



# HAWKEYE

CYBERDEFENDER

[HTTPS://CYBERDEFENDERS.ORG/BLUETEAM-CTF-  
CHALLENGES/91#NAV-QUESTIONS](https://cyberdefenders.org/blueteam-ctf-challenges/91#NAV-QUESTIONS)

Sudenur MURATOĞULLARI

## İçindekiler

Giriş(Introduction) .....	2
Metodoloji(Methodology) .....	2
Bulgular ve Analiz (Findings and Analysis) .....	2
Olay Zaman Çizelgesi (Timeline of Events).....	14
Sonuçlar(Conclusions).....	14



## Giriş(Introduction)

Bir şirketin muhasebecisine gönderilen bir e-posta, kötü amaçlı bir dosyanın muhasebecinin bilgisayarına düşmesine ve her 10 dakikada bir veri sızdırmasına neden oldu.

Kurban ve saldırgan hakkındaki bilgilere erişmeyi amaçlayarak bu saldırının trafiğini ve kötü niyetli e-postayı analiz edeceğiz.

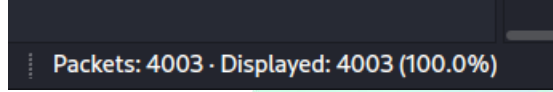
Kuruluş özel adresleme ve /24 ağ maskesi ile çalışmaktadır.

## Metodoloji(Methodology)

Analizimizde ağ trafiği için Wireshark aracını kullandık, IP adresi analizi içinse çevrimiçi toollardan faydalandık.

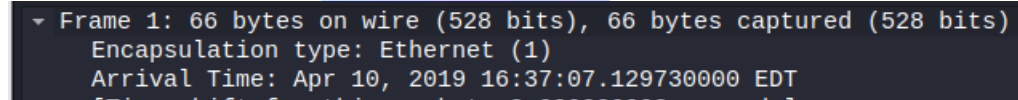
## Bulgular ve Analiz (Findings and Analysis)

Yakalamada 4003 paket var.

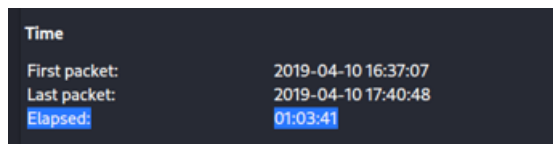
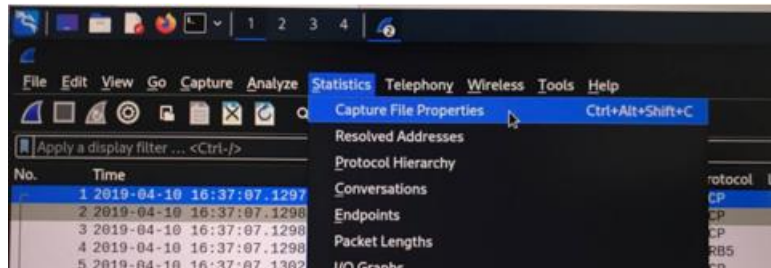


İlk paketin tarih ve saat bilgileri ekte EDT formatında gözükmemektedir. Koordineli Evrensel Saat(UTC) formatında bu tarih bilgisini düzenlememiz gerekmektedir.

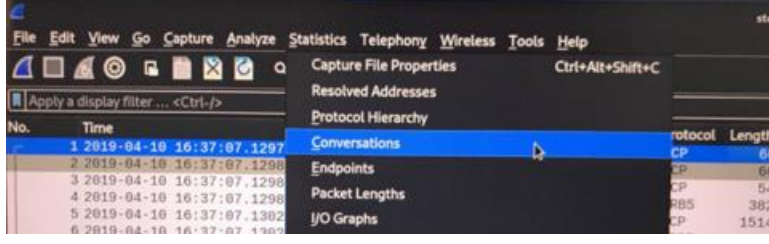
İlk paketin tarih ve saat bilgisi: 2019-04-10 20:37:07 UTC



Kaydedilen ağ trafiği paketlerinin yakalandığı süreye ulaşmamız gerekiyor. Statistics bölümünden yakalama dosyası özelliklerini inceleyerek elapsed bilgisine ulaşabiliriz.



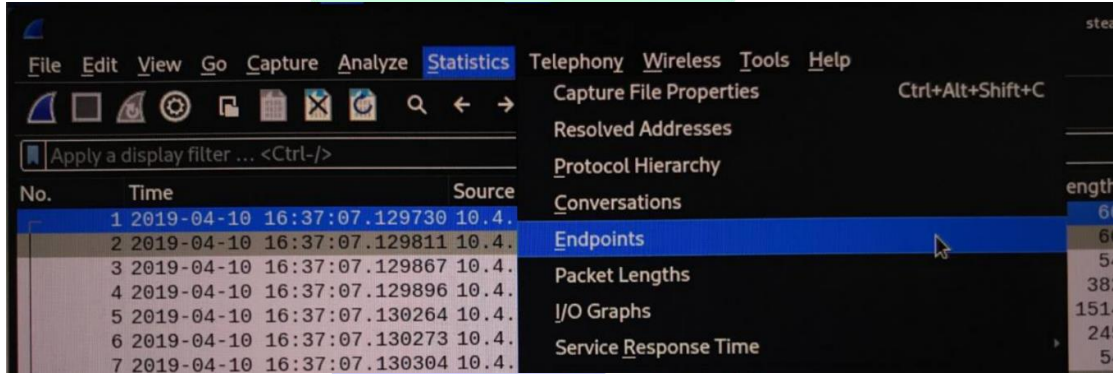
Aktif bilgisayarı bulmak için conversations (konuşmalar kısmında inceleme yapabiliriz.)



