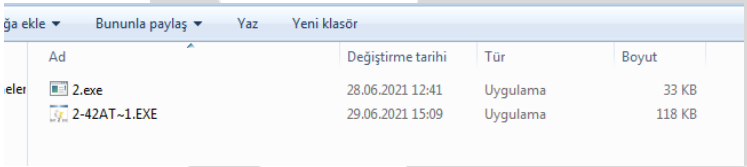


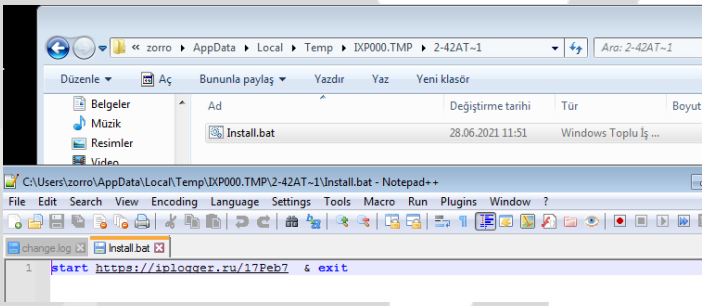






2-42at file is actually install.bat file and it redirects to iplogger page.

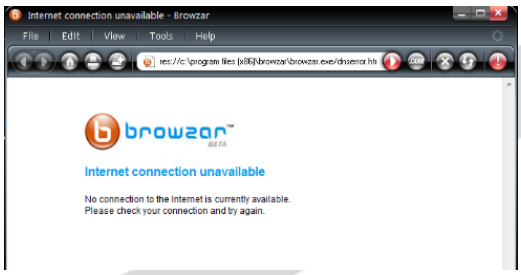




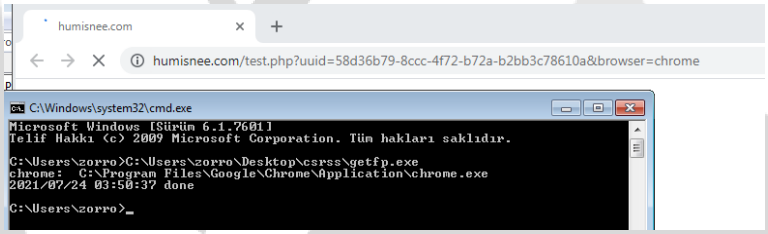
Adware and Linked Sites

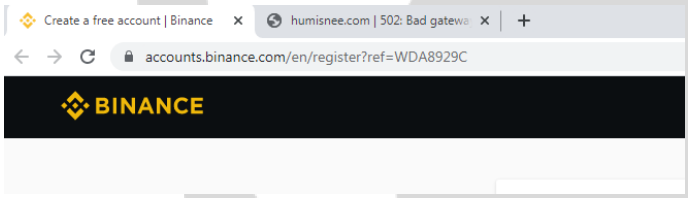
Humisnee.com	ip-api.com	facebook.com
Binance.com	37.0.11.41/base/api/getData.php	ipinfo.io
Browzar.com	addthis.com	cdn.discordapp.com
Bet365.com	steamcomunity.com	gql.twitch.com
Avito.ru	pastebin.com	i.instagram.com
oauth.vk.com	api.login.yahoo.com	spolaect.info
walmart.com	google.kz	google.com

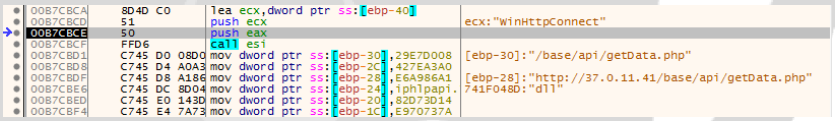
res://c:\program files (x86)\browzar\browzar.exe/dnserror.htm#http://www.browzar.com/start/?v=2000



