PCAP DOSYASI ANALİZİ

Hazırlayan:

Adı: Ayşe

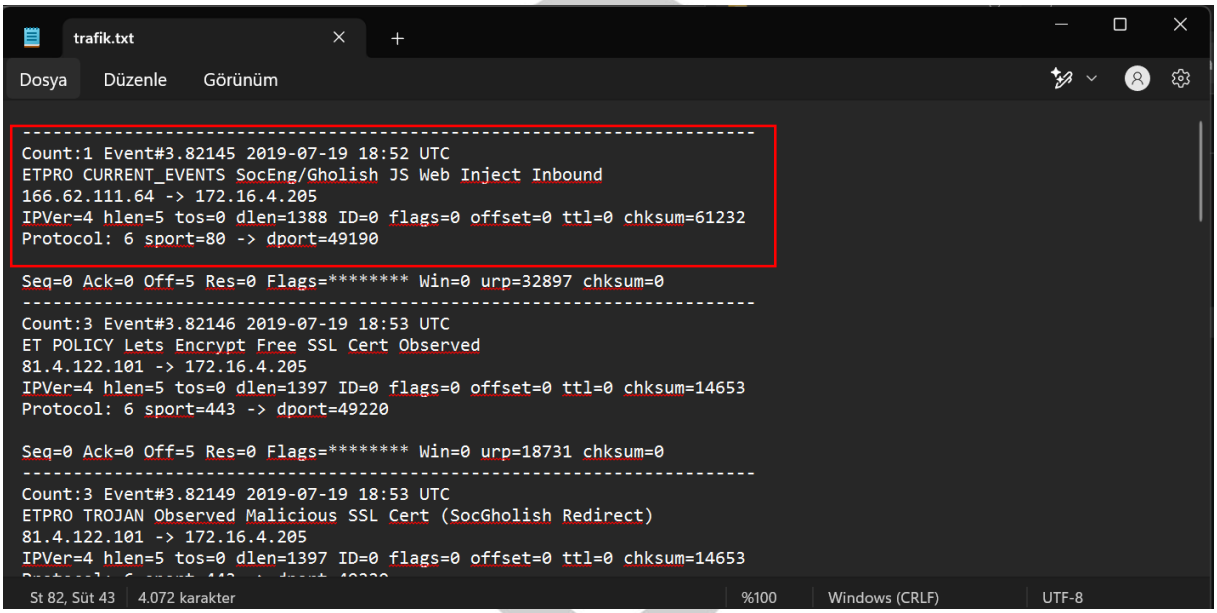
Soyadı: BALCI

Tarih: 15.03.2025

OLAY/VAKA ÖZETİ

Tarih/Zaman: 19 Temmuz 2019, 18:53 - 22:05
Etkilenen IP: 172.16.4.205
Saldırı Tipi: SocGholish Zararlı Yazılım Enfeksiyonu, Veri Sızdırma, Kötü Amaçlı SSL Sertifikaları, Uzaktan Yönetim Aracı (NetSupport) Kötüye Kullanımı

Özet:
Şirket ağına bağlı olan 172.16.4.205 IP adresine sahip Rotterdam-PC adlı cihazda, kötü amaçlı bir web sitesinden SocGholish zararlı yazılımının indirildiği tespit edilmiştir. Bu süreçte, sahte Let's Encrypt SSL sertifikaları kullanılarak güvenilmeyen bağlantılar yapılmıştır. Ayrıca, şüpheli POST istekleriyle veri sızdırılması gerçekleşmiştir. Saldırganın, NetSupport adlı uzaktan yönetim aracını kullanarak cihazın kontrolünü ele geçirmeye çalıştığı belirlenmiştir.

