Pcap Analizi

Hazırlayan: Saliha Polat

Tarih: 15.03.2025

İçindekiler

Olay/Vaka Özeti

19 Temmuz 2019 tarihinde, bir Windows kullanıcısı (172.16.4.205 – ROTTERDAM-PC) saldırıya uğramış bir web sitesini (mysocalledchaos.com) ziyaret etti. Kullanıcı, bu sayfadaki yönlendirmeye inanarak sahte bir güncelleme dosyasını indirdi.

İndirilen dosya, ZIP formatında bir arşiv olup içinde bir JavaScript (.js) dosyası barındırıyordu. Kullanıcının bu dosyayı çalıştırmasıyla birlikte sistemine zararlı yazılım bulaştı. Olayın ardından ağ trafiğinde anormal hareketler gözlemlendi.

166.62.111.64 adresinden gelen zararlı JavaScript web enjeksiyonu tespit edildi. Ardından sistem, Let's Encrypt sertifikası kullanılarak şifreli bir bağlantı kurdu. Bu, saldırganların yasal görünümlü HTTPS bağlantıları kullanarak zararlı dosya veya komutları aktardığını gösterdi.

Zararlı yazılımın çalıştırılmasının ardından, enfekte sistem 185.243.115.84 adresine HTTP POST istekleri göndermeye başladı. Daha sonra, enfekte sistem 31.7.62.214 adresine bağlantı kurarak NetSupport Manager RAT zararlısını yükledi. IDS/IPS sistemleri tarafından tespit edilen "NetSupport Remote Admin Checkin" ve "NetSupport Remote Admin Response" uyarıları, sistemin artık saldırganların kontrolüne geçtiğini gösterdi.

Detaylı Analiz

Kurban Ayrıntıları

Hostname: ROTTERDAM-PC

IP Addresi: 172.16.4.205

MAC Adresi: 00:59:07:b0:63:a4

User Account: matthijs.devries

Şirket ve Domain Bilgileri

Şirket: Mind-Hammer

Domain: mind-hammer.net

Domain Controller: 172.16.4.4

Gateway: 172.16.4.1

Broadcast: 172.16.4.255

Zararlı Türü

Windows Sürümü: Windows7 ya da 10

Saldırı Yöntemi: SocGholish

Son Yüklenen Zararlı Yazılım: NetSupport Manager RAT

Tehlike Göstergeleri (IOC'ler)

NetSupport RAT'ın C2 Sunucusu: 31.7.62.214

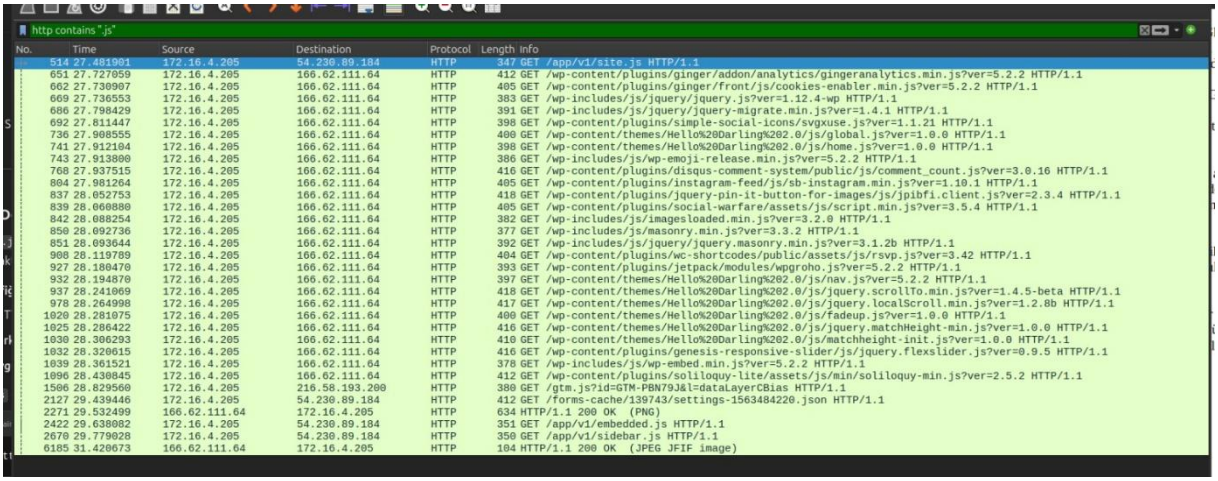
Sahte Güncelleme Bulunduran Alan Adı: ball.dardavies

