

# Report Esercizio 2: Studio IOC - Sandbox Any.run e analisi VirusTotal e Wireshark

## URL analizzato:

<https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/>

## Fonte sospetta:

<https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>

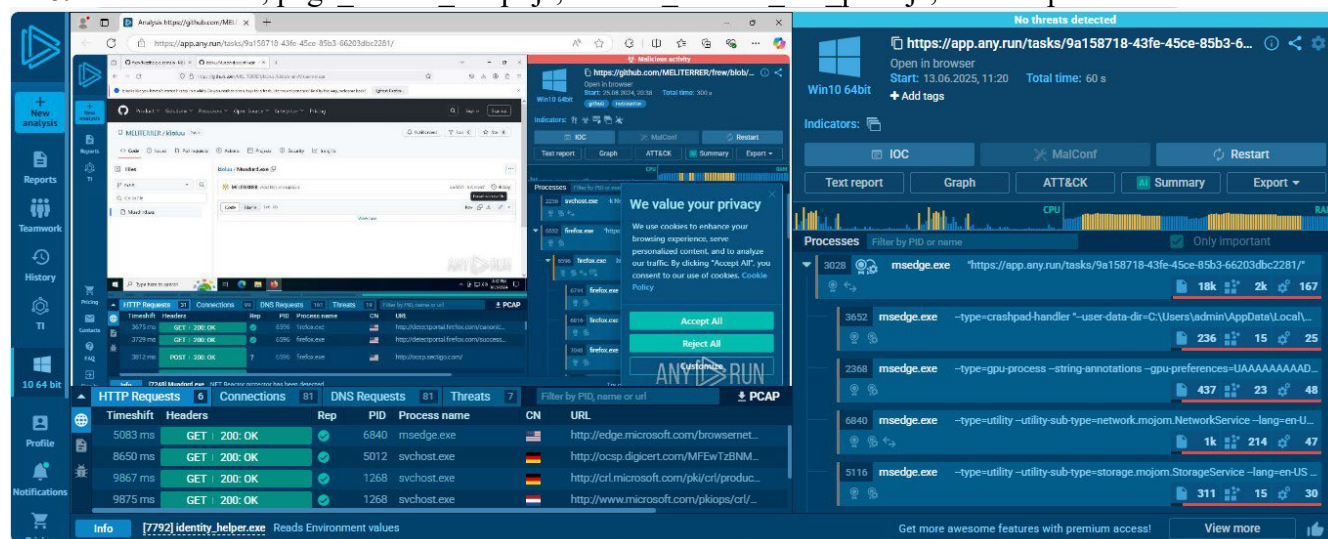
**Obiettivo:** Analizzare il comportamento del file Jvczfhe.exe ed eventuali indicatori di compromissione tramite sandbox online (Any.run) e verifica degli hash/URL su VirusTotal.

## 1. Any.run

- Il file Jvczfhe.exe viene scaricato tramite browser Edge.
- Crea numerosi processi Edge in background (msedge.exe) con attività nella directory temporanea.
- Vengono estratti file .js all'interno di chrome\_Unpacker (es. page\_embed\_script.js, service\_worker\_bin\_prod.js).
- Nessuna connessione esterna visibile oltre a quelle legittime.
- L'attività suggerisce un comportamento preparatorio o evasivo.

