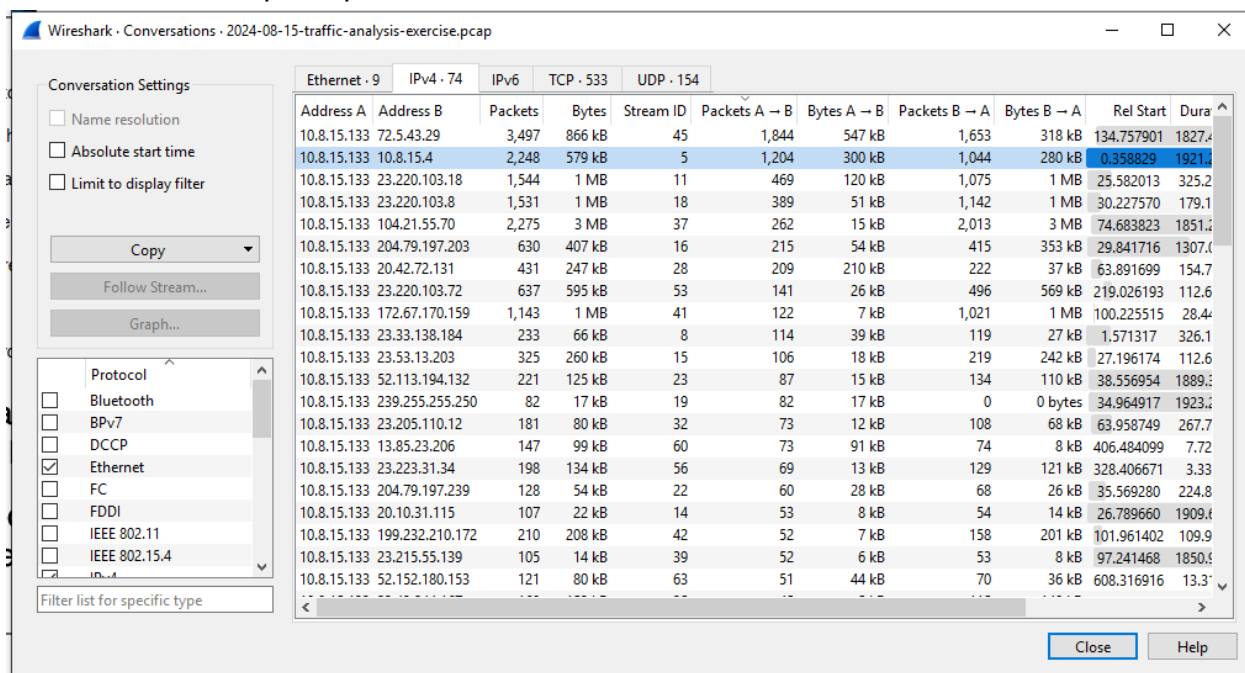


WarmCookie Malware Traffic Analysis

Analyzing the Traffic

My first step in analyzing the traffic from the malware was looking at the conversations between the infected machine and other IPs. The reason for this being that high amounts of packets being sent and received from specific IPs could indicate data exfiltration or contacting a command and control server. As you can see from the screenshot below, we can see some outliers in terms of packet count. Notably, 72.5.43.29 sits atop the packet count list.



Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Dura
10.8.15.133	72.5.43.29	3,497	866 kB	45	1,844	547 kB	1,653	318 kB	134.757901	1827.4
10.8.15.133	10.8.15.4	2,248	579 kB	5	1,204	300 kB	1,044	280 kB	0.358829	1921.6
10.8.15.133	23.220.103.18	1,544	1 MB	11	469	120 kB	1,075	1 MB	25.582013	325.2
10.8.15.133	23.220.103.8	1,531	1 MB	18	389	51 kB	1,142	1 MB	30.227570	179.1
10.8.15.133	104.21.55.70	2,275	3 MB	37	262	15 kB	2,013	3 MB	74.683823	1851.2
10.8.15.133	204.79.197.203	630	407 kB	16	215	54 kB	415	353 kB	29.841716	1307.6
10.8.15.133	20.42.72.131	431	247 kB	28	209	210 kB	222	37 kB	63.891699	154.7
10.8.15.133	23.220.103.72	637	595 kB	53	141	26 kB	496	569 kB	219.026193	112.6
10.8.15.133	172.67.170.159	1,143	1 MB	41	122	7 kB	1,021	1 MB	100.225515	28.4
10.8.15.133	23.33.138.184	233	66 kB	8	114	39 kB	119	27 kB	1.571317	326.1
10.8.15.133	23.53.13.203	325	260 kB	15	106	18 kB	219	242 kB	27.196174	112.6
10.8.15.133	52.113.194.132	221	125 kB	23	87	15 kB	134	110 kB	38.556954	1889.3
10.8.15.133	239.255.255.250	82	17 kB	19	82	17 kB	0	0 bytes	34.964917	1923.2
10.8.15.133	23.205.110.12	181	80 kB	32	73	12 kB	108	68 kB	63.958749	267.7
10.8.15.133	13.85.23.206	147	99 kB	60	73	91 kB	74	8 kB	406.484099	7.72
10.8.15.133	23.223.31.34	198	134 kB	56	69	13 kB	129	121 kB	328.406671	3.33
10.8.15.133	204.79.197.239	128	54 kB	22	60	28 kB	68	26 kB	35.569280	224.8
10.8.15.133	20.10.31.115	107	22 kB	14	53	8 kB	54	14 kB	26.789660	1909.4
10.8.15.133	199.232.210.172	210	208 kB	42	52	7 kB	158	201 kB	101.961402	109.9
10.8.15.133	23.215.55.139	105	14 kB	39	52	6 kB	53	8 kB	97.241468	1850.9
10.8.15.133	52.152.180.153	121	80 kB	63	51	44 kB	70	36 kB	608.316916	13.3

Because of the high amount of data being transferred between 72.5.43.29 and the infected machine, I used VirusTotal to check if the IP is associated with anything malicious. The following results show that the IP is associated with malicious attacks, therefore it is necessary to analyze interactions with this IP further. VirusTotal gives us some more detail to work with as well by showing files associated with the IP.



14/94 security vendors flagged this IP address as malicious

Reanalyze Similar More

72.5.43.29 (72.5.42.0/23)
AS 399629 (BLNWX)

RO Last Analysis Date
14 minutes ago

DETECTION DETAILS RELATIONS COMMUNITY 1

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?

alphaMountain.ai	Malicious	BitDefender	Malware
Certego	Malicious	CyRadat	Malicious
Dr.Web	Malicious	ESET	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
G-Dat	Malware	Kaspersky	Malware
Lionic	Malware	MalwareURL	Malware
SOCRadat	Phishing	Webroot	Malicious
ArcSight Threat Intelligence	Suspicious	Abusix	Clean

Passive DNS Replication (2)

Date resolved	Detections	Resolver	Domain
2024-09-03	9 / 94	VirusTotal	checking-bots.site
2024-09-03	0 / 94	VirusTotal	www.checking-bots.site

Communicating Files (4)

Scanned	Detections	Type	Name
2025-01-22	31 / 60	JavaScript	87f57a7a4b4c83ecb3cdd5f274c95cd452c703de604f68aff6e59964b662e3f8.js
2024-11-05	55 / 72	Win32 DLL	Updater.dll
2025-01-22	55 / 72	Win32 DLL	0f60a3e7baecf2748b1c8183ed37d1e4
2024-11-05	57 / 72	Win32 DLL	f4d2c9470b322af29b9188a3a590cbe85bacb9cc8fcd7c2e94d82271ded3f659.dll

Files Referring (5)

Scanned	Detections	Type	Name
2024-08-19	17 / 65	unknown	malicious.exe
2025-01-28	0 / 61	Network capture	2024-08-15-traffic-analysis-exercise.pcap
-	-	file	e4337a9c8ec9b6eef007c0be6b492a7c8d64ee0610f0da597104ecd60b63d7a0
2024-12-05	0 / 62	Text	2024-08-15-traffic-analysis-exercise-alerts.txt
2024-10-02	0 / 62	Text	attack 2

Historical Whois Lookups (1)

The screenshot shows a Wireshark interface with a packet capture titled "2024-08-15-traffic-analysis-exercise.pcap". The packet list pane displays several packets, with packet 10608 selected. This packet is a TCP Reset (RST) from source IP 72.5.43.29 to destination IP 106.08.135.939318. The reset sequence number is 49810, and the window size is 256.

