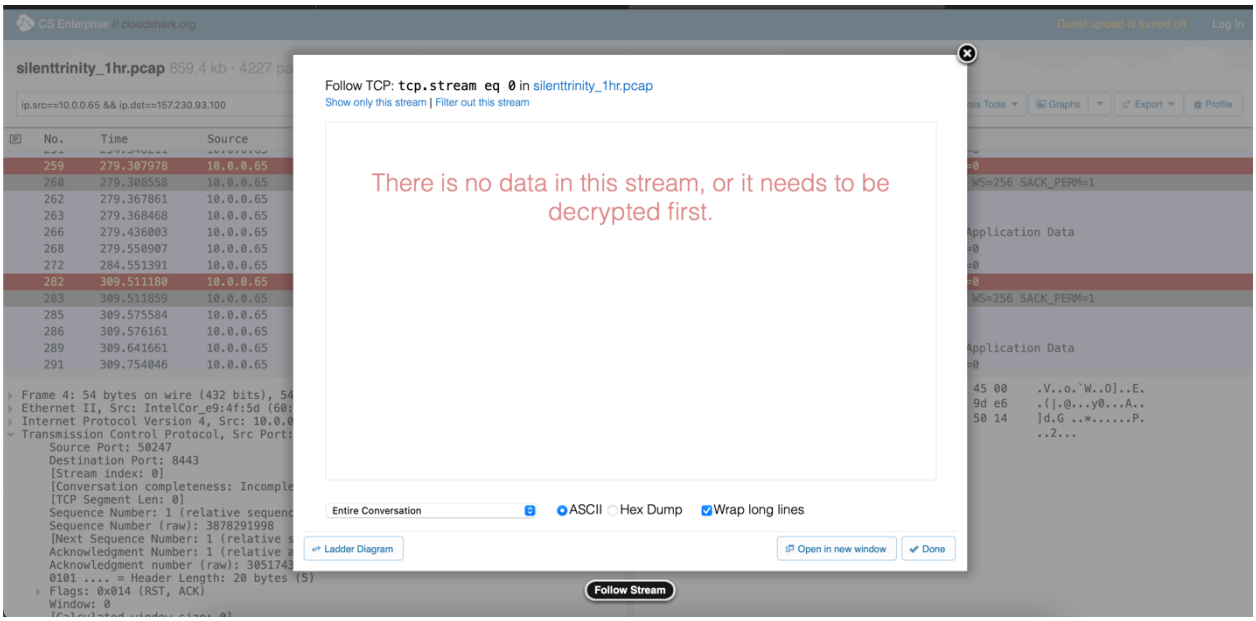
MALWARE INVESTIGATION LAB

STEPHEN MENSAH

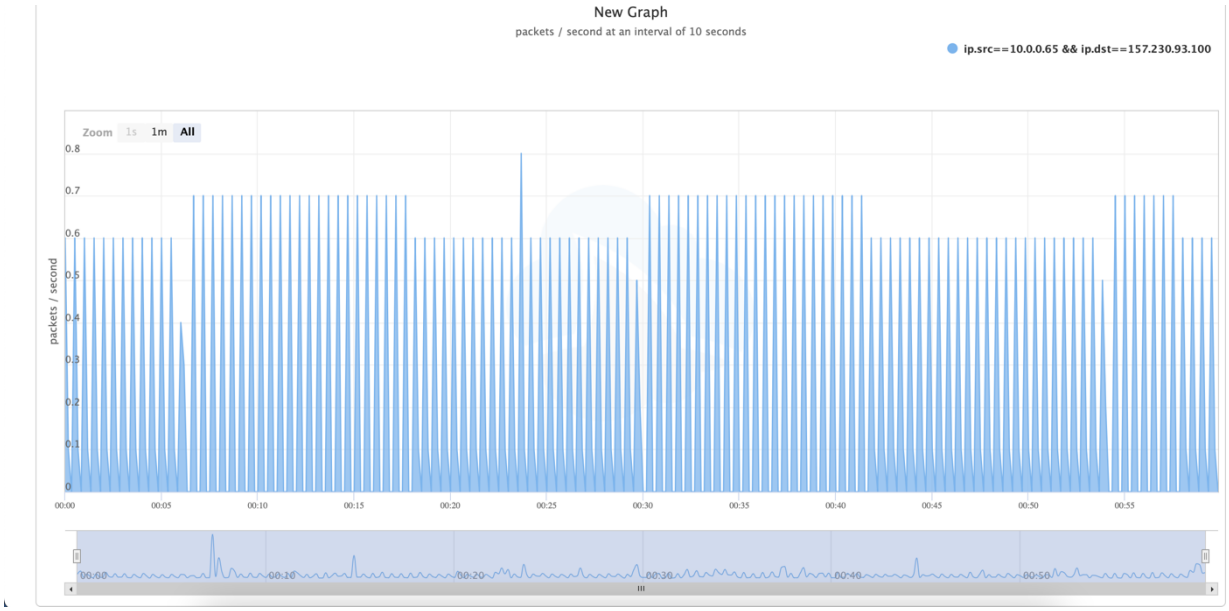
