*PCAP

Detection and Response Analyst Task

Detected & Reported by,

Bharani Moorthy.

Contents

The Big Picture

This report is about the static analysis and intuitive findings of all traffic behaviour that would indicate a compromise or an anomaly on the network in the .pcap file. I used Wireshark, a packet capturing tool to analyse the PCAP file. PCAP means “Packet Capture”, as its name says, this kind of file contains complete packet going through a network interface. Complete packet means that PCAP files will contain data from **second to the seventh layer** of the OSI model, excluding the physical layer.

Before inspecting the elements, I started to see the Protocol hierarchy statistics (dashboard) to get an overall Protocols which involved during this traffic and started my analysis from the maximum percentage of traffic flow.

Wireshark · Protocol Hierarchy Statistics · DetectResponse_HomeTask.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	88892	100.0	61890887	1379 k	0	0	0
Ethernet	100.0	88892	2.0	1244488	27 k	0	0	0
Internet Protocol Version 6	0.2	139	0.0	5560	123	0	0	0
User Datagram Protocol	0.1	112	0.0	896	19	0	0	0
Domain Name System	0.1	112	0.0	5780	128	112	5780	128
Internet Control Message Protocol v6	0.0	27	0.0	1175	26	27	1175	26
Internet Protocol Version 4	99.7	88667	2.9	1773340	39 k	0	0	0
User Datagram Protocol	61.5	54699	0.7	437592	9753	0	0	0
WireGuard Protocol	13.0	11595	26.3	16274373	362 k	11504	16266502	362 k
Malformed Packet	0.1	91	0.0	0	0	91	0	0
Simple Service Discovery Protocol	0.0	12	0.0	1992	44	12	1992	44
Network Time Protocol	0.0	22	0.0	1056	23	22	1056	23
Domain Name System	0.8	681	0.1	46239	1030	681	46239	1030
Data	47.7	42389	35.3	21838523	486 k	42389	21838523	486 k
Transmission Control Protocol	38.2	33921	32.6	20191991	450 k	24618	4262093	94 k
Transport Layer Security	3.6	3207	19.8	12268190	273 k	2897	10895647	242 k
Hypertext Transfer Protocol	0.2	136	0.3	185486	4134	53	13517	301
Portable Network Graphics	0.0	1	0.0	681	15	1	903	20
Online Certificate Status Protocol	0.1	56	0.0	24173	538	56	24173	538
Line-based text data	0.0	21	0.2	107518	2396	21	109014	2429
JavaScript Object Notation	0.0	3	0.0	2033	45	3	2845	63
HTML Form URL Encoded	0.0	2	0.0	9013	200	2	9186	204
Data	6.9	6155	12.2	7551567	168 k	6155	7551567	168 k
BitTorrent	0.1	115	0.0	19882	443	114	19288	429
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Internet Control Message Protocol	0.1	47	0.0	2003	44	47	2003	44
Address Resolution Protocol	0.1	86	0.0	3218	71	86	3218	71

No display filter.

Close Copy Help

Additionally, the complete traffic was captured in 4th Feb 2020, Starting 03:00:16 to 03:06:03 (6 minutes traffic).

1. VPN Activity:

The entire network traffic was happened via VPN network, the provider named Wire guard – it is an open and free software application, by checking the VPN user and login attempt logs whether this traffic is legitimate.

No.	Time	Source	Sender IP address	Destination	Source Pc	Destination	Protocol
1	2020-02-04 03:00:04.943389	94.74.218.102		192.168.10.104	52956	51413	WireGuard
2	2020-02-04 03:00:04.944369	94.74.218.102		192.168.10.104	52956	51413	WireGuard

It was initiated from Czech republic , if it is static public IP.

