



AZORULT

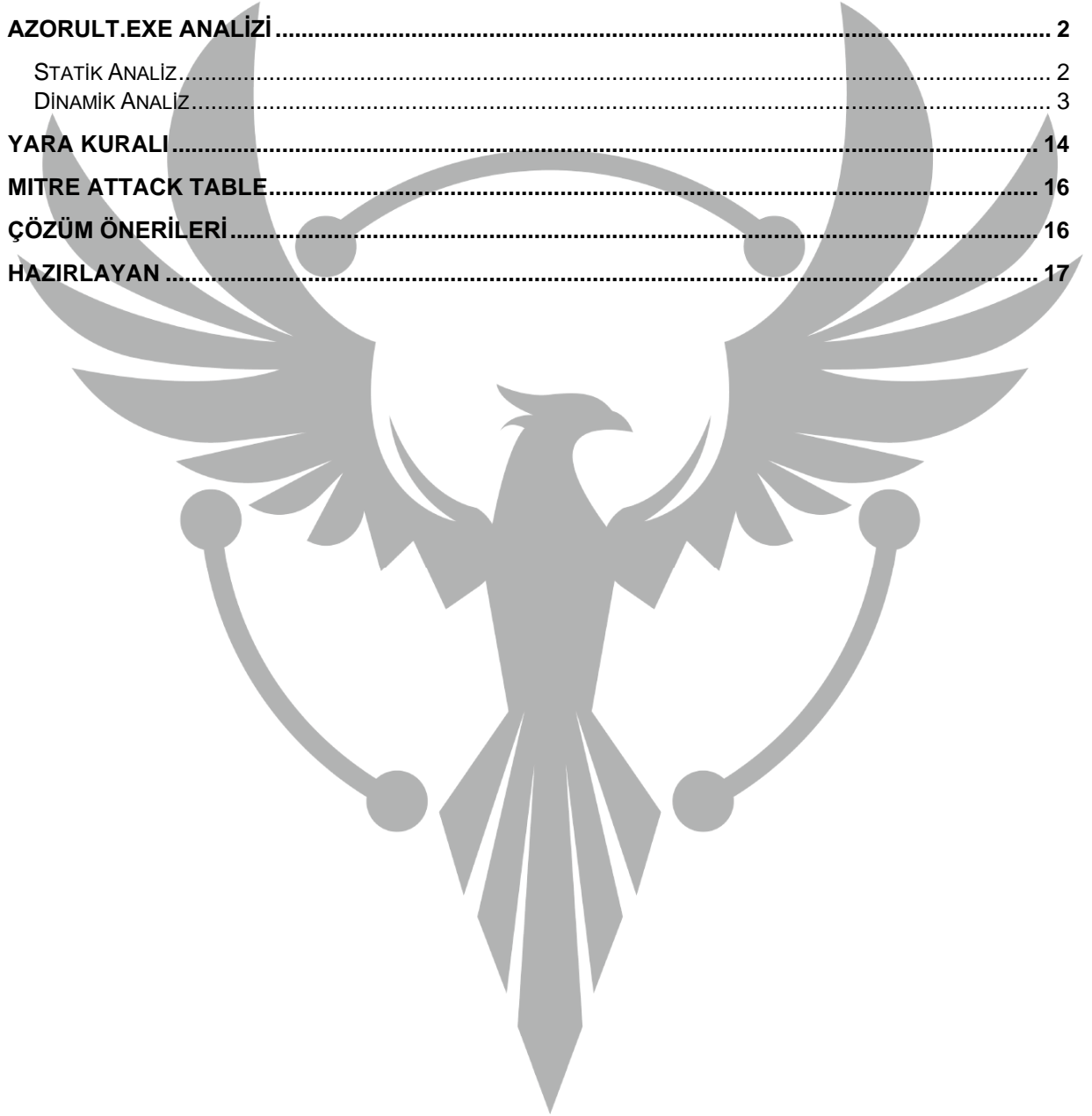
TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

İÇİNDEKİLER.....	i
ÖN BAKIŞ	1
AZORULT.EXE ANALİZİ	2
STATİK ANALİZ.....	2
DİNAMİK ANALİZ.....	3
YARA KURALI.....	14
MITRE ATTACK TABLE.....	16
ÇÖZÜM ÖNERİLERİ.....	16
HAZIRLAYAN	17



Ön Bakış

Azorult, 2016 yılından beri kullanımda olan bilgi hırsızı bir Truva atıdır. Birçok versiyonu olmasına karşın çoğunlukla spam e-postalar aracılığıyla dağıtılır. 2018 yılında gelen güncelleme ile Azorult zararlı yazılımı bir yükleyici (installer) olarak da hareket edebilmektedir. Bilgi sızdırma işlevini yerine getirdikten sonra kendisini silecek şekilde güncellenmiştir.

Azorult zararlı yazılımı tarayıcılardan e-posta ve FTP sunuculardan kaydedilmiş şifreleri, çerezleri, kripto para cüzdanı dosyalarını, Skype gibi mesajlaşma uygulamalarının mesaj geçmişini, masaüstü dosyaları, çalışan işlemlerin listelerini, kullanıcı adı, bilgisayarın bilgileri gibi bilgileri arar ve bu bilgileri komuta kontrol sunucusuna gönderir.