Ethernet - 6												
IPv4 - 11		IPv6	TCP - 39	UDP - 51								
Address A	Address B		Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:08:02:1c:47:ae	01:00:5e:00:00:16		23	1,229 KiB	23	1,229 KiB	0	0 bytes	109.878104	3651.2201	2 bytes	0 bytes
00:08:02:1c:47:ae	01:00:5e:00:00:fc		10	750 bytes	10	750 bytes	0	0 bytes	2663.801528	1096.9531	5 bytes	0 bytes
00:08:02:1c:47:ae	01:00:5e:7fff:fa		74	28,291 KiB	74	28,291 KiB	0	0 bytes	109.882622	3666.1008	63 bytes	0 bytes
00:08:02:1c:47:ae	20:e5:2a:b6:93:f1		3,352	2,138 MiB	1,576	107,064 KiB	1,776	2,034 MiB	47.459211	3730.4030	235 bytes	4,465 KiB
00:08:02:1c:47:ae	a4:1f:72:c2:09:6a		513	110,976 KiB	279	66,461 KiB	234	44,515 KiB	0.000000	3821.5612	142 bytes	95 bytes
00:08:02:1c:47:ae	ff:ff:ff:ff:ff:ff		31	3,451 KiB	31	3,451 KiB	0	0 bytes	46.633556	2823.2623	10 bytes	0 bytes

Konuşmaları incelediğimizde en aktif cihazın 00:08:02:1c:47:ae mac adresine sahip cihaz olduğunu görüyoruz.

Bir başka yöntem de Endpoints kısmını incelemek.



Wireless - Enpoints - Statistics							
Ethernet - 7	IPv4 - 12	IPv6	TCP - 48	UDP - 58			
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	
00:08:02:1c:47:ae	3.909 KiB	2.279 MiB	1.946 KiB	207.229 KiB	1.963 KiB	2.077 MiB	
01:00:5e:00:00:16	23 bytes	1.229 KiB	0 bytes	0 bytes	23 bytes	1.229 KiB	
01:00:5e:00:00:fc	10 bytes	750 bytes	0 bytes	0 bytes	10 bytes	750 bytes	
01:00:5e:7f:ff:fa	74 bytes	28.291 KiB	0 bytes	0 bytes	74 bytes	28.291 KiB	
20:e5:2a:b6:93:f1	3.273 KiB	2.138 MiB	1.734 KiB	2.034 MiB	1.539 KiB	107.064 KiB	
a4:1f:72:c2:09:6a	513 bytes	110.976 KiB	234 bytes	44.515 KiB	279 bytes	66.461 KiB	
ff:ff:ff:ff:ff:ff	31 bytes	3.451 KiB	0 bytes	0 bytes	31 bytes	3.451 KiB	

Endpoints kısmını incelediğimizde mac adreslerinin en aktiften başlayarak sıralandığını görüyoruz. Bu incelememiz sonucunda da yine en aktif mac adresinin 00:08:02:1c:47:ae olduğu sonucuna ulaştık.

Şimdi bu mac adresini( 00:08:02:1c:47:ae) NIC'sinin üreticisini bulmak için sorgumuzda kullanacağız.

**Mac Adres Sorgulama Kutusu**

00:08:02:1c:47:ae

Sorgula

"MAC Adres" yazın ve "Sorgula" butonuna tıklayın.  
Örn: 30:8A:49:75:CB:34

**Mac Adresi "00:08:02:1c:47:ae" Sorgu Sonucu**

Hewlett Packard (was: Compaq Computer Corp)

Hawlett Packard bilgisini edindik.

Bu bilgiyi kullanarak da NIC üreticisinin merkezinin bulunduğu şehri bulabiliriz.

× 🔍 🗨️ 🔊 🔍

🔍 Tümü
🖼️ Görseller
🛒 Alışveriş
📰 Haberler
📺 Videolar
⋮ Daha fazla
Araçlar

Yaklaşık 74.000.000 sonuç bulundu (0,73 saniye)

Yazımı düzeltilmiş şu sorgu için sonuçları görüyorsunuz: **Hewlett Packard**  
Yine de şu sorguyu ara: **Hawlett Packard**

**Hewlett Packard Enterprise**  
<https://www.hpe.com> · Bu sayfanın çevirisini yap

**Hewlett Packard Enterprise (HPE)**  
From HPE's new high-end storage platform to driving the next wave of the Intelligent Edge and cloud choices, HPE delivers, and now HPE plans to deliver ...  
[About Us](#) · [Careers](#) · [High Performance Computing](#) · [Services](#)

**Wikipedia**  
<https://tr.wikipedia.org/wiki/Hewlett-Packard>

**Hewlett-Packard**  
Hewlett-Packard Company ya da kısaca **HP**, merkezi ABD'de Palo Alto, Kaliforniya'da bulunan çok büyük bir uluslararası şirkettir.  
[Alt birim/ler](#) · [Palm](#) · [TOWER Software](#) · [Genel merkezi: Palo Alto, Kaliforniya](#)

**Hewlett-Packard (HP)**  
Şirket

Hewlett-Packard Company ya da kısaca **HP**, merkezi ABD'de Palo Alto, Kaliforniya'da bulunan çok büyük bir uluslararası şirkettir. Bilgi işlem, baskı sistemleri ve sayısal görüntüleme donanımları üreticisidir. [Vikipedi](#)

**Hisse senedi fiyatı: HPQ** (NYSE)  
\$33,62 +0,19 (+%0,57)  
12 Tem 09:32 GMT-4 - Sorumluluk

**Genel merkezi:** [Palo Alto](#), Kaliforniya, ABD

Merkez Palo Alto'da.

"Kuruluş özel adresleme ve ağ maskesi /24 ile çalışır." Bilgisine sahibiz.

Wireshark aracının Endpoints kısmında bulunan IPv4 değerlerine bakarak kuruluştaki hangi IP adreslerinin yakalama işlemine dahil olduğunu gözlemliyoruz.

