

NetWire

Teknik Analiz Raporu

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

İÇİNDEKİLER	i
ÖN İNCELEME	1
XOX.EXE ANALİZİ	2
STATİK ANALİZ	2
DİNAMİK ANALİZ	3
OTHNL.EXE ANALİZİ	4
DİNAMİK ANALİZ	5
KIPIRKIPİR.EXE ANALİZİ	7
STATİK ANALİZ	7
DİNAMİK ANALİZ	9
YARA KURALI	12
MITRE ATTACK TABLOSU	14
ÇÖZÜM ÖNERİLERİ	14
HAZIRLAYAN	15

Ön İnceleme

NetWire ailesine ait olan yazılım, kayıtlı kimlik bilgileri, klavye vuruşları gibi kullanıcı hareketlerini takip eden ve uzak sunucudan gelen komutları yürütebilen RAT türünde bir zararlı yazılımdır. Bu tehdit MS Office Dökümanları, PDF içeriğindeki indirme linkleri ve payload içeren sıkıştırılmış dosyalar ile yayılmaktadır.

Enfekte edilen cihazlardan elde edilen bilgilerden bazıları şunlardır;

- Tarayıcı kimlik bilgileri,
- Klavye tuş vuruşları,
- Kayıt defteri manipülasyonu,
- Cihaz özellikleri ve dosya bilgileri,
- Uzaktan erişim

xox.exe Analizi

Adı	xox.exe
MD5	5c9ad0440fef31403bd944a1a10a3b8
SHA256	2b1245c4547eee5a4545431f1969ab4dd5ba8ac4d0d2dd758d3c77a250e6ddb8
Dosya Türü	PE32 / EXE

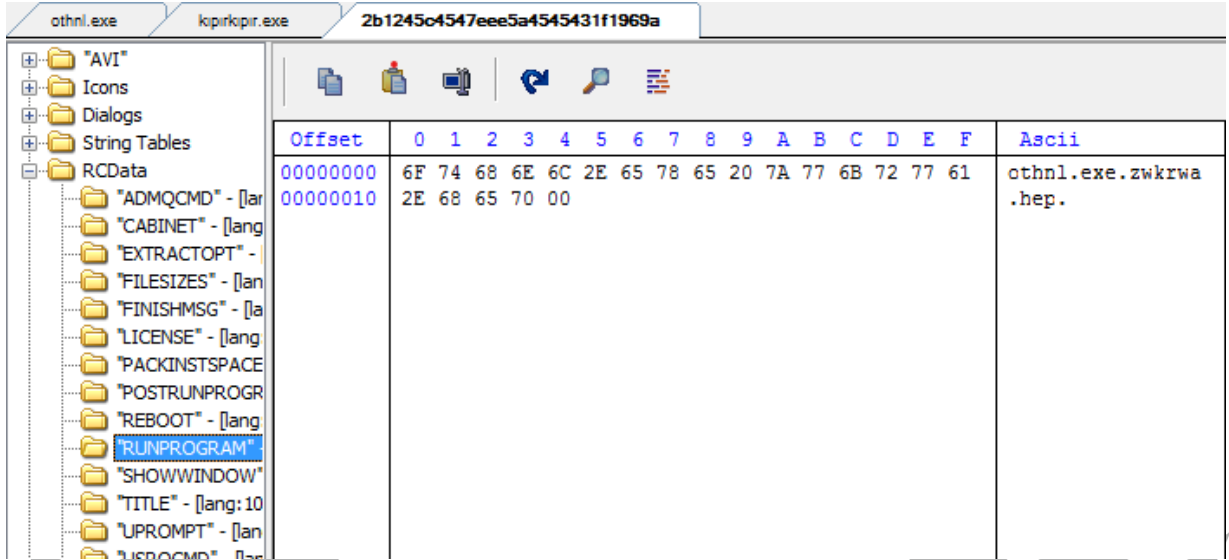
Statik Analiz

Zararlı dosya, **Microsoft Cabinet File (MSCF)** ile arşivlenmiş olarak gelen dosyaları kullanarak zararlı aktivitelerini meydana getirmektedir. Çalıştırıldığında yapacağı işlemlerle kalıcılık, info stealer gibi işlemleri gerçekleştirmektedir.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	53	43	46	00	00	00	00	20	3F	12	00	00	00	00	00	MSCF.....?].
00000010	2C	00	00	00	00	00	00	00	03	01	01	00	03	00	00	00	,.....' .l..
00000020	97	0C	00	00	7E	00	00	00	5D	0E	03	15	00	58	0E	00	-[.....]P..Xp.
00000030	00	00	00	00	00	00	49	49	9A	7A	20	00	6F	74	68	6EIİşz..othn
00000040	6C	2E	65	78	65	00	B8	8E	1B	07	00	58	0E	00	00	00	l.exe., +.Xp...
00000050	FF	54	2B	B3	20	00	7A	77	6B	72	77	61	2E	68	65	70	ÿT+'.zwwrwa.hep
00000060	00	00	46	04	00	B8	E6	29	07	00	00	FF	54	2A	B3	20	..E'.æ)•..ÿT*'.
00000070	00	6C	79	7A	62	6F	6C	63	74	2E	6F	73	6E	00	AE	59	.lyzbolct.osn.eY
00000080	24	EB	A0	4C	00	80	5B	80	80	8D	15	10	60	14	00	00	şè L.€[€€ +`q..
00000090	22	63	60	24	00	00	5E	00	EA	EA	6E	B9	E4	5E	20	20	"c`\$..^..êên'a^..