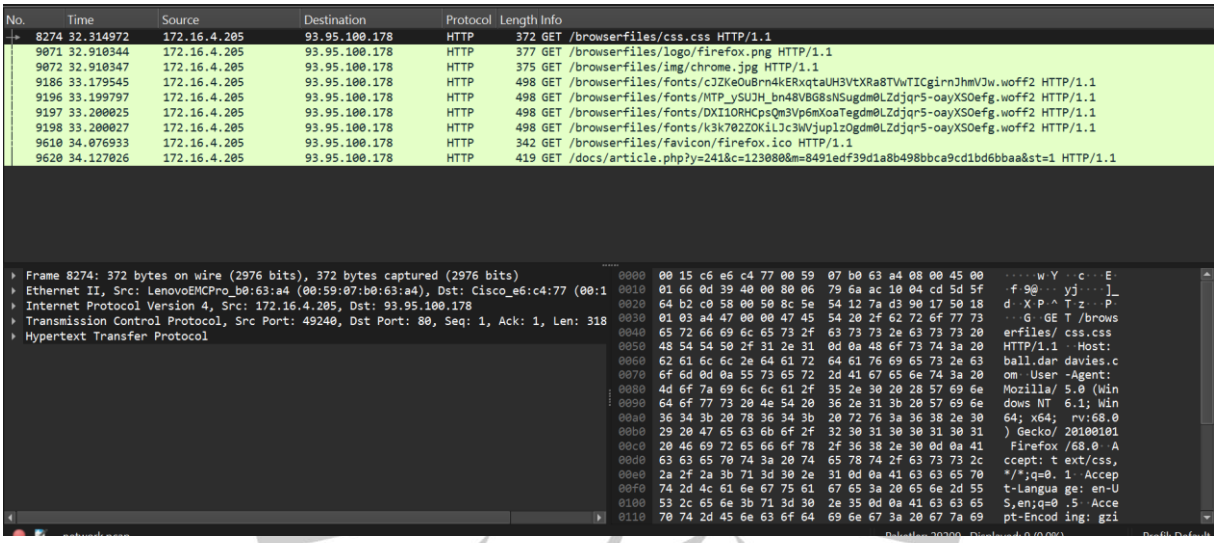


2. DETAYLI ANALİZ

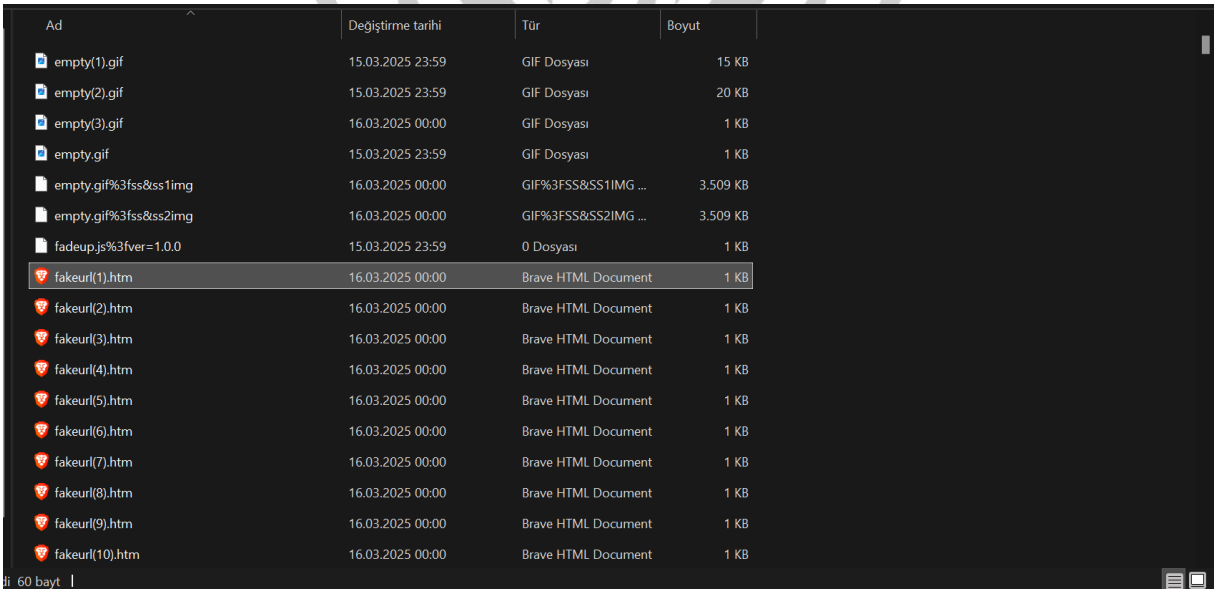
Zararlı Bulaşmış Cihazın Bilgileri

- **IP Adresi:** 172.16.4.205
- **MAC Adresi:** 00:59:07:b0:63:a4
- **Hostname:** Rotterdam-PC
- **Kullanıcı Hesabı:** Tespit edilemedi, işletim sisteminin MSFT 5.0 - Windows olduğu tespit edildi.
- **Şirket Adı:** Mind-Hammer
- **Domain:** mind-hammer.net
- **İşletim Sistemi:** Windows

Saldırı Vektörü:
Saldırının, kötü amaçlı bir web sitesine (SocGholish ile bağlantılı) erişilmesiyle başladığı anlaşılmaktadır. Saldırı sırasında ball.dardavies.com ve mysocalledchaos.com gibi şüpheli web sitelerinden GET istekleri yapılmıştır. Bu sitelerden zararlı JavaScript kodlarının indirildiği düşünülmektedir.

