PCAP ANALİZİ

Hazırlayan

Neslihan ASLAN

17/03/2025

İçindekiler

OLAY/ VAKA ÖZETİ

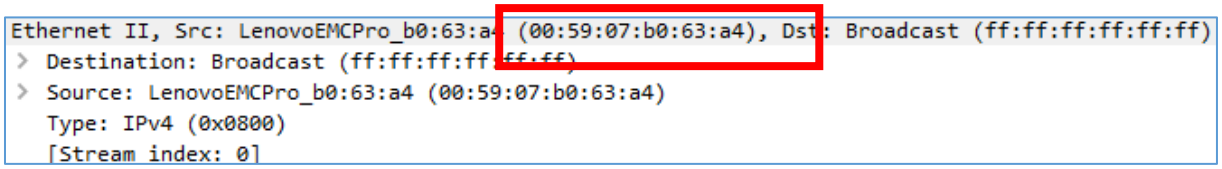
19 Temmuz 2019 tarihinde gerçekleşen olayda kötü amaçlı yazılımın şirket ağına bulaştığı görülmektedir. **172.16.4.205** IP adresine sahip bir sistemin **SocGholish** kötü amaçlı yazılımına maruz kaldığı tespit edilmiştir. Saldırı, sahte **Let's Encrypt SSL** sertifikalarıyla güvenli bağlantı izlenimi vererek kötü amaçlı bir web sitesinden zararlı kod indirilmesiyle başlamıştır. Ardından, sistemden dışarıya şüpheli POST istekleriyle veri transferi gerçekleştirilmiş ve saldırganlar, **NetSupport** uzaktan erişim aracını kullanarak cihaz üzerinde yetki kazanmaya çalışmıştır.

```
Count:1 Event#3.82145 2019-07-19 18:52 UTC
ETPRO CURRENT_EVENTS SocEng/Gholish JS Web Inject Inbound
166.62.111.64 -> 172.16.4.205
IPVer=4 hlen=5 tos=0 dlen=1388 ID=0 flags=0 offset=0 ttl=0 chksum=61232
Protocol: 6 sport=80 -> dport=49190

Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=32897 chksum=0
------------------------------------------------------------------------
Count:3 Event#3.82146 2019-07-19 18:53 UTC
ET POLICY Lets Encrypt Free SSL Cert Observed
81.4.122.101 -> 172.16.4.205
IPVer=4 hlen=5 tos=0 dlen=1397 ID=0 flags=0 offset=0 ttl=0 chksum=14653
Protocol: 6 sport=443 -> dport=49220

Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=18731 chksum=0
------------------------------------------------------------------------
Count:3 Event#3.82149 2019-07-19 18:53 UTC
ETPRO TROJAN Observed Malicious SSL Cert (SocGholish Redirect)
81.4.122.101 -> 172.16.4.205
IPVer=4 hlen=5 tos=0 dlen=1397 ID=0 flags=0 offset=0 ttl=0 chksum=14653
Protocol: 6 sport=443 -> dport=49220

Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=18731 chksum=0
------------------------------------------------------------------------
Count:6 Event#3.82152 2019-07-19 18:53 UTC
ET POLICY Lets Encrypt Free SSL Cert Observed
93.95.100.178 -> 172.16.4.205
IPVer=4 hlen=5 tos=0 dlen=1397 ID=0 flags=0 offset=0 ttl=0 chksum=17045
Protocol: 6 sport=443 -> dport=49236

Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=17891 chksum=0
------------------------------------------------------------------------
Count:6 Event#3.82159 2019-07-19 18:53 UTC
ET POLICY Data POST to an image file (gif)
172.16.4.205 -> 185.243.115.84
IPVer=4 hlen=5 tos=0 dlen=532 ID=0 flags=0 offset=0 ttl=0 chksum=55999
Protocol: 6 sport=49249 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags******** Win=0 urp=53966 chksum=0
```