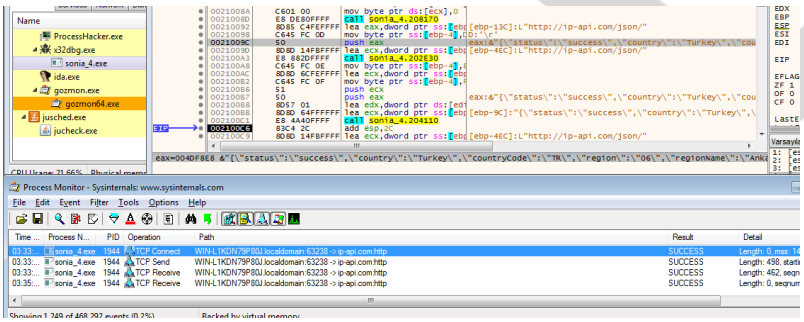
The getfp.exe in the csrss folder goes to humisnee.com.

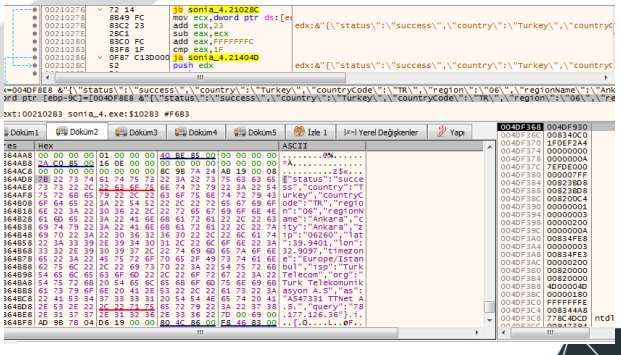






It connects to ip-api.com and gets various information.





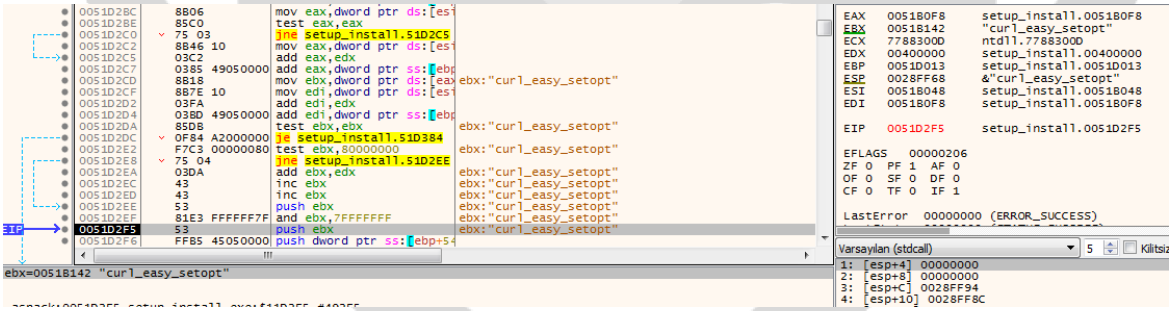
Compact_Layer

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

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.

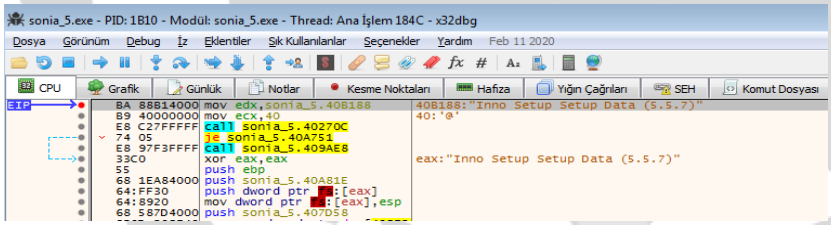


pthread_cond_broadcast

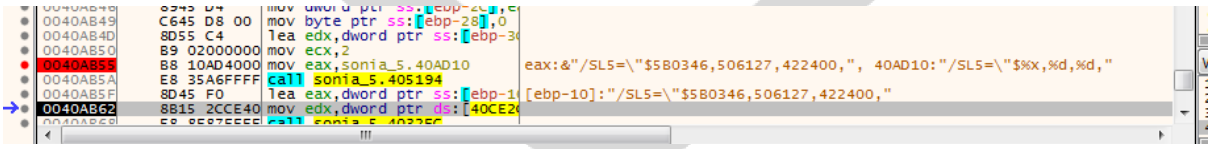
The pthread_cond_broadcast() function is used to unblock all threads currently blocked by the specified state variable.

