

Identify Host and the Client

With Kerberos.CNameString

kerberos.CNameString										
No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	CNameString	Info	
200	2024-08-15 00:09:46.122729	10.8.15.133	49684	10.8.15.4	88	KRB5	360	desktop-hbalzlv\$	S-REQ	
224	2024-08-15 00:09:46.133379	10.8.15.133	49687	10.8.15.4	88	KRB5	380	desktop-hbalzlv\$	S-REQ	
226	2024-08-15 00:09:46.134061	10.8.15.4	88	10.8.15.133	49686	KRB5	447	DESKTOP-HBALZBV\$	GS-REP	
228	2024-08-15 00:09:46.134977	10.8.15.4	88	10.8.15.133	49685	KRB5	477	DESKTOP-HBALZBV\$	GS-REP	
231	2024-08-15 00:09:46.134939	10.8.15.4	88	10.8.15.133	49687	KRB5	437	DESKTOP-HBALZBV\$	S-REP	
261	2024-08-15 00:09:46.153796	10.8.15.4	88	10.8.15.133	49688	KRB5	296	DESKTOP-HBALZBV\$	GS-REP	
264	2024-08-15 00:09:46.154217	10.8.15.4	88	10.8.15.133	49689	KRB5	477	DESKTOP-HBALZBV\$	GS-REP	
390	2024-08-15 00:09:46.347727	10.8.15.4	88	10.8.15.133	49694	KRB5	447	DESKTOP-HBALZBV\$	GS-REP	
493	2024-08-15 00:09:46.914545	10.8.15.4	88	10.8.15.133	49700	KRB5	396	DESKTOP-HBALZBV\$	GS-REP	
521	2024-08-15 00:09:46.976933	10.8.15.4	88	10.8.15.133	49702	KRB5	477	DESKTOP-HBALZBV\$	GS-REP	
533	2024-08-15 00:09:46.976922	10.8.15.4	88	10.8.15.133	49703	KRB5	281	DESKTOP-HBALZBV\$	GS-REP	
922	2024-08-15 00:09:54.933396	10.8.15.133	49714	10.8.15.4	88	KRB5	360	DESKTOP-HBALZBV\$	S-REQ	
930	2024-08-15 00:09:54.934916	10.8.15.133	49715	10.8.15.4	88	KRB5	387	DESKTOP-HBALZBV\$	S-REQ	
932	2024-08-15 00:09:54.935625	10.8.15.4	88	10.8.15.133	49715	KRB5	437	DESKTOP-HBALZBV\$	S-REQ	
944	2024-08-15 00:09:54.937913	10.8.15.4	88	10.8.15.133	49716	KRB5	377	DESKTOP-HBALZBV\$	GS-REP	
975	2024-08-15 00:10:08.106952	10.8.15.133	49717	10.8.15.4	88	KRB5	285	plucero	S-REQ	
983	2024-08-15 00:10:08.115612	10.8.15.133	49718	10.8.15.4	88	KRB5	368	plucero	S-REQ	
985	2024-08-15 00:10:08.116435	10.8.15.4	88	10.8.15.133	49718	KRB5	348	plucero	S-REP	
997	2024-08-15 00:10:08.118716	10.8.15.4	88	10.8.15.133	49719	KRB5	279	plucero	GS-REP	
1011	2024-08-15 00:10:08.253051	10.8.15.4	88	10.8.15.133	49720	KRB5	465	plucero	GS-REP	
1059	2024-08-15 00:10:08.280903	10.8.15.4	88	10.8.15.133	49723	KRB5	385	plucero	GS-REP	

Frame 533: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on Ethernet II, Src: Dell_8c:9c:4b (04:00:08:0c:9c:4b), Dst: Intel_03:54:82 (00:1c:bf:03:54:82)
Address: Intel_03:54:82 (00:1c:bf:03:54:82)