SCREENSHOTS FROM THE LAB

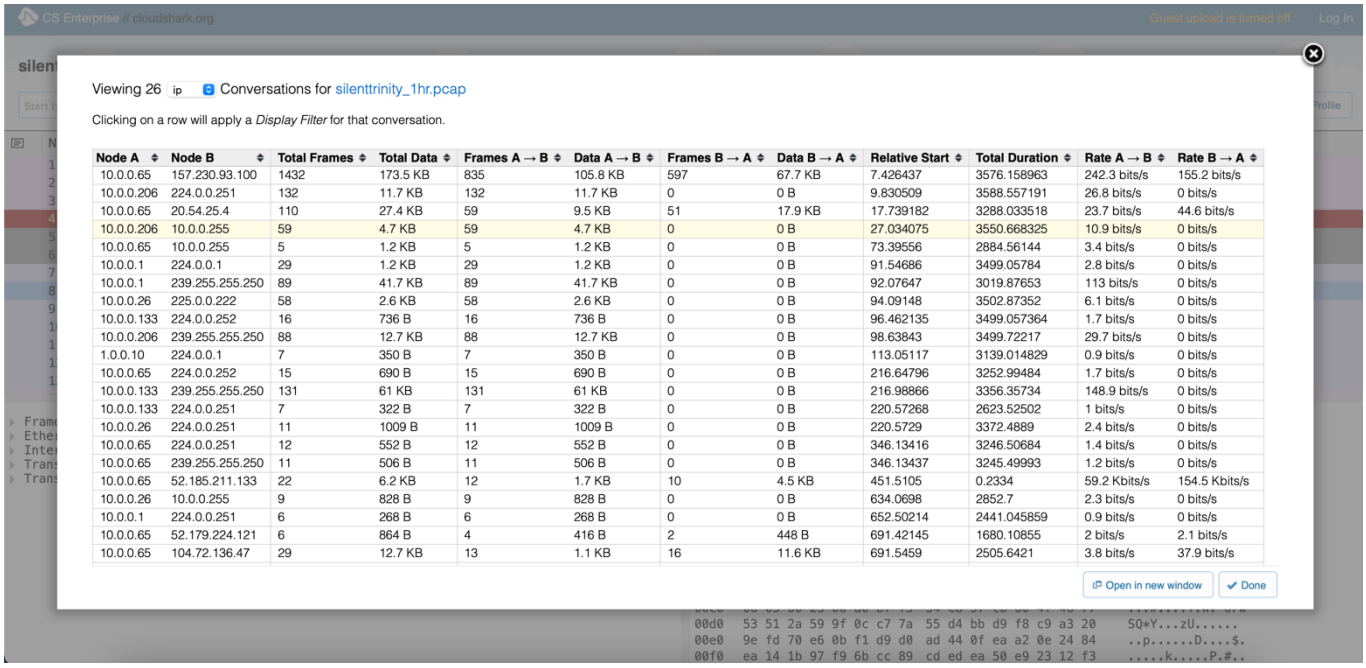
SERENETRINITY

Following TCP stream. Everything is encrypted.



