



# Traffic Analysis Report 2023/2024

**Réalisé par : oussama binike**

**Encadré par : amine raghip**



## basic static analysis

Victim's ip address: **172.16.1.137**

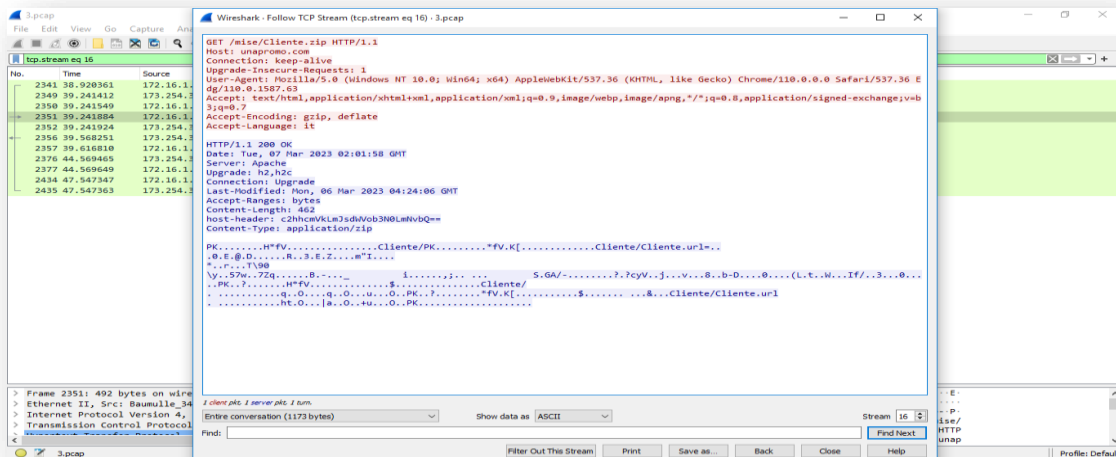
Victim's mac address: **00:02:fb:34:b4:fa**

host name : **DESKTOP-3GJL3PV\$**

user account name: **sherita.kolb**

## scenario

The user, identified with IP address **172.16.1.137** on '**Tue, Mar 07, 2023 at 02:01:58 GMT**', began downloading a potentially malicious zip file '**Client.zip**' from the host located at '**unapromo.com**'





The compressed file is infected with malware

hash of the malicious file:

33db5b2a2cc592fd10c65ba38396e4c7574ad78e786d78e8a3acdc93a90c3209

The screenshot displays the VirusTotal web interface for a file analysis. The file name is 'Cliente.zip' with a size of 462 B. The hash is 33db5b2a2cc592fd10c65ba38396e4c7574ad78e786d78e8a3acdc93a90c3209. The interface shows a '26 / 63' score, indicating that 26 security vendors have flagged the file as malicious. The file is categorized as a 'zip' and has several tags: 'cve-2023-32046', 'exploit', 'sets-process-name', and 'detect-debug-environment'. The 'DETECTION' tab is active, showing a table of security vendors' analysis results.

Security vendors' analysis	Do you want to automate checks?		
AhnLab-V3	Trojan/LNK.Agent.SC186819	Antiy-AVL	Trojan/JS.Ursnif
Arcabit	Trojan.Agent.GDJW	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	BitDefender	Trojan.Agent.GDJW



Following the aforementioned activities, the victim system exhibited a pattern of behavior characterized by sending **GET requests** to random sites within the specified path **"/drew/..."**.