Şekil 1- MSCF ve çıkarılacak dosyalar

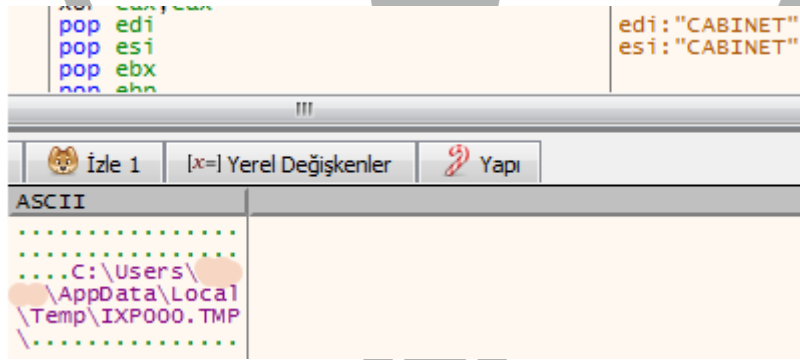
MSCF, ".cab" uzantısına sahip dosyalar çeşitli Windows yüklemelerine ilişkin verileri depolamaktadır. Çıkarılacak uygulamalar ".cab" (MSCF) dosyası içerisinde açıkça görülmektedir. Çalıştırıldığında hedeflenmiş dizine dosyaları kaydetmektedir.



Şekil 2- Kaynak görünümü

Kaynaklarında bulunan “**RUNPROGRAM**” ile dosyanın nasıl çalıştırılacağı bilgisine ulaşılmaktadır. “**Othnl.exe**”, “**zwkrwa.hep**” dosyasını parametre olarak çalıştırdığında zararlı aktiviteler gerçekleşmektedir.

Dinamik Analiz



Şekil 3- Çıkarılan dosya konumu

Şekil-3’de hafızada belirtilen “**C:\Users\%USERNAME%\AppData\Local\Temp**” dizinine oluşturulan “**IXP000.TMP**” klasörünün içine dosyaları geçici olarak tutmak amacıyla çıkarmaktadır.

Ad	Değiştirme tarihi	Tür	Boyut
lyzbolct.osn	31.07.2022 22:25	OSN Dosyası	274 KB
othnl.exe	09.10.2016 15:20	Uygulama	918 KB
zwwrwa.hep	31.07.2022 22:25	HEP Dosyası	116.452 KB

Şekil 4-Çıkarılan dosyalar

Zwwrwa.hep dosyası **othnl.exe**'ye parametre olarak verilmeli aksi takdirde **othnl.exe** yalnızca **AU3** uzantılı dosyaları yürütmek üzere komut bekleyen bir yazılım olarak gelmektedir. Zararlı aktivitelere sahip olan yazılım Şekil-4'te görülen othnl.exe (Autolt V3, 3, 10, 0) ile yüklenmektedir. Ayrıca **lyzbolct.osn** encrypt edilmiş bir dosyadır.

Othnl.exe Analizi

Adı	Othnl.exe
MD5	ad5e6eb33f8b6b48fab6d9ab3e1212c1
SHA256	dd998d69304649d295691a188f8d0b04b4c2ca5dc7fb03494867bd7738200daa
Dosya Türü	PE32 / EXE

Dinamik Analiz

```

01354ABA 5F          pop edi
01354ABB 8052 04    lea edx,dword ptr ds:[edx+4]
01354ABE 41        inc ecx
01354ABF 8B02      mov eax,dword ptr ds:[edx]
01354AC1 66:3978 08      cmp word ptr ds:[eax+8],d1
01354AC5 75 F4     jne othnl.1354A8B
01354AC7 8B55 D8   mov edx,dword ptr ss:[ebp-28]
01354ACA 894D DC   mov dword ptr ss:[ebp-24],ecx
01354ACD 8B45 DC   mov eax,dword ptr ss:[ebp-24]
01354AD0 8B4B 04   mov ecx,dword ptr ds:[ebx+4]
01354AD3 83CF FF   or edi,FFFFFFFF
01354AD6 85C0     test eax,ecx
01354AD8 74 04     je othnl.1354ADE
01354ADA 48       dec eax
01354ADB 8945 DC   mov dword ptr ss:[ebp-24],eax
01354ADE 8B45 F0   mov eax,dword ptr ss:[ebp-10]
01354AE1 66:85C0   test ax,ax
01354AE4 8B45 F8   mov eax,dword ptr ss:[ebp-8]
01354AE7 0F85 68FFFFFF jne othnl.1354A55
01354AE8 8B45 CC   mov eax,dword ptr ss:[ebp-34]
01354AF0 8B00     mov eax,dword ptr ds:[eax]
01354AF2 83F8 13   cmp eax,13