Analyzing the beaconing behavior of the Malware

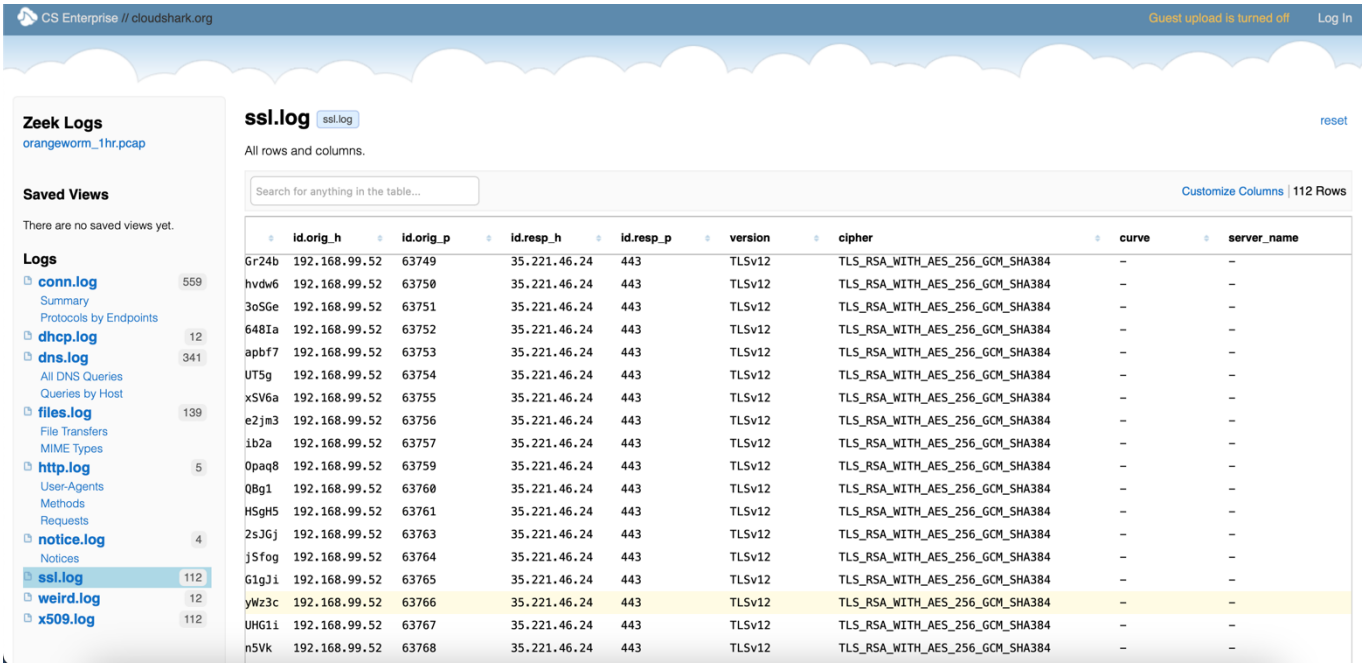




Node A	Node B	Total Frames	Total Data	Frames A → B	Data A → B	Frames B → A	Data B → A	Relative Start	Total Duration	Rate A → B	Rate B → A
10.0.0.65	157.230.93.100	1432	173.5 KB	835	105.8 KB	597	67.7 KB	7.426437	3576.158963	242.3 bits/s	155.2 bits/s
10.0.0.206	224.0.0.251	132	11.7 KB	132	11.7 KB	0	0 B	9.830509	3588.557191	26.8 bits/s	0 bits/s
10.0.0.65	20.54.25.4	110	27.4 KB	59	9.5 KB	51	17.9 KB	17.739182	3288.033518	23.7 bits/s	44.6 bits/s
10.0.0.206	10.0.0.255	59	4.7 KB	59	4.7 KB	0	0 B	27.034075	3550.668325	10.9 bits/s	0 bits/s
10.0.0.65	10.0.0.255	5	1.2 KB	5	1.2 KB	0	0 B	73.39556	2884.56144	3.4 bits/s	0 bits/s
10.0.0.1	224.0.0.1	29	1.2 KB	29	1.2 KB	0	0 B	91.54686	3499.05784	2.8 bits/s	0 bits/s
10.0.0.1	239.255.255.250	89	41.7 KB	89	41.7 KB	0	0 B	92.07647	3019.87653	113 bits/s	0 bits/s
10.0.0.26	225.0.0.222	58	2.6 KB	58	2.6 KB	0	0 B	94.09148	3502.87352	6.1 bits/s	0 bits/s
10.0.0.133	224.0.0.252	16	736 B	16	736 B	0	0 B	96.462135	3499.057364	1.7 bits/s	0 bits/s
10.0.0.206	239.255.255.250	88	12.7 KB	88	12.7 KB	0	0 B	98.63843	3499.72217	29.7 bits/s	0 bits/s
1.0.0.10	224.0.0.1	7	350 B	7	350 B	0	0 B	113.05117	3139.014829	0.9 bits/s	0 bits/s
10.0.0.65	224.0.0.252	15	690 B	15	690 B	0	0 B	216.64796	3252.99484	1.7 bits/s	0 bits/s
10.0.0.133	239.255.255.250	131	61 KB	131	61 KB	0	0 B	216.98866	3356.35734	148.9 bits/s	0 bits/s
10.0.0.133	224.0.0.251	7	322 B	7	322 B	0	0 B	220.57268	2623.52502	1 bits/s	0 bits/s
10.0.0.26	224.0.0.251	11	1009 B	11	1009 B	0	0 B	220.5729	3372.4889	2.4 bits/s	0 bits/s
10.0.0.65	224.0.0.251	12	552 B	12	552 B	0	0 B	346.13416	3246.50684	1.4 bits/s	0 bits/s
10.0.0.65	239.255.255.250	11	506 B	11	506 B	0	0 B	346.13437	3245.49993	1.2 bits/s	0 bits/s
10.0.0.65	52.185.211.133	22	6.2 KB	12	1.7 KB	10	4.5 KB	451.5105	0.2334	59.2 Kbits/s	154.5 Kbits/s
10.0.0.26	10.0.0.255	9	828 B	9	828 B	0	0 B	634.0698	2852.7	2.3 bits/s	0 bits/s
10.0.0.1	224.0.0.251	6	268 B	6	268 B	0	0 B	652.50214	2441.045859	0.9 bits/s	0 bits/s
10.0.0.65	52.179.224.121	6	864 B	4	416 B	2	448 B	691.42145	1680.10855	2 bits/s	2.1 bits/s
10.0.0.65	104.72.136.47	29	12.7 KB	13	1.1 KB	16	11.6 KB	691.5459	2505.6421	3.8 bits/s	37.9 bits/s