Bu kötü amaçlı yazılımın virüs bulaşmış bilgisayarların;

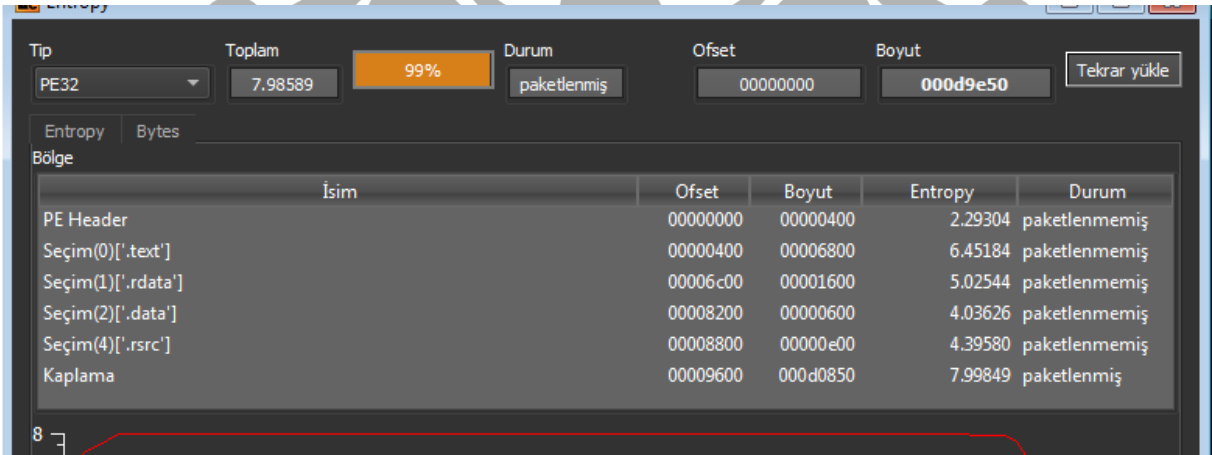
- Web tarayıcılarına kaydedilen kimlik bilgilerine,
- Masaüstü dosyalarına,
- Mesajlaşma istemcilerine,
- FTP/SSH istemcilerine,
- Kripto para cüzdanlarına,
- Bilgisayar belgelerine erişim sağlamasına olanak sağlamaktadır.

Azorult.exe Analizi

Adı	Azorult.exe
MD5	64CE3428700D7A0797CC4D779AC37C39
SHA256	6fa0833240b9e814ed3640ef92ae275eb3741b19358f46779a768ec6f5151c42
Dosya Türü	Portable Executable 32

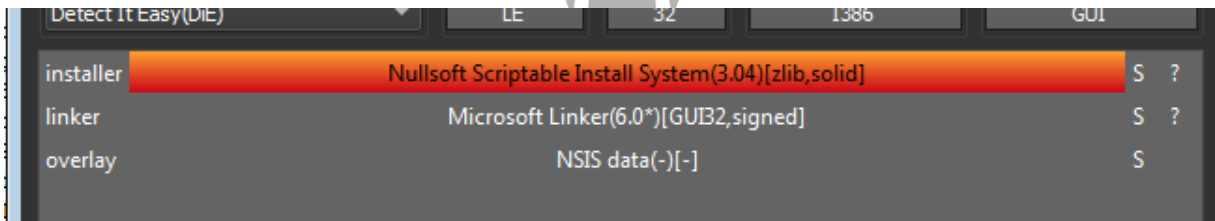
“6fa0833240b9e814ed3640ef92ae275eb3741b19358f46779a768ec6f5151c42.exe” orijinal isimli zararlının ismi analiz sırasında kolaylık olması adına “**Azorult.exe**” olarak değiştirilmiştir.

Statik Analiz



Bölge	İsim	Ofset	Boyut	Entropy	Durum
PE Header		00000000	00000400	2.29304	paketlenmemiş
Seçim(0)['.text']		00000400	00006800	6.45184	paketlenmemiş
Seçim(1)['.rdata']		00006c00	00001600	5.02544	paketlenmemiş
Seçim(2)['.data']		00008200	00000600	4.03626	paketlenmemiş
Seçim(4)['.rsrc']		00008800	00000e00	4.39580	paketlenmemiş
Kaplama		00009600	000d0850	7.99849	paketlenmiş

Görsel 1 Zararlının DIE Aracında İncelenmesi



İsim	Ofset	Boyut	Entropy	Durum
installer				S ?
linker				S ?
overlay				S

Görsel 2 Nullsoft Scriptable Install System

Azorult.exe zararlısı DIE aracında incelendiğinde **paketlenmiş** olduğu görülmektedir. Ayrıca zararlı **NSIS (Nullsoft Scriptable Install System)** tabanlı bir yapı bulundurmaktadır.

