HawkEye blue team ctf

DİGİTAL FORENSİCS

DUYGU KAÇAR

İçindekiler

Giriş

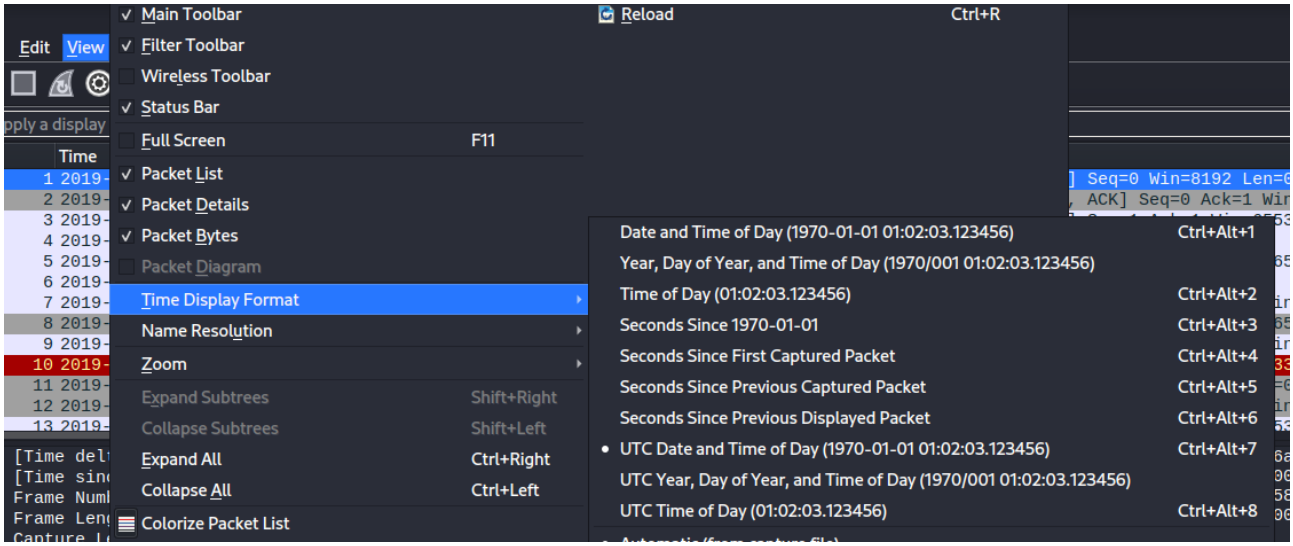
Kuruluşunuzdaki bir muhasebeciye, indirme bağlantısı olan bir faturayla ilgili bir e-posta geldi. E-postayı açtıktan kısa bir süre sonra şüpheli ağ trafiği gözlendi. Bunu da SOC analistlerine gönderdi.

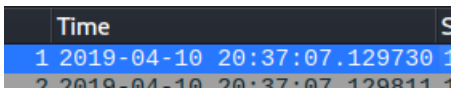
Metodoloji

Bu analizi yaparken wireshark kullanıldı. Virüs total, ip2location gibi benzeri internet toolları kullanıldı.

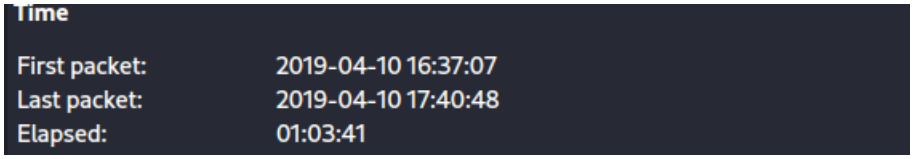
Bulgular ve Analizler

İlk paketin kaçta yakalandığını görmek istiyoruz fakat zaman kısmında UDT cinsinden yazılmış bunu UTC cinsine çevirdiğimizde ilk paketin 2019-4-10 da 20.37 de atıldığını tespite ettik. Tam 4003 tane paket yakalandığını tespit ettik.

