HAWKEYE

CYBERDEFENDER

HTTPS://CYBERDEFENDERS.ORG/BLUETEAM-CTF-CHALLENGES/91#NAV-QUESTİONS

Sudenur MURATOĞULLARI

İçindekiler

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.

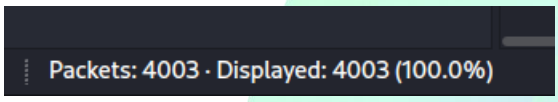
Kuruluş özel adresleme ve /24 ağ maskesi ile çalışmaktadır.

Metodoloji(Methodology)

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

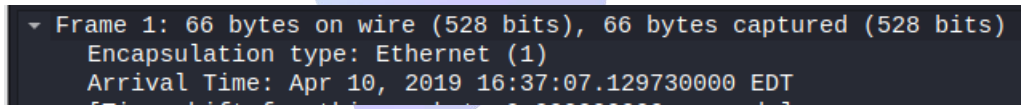
Bulgular ve Analiz (Findings and Analysis)

Yakalamada 4003 paket var.

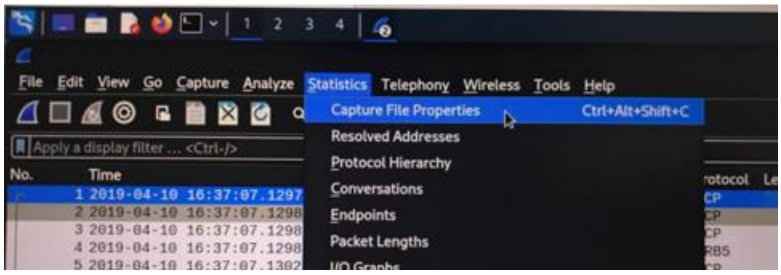


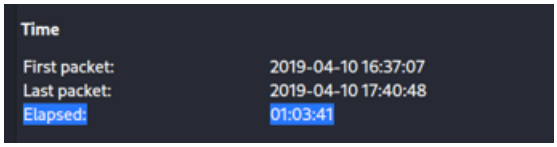
İlk paketin tarih ve saat bilgileri ekte EDT formatında gözükmektedir. Koordineli Evrensel Saat(UTC) formatında bu tarih bilgisini düzenlememiz gerekmekte.

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

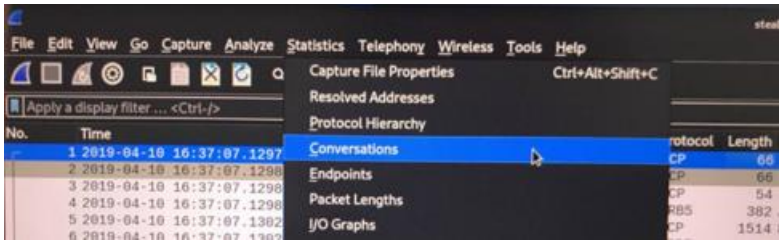


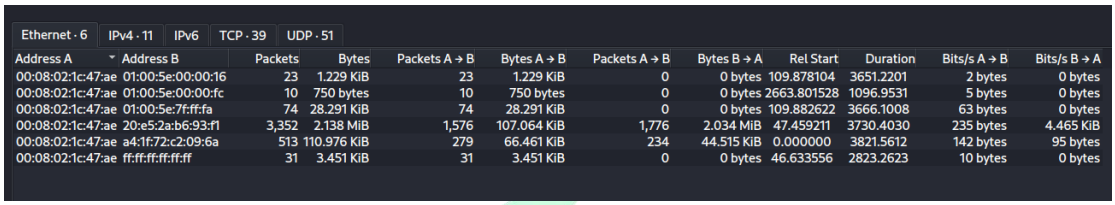
Kaydedilen ağ trafiği paketlerinin yakalandığı süreye ulaşmamız gerekiyor. Statistics bölümünden yakalama dosyası özelliklerini inceleyerek elapsed bilgisine ulaşabiliriz.





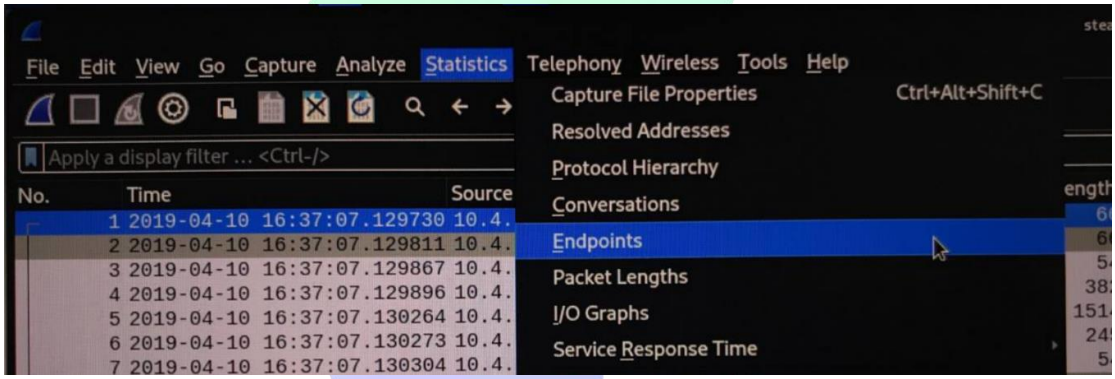
Aktif bilgisayarı bulmak için conversations (konuşmalar kısmında inceleme yapabiliriz.)