No.	Time	Source	Destination	Protocol	Length	Info
2351	39.241884	172.16.1.137	173.254.32.85	HTTP	492	GET /mise/Cliente.zip HTTP/1.1
3597	353.503095	172.16.1.137	62.173.140.103	HTTP	579	GET /drew/Q0EvhskDMeV_2B/hlZqNkHPY3pA7HNxtL/9pXV5RDXP/IncHG7Vufpd12hEx13M2/zb35UbdKsAKR20Sh...
3819	354.599691	172.16.1.137	62.173.140.103	HTTP	608	GET /drew/SP5U1P1seVnmC1/XxgojgHPnhrehjymv5j9h/KykwQdZntu0_2B_2FuTGy0Xej8v6D_2/Ff5cKDM4tUcH8...
4107	355.306573	172.16.1.137	62.173.140.103	HTTP	603	GET /drew/XXBCjkZMDTxLE17NN6B18N/sewChwVn3i5Mu/3Vj7fKXx/pPn5qADL_2FuoPCNCu6CCw/355onuVERC/mB...
4155	361.242641	172.16.1.137	62.173.138.138	HTTP	568	GET /drew/uyoXjOLPocHIEKQlytVakB/N_2B3o481_/2888gjjy1qo0bubKw/vIwIAJ4RuKNI/cCn13QTf8y/h_2B...
4171	361.923498	172.16.1.137	62.173.149.243	HTTP	232	GET /stilak32.rar HTTP/1.1
4611	363.282227	172.16.1.137	62.173.149.243	HTTP	232	GET /stilak64.rar HTTP/1.1
5447	374.430460	172.16.1.137	62.173.138.138	HTTP	1004	POST /drew/D1S1_2B5IFF7K/tUNoAF33/ohKhuYqRxx0le5whBjCtVbXY/zRDJAof4m4/5X0H5MhV3e8nNjcvM/x39X4P...
5500	381.107934	172.16.1.137	62.173.138.138	HTTP	680	POST /drew/cZceFW2s05ezxH/EUe6ceZRBkYCKbiW3Rxd/0ravm1DV14ahEAnB/gQB05qnn1cW8Xh/PAhUAzH0mz5n...
5645	421.025943	172.16.1.137	62.173.138.138	HTTP	663	GET /drew/at0eNEowDE_2F50b/NFBz3bCzAt61/AVGj299DNHP/XubanH9r19L161/3K0umHazY3Iac2W0XzoB/714...
5649	421.513393	172.16.1.137	62.173.149.243	HTTP	230	GET /cook32.rar HTTP/1.1
6042	422.864989	172.16.1.137	62.173.149.243	HTTP	230	GET /cook64.rar HTTP/1.1
6797	434.013480	172.16.1.137	62.173.138.138	HTTP	741	POST /drew/xxk6_2Bp25fh1Nwx0uet5/7AEfxXLwyGggfGT/8Q1KS1_2B0p95r4/QZqE1k_2Fm23u1W4we/LE13tvd...
6820	461.037578	172.16.1.137	62.173.138.138	HTTP	667	GET /drew/D01xa36NCdvBsA37/DWVhNhrw5Vlgzu/PgqHIGepHgV7gau1H_2FqKQ0_2B/rhV9Lpfes_2B0a1hr7sp/...
6831	541.266100	172.16.1.137	62.173.140.94	HTTP	585	GET /drew/VTjgncxGKO/Fb_2B36blv3YyBgEQ/yox7VjUMRU06/U362tcvC05Q/19K1tqMzCW031/drv5kpv8Bj09N...