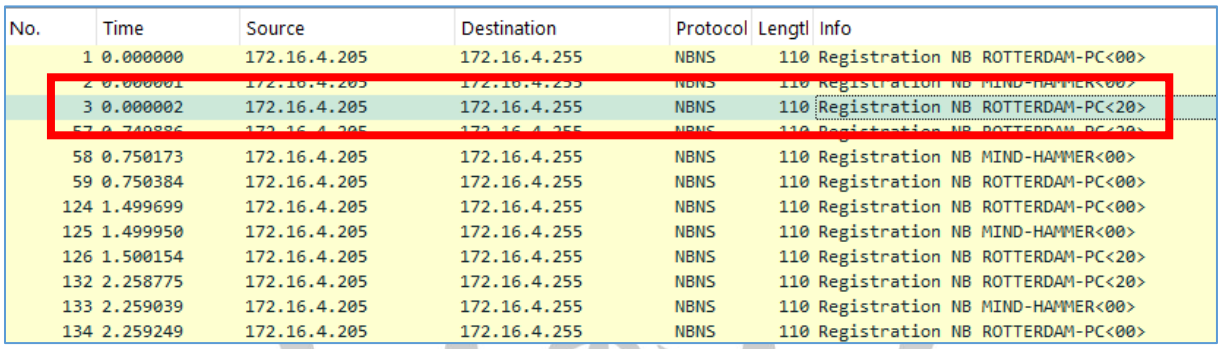
DETAYLI ANALİZ

Zararlı Bulaşmış Cihazın Bilgileri

- **IP Adresi:** 172.16.4.205
- **MAC Adresi:** 00:59:07: b0:63:a4

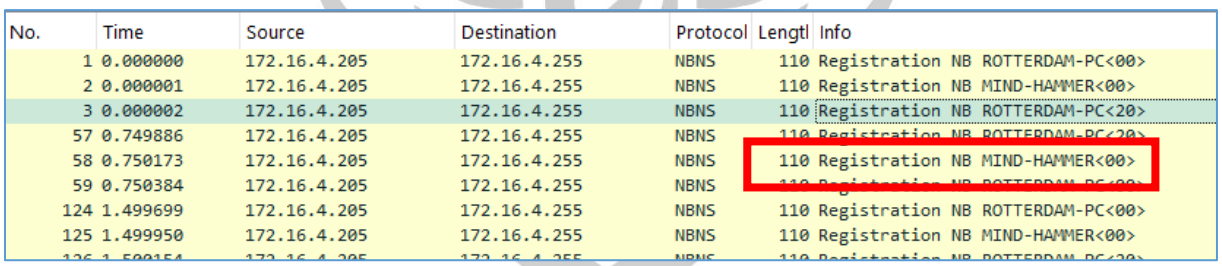


- **Hostname:** Rotterdam-PC



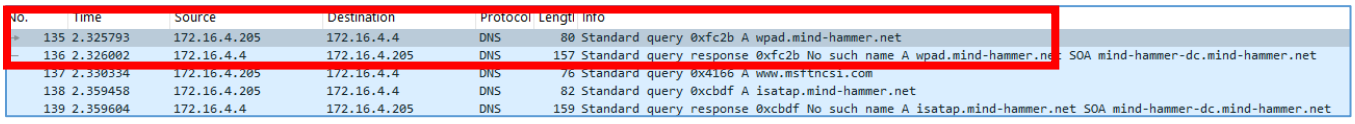
No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
3	0.000002	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
58	0.750173	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
59	0.750384	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
124	1.499699	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
125	1.499950	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
126	1.500154	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
132	2.258775	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
133	2.259039	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
134	2.259249	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>