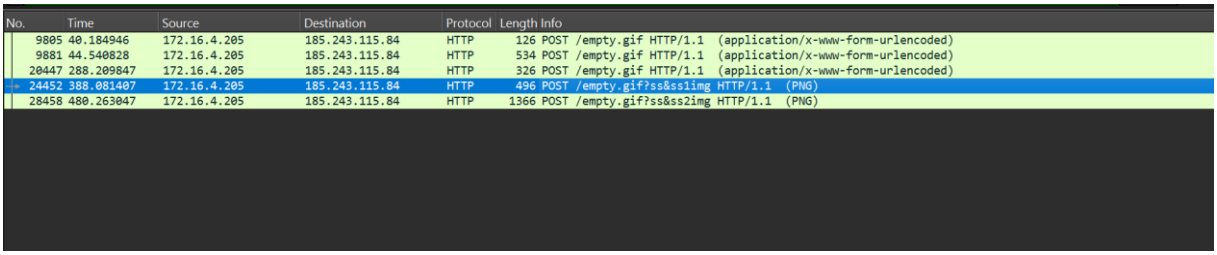


Pcap dosyası içindeki dosyalar dışarı aktarıldığında farklı resim, html, javascript gibi çok sayıda dosya olduğu görülmüştür.

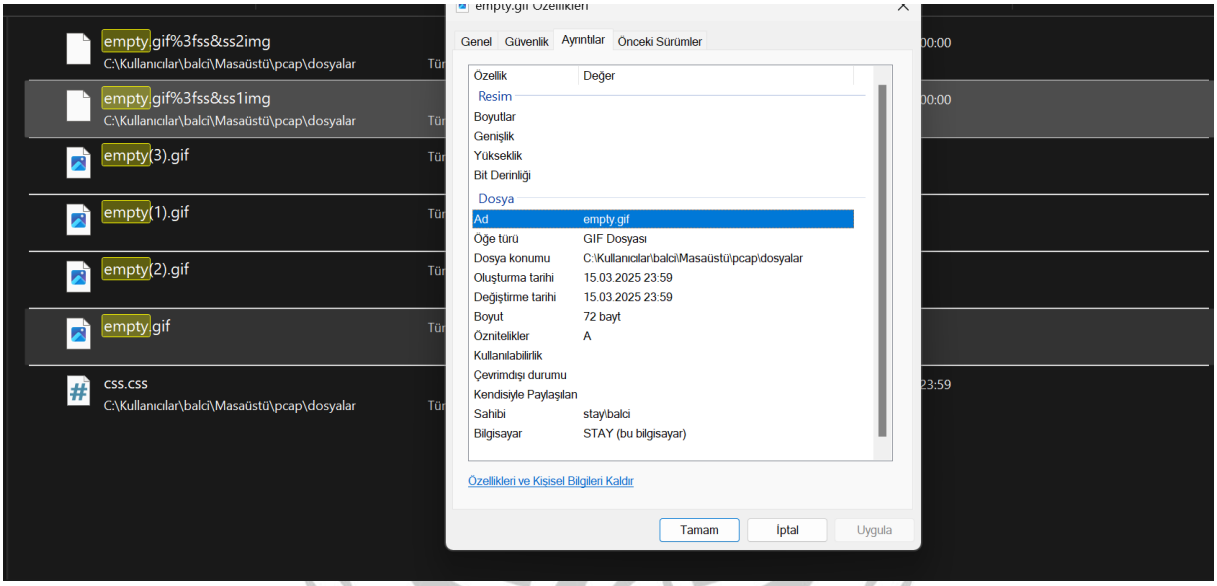


Cihazın, sahte SSL sertifikaları kullanarak güvenilmeyen bağlantılar kurduğu belirlenmiştir. Özellikle ball.dardavies.com sitesi üzerinden TLSv1.2 şifreleme ile güvenilmeyen SSL bağlantıları yapılmıştır.
Kullanılan SSL sertifikasının şifreleme algoritmasının TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 olduğu saptanmıştır.

Ayrıca, cihazın kötü amaçlı bir GIF dosyasına veri sızdırdığı tespit edilmiştir. b5689023.green.mattingsolutions.co adresine, empty.gif adlı dosya POST edilmiştir.