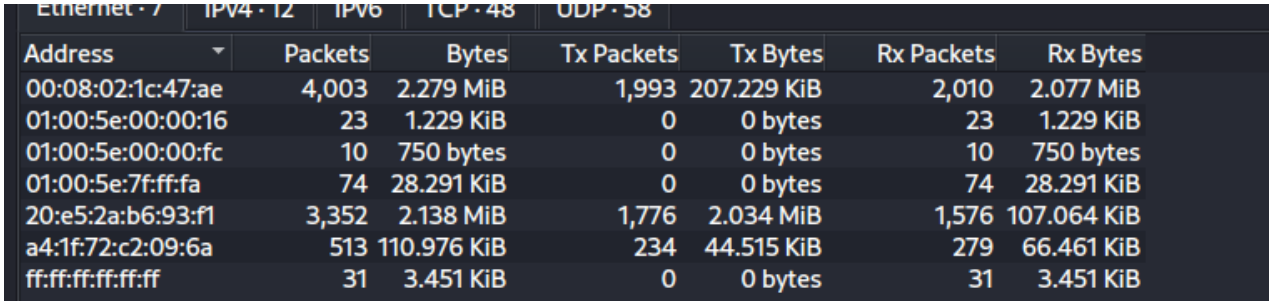




Yakalama süresini statics>capture file properites dosyasından tespit ettik.



Bağlantı düzeyindeki en etkin bilgisayarın "Static>endpoints" kısmından mac adresini(00:08:02:1c:47:ae) ve ıp adresini(10.4.10.132) tespit ettik.

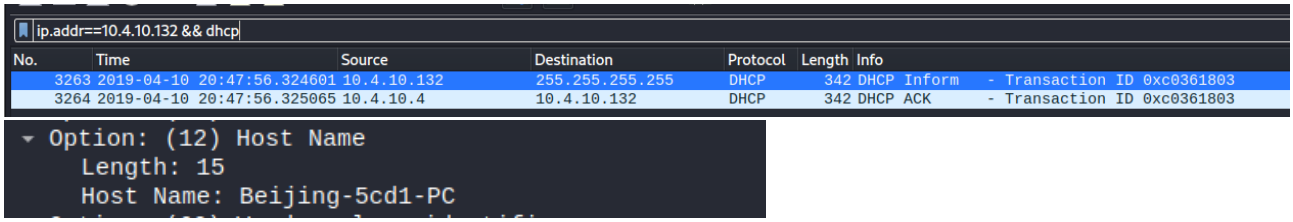


Ethernet · 7 | IPv4 · 12 | IPv6 | TCP · 48 | UDP · 58

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:08:02:1c:47:ae	4,003	2.279 MiB	1,993	207.229 KiB	2,010	2.077 MiB
01:00:5e:00:00:16	23	1.229 KiB	0	0 bytes	23	1.229 KiB
01:00:5e:00:00:fc	10	750 bytes	0	0 bytes	10	750 bytes
01:00:5e:7f:ff:fa	74	28.291 KiB	0	0 bytes	74	28.291 KiB
20:e5:2a:b6:93:f1	3,352	2.138 MiB	1,776	2.034 MiB	1,576	107.064 KiB
a4:1f:72:c2:09:6a	513	110.976 KiB	234	44.515 KiB	279	66.461 KiB
ff:ff:ff:ff:ff:ff	31	3.451 KiB	0	0 bytes	31	3.451 KiB

Aynı yerden 3 tane private ıp adres olduğunu bulduk.

Bu etkin bilgisayarın adını iste wireshark'ta ıp adresiyle beraber DHCP protokolünü araştırdığımızda "Beijing-5cd1-PC" olduğunu tespit ettik.