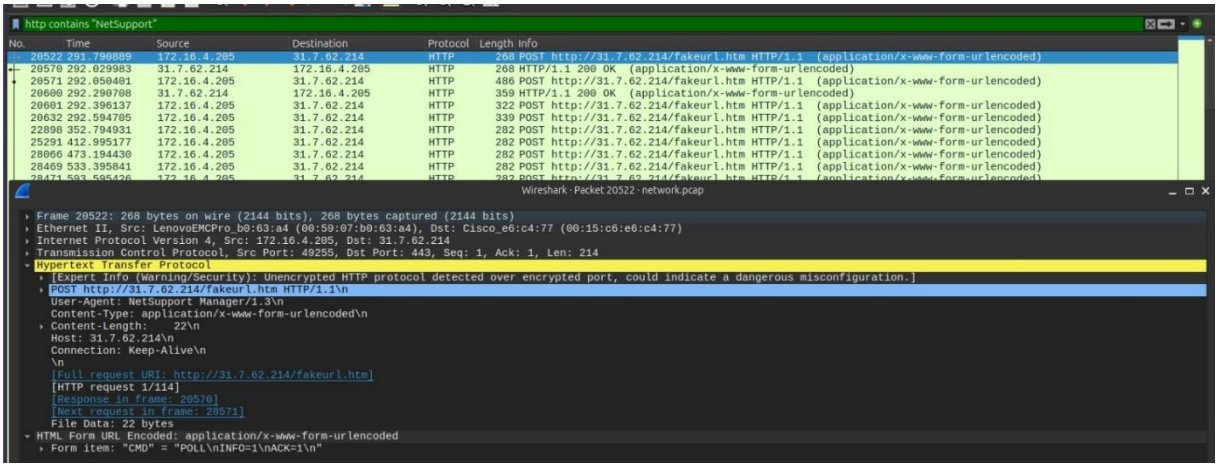
Güncelleme için yüklenen zararlı ZIP

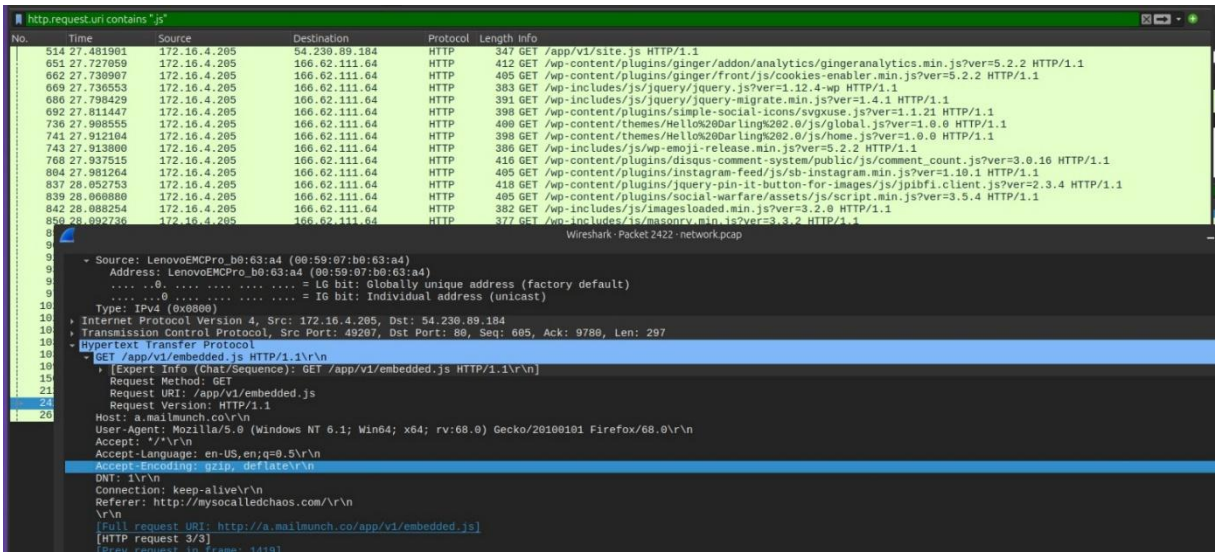
İçinde zararlı bulunan gif dosyası : /empty.gif?ss&ss1img, /empty.gif?ss&ss2img