IP Information for 94.74.218.102

Quick Stats

IP Location	Czechia Olomouc Nej.cz S.r.o.
ASN	AS16246 AS16246 Internet Provider, CZ (registered Feb 07, 2001)
Resolve Host	94-74-218-102.client.rionet.cz
Whois Server	whois.ripe.net
IP Address	94.74.218.102

2. ARP Traffic analysis:

By examining the ARP traffic, I can say, these are IP's list -192.168.10.1, 192.168.10.104, 192.168.10.116, 192.168.10.124 and 192.168.10.205 where the communication happened inside the LAN, also to confirm there is **no duplicate** packets / mac addresses that reflect there is no ARP Spoofing.

arp

No.	Time	Source	Sender IP address	Destination	Source Pc	Destination	Protocol	Length	Host	Response In	Info
66321	2020-02-04 03:04:47.172207	PcsCompu_ec:51:29	192.168.10.1	PcsCompu_0b:17:ba			ARP	42			Who has 192.168.10.205? Tell 192.168.10.1
57417	2020-02-04 03:04:18.132193	PcsCompu_ec:51:29	192.168.10.1	PcsCompu_0b:17:ba			ARP	42			Who has 192.168.10.205? Tell 192.168.10.1
49968	2020-02-04 03:03:39.492235	PcsCompu_ec:51:29	192.168.10.1	PcsCompu_0b:17:ba			ARP	42			Who has 192.168.10.205? Tell 192.168.10.1
26352	2020-02-04 03:01:56.852178	PcsCompu_ec:51:29	192.168.10.1	PcsCompu_0b:17:ba			ARP	42			Who has 192.168.10.205? Tell 192.168.10.1
17833	2020-02-04 03:01:26.132185	PcsCompu_ec:51:29	192.168.10.1	PcsCompu_0b:17:ba			ARP	42			Who has 192.168.10.205? Tell 192.168.10.1
10990	2020-02-04 03:00:55.413548	PcsCompu_ec:51:29	192.168.10.1	PcsCompu_0b:17:ba			ARP	42			Who has 192.168.10.205? Tell 192.168.10.1
57491	2020-02-04 03:04:18.233773	PcsCompu_0b:17:ba	192.168.10.205	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.205
47136	2020-02-04 03:03:34.447432	PcsCompu_0b:17:ba	192.168.10.205	Broadcast			ARP	60			Who has 192.168.10.1? Tell 192.168.10.205
26378	2020-02-04 03:01:56.921728	PcsCompu_0b:17:ba	192.168.10.205	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.205
17852	2020-02-04 03:01:26.201665	PcsCompu_0b:17:ba	192.168.10.205	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.205
11005	2020-02-04 03:00:55.482054	PcsCompu_0b:17:ba	192.168.10.205	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.205
4968	2020-02-04 03:00:24.249932	PcsCompu_0b:17:ba	192.168.10.205	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.205
41915	2020-02-04 03:03:07.990792	PcsCompu_f3:62:71	192.168.10.124	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.124
34040	2020-02-04 03:02:34.710743	PcsCompu_f3:62:71	192.168.10.124	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.124
74427	2020-02-04 03:05:17.439058	PcsCompu_f1:97:15	192.168.10.116	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.116
35719	2020-02-04 03:02:42.040473	PcsCompu_f1:97:15	192.168.10.116	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.116
29578	2020-02-04 03:02:11.576258	PcsCompu_f1:97:15	192.168.10.116	PcsCompu_ec:51:29			ARP	60			Who has 192.168.10.1? Tell 192.168.10.116
4173	2020-02-04 03:00:21.156098	PcsCompu_77:86:98	192.168.10.104	PcsCompu_f3:62:71			ARP	60			Who has 192.168.10.124? Tell 192.168.10.104

3.Remote Login Communication:

There is an initiation of outbound remote desktop protocol communication, someone from the Host **192.168.10.104** has initiated an RDP connection (Port 3389) to the IP -189.103.169.65 that is in Brazil.