Ethernet · 7	IPv4 · 12	IPv6	TCP · 48	UDP · 58			
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	
10.4.10.2	42 bytes	4.512 KiB	0 bytes	0 bytes	42 bytes	4.512 KiB	
10.4.10.4	513 bytes	110.976 KiB	234 bytes	44.515 KiB	279 bytes	66.461 KiB	
10.4.10.132	3.909 KiB	2.279 MiB	1.946 KiB	207.229 KiB	1.963 KiB	2.077 MiB	
10.4.10.255	30 bytes	3.117 KiB	0 bytes	0 bytes	30 bytes	3.117 KiB	
23.229.162.69	280 bytes	37.810 KiB	161 bytes	12.790 KiB	119 bytes	25.020 KiB	
66.171.248.178	63 bytes	5.093 KiB	28 bytes	2.652 KiB	35 bytes	2.440 KiB	
216.58.193.131	20 bytes	8.034 KiB	11 bytes	5.582 KiB	9 bytes	2.452 KiB	
217.182.138.150	2.878 KiB	2.084 MiB	1.539 KiB	2.013 MiB	1.339 KiB	72.641 KiB	
224.0.0.22	23 bytes	1.229 KiB	0 bytes	0 bytes	23 bytes	1.229 KiB	
224.0.0.252	10 bytes	750 bytes	0 bytes	0 bytes	10 bytes	750 bytes	
239.255.255.250	74 bytes	28.291 KiB	0 bytes	0 bytes	74 bytes	28.291 KiB	
255.255.255.255	1 bytes	342 bytes	0 bytes	0 bytes	1 bytes	342 bytes	

SAYFA 4

İlk 4 IP adresi elimizdeki bilgiyle fakat 10.4.10.255 IP adresi kuruluştaki bir cihaza ait olamaz çünkü bir broadcast IP adresidir. (10.4.10.0/24 alt ağındaki tüm cihazlara yayın yapmak için kullanılır.) Bu durumda 3 bilgisayar yakalama işlemine dahil olmuş sonucuna vardık.

En aktif cihazlar genellikle ağdaki önemli etkinlikleri gerçekleştiren cihazlardır. Bu sebeple ağdaki en aktif bilgisayarın ismine bakacağız.

00:08:02:1c:47:ae MAC adresinin en aktif cihaza sahip olduğunu bildiğim için sadece bu MAC adresine gelen DHCP trafiğini görüntülemek istiyorum.

No.	Time	Source	Destination	Protocol	Length	Info
3263	649.194871	10.4.10.132	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xc0361803
3264	649.195335	10.4.10.4	10.4.10.132	DHCP	342	DHCP ACK - Transaction ID 0xc0361803

Broadcast IP adresinin bulunduğu pakette DHCP bölümünden Host Bilgilerini görebilmekteyiz. Host Name: BEIJING-5CD1-PC

```

> Frame 3263: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.4.10.132, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Inform)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xc0361803
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 10.4.10.132
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Inform)
  Option: (61) Client identifier
  Option: (12) Host Name
    Length: 15
    Host Name: Beijing-5cd1-PC
  Option: (60) Vendor class identifier
  Option: (55) Parameter Request List
Dynamic Host Configuration Protocol: Protocol

```

DHCP protokolü üzerinde bir filtreleme yaparken, broadcast mesajlarına odaklanmanın nedeni DHCP'nin IP adresi tahsis etmek için genellikle broadcast mesajlarını kullanmasıdır.

Saldırı tespiti ve soruşturmasında ve IP adresi ilişkilendirmesi gibi konularda fayda sağlayabileceğinden DNS sunucusunun IP adresini bulmamız gerekmekte.

İlk paket DNS isteğini veya yanıtını içerir ve bu paketi seçmek, DNS trafiğini odaklanarak incelemek için başlangıç noktasıdır.



No.	Time	Source	Destination	Protocol	Length	Info
116	26.247746	10.4.10.132	10.4.10.4	DNS	134	Standard query 0x9a2c SRV _
117	26.248011	10.4.10.4	10.4.10.132	DNS	213	Standard query response 0x9
118	26.248515	10.4.10.132	10.4.10.4	DNS	103	Standard query 0x3ee5 SRV _
119	26.248660	10.4.10.4	10.4.10.132	DNS	182	Standard query response 0x3
174	26.781921	10.4.10.132	10.4.10.4	DNS	76	Standard query 0x8701 A dns

▶ Frame 116: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)  
 ▶ Ethernet II, Src: HewlettP\_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell\_c2:09:6a (a4:1f:72:c2:09:6a)  
 ▶ Destination: Dell\_c2:09:6a (a4:1f:72:c2:09:6a)  
 ▶ Source: HewlettP\_1c:47:ae (00:08:02:1c:47:ae)  
 ▶ Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 10.4.10.132, Dst: 10.4.10.4  
 ▶ User Datagram Protocol, Src Port: 51699, Dst Port: 53

Ethernet II kısmında Source bölümü kurbanın Destination bölümü ise DNS sunucusunun MAC adresidir.

Kurbanın 204. Pakette proforma-invoices.com domainine istek attığını gözlemliyoruz.

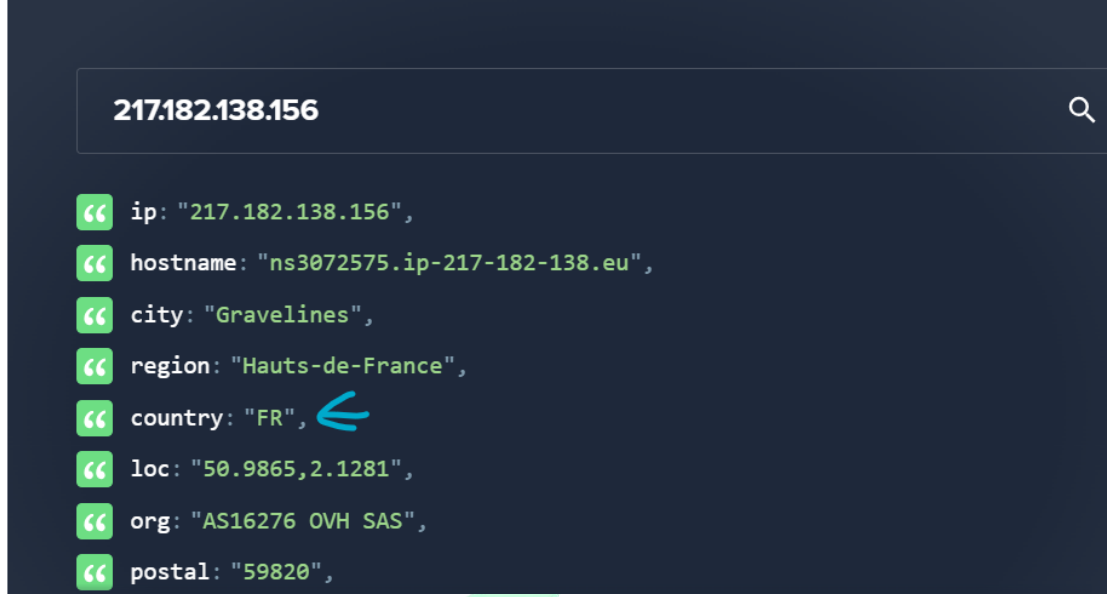
No.	Time	Source	Destination	Protocol	Length	Info
204	46.661287	10.4.10.132	10.4.10.4	DNS	81	Standard query 0xa002 A proforma-invoices.com