Kernel32.dll	User32.dll	Gdi32.dll
Shell32.dll	Advapi.dll	Comctl32.dll
Ole32.dll		

Tablo 1 Zararlının Kullandığı Bazı DLL'ler

Zararlı yazılımın kullandığı DLL'ler Tablo 1'de gösterilmektedir.

```

00000000909E 00000049C89E 0 Comments
0000000090B0 00000049C8B0 0 frankotvang deguelia vigter
0000000090EE 00000049C8EE 0 FileDescription
000000009110 00000049C910 0 reprosper affrdigelseerne
00000000914A 00000049C94A 0 InternalName
000000009164 00000049C964 0 kondensvandet capetonian.exe
0000000091A6 00000049C9A6 0 LegalCopyright
0000000091C4 00000049C9C4 0 vurderingstidspunkternes papirstrelers kabinescooterne

```

Görsel 3 Zararlının String'lerinin bintext Aracında incelenmesi

Zararlının string'leri incelendiğinde dosya açıklamasının “**reprosper affrdigelseerne**”, esas isminin ise “**kondensvandet capetonian.exe**” olduğu görülmüştür.

Dinamik Analiz

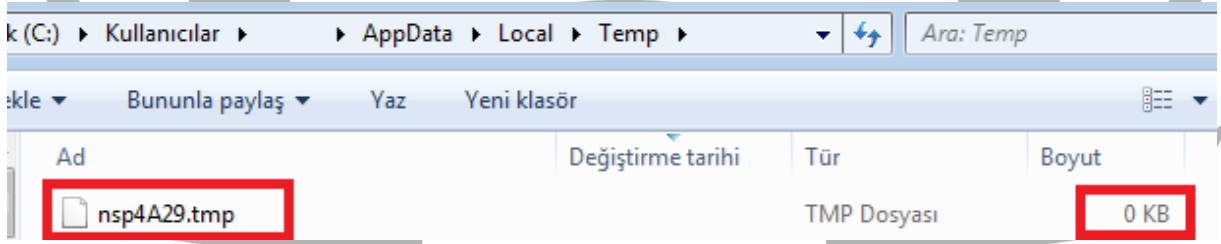
Uxtheme.dll	Userenv.dll	Setupapi.dll
Apphelp.dll	Propsys.dll	Dwmapi.dll
Cryptbase.dll	Oleacc.dll	Clbcatq.dll
Ntmarta.dll		

Tablo 2 Dinamik Olarak Çözömlenen DLL'ler

Zararlının kullandığı bazı DLL'ler dinamik olarak incelendiğinde görölmektedir. Bu DLL'ler Tablo 2'de gösterilmektedir.

```
0 | . 50 | push eax | [ebp+C]:L"C:\\User  
1 | . FF75 0C | push dword ptr ss:[ebp+C] |  
4 | . 66:0155 FC | add word ptr ss:[ebp-4],dx |  
8 | . FF15 DC804000 | call dword ptr ds:[<&GetTempFileNameW>] |  
E | . 85C0 | test eax, eax |  
0 | . 75 0D | jne azorult.405E2F |  
2 | . 85FF | test edi, edi |
```

Görsel 4 TMP Dosyasının Oluşturulmasında GetTempFileNameW API'sinin Kullanılması



Görsel 5 Temp Klasöründe Oluşan TMP Dosyası

Zararlı “C:\Users\%username%\AppData\Local\Temp” dosya yolunda boyutu **0KB** olan bir **TMP** dosyası oluşturmaktadır. Oluşan bu dosya için **GetTempFileNameW** API'si ile her seferinde benzersiz bir isim oluşturmaktadır. Oluşan bu dosyaların isimleri her zaman “ns” ile başlamaktadır.

```
62D | > 0F84 CB000000 | je azorult.4036FE | 441000:L"C:\\User  
633 | > 68 00104400 | push azorult.441000 |  
638 | FF15 40814000 | call dword ptr ds:[<&DeleteFileW>] |  
63E | FF7424 1C | push dword ptr ss:[esp+1C] |  
642 | E8 96F8FFFF | call <azorult.sub_402EDD> |
```

Görsel 6 DeleteFileW API'si Kullanılarak Oluşturulan TMP Dosyasının Silinmesi

Daha sonra **DeleteFileW** API'sini kullanarak oluşturduğu bu TMP dosyasını silmektedir.

. 56	push esi	esi:L"Fugitated Setup"
. E8 95250000	call <azorult.sub_4062DC>	esi:L"Fugitated Setup"
. 56	push esi	esi:L"Fugitated Setup"
. FF35 28D24200	push dword ptr ds:[42D228]	esi:L"Fugitated Setup"
. FF15 5C824000	call dword ptr ds:[<&SetWindowText>]	esi:L"Fugitated Setup"
. 8BC6	mov eax,esi	esi:L"Fugitated Setup"
. 5F	pop esi	esi:L"Fugitated Setup"

Görsel 7 SetWindowTextW API'si Kullanılarak Pencere Başlığının Değiştirilmesi

Daha sonra dinamik olarak çözümlediği **"Fugitated Setup"** stringini, **SetWindowTextW** API'si ile zararlı çalıştığında açılacak olan yükleyici penceresinin başlığı (title bar) olarak ayarlamaktadır.

