

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.

```
trafik.txt
Dosya  Düzenle  Görünüm

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

St 82, Süt 43 | 4.072 karakter | %100 | Windows (CRLF) | UTF-8
```

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.

No.	Time	Source	Destination	Protocol	Length	Info
8274	32.314972	172.16.4.205	93.95.100.178	HTTP	372	GET /browserfiles/css.css HTTP/1.1
9071	32.910344	172.16.4.205	93.95.100.178	HTTP	377	GET /browserfiles/logo/firefox.png HTTP/1.1
9072	32.910347	172.16.4.205	93.95.100.178	HTTP	375	GET /browserfiles/img/chrome.jpg HTTP/1.1
9186	33.179545	172.16.4.205	93.95.100.178	HTTP	498	GET /browserfiles/fonts/cJZKe0u8rn4kERxqtaUH3vtXRa8TWvTICgirn3hmVJw.woff2 HTTP/1.1
9196	33.199797	172.16.4.205	93.95.100.178	HTTP	498	GET /browserfiles/fonts/MTp_YSUJH_bn48VBG8sNSugdmlLZdjqr5-oayXS0efg.woff2 HTTP/1.1
9197	33.200025	172.16.4.205	93.95.100.178	HTTP	498	GET /browserfiles/fonts/DXI10RHcpsQm3Vp6mXoaTegdm8LZdjqr5-oayXS0efg.woff2 HTTP/1.1
9198	33.200027	172.16.4.205	93.95.100.178	HTTP	498	GET /browserfiles/fonts/k3k78220Kil3c3WjuplZogdm8LZdjqr5-oayXS0efg.woff2 HTTP/1.1
9610	34.076933	172.16.4.205	93.95.100.178	HTTP	342	GET /browserfiles/favicon/firefox.ico HTTP/1.1
9620	34.127026	172.16.4.205	93.95.100.178	HTTP	419	GET /docs/article.php?y=241&c=123888&m=8491edf39d1a8b498bbca9cd1bd6bbaa&st=1 HTTP/1.1

Frame 8274: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits)	0000	00 15 c6 e6 c4 77 00 59	07 b0 63 a4 08 00 45 00w.Y...c...E
Ethernet II, Src: LenovoEMCPro_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:1	0010	01 66 0d 39 40 00 80 06	79 6a ac 10 04 cd 5d 5f	.f.9@...y[...]_
Internet Protocol Version 4, Src: 172.16.4.205, Dst: 93.95.100.178	0020	64 b2 c0 58 00 50 8c 5e	54 12 7a d3 90 17 50 18	d.X.P.^T.z...P
Transmission Control Protocol, Src Port: 49240, Dst Port: 80, Seq: 1, Ack: 1, Len: 318	0030	01 03 a4 47 00 00 47 45	54 20 2f 62 72 6f 77 73	...G.GE.T./brows
Hypertext Transfer Protocol	0040	65 72 66 69 6e 65 73 2f	63 73 73 2e 63 73 73 20	erfiles/ css.css
	0050	48 54 54 50 2f 31 2e 31	0d 0a 48 6f 73 74 3a 20	HTTP/1.1 Host:
	0060	62 61 6c 6c 2e 64 61 72	64 61 76 69 65 73 2e 63	ball.dar davies.c
	0070	6f 6d 0d 0a 55 73 65 72	2d 41 67 65 6e 74 3a 20	om -User -Agent:
	0080	4d 6f 7a 69 6c 6c 61 2f	35 2e 30 20 28 57 69 6e	Mozilla/ 5.0 (Win
	0090	64 6f 77 73 20 4e 54 20	36 2e 31 3b 20 57 69 6e	dows NT 6.1; Win
	00a0	36 34 3b 20 78 36 34 3b	20 72 76 3a 36 38 2e 30	64; x64; rv:68.0
	00b0	29 20 47 65 63 6b 6f 2f	32 30 31 30 30 31 30 31) Gecko/ 20100101
	00c0	20 46 69 72 65 66 6f 78	2f 36 38 2e 30 0d 0a 41	Firefox /68.0 A
	00d0	63 63 65 70 74 3a 20 74	65 78 74 2f 63 73 73 2c	cept: text/css,
	00e0	2a 2f 2a 3b 71 3d 30 2e	31 0d 0a 41 63 63 65 70	/*;q=0.1 Accep
	00f0	74 2d 4c 61 6e 67 75 61	67 65 3a 20 65 6e 2d 55	t-Langua ge: en-U
	0100	53 2c 65 6e 3b 71 3d 30	2e 35 0d 0a 41 63 63 65	S,en;q=0.5 Acce
	0110	70 74 2d 45 6e 63 6f 64	69 6e 67 3a 20 67 7a 69	pt-Encod ing: gzi