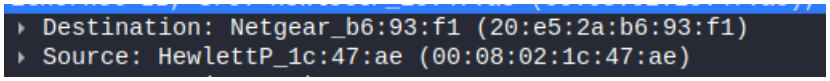
ip.addr==10.4.10.132 && dhcp

No.	Time	Source	Destination	Protocol	Length	Info
3263	2019-04-10 20:47:56.324601	10.4.10.132	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xc0361803
3264	2019-04-10 20:47:56.325065	10.4.10.4	10.4.10.132	DHCP	342	DHCP ACK - Transaction ID 0xc0361803

```
▾ Option: (12) Host Name
    Length: 15
    Host Name: Beijing-5cd1-PC
```

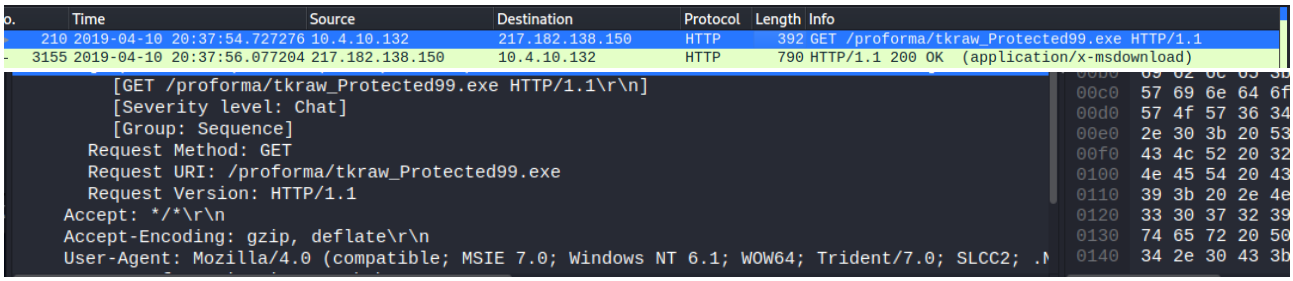
http isteklerine baktığımızda kaynak ve hedefin mac adreslerini tespit ettik.

Source: 00:08:02:1c:47:ae
Destination : 20:e5:2a:1c:47:ae



```
▸ Destination: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
▸ Source: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
```

ve yüklenen zararlı yazılımın adının tkraw_Protected99.exe olduğunu, muhasebecimizin windows işletim sistemli bilgisayarına atıldığını tespit ettik.

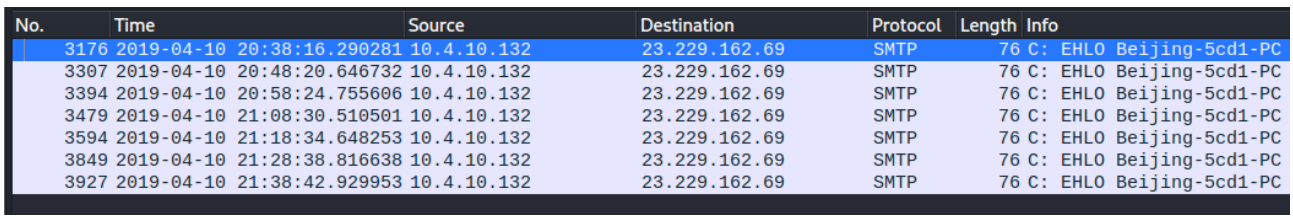


o.	Time	Source	Destination	Protocol	Length	Info
210	2019-04-10 20:37:54.727276	10.4.10.132	217.182.138.150	HTTP	392	GET /proforma/tkraw_Protected99.exe HTTP/1.1
3155	2019-04-10 20:37:56.077204	217.182.138.150	10.4.10.132	HTTP	790	HTTP/1.1 200 OK (application/x-msdownload)

```
        [GET /proforma/tkraw_Protected99.exe HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /proforma/tkraw_Protected99.exe
      Request Version: HTTP/1.1
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .N
```

```
00c0  57 69 6e 64 6f
00d0  57 4f 57 36 34
00e0  2e 30 3b 20 53
00f0  43 4c 52 20 32
0100  4e 45 54 20 43
0110  39 3b 20 2e 4e
0120  33 30 37 32 39
0130  74 65 72 20 50
0140  34 2e 30 43 3b
```

daha sonra smtp isteklerine analiz ettiğimizde EHLO mesajını filtreleyerek smtp oturumunun hangi zamanlarda başladığına baktığımızda 10 dakikada bir başladığını tespit ettik. Yani verilerin 10 dakikada bir sızdırıldığını anladık.