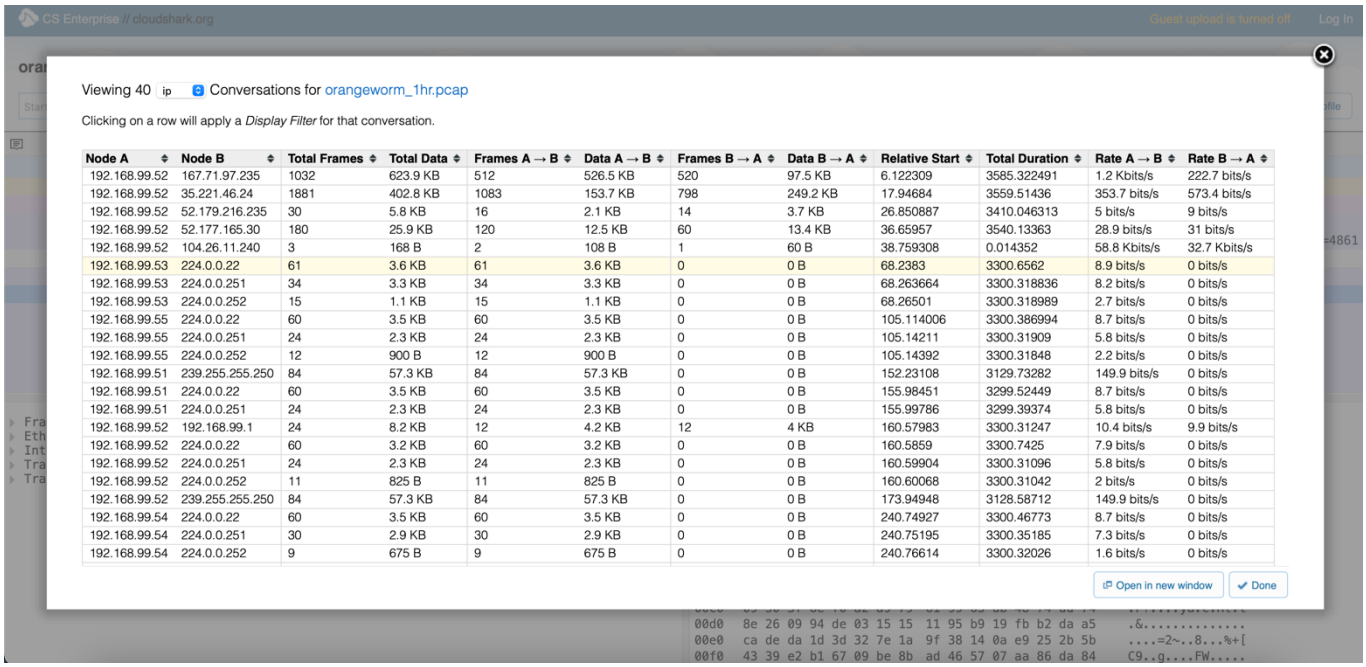
Orangeworm

Same encryption algorithm and destination port but different source ports



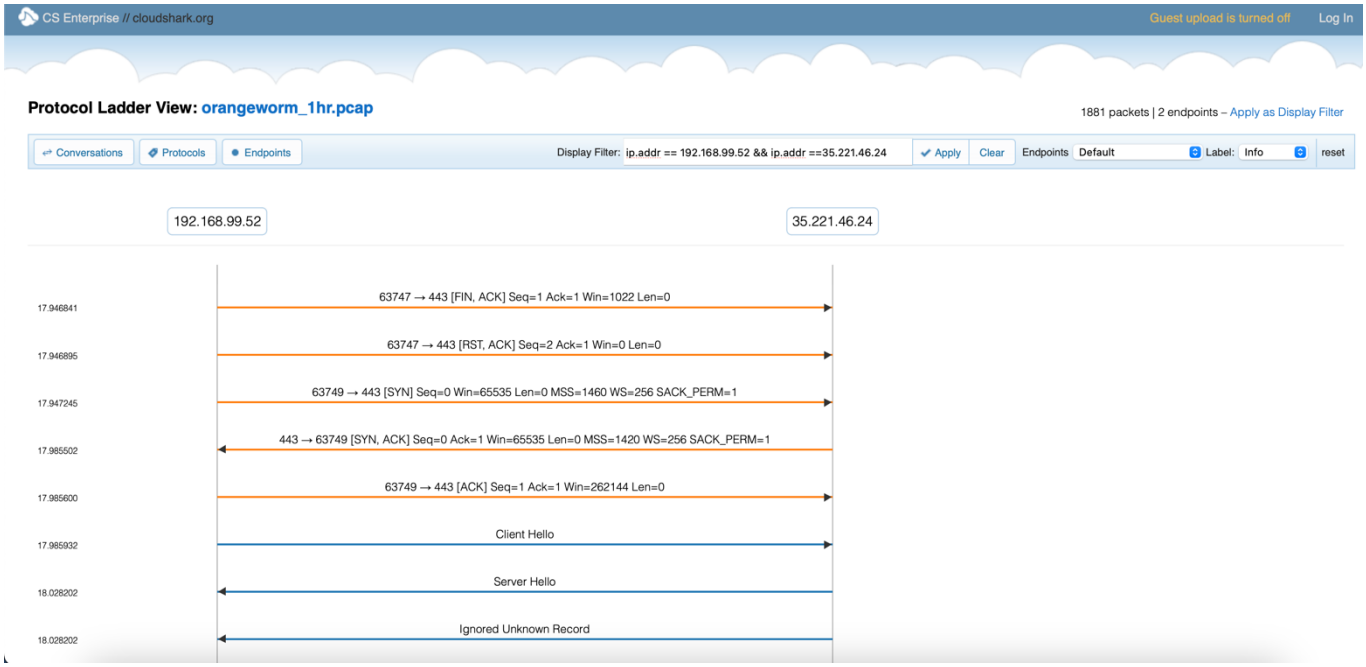
	id.orig_h	id.orig_p	id.resp_h	id.resp_p	version	cipher	curve	server_name
Gr24b	192.168.99.52	63749	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
hvdw6	192.168.99.52	63750	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
3oSGe	192.168.99.52	63751	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
648Ia	192.168.99.52	63752	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
apbf7	192.168.99.52	63753	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
UT5g	192.168.99.52	63754	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
xSV6a	192.168.99.52	63755	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
e2jm3	192.168.99.52	63756	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
ib2a	192.168.99.52	63757	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
Opaq8	192.168.99.52	63759	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
QBg1	192.168.99.52	63760	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
HSgH5	192.168.99.52	63761	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
2sJGj	192.168.99.52	63763	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
jSfog	192.168.99.52	63764	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
G1gJi	192.168.99.52	63765	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
yWz3c	192.168.99.52	63766	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
UHG1i	192.168.99.52	63767	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-
n5Vk	192.168.99.52	63768	35.221.46.24	443	TLSv12	TLS_RSA_WITH_AES_256_GCM_SHA384	-	-

The protocol conversation panel – 192.168.99.52 and 32.221.46 had highest number of packets