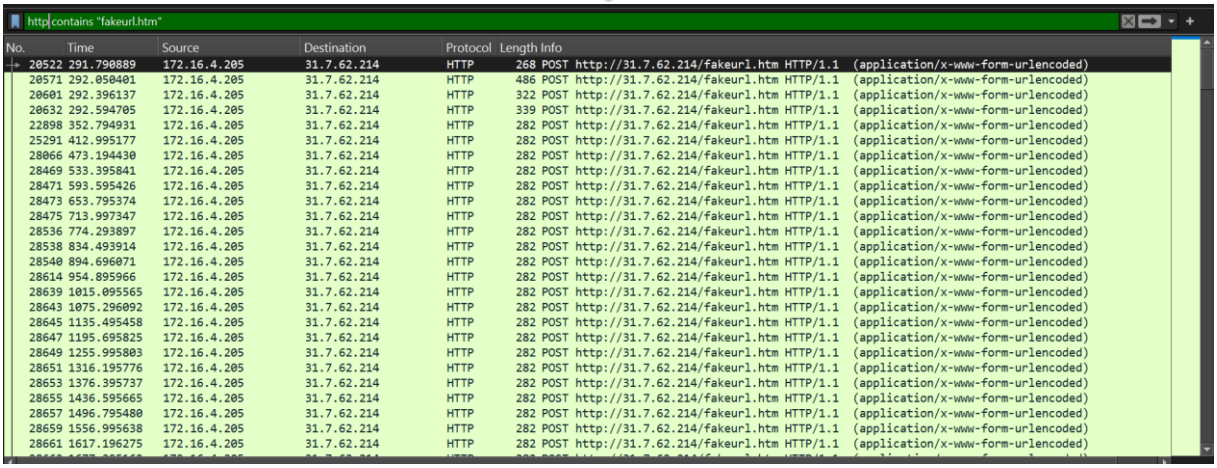


No.	Time	Source	Destination	Protocol	Length	Info
9805	40.184946	172.16.4.205	185.243.115.84	HTTP	126	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
9881	44.540828	172.16.4.205	185.243.115.84	HTTP	534	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
20447	288.209847	172.16.4.205	185.243.115.84	HTTP	326	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
24452	388.081407	172.16.4.205	185.243.115.84	HTTP	496	POST /empty.gif?ss&ss1img HTTP/1.1 (PNG)
28458	480.263047	172.16.4.205	185.243.115.84	HTTP	1366	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)