- **Kullanıcı Hesabı:** Bulunamadı
- **Şirket Adı:** Mind-Hammer



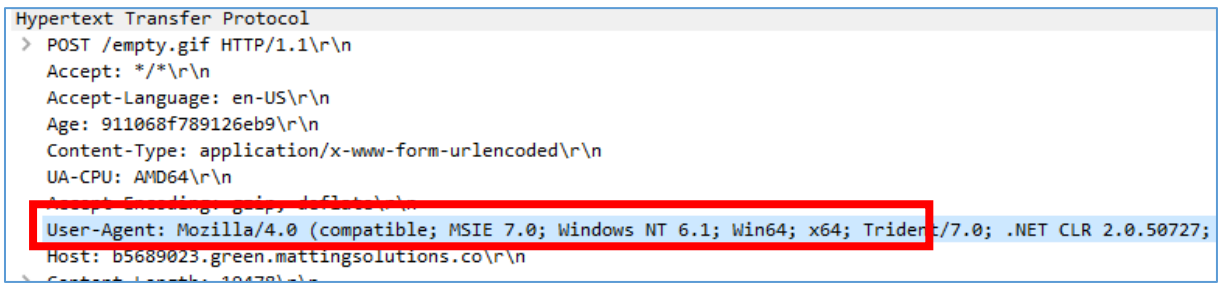
No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
2	0.000001	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
3	0.000002	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
57	0.749886	172.16.4.205	172.16.4.255	NBNS		
58	0.750173	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
59	0.750384	172.16.4.205	172.16.4.255	NBNS		
124	1.499699	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
125	1.499950	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>

- **Domain:** mind-hammer.net



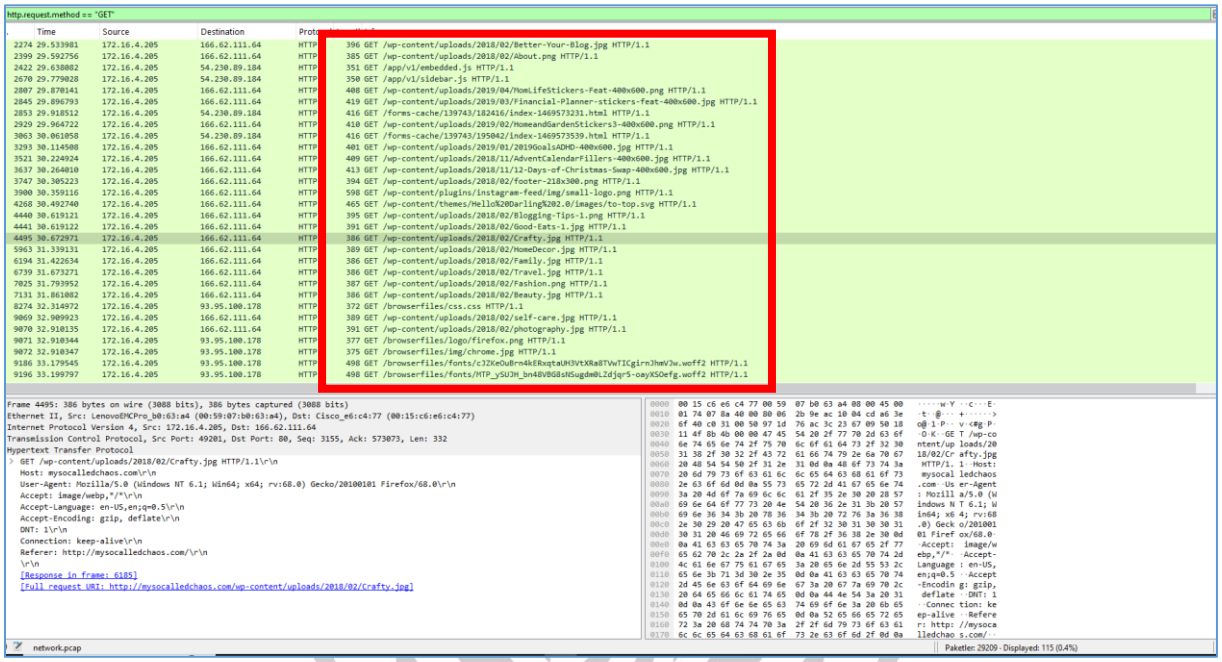
No.	Time	Source	Destination	Protocol	Lengtl	Info
135	2.325793	172.16.4.205	172.16.4.4	DNS	80	Standard query 0xfc2b A wpad.mind-hammer.net
136	2.326002	172.16.4.4	172.16.4.205	DNS	157	Standard query response 0xfc2b No such name A wpad.mind-hammer.net SOA mind-hammer-dc.mind-hammer.net
137	2.330334	172.16.4.205	172.16.4.4	DNS	76	Standard query 0x4166 A www.msftncsi.com
138	2.359458	172.16.4.205	172.16.4.4	DNS	82	Standard query 0xcbdf A isatap.mind-hammer.net
139	2.359604	172.16.4.4	172.16.4.205	DNS	159	Standard query response 0xcbdf No such name A isatap.mind-hammer.net SOA mind-hammer-dc.mind-hammer.net

