

The logo of Altay University is a shield-shaped emblem. Inside the shield is a stylized, circular floral or sunburst-like pattern. The text "Pcap Analizi" is centered over this pattern.

Pcap Analizi

Hazırlayan: Saliha Polat

Tarih: 15.03.2025

A L T A Y

İçindekiler

Olay/Vaka Özeti	3
Detaylı Analiz	4
Tehlike Göstergeleri (IOC'ler)	4
Bölüm başlığını yazın (düzey 1)	4
Wireshark' da Elde Edilen Bazı Veriler	5
Event Analizi	8

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 Adresi: 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

No.	Time	Source	Destination	Protocol	Length	Info
514	27.481991	172.16.4.205	54.230.89.184	HTTP	347	GET /app/v1/site.js HTTP/1.1
651	27.727059	172.16.4.205	166.62.111.64	HTTP	412	GET /wp-content/plugins/ginger/addon/analytics/gingeranalytics.min.js?ver=5.2.2 HTTP/1.1
662	27.739997	172.16.4.205	166.62.111.64	HTTP	405	GET /wp-content/plugins/ginger/front/js/cookies-enabler.min.js?ver=5.2.2 HTTP/1.1
669	27.736553	172.16.4.205	166.62.111.64	HTTP	383	GET /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp HTTP/1.1
686	27.798429	172.16.4.205	166.62.111.64	HTTP	391	GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1
692	27.811447	172.16.4.205	166.62.111.64	HTTP	398	GET /wp-content/plugins/simple-social-icons/svgxuse.js?ver=1.1.21 HTTP/1.1
736	27.908555	172.16.4.205	166.62.111.64	HTTP	400	GET /wp-content/themes/hello200arling202.0/js/global.js?ver=1.0.0 HTTP/1.1
741	27.912184	172.16.4.205	166.62.111.64	HTTP	398	GET /wp-content/themes/hello200arling202.0/js/home.js?ver=1.0.0 HTTP/1.1
743	27.913890	172.16.4.205	166.62.111.64	HTTP	386	GET /wp-includes/js/wp-emoji-release.min.js?ver=5.2.2 HTTP/1.1
768	27.937515	172.16.4.205	166.62.111.64	HTTP	416	GET /wp-content/plugins/disqus-comment-system/public/js/comment_count.js?ver=3.0.16 HTTP/1.1
804	27.981264	172.16.4.205	166.62.111.64	HTTP	495	GET /wp-content/plugins/instagram-feed/js/sb-instagram.min.js?ver=1.10.1 HTTP/1.1
837	28.052753	172.16.4.205	166.62.111.64	HTTP	418	GET /wp-content/plugins/jquery-pin-it-button-for-images/js/pinbf1.client.js?ver=2.3.4 HTTP/1.1
839	28.060880	172.16.4.205	166.62.111.64	HTTP	382	GET /wp-includes/js/imagesloaded.min.js?ver=3.2.0 HTTP/1.1
842	28.088254	172.16.4.205	166.62.111.64	HTTP	382	GET /wp-includes/js/imagesloaded.min.js?ver=3.2.0 HTTP/1.1
850	28.092736	172.16.4.205	166.62.111.64	HTTP	377	GET /wp-includes/js/masonry.min.js?ver=3.3.2 HTTP/1.1
851	28.093643	172.16.4.205	166.62.111.64	HTTP	392	GET /wp-includes/js/jquery/jquery.masonry.min.js?ver=3.1.2b HTTP/1.1
908	28.119789	172.16.4.205	166.62.111.64	HTTP	406	GET /wp-content/plugins/social-warfare/assets/js/script.min.js?ver=3.42 HTTP/1.1
927	28.180478	172.16.4.205	166.62.111.64	HTTP	393	GET /wp-content/plugins/jetpack/modules/wproho.js?ver=5.2.2 HTTP/1.1
932	28.194878	172.16.4.205	166.62.111.64	HTTP	397	GET /wp-content/themes/hello200arling202.0/js/nav.js?ver=5.2.2 HTTP/1.1
937	28.241899	172.16.4.205	166.62.111.64	HTTP	418	GET /wp-content/themes/hello200arling202.0/js/jquery.scrollTo.min.js?ver=1.4.5-beta HTTP/1.1
978	28.264998	172.16.4.205	166.62.111.64	HTTP	417	GET /wp-content/themes/hello200arling202.0/js/jquery.localScroll.min.js?ver=1.2.8b HTTP/1.1
1020	28.281075	172.16.4.205	166.62.111.64	HTTP	400	GET /wp-content/themes/hello200arling202.0/js/fadeup.js?ver=1.0.0 HTTP/1.1
1025	28.286422	172.16.4.205	166.62.111.64	HTTP	416	GET /wp-content/themes/hello200arling202.0/js/jquery.matchHeight.min.js?ver=1.0.0 HTTP/1.1
1038	28.306230	172.16.4.205	166.62.111.64	HTTP	410	GET /wp-content/themes/hello200arling202.0/js/matchHeight-init.js?ver=1.0.0 HTTP/1.1
1032	28.320615	172.16.4.205	166.62.111.64	HTTP	410	GET /wp-content/plugins/genesis-responsive-slider/js/jquery.flexSlider.js?ver=0.9.5 HTTP/1.1
1039	28.361521	172.16.4.205	166.62.111.64	HTTP	378	GET /wp-includes/js/wp-embed.min.js?ver=5.2.2 HTTP/1.1
1090	28.438845	172.16.4.205	166.62.111.64	HTTP	412	GET /wp-content/plugins/soliloquy-lite/assets/js/min/soliloquy-min.js?ver=2.5.2 HTTP/1.1
1506	28.829569	172.16.4.205	216.58.193.208	HTTP	380	GET /gcm.js?id=gcm-PBw793&l=daataLayerCBias HTTP/1.1
2127	28.439446	172.16.4.205	54.230.89.184	HTTP	412	POST http://31.7.62.214/fakeurl.htm HTTP/1.1
2129	29.532499	166.62.111.64	172.16.4.205	(PNG)	634	HTTP/1.1 200 OK (PNG)
2422	29.638082	172.16.4.205	54.230.89.184	HTTP	351	GET /app/v1/embedded.js HTTP/1.1
2678	29.779828	172.16.4.205	54.230.89.184	HTTP	350	GET /app/v1/sidebar.js HTTP/1.1
6185	31.428673	166.62.111.64	172.16.4.205	HTTP	184	HTTP/1.1 200 OK (JPEG JFIF image)