▶ Frame 204: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)  
 ▶ Ethernet II, Src: HewlettP\_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell\_c2:09:6a (a4:1f:72:c2:09:6a)  
 ▶ Internet Protocol Version 4, Src: 10.4.10.132, Dst: 10.4.10.4  
 ▶ User Datagram Protocol, Src Port: 54662, Dst Port: 53  
 ▶ Domain Name System (query)  
 Transaction ID: 0xa002  
 ▶ Flags: 0x0100 Standard query  
 Questions: 1  
 Answer RRs: 0  
 Authority RRs: 0  
 Additional RRs: 0  
 ▶ Queries  
 ▶ proforma-invoices.com: type A, class IN  
 [Response In: 206]

Bu domainin IP adresini bulmak için aşağıdaki sorguyla devam ediyorum.

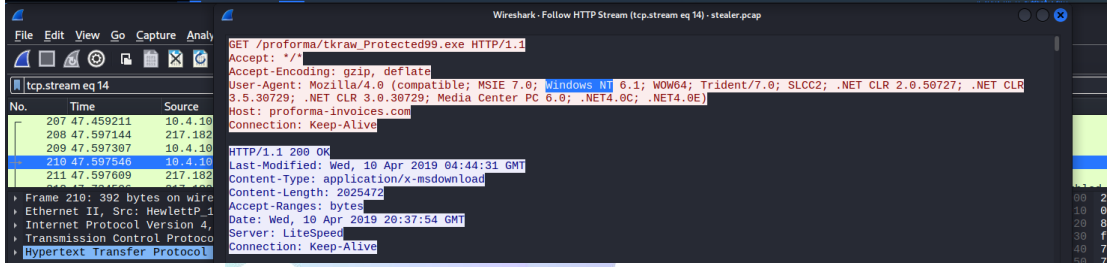
No.	Time	Source	Destination	Protocol	Length	Info
210	47.597546	10.4.10.132	217.182.138.150	HTTP	392	GET /pr

Destination bölümünde belirtilen 217.182.138.156 IP adresi proforma-invoices.com domainine aittir.



Basit bir sorgulama işlemiyle bu IP adresinin ait olduğu ülkeyi ve daha fazla bilgisine ulaşabiliyoruz.

Kurban bilgisayarının işletim sistemine bakacağız.



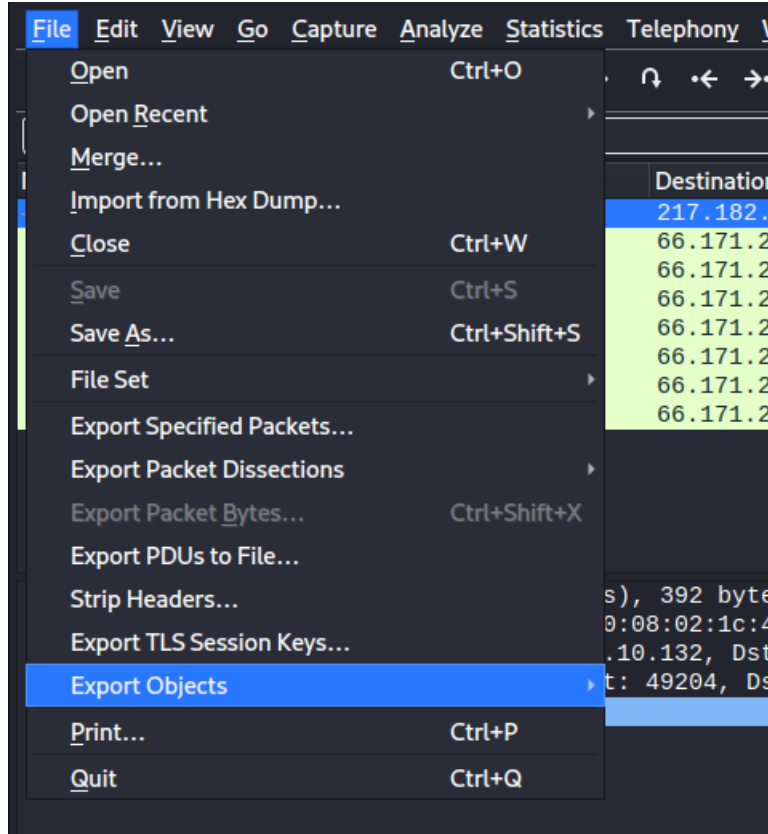
Kurbanın proforma-invoices.com domainine yaptığı isteğe ait olan paketin HTTP akışını takip ederek isteği atan bilgisayara ait işletim sistemi bilgisine erişiyoruz. Windows NT 6.1

İnternet faaliyetlerinin anlaşılması açısından HTTP GET isteklerini incelerken zararlı IP adresinden indirilen kötü amaçlı yazılımın tkraw\_Protected99.exe olduğunu bulduk. Dosya alan tek paket bu olduğundan başka bir dosya olmadığını da gözlemliyoruz.