6874	601.259865	172.16.1.137	31.41.44.60	HTTP	591	GET /drew/qgN9mk92QT/WaZy2IzgFwv_2B/BQ048Y4QhKoe_2B_2FF7/xz26FF_2F_2F2_2B/-G1i23ut8zh21R/X...
6887	670.251327	172.16.1.137	46.8.19.233	HTTP	601	GET /drew/au1cHufv4xgf17v8uQXiw/81LQHCChQVqHEq/rQ59UIPR/g57pgcSV3K_2F6wQubUVfy/K6_2FFFlup_2B...
6902	730.030607	172.16.1.137	46.8.19.233	HTTP	557	GET /drew/3bcV28UCDrEw_2FfnbUN/USk39jEPxFRayU19/fE72tvcL31DM8X1/B5LoJ2r1ckd1E1ZgQh/shgZg7Hq...
6915	790.217728	172.16.1.137	5.44.45.201	HTTP	585	GET /drew/TxwLwC4UFhMgZXRkxkt/VS1VI1dPLA53cizTEdL/n3qNAGUXUS1s1TerY0XFLD/Pa89_2Fx8ZCFX/BR_2B...
6930	850.266351	172.16.1.137	89.116.236.41	HTTP	598	GET /drew/3PqkF_2F_2BrrbhWPOTs/OwphZ2H2tkbojEjTb_2B_2FzLltIX5K7Ho/6x5_2F2F/aJLFZY7_2Fn4tbbJc...
6941	910.288177	172.16.1.137	62.173.140.76	HTTP	564	GET /drew/dofqF3DQdike/5dx_2FHCRmV/CewV15sc9TEIo_2FFHnhDsAqmkbEbvKhjH/VH356xlt9ATL76AF/e13p...
6988	970.280802	172.16.1.137	31.41.44.49	HTTP	568	GET /drew/LW7Yj7P8/au1Iw13vmot8F5NaoVH14_2Fol2M2428j/vm5nv18muEr0nHQ5Z/1Xvc1YB_2B_2F2F0prnd...
6999	995.209186	172.16.1.137	23.77.213.161	HTTP	281	GET / HTTP/1.1
7008	995.756243	172.16.1.137	8.253.198.120	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/pinrulesst1.cab?c1f6d5dae11c1e4c HTTP/1.1
7051	1030.304592	172.16.1.137	46.8.19.86	HTTP	583	GET /drew/87K0l3wsw64/XzU19sN5W8mE3o/Ry4an43vksM8Ymx60M605/PQtzODDyH1G1TtY/8vIHgHE3JhKHPdL/g...
7095	1090.090298	172.16.1.137	46.8.19.86	HTTP	589	GET /drew/tXyhbQe5_2B/2y51I6NGQZ5/7y1Mec2Ve_2B_2FLQm5pa0gKbtqj6h6f9b/IyF57o6UoFe5yNQV/YNzT...
9220	1299.164731	172.16.1.137	62.173.140.94	HTTP	585	GET /drew/uxz9_2FZjFA21sXSRhF/dn7GeVjur_2BkH0tFzjm/_2BdLWdpjVgZ/vuR1th07/GJ2H7UENP1U7ewh...
9359	1358.961686	172.16.1.137	62.173.140.94	HTTP	583	GET /drew/Gs60OGTSTNqjShjOSbvjN/e3N28at10gtuH/sNXR8jwc/NwGaI8hrP1PV1wQqtzeYul9/tKq8UdQZG5/7t...
9379	1419.205966	172.16.1.137	31.41.44.60	HTTP	566	GET /drew/1SHH01cltx6/Z8Dn0GFViz4L/FOC1M6PodyP1wc8CIUDUA/1Pz6vF1hNmrvM2_2FFI1ha9t1y0H_2B/e...