With LDAP

ldap contains "CN=Users"										
Source Port	Destination	Destination Port	Protocol	Length	CNameString	Info				
92	10.8.15.4	389	LDAP	214	SASL GSS-API Integrity: searchRequest(4) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" baseObject					
9	10.8.15.133	49828	LDAP	214	SASL GSS-API Integrity: searchResEntry(4) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" searchResDone(4) success [2 results]					
830	10.8.15.4	389	LDAP	236	SASL GSS-API Integrity: searchRequest(9) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" baseObject					
9	10.8.15.133	49830	LDAP	236	SASL GSS-API Integrity: searchResEntry(9) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" searchResDone(9) success [1 result]					
872	10.8.15.4	389	LDAP	214	SASL GSS-API Integrity: searchRequest(4) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" baseObject					
9	10.8.15.133	49872	LDAP	236	SASL GSS-API Integrity: searchResEntry(4) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" searchResDone(4) success [2 results]					
873	10.8.15.4	389	LDAP	214	SASL GSS-API Integrity: searchRequest(9) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" baseObject					
9	10.8.15.133	49873	LDAP	236	SASL GSS-API Integrity: searchResEntry(9) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" searchResDone(9) success [1 result]					
827	10.8.15.4	389	LDAP	214	SASL GSS-API Integrity: searchRequest(4) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" baseObject					
9	10.8.15.133	50027	LDAP	236	SASL GSS-API Integrity: searchResEntry(4) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" searchResDone(4) success [2 results]					
828	10.8.15.4	389	LDAP	214	SASL GSS-API Integrity: searchRequest(9) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" baseObject					
9	10.8.15.133	50028	LDAP	236	SASL GSS-API Integrity: searchResEntry(9) "CN=Pierce Lucero,CN=Users,DC=lafontainebleu,DC=org" searchResDone(9) success [1 result]					

Export the zip file.