No.	Time	Source	Destination	Protocol	Length	Info
3176	2019-04-10 20:38:16.290281	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3307	2019-04-10 20:48:20.646732	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3394	2019-04-10 20:58:24.755606	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3479	2019-04-10 21:08:30.510501	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3594	2019-04-10 21:18:34.648253	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3849	2019-04-10 21:28:38.816638	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC
3927	2019-04-10 21:38:42.929953	10.4.10.132	23.229.162.69	SMTP	76	C: EHLO Beijing-5cd1-PC

Browser üzerinden kısa bir araştıma ile mac adresinden NIC üreticisini Hewlett Packard olduğunu tespit ettik.

Browser üzerinden NIC üreticisinin merkezinin Palo Alto,Kaliforniya,ABD olduğunu tespit ettik.

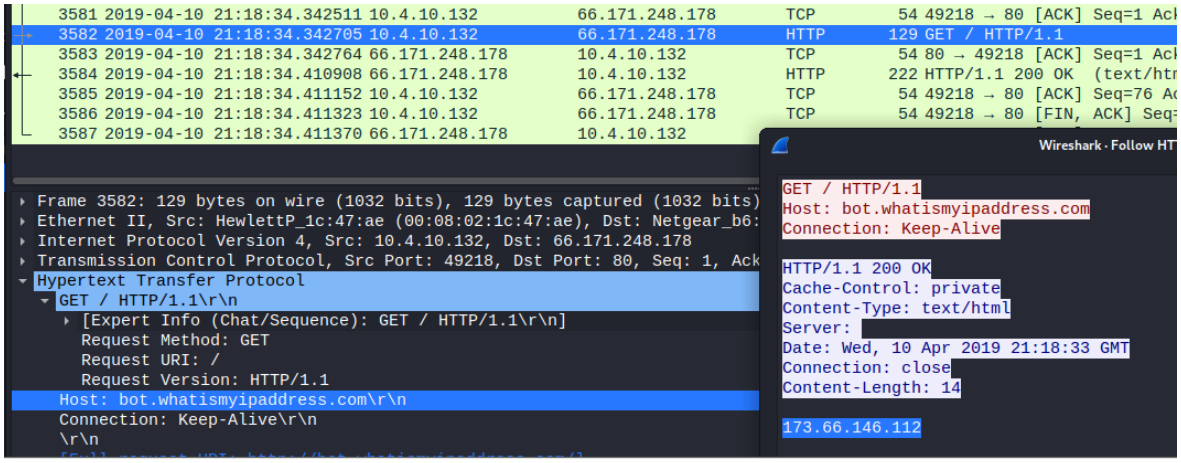
Dns sunucusunu ve respone(istek) yapılan sunucu bilgisini öğrenebiliriz

	Time	Source	Destination	Protocol	Length	Info
116	2019-04-10 20:37:33.377476	10.4.10.132	10.4.10.4	DNS	134	Standard query 0x9a2c SRV _ldap._tcp.Defau
117	2019-04-10 20:37:33.377741	10.4.10.4	10.4.10.132	DNS	213	Standard query response 0x9a2c No such nam
118	2019-04-10 20:37:33.378245	10.4.10.132	10.4.10.4	DNS	103	Standard query 0x3ee5 SRV _ldap._tcp.Pizza
119	2019-04-10 20:37:33.378390	10.4.10.4	10.4.10.132	DNS	182	Standard query response 0x3ee5 No such nam

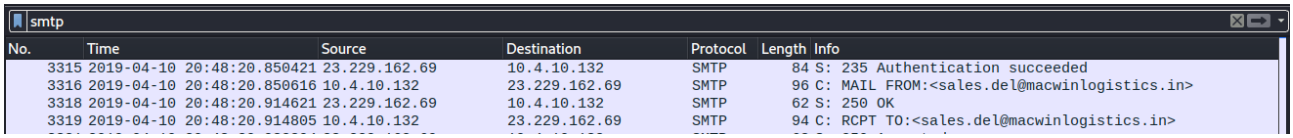
Gördüğümüz üzere query response (sorgu yanıtı) hep 10.4.10.4 ip adresine sahip kaynaktan gelmiş.

