Pattern of Life

MetaCTF 2021

The Problem:

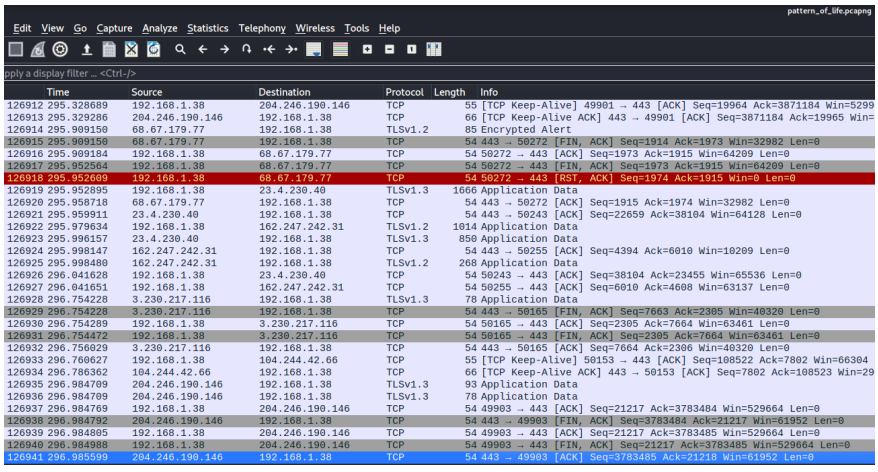
Hackers have breached our network. We know they are there, hiding in the shadows as users continue to browse the web like normal. As a threat hunter, your job is to constantly be searching our environment for any signs of malicious behavior.

Today you just received a packet capture (pcap) from a user's workstation. We think that an attacker may have compromised the user's machine and that the computer is beaconing out to their command and control (C2) server. Based on some other logs, we also think the attacker was *not* using a fully encrypted protocol and also did not put much care into making their C2 server look like a normal website. Your task? We'd like you to submit the port number that the C2 server is listening on in the form of MetaCTF{portnumber} as the flag.

The Solve:

We have got a big pcap file: *pattern_of_life.pcapng [121.6 MB]*

Read it with WireShark. We have 126941 rows.