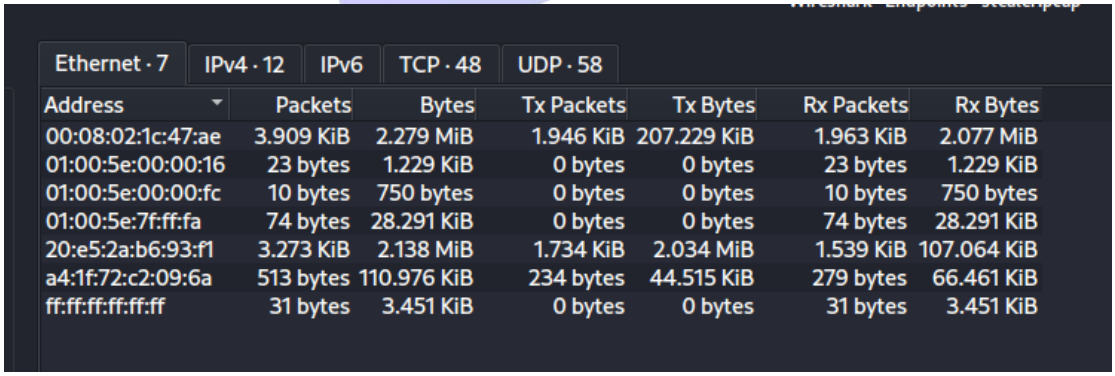




Konuşmaları incelediğimizde en aktif cihazın 00:08:02:1c:47:ae mac adresine sahip cihaz olduğunu görüyoruz.

Bir başka yöntem de Endpoints kısmını incelemek.



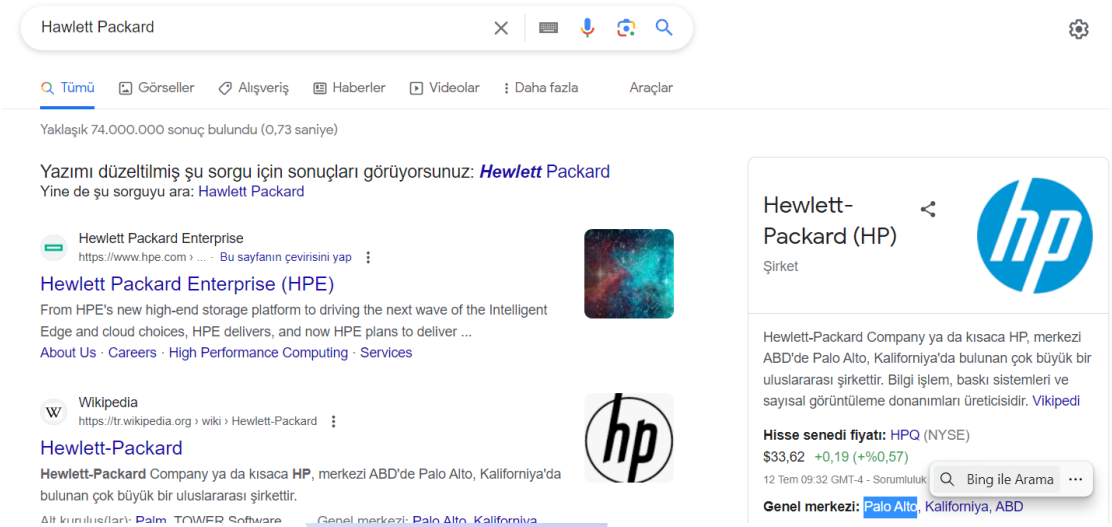


Endpoints kısmını incelediğimizde mac adreslerinin en aktiften başlayarak sıralandığını görüyoruz. Bu incelememiz sonucunda da yine en aktif mac adresinin 00:08:02:1c:47:ae olduğu sonucuna ulaştık.

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

Hawlett Packard bilgisini edindik.

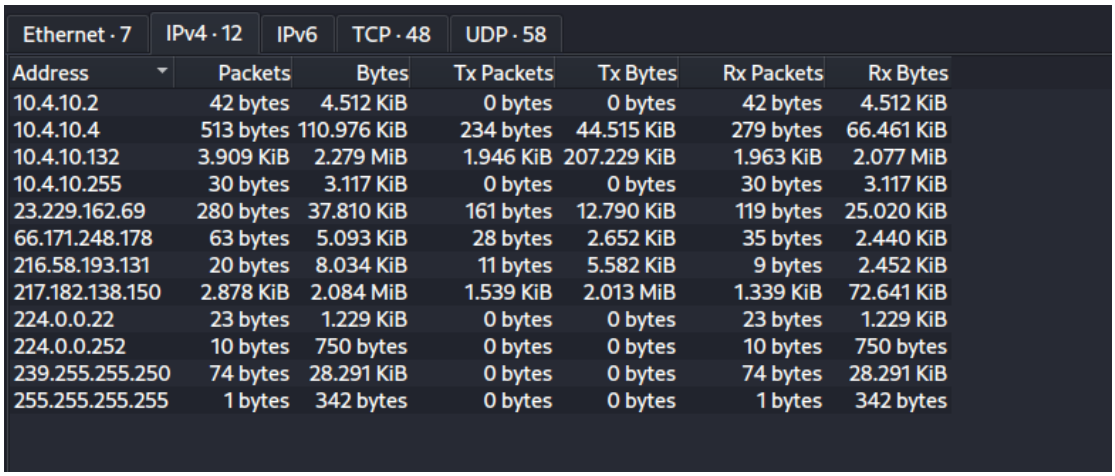
Bu bilgiyi kullanarak da NIC üreticisinin merkezinin bulunduğu şehri bulabiliriz.