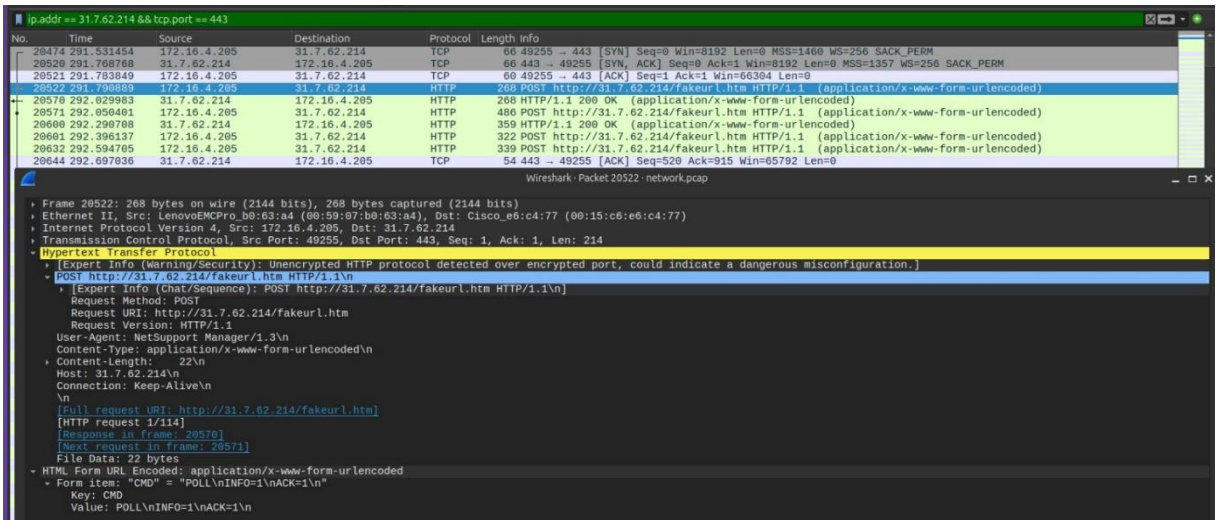
Certificate

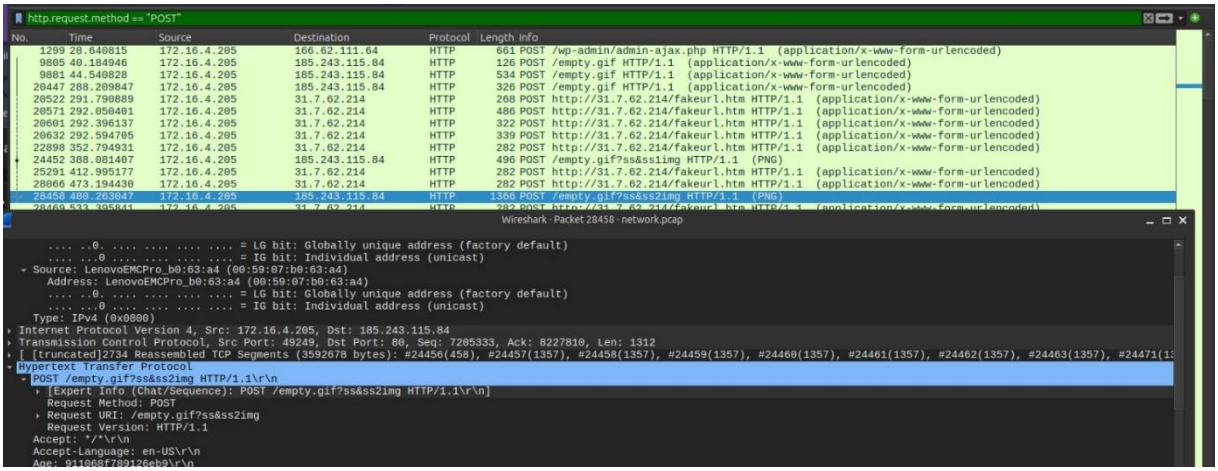
Wireshark' Elde Edilen Bazı Veriler

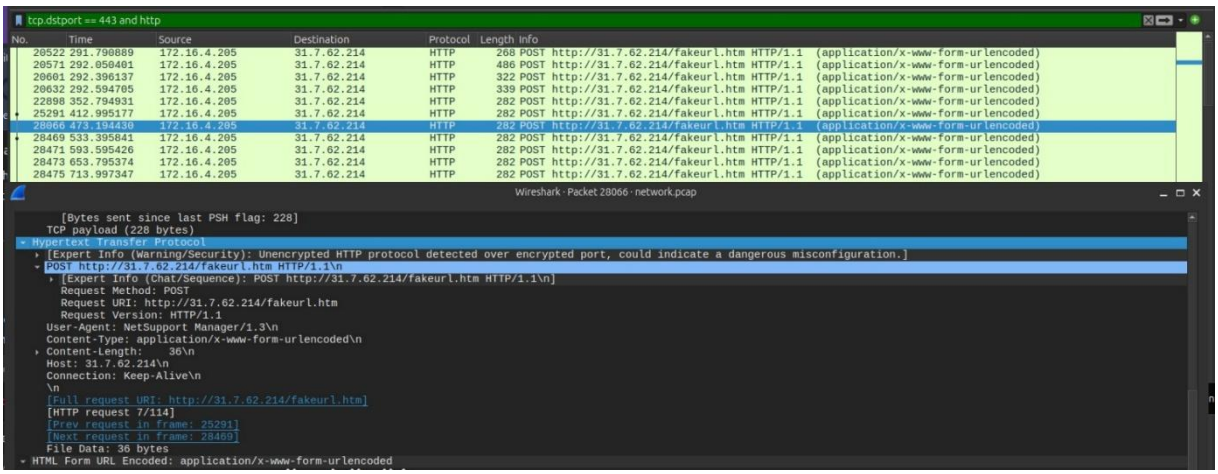


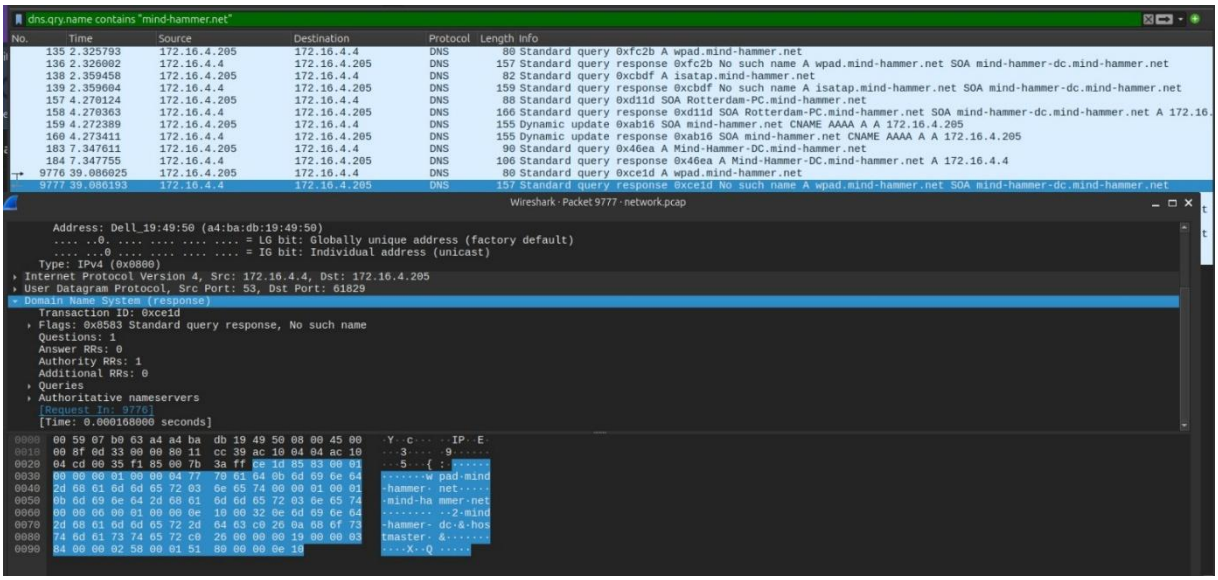


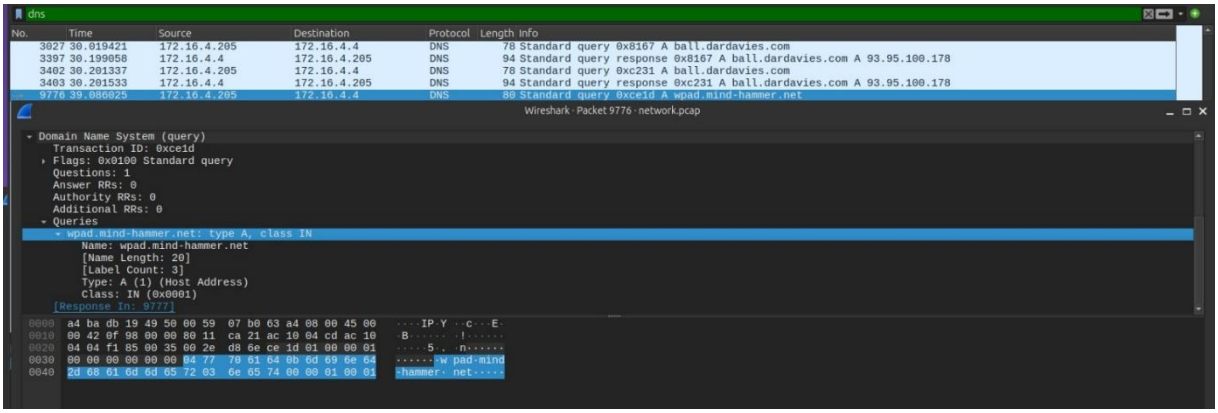


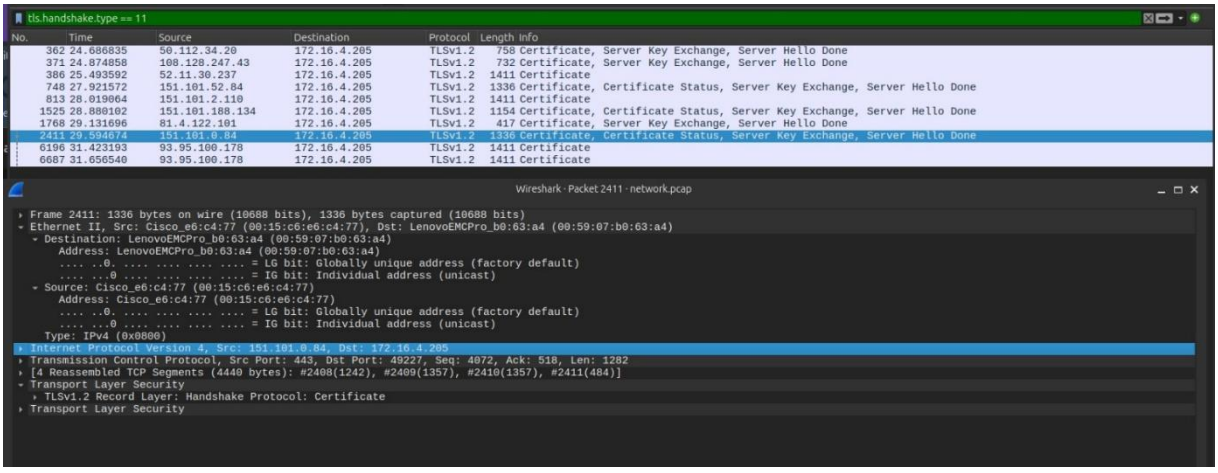

ip.addr == 31.7.62.214 && tcp.port == 443
No. Time Source Destination Protocol Length Info
20474 291.531454 172.16.4.205 31.7.62.214 TCP 66 49255 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
20520 291.768768 31.7.62.214 172.16.4.205 TCP 66 443 → 49255 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1357 WS=256 SACK_PERM
20521 291.783849 172.16.4.205 31.7.62.214 TCP 60 49255 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