tcp.port == 3389

No.	Time	Source	Sender IP address	Destination	Source Pc	Destination	Protocol	Length	Host	Response In	Info
1814	2020-02-04 03:00:12.759722	192.168.10.104		189.103.169.65	33857	3389	TCP	60			33857 → 3389 [FIN, ACK] Seq=1
1820	2020-02-04 03:00:12.764153	189.103.169.65		192.168.10.104	3389	33857	TCP	54			3389 → 33857 [ACK] Seq=1 Ack=2
1878	2020-02-04 03:00:13.123752	189.103.169.65		192.168.10.104	3389	33857	TCP	54			3389 → 33857 [RST, ACK] Seq=1
16142	2020-02-04 03:01:21.016021	192.168.10.104		189.103.169.65	43087	3389	TCP	74			43087 → 3389 [SYN] Seq=0 Win=2
16307	2020-02-04 03:01:21.340272	189.103.169.65		192.168.10.104	3389	43087	TCP	58			3389 → 43087 [SYN, ACK] Seq=0
16311	2020-02-04 03:01:21.340461	192.168.10.104		189.103.169.65	43087	3389	TCP	60			43087 → 3389 [ACK] Seq=1 Ack=1
16442	2020-02-04 03:01:21.505692	192.168.10.104		189.103.169.65	43087	3389	SSL	478			Continuation Data
16448	2020-02-04 03:01:21.509390	189.103.169.65		192.168.10.104	3389	43087	TCP	54			3389 → 43087 [ACK] Seq=1 Ack=4
16539	2020-02-04 03:01:21.828996	189.103.169.65		192.168.10.104	3389	43087	TCP	54			3389 → 43087 [RST, ACK] Seq=1

Besides, I find some drop of packets when RDP establishment.

IP Information for 189.103.169.65

Quick Stats

IP Location	Brazil Piracicaba Claro S.a.
ASN	AS28573 CLARO S.A., BR (registered Nov 27, 2003)
Resolve Host	bd67a941.virtua.com.br
Whois Server	whois.lacnic.net
IP Address	189.103.169.65

Recommendation:

- Should check this remote connection was legitimate.

4.SSH initiation:

The User from the host **192.165.10.205** tried to login remotely to the IP 120.203.25.58, which is located at china, also it was dropped, it seems suspicious.

tcp.port == 22

No.	Time	Source	Sender IP address	Destination	Source Pc	Destination	Protocol	Length	Host	Response In	Info
47171	2020-02-04 03:03:34.475878	192.168.10.205		192.168.10.1	64446	22	TCP	60			64446 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=
47172	2020-02-04 03:03:34.475895	192.168.10.1		192.168.10.205	22	64446	TCP	58			22 → 64446 [SYN, ACK] Seq=0 Ack=1 Win=2920
47173	2020-02-04 03:03:34.476084	192.168.10.205		192.168.10.1	64446	22	TCP	60			64446 → 22 [RST] Seq=1 Win=0 Len=0
59874	2020-02-04 03:04:26.843446	192.168.10.205		120.203.25.58	41936	22	TCP	74			41936 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS
59927	2020-02-04 03:04:27.143483	192.168.10.205		120.203.25.58	41974	22	TCP	74			41974 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS
59936	2020-02-04 03:04:27.182301	120.203.25.58		192.168.10.205	22	41936	TCP	58			22 → 41936 [SYN, ACK] Seq=0 Ack=1 Win=6553
59937	2020-02-04 03:04:27.182693	192.168.10.205		120.203.25.58	41936	22	TCP	60			41936 → 22 [RST] Seq=1 Win=0 Len=0
60388	2020-02-04 03:04:28.501837	120.203.25.58		192.168.10.205	22	41974	TCP	58			22 → 41974 [SYN, ACK] Seq=0 Ack=1 Win=6553
60412	2020-02-04 03:04:28.504062	192.168.10.205		120.203.25.58	41974	22	TCP	60			41974 → 22 [RST] Seq=1 Win=0 Len=0
63724	2020-02-04 03:04:43.360118	192.168.10.205		1.1.1.1	51422	22	TCP	74			51422 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS
63732	2020-02-04 03:04:43.433200	192.168.10.205		1.1.1.1	51438	22	TCP	74			51438 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS

IP Information for 120.203.25.58

Quick Stats

IP Location	China Nanchang China Mobile Communications Corporation
ASN	AS9808 CMNET-GD Guangdong Mobile Communication Co.Ltd., CN (registered Jan 10, 2000)
Whois Server	whois.apnic.net
IP Address	120.203.25.58

5.Tracking down the BitTorrent:

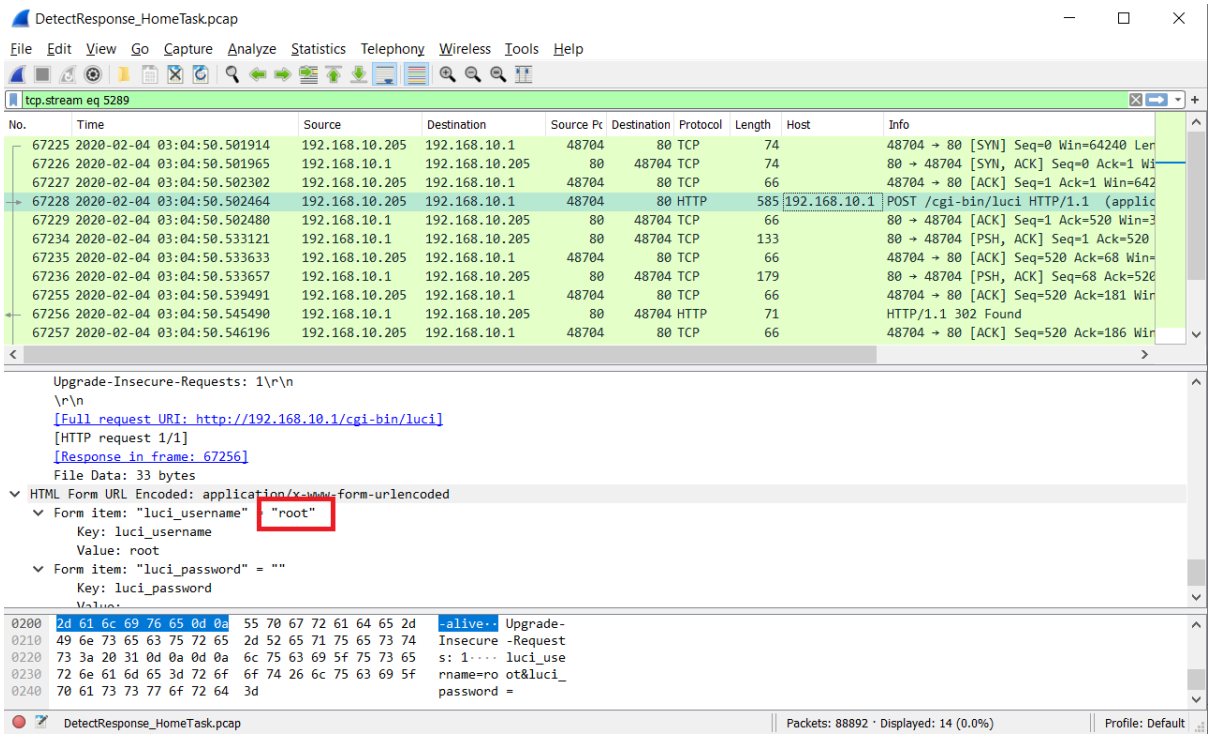
I am observing that there is an evidence of peer-to-peer communication, BitTorrent happened in this traffic, we need to find out who is using this communication and whether the traffic is legitimate.it was raised from **192.168.10.104**.