Subsequent to the aforementioned actions, the victim system proceeded to download an additional compressed file identified as "**stilak32.rar**," which is potentially malicious

```
Wireshark · Follow TCP Stream (tcp.stream eq 30) · 3.pcap

GET /stilak32.rar HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Host: 62.173.149.243
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 07 Mar 2023 02:07:20 GMT
Content-Type: application/x-rar-compressed
Content-Length: 335512
Last-Modified: Thu, 09 Feb 2023 21:25:34 GMT
Connection: keep-alive
ETag: "63e564ce-51e98"
Accept-Ranges: bytes

...I.d.>9S..?J..$.q..t9.....N.}..!T$.2.~....d.)...-4.~&...gzy.....2...e4.....s7...wr.=..N.....?CH'y...._t=6.]~F#.O..
y.....l[.....Is...ehHaiI.8.E....E.|..1..^..TC.!...@n.o....r..a;...>...a..l..E.7..]
...8.....a.....v1~..7.{.C.U_z...|i.....'....5XH..
...YA.....#G.K.<.....>.....<....C..y1.....w.....C.....G.Q...95..].G(.\.E...S"...$$E...rd.Bj.#fj...jJB...'\d...
...H.M..?.(y...L.@jg.#.Q:.....P.....x...".S..2.....(.4.G5.w.xw..._.....y_Z..Q...0kq..y.j
P.....Z...P..L.O...U.N..7.O...'.~X.&P...'.K...)y..2"IM.z...B\O).q...o.q.*.....<7.4.S.F..4...z...[...b..T...q
g...~..[.G...Q%....2..D...S.....V1[{.d!...^~..
...':.....}.#.)..
...Z7...y...~.#.7.Q.....l.S@....?....!.=n8pb.i..KW...FB]R.6...t...-0c+.....].$d..M..)5D.....bz.>..d`1...f'
.....`V$F.HI\..v1...._t...E.M..Z$LnG.....=..
#
...Z..f....>....q.....{.=fFL.....R\..I..:}*.....#..J..&.....>^.{...=.1h6..}l.F.9..%....&=O.d....L....I....8...K....
....
0...c.....UM.!/.6..5i...|.\.e.....P.^..N.....k...F.....n..rU.^3..X.#
s..}.V.+..V@..."r.V.*F...#%.x.....o..v.r...h.V...M#>2.6y.a..7...p\...[e...k
^.._Q.....U(.
.S....[#.hD/.....{Y...E.Y..j.VV..\...D.."YS..Op.N.4.&..M..U'[E.....^x@.6.k...9iiV%....ro...x.B.u..-5...n..K.....
.i_j...b.>o..({q.S..JJ..1.@Wgh..#.cz..X...2.z..t..=fKt.V..+...u..F.....KZKP...J.J....X#..$S.P...C...-.\_%..
.g..
7...(.xw.+j...E.|t.....k^o.k...)d.....02z...c.Z.....Or
..6.2*..&.s.Y.J;2!M..P.9g.....F...:H.y..iIfi.h.
0.~...../).J.c.<+.A.2&+..TD#3=.e.+.%..({b.._8...Y...+;..C.t1...@x..`h...Uq|...T....u}..%.X#A.....+Yy...h1aH.R...
```