- **İşletim Sistemi:** Windows

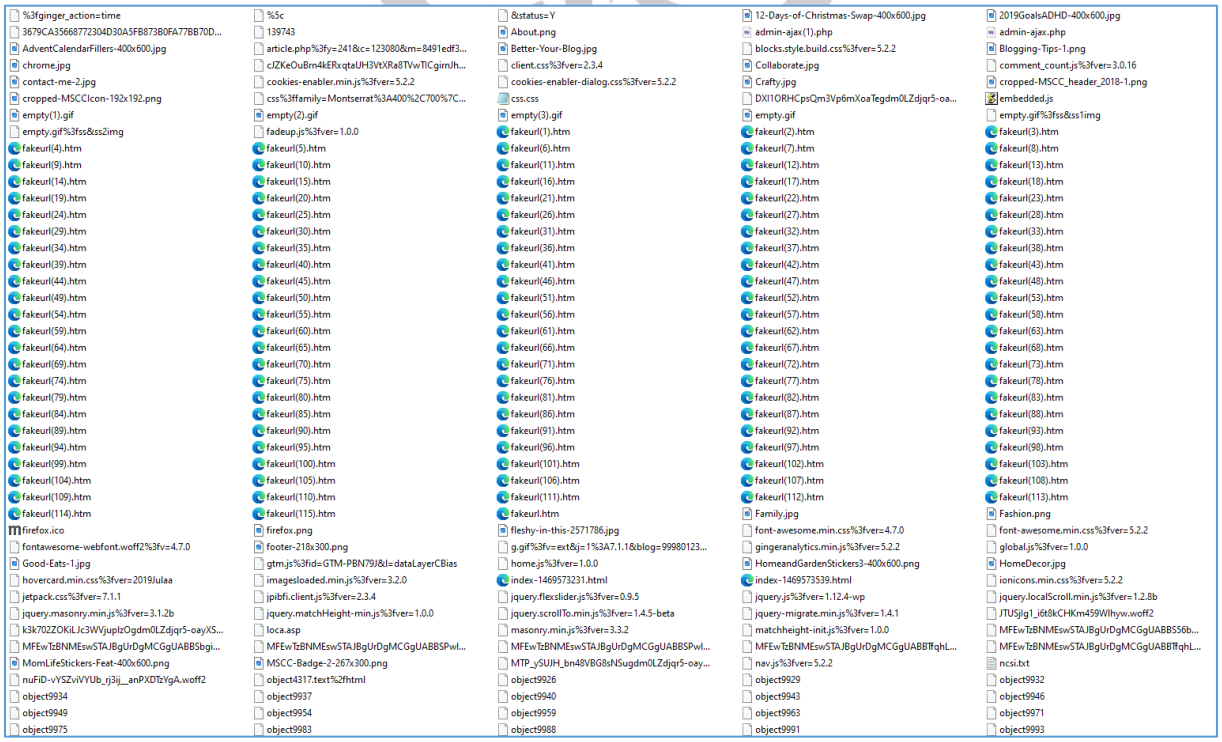


Saldırı Vektörü:

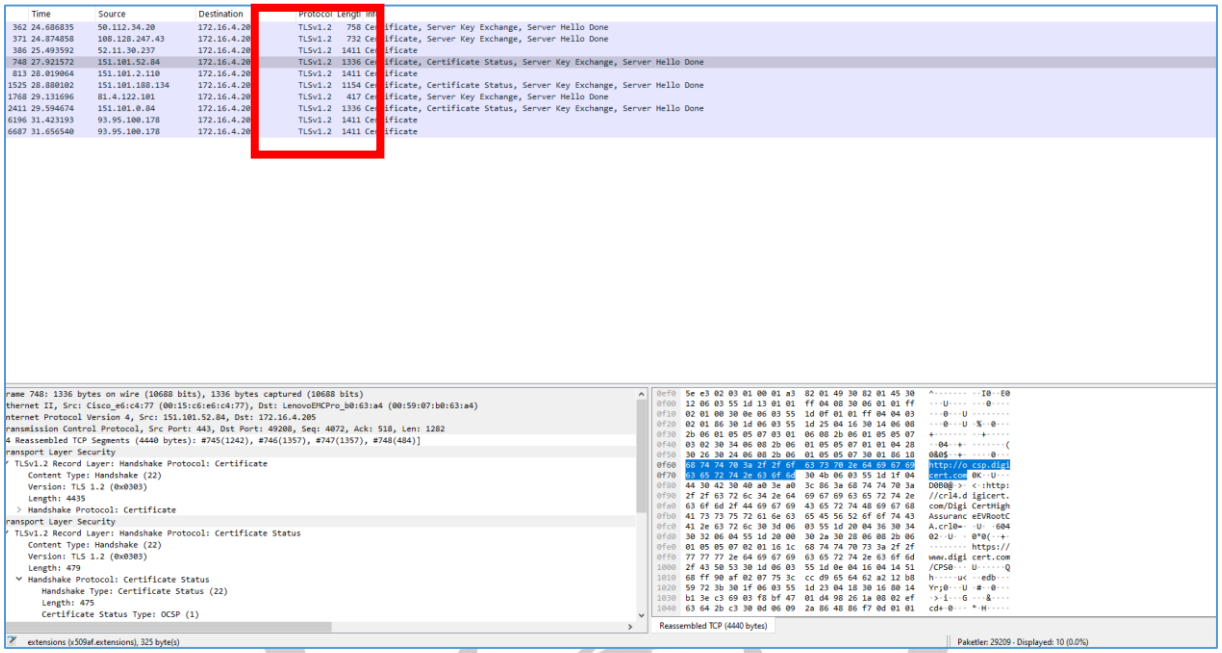
ball.dardavies.com ve **mysocalledchaos.com** gibi güvenilmeyen alan adlarına yapılan HTTP GET isteklerinin gözlenlenmesiyle saldırının, kullanıcının kötü amaçlı bir web sitesini ziyaret etmesiyle başladığı gözlemlenmiştir. Bu isteklerin, cihazın SocGholish zararlısını indirmiş olabileceğine işaret etmektedir.