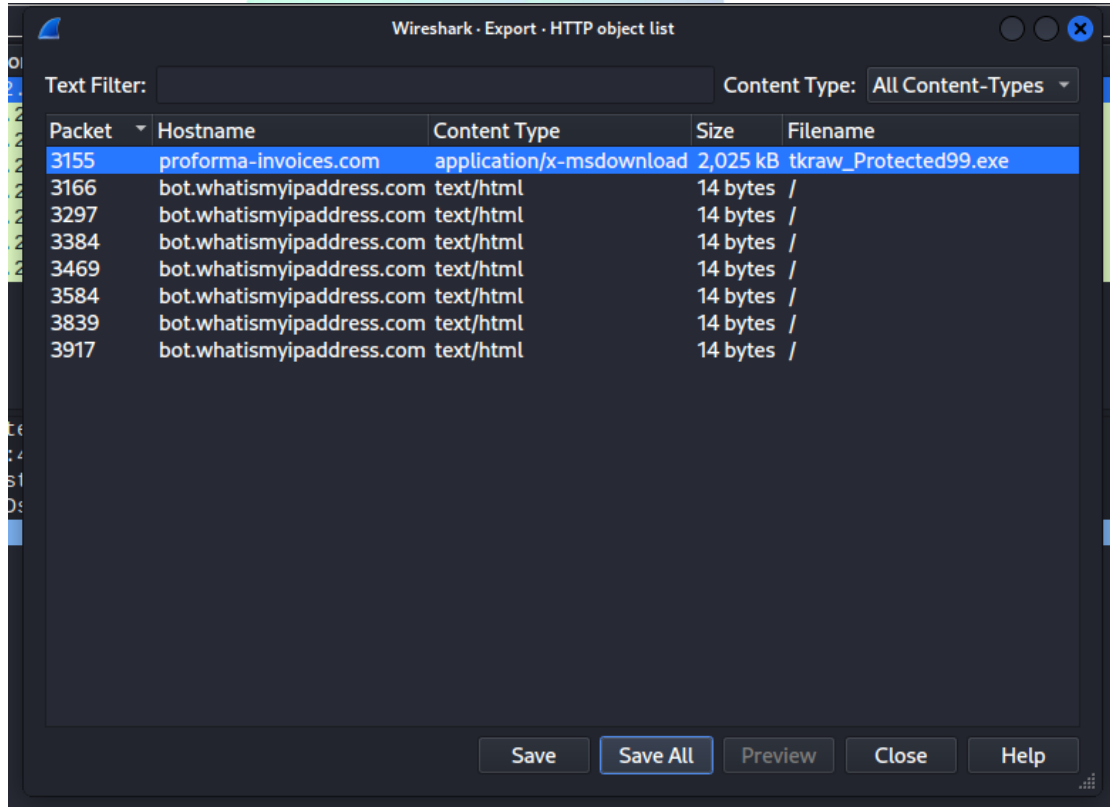
No.	Time	Source	Destination	Protocol	Length	Info
210	47.597546	10.4.10.132	217.182.138.150	HTTP	392	GET /proforma/tkraw_Protected99.exe HTTP/1.1
3164	68.640169	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3295	673.005938	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3382	1277.329651	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3467	1883.097476	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1
3582	2487.212975	10.4.10.132	66.171.248.178	HTTP	129	GET / HTTP/1.1

Şimdi bu dosyayı dışa aktararak dosya hakkında daha ayrıntılı bir analiz yapacağım.





Bu alanda HTTP seçeneğini seçerek devam ediyorum.



3155 'i seçerek kaydediyorum.

Dosyayı CyberChef'e attığımızda MD5 karmasını görmekteyiz.

The screenshot shows the CyberChef web interface. The 'Recipe' tab is active, displaying a list of operations on the left, including MD2, MD4, MD5, MD6, Microsoft Script Decoder, SM4 Decrypt, Median, Play Media, Hamming Distance, and From Decimal. The 'MD5' operation is selected. The 'Input' field contains a file named 'krav\_Protected99.exe' with a size of 2,025,472 bytes and a type of 'application/x-ms-dos-executable'. The 'Output' field displays the MD5 hash: 71826ba081e303866ce2a2534491a2f7. Below the CyberChef interface, a VirusTotal analysis is shown for the same file. The VirusTotal interface indicates that 56 security vendors and 2 sandboxes flagged the file as malicious. The file is identified as 'krav\_Protected99.exe' with a size of 1.93 MB and a last analysis date of 1 day ago. The VirusTotal interface also shows a 'Community Score' of 56/70 and a 'Popular threat label' of 'trojan.autoknymeria'.

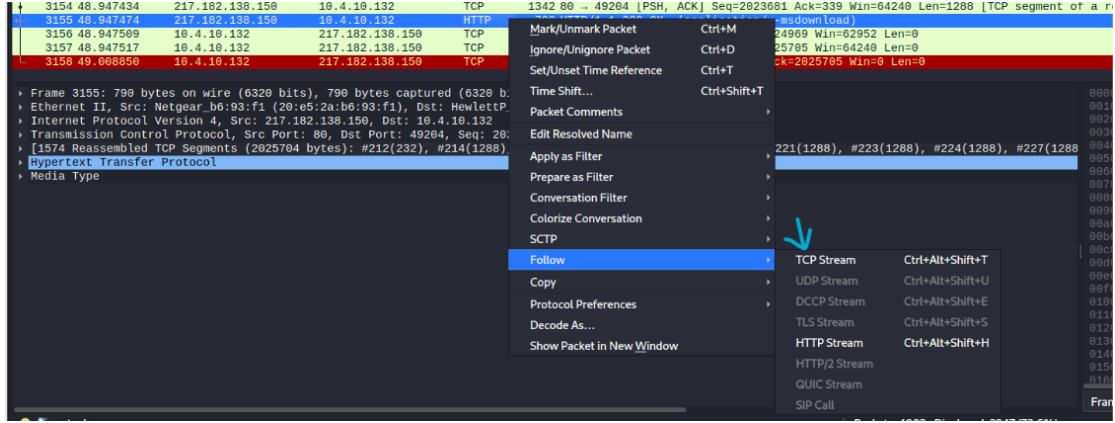
Dosyayı virustotele attığımda çeşitli platformlarda bu kötü amaçlı yazılımın adının ne olarak geçtiğiyle birlikte birçok bilgiye erişebiliyorum.

Malwarebytes

! Spyware.HawkEyeKeyLogger

Örneğin Malwarebytes'e göre Spyware.HawkEyeKeyLogger adında bir zararlı yazılım.