No.	Time	Source	Destination	Protocol	Length	Info
10598	134.757901	10.8.15.133	72.5.43.29	TCP	66	49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S...
10608	135.762299	72.5.43.29	106.08.135.939318	TCP	66	[TCP Retransmission] 49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S...
10609	135.939318	72.5.43.29	10.8.15.133	TCP	58	80 → 49810 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=256 S...
10610	135.939767	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10611	135.940137	10.8.15.133	72.5.43.29	HTTP	224	HEAD /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1
10612	135.940407	72.5.43.29	10.8.15.133	TCP	54	80 → 49810 [ACK] Seq=1 Ack=171 Win=64240 Len=0
10613	136.132929	72.5.43.29	10.8.15.133	HTTP	134	HTTP/1.1 200 OK
10614	136.156102	10.8.15.133	72.5.43.29	HTTP	223	GET /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1
10615	136.156363	72.5.43.29	10.8.15.133	TCP	54	80 → 49810 [ACK] Seq=81 Ack=340 Win=64240 Len=0
10616	136.342163	72.5.43.29	10.8.15.133	TCP	1418	80 → 49810 [PSH, ACK] Seq=81 Ack=340 Win=64240 Len=1364 [FIN]
10617	136.342350	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=1445 Ack=340 Win=64240 Len=1460 [TCP
10618	136.342355	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=2905 Ack=340 Win=64240 Len=1460 [TCP
10619	136.342356	72.5.43.29	10.8.15.133	TCP	1226	80 → 49810 [PSH, ACK] Seq=4365 Ack=340 Win=64240 Len=1172
10620	136.342541	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=340 Ack=5537 Win=64240 Len=0

```
> Frame 10611: 224 bytes on wire (1792 <
> Ethernet II, Src: Intel:8c:54:82:00
> Internet Protocol Version 4, Src: 10
> Transmission Control Protocol, Src Po
  Hypertext Transfer Protocol
    HEAD /data/0f60a3e7baecf2748b1c81e
      Request Method: HEAD
      Request URI: /data/0f60a3e7baec
      Request Version: HTTP/1.1
      Connection: Keep-Alive\r\n
      Accept: */*\r\n
      Accept-Encoding: identity\r\n
      User-Agent: Microsoft BITS/7.0\r\n
      Host: 72.5.43.29\r\n
0000 00 16 9c 02 a7 4b 00 1c bf 03 54 82 08 00 45 00 .....K...T...E...
0010 00 d2 70 81 40 00 80 06 f7 c5 f5 0a 08 0f 85 48 05 ...p@.....H...
0020 2b 1d c2 92 00 50 46 f1 27 a1 9e b1 2e a7 50 18 +...PF.....P...
0030 fa f0 b1 7e 00 00 48 45 44 20 2f da 61 74 61 ..F..o.b1..7e...H AD /data
0040 2f 30 66 36 30 61 33 65 37 62 61 65 63 62 37 /of60a3e7baecf27
0050 34 38 62 31 63 38 31 38 33 65 64 33 37 64 31 65 48b1c818 3ed37d1e
0060 34 20 48 54 50 2f 31 2d 31 0d 0a 43 6f 6e 68 4 HTTP/1.1 [conn
0070 65 63 74 69 6f 6e 3a 20 4b 65 70 2d 41 6c 6d action: Keep-Al
0080 76 65 0d 0a 41 63 65 70 74 2d 45 6e 63 2a 2f da ve-Accept: */*
0090 0a 41 63 63 65 70 74 2d 45 6e 63 64 69 6e 67 -Accept-Encod
00a0 3a 20 69 64 6e 74 6e 74 69 74 79 0d 0a 55 73 65 72 : identit y-User
00b0 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 -Agent: Microsof
00c0 74 20 42 49 54 53 2f 37 2e 38 0d 0a 48 6f 73 74 t BITS/7.0 .Host
00d0 3a 20 37 32 e 35 2e 34 33 2e 32 39 0d 0a 0d 0a : 72.5.4 3.29...
```

So we can see that known malicious files are being downloaded to the infected host. In order to broaden the scope of the analysis, I searched through the HTTP traffic to see if there are any other odd GET requests. After some searching, I found a GET request to the IP 104.21.55.70. This IP was also one of the outliers found when analyzing the different conversations between the infected machine and other IPs. I was able to resolve the hostname of this traffic, the hostname being "quote.checkfedexp.com". Searching this domain in VirusTotal shows that this is a malicious domain, and further analysis of the HTTP stream for this conversation shows that the infected machine is using a GET request to download a malicious file named "Invoice_876597035_003.zip". Analyzing this conversation also revealed the MAC address for the victim machine.