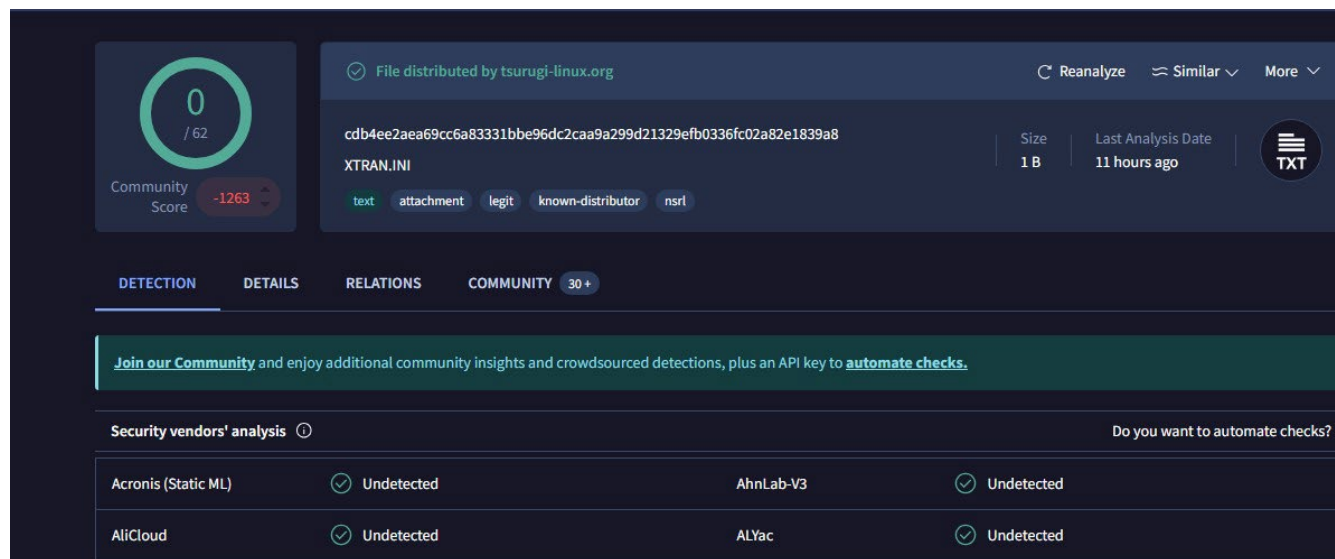
**Processi rilevanti:** - msedge.exe - svchost.exe

**File:** - XTRAN.INI, page\_embed\_script.js, service\_worker\_bin\_prod.js, altri .tmp



## Utilizziamo VirusTotal - Analisi SHA256

a. Hash **cdb4ee2aae69cc6a83331bbe96dc2caa9a299d1329efb0336fc02a82e1839a8** - Nome: XTRAN.INI - Tipo: file .INI da 1 byte - Stato: 0/62 engine lo rilevano come malevolo -



The screenshot shows the VirusTotal analysis page for a file named XTRAN.INI. The file is 1 B in size and was last analyzed 11 hours ago. The community score is 0/62, with a score of -1263. The file is categorized as text, attachment, legit, known-distributor, and nsrl. The analysis shows that no security vendors flagged this file as malicious. The interface includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY (30+).

File distributed by tsurugi-linux.org

Reanalyze Similar More

cdb4ee2aae69cc6a83331bbe96dc2caa9a299d1329efb0336fc02a82e1839a8

Size: 1 B | Last Analysis Date: 11 hours ago

XTRAN.INI

text attachment legit known-distributor nsrl

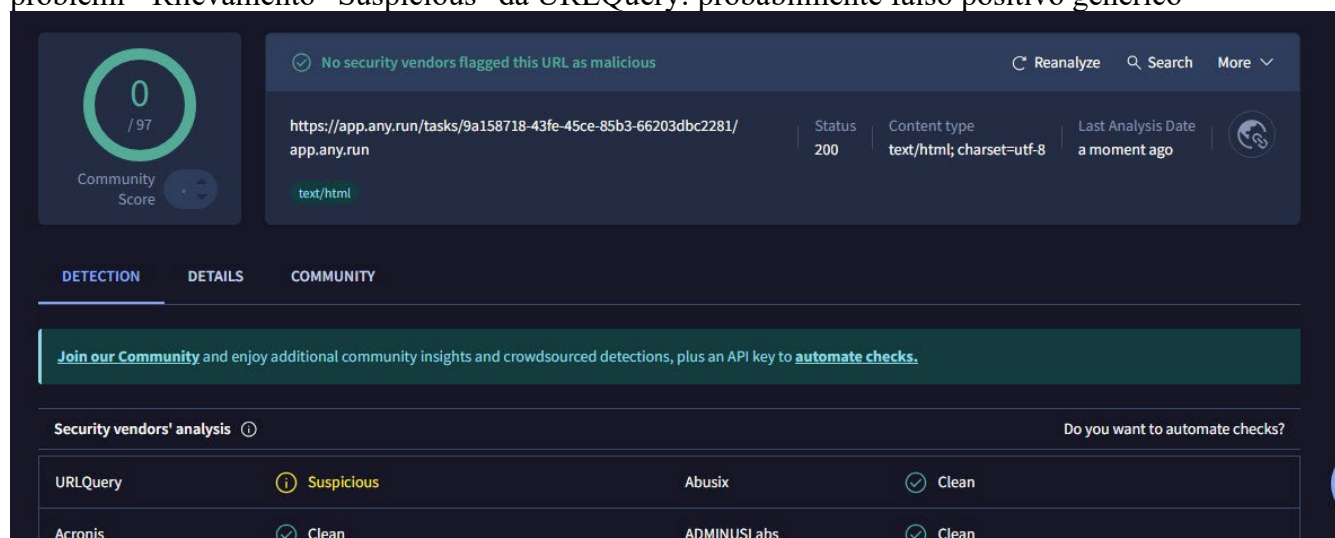
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Vendor	Status	Vendor	Status
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected

## URL Any.run

<https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/> - Stato: 0/97 motori rilevano problemi - Rilevamento “Suspicious” da URLQuery: probabilmente falso positivo generico



The screenshot shows the Any.run analysis page for the URL https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/. The URL is categorized as text/html. The community score is 0/97. The analysis shows that no security vendors flagged this URL as malicious. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY.

No security vendors flagged this URL as malicious

Reanalyze Search More

https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/

Status: 200 | Content type: text/html; charset=utf-8 | Last Analysis Date: a moment ago

text/html

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

Security vendors' analysis

Vendor	Status	Vendor	Status
URLQuery	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

L'analisi dinamica dell'URL <https://app.any.run/tasks/9a158718...> con URLQuery ha confermato che non sono presenti contenuti pericolosi, reindirizzamenti né tentativi di connessione sospetti. L'unica rilevazione "Suspicious" su VirusTotal è probabilmente dovuta alla natura dinamica della piattaforma Any.run e non indica una minaccia reale.

## Report Overview

Visited public

2025-06-13 09:59:59

URL

[app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/](https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/)

Finishing URL

[app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/](https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/)

IP / ASN

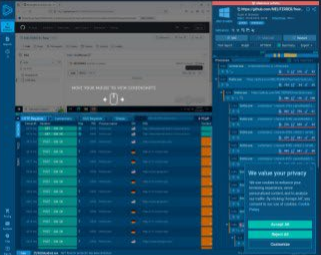
104.22.48.74

#13335 CLOUDFLARENET

Tags

Title

Analysis <https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe> Malicious activity - Interactive analysis ANY.RUN




Detections

urlquery | 0

Network Intrusion Detection | 0

Threat Detection Systems | 0

**URL GitHub del file sospetto** <https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe> - Stato HTTP: 404 (non più disponibile) - VirusTotal: 0/97 segnalazioni