Şimdi bu dosyanın indirildiği paketin TCP akışını aşağıdaki aşamalarla takip edeceğim.



```

HTTP/1.1 200 OK
Last-Modified: Wed, 10 Apr 2019 04:44:31 GMT
Content-Type: application/x-msdownload
Content-Length: 2025472
Accept-Ranges: bytes
Date: Wed, 10 Apr 2019 20:37:54 GMT
Server: LiteSpeed
Connection: Keep-Alive

```

Kötü amaçlı yazılımı barındıran web sunucusunu Server değerinden LiteSpeed yazılımının çalıştırdığını gözlemliyoruz.

Bir saldırganın ağa erişmek için hangi IP adresini hedef aldığını bilmek bu saldırının kapsamını ve etkisini anlamamıza yardımcı olabilir. Bu nedenle kurbanın public IP'sini bulmak için "HTTP 200 OK" paketlerine odaklanıyoruz. Çünkü bu paketler genellikle sunucunun public IP adresine döner.

```

GET / HTTP/1.1
Host: bot.whatismyipaddress.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html
Server:
Date: Wed, 10 Apr 2019 20:48:19 GMT
Connection: close
Content-Length: 14

173.66.146.112

```

Ve HTTP akışını takip ettiğimiz bir HTTP 200 OK paketinde public IP ye döndüğünü görüyor ve public IP bilgisine erişiyoruz.

➔ 173.66.146.112

Çalınan bilgilerin gönderildiği bir e-posta sunucusu olduğunu biliyoruz. Bunun hangi ülkede olduğunu araştırmak için SMTP isteklerini görüntülüyoruz. Çünkü SMTP trafiği e-posta gönderenin ve alanın arasında geçen mesaj alışverişini içerir.

No.	Time	Source	Destination	Protocol	Length	Info
3176	69.160551	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZ
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNAMjM=

Destination kısmının altındaki IP adresi hedef olarak belirlenen sistemdeki E-posta Sunucusunun IP adresidir bulunmaktadır.

IP Adresi yazın: **23.229.162.69**
**IP Sorgula**

**Sorgulanan '23.229.162.69' IP Adresine Ait Bilgiler**

**Ülke :** [United States of America](#)  
Sorgulama yaptığınız ip ülke bilgisi.

**Bölge/Şehir :** [Arizona / Tempe](#)  
Sorgulama yaptığınız ip adresi bölge ve şehir bilgisi.

**IP :** [23.229.162.69](#)  
Sorgulama yaptığınız ip adresi

**HOST :** [69.162.229.23.host.secureserver.net](#)  
IP sorgulama yapılan ip adresinin kayıtlı host adresi

**Ülke Bayrağı :** [United States of America](#)  bölgeye/şehire ait plaka kodu, posta kodu, ülke telefon kodu değişkenlik gösterebileceğinden listelenemedi.

IP adresini sorgulayarak ülkesini öğrendik.

Aynı sorgudaki ilk paketin TCP akışını takip ederek bilgilerin sızdırıldığı e-postayı ve alan adını buldum.

```
MAIL FROM:<sales.del@macwinlogistics.in>
250 OK
RCPT TO:<sales.del@macwinlogistics.in>
250 Accepted
```

- ➔ Sales.del@macwinlogistics.in
- ➔ macwinlogistics.in

```
Wireshark - Follow TCP Stream (tcp.stream eq 16) - stealer.pcap
220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO Beijing-5cd1-PC
250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]
250-SIZE 52428800
250-8BITIME
250-PIPELINING
```

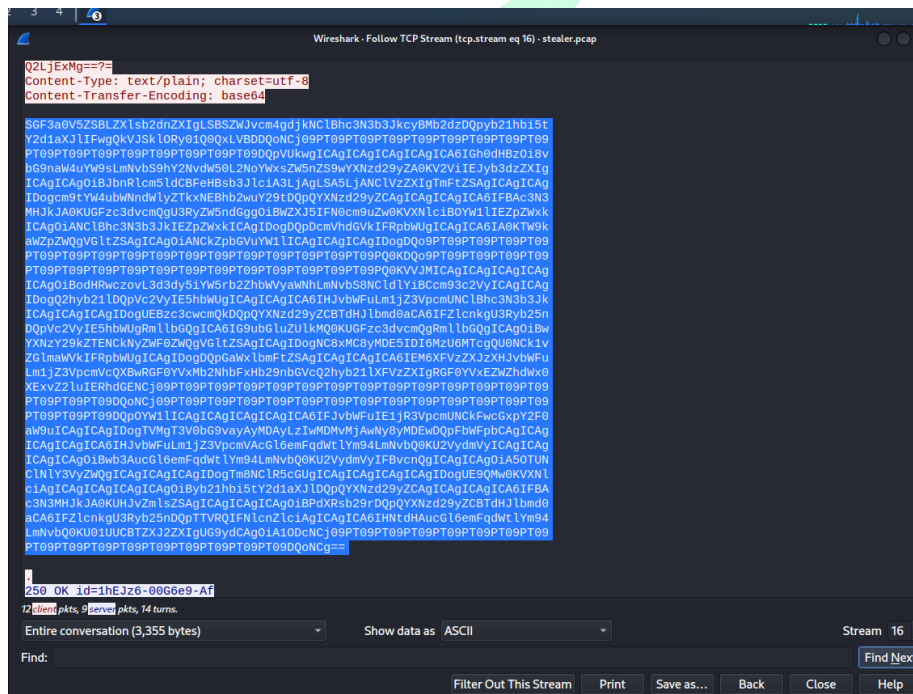
SMTP protokolü trafiğinden bir paketin TCP akışını takip ederek çalınan verilerin gönderildiği e-posta sunucusunu hangi yazılımı çalıştırdığını gözlemledik.

The image shows a Wireshark packet capture of SMTP traffic. The packet list on the left shows a series of SMTP messages. The selected packet (No. 3192) is an SMTP message with the subject 'Pass: U2F5ZKXANJM='.