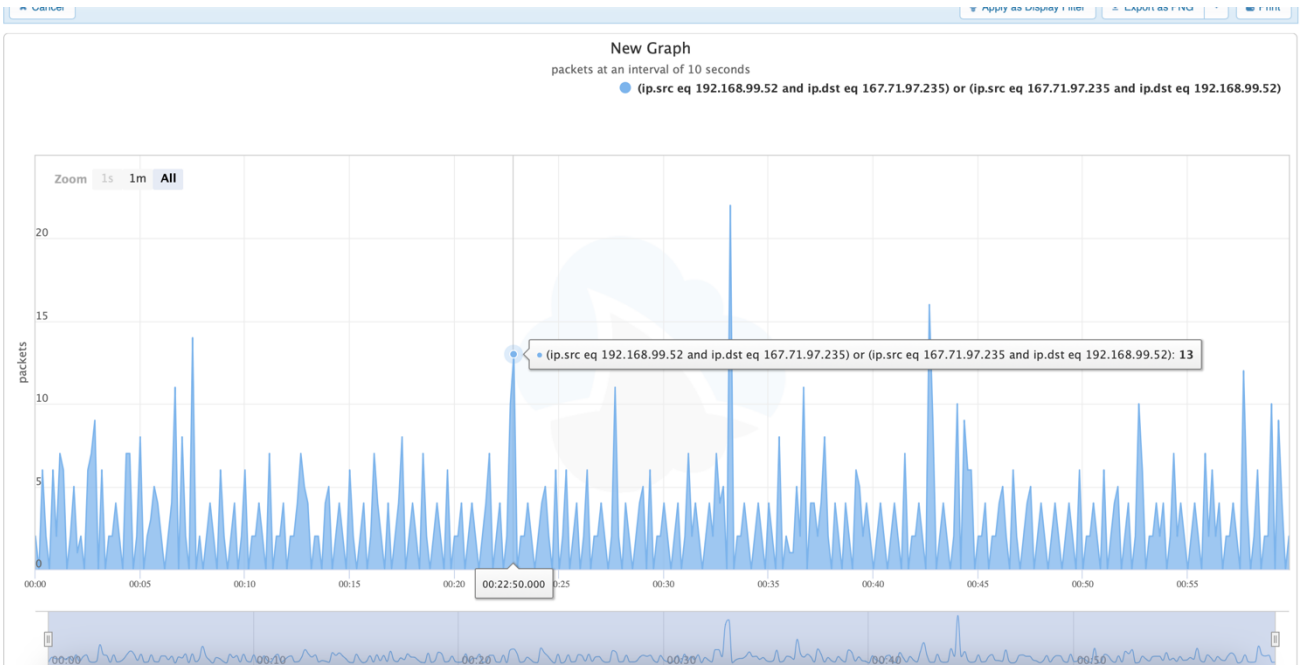


Node A	Node B	Total Frames	Total Data	Frames A → B	Data A → B	Frames B → A	Data B → A	Relative Start	Total Duration	Rate A → B	Rate B → A
192.168.99.52	167.71.97.235	1032	623.9 KB	512	526.5 KB	520	97.5 KB	6.122309	3585.322491	1.2 Kbits/s	222.7 bits/s
192.168.99.52	35.221.46.24	1881	402.8 KB	1083	153.7 KB	798	249.2 KB	17.94684	3559.51436	353.7 bits/s	573.4 bits/s
192.168.99.52	52.179.216.235	30	5.8 KB	16	2.1 KB	14	3.7 KB	26.850887	3410.046313	5 bits/s	9 bits/s
192.168.99.52	52.177.165.30	180	25.9 KB	120	12.5 KB	60	13.4 KB	36.65957	3540.13363	28.9 bits/s	31 bits/s
192.168.99.52	104.26.11.240	3	168 B	2	108 B	1	60 B	38.759308	0.014352	58.8 Kbits/s	32.7 Kbits/s
192.168.99.53	224.0.0.22	61	3.6 KB	61	3.6 KB	0	0 B	68.2383	3300.6562	8.9 bits/s	0 bits/s
192.168.99.53	224.0.0.251	34	3.3 KB	34	3.3 KB	0	0 B	68.263664	3300.318836	8.2 bits/s	0 bits/s
192.168.99.53	224.0.0.252	15	1.1 KB	15	1.1 KB	0	0 B	68.26501	3300.318989	2.7 bits/s	0 bits/s
192.168.99.55	224.0.0.22	60	3.5 KB	60	3.5 KB	0	0 B	105.114006	3300.386994	8.7 bits/s	0 bits/s
192.168.99.55	224.0.0.251	24	2.3 KB	24	2.3 KB	0	0 B	105.14211	3300.31909	5.8 bits/s	0 bits/s
192.168.99.55	224.0.0.252	12	900 B	12	900 B	0	0 B	105.14392	3300.31848	2.2 bits/s	0 bits/s
192.168.99.51	239.255.255.250	84	57.3 KB	84	57.3 KB	0	0 B	152.23108	3129.73282	149.9 bits/s	0 bits/s
192.168.99.51	224.0.0.22	60	3.5 KB	60	3.5 KB	0	0 B	155.98451	3299.52449	8.7 bits/s	0 bits/s
192.168.99.51	224.0.0.251	24	2.3 KB	24	2.3 KB	0	0 B	155.99786	3299.39374	5.8 bits/s	0 bits/s
192.168.99.52	192.168.99.1	24	8.2 KB	12	4.2 KB	12	4 KB	160.57983	3300.31247	10.4 bits/s	9.9 bits/s
192.168.99.52	224.0.0.22	60	3.2 KB	60	3.2 KB	0	0 B	160.5859	3300.7425	7.9 bits/s	0 bits/s
192.168.99.52	224.0.0.251	24	2.3 KB	24	2.3 KB	0	0 B	160.59904	3300.31096	5.8 bits/s	0 bits/s
192.168.99.52	224.0.0.252	11	825 B	11	825 B	0	0 B	160.60068	3300.31042	2 bits/s	0 bits/s
192.168.99.52	239.255.255.250	84	57.3 KB	84	57.3 KB	0	0 B	173.94948	3128.58712	149.9 bits/s	0 bits/s
192.168.99.54	224.0.0.22	60	3.5 KB	60	3.5 KB	0	0 B	240.74927	3300.46773	8.7 bits/s	0 bits/s
192.168.99.54	224.0.0.251	30	2.9 KB	30	2.9 KB	0	0 B	240.75195	3300.35185	7.3 bits/s	0 bits/s
192.168.99.54	224.0.0.252	9	675 B	9	675 B	0	0 B	240.76614	3300.32026	1.6 bits/s	0 bits/s