The compressed file is infected with malware

hash of the malicious file:

**c15aedd520ea6c57768c2c00abe19bef9842d55582dd705ea56bc260b6773284**

10 / 59

10 security vendors and no sandboxes flagged this file as malicious

c15aedd520ea6c57768c2c00abe19bef9842d55582dd705ea56bc260b6773284

Size: 459.15 KB | Last Analysis Date: 2 months ago

Community Score: 10 / 59

DETECTION DETAILS COMMUNITY 3

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan. Threat categories: trojan

Security vendors' analysis

Vendor	Detection	Threat Category
ALYac	Trojan.GenericKD.66029140	Anti-AVL
Arcabit	Trojan.GenericKD.66029140	BitDefender
Emsisoft	Trojan.GenericKD.66029140 (B)	eScan

Do you want to automate checks?

Following the described activities, the victim system engaged in sending **POST requests** to malicious website with the IP address **62.173.138.138** at **Tue, 07 Mar 2023 02:07:20 GMT**.

```
POST /drew/D1S1_2B5IFF7x/tlUnof33/ohkhuVgRo0le5whBjctVbXV/zRDjaOf4m4/SXhSHHV3eBnIjcVm/xJ9X4P02yhnn/k3lncOQ9TbL/s78_2FAP_2B_2F/1jHwJ7CSsplt2w_2FII14/oaYjUA8nknKAHQTC/1YbU6Yd66oa5Zmg/0vvpRj
xCHuVAVdQy/1m0VsgJKL/yvQOZm_2Bm3Gste9Z7/qFDC6THM3M6FK2qI4z/Y8jRuK_2B_2B8rdim647_2/BGsljia_2Fah7/2bQblwasf/oaFhftfveU5FFNEAvgf2bVW/KkPGZU.bmp HTTP/1.1
Content-Type: multipart/form-data; boundary=106571479542639481391
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Host: 62.173.138.138
Content-Length: 369
Connection: Keep-Alive
Cache-Control: no-cache

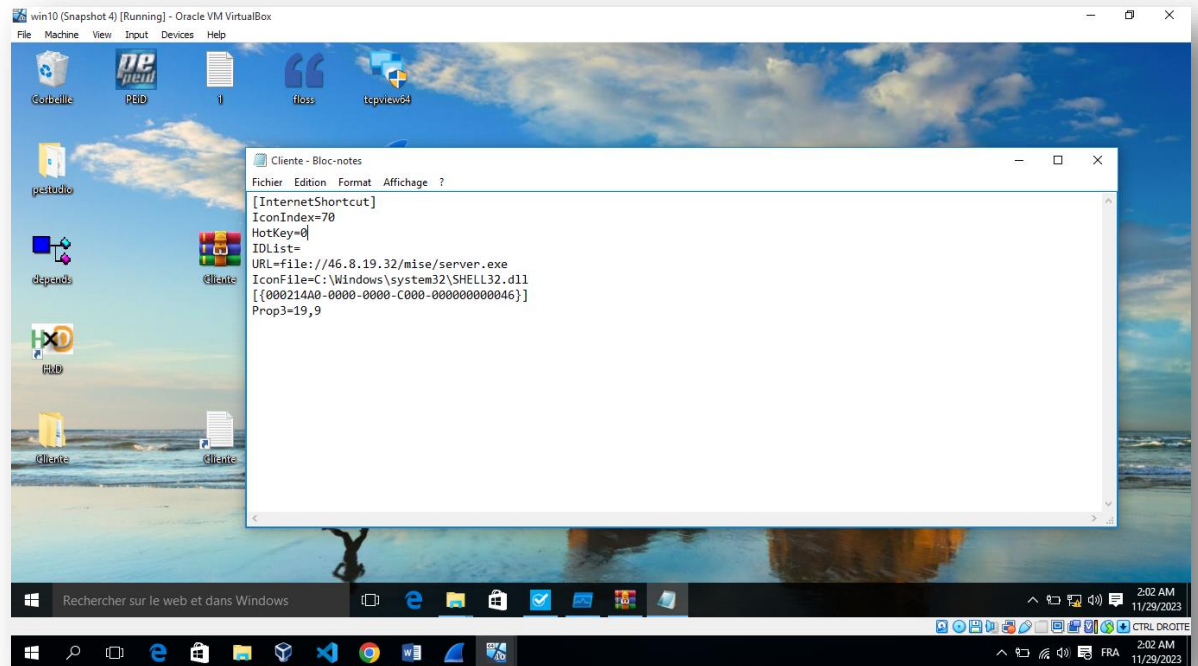
--106571479542639481391
Content-Disposition: form-data; name="upload_file"; filename="FA1D.bin"

..(I
..R+.....0j:~94,5X
..w.k...%.R...T.T*.qw.i'...^,B.4.Y .@H. SL(.z.f....J...0..h@.h).%......S)...FNM.z.t..S.....P.Ya.J...h..$. p...eE.4.<...t..6.....Y.D.PW.....j...m.<.....)).S2...)F.G...J.e.....
W.-.....\G.....I.....Z[q?...7.
--106571479542639481391--
```



## Static analysis of 'Client.zip'

- **Malware creation time:** 2023-03-06 10:26:08 UTC
- **Last Analysis :** 2023-11-17 11:35:09 UTC
- **malwer's name:** Cliente.zip , output.230371700.txt , Cliente , Cliente(1).zip , Client.zip
- **straings and flous output:** Cliente/Cliente.url, Cliente/Cliente.url=, Cliente/PK