No.	Time	Source	Destination	Protocol	Length	Info
3176	69.168551	10.4.10.132	23.229.162.69	SMTP	76 C	EHLO Beijing-5cd1-PC
3179	69.223144	10.4.10.132	23.229.162.69	SMTP	107 C	AUTH Login User: c2FsZXMuVGVsQGh1Y3dpbmVxZ2ZldGJcy5pbG==
3182	69.292845	10.4.10.132	23.229.162.69	SMTP	68 C	Pass: U2F5ZKXANJM=
3185	69.362954	10.4.10.132	23.229.162.69	SMTP	96 C	MAIL FROM:<sales.del@macwinlogistics.in>
3188	69.432635	10.4.10.132	23.229.162.69	SMTP	94 C	RCPT TO:<sales.del@macwinlogistics.in>
3191	69.499747	10.4.10.132	23.229.162.69	SMTP	60 C	DATA
3307	673.517002	10.4.10.132	23.229.162.69	SMTP	76 C	EHLO Beijing-5cd1-PC
3310	673.585529	10.4.10.132	23.229.162.69	SMTP	107 C	AUTH Login User: c2FsZXMuVGVsQGh1Y3dpbmVxZ2ZldGJcy5pbG==
3313	673.652869	10.4.10.132	23.229.162.69	SMTP	68 C	Pass: U2F5ZKXANJM=
3316	673.720886	10.4.10.132	23.229.162.69	SMTP	96 C	MAIL FROM:<sales.del@macwinlogistics.in>
3319	673.785075	10.4.10.132	23.229.162.69	SMTP	94 C	RCPT TO:<sales.del@macwinlogistics.in>
3322	673.853337	10.4.10.132	23.229.162.69	SMTP	60 C	DATA
3394	1277.625876	10.4.10.132	23.229.162.69	SMTP	76 C	EHLO Beijing-5cd1-PC

SMTP trafiğine bakarken login ve pass bilgilerini de gözlemleyebiliyoruz. Base64 kullanarak encode edilmiş Pass bilgisini decode ederek Pass değerinin Sales@23 olduğunu bulduk.

TCP akışını takip ederken yine Base64 le encode edilmiş veriler gözlemliyoruz.



Bunları encode ederek Reborn v9 kötü amaçlı yazılım varyantının verileri sızdırmaya yol açtığını gözlemliyoruz.

```

=====
URL           : https://login.aol.com/account/challenge/password
Web Browser   : Internet Explorer 7.0 - 9.0
User Name     : roman.mcguire914@aol.com
Password      : P@ssw0rd$
Password Strength : Very Strong
User Name Field :
Password Field :
Created Time  :
Modified Time :
Filename     :
=====

```

```

=====
URL           : https://www.bankofamerica.com/
Web Browser   : Chrome
User Name     : roman.mcguire
Password      : P@ssw0rd$
Password Strength : Very Strong
User Name Field : onlineId1
Password Field : passcode1
Created Time  : 4/10/2019 2:35:17 AM
Modified Time :
Filename     : C:\Users\roman.mcguire\AppData\
Local\Google\Chrome\User Data\Default>Login Data
=====

```

```

=====
Name          : Roman McGuire
Application   : MS Outlook 2002/2003/2007/2010
Email         : roman.mcguire@pizzajukebox.com
Server        : pop.pizzajukebox.com
Server Port   : 995
Secured       : No
Type          : POP3
User          : roman.mcguire
Password      : P@ssw0rd$
Profile       : Outlook
Password Strength : Very Strong
SMTP Server   : smtp.pizzajukebox.com
SMTP Server Port : 587
=====

```

Bankofamerica erişim kimlik bilgilerini de açığa çıktığını gözlemliyoruz.

No.	Time	Source	Destination	Protocol	Length	Info
3175	2019-04-10 20:38:16.289945	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpln0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15
3176	2019-04-10 20:38:16.296261	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3178	2019-04-10 20:38:16.352374	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpln0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]   SIZE
3179	2019-04-10 20:38:16.352874	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQ61hY3dpbmV2Z2lzdGljcy5pbG==
3181	2019-04-10 20:38:16.422343	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcmQ=
3182	2019-04-10 20:38:16.422575	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNANjM=
3184	2019-04-10 20:38:16.492434	23.229.162.69	10.4.10.132	SMTP	84	S: 235 Authentication succeeded
3185	2019-04-10 20:38:16.492684	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>
3187	2019-04-10 20:38:16.561414	23.229.162.69	10.4.10.132	SMTP	62	S: 250 OK
3188	2019-04-10 20:38:16.561765	10.4.10.132	23.229.162.69	SMTP	94	C: RCPT TO:<sales.del@macwinlogistics.in>
3190	2019-04-10 20:38:16.629231	23.229.162.69	10.4.10.132	SMTP	68	S: 250 Accepted
3191	2019-04-10 20:38:16.629477	10.4.10.132	23.229.162.69	SMTP	60	C: DATA
3193	2019-04-10 20:38:16.691862	23.229.162.69	10.4.10.132	SMTP	118	S: 354 Enter message, ending with "." on a line by itself
3194	2019-04-10 20:38:16.712251	10.4.10.132	23.229.162.69	SMTP	419	C: DATA fragment, 356 bytes
3196	2019-04-10 20:38:16.712359	10.4.10.132	23.229.162.69	SMTP	1076	C: DATA fragment, 1022 bytes
3198	2019-04-10 20:38:16.712458	10.4.10.132	23.229.162.69	SMTP	1078	C: DATA fragment, 1024 bytes
3200	2019-04-10 20:38:16.712516	10.4.10.132	23.229.162.69	SMTP	198	C: DATA fragment, 144 bytes
3202	2019-04-10 20:38:16.712598	10.4.10.132	23.229.162.69	SMTP	56	C: DATA fragment, 2 bytes
3204	2019-04-10 20:38:16.712661	10.4.10.132	23.229.162.69	SMTP/I...	59	from: sales.del@macwinlogistics.in, subject: =?utf-8?B?SGF3a0V5ZS8LZXlsb2dnZXIglS8SZWJvc4g0
3206	2019-04-10 20:38:16.853704	23.229.162.69	10.4.10.132	SMTP	82	S: 250 OK id=1hEJz6-0066e8-Af
3253	2019-04-10 20:39:56.111682	23.229.162.69	10.4.10.132	SMTP	121	S: 421 p3plcpln0413.prod.phx3.secureserver.net lost input connection
3306	2019-04-10 20:48:20.646402	23.229.162.69	10.4.10.132	SMTP	251	S: 220-p3plcpln0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:48:20
3307	2019-04-10 20:48:20.646732	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3309	2019-04-10 20:48:20.715925	23.229.162.69	10.4.10.132	SMTP	261	S: 250-p3plcpln0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]   SIZE
3310	2019-04-10 20:48:20.715259	10.4.10.132	23.229.162.69	SMTP	107	C: AUTH login User: c2FsZXMuZGVsQ61hY3dpbmV2Z2lzdGljcy5pbG==
3312	2019-04-10 20:48:20.782363	23.229.162.69	10.4.10.132	SMTP	72	S: 334 UGFzc3dvcmQ=
3313	2019-04-10 20:48:20.782599	10.4.10.132	23.229.162.69	SMTP	68	C: Pass: U2FsZXNANjM=
3315	2019-04-10 20:48:20.850421	23.229.162.69	10.4.10.132	SMTP	84	S: 235 Authentication succeeded
3316	2019-04-10 20:48:20.850616	10.4.10.132	23.229.162.69	SMTP	96	C: MAIL FROM:<sales.del@macwinlogistics.in>