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.

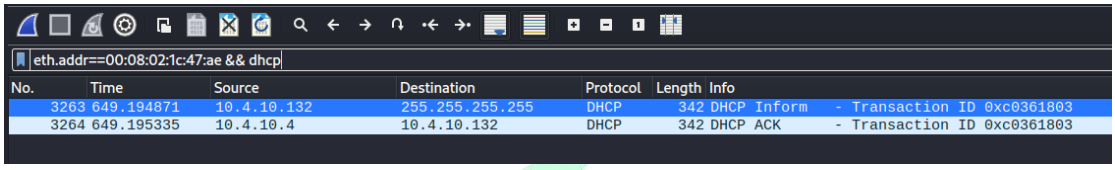


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.4.10.2	42 bytes	4.512 KiB	0 bytes	0 bytes	42 bytes	4.512 KiB
10.4.10.4	513 bytes	110.976 KiB	234 bytes	44.515 KiB	279 bytes	66.461 KiB
10.4.10.132	3.909 KiB	2.279 MiB	1.946 KiB	207.229 KiB	1.963 KiB	2.077 MiB
10.4.10.255	30 bytes	3.117 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

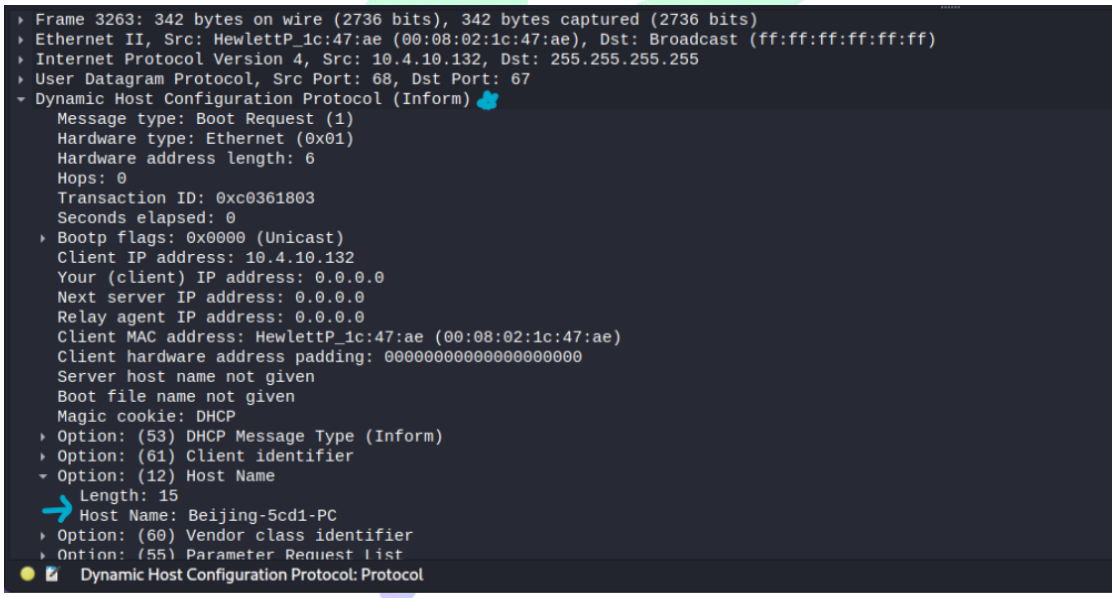
İlk 4 IP adresi elimizdeki bilgiyle fakat 10.4.10.255 IP adresi kuruluştaki bir cihaza ait olamaz çünkü bir broadcast IP adresidir.(10.4.10.0/24 alt ağındaki tüm cihazlara yayın yapmak için kullanılır.) Bu durumda 3 bilgisayar yakalama işlemine dahil olmuş sonucuna vardık.

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.



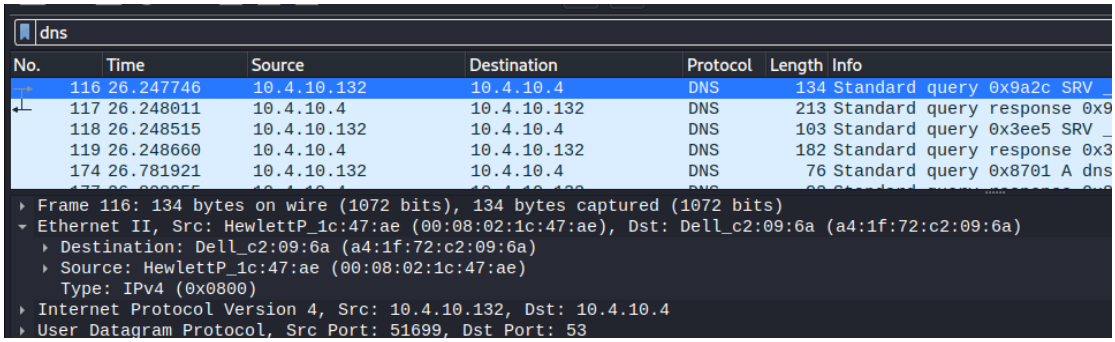
Broadcast IP adresinin bulunduğu pakette DHCP bölümünden Host Bilgilerini görebilmekteyiz. Host Name: BEIJING-5CD1-PC