No.	Time	Source	Destination	Protocol	Length	Info
20522	291.780889	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	292.039483	172.16.4.205	172.16.4.205	HTTP	268	HTTP/1.1 200 OK (application/x-www-form-urlencoded)
20571	292.050481	172.16.4.205	31.7.62.214	HTTP	404	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	292.594795	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)
22808	292.704931	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)
28060	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)
28409	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)
28411	533.506476	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 20522 - network.pcap

Frame 20522: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on Ethernet II, Src: LenovoEMCPPro_b0:63:a4 (08:50:07:b8:63:a4), Dst: Cisco_e6:c4:77 (00:15:c0: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

User-Agent: NetSupport Manager/1.3.0

Content-Type: application/x-www-form-urlencoded

Content-Length: 22

Host: 31.7.62.214

Connection: Keep-Alive

[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"

No.	Time	Source	Destination	Protocol	Length	Info
514	27.481991	172.16.4.205	54.230.89.184	HTTP	347	GET /app/v1/site.js HTTP/1.1
651	27.727059	172.16.4.205	166.62.111.64	HTTP	412	GET /wp-content/plugins/ginger/addon/analytics/gingeranalytics.min.js?ver=5.2.2 HTTP/1.1
662	27.739997	172.16.4.205	166.62.111.64	HTTP	405	GET /wp-content/plugins/ginger/front/js/cookies-enabler.min.js?ver=5.2.2 HTTP/1.1
669	27.736553	172.16.4.205	166.62.111.64	HTTP	383	GET /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp HTTP/1.1
686	27.798429	172.16.4.205	166.62.111.64	HTTP	391	GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1
692	27.811447	172.16.4.205	166.62.111.64	HTTP	398	GET /wp-content/plugins/simple-social-icons/svgxuse.js?ver=1.1.21 HTTP/1.1
736	27.908555	172.16.4.205	166.62.111.64	HTTP	400	GET /wp-content/themes/hello200arling202.0/js/global.js?ver=1.0.0 HTTP/1.1
741	27.912184	172.16.4.205	166.62.111.64	HTTP	398	GET /wp-content/themes/hello200arling202.0/js/home.js?ver=1.0.0 HTTP/1.1
743	27.913890	172.16.4.205	166.62.111.64	HTTP	386	GET /wp-includes/js/wp-emoji-release.min.js?ver=5.2.2 HTTP/1.1
768	27.937515	172.16.4.205	166.62.111.64	HTTP	416	GET /wp-content/plugins/disqus-comment-system/public/js/comment_count.js?ver=3.0.16 HTTP/1.1
804	27.981264	172.16.4.205	166.62.111.64	HTTP	495	GET /wp-content/plugins/instagram-feed/js/sb-instagram.min.js?ver=1.10.1 HTTP/1.1
837	28.052753	172.16.4.205	166.62.111.64	HTTP	418	GET /wp-content/plugins/jquery-pin-it-button-for-images/js/pinbf1.client.js?ver=2.3.4 HTTP/1.1
839	28.060880	172.16.4.205	166.62.111.64	HTTP	405	GET /wp-content/plugins/social-warfare/assets/js/script.min.js?ver=3.5.4 HTTP/1.1
842	28.088254	172.16.4.205	166.62.111.64	HTTP	382	GET /wp-includes/js/imagesloaded.min.js?ver=3.2.0 HTTP/1.1
850	28.092736	172.16.4.205	166.62.111.64	HTTP	377	GET /wp-includes/js/masonry.min.js?ver=3.3.2 HTTP/1.1

Wireshark - Packet 2422 - network.pcap

Source: LenovoEMCPPro_b0:63:a4 (08:50:07:b8:63:a4)