. 74 1B	je azorult.403D34	eax:L"Nondistributively"
. 8BF8	mov edi, eax	eax:L"Nondistributively"
> 8B06	mov eax, dword ptr ds:[esi]	eax:L"Nondistributively"
. 85C0	test eax, eax	eax:L"Nondistributively"
. 74 0A	je azorult.403D28	eax:L"Nondistributively"
. 50	push eax	eax:L"Nondistributively"
. 8D46 18	lea eax, dword ptr ds:[esi+18]	eax:L"Nondistributively"
. 50	push eax	eax:L"Nondistributively"
. E8 81250000	call <azorult.sub_4062DC>	eax:L"Nondistributively"
> 81C6 18080000	add esi, 818	eax:L"Nondistributively"
. 4F	dec edi	

Görsel 8 String'lerin Çözümlemesi

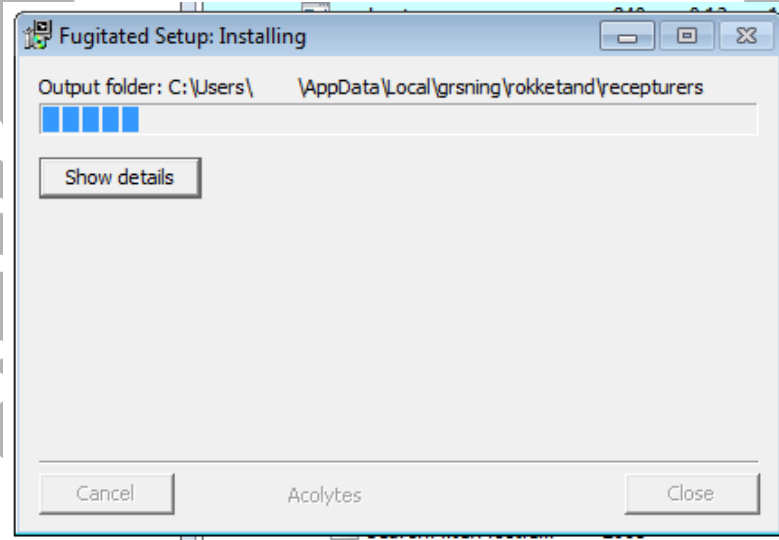
Sonrasında zararlı, bir döngü kullanarak anlamlı ve/veya anlamsız bazı stringler oluşturmaktadır. Bu stringler zararlı her çalıştırıldığı aynı sırayla çözümlenmektedir. Sırasıyla ilk on string Tablo 3'te gösterilmektedir.

Stnderforsamlingen
Concourse206
Sanses
Hviderne
Nondistributively
Gioldaoram
Stokkepryglenes
Bevidsthedsniveau
Spillebordene
Prolongeredes

Tablo 3 Dinamik Olarak Çözümlenen String'ler

50	FF35 E04E4300	push eax
FF15 44824000	call dword ptr ds:[434EE0]	
6A 05	push 5	
8BF0	mov esi, eax	
E8 C9D7FFFF	call <azorult.sub_40140B>	
6A 01	push 1	

Görsel 9 DialogBoxParamW API'si

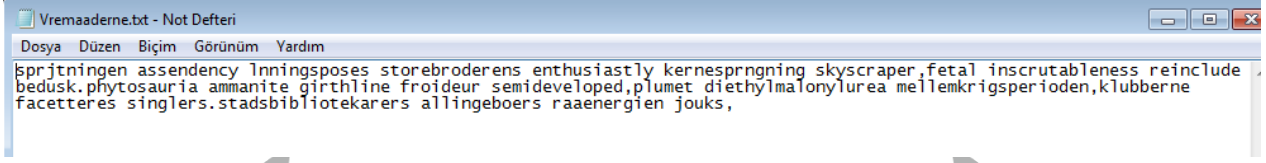


Görsel 10 Açılan "Fugitated Setup" İsimli Kurulum Penceresi

Daha sonrasında **DialogBoxParamW** API'si kullanılarak kurulum dosyası iletişim kutusu oluşturulmaktadır. Sonra **"C:\Users\%username%\AppData\Local"** dosya yolunda **"grsning"** isimli bir klasör oluşmaktadır. Bu klasörün içinde de çeşitli ve iç içe klasörler ve dosyalar bulunmaktadır.

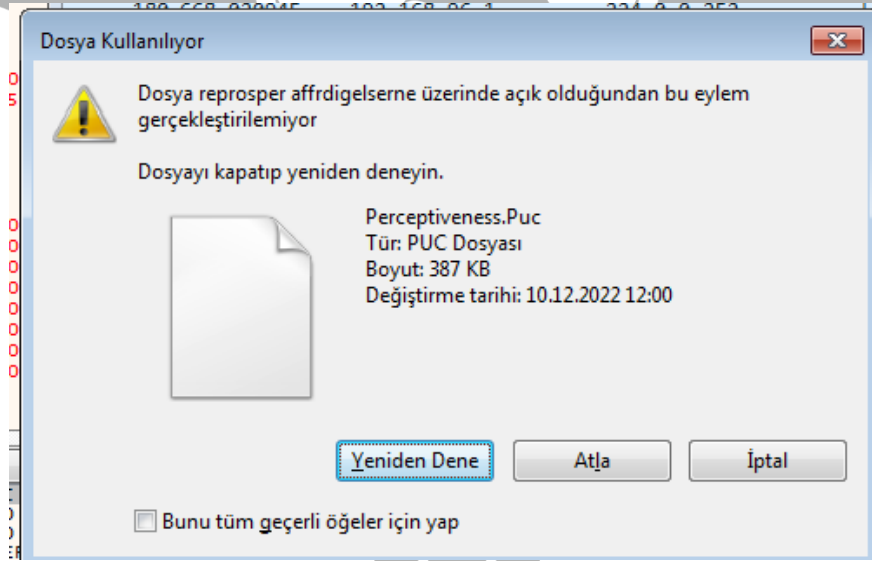
Aşağıda oluşan dosyaların isimleri ve hiyerarşik olarak konumları gösterilmektedir.