2024-08-15-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
66	1.320472	10.8.15.133	23.205.110.48	HTTP	165	GET /connecttest.txt HTTP/1.1
68	1.361053	23.205.110.48	10.8.15.133	HTTP	241	HTTP/1.1 200 OK (text/plain)
6418	74.732575	10.8.15.133	104.21.55.70	HTTP	663	GET /managements?16553a25e45250a41fd5&endeds=MIGppq&JStx=59bf050d37df88a9-ade43358-eaa1220b-59bf050d37df88a9-ade43358-eaa1220b HTTP/1.1
8659	80.268107	104.21.55.70	10.8.15.133	HTTP	105	HTTP/1.1 200 OK (application/octet-stream)
10198	101.996963	10.8.15.133	199.232.210.172	HTTP	407	HEAD /filestreamingservice/files/8f2381c2-652d-48a2-86f6-10200-102028788 HTTP/1.1
10200	102.028788	199.232.210.172	10.8.15.133	HTTP	648	HTTP/1.1 200 OK
10201	102.056752	10.8.15.133	199.232.210.172	HTTP	479	GET /filestreamingservice/files/8f2381c2-652d-48a2-86f6-10200-102028788 HTTP/1.1
10204	102.088412	199.232.210.172	10.8.15.133	HTTP	355	HTTP/1.1 206 Partial Content (application/x-chrome-extension)
10209	104.166688	10.8.15.133	199.232.210.172	HTTP	482	GET /filestreamingservice/files/8f2381c2-652d-48a2-86f6-10200-102028788 HTTP/1.1
10212	104.388566	199.232.210.172	10.8.15.133	HTTP	578	HTTP/1.1 206 Partial Content (application/x-chrome-extension)
10214	105.385210	10.8.15.133	199.232.210.172	HTTP	482	GET /filestreamingservice/files/8f2381c2-652d-48a2-86f6-10200-102028788 HTTP/1.1
10219	105.418694	199.232.210.172	10.8.15.133	HTTP	1236	HTTP/1.1 206 Partial Content (application/x-chrome-extension)
10222	106.603186	10.8.15.133	199.232.210.172	HTTP	483	GET /filestreamingservice/files/8f2381c2-652d-48a2-86f6-10200-102028788 HTTP/1.1
10232	106.645994	199.232.210.172	10.8.15.133	HTTP	349	HTTP/1.1 206 Partial Content (application/x-chrome-extension)

Ethernet II, Src: Intel_03:54:82 (00:1c:bf:03:54:82), Dst: Cisco_02:a7:4b (00:16:9c:02:a7:4b)

- Destination: Cisco_02:a7:4b (00:16:9c:02:a7:4b)
- Source: Intel_03:54:82 (00:1c:bf:03:54:82)
 - = LG bit: Globally unique address (factory default)
 - = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- [Stream index: 2]
- Internet Protocol Version 4, Src: 10.8.15.133, Dst: 104.21.55.70
- Transmission Control Protocol, Src Port: 49785, Dst Port: 80, Seq: 1, Ack: 1, Len: 609
- Hypertext Transfer Protocol
 - GET /managements?16553a25e45250a41fd5&endeds=MIGppq&JStx=59bf050d37df88a9-ade43358-eaa1220b-59bf050d37df88a9-ade43358-eaa1220b
 - Request Method: GET
 - Request URI: /managements?16553a25e45250a41fd5&endeds=MIGppq&JStx=59bf050d37df88a9-ade43358-eaa1220b-59bf050d37df88a9-ade43358-eaa1220b
 - Request Version: HTTP/1.1
 - Host: quote.checkfedexp.com\r\n
 - Connection: keep-alive\r\n

HTTP Host (http.host), 31 bytes

Packets: 18189 · Displayed: 658 (3.6%)

Profile: Default

12/94

Community Score

12/94 security vendors flagged this domain as malicious

Reanalyze Similar More

quote.checkfedexp.com

checkfedexp.com

Creation Date9 months ago

Last Analysis Date21 hours ago

DETECTIONDETAILSRELATIONSCOMMUNITY

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?