Address: LenovoEMCPPro_b0:63:a4 (08:50:07:b8:63:a4)

Type: IPv4 (0x0800)

.....0..... = LG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

Internet Protocol Version 4, Src: 172.16.4.205, Dst: 54.230.89.184

Transmission Control Protocol, Src Port: 49207, Dst Port: 80, Seq: 605, Ack: 9780, Len: 297

Hypertext Transfer Protocol

GET /app/v1/embedded.js HTTP/1.1

[Expert Info (Content/Sequence): GET /app/v1/embedded.js HTTP/1.1]

Request Method: GET

Request URI: /app/v1/embedded.js

Request Version: HTTP/1.1

Host: a.mallaunch.co

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: */*

Accept-Language: en-US,en;q=0.3

Accept-Encoding: gzip, deflate

DNT: 1

Connection: keep-alive

Referer: http://mysocalledchaos.com/

[Full request URI: http://a.mallaunch.co/app/v1/embedded.js]

[HTTP request 3/3]

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	60	49255 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
29520	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	291.790869	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) on Ethernet II, Src: lenovoEMCPro_b0:63:a4 (08:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (08:15: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

[Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeurl.htm HTTP/1.1]

Request Method: POST

Request URI: http://31.7.62.214/fakeurl.htm

Request Version: HTTP/1.1

User-Agent: NetSupport Manager/1.3

Content-Type: application/x-www-form-urlencoded

Content-Length: 22

Host: 31.7.62.214

Connection: Keep-Alive

[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"

Key: CMD

Value: POLL\nINFO=1\nACK=1

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)
9895	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	288.299847	172.16.4.205	185.243.115.84	HTTP	326	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
20522	291.790869	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	308.081407	172.16.4.205	185.243.115.84	HTTP	496	POST /empty.gif?ss&ss2img 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	488.203847	172.16.4.205	185.243.115.84	HTTP	1360	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)

Wireshark - Packet 28458 - network.pcap

Frame 28458: 1360 bytes on wire (10880 bits), 1360 bytes captured (10880 bits) on Ethernet II, Src: lenovoEMCPro_b0:63:a4 (08:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (08:15:c6:e6:c4:77)

Internet Protocol Version 4, Src: 172.16.4.205, Dst: 185.243.115.84

Transmission Control Protocol, Src Port: 49249, Dst Port: 80, Seq: 7285333, 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(1357)

Hypertext Transfer Protocol

POST /empty.gif?ss&ss2img HTTP/1.1

[Expert Info (Chat/Sequence): POST /empty.gif?ss&ss2img HTTP/1.1]

Request Method: POST

Request URI: http://31.7.62.214/fakeurl.htm

Request Version: HTTP/1.1

Accept: */*

Accept-Language: en-US

Accept-Charset: utf-8

tcp.dstport == 443 and http

No.	Time	Source	Destination	Protocol	Length	Info
20522	291.790869	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)
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