## ➤ Process information: c:\Windows\system32\SHELL32.DLL

Process Monitor - Sysinternals.com

File Edit Event Filter Tools Options Help

Time Process Name PID Operation Path Result Detail

Time	Process Name	PID	Operation	Path	Result	Detail
45.2	WinRAR.exe	4958	Load Image	C:\Windows\System32\shell32.dll	SUCCESS	Image Base: 0x7fc80000, Image Size: 0x1525000
45.2	WinRAR.exe	4958	CreateFile	C:\Windows\System32\shell32.dll	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode:...
45.2	WinRAR.exe	4958	QueryBasicInfo	C:\Windows\System32\shell32.dll	SUCCESS	CreationTime: 7/10/2015 11:00:18 AM, LastAccessTime: 7/10/2015 11:00:18 AM, LastWriteTime: 7/10/2015 11:00:18 AM, Change...
45.2	WinRAR.exe	4958	CloseFile	C:\Windows\System32\shell32.dll	SUCCESS	
45.3	WinRAR.exe	4958	QueryNameInfo	C:\Windows\System32\shell32.dll	SUCCESS	Name: \Windows\System32\shell32.dll
52.5	WinRAR.exe	5864	QueryNameInfo	C:\Windows\System32\shell32.dll	SUCCESS	Name: \Windows\System32\shell32.dll
53.0	WinRAR.exe	4196	Load Image	C:\Windows\System32\shell32.dll	SUCCESS	Image Base: 0x7fc80000, Image Size: 0x1525000
53.0	WinRAR.exe	4196	CreateFile	C:\Windows\System32\shell32.dll	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode:...
53.0	WinRAR.exe	4196	QueryBasicInfo	C:\Windows\System32\shell32.dll	SUCCESS	CreationTime: 7/10/2015 11:00:18 AM, LastAccessTime: 7/10/2015 11:00:18 AM, LastWriteTime: 7/10/2015 11:00:18 AM, Change...
53.0	WinRAR.exe	4196	CloseFile	C:\Windows\System32\shell32.dll	SUCCESS	

Process Monitor Filter

Display entries matching these conditions:

Architecture is then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process N...	contains	winrar	Include
<input checked="" type="checkbox"/> Path	contains	C:\Windows\sys...	Include
<input checked="" type="checkbox"/> Process N...	is	Process.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Process.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Autounst.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Process64.exe	Exclude
<input checked="" type="checkbox"/> Process N...	is	Process64.exe	Exclude