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)
20570 292.029983 31.7.62.214 172.16.4.205 HTTP 268 HTTP/1.1 200 OK (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)
20600 292.290708 31.7.62.214 172.16.4.205 HTTP 359 HTTP/1.1 200 OK (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)
20644 292.697036 31.7.62.214 172.16.4.205 TCP 54 443 → 49255 [ACK] Seq=520 Ack=915 Win=65792 Len=0
Wireshark · Packet 20522 · network.pcap
Frame 20522: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits)
Ethernet II, Src: LenovoEMCPro_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
Internet Protocol Version 4, Src: 172.16.4.205, Dst: 31.7.62.214
Transmission Control Protocol, Src Port: 49255, Dst Port: 443, Seq: 1, Ack: 1, Len: 214
Hypertext Transfer Protocol
[Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n
[Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n]
Request Method: POST
Request URI: http://31.7.62.214/fakeurl.htm
Request Version: HTTP/1.1
User-Agent: NetSupport Manager/1.3\n
Content-Type: application/x-www-form-urlencoded\n
Content-Length: 22\n
Host: 31.7.62.214\n
Connection: Keep-Alive\n
\n
[Full request URI: http://31.7.62.214/fakeurl.htm]
[HTTP request 1/114]
[Response in frame: 20570]
[Next request in frame: 20571]
File Data: 22 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "CMD" = "POLL\nINFO=1\nACK=1\n"
Key: CMD
Value: POLL\nINFO=1\nACK=1\n