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).



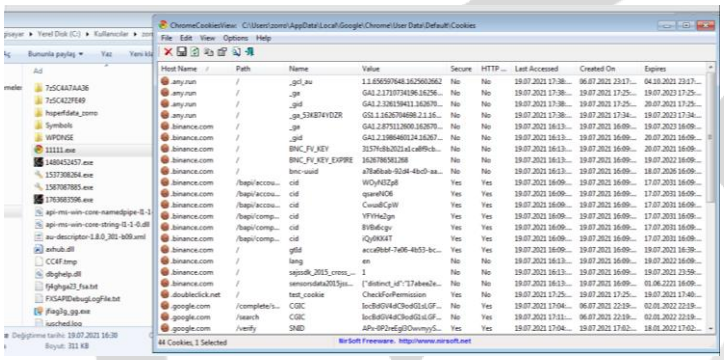
Command line: "C:\Users\zorro\AppData\Local\Temp\is-4GL93.tmp\sonia_5.tmp" /SL5="$5B0346,506127,422400,C:\Users\zorro\Desktop\210703-g9ppb8b36j_pw_infected\vürüs\setup_installer\sonia_5.exe

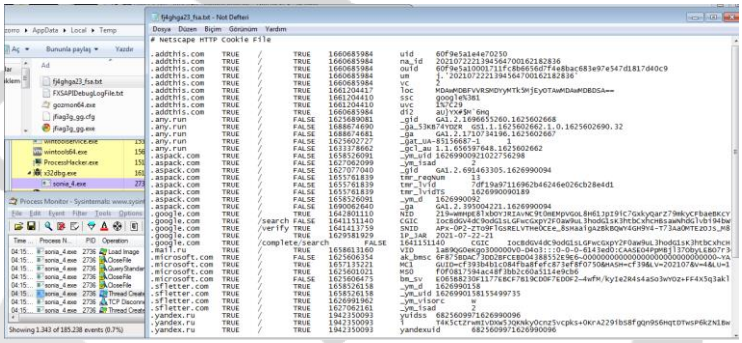


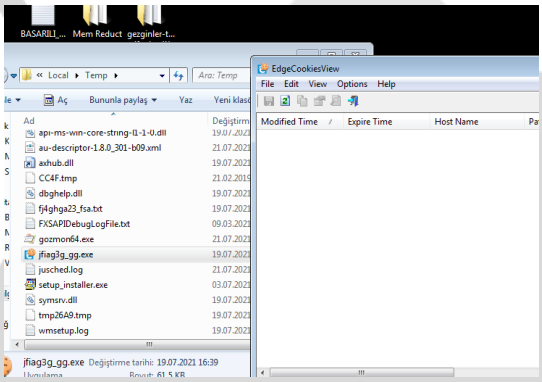
Cookie Steal

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	

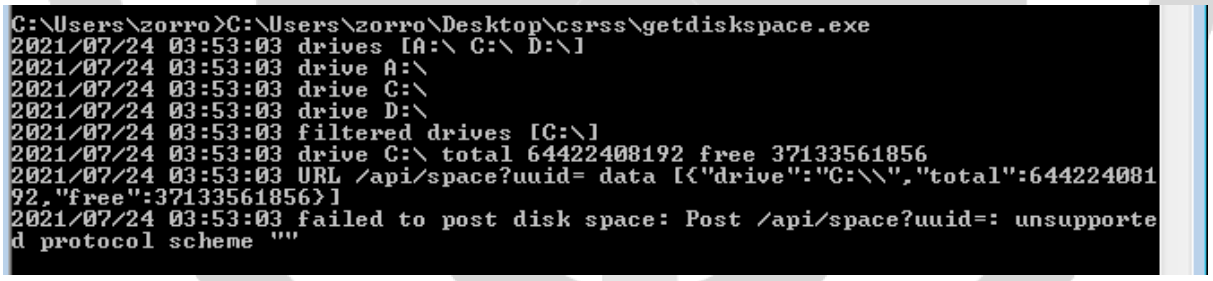
ee.exe / zz.exe

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.