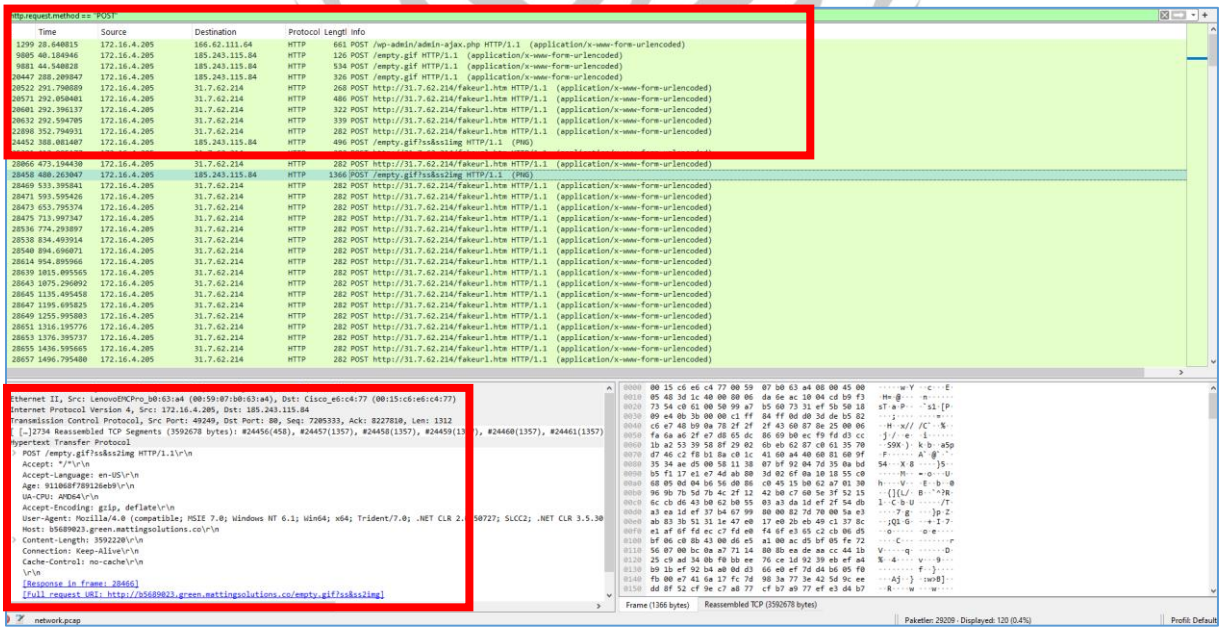
PCAP içindeki HTTP üzerinden indirilen resim, HTML, JavaScript veya diğer dosyaları dışarı aktardığımızda:



Server Hello paketlerindeki sertifika bilgilerine baktığımızda **ball.dardavies.com** alan adına **TLSv1.2 şifreleme** ile bağlantı kurulduğu ve kullanılan sertifikanın şüpheli olduğu görülmüştür.