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

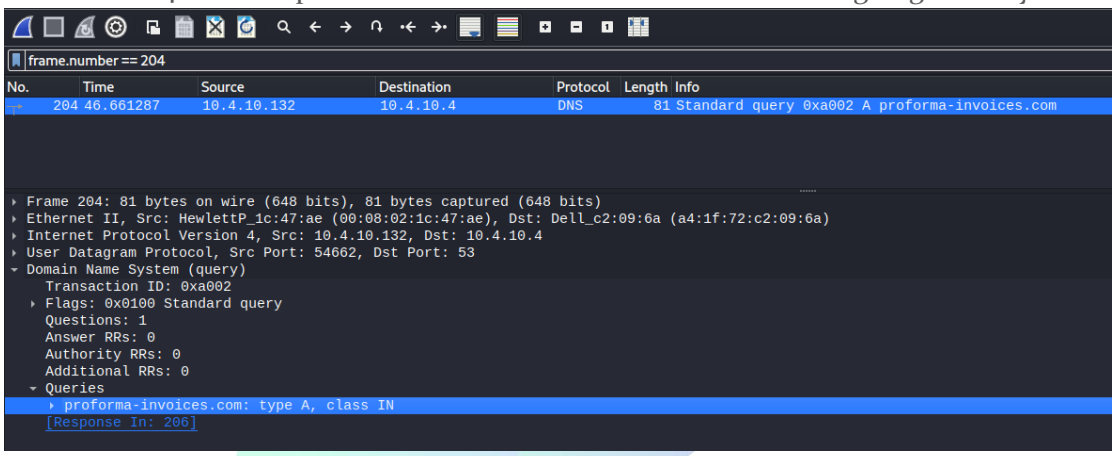
Saldırı tespiti ve soruşturmasında ve IP adresi ilişkilendirmesi gibi konularda fayda sağlayabileceğinden DNS sunucusunun IP adresini bulmamız gerekmekte.

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

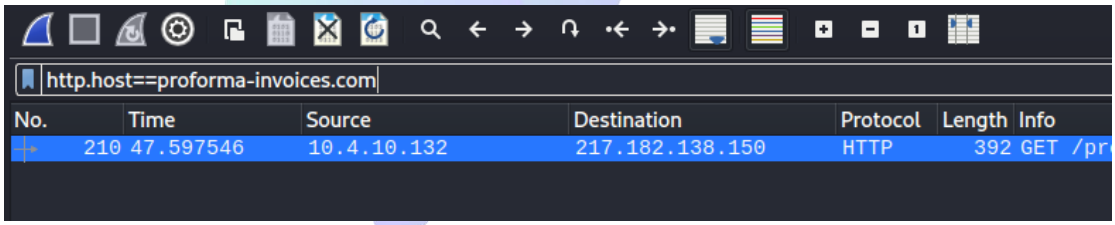


Ethernet II kısmında Source bölümü kurbanın Destination bölümü ise DNS sunucusunun MAC adresidir.

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



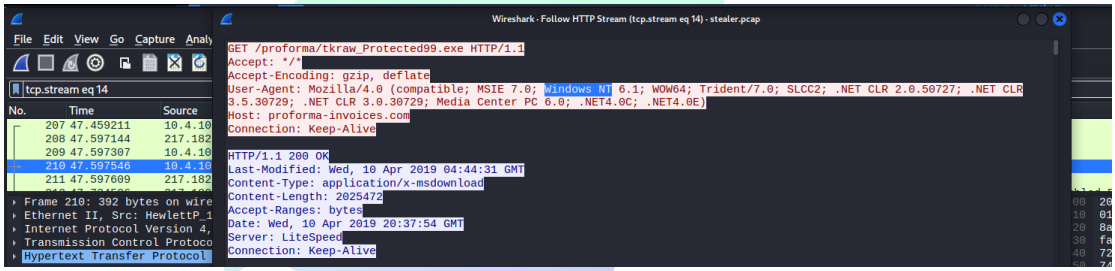
Bu domainin IP adresini bulmak için aşağıdaki sorguyla devam ediyorum.



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

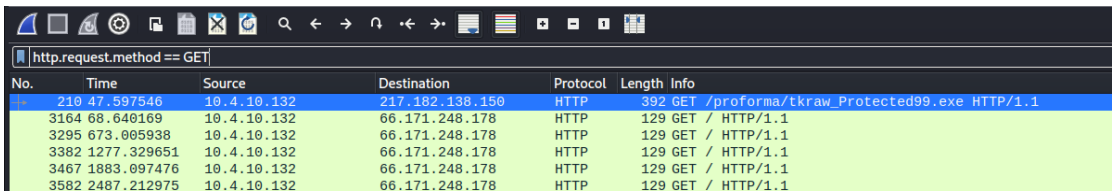
Basit bir sorgulama işlemiyle bu IP adresinin ait olduğu ülkeyi ve daha fazla bilgisine ulaşabiliyoruz.

Kurban bilgisayarının işletim sistemine bakacağız.