bittorrent

No.	Time	Source	Source Port	Sender IP address	Destination	Destination Po	Protocol	Info
24532	2020-02-04 03:01:50.626561	192.168.10.104	49929		202.133.5.81	7772	BitTorrent	Handshake
24618	2020-02-04 03:01:51.126612	192.168.10.104	55641		187.26.209.81	54372	BitTorrent	Handshake
26597	2020-02-04 03:01:57.267466	192.168.10.104	46947		170.83.37.108	8999	BitTorrent	Handshake
27482	2020-02-04 03:02:01.665795	192.168.10.104	50083		122.116.118.43	6881	BitTorrent	Continuation data
27546	2020-02-04 03:02:02.142723	122.116.118.43	6881		192.168.10.104	50083	BitTorrent	Bitfield[Malformed Packet]
27549	2020-02-04 03:02:02.164275	192.168.10.104	50083		122.116.118.43	6881	BitTorrent	Continuation data
28159	2020-02-04 03:02:05.167742	192.168.10.104	52609		185.98.164.106	1024	BitTorrent	Handshake
35528	2020-02-04 03:02:41.240636	192.168.10.104	38887		1.9.12.26	6881	BitTorrent	Continuation data
35553	2020-02-04 03:02:41.444026	192.168.10.104	42295		170.83.37.6	8999	BitTorrent	Handshake
35563	2020-02-04 03:02:41.570285	192.168.10.104	53673		101.118.158.167	34206	BitTorrent	Handshake
35883	2020-02-04 03:02:42.242083	192.168.10.104	56205		65.49.126.172	59909	BitTorrent	Handshake
36054	2020-02-04 03:02:43.069679	192.168.10.104	38057		101.118.158.39	33950	BitTorrent	Handshake
36500	2020-02-04 03:02:44.744858	192.168.10.104	38073		79.106.209.170	6881	BitTorrent	Continuation data
36607	2020-02-04 03:02:45.747244	192.168.10.104	56109		62.44.138.102	6881	BitTorrent	Continuation data
36610	2020-02-04 03:02:45.747302	192.168.10.104	55059		185.203.118.36	6881	BitTorrent	Continuation data
36943	2020-02-04 03:02:46.247179	192.168.10.104	37915		65.49.14.171	41659	BitTorrent	Handshake
37003	2020-02-04 03:02:46.474056	192.168.10.104	38379		120.23.177.71	38848	BitTorrent	Handshake
37112	2020-02-04 03:02:47.122013	192.168.10.104	51641		101.118.158.55	33958	BitTorrent	Handshake
38677	2020-02-04 03:02:52.262740	192.168.10.104	44333		89.108.84.43	51417	BitTorrent	Handshake
38846	2020-02-04 03:02:53.010555	192.168.10.104	45415		120.23.177.87	38856	BitTorrent	Handshake
39114	2020-02-04 03:02:54.613594	192.168.10.104	36079		187.26.209.75	1	BitTorrent	Handshake
39222	2020-02-04 03:02:54.819231	192.168.10.104	47825		187.44.129.30	8999	BitTorrent	Handshake
41000	2020-02-04 03:03:03.314562	192.168.10.104	45257		166.249.93.10	6881	BitTorrent	Continuation data
41047	2020-02-04 03:03:03.815365	192.168.10.104	53175		178.254.226.28	6881	BitTorrent	Have None
44776	2020-02-04 03:03:21.375621	192.168.10.104	54227		178.217.31.157	6881	BitTorrent	Continuation data
44805	2020-02-04 03:03:21.544076	192.168.10.104	58569		202.133.5.81	7772	BitTorrent	Handshake
44821	2020-02-04 03:03:21.628465	178.217.31.157	6881		192.168.10.104	54227	BitTorrent	Continuation data
44839	2020-02-04 03:03:21.871440	192.168.10.104	54227		178.217.31.157	6881	BitTorrent	Continuation data
45163	2020-02-04 03:03:22.375680	192.168.10.104	38955		178.217.31.157	6881	BitTorrent	Allowed Fast, Piece (Idx:0xc44314f2)

6.Anomalies in Privileged User Account Activity:

By examining the http traffic, the end-user from the host **192.168.10.205** tried to access the Router (OPENWrt) 192.168.10.1 as a privileged user account **root**, is can be seen in payload.