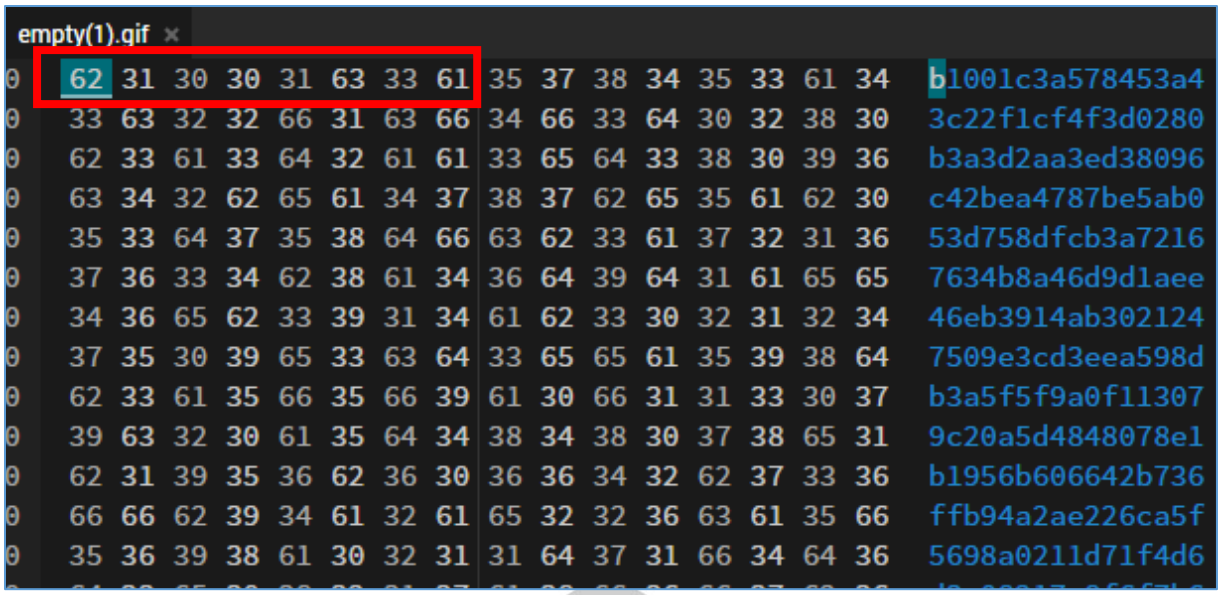


Post isteklerini kontrol ederken **b5689023.green.mattingsolutions.co** adresine **empty.gif** adlı bir dosya üzerinden **POST** isteği dikkat çekmektedir.



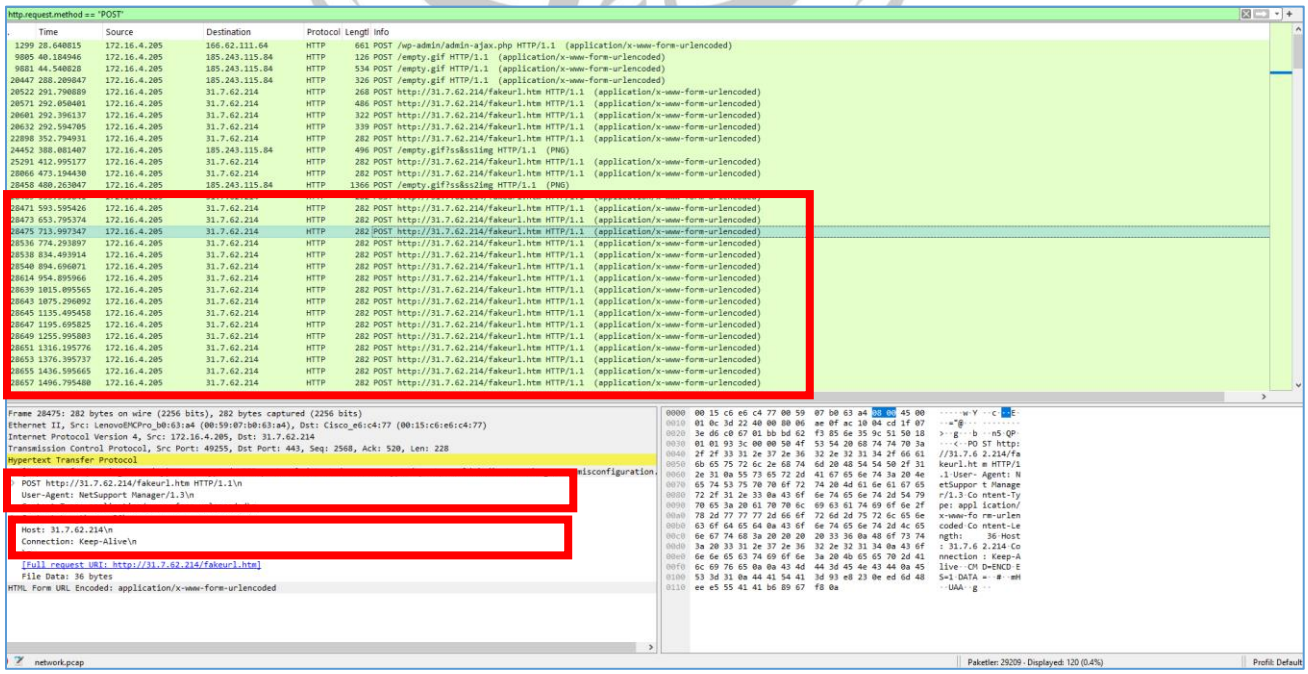
GIF dosyasını kontrol ettiğimizde:

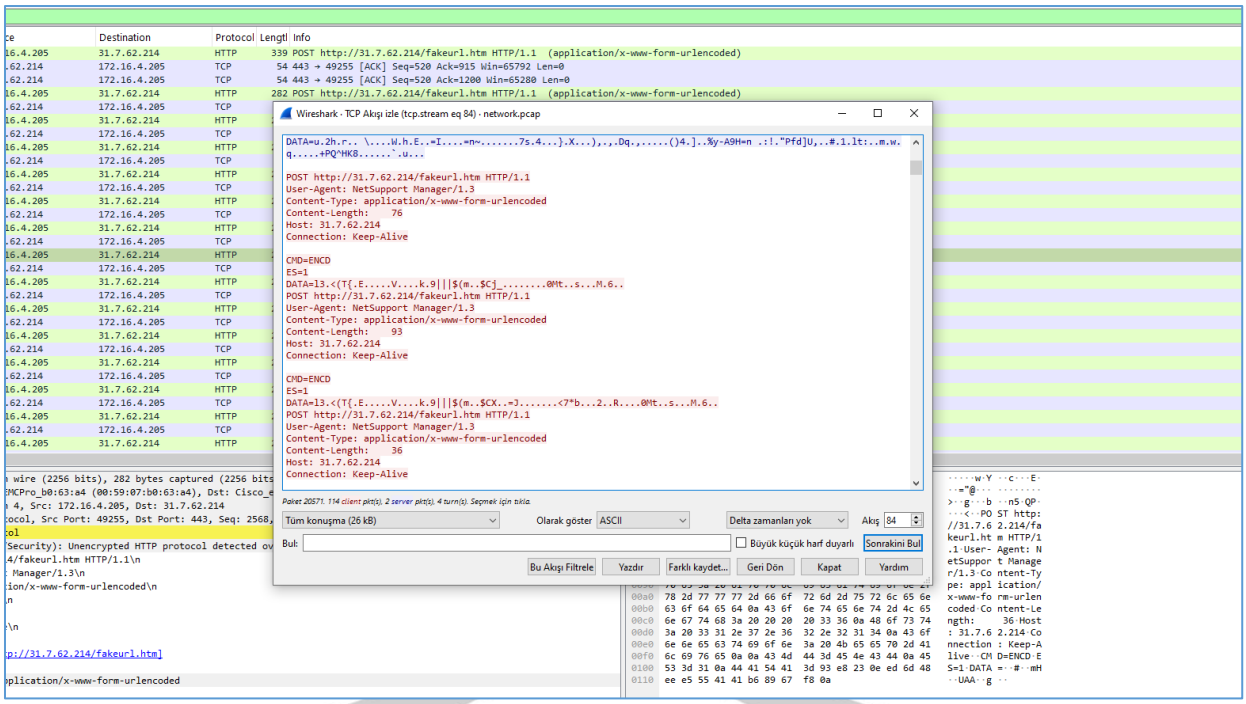
47 49 46 38 37 61 47 49 46 38 39 61	GIF87a GIF89a	0	gif	Image file encoded in the Graphics Interchange Format (GIF)[9]



Bu durum, saldırganların veri sızdırma amacıyla bir GIF dosyası içine gizlenmiş kötü amaçlı kod kullanmış olabileceği fikrini güçlendirmektedir.

NetSupport uzaktan erişim aracını kullanarak cihazın kontrol edilmeye çalıştığı görülmüştür. **31.7.62.214** IP adresine, sahte bir web sayfası üzerinden **fakeurl.htm** adlı bir dosya POST edilmiştir. Bu durum, saldırganın kurban cihazda uzaktan yönetim sağlamak için NetSupport'u kötüye kullandığına gösterir.





TEHLİKE GÖSTERGELERİ (IOC'LER)

IP Adresleri:

- 166.62.111.64: mysocalledchaos.co
- 81.4.122.101: ball.dardavies.com
- 93.95.100.178: b5689023.green.mattingsolutions.co
- 31.7.62.214: fakeurl.htm
- 185.243.115.84: geo.netsupportsoftware.com

Kötü Amaçlı POST & Veri Sızdırma

• http://b5689023.green.mattingsolutions.co/empty.gif

• http://31.7.62.214/fakeurl.htm