```

Şekil 5- Kalıcılık sağlamak için kullanılan komut

Zararlı , cihazda devamlılığını sürdürebilmek için görev zamanlayıcısı yönetim uygulaması olan **schtasks.exe**'yi komut satırı ile aktive ederek her 5 dakikada bir zararlı uygulamasını başlatarak kalıcılık sağlamaktadır.
(schtasks /create /sc minute /mo 5 /tn %s)

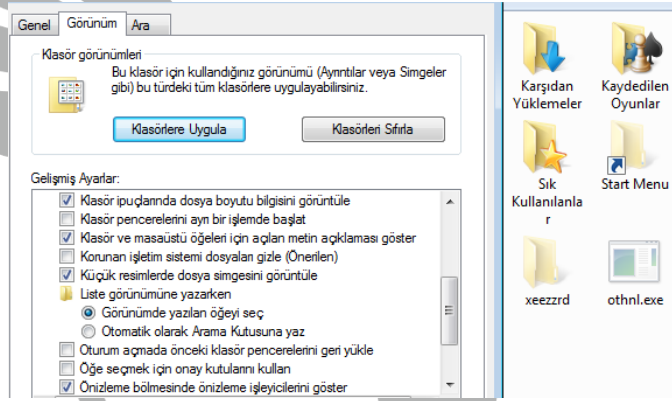
```

012A482E 50          push  eax
012A482F 8BCF      mov  ecx,edi
012A4831 C747 0C 01000000  mov  dword ptr ds:[edi+C],1
012A4838 C707 00000000  mov  dword ptr ds:[edi],0
012A483E E8 CDDFFFFFFF  call othnl.12A2810
012A4843 8B4D 08    mov  ecx,dword ptr ss:[ebp+8]
012A4846 8B45 0C    mov  eax,dword ptr ss:[ebp+C]
012A4849 8B30      mov  esi,dword ptr ds:[eax]
012A484B 8B43 04    mov  eax,dword ptr ds:[ebp-4]
012A484E 8B04B0    mov  eax,dword ptr ds:[eax+esi*4]
012A4851 66:8378 08 4E  cmp  word ptr ds:[eax+8],4E
012A4856 0F84 E0040000  je   othnl.12A403C
012A485C 837F 0C 05  cmo  dword ptr ds:[edi+C],5

```

Şekil 6- Zararlı dosya klasörü

Othnl.exe “C:\Users%\USERNAME%\xeezzrd” dizinini oluşturup zararlısını bu dizine kaydetmektedir . Şayet bu izin mevcut ise **zararlı bir aktivite görülmemektedir**.



Şekil 7- Kalıcılık için gizleme işlemi

Görünüm sekmesinden “**Korunan işletim sistemi dosyaları gizle**” seçeneği kapatılınca oluşturulan dosya ve klasör gözükmemektedir. Saldırgan bu yöntemle kendi uygulamalarını sisteme aitmiş gibi göstererek tespiti zorlaştırmayı hedeflemektedir.

```

0000007F
00000000
00000000
00820000
00000001
009C8340
00000000
00000000
00000000
01370000
00000000
00000000
00990000
00000000
00000000
00990000
L"inject1 = $unicode_windows & "\\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe"
L"inject1 = $unicode_windows & "\\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe"

```

Şekil 8-Process injection

Process Injection “RegSvcs.exe” legal yazılımı üzerine uygulanmaktadır . Bu sayede güvenlik uygulamaları tarafından tespit edilmemeyi hedeflemektedir. Aynı zamanda analizi zorlaştırmaktadır.

wintoolservice.exe		1.340 K	5.176 K	2552 VMware SVGA Helper Service	VMware, Inc.
wintools64.exe		14.592 K	27.340 K	2560 VMware Tools Core Service	VMware, Inc.
x32dbg.exe		61.724 K	87.996 K	2920 x64dbg	
pthnl.exe		3.908 K	11.360 K	3060 AutoIt v3 Script	AutoIt Team
pthnl.exe	Susp...	131.144 K	130.904 K	3692 Microsoft .NET Services Inst...	Microsoft Corporat...
ida.exe		272.248 K	256.104 K	348 The Interactive Disassembler	Hex-Rays SA
gozcu64.exe		21.400 K	39.820 K	160 Sysintemals Process Explorer	Sysintemals - www.
jusched.exe		2.432 K	8.420 K	2612 Java Update Scheduler	Oracle Corporation
juchek.exe		4.408 K	13.680 K	2380 Java Update Checker	Oracle Corporation

Şekil 9- Process Hollowing

İşlem “Suspend” olarak başlatılmakta ayrıca adından ve dosya boyutlarından da “RegSvc.exe” olmadığı açıkça gözlemlenmektedir. Kendini **Process Hollowing** tekniği ile **legal** bir işlem gibi göstermektedir.