File → Export Object → HTTP

Hostname					Content Type	All Content-Types
1	www.msfnconnecttest.com	text/plain	22 bytes	monoclient.zip		
2	quote.checkfreeexp.com	application/octet-stream	1,787 KB	monoclient.zip		
3	medge.b.tlu.delivery.mp.microsoft.com	application/x-chrome-extension	1,120 bytes	monoclient.zip		
4	medge.b.tlu.delivery.mp.microsoft.com	application/x-chrome-extension	1,340 bytes	monoclient.zip		
5	medge.b.tlu.delivery.mp.microsoft.com	application/x-chrome-extension	4,630 bytes	monoclient.zip		
6	medge.b.tlu.delivery.mp.microsoft.com	application/x-chrome-extension	7,930 bytes	monoclient.zip		
7	medge.b.tlu.delivery.mp.microsoft.com	application/x-chrome-extension	18 KB	monoclient.zip		
8	medge.b.tlu.delivery.mp.microsoft.com	application/x-chrome-extension	11 KB	monoclient.zip		
9	medge.b.tlu.delivery.mp.microsoft.com	application/x-chrome-extension	100 KB	monoclient.zip		
10	72.5.43.29	text/html	159 KB	monoclient.zip		
11	72.5.43.29	text/html	124 bytes	monoclient.zip		
12	72.5.43.29	text/html	94 bytes	monoclient.zip		
13	72.5.43.29	text/html	94 bytes	monoclient.zip		
14	72.5.43.29	text/html	94 bytes	monoclient.zip		
15	72.5.43.29	text/html	94 bytes	monoclient.zip		
16	72.5.43.29	text/html	94 bytes	monoclient.zip		
17	72.5.43.29	text/html	94 bytes	monoclient.zip		
18	72.5.43.29	text/html	94 bytes	monoclient.zip		
19	72.5.43.29	text/html	94 bytes	monoclient.zip		
20	72.5.43.29	text/html	94 bytes	monoclient.zip		
21	72.5.43.29	text/html	94 bytes	monoclient.zip		
22	72.5.43.29	text/html	94 bytes	monoclient.zip		
23	72.5.43.29	text/html	94 bytes	monoclient.zip		
24	72.5.43.29	text/html	94 bytes	monoclient.zip		
25	72.5.43.29	text/html	94 bytes	monoclient.zip		
26	72.5.43.29	text/html	94 bytes	monoclient.zip		
27	72.5.43.29	text/html	94 bytes	monoclient.zip		
28	72.5.43.29	text/html	94 bytes	monoclient.zip		
29	72.5.43.29	text/html	94 bytes	monoclient.zip		
30	72.5.43.29	text/html	94 bytes	monoclient.zip		
31	72.5.43.29	text/html	94 bytes	monoclient.zip		
32	72.5.43.29	text/html	94 bytes	monoclient.zip		
33	72.5.43.29	text/html	94 bytes	monoclient.zip		
34	72.5.43.29	text/html	94 bytes	monoclient.zip		
35	72.5.43.29	text/html	94 bytes	monoclient.zip		
36	72.5.43.29	text/html	94 bytes	monoclient.zip		
37	72.5.43.29	text/html	94 bytes	monoclient.zip		
38	72.5.43.29	text/html	94 bytes	monoclient.zip		
39	72.5.43.29	text/html	94 bytes	monoclient.zip		
40	72.5.43.29	text/html	94 bytes	monoclient.zip		
41	72.5.43.29	text/html	94 bytes	monoclient.zip		
42	72.5.43.29	text/html	94 bytes	monoclient.zip		
43	72.5.43.29	text/html	94 bytes	monoclient.zip		
44	72.5.43.29	text/html	94 bytes	monoclient.zip		
45	72.5.43.29	text/html	94 bytes	monoclient.zip		
46	72.5.43.29	text/html	94 bytes	monoclient.zip		
47	72.5.43.29	text/html	94 bytes	monoclient.zip		
48	72.5.43.29	text/html	94 bytes	monoclient.zip		
49	72.5.43.29	text/html	94 bytes	monoclient.zip		
50	72.5.43.29	text/html	94 bytes	monoclient.zip		
51	72.5.43.29	text/html	94 bytes	monoclient.zip		
52	72.5.43.29	text/html	94 bytes	monoclient.zip		
53	72.5.43.29	text/html	94 bytes	monoclient.zip		
54	72.5.43.29	text/html	94 bytes	monoclient.zip		
55	72.5.43.29	text/html	94 bytes	monoclient.zip		
56	72.5.43.29	text/html	94 bytes	monoclient.zip		
57	72.5.43.29	text/html	94 bytes	monoclient.zip		
58	72.5.43.29	text/html	94 bytes	monoclient.zip		
59	72.5.43.29	text/html	94 bytes	monoclient.zip		
60	72.5.43.29	text/html	94 bytes	monoclient.zip		
61	72.5.43.29	text/html	94 bytes	monoclient.zip		
62	72.5.43.29	text/html	94 bytes	monoclient.zip		
63	72.5.43.29	text/html	94 bytes	monoclient.zip		
64	72.5.43.29	text/html	94 bytes	monoclient.zip		
65	72.5.43.29	text/html	94 bytes	monoclient.zip		
66	72.5.43.29	text/html	94 bytes	monoclient.zip		
67	72.5.43.29	text/html	94 bytes	monoclient.zip		
68	72.5.43.29	text/html	94 bytes	monoclient.zip		
69	72.5.43.29	text/html	94 bytes	monoclient.zip		
70	72.5.43.29	text/html	94 bytes	monoclient.zip		
71	72.5.43.29	text/html	94 bytes	monoclient.zip		
72	72.5.43.29	text/html	94 bytes	monoclient.zip		
73	72.5.43.29	text/html	94 bytes	monoclient.zip		
74	72.5.43.29	text/html	94 bytes	monoclient.zip		
75	72.5.43.29	text/html	94 bytes	monoclient.zip		
76	72.5.43.29	text/html	94 bytes	monoclient.zip		
77	72.5.43.29	text/html	94 bytes	monoclient.zip		
78	72.5.43.29	text/html	94 bytes	monoclient.zip		
79	72.5.43.29	text/html	94 bytes	monoclient.zip		
80	72.5.43.29	text/html	94 bytes	monoclient.zip		
81	72.5.43.29	text/html	94 bytes	monoclient.zip		
82	72.5.43.29	text/html	94 bytes	monoclient.zip		
83	72.5.43.29	text/html	94 bytes	monoclient.zip		
84	72.5.43.29	text/html	94 bytes	monoclient.zip		
85	72.5.43.29	text/html	94 bytes	monoclient.zip		
86	72.5.43.29	text/html	94 bytes	monoclient.zip		
87	72.5.43.29	text/html	94 bytes	monoclient.zip		
88	72.5.43.29	text/html	94 bytes	monoclient.zip		
89	72.5.43.29	text/html	94 bytes	monoclient.zip		
90	72.5.43.29	text/html	94 bytes	monoclient.zip		
91	72.5.43.29	text/html	94 bytes	monoclient.zip		
92	72.5.43.29	text/html	94 bytes	monoclient.zip		
93	72.5.43.29	text/html	94 bytes	monoclient.zip		
94	72.5.43.29	text/html	94 bytes	monoclient.zip		
95	72.5.43.29	text/html	94 bytes	monoclient.zip		
96	72.5.43.29	text/html	94 bytes	monoclient.zip		
97	72.5.43.29	text/html	94 bytes	monoclient.zip		
98	72.5.43.29	text/html	94 bytes	monoclient.zip		
99	72.5.43.29	text/html	94 bytes	monoclient.zip		
100	72.5.43.29	text/html	94 bytes	monoclient.zip		