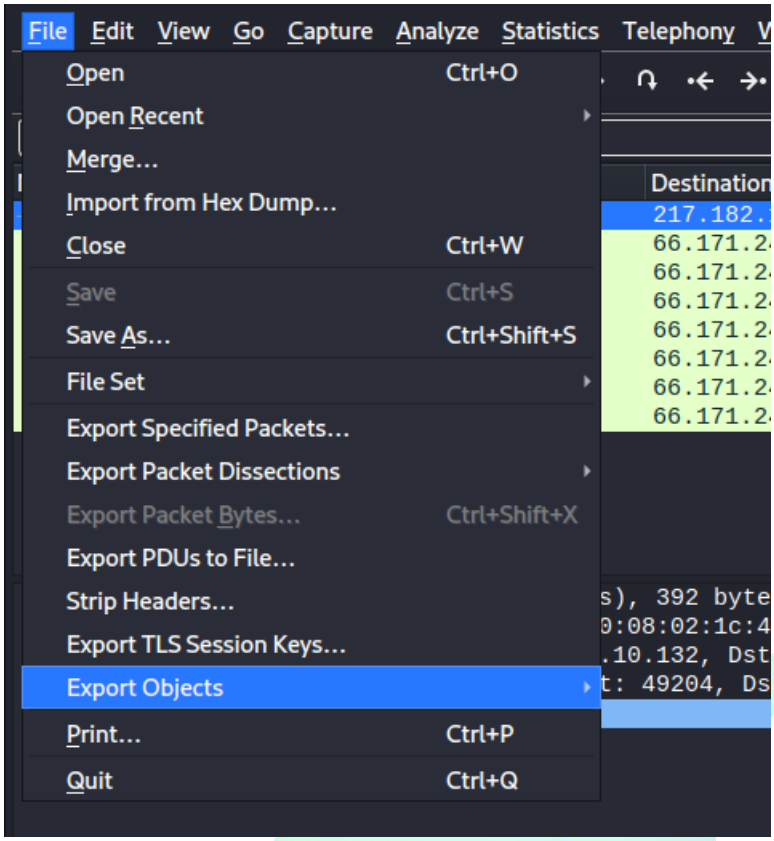


Kurbanın proforma-invoices.com domainine yaptığı isteğe ait olan paketin HTTP akışını takip ederek isteği atan bilgisayara ait işletim sistemi bilgisine erişiyoruz. Windows NT 6.1

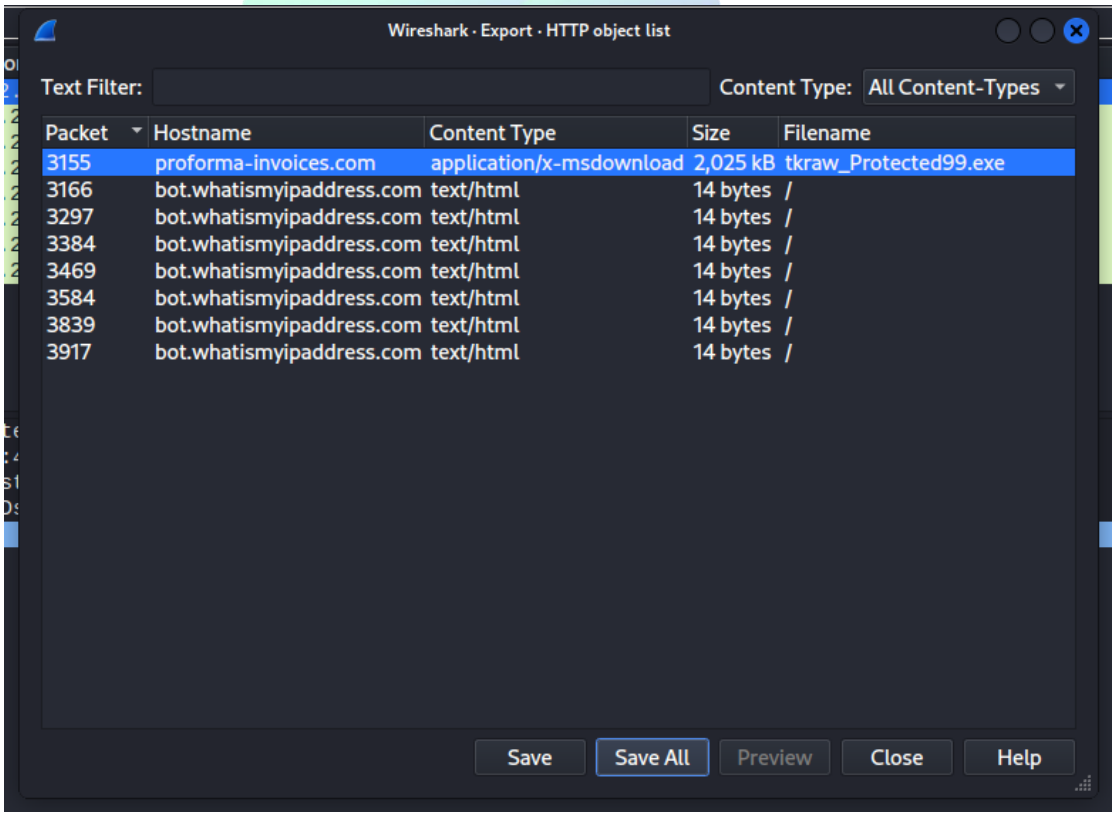
İnternet faaliyetlerinin anlaşılması açısında HTTP GET isteklerini incelerken zararlı IP adresinden indirilen kötü amaçlı yazılımın tkraw_Protected99.exe olduğunu bulduk. Dosya alan tek paket bu olduğundan başka bir dosya olmadığını da gözlemliyoruz.