192.168.247.2	192.168.247.128	DNS	183 Standard query response 0x9fd4 A banqueislamik.ddrive.online
192.168.247.128	46.246.12.18	TCP	66 49250 → 3360 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
192.168.247.128	162.243.25.33	TCP	66 49251 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
192.168.247.128	46.246.12.18	TCP	66 [TCP Retransmission] 49250 → 3360 [SYN] Seq=0 Win=8192 Len=0
192.168.247.128	162.243.25.33	TCP	66 [TCP Retransmission] 49251 → 443 [SYN] Seq=0 Win=8192 Len=0
fe80::8d4b:33b7:9a2-ff02::1:2	ff02::1:2	DHCPv6	157 Solicit XID: 0xfcc0e2 CID: 0001000127d92ada000c29df205a
192.168.247.128	46.246.12.18	TCP	62 [TCP Retransmission] 49250 → 3360 [SYN] Seq=0 Win=8192 Len=0
192.168.247.128	162.243.25.33	TCP	62 [TCP Retransmission] 49251 → 443 [SYN] Seq=0 Win=8192 Len=0

Şekil 10- Kontrol sunucusuna ait IP ve Domain

Zararlı, **devamlı** olarak komuta kontrol sunucusuna bağlanmayı denemektedir. Burada bağlantı alınamadığı için işlem sürekli tekrar etmektedir.

```

UDrj\F4YOW6W85\D
Y542d Md5Qs\XR65
Ciids FWlsWRdR56
...NetWire.SOFT
WARE\...cmd.exe
/C ping 1.1.1.1
-n 1 -w 3000 > N
ul & Del /f /q "
$s".HostId..SOFT
WARE\NetWire....
Install Date....

```

Şekil 11-CMD Scripti

Şekildeki CMD Script'i ile network bağlantısı kontrol edilip ardından kendini silmektedir. Ayrıca “**NetWire SOFTWARE**” metni ve şifrelenmiş dosya dizinleri açıkça gözlemlenmektedir.

```
cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "s"
```


Kıpırkıpır.exe Analizi

Adı	kıpırkıpır.exe
MD5	5b7e592b91d231807c75fd166e51e144
SHA256	45803a77c6a4211b8d7a342c9d9fc4625e90bbc9195675e01191638b8f05718a
Dosya Türü	PE32 / EXE

Statik Analiz

Saldırgan, enfekte olan cihazlardan **tarayıcı kimlik bilgileri** ve **parolalarını** çalmayı hedeflemektedir . Aşağıdaki tabloda hedeflenen bazı tarayıcılar mevcuttur.

Google\Chrome\User Data\Default>LoginDataCopy	Google\Chrome\User Data\Default>Login Data
Google\Chrome\User Data\Local State	Chromium\User Data Default>LoginDataCopy
Chromium\User Data\Default>Login Data	Chromium\User Data\Local State
Comodo\Dragon\User Data\Default>LoginDataCopy	Comodo\Dragon\User Data\Local State
BraveSoftware\Brave-Browser\User Data\Default>LoginDataCopy	Yandex\YandexBrowser\User Data\Default>LoginDataCopy
Yandex\YandexBrowser User Data\Default>Login Data	Comodo\Dragon\User Data\Default>Login Data
Yandex\YandexBrowser\User Data\Local State	360Chrome\Chrome\User Data\Local State
BraveSoftware\Brave-Browser\User Data\Default>Login Data	Brave Software\Brave-Browser\User Data\Local State
360 Chrome\Chrome\User Data\Default>LoginDataCopy	Opera Software\Opera Stable>Login Data
Opera Software\Opera Stable>LoginDataCopy	Opera Software\Opera Stable\Local State

Hedeflenmiş olan çeşitli tarayıcılar üzerindeki hassas verilere ait dosya yollarının bir kısmı tablo üzerinde gösterilmektedir.

Aşağıdaki tablolarda gösterilen metinler saldırgan tarafından **substitution (yer değiştirme)** yöntemi ile şifrelenmiş olup çalışma zamanında decode edilmektedir.

9HGGpEd5XR5dOR CIHdZMIW5	9HGGpDQ5ld R54YC5d	9mpcC6do OadywSd	MjPXqjFpx8 0ddX5d1	9HGGMarpa dYOZ55
9HGGp_OddMiw5	LMMPMIQ5S WER	67145dNp WsR	67i45dNpYi W6d	67i45dNpsOd sCodp2h
67i45dNp65ds	67145dNpYWI QIRp5df5	MT_qUDrjF Wk4ii	PQO0dR5zd 064WR	IWkniQd.Sii
6didY5 * 80WI IWkpiWn4R6	XR65Cii a40dY5WOZ	IWKQ5416. Sii	IWk67i45dN .Sii	QYO5VC6d. Sii
MT_qUDrj\FWk4iiC\ %6%\%6\FC4R	%6\FWk4iiC_ 40d8Wf %6	2YOQR541 dGOy.Sii	162YsGOy. Sii	MT_qUDrj\F Wk4iiC\ siYO.Sii
%6\FWk4iiC\ 40d8 Wf\so W84id6.4R4	%6\qIQR5JO V40S\%6	PQO0dR5z d064WR	R6500.Sii	
%6\qIQRSDOV40S\ s0W84id6.4R4	XR65Cii a40dY5WOZ	siS60.Sii	162YOGYy. Sii	R66054iN.Sii
MT_qUDrj\FWk4jC\ %6%\%6\FC4R	67145dN.Sii	6W85WwR N.Sii	162YOGhy. Sii	162YsGhy.Sii