OK Cancel Apply

Showing 10 of 1,069,944 events (0.00093%) Backed by virtual memory

Rechercher sur le web et dans Windows

2:11 AM 11/29/2023

## ➤ HTTP requests:

Initiating HTTP Requests to the Specified URL: <http://46.8.19.32:445>

Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Address: 46.8.19.32

No.	Time	Source	Destination	Protocol	Length	Info
3566	272.183643	46.8.19.32	172.16.1.137	TCP	54	445 → 59376 [ACK] Seq=406610 Ack=25003 Win=64240 Len=0
3567	272.399703	46.8.19.32	172.16.1.137	SMTP	131	Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3568	272.405250	172.16.1.137	46.8.19.32	SMTP	250	Create Request File: ur\mon.dll
3569	272.405301	46.8.19.32	172.16.1.137	TCP	54	445 → 59376 [ACK] Seq=406687 Ack=25199 Win=64240 Len=0
3570	272.626808	46.8.19.32	172.16.1.137	SMTP	131	Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3571	272.628092	172.16.1.137	46.8.19.32	SMTP	250	Create Request File: srvcli.dll
3572	272.628125	172.16.1.137	46.8.19.32	SMTP	250	Create Request File: netutils.dll
3573	272.628137	46.8.19.32	172.16.1.137	TCP	54	445 → 59376 [ACK] Seq=406764 Ack=25395 Win=64240 Len=0
3574	272.628155	46.8.19.32	172.16.1.137	TCP	54	445 → 59376 [ACK] Seq=406764 Ack=25395 Win=64240 Len=0
3575	272.849669	46.8.19.32	172.16.1.137	SMTP	131	Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3576	272.909903	172.16.1.137	46.8.19.32	TCP	54	59376 → 445 [ACK] Seq=25591 Ack=406841 Win=65007 Len=0
3577	273.040819	46.8.19.32	172.16.1.137	SMTP	131	Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3578	273.126901	172.16.1.137	46.8.19.32	TCP	54	59376 → 445 [ACK] Seq=25591 Ack=406841 Win=65007 Len=0
3585	303.078830	172.16.1.137	46.8.19.32	TCP	55	[TCP Keep-Alive] 59376 → 445 [ACK] Seq=25590 Ack=406918 Win=64930 Len=1
3586	304.085234	172.16.1.137	46.8.19.32	TCP	55	[TCP Keep-Alive] 59376 → 445 [ACK] Seq=25590 Ack=406918 Win=64930 Len=1
3587	304.085325	46.8.19.32	172.16.1.137	TCP	54	[TCP Keep-Alive ACK] 445 → 59376 [ACK] Seq=406918 Ack=25591 Win=64240 Len=0
3590	334.095708	172.16.1.137	46.8.19.32	TCP	55	[TCP Keep-Alive] 59376 → 445 [ACK] Seq=25590 Ack=406918 Win=64930 Len=1
3591	334.095737	46.8.19.32	172.16.1.137	TCP	54	[TCP Keep-Alive ACK] 445 → 59376 [ACK] Seq=406918 Ack=25591 Win=64240 Len=0
4137	360.201488	172.16.1.137	46.8.19.32	SMTP	162	GetInfo Request SEC_INFO/SMTP_SEC_INFO_00 File: server.exe
4138	360.201563	46.8.19.32	172.16.1.137	TCP	54	445 → 59376 [ACK] Seq=406918 Ack=25699 Win=64240 Len=0
4139	360.456410	46.8.19.32	172.16.1.137	SMTP	150	GetInfo Response
4140	360.505901	172.16.1.137	46.8.19.32	TCP	54	59376 → 445 [ACK] Seq=25699 Ack=407014 Win=64834 Len=0
4141	360.512784	172.16.1.137	46.8.19.32	SMTP	226	Create Request File: server.exe
4142	360.512824	46.8.19.32	172.16.1.137	TCP	54	445 → 59376 [ACK] Seq=407014 Ack=25871 Win=64240 Len=0
4143	360.737350	46.8.19.32	172.16.1.137	SMTP	242	Create Response File: server.exe
4144	360.737649	172.16.1.137	46.8.19.32	SMTP	146	Close Request File: server.exe
4145	360.737689	46.8.19.32	172.16.1.137	TCP	54	445 → 59376 [ACK] Seq=407202 Ack=25963 Win=64240 Len=0
4146	360.949358	46.8.19.32	172.16.1.137	SMTP	358	Create Response File: server.exe
4147	360.949752	172.16.1.137	46.8.19.32	SMTP	358	Create Request File: server.exe
4148	360.949790	46.8.19.32	172.16.1.137	TCP	54	445 → 59376 [ACK] Seq=407330 Ack=26267 Win=64240 Len=0
4150	361.176422	46.8.19.32	172.16.1.137	SMTP	318	Create Response File: server.exe
4151	361.176756	172.16.1.137	46.8.19.32	SMTP	346	Close Request File: server.exe
4152	361.176794	46.8.19.32	172.16.1.137	TCP	54	445 → 59376 [ACK] Seq=407594 Ack=26359 Win=64240 Len=0

3.pcap

Packets: 9936 Displayed: 1369 (13.8%) Profile: Default

2:26 AM 11/29/2023