http.request.method == "POST"
No. Time Source Destination Protocol Length Info
1299 28.640815 172.16.4.205 166.62.111.64 HTTP 661 POST /wp-admin/admin-ajax.php HTTP/1.1 (application/x-www-form-urlencoded)
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)
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)
24452 388.081407 172.16.4.205 185.243.115.84 HTTP 490 POST /empty.gif?ss&ss1img HTTP/1.1 (PNG)
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)
28458 480.263047 172.16.4.205 185.243.115.84 HTTP 1366 POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)
Wireshark · Packet 28458 · network.pcap
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: LenovoEMCPro_b0:63:a4 (00:59:07:b0:63:a4)
Address: LenovoEMCPro_b0:63:a4 (00:59:07:b0:63:a4)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.4.205, Dst: 185.243.115.84
Transmission Control Protocol, Src Port: 49249, Dst Port: 80, Seq: 7205333, Ack: 8227810, Len: 1312
[truncated]2734 Reassembled TCP Segments (3592678 bytes): #24456(458), #24457(1357), #24458(1357), #24459(1357), #24460(1357), #24461(1357), #24462(1357), #24463(1357), #24471(1
Hypertext Transfer Protocol
POST /empty.gif?ss&ss2img HTTP/1.1\r\n
[Expert Info (Chat/Sequence): POST /empty.gif?ss&ss2img HTTP/1.1\r\n]
Request Method: POST
Request URI: /empty.gif?ss&ss2img
Request Version: HTTP/1.1
Accept: */*\r\n
Accept-Language: en-US\r\n
Age: 911068f789126eb9\r\n


tcp.dstport == 443 and http
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)
Wireshark · Packet 28066 · network.pcap
[Bytes sent since last PSH flag: 228]
TCP payload (228 bytes)
Hypertext Transfer Protocol
[Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n
[Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n]
Request Method: POST
Request URI: http://31.7.62.214/fakeurl.htm
Request Version: HTTP/1.1
User-Agent: NetSupport Manager/1.3\n
Content-Type: application/x-www-form-urlencoded\n
Content-Length: 36\n
Host: 31.7.62.214\n
Connection: Keep-Alive\n
\n
[Full request URI: http://31.7.62.214/fakeurl.htm]
[HTTP request 7/114]
[Prev request in frame: 25291]
[Next request in frame: 28469]
File Data: 36 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded


dns.qry.name contains "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
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
157 4.270124 172.16.4.205 172.16.4.4 DNS 88 Standard query 0xd11d SOA Rotterdam-PC.mind-hammer.net
158 4.270363 172.16.4.4 172.16.4.205 DNS 166 Standard query response 0xd11d SOA Rotterdam-PC.mind-hammer.net SOA mind-hammer-dc.mind-hammer.net A 172.16.
159 4.272389 172.16.4.205 172.16.4.4 DNS 155 Dynamic update 0xab16 SOA mind-hammer.net CNAME AAAA A 172.16.4.205
160 4.273411 172.16.4.4 172.16.4.205 DNS 155 Dynamic update response 0xab16 SOA mind-hammer.net CNAME AAAA A 172.16.4.205
183 7.347611 172.16.4.205 172.16.4.4 DNS 90 Standard query 0x46ea A Mind-Hammer-DC.mind-hammer.net
184 7.347755 172.16.4.4 172.16.4.205 DNS 106 Standard query response 0x46ea A Mind-Hammer-DC.mind-hammer.net A 172.16.4.4
9776 39.086025 172.16.4.205 172.16.4.4 DNS 80 Standard query 0xce1d A wpad.mind-hammer.net
9777 39.086193 172.16.4.4 172.16.4.205 DNS 157 Standard query response 0xce1d No such name A wpad.mind-hammer.net SOA mind-hammer-dc.mind-hammer.net
Wireshark · Packet 9777 · network.pcap
Address: Dell_19:49:50 (a4:ba:db:19:49:50)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205
User Datagram Protocol, Src Port: 53, Dst Port: 61829
Domain Name System (response)
Transaction ID: 0xce1d
Flags: 0x8583 Standard query response, No such name
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
Authoritative nameservers
[Request In: 9776]
[Time: 0.000168000 seconds]
0000 00 59 07 b0 63 a4 a4 ba db 19 49 50 08 00 45 00 ·Y··c····· IP··E·
0010 00 8f 0d 33 00 00 80 11 cc 39 ac 10 04 04 ac 10 ···3···· ·9·····
0020 04 cd 00 35 f1 85 00 7b 3a ff ce 1d 85 83 00 01 ···5···{ :·····
0030 00 00 00 01 00 00 04 77 70 61 64 0b 6d 69 6e 64 ·····w pad·mind
0040 2d 68 61 6d 6d 65 72 03 6e 65 74 00 00 01 00 01 ·hammer· net·····
0050 0b 6d 69 6e 64 2d 68 61 6d 6d 65 72 03 6e 65 74 ·mind-ha mmer·net
0060 00 00 06 00 01 00 00 0e 10 00 32 0e 6d 69 6e 64 ·····2·mind
0070 2d 68 61 6d 6d 65 72 2d 64 63 c0 26 0a 68 6f 73 -hammer- dc·&·hos
0080 74 6d 61 73 74 65 72 c0 26 00 00 00 19 00 00 03 tmaster· &·····
0090 84 00 00 02 58 00 01 51 80 00 00 0e 10 ···· ····X··Q ····


dns
No. Time Source Destination Protocol Length Info
3027 30.019421 172.16.4.205 172.16.4.4 DNS 78 Standard query 0x8167 A ball.dardavies.com
3397 30.199058 172.16.4.4 172.16.4.205 DNS 94 Standard query response 0x8167 A ball.dardavies.com A 93.95.100.178
3402 30.201337 172.16.4.205 172.16.4.4 DNS 78 Standard query 0xc231 A ball.dardavies.com
3403 30.201533 172.16.4.4 172.16.4.205 DNS 94 Standard query response 0xc231 A ball.dardavies.com A 93.95.100.178
9776 39.086025 172.16.4.205 172.16.4.4 DNS 80 Standard query 0xce1d A wpad.mind-hammer.net
Wireshark · Packet 9776 · network.pcap
Domain Name System (query)
Transaction ID: 0xce1d
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
wpad.mind-hammer.net: type A, class IN
Name: wpad.mind-hammer.net
[Name Length: 20]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
[Response In: 9777]
0000 a4 ba db 19 49 50 00 59 07 b0 63 a4 08 00 45 00 ····IP·Y ··c···E·
0010 00 42 0f 98 00 00 80 11 ca 21 ac 10 04 cd ac 10 ·B····· ·!·····
0020 04 04 f1 85 00 35 00 2e d8 6e ce 1d 01 00 00 01 ·····5·. ·n·····
0030 00 00 00 00 00 00 04 77 70 61 64 0b 6d 69 6e 64 ·····w pad·mind
0040 2d 68 61 6d 6d 65 72 03 6e 65 74 00 00 01 00 01 -hammer· net·····


tls.handshake.type == 11
No. Time Source Destination Protocol Length Info
362 24.686835 50.112.34.20 172.16.4.205 TLSv1.2 758 Certificate, Server Key Exchange, Server Hello Done
371 24.874858 108.128.247.43 172.16.4.205 TLSv1.2 732 Certificate, Server Key Exchange, Server Hello Done
386 25.493592 52.11.30.237 172.16.4.205 TLSv1.2 1411 Certificate
748 27.921572 151.101.52.84 172.16.4.205 TLSv1.2 1336 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
813 28.019064 151.101.2.110 172.16.4.205 TLSv1.2 1411 Certificate
1525 28.880102 151.101.188.134 172.16.4.205 TLSv1.2 1154 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1768 29.131696 81.4.122.101 172.16.4.205 TLSv1.2 417 Certificate, Server Key Exchange, Server Hello Done
2411 29.594674 151.101.0.84 172.16.4.205 TLSv1.2 1336 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
6196 31.423193 93.95.100.178 172.16.4.205 TLSv1.2 1411 Certificate
6687 31.656540 93.95.100.178 172.16.4.205 TLSv1.2 1411 Certificate
Wireshark · Packet 2411 · network.pcap
Frame 2411: 1336 bytes on wire (10688 bits), 1336 bytes captured (10688 bits)
Ethernet II, Src: Cisco_e6:c4:77 (00:15:c6:e6:c4:77), Dst: LenovoEMCPro_b0:63:a4 (00:59:07:b0:63:a4)
Destination: LenovoEMCPro_b0:63:a4 (00:59:07:b0:63:a4)
Address: LenovoEMCPro_b0:63:a4 (00:59:07:b0:63:a4)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
Address: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 151.101.0.84, Dst: 172.16.4.205
Transmission Control Protocol, Src Port: 443, Dst Port: 49227, Seq: 4072, Ack: 518, Len: 1282
[4 Reassembled TCP Segments (4440 bytes): #2408(1242), #2409(1357), #2410(1357), #2411(484)]
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Transport Layer Security