BitDefender	Malware	CyRadar	Malware
Dr.Web	Malicious	ESET	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
G-DATA	Malware	Lionic	Malware
Seclookup	Malicious	Sophos	Malware
VIPRE	Malware	Webroot	Malicious
ArcSight Threat Intelligence	Suspicious	Abusix	Clean

Wireshark · Follow HTTP Stream (tcp.stream eq 112) · 2024-08-15-traffic-analysis-exercise.pcap

GET /managements?16553a25e45250a41fd5&endeds=MIGPq&JStx=59bf050d37df88a9-ade43358-eea1220b-0571422b-0f33e6aa150e86bafd0ed4&ld=9d7502d88d752a27b1d00587309184b5a215 HTTP/1.1

Host: quote.checkfedexp.com

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK

Date: Thu, 15 Aug 2024 00:11:03 GMT

Content-Type: application/octet-stream

Transfer-Encoding: chunked

Connection: keep-alive

Content-Disposition: attachment; filename="Invoice 876597035_003.zip"

Pragma: no-cache

Cache-Control: no-cache, no-store

CF-Cache-Status: DYNAMIC

Report-To: { "endpoints": [{ "url": "https://a.nel.cloudflare.com/report/v4?s=NUoMw8HJmmJsvbLdk8wEDsT2gaQLQoxH2wtjVP4su2JkUFdfw8J0leg9bawjZRY18R4amKtgnIgEd7l3%2B4Innr1FKm0S15c0%2FmX2WrejsQ7B%2FC2fMQE8eNhZYMEYd6IhuvNBzZ2US4o7Q%3D%3D" }], "group": "cf-nel", "max_age": 604800 }

NEL: { "success_fraction": 0, "report_to": "cf-nel", "max_age": 604800 }

Server: cloudflare

CF-RAY: 8b34f6f53c4c6bb6-DFW

alt-svc: h3="443"; ma=86400

PK...

.....E.X....

;*.j.(...Invoice-876597035-003-8331775-8334138.js...ko#W.%...`...>x.8T7..]R5.~(.....\$U.6."E&.t.L6..Jn....3.....J.5/{.e....h.M..M<..Y:IV..a.m....>..S..*ZE..2^m'...X.....(.'.....A/].7...T....I)2Y.....q2..j....A.(9....d.../...o...1.?N..&.....=G..@..Q..68...f.D...".L.....E.e..qmr..>.O...YM...y.YF...4..).L.l.M...2....&l.l.l..*.<FO.|d.....v...'.V.6.w&.#9.f...%.~.O.E<.n.U2.....r...<..7

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (2769 kB)

Show asASCII

No delta times

Stream112

Find:

Case sensitive

Find Next

Filter Out This Stream

Print

Save as...