Frame 28066: 36 bytes on wire (288 bits), 36 bytes captured (288 bits) on Ethernet II, Src: lenovoEMCPro_b0:63:a4 (08:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (08:15:c6:e6:c4:77)

Bytes sent since last PSF 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

[Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeurl.htm HTTP/1.1]

Request Method: POST

Request URI: http://31.7.62.214/fakeurl.htm

Request Version: 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

[Full request URI: http://31.7.62.214/fakeurl.htm]

[HTTP request 7/114]

[Prev request in frame: 25291]

[Next request in frame: 28460]

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 0xf2b A wpad.mind-hammer.net
136	2.326002	172.16.4.4	172.16.4.205	DNS	157	Standard query response 0xf2b 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 0xc0df A isatap.mind-hammer.net
139	2.359604	172.16.4.4	172.16.4.205	DNS	159	Standard query response 0xc0df 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 0xd1d SOA Rotterdam-PC.mind-hammer.net
158	4.270363	172.16.4.4	172.16.4.205	DNS	166	Standard query response 0xd1d SOA Rotterdam-PC.mind-hammer.net SOA mind-hammer-dc.mind-hammer.net A 172.16.4.205
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
197	39.086625	172.16.4.205	172.16.4.4	DNS	80	Standard query 0xc0d A wpad.mind-hammer.net
197	39.086193	172.16.4.4	172.16.4.205	DNS	157	Standard query response 0xc0d 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: 0xc0d
 Flags: 0x8583 Standard query response, No such name
 Questions: 1
 Answer RRs: 0
 Authority RRs: 1
 Additional RRs: 0
 Queries
 Authoritative nameservers
 [Time: 0.000109000 seconds]

0000 00 59 07 b0 63 a4 a4 ba db 19 49 50 08 00 45 00 ...Y.C...IP.E
 0018 00 8f 0d 33 08 00 00 11 cc 39 ac 10 04 04 ac 10 ...3...9....
 0020 04 cd 00 35 f1 85 08 7b 3a ff 0e 1d 85 83 08 01 ...5...n....
 0030 00 00 00 01 00 00 04 77 70 61 64 00 00 00 00wpad.mind
 0040 2d 08 01 0d 00 05 72 03 0e 05 74 00 00 01 00 01hammer.net....
 0050 00 0d 09 0e 04 2d 08 01 0d 00 05 72 03 0e 05 74mind-hammer.net
 0060 00 00 00 00 01 00 00 0e 10 00 32 0e 0d 09 0e 042.mind
 0070 2d 08 01 0d 00 05 72 03 04 03 00 20 0a 08 0f 73hammer-dc&hds
 0080 74 0d 01 73 74 05 72 03 20 00 00 00 19 00 00 88hammer-dc&hds
 0090 84 00 00 02 58 00 01 51 80 00 00 0e 18X-Q.....

dns

No.	Time	Source	Destination	Protocol	Length	Info
3827	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	30.201327	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	39.086625	172.16.4.205	172.16.4.4	DNS	80	Standard query 0xc0d A wpad.mind-hammer.net

Wireshark - Packet 9776 - network.pcap

Domain Name System (query)
 Transaction ID: 0xc0d
 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 08 00 59 07 b0 63 a4 08 00 45 00 ...IP-Y...C...E
 0010 00 42 0f 98 00 00 00 11 ca 21 ac 10 04 cd ac 10 ...B.....f.....
 0020 04 04 f1 85 00 35 00 2e d8 0e ce 1d 01 00 00 015...n....
 0030 00 00 00 00 00 00 04 77 70 61 64 00 00 00 00wpad.mind
 0040 2d 08 01 0d 00 05 72 03 0e 05 74 00 00 01 00 01hammer.net....

tls.handshake.type == 11

No.	Time	Source	Destination	Protocol	Length	Info
362	24.086835	50.112.34.20	172.16.4.205	TLSv1.2	758	Certificate, Server Key Exchange, Server Hello Done
371	24.074858	100.128.247.43	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	1330	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
2118	30.021042	151.101.80.7	172.16.4.205	TLSv1.2	1330	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	31.050540	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: 151.101.8.85, 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

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 üzerinden 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.