Stringlerin çözümü için sözlük kullanılarak Python scripti oluşturulmuştur.

```

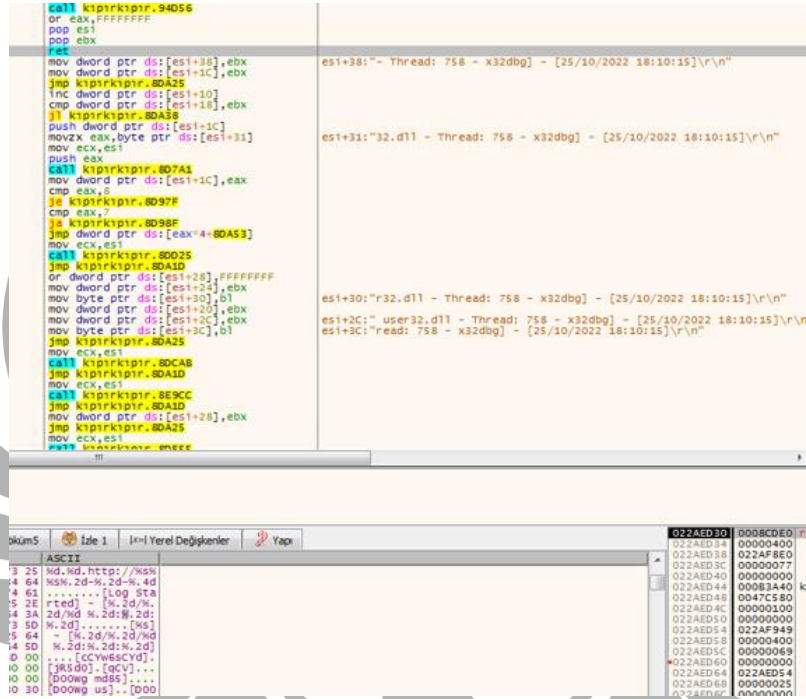
QY05VC6d.Sii = ucrtbase.dll
2Y0QR541dGOy.Sii = vcruntime140.dll
162YsGOy.Sii = msvcpl40.dll
lwkQ5416.Sii = mozutils.dll
lwkniQd.Sii = mozglue.dll
lwk67i45dN.Sii = mozsqlite3.dll
Fwk4iiC\MdCFWRwdZ\s0W84id6.4R4 = Mozilla\SeaMonkey\profiles.ini
64nRWR6.67i45d = signons.sqlite
iwn4R6.e6WR = logins.json
s00sid\CYVWQR56.fli = purple\accounts.xml
qIQR5d0V40S\s0W84id6.4R4 = Thunderbird\profiles.ini
67i45dNpYiW6d = sqlite3.close
67i45dNpWsdR = sqlite3.open
67i45dNps0dsC0dp2h = sqlite3.prepare.v2
67i45dNp65ds = sqlite3.stap
67i45dNpYiQIRp5df5 = sqlite3.column.text
6didY5 * 80WI lwkpiWn4R6 = select * from moz.logins
IW65RCld = hostname
MFq9 9C66gW0S = SMTP password
jDM u6d0 = EAS User
jDM Md02d0 urm = EAS Server URm
jDM 9C66gW0S = EAS password
Y0Zs5Nh.Sii = crypt32.dll
P0Zs5uRs0W5dY5aC5C = CryptUnprotectData
4R5df.SC5 = index.dat
2CQ15Yi4.Sii = vaultcli.dll
zCQ15TsdRzCQ15 = VaultOpenVault
zCQ15P1W6dZCQ15 = VaultCloseVault
zCQ15jRQld0C5dX5d16 = VaultEnumerateItems
zCQ15Ed5X5d1 = VaultGetitem
6Z65d1NH\Y1S.dfd = system32\cmd.exe
Ed5LC542dM265d1XR8 = GetNativeSysteminf
wd0Rd1NH.Sii = kernel32.dll
EiW(CiFd1W0ZM5C5Q6jf = GlobalMemoryStatusEx
-DraUDrj jMPPrX9qXTL\WZ65d1\PdR50C190WYd66W0y = HARDWARE ESCRipTION\System\Centralprocessor\0
D1iWYc5dDR5XR454C14kdW4S = AllocateAndInitializeSid
P1dYwqWdRFd1Vd0614s = CheckTokenMembership
jMPPrX9qXTL = ESCRipTION

```

Şekil 12-Metin çözümleri

Metinler arasında **SQL sorgusu, tarayıcıya ait bilgiler, şifreler** ile alakalı birçok işlem olduğu gözükmemektedir.