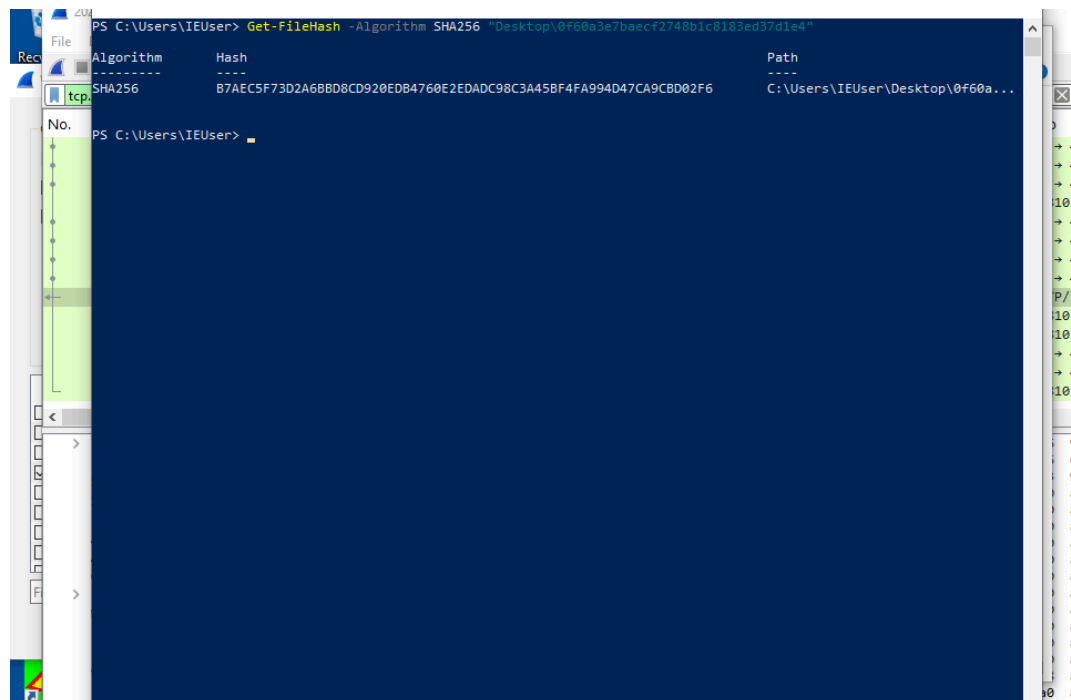
Back

Close

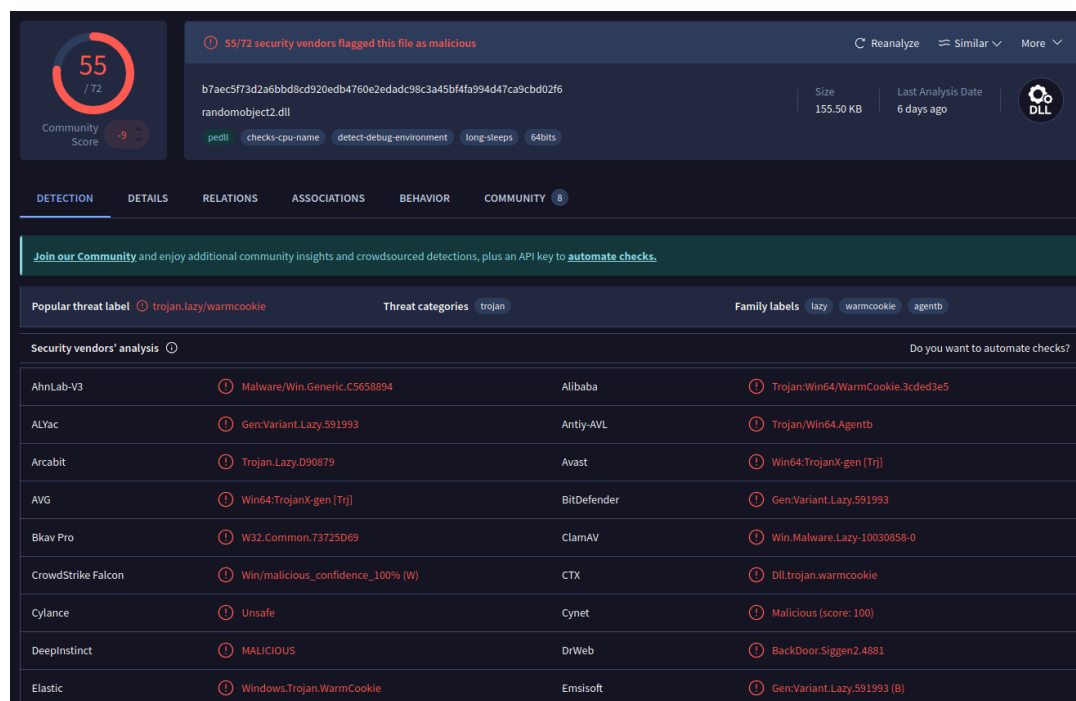
Help

I then exported the files associated with the GET requests to check their SHA-256 hashes in the VirusTotal database.

For the .dll file I received the following:



```
PS C:\Users\IEUser> Get-FileHash -Algorithm SHA256 "Desktop\0f60a3e7baecf2748b1c0183ed37d1e4"
Algorithm Hash Path
-----
SHA256 B7AEC5F73D2A68BD8CD920EDB4760E2EDADC98C3A45BF4FA994D47CA9C8D02F6 C:\Users\IEUser\Desktop\0f60a...
```



55 / 72 Community Score

55/72 security vendors flagged this file as malicious

Reanalyze Similar More

b7aec5f73d2a68bd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6
randomobject2.dll