SMTP trafiğinde Pass bilgilerinin açığa çıktığı 2 paket görebiliyoruz tarih ve saat bilgilerinden yola çıkarak toplanan verilerin 10 dakikada bir sızdırıldığını da gözlemliyoruz.

## Olay Zaman Çizelgesi (Timeline of Events)

**Apr 10, 2019 16:38:16.289945000 EDT:**

Saldırgan içinde kötü amaçlı tkraw\_Protected99.exe dosyası olan e-postayı muhasebeciye gönderir.

**Apr 10, 2019 16:38:16.290281000 EDT:**

Muhasebeci bu e-postayı açar ve tkraw\_Protected99.exe dosyasını indirir.

Dosya kurbanın bilgisayarında çalıştırdığı Windows NT 6.1 yazılımında çalıştırılıyor.

**Apr 10, 2019 16:38:16.422343000 EDT:**

Tkraw\_Protected99.exe dosyası çalışmaya başladıktan sonra saldırı kontrolü sağlar.

Kurbanın bilgisayarında veri sızıntısı başlar ve sızdırılan bu veriler Exim 4.91 yazılımını kullanan e-posta sunucusuna gönderilir.

**Apr 10, 2019 16:48:20.782599000 EDT:**

Her 10 dakikada bir veri sızıntısı gerçekleşmeye başladı.

## Sonuçlar(Conclusions)

Analizlerime göre ulaştığım güvenlik açıklarını listeliyorum.

Personel arasında siber saldırılar konusunda farkındalık eksikliği.

Sistemde e-postalar için zayıf güvenlik.

Kurbanın bilgisayarında kullanılan yazılımın zararlı dosyayı tespit etmemesi.

Veri sızıntısının her 10 dakikada bir gerçekleştiğini gözlemlediğimizde 1 saat sonra tespit edilmiş olması, şirketin olayı erken tespit edemediğini göstermektedir.

Erken tespit eksikliğine ek olarak, olaya müdahale eksikliği de söz konusudur.

Virustotal'da yapılan bir inceleme, bu kötü amaçlı yazılımın güncel yazılımlar tarafından kolayca tespit edilebildiğini gösteriyor. Bu kötü amaçlı yazılımın şirketin sisteminde çalışıyor olması, sistemin güncel olmayan bir yazılım kullandığının göstergesidir.

Zararın tespiti konusunda aşağıda belirttiğim tablodaki veriler sızdırılmış olup itibar ve finansal kayıp riski taşımaktadır.

```

=====
URL                : https://login.aol.com/account/challenge/password
Web Browser       : Internet Explorer 7.0 - 9.0
User Name         : roman.mcguire914@aol.com
Password          : P@ssw0rd$
Password Strength : Very Strong
User Name Field   :
Password Field    :
Created Time      :
Modified Time     :
Filename          :
=====

```

```

=====
URL                : https://www.bankofamerica.com/
Web Browser       : Chrome
User Name         : roman.mcguire
Password          : P@ssw0rd$
Password Strength : Very Strong
User Name Field   : onlineId1
Password Field    : passcode1
Created Time      : 4/10/2019 2:35:17 AM
Modified Time     :
Filename          : C:\Users\roman.mcguire\AppData\
Local\Google\Chrome\User Data\Default>Login Data
=====

```

```

=====
Name              : Roman McGuire
Application       : MS Outlook 2002/2003/2007/2010
Email             : roman.mcguire@pizzajukebox.com
Server            : pop.pizzajukebox.com
Server Port       : 995
Secured           : No
Type              : POP3
User              : roman.mcguire
Password          : P@ssw0rd$
Profile           : Outlook
Password Strength : Very Strong
SMTP Server       : smtp.pizzajukebox.com
SMTP Server Port  : 587
=====

```

Olası bir saldırının tekrar yaşanmaması için lütfen aşağıdaki adımları takip ediniz. Siber saldırılar konusunda bilinçsiz olan kullanıcılar bu konuda bilinçlendirilmeli ve eğitilmelidir.

Kullanıcılarınızın şifrelerini düzenli olarak değiştirmelerini sağlayan bir politika izleyin.

Şifreler dışında iki faktörlü kimlik doğrulama gibi farklı kimlik doğrulama gereksinimleri sunun.

Kötü niyetli e-postaları filtrelemek için güvenlik önlemlerini artırın.

Sistem üzerinde kullanılan tüm yazılımları güncel tutun.

Ağ üzerindeki sistemleri herhangi bir veri sızıntısı riskine karşı sürekli olarak izleyin ve bir saldırı durumunda erken tepki verin.

Verileri řifreli tutarsanız, alınsa bile kullanılamaz. Bu nedenle verileri řifreli tutun. İ ve dıř ağı birbirinden ayırın ve bu iki ağı arasındaki iletişimi mümkün olduėunca sınırlı tutun.