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

Ad	Değiştirme tarihi	Tür	Boyut
empty(1).gif	15.03.2025 23:59	GIF Dosyası	15 KB
empty(2).gif	15.03.2025 23:59	GIF Dosyası	20 KB
empty(3).gif	16.03.2025 00:00	GIF Dosyası	1 KB
empty.gif	15.03.2025 23:59	GIF Dosyası	1 KB
empty.gif%3fss&ss1img	16.03.2025 00:00	GIF%3FSS&SS1IMG ...	3.509 KB
empty.gif%3fss&ss2img	16.03.2025 00:00	GIF%3FSS&SS2IMG ...	3.509 KB
fadeup.js%3fver=1.0.0	15.03.2025 23:59	0 Dosyası	1 KB
fakeurl(1).htm	16.03.2025 00:00	Brave HTML Document	1 KB
fakeurl(2).htm	16.03.2025 00:00	Brave HTML Document	1 KB
fakeurl(3).htm	16.03.2025 00:00	Brave HTML Document	1 KB
fakeurl(4).htm	16.03.2025 00:00	Brave HTML Document	1 KB
fakeurl(5).htm	16.03.2025 00:00	Brave HTML Document	1 KB
fakeurl(6).htm	16.03.2025 00:00	Brave HTML Document	1 KB
fakeurl(7).htm	16.03.2025 00:00	Brave HTML Document	1 KB
fakeurl(8).htm	16.03.2025 00:00	Brave HTML Document	1 KB
fakeurl(9).htm	16.03.2025 00:00	Brave HTML Document	1 KB
fakeurl(10).htm	16.03.2025 00:00	Brave HTML Document	1 KB

Cihazın, sahte SSL sertifikaları kullanarak güvenilmeyen bağlantılar kurduğu belirlenmiştir. Özellikle ball.dardavies.com sitesi üzerinden TLSv1.2 şifreleme ile güvenilmeyen SSL bağlantıları yapılmıştır.

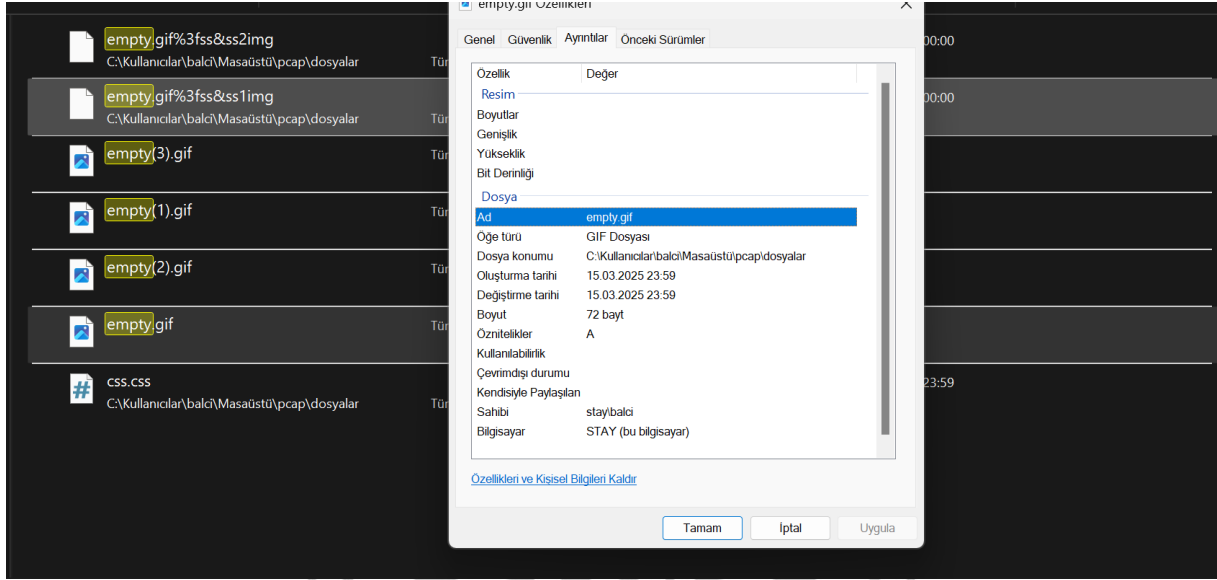
Kullanılan SSL sertifikasının şifreleme algoritmasının

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	44.549828	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	480.263947	172.16.4.205	185.243.115.84	HTTP	1366	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)



Saldırganın SocGhosh 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	894.696871	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	1015.895565	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)

```
Wireshark - TCP Akışı İzle (tcp.stream eq 84) - network.pcap
Git
CMD=POLL
INFO=1
ACK=1
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.6 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Connection: Keep-Alive
CMD=ENCD
ES=1
DATA=.g+$.{.. \...W...bb...).w}..o..X..xf...
POST http://31.7.62.214/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length: 240
Host: 31.7.62.214
Connection: Keep-Alive
CMD=ENCD
ES=1
DATA=u.2h.r..4.]..%y-.....=I...D3.W..i.7?....=@....F.f....&t[..6ra..L....C.Lr...vJ.OE@k.}.[.jo\s.+Y.....]8...
....o...MQ..Y.....z.8.]a5.(..... ./..7. .\.(..."y.o.h..l.....Hb...@C.=@.....6.p...g..r...f.V=@.t..i.....
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.6 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-Length: 151
Connection: Keep-Alive
Paket 20570. 114 client pkt(s), 2 server pkt(s), 4 turn(s). Seçmek için tıkla.
```

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 Trafiki

- **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.