<https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>

Sign in

0

/ 97

Community Score

✓ No security vendors flagged this URL as malicious

Reanalyze

Search

More

<https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>

github.com

Status

404

Content type

text/html; charset=utf-8

Last Analysis Date

1 month ago

text/html

contains-pe

external-resources

password-input

DETECTION

DETAILS

COMMUNITY

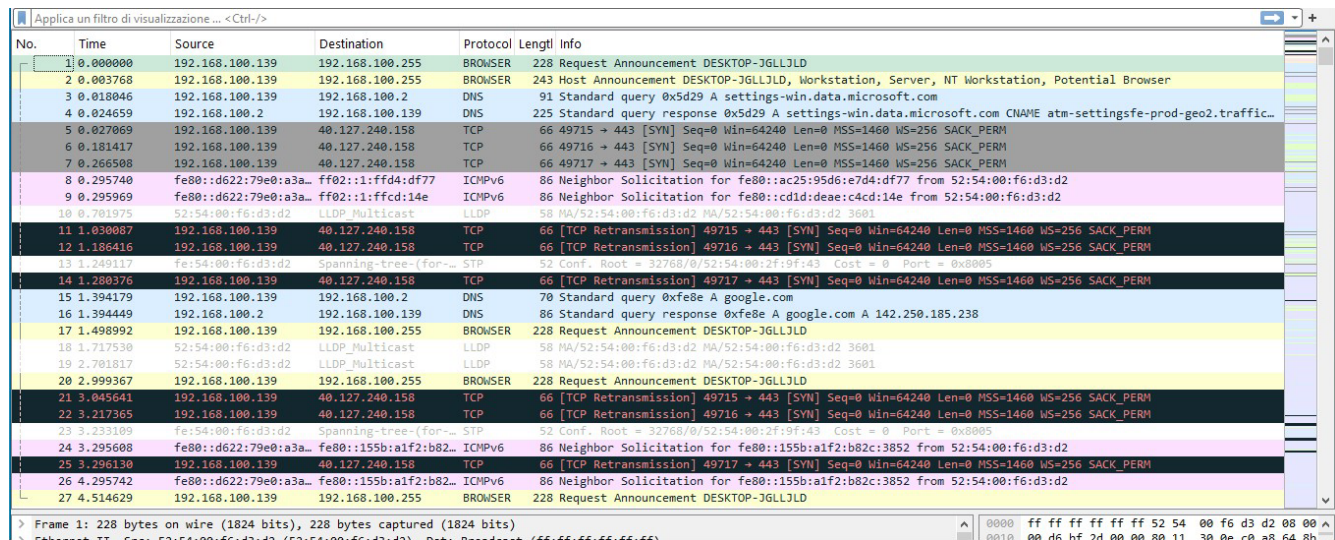
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean

## Analisi del file .pcap con wireshark



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.139	192.168.100.255	BROWSER	228	Request Announcement DESKTOP-JGLJLJD
2	0.003768	192.168.100.139	192.168.100.255	BROWSER	243	Host Announcement DESKTOP-JGLJLJD, Workstation, Server, NT Workstation, Potential Browser
3	0.018046	192.168.100.139	192.168.100.2	DNS	91	Standard query 0x5d29 A settings-win.data.microsoft.com
4	0.024659	192.168.100.2	192.168.100.139	DNS	225	Standard query response 0x5d29 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.traffic...
5	0.027069	192.168.100.139	40.127.240.158	TCP	66	49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6	0.181417	192.168.100.139	40.127.240.158	TCP	66	49716 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7	0.266508	192.168.100.139	40.127.240.158	TCP	66	49717 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8	0.295740	fe80::d622:79e0:a3a...	ff02::1:fffd:df77	ICMPv6	86	Neighbor Solicitation for fe80::ac25:95d6:e7d4:df77 from 52:54:00:f6:d3:d2
9	0.295969	fe80::d622:79e0:a3a...	ff02::1:ffcd:14e	ICMPv6	86	Neighbor Solicitation for fe80::cd1d:deae:c4cd:14e from 52:54:00:f6:d3:d2
10	0.701975	52:54:00:f6:d3:d2		LLDP_Multicast	58	MA/52:54:00:f6:d3:d2 MA/52:54:00:f6:d3:d2 3601
11	1.030887	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12	1.186416	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49716 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
13	1.249117	fe:54:00:f6:d3:d2	Spanning-tree-(for-...	STP	52	Conf. Root = 32768/0/52:54:00:2f:9f:43 Cost = 0 Port = 0x8005
14	1.280376	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49717 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15	1.394179	192.168.100.139	192.168.100.2	DNS	70	Standard query 0xfe8e A google.com
16	1.394449	192.168.100.2	192.168.100.139	DNS	86	Standard query response 0xfe8e A google.com A 142.250.185.238
17	1.498992	192.168.100.139	192.168.100.255	BROWSER	228	Request Announcement DESKTOP-JGLJLJD
18	1.717530	52:54:00:f6:d3:d2		LLDP_Multicast	58	MA/52:54:00:f6:d3:d2 MA/52:54:00:f6:d3:d2 3601
19	2.701817	52:54:00:f6:d3:d2		LLDP_Multicast	58	MA/52:54:00:f6:d3:d2 MA/52:54:00:f6:d3:d2 3601
20	2.999367	192.168.100.139	192.168.100.255	BROWSER	228	Request Announcement DESKTOP-JGLJLJD
21	3.045641	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
22	3.217365	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49716 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23	3.233182	fe:54:00:f6:d3:d2	Spanning-tree-(for-...	STP	52	Conf. Root = 32768/0/52:54:00:2f:9f:43 Cost = 0 Port = 0x8005
24	3.295608	fe80::d622:79e0:a3a...	fe80::155b:a1f2:b82...	ICMPv6	86	Neighbor Solicitation for fe80::155b:a1f2:b82c:3852 from 52:54:00:f6:d3:d2
25	3.296130	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49717 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
26	4.295742	fe80::d622:79e0:a3a...	fe80::155b:a1f2:b82...	ICMPv6	86	Neighbor Solicitation for fe80::155b:a1f2:b82c:3852 from 52:54:00:f6:d3:d2
27	4.514629	192.168.100.139	192.168.100.255	BROWSER	228	Request Announcement DESKTOP-JGLJLJD