Save this file and export to your machine.

Extract the file type and hashes

```
saF-Lx@Saf-Ubuntu:~/Desktop/PCAP_Files$ file management$3f16533a25e45250a4f5d5&endeds=MIHQpQJ5tX=59bF050d37df88a9-ade43358-aa1220b-0571422b-0f33e6aa150e86baf0ed4&ld=9d7502d88d752a7b1d00587309184b5a215
management$3f16533a25e45250a4f5d5&endeds=MIHQpQJ5tX=59bF050d37df88a9-ade43358-aa1220b-0571422b-0f33e6aa150e86baf0ed4&ld=9d7502d88d752a7b1d00587309184b5a215
saF-Lx@Saf-Ubuntu:~/Desktop/PCAP_Files$
```

Shown above: File type is zip achieve data.

```
saf-lx@saf-Ubuntu:~/Desktop/PCAP Files$ sha256sum managements%3f16553a25e45250a41fd5&endeds=MIGpq&JS tx=59bf050d37df88a9-ade43358-eaa1220b-0571422b-0f33e6aa150e86bafd8ed4\&ld=9d7502d88d752a27b1d00587309184b5a215
798563cf76087ef1a35996291a9dfbf9902733404dd499e2e736e1dc6fc5 managements%3f16553a25e45250a41fd5&endeds=MIGpq&JS tx=59bf050d37df88a9-ade43358-eaa1220b-0571422b-0f33e6aa150e86bafd8ed4&ld=9d7502d88d752a27b1d00587309184b5a215
saf-lx@saf-Ubuntu:~/Desktop/PCAP Files$
```

Shown above: sha256 hash of the zip file

```
84b5a215 (2)$ sha256sum Invoice-876597035-003-8331775-8334138.js
dab98819d1d7677a60f5d06be210d45b74ae5fd8cf0c24ec1b3766e25ce6dc2c Invoice-876597035-003-8331775-8334138.js
saf-lx@saf-Ubuntu:~/Desktop/PCAP Files/managements%3f16553a25e45250a41fd5&endeds=MIGpq&JS tx=59bf050d37df88a9-ade43358-eaa1220b-0571422b-0f33e6aa150e86bafd8ed4&ld=9d7502d88d752a27b1d00587309184b5a215$
```

Shown above: sha256 hash of the js file inside zip file

```
saf-lx@saf-Ubuntu: ~
saf-lx@saf-Ubuntu:~/Desktop/PCAP Files$ file 0f60a3e7baecf2748b1c8183ed37d1e4
0f60a3e7baecf2748b1c8183ed37d1e4: PE32+ executable (DLL) (GUI) x86-64, for MS Windows, 7 sections
saf-lx@saf-Ubuntu:~/Desktop/PCAP Files$
```

Shown above: sha256 hash of the dll file

Copy the extracted hashes in **VirusTotal** and **MalwareBazaar**

19
/ 61
Community Score

19/61 security vendors flagged this file as malicious
Reanalyze Similar More
dab98819d1d7677a60f5d06be210d45b74ae5fd8cf0c24ec1b3766e25ce6dc2c
Invoice-876597035-003-8331775-8334138.js
Size 6.67 MB Last Analysis Date 4 months ago
text long-sleeps detect-debug-environment

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 5

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 Do you want to automate checks?