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

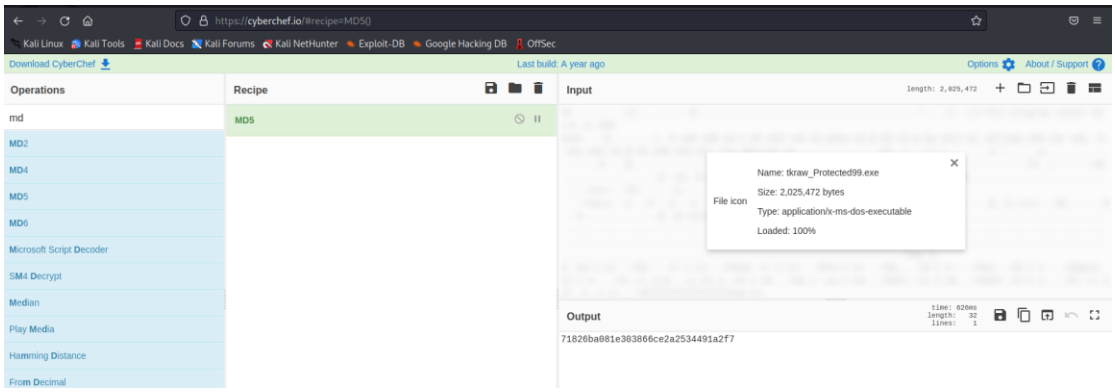


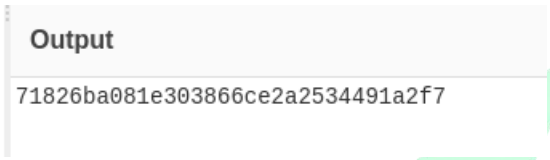
Bu alanda HTTP seçeneğini seçerek devam ediyorum.



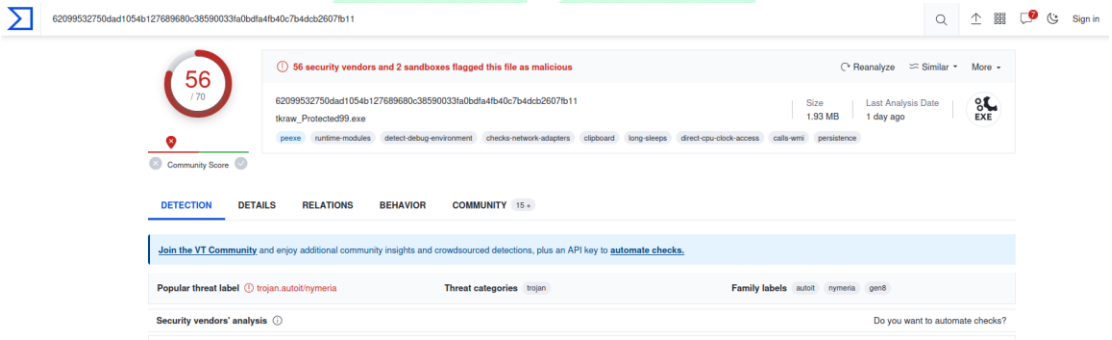
3155 'i seçerek kaydediyorum.

Dosyayı CyberChef'e attığımızda MD5 karmasını görmekteyiz.

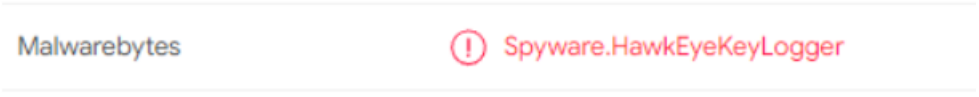




➔ 71826ba081e303866ce2a2534491a2f7

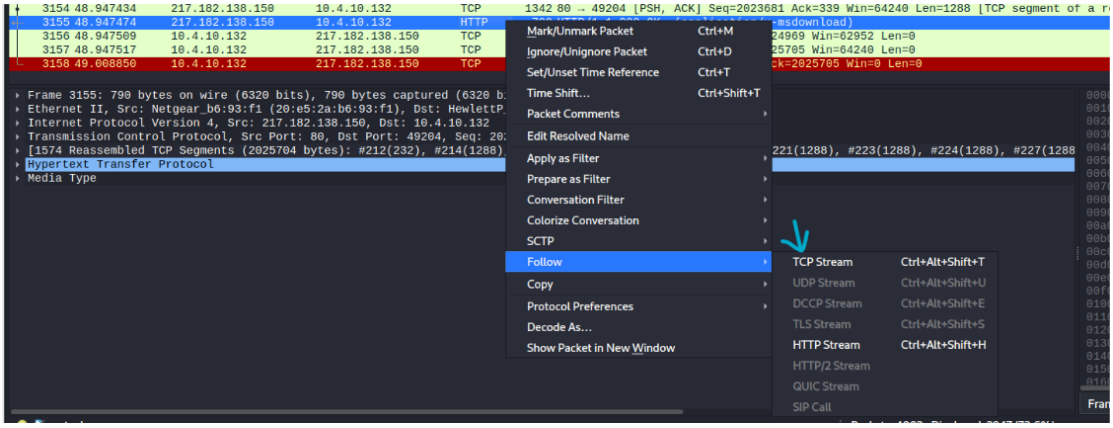


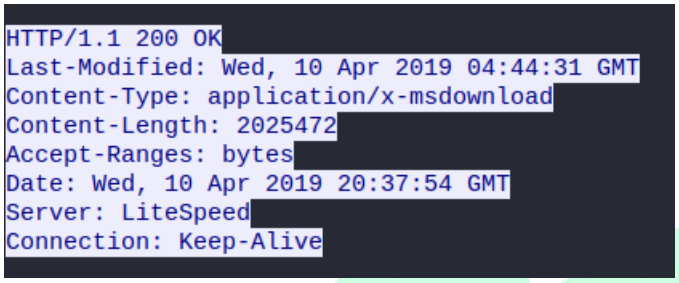
Dosyayı virustotele attığımda çeşitli platformlarda bu kötü amaçlı yazılımın adının ne olarak geçtiğiyle birlikte birçok bilgiye erişebiliyorum.