IP sorgente 192.168.100.139

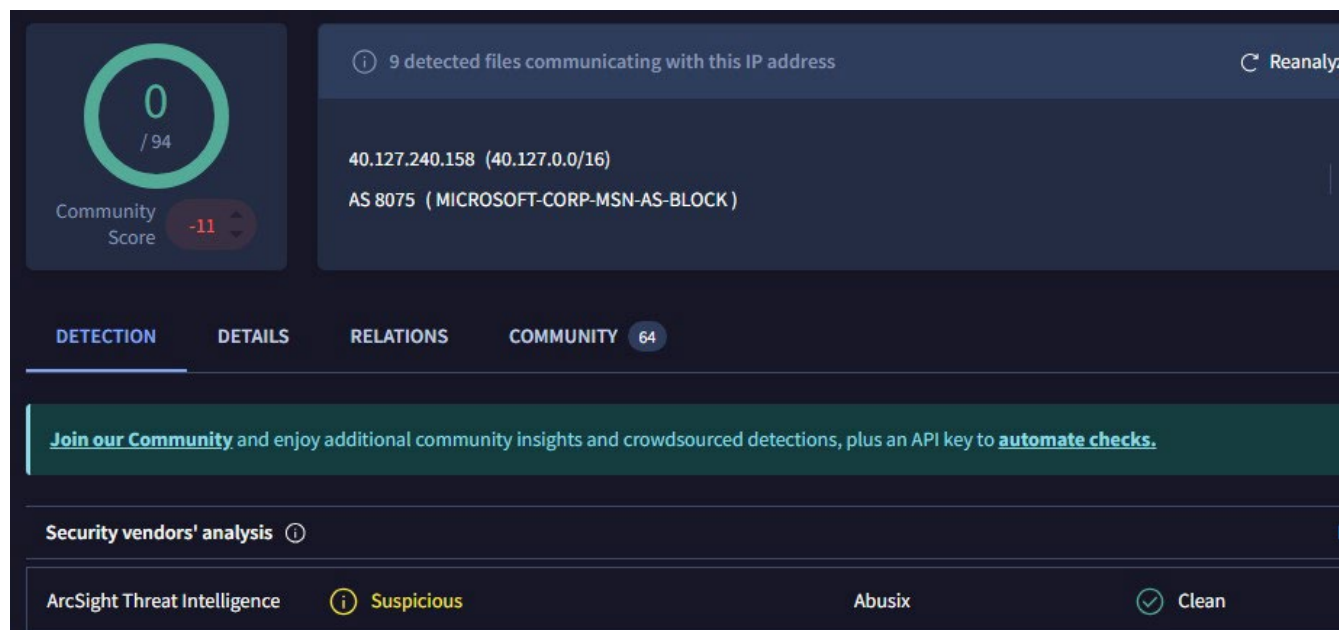
IP di destinazione sospetto 40.127.240.158 → **IP pubblico**, TCP porta 443 (HTTPS)