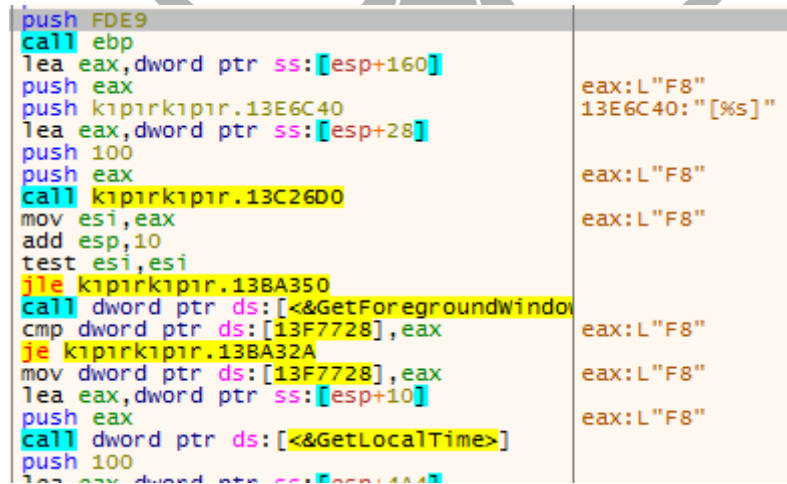
Dinamik Analiz



```
call k1p1rk1p1r.94056
or eax,FFFFFFFF
pop esi
pop ebx
ret
mov dword ptr ds:[esi+30],ebx
mov dword ptr ds:[esi+1C],ebx
jmp k1p1rk1p1r.80A25
inc dword ptr ds:[esi+10]
cmp dword ptr ds:[esi+18],ebx
j1 k1p1rk1p1r.80A38
push dword ptr ds:[esi+1C]
movzx eax,byte ptr ds:[esi+31]
mov ecx,esi
push eax
call k1p1rk1p1r.807A1
mov dword ptr ds:[esi+1C],eax
cmp eax,0
je k1p1rk1p1r.8097F
cmp eax,0
ja k1p1rk1p1r.8098F
jmp dword ptr ds:[eax*4+80A53]
mov ecx,esi
call k1p1rk1p1r.80D25
jmp k1p1rk1p1r.80A1D
or dword ptr ds:[esi+28],FFFFFFFF
mov dword ptr ds:[esi+28],ebx
mov byte ptr ds:[esi+30],b1
mov dword ptr ds:[esi+20],ebx
mov dword ptr ds:[esi+2C],ebx
mov byte ptr ds:[esi+3C],b1
jmp k1p1rk1p1r.80A25
mov ecx,esi
call k1p1rk1p1r.80CAB
jmp k1p1rk1p1r.80A1D
call k1p1rk1p1r.BE9CC
jmp k1p1rk1p1r.80A1D
mov dword ptr ds:[esi+28],ebx
jmp k1p1rk1p1r.80A25
mov ecx,esi
push FDE9
call ebp
lea eax,dword ptr ss:[esp+160]
push eax
push k1p1rk1p1r.13E6C40
lea eax,dword ptr ss:[esp+28]
push 100
push eax
call k1p1rk1p1r.13C26D0
mov esi,eax
add esp,10
test esi,esi
jle k1p1rk1p1r.13BA350
call dword ptr ds:[<&GetForegroundWindow]
cmp dword ptr ds:[13F7728],eax
je k1p1rk1p1r.138A32A
mov dword ptr ds:[13F7728],eax
lea eax,dword ptr ss:[esp+10]
push eax
call dword ptr ds:[<&GetLocalTimes]
push 100
lea eax,dword ptr ss:[esp+144]
```

Şekil 13-Log dosyası (DD:MM:YYYY)

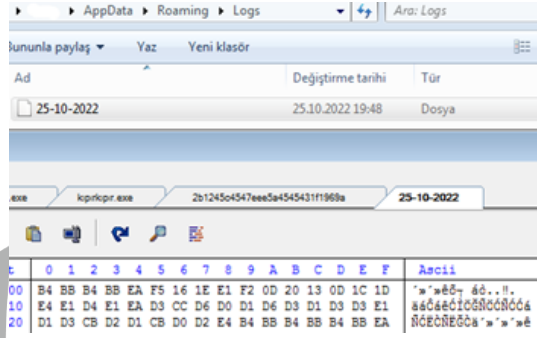
Log dosyasına kaydetmek için elde edilen bilgilerin şifrlenmeden önceki durumu gözlemlenmektedir.



```
push FDE9
call ebp
lea eax,dword ptr ss:[esp+160]
push eax
push k1p1rk1p1r.13E6C40
lea eax,dword ptr ss:[esp+28]
push 100
push eax
call k1p1rk1p1r.13C26D0
mov esi,eax
add esp,10
test esi,esi
jle k1p1rk1p1r.13BA350
call dword ptr ds:[<&GetForegroundWindow]
cmp dword ptr ds:[13F7728],eax
je k1p1rk1p1r.138A32A
mov dword ptr ds:[13F7728],eax
lea eax,dword ptr ss:[esp+10]
push eax
call dword ptr ds:[<&GetLocalTimes]
push 100
lea eax,dword ptr ss:[esp+144]
```

Şekil 14-Mevcut process API ve üzerindeki tuş vuruşu

Kullanılan API ile anlık uygulamayı tespit edip ardından uygulama içinde yapılan tuş vuruşlarını kaydetmektedir ve bu şekilde log verileri toplamaktadır.