getdiskspace.exe

Provides information about disk spaces



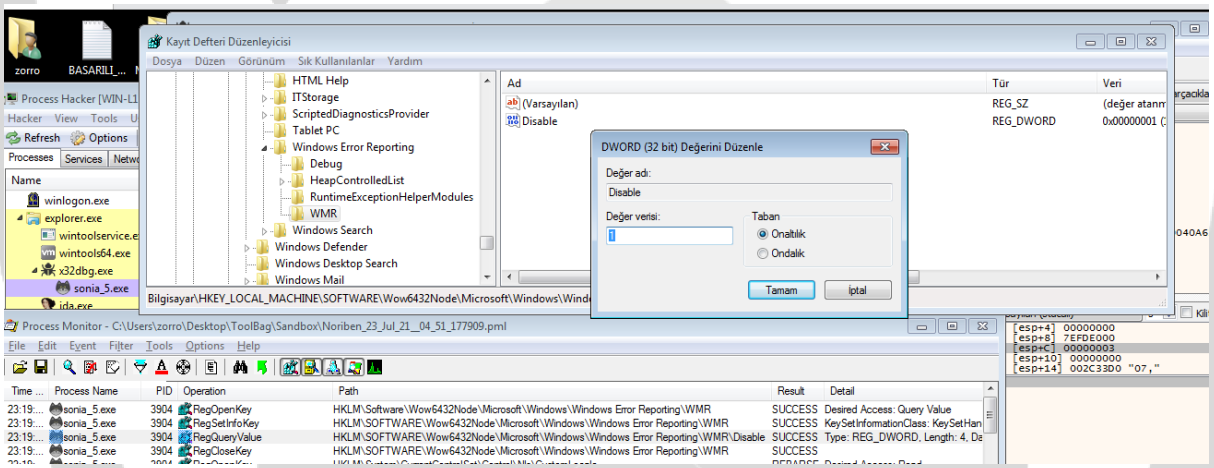
smbscanlocal10906.exe

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

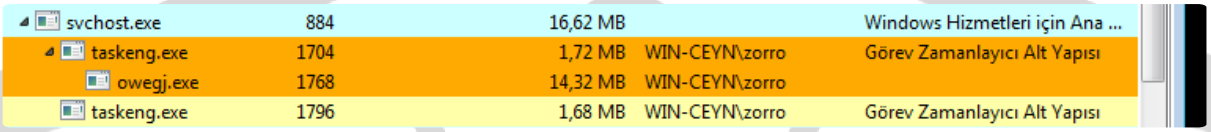


İOCs

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

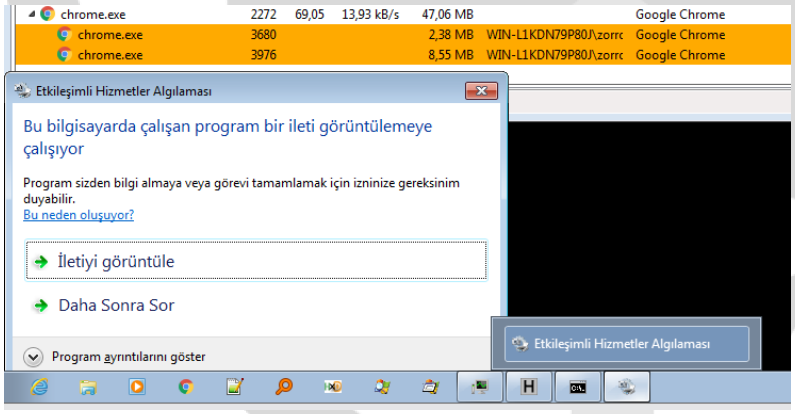
Scheduled Task

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



Chrome Secretly Steals Information In The Background

Chrome arka planda gizlice çalışırken bilgi almak için izin istemektedir.