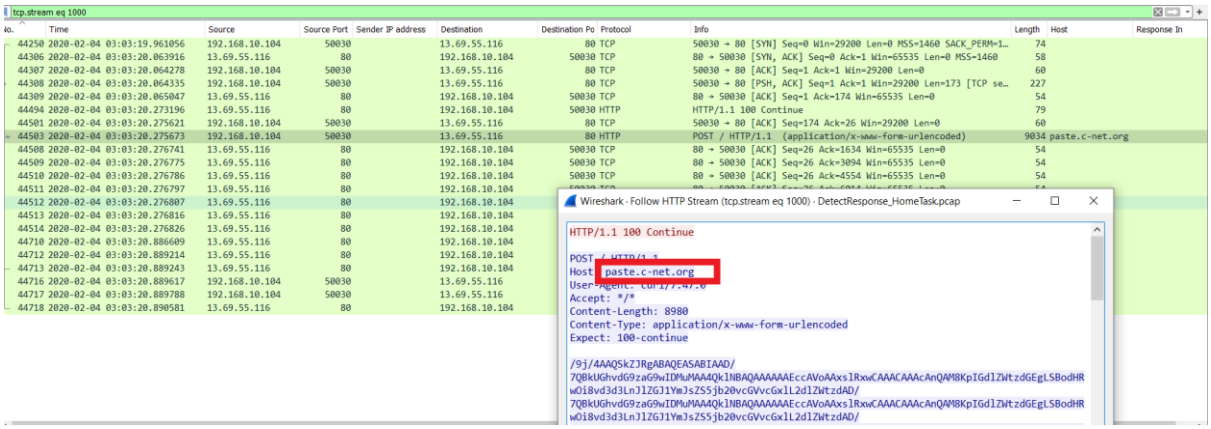


If the end-user might be hacker and he get a control of the router, it leads to stealing our personal information, redirecting to fake websites, upload malware, or even use our network to attack other networks.

Remediation: Monitor the privileged user group is essential and necessary steps must be taken if any unauthorised access.

7. Paste bin Vulnerability:

There is an indication that the text copy has happened of size >9kb, from the user **192.168.10.104** to the IP 13.69.55.116 via past-bin utility.



Geolocation data from IP2Location (Product: DB6, updated on 2020-7-1)

IP Address	Country	Region	City
13.69.55.116	Netherlands	Noord-Holland	Amsterdam
ISP	**Organization**	**Latitude**	**Longitude**
Microsoft Corporation	Not Available	52.3740	4.8897

Since the data breach and IRC bot vulnerability, it is advisable to not use paste bin and **blacklisted** in most of the organisation.

8. Authentication Logs:

I am observing the below are the list of sources has authenticated to the machine and there is drop of authentication which has been initiated by the machine **192.168.10.205 to** router 192.168.10.1.

No.	Time	Source	Source Port	Sender IP address	Destination	Destination Po	Protocol	Info
47140	2020-02-04 …	192.168.10.205	64446		192.168.10.1	113	TCP	64446 → 113 [SYN] Seq=0 Win=1024
47141	2020-02-04 …	192.168.10.1	113		192.168.10.205	64446	TCP	113 → 64446 [RST, ACK] Seq=1 Ack=
59861	2020-02-04 …	192.168.10.205	33176		120.203.25.58	113	TCP	33176 → 113 [SYN] Seq=0 Win=64240
59915	2020-02-04 …	192.168.10.205	33212		120.203.25.58	113	TCP	33212 → 113 [SYN] Seq=0 Win=64240
63373	2020-02-04 …	192.168.10.205	53926		1.1.1.1	113	TCP	53926 → 113 [SYN] Seq=0 Win=64240
63704	2020-02-04 …	192.168.10.205	53926		1.1.1.1	113	TCP	[TCP Retransmission] 53926 → 113
63717	2020-02-04 …	192.168.10.205	53946		1.1.1.1	113	TCP	53946 → 113 [SYN] Seq=0 Win=64240

9. PING SCAN:

I am seeing that there is a ping scan has been initiated by the source 10.0.3.2 , the IP is not in the LAN , also the destination is not replied to the host , most of the cases the Ping response is disabled.