Md5 karmasını araştırdığımda anyrun sitesinde bulduk.

GET paketlerinden ziyade bizim için "HTTP 200 OK" paketlerine bakmak daha sağlıklı oldu. Çünkü dönen OK mesajları public IP ye dönecektir. Bu bilgiden yola çıkarak "Follow->TCP Stream" ile hareket ettiğimizde paket içeriğinde Public IP bilgisine ulaşmış olduk.



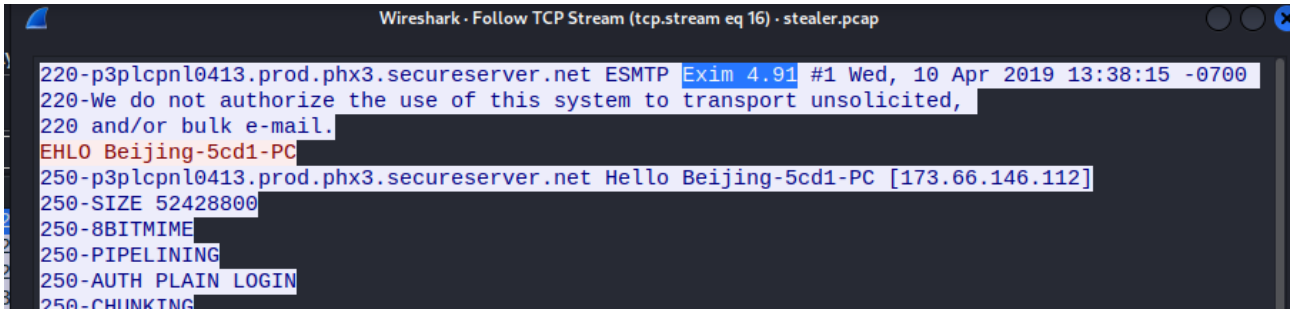
Çalınan verilerin hangi kaynağa gönderileceğine smtp isteklerini inceleyerek bakıyoruz.



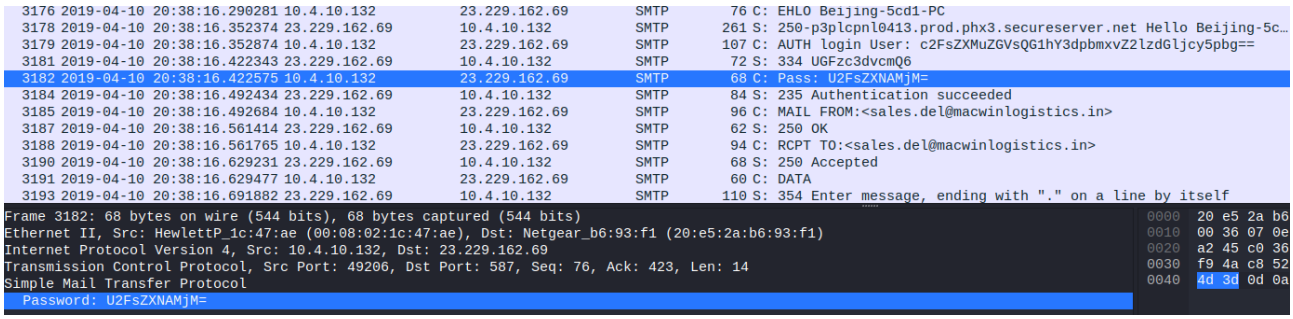
Çalınan bilgiler Sales.del@macwinlogistics.in e posta adresine gönderildi.

Bu gönderilen ıp adresi araştırdığımızda göndeliği e posta sunucusunun United States olduğunu tespit ettik.