Conversations between two endpoints

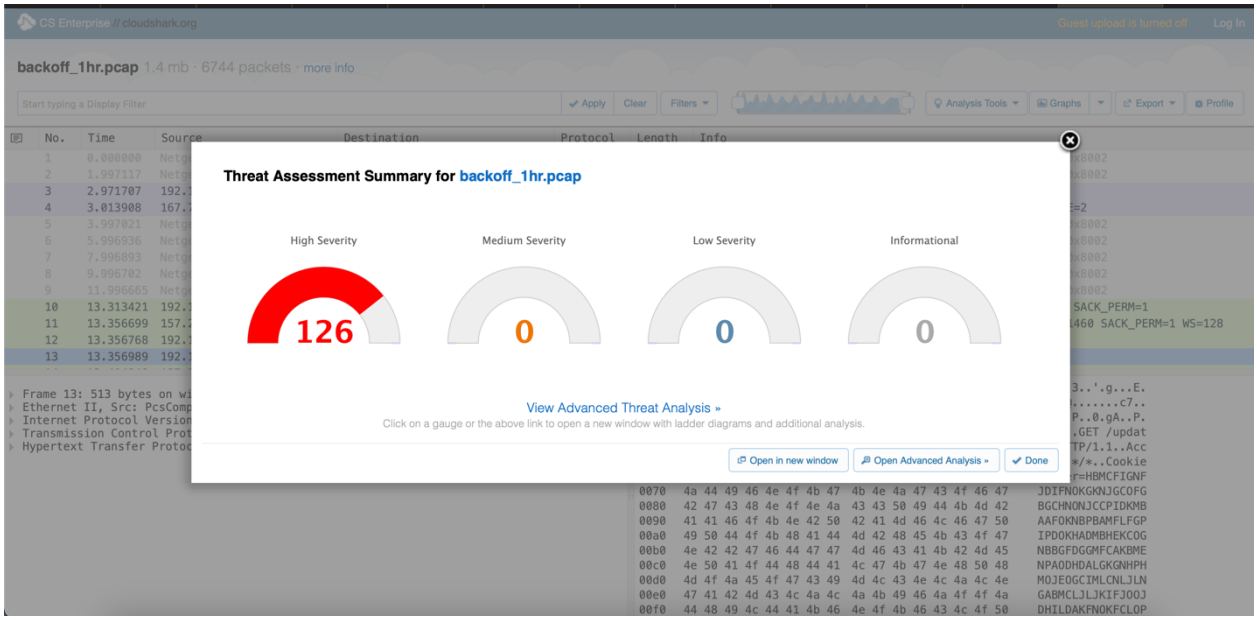


Beaconing behavior of the orange worm

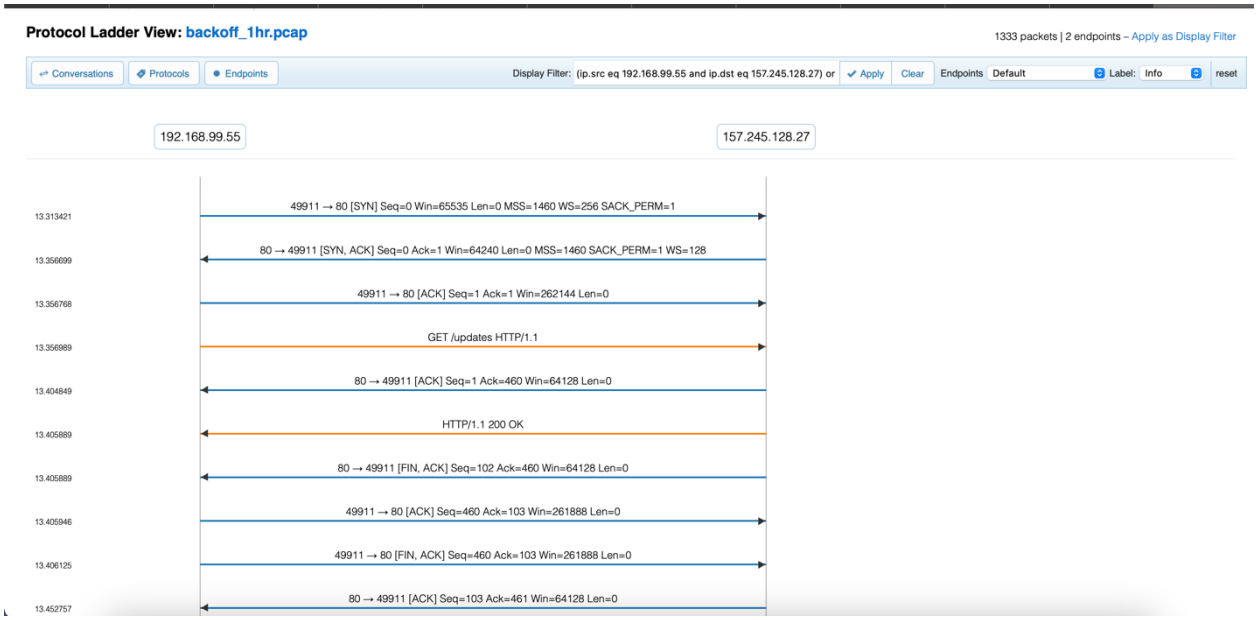


Backoff