- ✓ grsining
 - ↳ rokketand
 - ↳ recepturers
 - ↳ Daddelpalmers
 - ↳ Studiesituationerne
 - ↳ afslapningsvelsernes.dip
 - ↳ Enakter
 - ↳ Astigmatikeren
 - ↳ Gladiatorism
 - ↳ Eklektikerne.smu
 - ↳ Perceptiveness.Puc
 - ↳ Vremaaderne.txt
 - ↳ masseskrivelse
 - ↳ Sukkerskeerne
 - ↳ Ssygen126
 - ↳ equison.mul
 - ↳ lydhrt.non
 - ↳ rflen.pol
 - ↳ skipperlgnenes.toe
 - ↳ tallotterier.cut



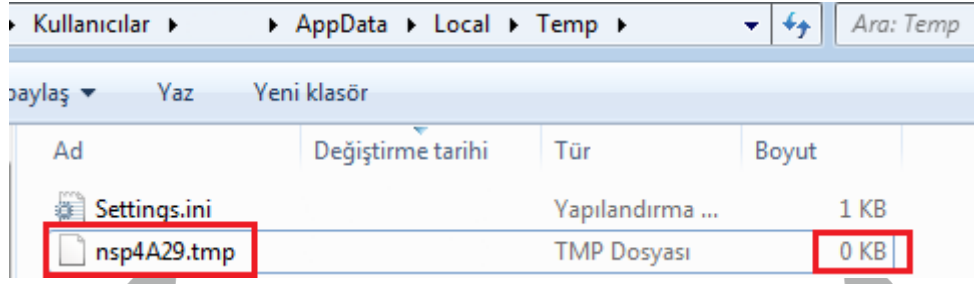
Görsel 11 "Vremaaderne.txt" Dosyasının İçeriği

"grsining\rokketand\recepturers\Enakter\Astigmatikeren\Gladiatorism\Vremaaderne.txt" dosya yolunda oluşan metin dosyası açıldığında içerisinde Görsel 11'da gösterilen metin bulunmaktadır. Bu metnin içeriğinde bazı anlamlı ve anlamsız Danca kelimeler bulunmaktadır ancak bir bütün olarak bir anlam ifade etmemektedir.



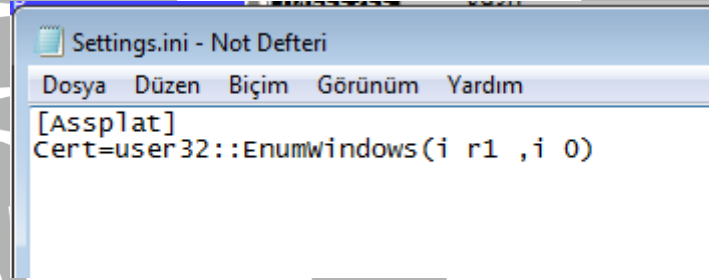
Görsel 12 Kullanılmaya Devam Eden PUC Dosyası

Kurulum ekranı kapandıktan veya gizlendikten sonra sadece **"grsining\rokketand\recepturers\Enakter\Astigmatikeren\Gladiatorism\Perceptiveness.Puc"** dosya konumunda bulunan PUC uzantılı binary veri tipindeki dosyanın kullanılmaya devam ettiği görülmektedir.



Görsel 13 Oluşan TMP ve Settings.ini Dosyası

Bununla birlikte “C:\Users\%username%\AppData\Local\Temp” dosya yolunda her seferinde farklı isimde boyutu **0KB** olan bir **TMP dosyası** ve **Settings.ini** isimli bir yapılandırma dosyası oluşmaktadır. Oluşan bu TMP dosyası daha önce silinen TMP dosyası ile aynı ismi taşımaktadır.



Görsel 14 "Settings.ini" Dosyasının İçeriği ve EnumWindows API'si

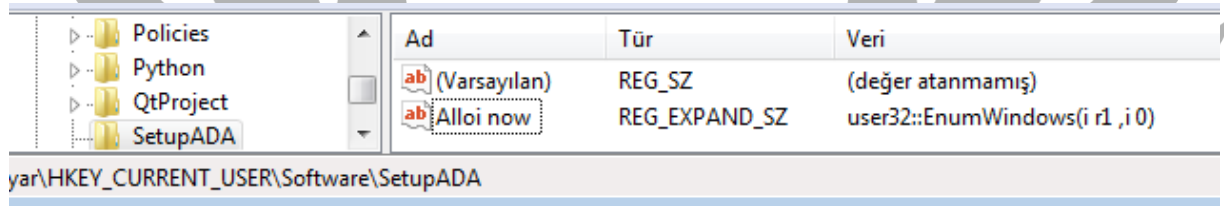
Yapılandırma dosyasının içeriği Görsel 14'te gösterilmektedir.