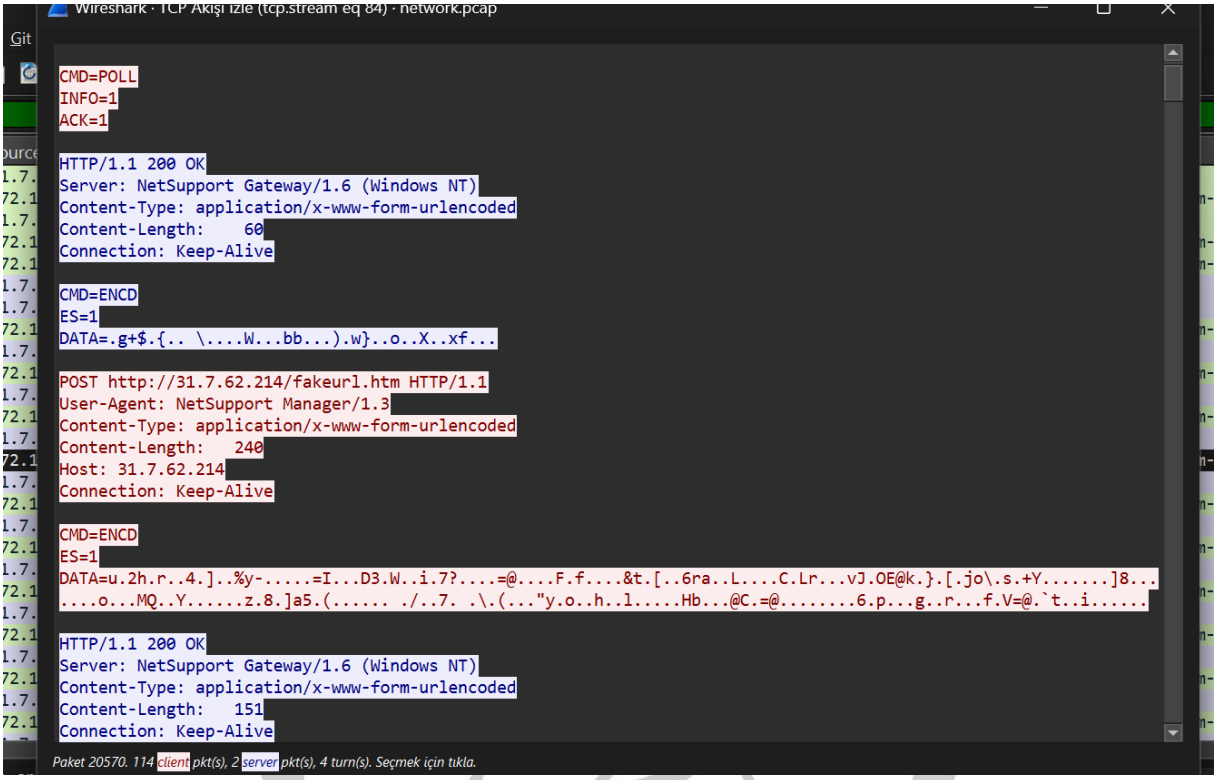


Saldırganın SocGholish zararlısını kullanarak çalınan verileri bir GIF dosyasının içinde gizlemiştir.

Saldırgan, NetSupport aracıyla cihazın kontrolünü ele geçirmeye çalışmıştır. 31.7.62.214 adresine, fakeurl.htm adlı sahte bir web sayfası üzerinden POST isteği yapılmıştır.



No.	Time	Source	Destination	Protocol	Length	Info
20522	291.790889	172.16.4.205	31.7.62.214	HTTP	268	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20571	292.050401	172.16.4.205	31.7.62.214	HTTP	486	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20601	292.396137	172.16.4.205	31.7.62.214	HTTP	322	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
20632	292.594705	172.16.4.205	31.7.62.214	HTTP	339	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
22898	352.794931	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
25291	412.995177	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28066	473.194430	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28469	533.395841	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28471	593.595426	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28473	653.795374	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28475	713.997347	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28536	774.293897	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28538	834.493914	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28540	894.696071	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28614	954.895966	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28639	1015.095565	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28643	1075.296092	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28645	1135.495458	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28647	1195.695825	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28649	1255.995803	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28651	1316.195776	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28653	1376.395737	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28655	1436.595665	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28657	1496.795480	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28659	1556.995638	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
28661	1617.196275	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)



Ayrıca, ağ içinde başka şüpheli IP adreslerine ait hareketlilik de tespit edilmiştir:

- **195.171.92.116** → geo.netsupportsoftware.com
  Saldırganlar, NetSupport aracı üzerinden kurban makinelerini uzaktan yönetebilir ve ağdaki diğer cihazlara bulaştırma girişiminde bulunabilirler.

3. IOC'LER

Şüpheli IP Adresleri ve Alan Adları

- **166.62.111.64** → mysocalledchaos.com (Bu adresin kötü amaçlı JavaScript içerdiği düşünülmektedir).
- **93.95.100.178** → ball.dardavies.com (Sahte SSL bağlantılarının bulunduğu tespit edilmiştir).
- **185.243.115.84** → b5689023.green.mattingsolutions.co (Veri sızdırmak için kullanıldığı anlaşılmıştır).
- **31.7.62.214** → fakeurl.htm (Saldırganın, NetSupport üzerinden cihazı ele geçirmeye çalıştığı belirlenmiştir).
- **195.171.92.116** → geo.netsupportsoftware.com (NetSupport aracının kötüye kullanımıyla ilişkilendirilen bir IP adresidir).

Şüpheli Ağ Trafiği

- **ETPRO CURRENT_EVENTS SocEng/Gholish JS Web Inject** → Zararlı JavaScript kodlarının ağda tespit edildiği anlaşılmıştır.
- **ETPRO TROJAN Observed Malicious SSL Cert (SocGholish Redirect)** → Sahte SSL sertifikalarının kullanıldığını gösteren bir trafik kaydı tespit edilmiştir.

- **ET POLICY Lets Encrypt Free SSL Cert Observed** → Güvenilmeyen SSL bağlantılarının yapıldığı gözlemlenmiştir.
- **ETPRO POLICY NetSupport Remote Admin Checkin & Response** → NetSupport aracının kötüye kullanımıyla ilgili ağ trafiği tespit edilmiştir.

Kötü Amaçlı POST & Veri Sızdırma

- **http://b5689023.green.mattingsolutions.co/empty.gif**
  Çalınan verilerin bir GIF dosyası aracılığıyla sızdırıldığı belirlenmiştir.
- **http://31.7.62.214/fakeurl.htm**
  Saldırganın, NetSupport aracını kullanarak cihazı ele geçirmeye çalıştığı belirlenen bir sahte web sayfasıdır.