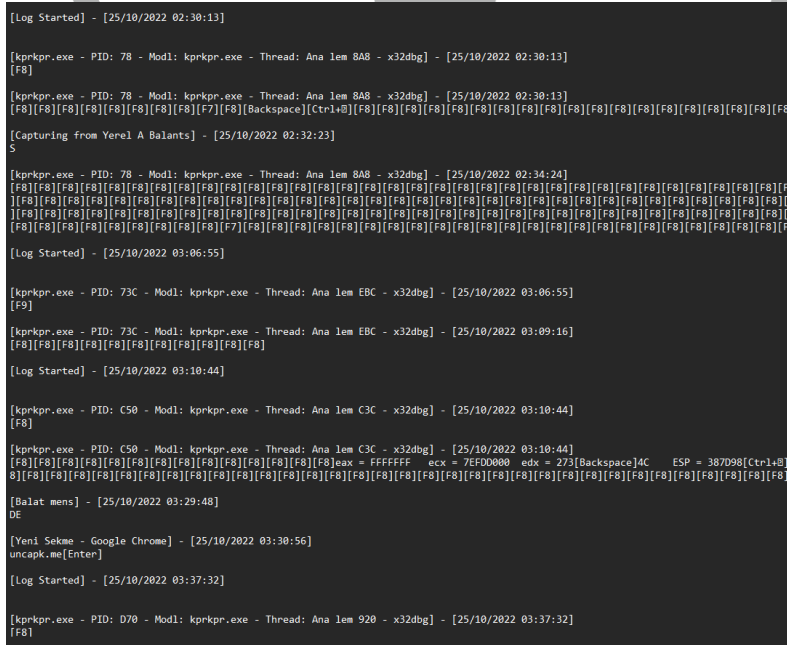
Şekil 15-Dosya yolu & dosya & şifreli loglar

“AppData\Roaming\Logs” dizinine (tarih, dosya adı mahiyetinde kullanılarak) oluşturulan ve içerisinde şifrelenmiş halde kaydedilen tuş vuruşları ve pencere bilgisi komuta kontrol sunucusuna gönderilmek için görseldeki şekilde tutulmaktadır.

```
mov al,byte ptr ds:[ecx+esi]
xor al,90
add al,24
mov byte ptr ds:[ecx+esi],al
```

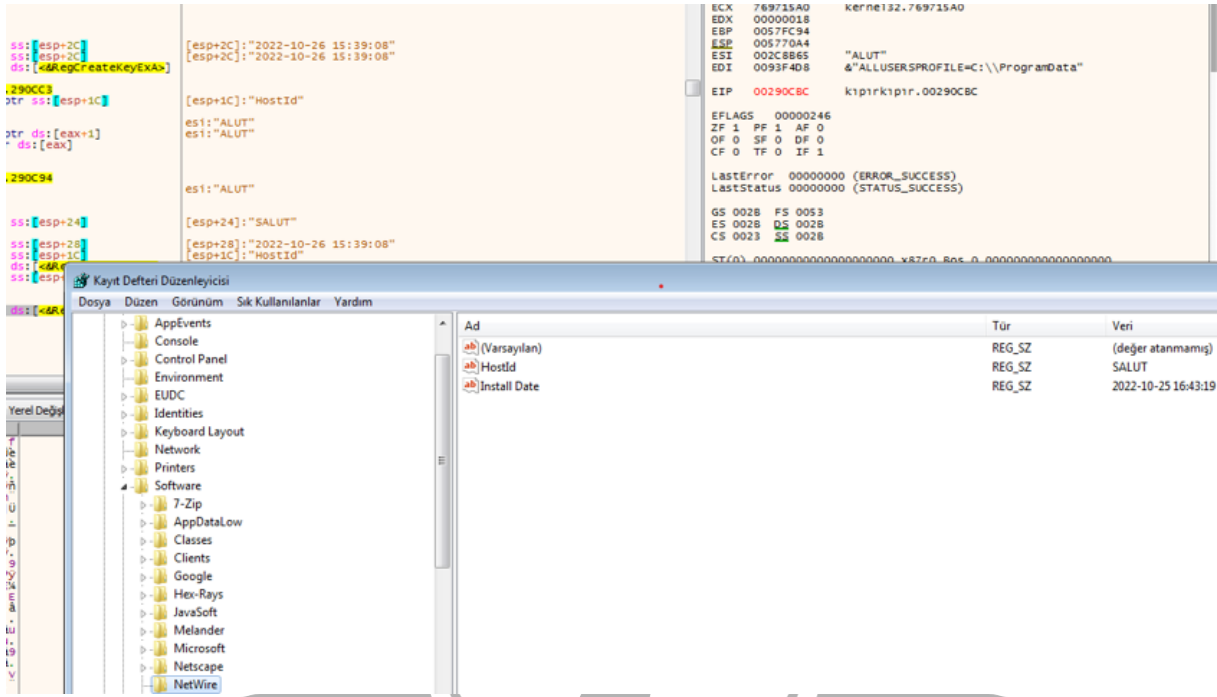
Şekil 16-Encryption

Görseldeki işlem uygulanarak kaydedilen veriler şifrelenmektedir. Bu işlemin tersi uygulanarak verilerin ham hali elde edilmektedir.