Ripetute **SYN** e **Retransmission** Segnale che il malware cerca di aprire una connessione HTTPS verso quell'IP ma **non riceve risposta**

DNS request google.com, settings-win.data.microsoft.com → possono essere innocui, ma vale la pena monitorarli

Connessioni attive Solo **tentativi di connessione TCP su porta 443**, niente POST/GET ancora visibili

## Analisi Indirizzo IP sospetto tramite Virustotal:



- L'IP è su **Microsoft Azure**, spesso usato da C2 (Command and Control) perché consente ai malware writer di creare **server temporanei**.
- Anche se **non ci sono firme antivirus che lo bloccano**, il fatto che altri malware ci abbiano comunicato è molto indicativo.
- ArcSight (una fonte TI affidabile) lo reputa **"Suspicious"**
- 9 file malware noti comunicano con questo ip



## Torniamo su Wireshark, provando alcuni filtri: dns,http e tcp.port == 443

dns						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.018046	192.168.100.139	192.168.100.2	DNS	91	Standard query 0x5d29 A settings-win.data.microsoft.com
4	0.024659	192.168.100.2	192.168.100.139	DNS	225	Standard query response 0x5d29 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.traffic...
15	1.394179	192.168.100.139	192.168.100.2	DNS	70	Standard query 0xfe8e A google.com
16	1.394449	192.168.100.2	192.168.100.139	DNS	86	Standard query response 0xfe8e A google.com A 142.250.185.238
34	5.809470	192.168.100.139	192.168.100.2	DNS	70	Standard query 0xbc69 A github.com
35	5.809680	192.168.100.139	192.168.100.2	DNS	84	Standard query 0xb49 A detectportal.firefox.com
36	5.815188	192.168.100.2	192.168.100.139	DNS	195	Standard query response 0xb49 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod...
37	5.818075	192.168.100.2	192.168.100.139	DNS	86	Standard query response 0xbc69 A github.com A 140.82.121.3
38	5.818311	192.168.100.139	192.168.100.2	DNS	102	Standard query 0xb3e5 A prod.detectportal.prod.cloudops.mozgcp.net
39	5.818423	192.168.100.2	192.168.100.139	DNS	118	Standard query response 0xb3e5 A prod.detectportal.prod.cloudops.mozgcp.net A 34.107.221.82
40	5.818807	192.168.100.139	192.168.100.2	DNS	102	Standard query 0xfcd1 AAAA prod.detectportal.prod.cloudops.mozgcp.net
41	5.819029	192.168.100.139	192.168.100.2	DNS	70	Standard query 0xbaf8 A github.com
42	5.819133	192.168.100.2	192.168.100.139	DNS	86	Standard query response 0xbaf8 A github.com A 140.82.121.3
44	5.819892	192.168.100.139	192.168.100.2	DNS	70	Standard query 0xd537 AAAA github.com
45	5.824324	192.168.100.2	192.168.100.139	DNS	130	Standard query response 0xfcd1 AAAA prod.detectportal.prod.cloudops.mozgcp.net AAAA 2600:1901:0:38d7::
46	5.825555	192.168.100.2	192.168.100.139	DNS	135	Standard query response 0xd537 AAAA github.com SOA dns1.p08.nsnone.net
60	5.882405	192.168.100.139	192.168.100.2	DNS	71	Standard query 0x344f A example.org
61	5.883153	192.168.100.139	192.168.100.2	DNS	73	Standard query 0xab9a A ipv4only.arpa
62	5.888056	192.168.100.2	192.168.100.139	DNS	87	Standard query response 0x344f A example.org A 93.184.215.14
63	5.889327	192.168.100.2	192.168.100.139	DNS	105	Standard query response 0xab9a A ipv4only.arpa A 192.0.0.170 A 192.0.0.171
64	5.914754	192.168.100.139	192.168.100.2	DNS	84	Standard query 0x9b73 A detectportal.firefox.com
65	5.915010	192.168.100.2	192.168.100.139	DNS	198	Standard query response 0x9b73 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod...
73	5.946834	192.168.100.139	192.168.100.2	DNS	88	Standard query 0x6cb6 A contile.services.mozilla.com
74	5.952760	192.168.100.2	192.168.100.139	DNS	104	Standard query response 0x6cb6 A contile.services.mozilla.com A 34.117.188.166
75	5.954245	192.168.100.139	192.168.100.2	DNS	88	Standard query 0xb332 A contile.services.mozilla.com
76	5.954413	192.168.100.2	192.168.100.139	DNS	104	Standard query response 0xb332 A contile.services.mozilla.com A 34.117.188.166
77	5.954927	192.168.100.139	192.168.100.2	DNS	88	Standard query 0x8182 AAAA contile.services.mozilla.com