Java

Here is the command info for base64 encoded java.

"C:\Program Files\Java\jre1.8.0_281\bin\jp2launcher.exe" -secure -javaws -jre "C:\Program Files\Java\jre1.8.0_281" -vma LWNsYXNzcGF0aABDOlxQcm9ncmFtIEZpbGVzXEphdmFcanJlMS44LjBfMjgxXGxpYlxkZXBsb3kuamFyAC1EamF2YS5zZWN1cml0eS5wb2xpY3k9ZmlsZTpDOlxQcm9ncmFtIEZpbGVzXEphdmFcanJlMS44LjBfMjgxXGxpYlxzZWN1cml0eVxqYXZhd3MucG9saWN5AC1EdHJ1c3RQcm94eT10cnVlAC1YdmVyaWZ5OnJlbW90ZQAtRGpubHB4LmhvbWU9QzpcUHJvZ3JhbSBGaWxlc1xKYXZhXGpyZTEuOC4wXzI4MVxiaW4ALURqYXZhLnNlY3VyaXR5Lm1hbmFnZXIALURzdW4uYXd0Lndhcm11cD10cnVlAC1YYm9vdGNsYXNzcGF0aC9hOkM6XFByb2dyYW0gRmlsZXNcSmF2YVxqcmUxLjguMF8yODFcbGliXGphdmF3cy5qYXI7QzpcUHJvZ3JhbSBGaWxlc1xKYXZhXGpyZTEuOC4wXzI4MVxsaWJcZGVwbG95LmphcjtDOlxQcm9ncmFtIEZpbGVzXEphdmFcanJlMS44LjBfMjgxXGxpYlxwbHVnaW4uamFyAC1EamRrLmRpc2FibGVMYXN0VXNhZ2VUcmFja2luZz10cnVlAC1Eam5scHguanZtPUM6XFByb2dyYW0gRmlsZXNcSmF2YVxqcmUxLjguMF8yODFcYmluXGphdmF3LmV4ZQAtRGpubHB4LnZtYXJncz1MVVJxWkdzdVpHbHpZV0pzWlV4aGMzUlZjMkZuWlZSeVlXTnJhVzVuUFhSeWRXVUE= -ma LVNTVkJhc2VsaW5lVXBkYXRlAC1ub3RXZWJKYXZh

Decoded version.

"C:\Program Files\Java\jre1.8.0_281\bin\jp2launcher.exe" -secure -javaws -jre "C:\Program Files\Java\jre1.8.0_281" -vma -classpathC:\Program Files\Java\jre1.8.0_281\lib\deploy.jar-Djava.security.policy=file:C:\Program Files\Java\jre1.8.0_281\lib\security\javaws.policy-DtrustProxy=true-Xverify:remote-Djnlpx.home=C:\Program Files\Java\jre1.8.0_281\bin-Djava.security.manager-Dsun.awt.warmup=true-Xbootclasspath/a:C:\Program Files\Java\jre1.8.0_281\lib\javaws.jar;C:\Program Files\Java\jre1.8.0_281\lib\deploy.jar;C:\Program Files\Java\jre1.8.0_281\lib\plugin.jar-Djdk.disableLastUsageTracking=true-Djnlpx.jvm=C:\Program Files\Java\jre1.8.0_281\bin\javaw.exe-Djnlpx.vmargs= -Djdk.disableLastUsageTracking=true -ma -SSVBaselineUpdate-notWebJava

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="9e285901af26b01bafe9afb312620887"
                $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/