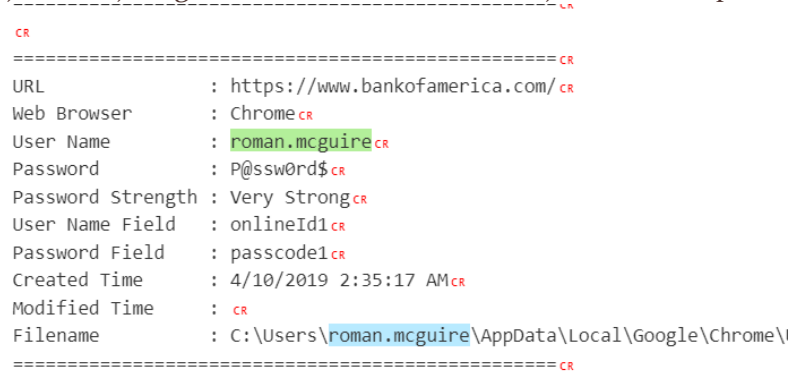
Çalınan verilerin gönderildiği e-posta sunucusunu Exim 4.91 yazılımının çalıştırdığını tespit ettik.



Gönderilen emailin şifresi SMTP isteklerini incelediğimizde base 64 ile şifrelendiğini gördük . bunu çözdüğümüzde şifrenin Sales@23 olduğunu tespit ettik.



Aslında bu soruda bize verileri çalan aracın versiyonunu sormaktadır. Bir önceki soruda password bilgisinin bulunduğu paketi incelediğimizde ve biraz aşağıya doğru kaydırdığımızda anlamsız, sanki base64 ile şifrelenmiş uzun bir veri bloğu dikkatimizi çekmektedir. Bu veri bloğunu farklı bir text dosyasına kaydedip online bir base64decoder'e yüklediğimde çıkan çıktıyı inceledik. decoder ile şifresini çödüğümüzde kullanıcının adı ve şifresni de tespit ettik.



Olayların Zaman Çizelgesi

- Apr 10, 2019 16:38:16.289945000 EDT
  Muhasebeciye içinde kötü amaçlı tkraw_Protected99.exe dosyası olan e-postayı gönderir.
- Apr 10, 2019 16:38:16.290281000 EDT
  Muhasebeci gelen e-postayı açar ve kötü amaçlı keyloger bilgisayarına indirir.
- Apr 10, 2019 16:38:16.422343000 EDT
  Dosya çalışmaya başladıktan sonra kurbanın bilgisayarında veri sızıntısı başlar. Exim 4.91 yazılımını kullanan US 'deki e-posta sunucusuna gönderilir.
- Apr 10, 2019 16:38:16.290281000 EDT
  Mail sunucusu da "Sales.del@macwinlogistics.in" adresine 10 dakikada bir veri sızdırmaya başlıyor.

Sonuç

Yapılan analizler sonucunda muhasebeciye gönderilen indirme bağlantılı e-mailin şüpeli olduğu doğrulandı. Muhasebecinin ihmali sebebi ile inen bu keyloger çalıştırıldığı süre zarfında 10 dakikada bir saldırgana bilgilerini sızdırdığı tespit edildi. Ağ trafiğinin analizi ile Saldırgan hakkında birçok bilgiye ulaşıldı. Saldırgan muhasebecinin ihmali ile muhasebeci hakkında bir çok bilgi toplayarak amacına (veri hırsızlığı, kimlik avı, sosyal mühendislik, yetkisiz erişim)ulaştı. Bu yüzden çalışanlarınıza siber güvenlik farkındalığı kazandırmalıyız.

Öneriler

- Şirketteki çalışanlara veya müşterilereilgili olay hakkında bilgi verilmeli.
- Saldırgan hakkında toplanan veriler ilgili birimlere verilmeli
- Saldırgan engellenmeli gerekeli zararlı yazılım temizlenmesi yapılmalı
- Şifreler ve saldırganın öğrendiği önemli değiştirilebilecek bilgiler değiştirilmeli
- Eğer etkilenen kişinin kullandığı hesaplarda 2FA (iki adımlı doğrulama) özelliği varsa, bu özelliği hemen etkinleştirmelidir.

Önlemler

- Bilinmeyen e-postalara dikkat edin.
- Güvenilir antivirüs ve güvenlik yazılımları kullanın.
- Güvenli olmayan ve bilinmeyen sitelerden uzak durun.
- Güçlü şifreler kullanın.
- İki adımlı doğrulama kullanın.
- Bilinmeyen e-posta veya kaynaklardan dosya indirirken dikkat edin.