http						
No.	Time	Source	Destination	Protocol	Length	Info
57	5.863406	192.168.100.139	34.107.221.82	HTTP	357	GET /canonical.html HTTP/1.1
59	5.872841	34.107.221.82	192.168.100.139	HTTP	352	HTTP/1.1 200 OK (text/html)
69	5.922817	192.168.100.139	34.107.221.82	HTTP	359	GET /success.txt?ipv4 HTTP/1.1
72	5.930143	34.107.221.82	192.168.100.139	HTTP	270	HTTP/1.1 200 OK (text/plain)
118	6.027133	192.168.100.139	172.64.149.23	OCSP	479	Request
121	6.029373	192.168.100.139	184.24.77.69	OCSP	480	Request
129	6.037751	184.24.77.69	192.168.100.139	OCSP	944	Response
132	6.042000	192.168.100.139	184.24.77.69	OCSP	480	Request
141	6.049261	184.24.77.69	192.168.100.139	OCSP	944	Response
145	6.066100	172.64.149.23	192.168.100.139	OCSP	830	Response
220	6.204982	192.168.100.139	184.24.77.81	OCSP	480	Request
225	6.207333	192.168.100.139	184.24.77.81	OCSP	480	Request
233	6.212271	184.24.77.81	192.168.100.139	OCSP	944	Response
236	6.214928	184.24.77.81	192.168.100.139	OCSP	943	Response
285	6.290949	192.168.100.139	142.250.186.67	OCSP	477	Request
305	6.327297	142.250.186.67	192.168.100.139	OCSP	756	Response
313	6.337714	192.168.100.139	184.24.77.81	OCSP	480	Request
330	6.348198	184.24.77.81	192.168.100.139	OCSP	944	Response
537	6.446984	192.168.100.139	142.250.186.67	OCSP	477	Request
636	6.483963	142.250.186.67	192.168.100.139	OCSP	756	Response
1793	6.862926	192.168.100.139	184.24.77.69	OCSP	480	Request
1812	6.870159	192.168.100.139	184.24.77.74	OCSP	480	Request
1823	6.875649	184.24.77.69	192.168.100.139	OCSP	944	Response
1837	6.878616	184.24.77.74	192.168.100.139	OCSP	944	Response
4706	8.240708	192.168.100.139	172.64.149.23	OCSP	480	Request
4805	8.280530	192.168.100.139	192.229.221.95	OCSP	480	Request
4808	8.280730	192.168.100.139	192.229.221.95	OCSP	480	Request

Durante l'analisi è stato inoltre esaminato il traffico DNS e HTTP generato dal malware. Le richieste DNS hanno interessato esclusivamente domini legittimi (Microsoft, GitHub, Mozilla), mentre il traffico HTTP si è limitato a connessioni di controllo della connettività, senza evidenza di comportamenti anomali o comunicazioni malevole.