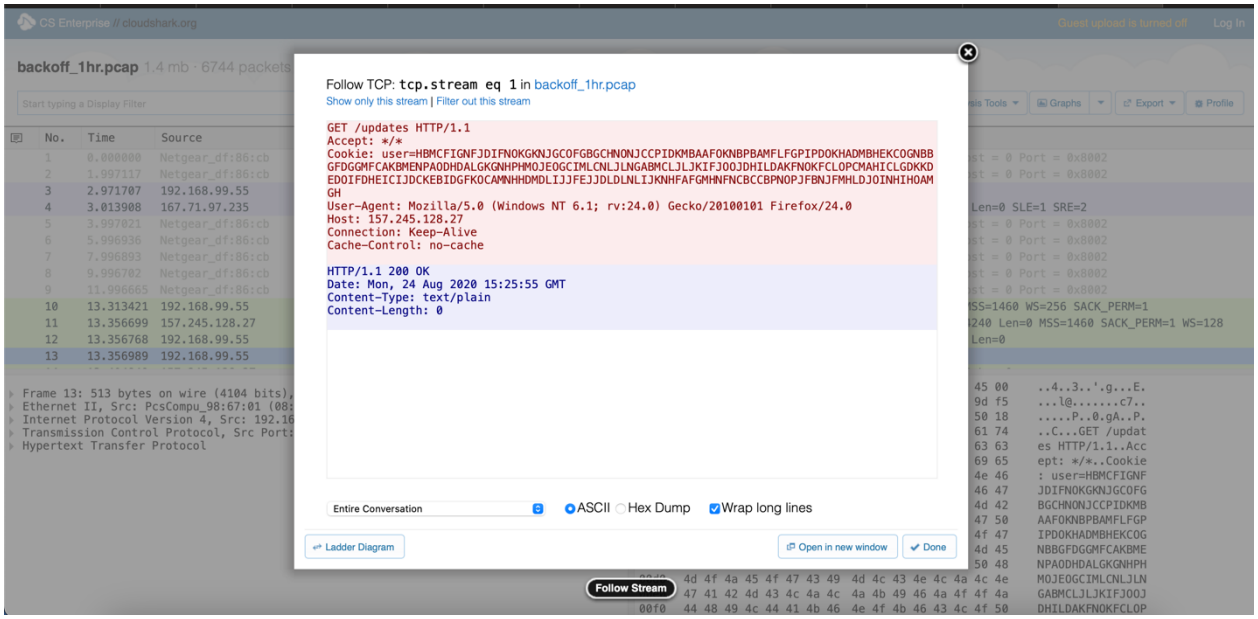
Threat Assessment View



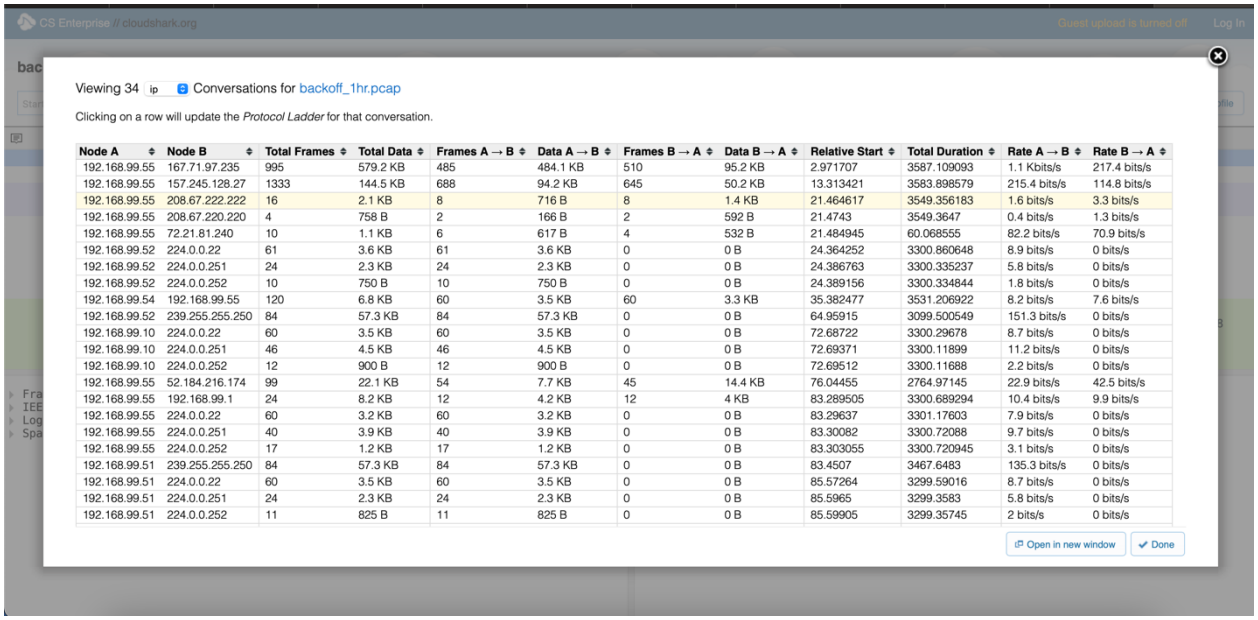
Ladder Diagram to view the conversations between the host and the C2 server