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

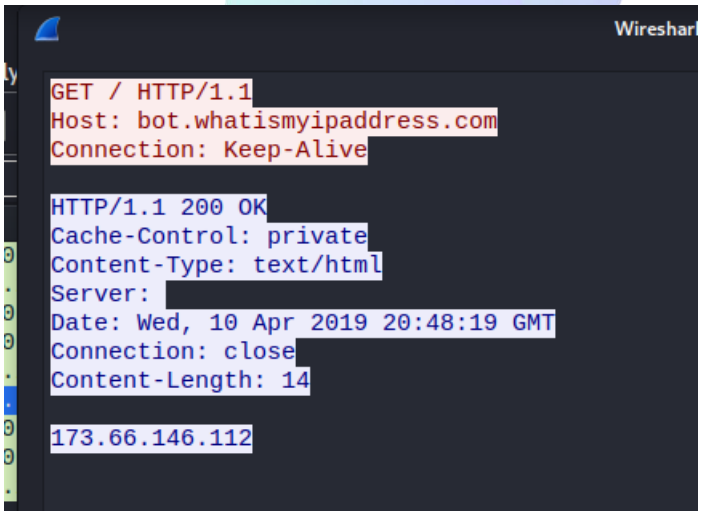
Şimdi bu dosyanın indirildiği paketin TCP akışını aşağıdaki aşamalarla takip edeceğim.





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

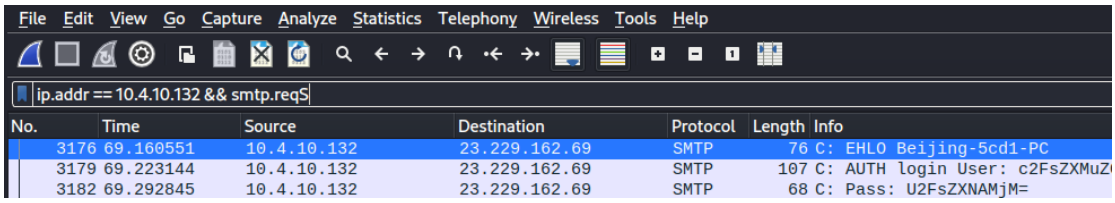
Bir saldırganın ağa erişmek için hangi IP adresini hedef aldığını bilmek bu saldırının kapsamını ve etkisini anlamamıza yardımcı olabilir. Bu nedenle kurbanın public IP'sini bulmak için "HTTP 200 OK" paketlerine odaklanıyoruz. Çünkü bu paketler genellikle sunucunun public IP adresine döner.



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

➔ 173.66.146.112

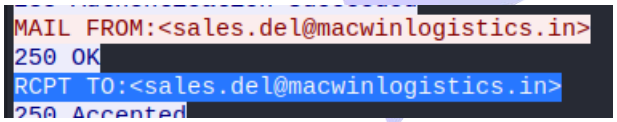
Çalınan bilgilerin gönderildiği bir e-posta sunucusu olduğunu biliyoruz. Bunun hangi ülkede olduğunu araştırmak için SMTP isteklerini görüntülüyoruz. Çünkü SMTP trafiği e-posta gönderenin ve alanın arasında geçen mesaj alışverişini içerir.



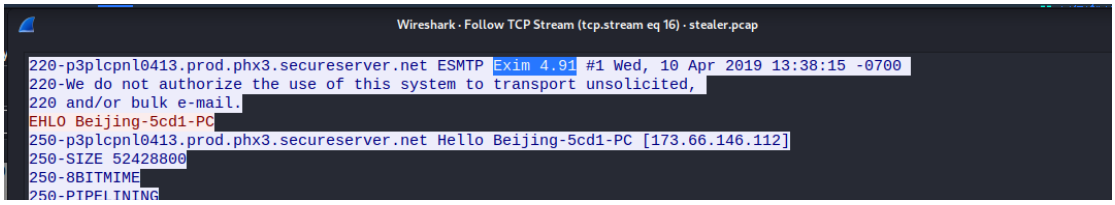
Destination kısmının altındaki IP adresi hedef olarak belirlenen sistemdeki E-posta Sunucusunun IP adresidir bulunmaktadır.

IP adresini sorgulayarak ülkesini öğrendik.