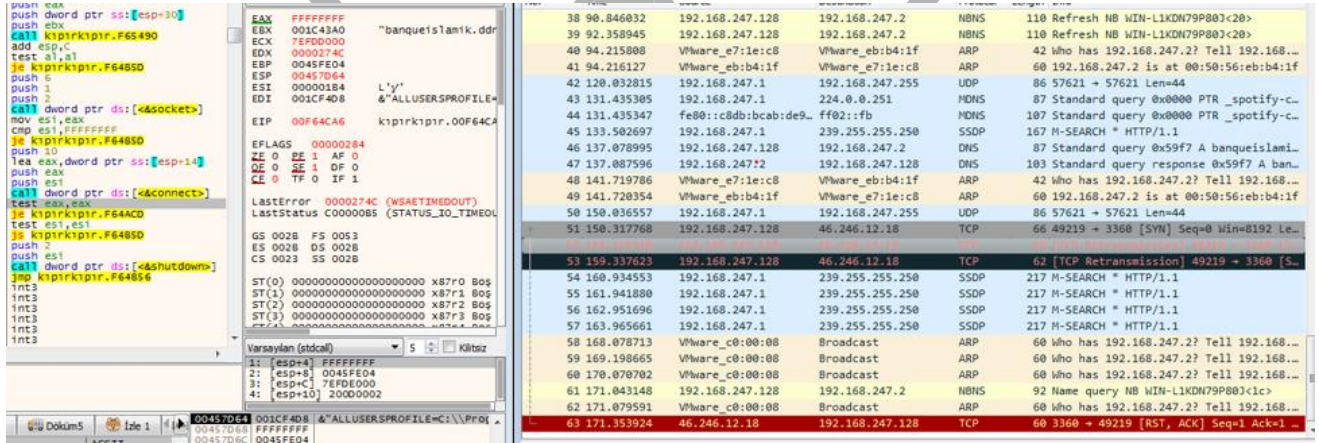
Şekil 17-Çözülen loglar

Tüm klavye ve uygulama etkinlikleri şifrelenmiş halde bulunmaktadır. Çözülmemiş hali şekil-17’de görülmektedir. Saldırgan bu yöntem ile kullanıcıya ait **kredi kartı, banka, hesap bilgileri** gibi hassas verileri ele geçirebilmektedir.



Şekil 18-Kayıt defteri aktivitesi

Yeni kayıt oluşturularak **Hostid** değeri ve **Install Date** kayıt defterine “**NetWire**” dizini altına eklenmektedir.



Şekil 19- TCP bağlantısı

Sokete bağlanmayı denemekte fakat **RST paketi** alınıyor çünkü server halihazırda kapalı bir vaziyette beklemektedir. (banqueislamık[.]ddrive[.]online:3360)

YARA Kuralı

```
import "hash"

rule xox

{

  meta:

    author = "enessakircolak"

    date = "28.10.2022"

  strings:

    $a = "zwrwa.hep"

    $b = "othnl.exe"

    $c = "lyzbolct.osn"

    $d = "ISOBURN.EXE.MUI"

    $e = "POSTRUNPROGRAM"

    $f = "IXP000.TMP"

  condition:

    hash.m5(0,filesize) == "5c9ad0440fefa31403bd944a1a10a3b8" or all of
    them

}
```

```
import "hash"

rule kprkpr

{

  meta:

    author = "enessakircolak"

    date = "28.10.2022"

  strings:

    $a = "SOFTWARE\NetWire"

    $b = "Cs43l63g4R3YW0d34R5d0iWYwdS3iG3G3y.Sii"

    $c = "%%.2d/%.2d/%d %.2%.4d-%.2d-%.2d %GRN9sY1n3Ppc7g-
CIJWhj0m5o2ErLt6vQASx4VuXdZibUley_BqwHaF8TkKDMfOz%s"

    $d = "http://%s%%s%.2d-%.2d-%.4d"

    $e = "MT_qUDrj\F4Y0W6W85\U4RSWg6\PQ00dR5zd064WR\rQR\"

    $f="Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CF
F0413111d3B88A00104B2A6676"

    $g = "banqueislamik.ddrive.online:3360"

  condition:

    hash.md5(0,filesize) == "5b7e592b91d231807c75fd166e51e144" or
any of ($g, $a, $e) or all of ($b, $c, $d, $f)

}
```

MITRE ATTACK TABLOSU

Reconnaissance	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	C&C	Exfiltration
Gather Victim Host Information (T1592)	Windows Command Shell (T1059)	Scheduled Tasks/Job (T1053.005)	Manipulate System Process (T1053)	Hidden Files and Directories (T1564.001)	OS Credential Dumping (T1003)	Remote Access Software (T1219)	Exfiltration Over C2 Channel (T1041)
Hardware (T1592)	Scheduled Task (T1053)	Startup Folder (T1547.001)	Process Injection (T1055)	File / String Obfuscation (T1027)	Credentials From Web Browsers (T1606)	Application Layer Protocol (T1071)	
	Startup Folder (T1547.001)	Modify System Process (T1543)	Registry Run Keys (T1547)	Anti-Debugger (T1622)	Keylogging (T1056)	Encrypted Channel (T1573)	
				Software Packing (T1027)			

Çözüm Önerileri

1. Sistem güncel tutulmalıdır.
2. Hedef adrese bakılmadan PDF içerisindeki linklere tıklanmamalıdır.
3. Ticari, bireysel, topluluk fark etmeksizin, e-mail dökümanları teftiş edilmelidir.
4. Her işlem çalışma anında denetlenmelidir.
5. Güvenilir bir anti-virüs yazılımı kullanılmalıdır.

HAZIRLAYAN

Enes Şakir Çolak

[LinkedIn](#)