DialogBoxParamW API'si ile Görsel 10'da gösterilen kurulum penceresinin çalışması sırasında kayıt defterinde “HKCU\Software\SetupADAlloi now” anahtarının değeri değiştirilmektedir. Ayarlanan değerler sırasıyla Tablo 4'te gösterilmektedir.

user32::ShowWindow(ir4,i0)
kernel32::CreateFileA(m r4 ,i 0x80000000,i 0, p 0, i 4, i 0x80, i 0)i.r5
kernel32::VirtualAlloc(i 0,i R2,i 12288,i 64)p.r1
kernel32::ReadFile(i r5, i r1,i R2,*i 0, i 0)i.r3
user32::EnumWindows(i r1 ,i 0)

Tablo 4 Kayıt Defterinde "Alloi now" Anahtarının Aldığı Değerler

Bu değerler **NSIS (Nullsoft Scriptable Install System)** ile sisteme kurulum yapmak için kullanılan işlevleri göstermektedir. **ShowWindow** işlevi aldığı “i0” değeriyle pencereyi gizlemekte veya kapatmaktadır. **CreateFileA** işlevi ile okuma izni bulunan (0x80000000; GENERIC_READ) bir dosya oluşturmaktadır. **VirtualAlloc** işlevi ile 12.288 bayt’lık bir sanal bellek bölgesi ayrılmaktadır. **ReadFile** işlevi bu dosyayı okumaktadır ve en son **EnumWindows** işlevi ile açık olan üst seviye pencerelerin bilgisi elde edilmektedir.

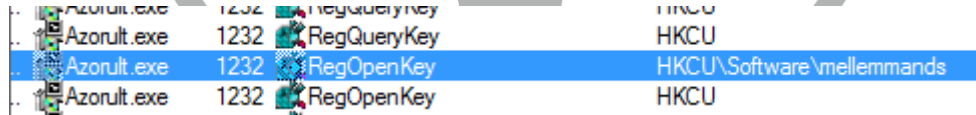


Ad	Tür	Veri
(Varsayılan)	REG_SZ	(değer atanmamış)
Alloi now	REG_EXPAND_SZ	user32::EnumWindows(i r1 ,i 0)

yar\HKEY_CURRENT_USER\Software\SetupADA

Görsel 15 Kayıt Defterindeki Değerin Son Durumu

Kayıt defterinde en son atanan değer olan EnumWindows değeri değişmemektedir.



Process Name	PID	Operation	Path
Azorult.exe	1232	RegQueryValue	HKCU
Azorult.exe	1232	RegQueryKey	HKCU
Azorult.exe	1232	RegOpenKey	HKCU\Software\mellemands
Azorult.exe	1232	RegOpenKey	HKCU

Görsel 16 "mellemands" Anahtarı

Daha sonra kayıt defterinde **HKCU\Software\mellemands** isminde bir anahtara ulaşmaya çalıştığı görülmektedir. Kayıt defterinde belirtilen konumda **mellemands** isimli bir anahtar bulunmamaktadır. Bu kelime Danca’da ‘**aracı**’ anlamına gelmektedir.

64 RegOpenKey
64 RegSetInfoKey
64 RegQueryValue
64 RegCloseKey

HKLM\Software\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR

Görsel 17 Hata Gözükmesini Engellemek İçin Devre Dışı Bırakılan Anahtar

Bu işlemler sırasında zararlı ekranda herhangi bir hatanın gözükmesini engellemek için “HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable” anahtarını ‘Disable’ olarak ayarlamaktadır.

192.168.96.132	104.120.110.77	TCP	66 49224 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
104.120.110.77	192.168.96.132	TCP	60 443 → 49224 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.96.132	104.120.110.77	TCP	54 49224 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.96.132	104.120.110.77	TLsv1.2	253 Client Hello
104.120.110.77	192.168.96.132	TCP	60 443 → 49224 [ACK] Seq=1 Ack=200 Win=64240 Len=0
104.120.110.77	192.168.96.132	TLsv1.2	1514 Server Hello
104.120.110.77	192.168.96.132	TCP	1514 443 → 49224 [ACK] Seq=1461 Ack=200 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
104.120.110.77	192.168.96.132	TLsv1.2	1222 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
192.168.96.132	104.120.110.77	TCP	54 49224 → 443 [ACK] Seq=200 Ack=4089 Win=64240 Len=0
192.168.96.132	104.120.110.77	TLsv1.2	236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
104.120.110.77	192.168.96.132	TCP	60 443 → 49224 [ACK] Seq=4089 Ack=382 Win=64240 Len=0
104.120.110.77	192.168.96.132	TLsv1.2	161 Change Cipher Spec, Encrypted Handshake Message
192.168.96.132	104.120.110.77	TCP	54 49224 → 443 [ACK] Seq=382 Ack=4196 Win=64133 Len=0
192.168.96.132	104.120.110.77	TLsv1.2	267 Application Data
104.120.110.77	192.168.96.132	TCP	60 443 → 49224 [ACK] Seq=4196 Ack=595 Win=64240 Len=0
104.120.110.77	192.168.96.132	TCP	1514 443 → 49224 [ACK] Seq=4196 Ack=595 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
104.120.110.77	192.168.96.132	TCP	1514 443 → 49224 [ACK] Seq=5656 Ack=595 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
104.120.110.77	192.168.96.132	TCP	1514 443 → 49224 [ACK] Seq=7116 Ack=595 Win=64240 Len=1460 [TCP segment of a reassembled PDU]