	Time	Source	Destination	Protocol	Length	Info
126912	295.320689	192.168.1.38	204.246.190.146	TCP	55	[TCP Keep-Alive] 49901 → 443 [ACK] Seq=19964 Ack=3871184 Win=5299
126913	295.329286	204.246.190.146	192.168.1.38	TCP	66	[TCP Keep-Alive ACK] 443 → 49901 [ACK] Seq=3871184 Ack=19965 Win=
126914	295.909150	68.67.179.77	192.168.1.38	TLSv1.2	85	Encrypted Alert
126915	295.909150	68.67.179.77	192.168.1.38	TCP	54	443 → 50272 [FIN, ACK] Seq=1914 Ack=1973 Win=32982 Len=0
126916	295.909184	192.168.1.38	68.67.179.77	TCP	54	50272 → 443 [ACK] Seq=1973 Ack=1915 Win=64209 Len=0
126917	295.952564	192.168.1.38	68.67.179.77	TCP	54	50272 → 443 [FIN, ACK] Seq=1973 Ack=1915 Win=64209 Len=0
126918	295.952609	192.168.1.38	68.67.179.77	TCP	54	50272 → 443 [RST, ACK] Seq=1974 Ack=1915 Win=0 Len=0
126919	295.952895	192.168.1.38	23.4.230.40	TLSv1.3	1666	Application Data
126920	295.958718	68.67.179.77	192.168.1.38	TCP	54	443 → 50272 [ACK] Seq=1915 Ack=1974 Win=32982 Len=0
126921	295.959911	23.4.230.40	192.168.1.38	TCP	54	443 → 50243 [ACK] Seq=22659 Ack=38104 Win=64128 Len=0
126922	295.979634	192.168.1.38	162.247.242.31	TLSv1.2	1014	Application Data
126923	295.996157	23.4.230.40	192.168.1.38	TLSv1.3	850	Application Data
126924	295.998147	162.247.242.31	192.168.1.38	TCP	54	443 → 50255 [ACK] Seq=4394 Ack=6010 Win=10209 Len=0
126925	295.998480	162.247.242.31	192.168.1.38	TLSv1.2	268	Application Data
126926	296.041628	192.168.1.38	23.4.230.40	TCP	54	50243 → 443 [ACK] Seq=38104 Ack=23455 Win=65536 Len=0
126927	296.041651	192.168.1.38	162.247.242.31	TCP	54	50255 → 443 [ACK] Seq=6010 Ack=4608 Win=63137 Len=0
126928	296.754228	3.230.217.116	192.168.1.38	TLSv1.3	78	Application Data
126929	296.754228	3.230.217.116	192.168.1.38	TCP	54	443 → 50165 [FIN, ACK] Seq=7663 Ack=2305 Win=40320 Len=0
126930	296.754289	192.168.1.38	3.230.217.116	TCP	54	50165 → 443 [ACK] Seq=2305 Ack=7664 Win=63461 Len=0
126931	296.754472	192.168.1.38	3.230.217.116	TCP	54	50165 → 443 [FIN, ACK] Seq=2305 Ack=7664 Win=63461 Len=0
126932	296.756029	3.230.217.116	192.168.1.38	TCP	54	443 → 50165 [ACK] Seq=7664 Ack=2306 Win=40320 Len=0
126933	296.760627	192.168.1.38	104.244.42.66	TCP	55	[TCP Keep-Alive] 50153 → 443 [ACK] Seq=108522 Ack=7802 Win=66304
126934	296.786362	104.244.42.66	192.168.1.38	TCP	66	[TCP Keep-Alive ACK] 443 → 50153 [ACK] Seq=7802 Ack=108523 Win=29
126935	296.984709	204.246.190.146	192.168.1.38	TLSv1.3	93	Application Data
126936	296.984709	204.246.190.146	192.168.1.38	TLSv1.3	78	Application Data
126937	296.984769	192.168.1.38	204.246.190.146	TCP	54	49903 → 443 [ACK] Seq=21217 Ack=3783484 Win=529664 Len=0
126938	296.984792	204.246.190.146	192.168.1.38	TCP	54	443 → 49903 [FIN, ACK] Seq=3783484 Ack=21217 Win=61952 Len=0
126939	296.984805	192.168.1.38	204.246.190.146	TCP	54	49903 → 443 [ACK] Seq=21217 Ack=3783485 Win=529664 Len=0
126940	296.984988	192.168.1.38	204.246.190.146	TCP	54	49903 → 443 [FIN, ACK] Seq=21217 Ack=3783485 Win=529664 Len=0
126941	296.985599	204.246.190.146	192.168.1.38	TCP	54	443 → 49903 [ACK] Seq=3783485 Ack=21218 Win=61952 Len=0

Use filter following the instructions:

- browse the web
- *not* using a fully encrypted protocol
- did not put much care into making their C2 server look like a normal website

The applied filter:
http

http

No.	Time	Source	Destination	Protocol	Length	Info
7	0.097825	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1
9	0.099072	169.254.169.254	192.168.1.38	HTTP	311	HTTP/1.0 200 OK (text/plain)
112	4.451818	192.168.1.38	18.216.136.68	HTTP	492	GET / HTTP/1.1
114	4.463774	18.216.136.68	192.168.1.38	HTTP	389	HTTP/1.1 301 Moved Permanently (text/html)
16656	24.670551	192.168.1.38	52.44.115.131	HTTP	286	GET /en-us/index.html HTTP/1.1
16665	24.812251	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
35197	52.814087	192.168.1.38	52.44.115.131	HTTP	286	GET /en-us/index.html HTTP/1.1
35200	52.872926	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
36879	60.113018	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1
36881	60.114494	169.254.169.254	192.168.1.38	HTTP	311	HTTP/1.0 200 OK (text/plain)
38049	81.874121	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/docs.html HTTP/1.1
38090	81.917134	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
50243	110.923905	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/docs.html HTTP/1.1
50268	110.967155	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
50773	118.854940	192.168.1.38	146.75.33.164	HTTP	492	GET / HTTP/1.1
50775	118.856397	146.75.33.164	192.168.1.38	HTTP	609	HTTP/1.1 301 Moved Permanently
53685	120.113266	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1
53687	120.114825	169.254.169.254	192.168.1.38	HTTP	311	HTTP/1.0 200 OK (text/plain)
66650	138.969735	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/test.html HTTP/1.1
66652	139.072462	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
73468	169.073527	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/test.html HTTP/1.1
73470	169.150662	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
78156	180.123586	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1
78159	180.125558	169.254.169.254	192.168.1.38	HTTP	311	HTTP/1.0 200 OK (text/plain)
89373	201.366762	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/docs.html HTTP/1.1
89375	201.406589	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
96528	211.507607	192.168.1.38	72.21.91.29	HTTP	287	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQ
96541	211.529853	72.21.91.29	192.168.1.38	OCSP	853	Response
99340	231.425769	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/test.html HTTP/1.1
99342	231.489524	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
100058	240.125922	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1