Might be suspicious, someone might initiate Ping scan to check whether the other end host is Alive.

icmp.code == 2

No.	Time	Source	Sender IP address	Destination	Source Pc	Destination	Protocol	Length	Host	Response In	Info
770	2020-02-04 03:00:08.717146	10.0.3.2		192.168.10.104	45881	47056	ICMP	70			Destination unreachable (Host unreachable)
1924	2020-02-04 03:00:13.583467	10.0.3.2		192.168.10.104	55491	14082	ICMP	70			Destination unreachable (Host unreachable)
2414	2020-02-04 03:00:15.175939	10.0.3.2		192.168.10.104	59065	14082	ICMP	70			Destination unreachable (Host unreachable)
18094	2020-02-04 03:01:27.297171	10.0.3.2		192.168.10.104	60535	62094	ICMP	70			Destination unreachable (Host unreachable)
18169	2020-02-04 03:01:27.777588	10.0.3.2		192.168.10.104	35127	62094	ICMP	70			Destination unreachable (Host unreachable)
24049	2020-02-04 03:01:48.627622	10.0.3.2		192.168.10.104	51413	51413	ICMP	70			Destination unreachable (Network unreachable)
24686	2020-02-04 03:01:51.657569	10.0.3.2		192.168.10.104	51413	51413	ICMP	70			Destination unreachable (Network unreachable)
36084	2020-02-04 03:02:43.250528	10.0.3.2		192.168.10.104	51413	51413	ICMP	70			Destination unreachable (Network unreachable)
36964	2020-02-04 03:02:46.271966	10.0.3.2		192.168.10.104	51413	51413	ICMP	70			Destination unreachable (Network unreachable)
44791	2020-02-04 03:03:21.471505	10.0.3.2		192.168.10.104	51211	11886	ICMP	70			Destination unreachable (Host unreachable)
45394	2020-02-04 03:03:24.541048	10.0.3.2		192.168.10.104	38273	11886	ICMP	70			Destination unreachable (Host unreachable)
57660	2020-02-04 03:04:19.234580	10.0.3.2		192.168.10.104	43219	62094	ICMP	70			Destination unreachable (Host unreachable)
57717	2020-02-04 03:04:19.736758	10.0.3.2		192.168.10.104	47885	62094	ICMP	70			Destination unreachable (Host unreachable)
59538	2020-02-04 03:04:26.266471	10.0.3.2		192.168.10.104	59203	12498	ICMP	70			Destination unreachable (Host unreachable)
59852	2020-02-04 03:04:26.746469	10.0.3.2		192.168.10.104	42841	12498	ICMP	70			Destination unreachable (Host unreachable)
63949	2020-02-04 03:04:44.020066	10.0.3.2		192.168.10.104	51413	51413	ICMP	70			Destination unreachable (Network unreachable)
66159	2020-02-04 03:04:47.029976	10.0.3.2		192.168.10.104	51413	51413	ICMP	70			Destination unreachable (Network unreachable)
67402	2020-02-04 03:04:51.335016	10.0.3.2		192.168.10.104	38691	62287	ICMP	70			Destination unreachable (Host unreachable)
67540	2020-02-04 03:04:51.784633	10.0.3.2		192.168.10.104	40741	62287	ICMP	70			Destination unreachable (Host unreachable)
69931	2020-02-04 03:04:59.277168	10.0.3.2		192.168.10.104	57803	27001	ICMP	70			Destination unreachable (Host unreachable)
71075	2020-02-04 03:05:04.897761	10.0.3.2		192.168.10.104	35577	25889	ICMP	70			Destination unreachable (Host unreachable)
71564	2020-02-04 03:05:06.935918	10.0.3.2		192.168.10.104	57551	27001	ICMP	70			Destination unreachable (Host unreachable)
84485	2020-02-04 03:05:48.050565	10.0.3.2		192.168.10.104	32875	47056	ICMP	70			Destination unreachable (Host unreachable)
84591	2020-02-04 03:05:48.548805	10.0.3.2		192.168.10.104	45127	47056	ICMP	70			Destination unreachable (Host unreachable)
85643	2020-02-04 03:05:51.707904	10.0.3.2		192.168.10.104	51413	51413	ICMP	70			Destination unreachable (Network unreachable)
86202	2020-02-04 03:05:54.740326	10.0.3.2		192.168.10.104	51413	51413	ICMP	70			Destination unreachable (Network unreachable)
62359	2020-02-04 03:04:36.867051	180.247.243.102		192.168.10.104	51413	21993	ICMP	100			Destination unreachable (Port unreachable)