AhnLab-V3	Downloader/JS.WormCookie	AllCloud	Trojan(downloader);Multi/Generic.Gen
ALYac	Trojan.GenericKD.74052307	Antiy-AVL	Trojan[Downloader]/Script.Agent
Arcabit	Trojan.Generic.D469F2D3	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	BitDefender	Trojan.GenericKD.74052307
CTX	Txt.trojan.generic	Emsisoft	Trojan.GenericKD.74052307 (B) Press the PRINT SCREEN key to capture a screenshot
eScan	Trojan.GenericKD.74052307	GData	Trojan.GenericKD.74052307

798563cf76007ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5

24

Community Score

24/66 security vendors flagged this file as malicious

ReanalyzeSimilarMore

798563cf76007ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5

managements%3f16553a25e45250a41fd56endeds=MIGpg&JSbr=59b0f050d37df88a9-ade43358-aaa1220b-0571422b-0f33e...

Size2.64 MB

Last Analysis Date1 month ago

ZIP

zipidlelong sleeps

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY4

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

Popular threat labeltrojanThreat categoriestrojandownloader

Security vendors' analysisDo you want to automate checks?

AhnLab-V3	Downloader/JS.WormCookie	Alibaba	TrojanDownloader.JS/Generic.f64a9e11
AliCloud	Trojan[downloader].Javascript/Generic...	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.generic
Emnecore	Trojan.GenericKD.74053067 (B)	eScan	Trojan.GenericKD.74053067

b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6

58

Community Score

58/72 security vendors flagged this file as malicious

ReanalyzeSimilarMore

b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6

download.exe

Size155.50 KB

Last Analysis Date2 months ago

DDL

pe3264bitschecks cpu namelong sleepsdetect-debug environment

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY9

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

Popular threat labeltrojan.lazy/warmcookieThreat categoriestrojanFamily labelslazywarmcookieagentb

Security vendors' analysisDo you want to automate checks?

AhnLab-V3	Malware/Win.Generic.C5658894	Alibaba	Trojan.Win64/WarmCookie.3cded3e5
AliCloud	Trojan:Win/Agent_Agen.85Z	ALYac	GenVariant.Lazy.591993
Antiy-AVL	Trojan/Win64.Agentb	Arcabit	Trojan.Lazy.D90879
Arctic Wolf	Unsafe	Avast	Win64/MalwareX-gen [Trj]
AVG	Win64/MalwareX-gen [Trj]	BitDefender	GenVariant.Lazy.591993
Blau-Bin	Win32/Trj.Generic.T333CAB6	ClamAV	Win.MalwareX.gen.10030866.0

Shown above: VirusTotal Entry

Authenticate for API access | If you are experiencing issues with receiving data from abuse.ch platforms via API, please ensure your requests are authenticated. [Read here for more info](#)

MALWAREbazaar

BrowseUploadHunting AlertsAccess DataFAQAboutLogin

Submissions (past 24 hours)Most seen malware family (past 24 hours)Malware samples in corpus

Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tish hash, ClamAV signature, tag or malware family.

Browse Database

See search syntax see below, example: tag:TrickBot

Search

Search Syntax

Search:

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2024-08-15 03:23	b7aec5f73d2a6bbd8cd9...	exe	WarmCookie	backdoor exe warmcookie	IdaNotPro	

Showing 1 to 1 of 1 entries

Previous1Next

Shown above: MalwareBazaar Entry

The VirusTotal entry for this DLL, zip and js file indicates a crowd-sourced YARA rule identifies this as WarmCookie. The MalwareBazaar analysis of this file also identifies it as WarmCookie.