## Filtro tcp.port == 443

Sono stati rilevati **tentativi di connessione su porta 443** verso l'IP pubblico:

**IP:** 40.127.240.158

**Esito:** solo pacchetti SYN → **nessuna risposta**

**Comportamento sospetto:** connessione diretta via IP, **senza uso di DNS**

Altre comunicazioni cifrate sono state stabilite con server legittimi:

github.com → hosting del malware

contile.services.mozilla.com e ocsf.pki.goog → servizi Mozilla e Google

No.	Time	Source	Destination	Protocol	Length	Info
11	1.030087	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12	1.186416	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49716 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
14	1.280376	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49717 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
21	3.045641	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
22	3.217365	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49716 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
25	3.296130	192.168.100.139	40.127.240.158	TCP	66	[TCP Retransmission] 49717 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
43	5.819283	192.168.100.139	140.82.121.3	TCP	66	49724 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
47	5.825584	140.82.121.3	192.168.100.139	TCP	66	443 → 49724 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1361 SACK_PERM WS=1024
48	5.826867	192.168.100.139	140.82.121.3	TCP	54	49724 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
49	5.834560	192.168.100.139	140.82.121.3	TLSv1.3	712	Client Hello (SNI=github.com)
50	5.841721	140.82.121.3	192.168.100.139	TLSv1.3	1415	Server Hello, Change Cipher Spec, Application Data
51	5.841740	140.82.121.3	192.168.100.139	TCP	1415	443 → 49724 [PSH, ACK] Seq=1362 Ack=659 Win=67584 Len=1361 [TCP PDU reassembled in 52]
52	5.841756	140.82.121.3	192.168.100.139	TLSv1.3	824	Application Data, Application Data, Application Data
53	5.842005	192.168.100.139	140.82.121.3	TCP	54	49724 → 443 [ACK] Seq=659 Ack=3493 Win=262656 Len=0
78	5.956899	192.168.100.139	34.117.188.166	TCP	66	49727 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
81	5.962789	34.117.188.166	192.168.100.139	TCP	66	443 → 49727 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1361 SACK_PERM WS=256
82	5.963681	192.168.100.139	34.117.188.166	TCP	54	49727 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
83	5.965891	192.168.100.139	34.117.188.166	TLSv1.3	730	Client Hello (SNI=contile.services.mozilla.com)
85	5.968218	192.168.100.139	34.117.188.166	TCP	66	49728 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
89	5.972503	34.117.188.166	192.168.100.139	TCP	54	443 → 49727 [ACK] Seq=1 Ack=677 Win=67072 Len=0
92	5.975936	34.117.188.166	192.168.100.139	TLSv1.3	1415	Server Hello, Change Cipher Spec
93	5.975998	34.117.188.166	192.168.100.139	TCP	1415	443 → 49727 [ACK] Seq=1362 Ack=677 Win=67072 Len=1361 [TCP PDU reassembled in 94]
94	5.976043	34.117.188.166	192.168.100.139	TLSv1.3	401	Application Data
95	5.976084	34.117.188.166	192.168.100.139	TCP	66	443 → 49728 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1361 SACK_PERM WS=256
96	5.977196	192.168.100.139	34.117.188.166	TCP	54	49727 → 443 [ACK] Seq=677 Ack=3070 Win=262656 Len=0
97	5.977297	192.168.100.139	34.117.188.166	TCP	54	49728 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
98	5.982880	192.168.100.139	34.117.188.166	TLSv1.3	721	Client Hello (SNI=spocs.getpocket.com)

Il malware ha tentato connessioni HTTPS dirette verso un **IP pubblico potenzialmente utilizzato come server C2**, senza tuttavia ricevere risposta.

## - **Conclusione**

Il file si comporta come un **malware potenzialmente connesso a un'infrastruttura Command & Control (C2)**.

Durante l'esecuzione:

- Ha tentato di stabilire **una connessione cifrata HTTPS (porta 443)** verso un **IP pubblico ospitato su Microsoft Azure (40.127.240.158)**
- Questo IP, secondo l'analisi OSINT su **VirusTotal**, è stato **etichettato come sospetto** da fonti di threat intelligence (es. ArcSight) ed è **stato contattato da altri malware noti**
- Il malware ha tentato **connessioni dirette tramite IP**, evitando il DNS per **eludere controlli**
- Tuttavia, **non è riuscito a completare la connessione**, quindi **non si sono osservate esfiltrazioni attive**

Questa tecnica rappresenta una **minaccia potenziale** in quanto:

- Usa la **porta 443 cifrata** per **nascondere la comunicazione**
- Elude controlli DNS e si nasconde nel traffico apparentemente legittimo