Görsel 18 Wireshark'ta Gözlemlenen Veriler

Zararlı 104[.]120[.]110[.]77[:]443 soketine istek göndererek komuta kontrol sunucusuyla şifreli bağlantı kurmaktadır. Bu IP adresine bazı paketler göndermekte TCP segmentlerini birleştirerek orijinal PDU'yu oluşturmaktadır.

DNS	88 Standard query 0x20cf A javadl-esd-secure.oracle.com
DNS	195 Standard query response 0x20cf A javadl-esd-secure.oracle.com CNAME javadl-esd-secure.oracle.com.edgekey.net CNAME e13073.g.akamaiedge.net A 104.120.110.77
TCP	66 49226 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
TCP	60 443 → 49226 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Görsel 19 Karmaşık DNS Çözümlemesi

Zararlının bazı karmaşık DNS çözümleri yaptığı görülmektedir. Zararlı güvenlik önlemlerini atlatmak ve zararlı içeriği saklamak adına Akamai içerik dağıtım ağını kullanmaktadır.

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 EF BE AD DE 4E 75 6C 6C 73 6F 66 74i%.Nullsoft
49 6E 73 74 D0 02 02 00 A0 E4 0C 00 97 2D 00 80	InstG... ä...—.
ED 7D 0B 7C 5C 67 75 E7 9D 91 42 12 27 8E 1D C7	i}.\guç.'B.'...Ç
76 FC 4A 3C B1 A3 BC 7E 8E 90 64 D9 96 9D 04 22	vüJ<±f4~..dÜ-.."
3B B1 93 38 7E AC 1F 09 64 27 8F 91 66 24 8D 35	;±"8~..d'. 'f\$.5
AF CC 43 B1 4C 0B 32 2C 4D 48 DA 84 00 29 AF 52	~İC±L.2,MHÜ,,.)~R

Alıntı (hex)

Alıntı (metin)

63 74 75 72 65 3D 22 2A 22 20 6E 61 6D 65 3D 22 4E 75 6C 6C 73 6F 66 74 2E 4E 53 49 53 2E 65 78

cture="*" name="Nullsoft.NSIS.ex

22 2F 3E 3C 64 65 73 63 72 69 70 74 69 6F 6E 3E 4E 75 6C 6C 73 6F 66 74 20 49 6E 73 74 61 6C 6C

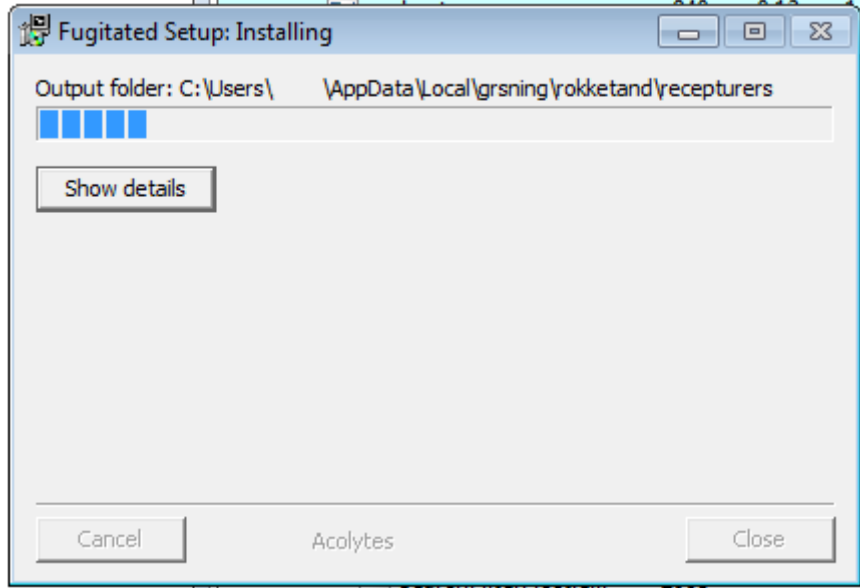
"/><description>Nullsoft Install

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 EF BE AD DE 4E 75 6C 6C 73 6F 66 74 49 6E 73 74 D0 02 02 00

.....i%.NullsoftInstG...