Event Analizi

İlk eventde “ETPRO CURRENT_EVENTS SocEng/Gholish JS Web Inject Inbound SocGholish” adında bir sosyal mühendislik saldırısı gösteriliyor. SocGholish JS tabanlı kötü amaçlı yazılım bulunduran bir tehdit. Kaynak ve hedef IP’ ye zararlı JS kodları enjekte edilmeye çalışıyor.

80 portu kullanılmış muhtemelen HTTP üzeriden gerçekleşen bir saldırı. Hedef IP iç ağdaki makineyi temsil ediyor.

“ET POLICY Lets Encrypt Free SSL Cert Observed” Event’ de IDS, b,r Let’s Encrypt SSL sertifikası kullanan bağlantı tespit edilmiş. Let’s Encrypt yasal bir sertifikaya sahip olmasına rağmen saldırganlar SSL/TLS şifrelemesiyle kötü amaçlı trafiği gizlemek için kullanabilir. Bağlantılar 443 portu üzerinden (HTTPS) gerçekleşiyor şifrelenmiş trafik mevcut.

“ETPRO TROJAN Observed Malicious SSL Cert (SocGholish Redirect)” Event’ de yine SocGholish ile ilişkili zararlı bir SSL sertifikası tespit edilmiş. Saldırganlar kullanıcının dikkatini çekmeden zararlıları indirmesi için meşru görünen HTTPS bağlantılarını kullanabilir. Bu da SocGholish saldırısının bir parçası olarak şifrelenmiş bir yönlendirme yapıldığını gösteriyor.

“ET POLICY Data POST to an image file (gif) & gif file” Event’ lerde IDS, resim dosyasına (GIF) veri gönderildiğini (HTTP POST request) tespit etmiş.

Normalde GIF dosyalarına veri gönderilmez, ancak saldırganlar bazen kötü amaçlı yazılımları tespit edilmekten kaçınmak için gizli veri iletimi yapmak amacıyla resim dosyalarını kullanır. Data exfiltration tekniği olabilir.

“ETPRO CURRENT_EVENTS JS.SocGholish POST Request” SocGholish zararlı yazılımı iç ağdaki makineden uzaktaki bir sunucuya HTTP POST isteği yapıyor. Bu zararlının indirildiğini veya saldırganların kontrolündeki bir C2 (Command and Control) sunucusuna veri gönderildiğini gösterir. Bu enfeksiyonun gerçekleştiğini ve makinenin muhtemelen ele geçirildiğini gösteren kritik bir uyarıdır.

“ET POLICY HTTP Request on Unusual Port Possibly Hostile” Event’ de HTTP trafiği genellikle 80 ve 443 portlarında gerçekleşirken, burada farklı bir port kullanılmış. Saldırganlar, tespit edilmemek için alışılmadık portlardan veri göndererek güvenlik sistemlerini atlatmaya çalışabilir. Bu, zararlı trafiğin veya veri sızıntısının işareti olabilir.

“ETPRO POLICY NetSupport Remote Admin Checkin & Response” NetSupport Manager, bir uzaktan yönetim yazılımıdır. Yasal bir yazılım olmasına rağmen, siber suçlular tarafından sistemleri ele geçirmek için RAT olarak kötüye kullanılabilir. Bu aletler. 172.16.4.205 IP’sine NetSupport Manager’ın bulaşmış olabileceğini gösteriyor. Bu sistemin saldırganlar tarafından kontrol ediliyor olabilir.