Size: 155.50 KB | Last Analysis Date: 6 days ago

peDll checks-cpu-name detect-debug-environment long-sleeps 64bits

DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 8

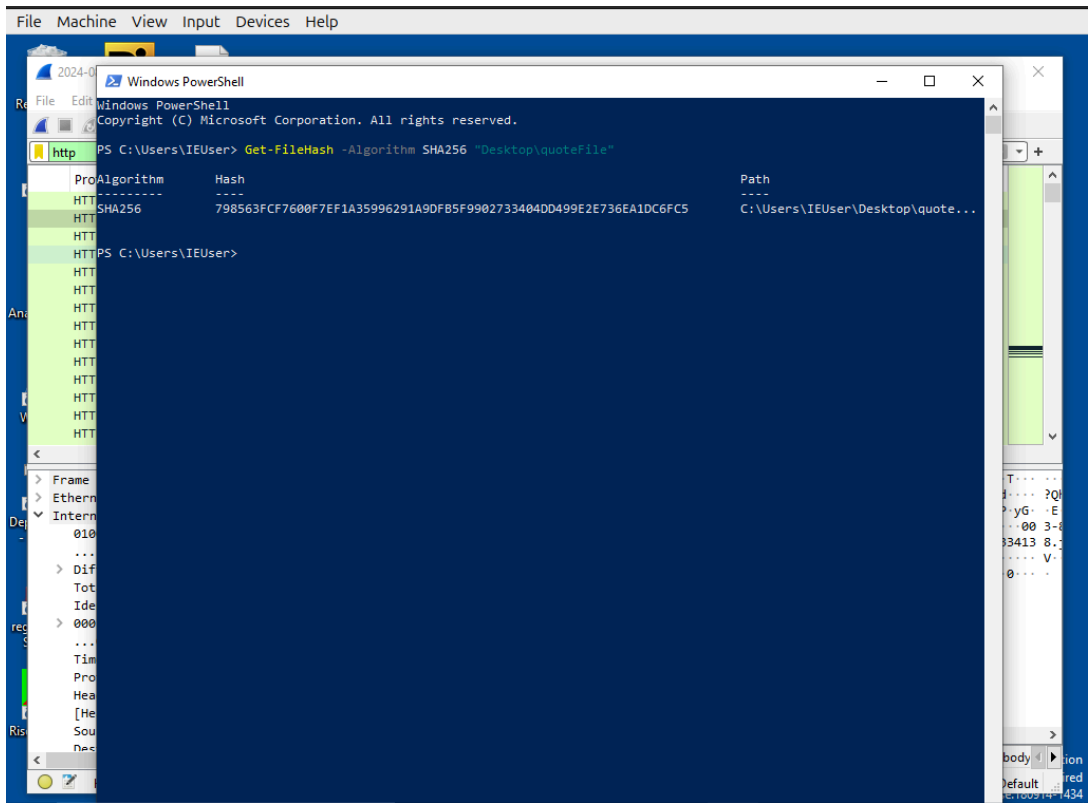
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.lazy/warmcookie | Threat categories: trojan | Family labels: lazy, warmcookie, agentb

Security vendors' analysis

Do you want to automate checks?			
AhnLab-V3	Malware/Win.Generic.C5658894	Alibaba	Trojan:Win64/WarmCookie.3cded3e5
ALYac	Gen:Variant.Lazy.591993	Antiy-AVL	Trojan:Win64.Agentb
Arcabit	Trojan.Lazy.090879	Avast	Win64:TrojanX-gen [Trj]
AVG	Win64:TrojanX-gen [Trj]	BitDefender	Gen:Variant.Lazy.591993
Bkav Pro	W32.Common.73725D69	ClamAV	Win.Malware.Lazy-10030859-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Dll.trojan.warmcookie
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Siggen2.4881
Elastic	Windows.Trojan.WarmCookie	Emsisoft	Gen:Variant.Lazy.591993 (B)

For the .zip file I received the following:



26 / 65
Community Score -1

26/65 security vendors flagged this file as malicious

798563fc7600f7ef1a35996291a9dfb5f9902733404d499e2e736ea1dc6fc5
managements.zip

Size 2.64 MB Last Analysis Date 15 days ago

zip idle long-sleeps

Reanalyze Similar More

DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 4

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

Popular threat label trojan. Threat categories trojan downloader

Security vendors' analysis

Vendor	Detection	Vendor	Detection
Alibaba	TrojanDownloader.JS.Generic.f64a9e11	AliCloud	Trojan(downloader).Javascript/Wacatac...
ALYac	Trojan.GenericKD.74052307	Antiy-AVL	Trojan(Downloader)/JS.Agent
Arcabit	Trojan.Generic.D469F201	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	BitDefender	Trojan.GenericKD.74052097
CTX	Zip.trojan.wacatac	Emsisoft	Trojan.GenericKD.74052097 (B)
eScan	Trojan.GenericKD.74052097	ESET-NOD32	JS/TrojanDownloader.Agent.ABKZ
GData	Trojan.GenericKD.74052097	Google	Detected
Huorong	Trojan.GenericI928D4FD695038E52	Kaspersky	HEUR:Trojan-Downloader.Script.Generic
Kingsoft	Script.Trojan-Downloader.Generic.a	Lionic	Trojan.ZIP.Generic.atc

Do you want to automate checks?

As we can see, the results for .dll show that the file is associated with the WarmCookie malware, confirming we have correctly identified the malicious files. The results for the .zip file show that the malware is a Trojan. Lastly, I found the Windows username used on the infected machine by searching through Kerberos for the CNameString associated with the victim IP, and searched through the NBNS traffic for the name of the desktop that was infected .

The screenshot displays a Wireshark capture of network traffic from a file named '2024-08-15-traffic-analysis-exercise.pcap'. The filter applied is 'ip.addr == 10.8.15.133 && kerberos'. The packet list shows several Kerberos messages (TGS-REQ, TGS-REP, DCERPC, LDAP) and an SMB2 session setup request. The selected packet is a Kerberos TGS-REP (packet 1011), which is expanded to show its structure: a TGS-REP message with a CNameString field containing 'plucero'. The packet details pane also shows the 'enc-part' field. The packet bytes pane displays the raw hex and ASCII data for the selected packet. At the bottom, a summary bar indicates 'Bytes 184-1461: enc-part (kerberos.enc_part_element)' and 'Packets: 18189 · Displayed: 164 (0.9%)'. Below the main window, a table of NBNS traffic is visible, showing registration requests for 'DESKTOP-H8ALZBV' and 'LAFONTAINEBLEU'.

No.	Time	Source	Destination	Protocol	Length	Host	Info
1008	24.447787	10.8.15.133	10.8.15.4	KRB5	428		TGS-REQ
1011	24.448760	10.8.15.4	10.8.15.133	KRB5	405		TGS-REP
1017	24.449490	10.8.15.133	10.8.15.4	DCERPC	704		Alter_context: call
1019	24.450027	10.8.15.4	10.8.15.133	DCERPC	286		Alter_context_resp
1020	24.450220	10.8.15.133	10.8.15.4	DCERPC	274		Alter_context: call
1034	24.457884	10.8.15.133	10.8.15.4	LDAP	725		bindRequest(15) "<RO
1036	24.458725	10.8.15.4	10.8.15.133	LDAP	264		bindResponse(15) suc
1043	24.465129	10.8.15.133	10.8.15.4	LDAP	683		bindRequest(19) "<RO
1045	24.465850	10.8.15.4	10.8.15.133	LDAP	264		bindResponse(19) suc
1056	24.474711	10.8.15.133	10.8.15.4	KRB5	408		TGS-REQ
1059	24.475712	10.8.15.4	10.8.15.133	KRB5	381		TGS-REP
1068	24.476422	10.8.15.133	10.8.15.4	KRB5	201		TGS-REQ
1071	24.476871	10.8.15.4	10.8.15.133	KRB5	230		TGS-REP
1078	24.477427	10.8.15.133	10.8.15.4	SMB2	787		Session Setup Request

No.	Time	Source	Destination	Protocol	Length	Host	Info
30	0.437265	10.8.15.133	10.8.15.255	NBNS	110		Registration NB DESKTOP-H8ALZBV<00>
31	0.437739	10.8.15.133	10.8.15.255	NBNS	110		Registration NB LAFONTAINEBLEU<00>

Summary

Victim Details:

- Host Name: DESKTOP-H8ALZBV
- IP Address: 10.8.15.133
- MAC Address: 00:1c:bf:03:54:82
- Windows Username: plucero

Malicious IP Addresses:

- 72.5.43.29
- 104.21.55.70

Domain:

- quote[.]checkfedexp[.]com

Malware File Names:

- Invoice_876597035_003.zip
- 0f60a3e7baecf2748b1c8183ed37d1e4

Malware SHA-256 Hashes:

- DLL File:
b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6
- ZIP File:
798563fcf7600f7ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5