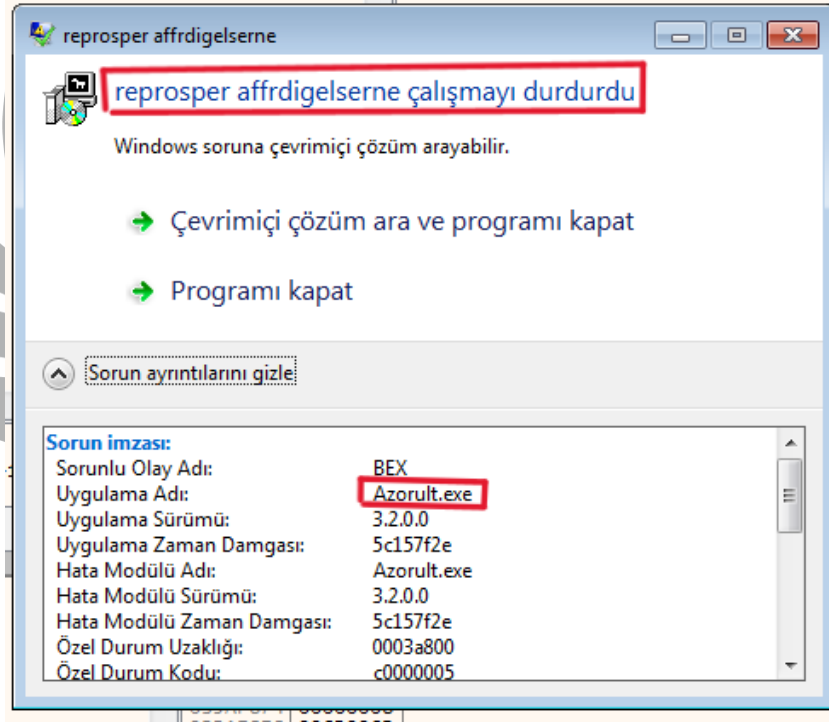
Görsel 20 NSIS Tabanlı Yapının Kullanılması

Zararlı **NSIS (Nullsoft Scriptable Install System)** tabanlı bir yapı bulundurmaktadır. **NSIS Installer** kullanarak zararlının çözülmesini ve dağıtımını gerçekleştirmektedir. NSIS, kullanıcıların kurulum dosyalarını özelleştirmelerini sağlamak adına bir dizi betik ve komut içermektedir. Böylece kurulum sırasında çeşitli işlemleri gerçekleştirebilmektedir.



Görsel 21 "Fugitated Setup" İsimli Kurulum Dosyası

Zararlı kodun gizlenmiş olduđu bu kurulum dosyası yukarıda da belirtildiđi gibi **“Fugitated Setup”** başlığı ile bir pencere açmakta ve zararlı kodunu çalıştırarak hedeflediđi verileri çalmaktadır.



Görsel 22 "reprosper affrdigelse'ne çalışmayı durdurdu" Hatası Ekranı

Zararlı **“reprosper affrdigelse'ne çalışmayı durdurdu”** şeklinde bir hata vererek kendi process'ini sonlandırmaktadır.

YARA Kuralı

```
import "hash"

rule Azorult {

meta:

    description = "Azorult"

    aauthor = "zayotem"

strings:

    $api1 = "DialogBoxParamW" ascii

    $api2 = "DeleteFileW" ascii

    $api3 = "GetTempFileNameW" ascii

    $api4 = "ExitProcess" ascii

    $api5 = "SetWindowTextW" ascii

    $str1 = "\\Microsoft\\Internet Explorer\\Quick Launch" wide

    $str2 = "Software\\Microsoft\\Windows\\CurrentVersion" wide

    $str3 = "Control Panel\\Desktop\\ResourceLocale" wide
```


\$str4 = "http://nsis.sf.net/NSIS_Error" wide

\$str5 = "reprosper affrdigelserne" wide

\$str6 = "kondensvandet capetonian" wide

\$hex_1 = {74 1B 8B F8 8B 06 85 C0 74 0A 50 8D 46 18 50 E8}

\$hex_2 = {4E 75 6C 6C 73 6F 66 74}

condition:

hash.md5 (0, filesize) == "64CE3428700D7A0797CC4D779AC37C39" or (4 of (\$api*)) or (5 of (\$str*)) or (1 of (\$hex*))

}

MITRE ATTACK TABLE

Reconnaissance	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	C&C	Exfiltration
Gather Victim Host Information (T1592)	Command and Scripting Interpreter (T1059)	Account Manipulation (T1098)	Create Process with Token (T1134.002)	Access Token Manipulation	Credentials from Web Browsers (T1555.003)	File Transfer Protocols (T1071.002)	Exfiltration Over C2 Channel (T1041)
Gather Victim Network Information (T1590)	Native API (T1106)	Valid Accounts (T1078)	Process Injection (T1055)	Deobfuscate/Decode Files or Information (T1140)	Steal Web Session Cookie (T1539)	Encrypted Channel (T1573)	
				Process Injection (T1055)	Input Capture (T1056)		
				Input Capture (T1056)			

Çözüm Önerileri

1. Güncel antivirüs koruması kullanılmalı
2. Bilinmeyen kaynaklardan dosya indirilmemeli
3. Güvenilmeyen e-postalar açılmamalı, ekleri indirilmemeli
4. Teknoloji okuryazarı olunmalı
5. İşletim sistemi güncel tutulmalı
6. Kaynağı bilinmeyen linklere tıklanmamalı

HAZIRLAYAN

Betül ŞAHİN

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