10.Abnormal traffic:

About **87 percent** of the total traffic in the Pcap file has been raised from the host IP **192.168.10.104**, also there is some abnormal traffic patterns such as illegal characters found in the header, a duplicate TCP packet a lot of outbound and inbound communication to public IP address has happened.

Source	Source Port	Sender IP address	Destination	Destination Po	Protocol	Unknown header
192.168.10.104	54643		201.20.70.245	8080	TCP	(\9\0\0/1\021t\tC\0Vzr\0:nn\0\0I\0#\0\021\0\034\0-\035}\0\0A\005oY\0\0\3\n
192.168.10.104	38537		177.75.21.186	8080	TCP	;\0\0\7-\0u5k\0\0y_\0\020'C\0:\0\0\0TSoS;\0\0\7h\0s\0u\v\0\0\0\1\017\0\0QN~k\0\0\023YGU\0\0\0\0\0cC\0\1\0s&\0\0\0\0v\035\0\0\0\0\0\0N,\027E\0E\0\032\0@\0
192.168.10.104	52797		201.20.70.245	8080	TCP	kG\0\0\t\f.\0o\0\017\003%\0H\0X\f\0\006\027&,\0\a\0T\0\0\0\0"+\024:Wa\023|\026Vj\0NM\0\0\0\0\027-

Some predictions,

- The traffic flow was happened in the Cloudflare DNS - 1.1.1.1,
- 192.168.10.1 – Router
- 192.168.10.104- Suspicious Host – need to check the behaviour
- 192.168.10.205- Suspicious Host – need to check the behaviour

Besides, I checked the hash file of Html objects .jar file and executables, downloaded in Export object in Virus total , it is predicted to be Clean.

Conclusion:

By defining and creating the use cases and rules for the above found animalities and below warnings in the SIEM and investigating the user behavioural pattern can increase the security on the network.

Wireshark · Expert Information · DetectResponse_HomeTask.pcap

Severity	Summary	Group	Protocol	Count
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	12
Note	ACK to a TCP keep-alive segment	Sequence	TCP	201
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	30
Error	Malformed Packet (Exception occurred)	Malformed	WireGuard	91
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	4
Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP	45
Warning	Connection reset (RST)	Sequence	TCP	481
Warning	Illegal characters found in header name	Protocol	HTTP	3
Note	TCP keep-alive segment	Sequence	TCP	203
Note	Duplicate ACK (#1)	Sequence	TCP	87
Note	This frame is a (suspected) retransmission	Sequence	TCP	440
Chat	TCP window update	Sequence	TCP	2
Chat	GET /info.php HTTP/1.1\r\n	Sequence	HTTP	133
Note	A new tcp session is started with the same ports as an earlier session in this trace	Sequence	TCP	1
Chat	Connection finish (FIN)	Sequence	TCP	1938
Chat	Connection establish acknowledge (SYN+ACK): server port 26269	Sequence	TCP	1481
Chat	Connection establish request (SYN): server port 51586	Sequence	TCP	6067

No display filter set.

References:

- https://www.wireshark.org/
- https://osintframework.com/
- https://mxtoolbox.com/
- https://www.virustotal.com/

The end