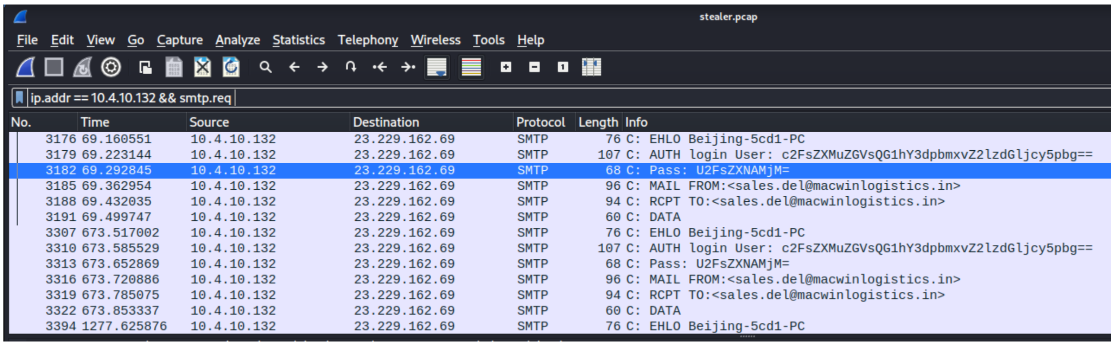
Aynı sorgudaki ilk paketin TCP akışını takip ederek bilgilerin sızdırıldığı e-postayı ve alan adını buldum.



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

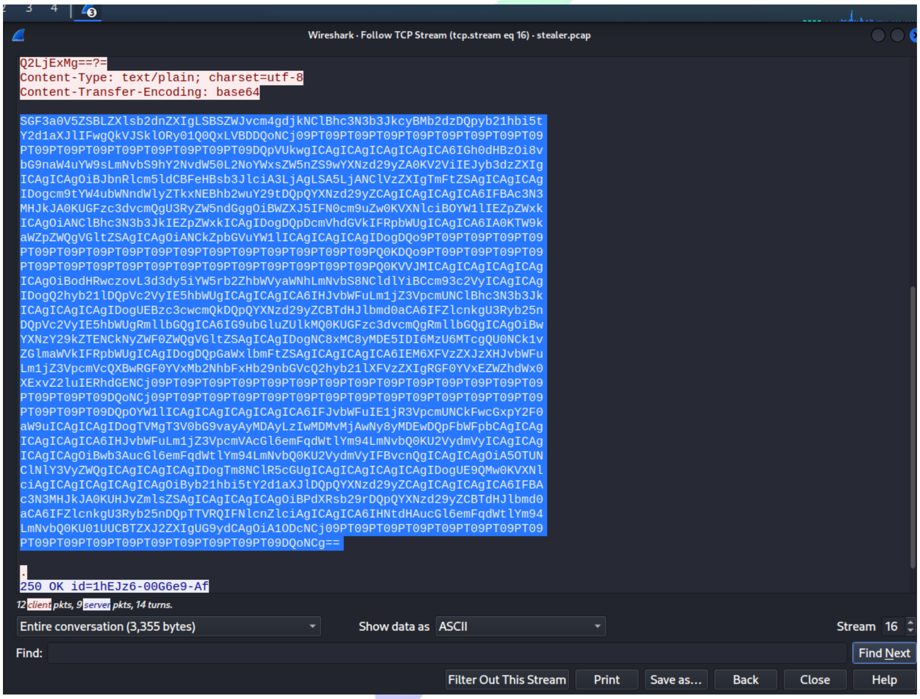


SMTP protokolü trafiğinden bir paketin TCP akışını takip ederek çalınan verilerin gönderildiği e-posta sunucusunu hangi yazılımı çalıştırdığını gözlemledik.



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.



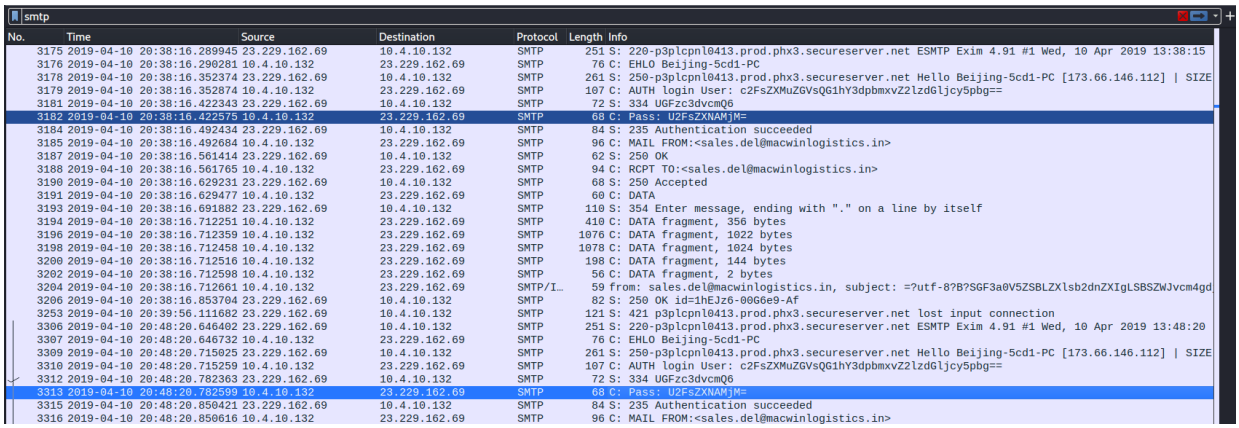
Bunları encode ederek Reborn v9 kötü amaçlı yazılım varyantının verileri sızdırmaya yol açtığını gözlemliyoruz.

```
================================================
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.



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 saldırgan 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 şifreli tutarsanız, çalınsa bile kullanılamaz. Bu nedenle verileri şifreli tutun. İç ve dış ağı birbirinden ayırın ve bu iki ağ arasındaki iletişimi mümkün olduğunca sınırlı tutun.