Find the first row what looks like a server-client communication:

http

No.	Time	Source	Destination	Protocol	Length	Info
7	0.097825	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1
9	0.099072	169.254.169.254	192.168.1.38	HTTP	311	HTTP/1.0 200 OK (text/plain)
112	4.451818	192.168.1.38	18.216.136.68	HTTP	492	GET / HTTP/1.1
114	4.463774	18.216.136.68	192.168.1.38	HTTP	389	HTTP/1.1 301 Moved Permanently (text/html)
16656	24.670551	192.168.1.38	52.44.115.131	HTTP	286	GET /en-us/index.html HTTP/1.1
16665	24.812251	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
35197	52.814087	192.168.1.38	52.44.115.131	HTTP	286	GET /en-us/index.html HTTP/1.1
35200	52.872926	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
36879	60.113018	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1
36881	60.114494	169.254.169.254	192.168.1.38	HTTP	311	HTTP/1.0 200 OK (text/plain)
38049	81.874121	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/docs.html HTTP/1.1
38090	81.917134	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
50243	110.923905	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/docs.html HTTP/1.1
50268	110.967155	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
50773	118.854940	192.168.1.38	146.75.33.164	HTTP	492	GET / HTTP/1.1
50775	118.856397	146.75.33.164	192.168.1.38	HTTP	609	HTTP/1.1 301 Moved Permanently
53685	120.113266	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1
53687	120.114825	169.254.169.254	192.168.1.38	HTTP	311	HTTP/1.0 200 OK (text/plain)
66650	138.969735	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/test.html HTTP/1.1
66652	139.072462	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
73468	169.073527	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/test.html HTTP/1.1
73470	169.150662	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
78156	180.123586	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1
78159	180.125558	169.254.169.254	192.168.1.38	HTTP	311	HTTP/1.0 200 OK (text/plain)
89373	201.366762	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/docs.html HTTP/1.1
89375	201.406589	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
96528	211.507607	192.168.1.38	72.21.91.29	HTTP	287	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZP
96541	211.529853	72.21.91.29	192.168.1.38	OCSP	853	Response
99340	231.425769	192.168.1.38	52.44.115.131	HTTP	285	GET /en-us/test.html HTTP/1.1
99342	231.489524	52.44.115.131	192.168.1.38	HTTP	366	HTTP/1.1 200 OK (text/plain)
100058	240.125922	192.168.1.38	169.254.169.254	HTTP	235	GET /latest/meta-data/instance-action HTTP/1.1

```
▸ Frame 16656: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface \Device\NPF_{0D80B415-918B-4238-94C4-529
▸ Ethernet II, Src: 12:66:8a:76:b3:f9 (12:66:8a:76:b3:f9), Dst: 12:c1:4b:44:ca:76 (12:c1:4b:44:ca:76)
▸ Internet Protocol Version 4, Src: 192.168.1.38, Dst: 52.44.115.131
▾ Transmission Control Protocol, Src Port: 49694, Dst Port: 8080, Seq: 1, Ack: 1, Len: 232
    Source Port: 49694
    Destination Port: 8080
```

Candidate 8080 Destination port by as unusual behavior.

Lucky a first find, it must to be investigate.

Use Follow the HTTP stream function:

It looks like the conditions. Continuous beaconing with different filenames (*beaconing out to their command and control (C2) server*).

That is enough to Proof and the accepted flag is:
MetaCTF{8080}