Following and analyzing an HTTP stream. Identified a malicious user-agent string

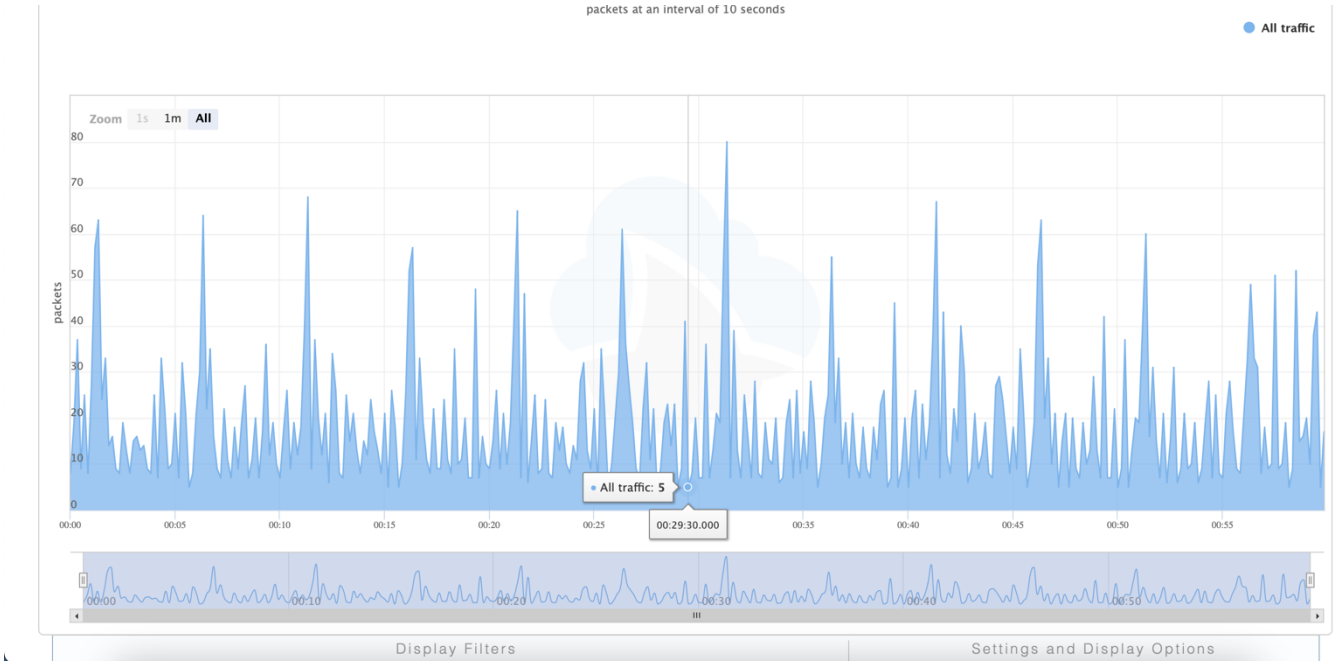


A summary of the conversations that were captured

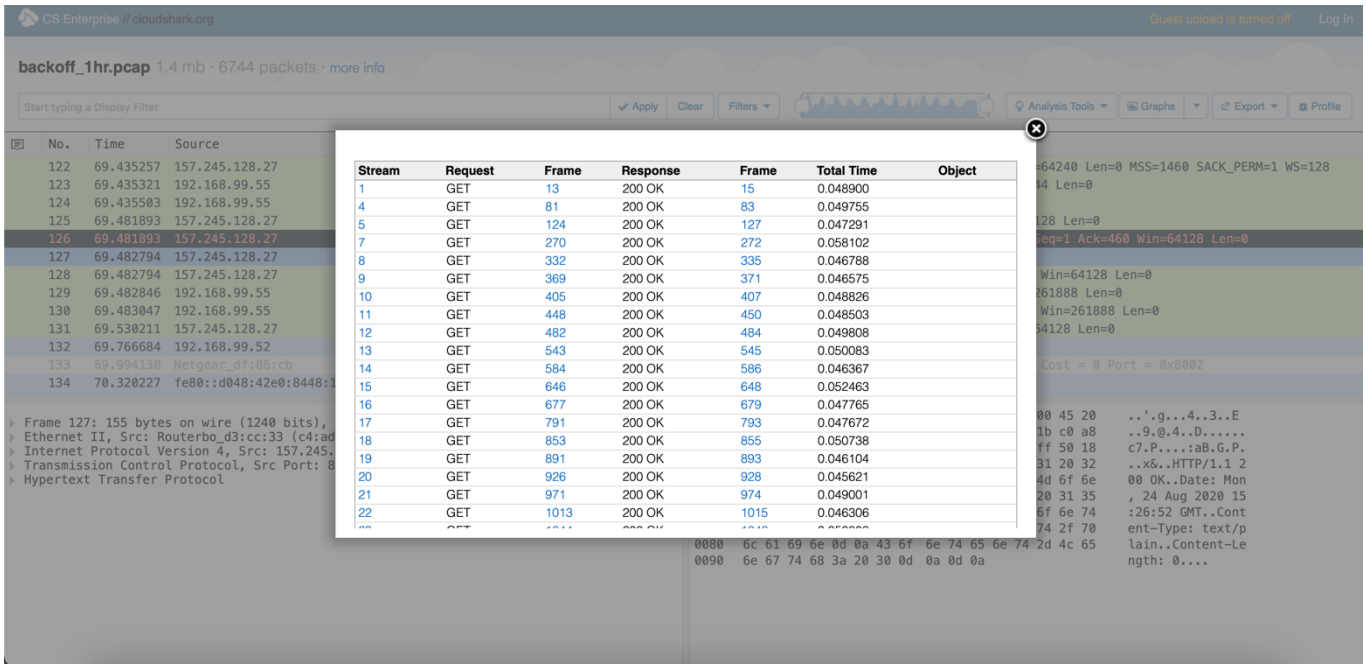


Node A	Node B	Total Frames	Total Data	Frames A → B	Data A → B	Frames B → A	Data B → A	Relative Start	Total Duration	Rate A → B	Rate B → A
192.168.99.55	167.71.97.235	995	579.2 KB	485	484.1 KB	510	95.2 KB	2.971707	3587.109093	1.1 Kbits/s	217.4 bits/s
192.168.99.55	157.245.128.27	1333	144.5 KB	688	94.2 KB	645	50.2 KB	13.313421	3583.898579	215.4 bits/s	114.8 bits/s
192.168.99.55	208.67.222.222	16	2.1 KB	8	716 B	8	1.4 KB	21.464617	3549.356183	1.6 bits/s	3.3 bits/s
192.168.99.55	208.67.220.220	4	758 B	2	166 B	2	592 B	21.4743	3549.3647	0.4 bits/s	1.3 bits/s
192.168.99.55	72.21.81.240	10	1.1 KB	6	617 B	4	532 B	21.484945	60.068555	82.2 bits/s	70.9 bits/s
192.168.99.52	224.0.0.22	61	3.6 KB	61	3.6 KB	0	0 B	24.364252	3300.860648	8.9 bits/s	0 bits/s
192.168.99.52	224.0.0.251	24	2.3 KB	24	2.3 KB	0	0 B	24.386763	3300.335237	5.8 bits/s	0 bits/s
192.168.99.52	224.0.0.252	10	750 B	10	750 B	0	0 B	24.389156	3300.334844	1.8 bits/s	0 bits/s
192.168.99.54	192.168.99.55	120	6.8 KB	60	3.5 KB	60	3.3 KB	35.382477	3531.206922	8.2 bits/s	7.6 bits/s
192.168.99.52	239.255.255.250	84	57.3 KB	84	57.3 KB	0	0 B	64.95915	3099.500549	151.3 bits/s	0 bits/s
192.168.99.10	224.0.0.22	60	3.5 KB	60	3.5 KB	0	0 B	72.68722	3300.29678	8.7 bits/s	0 bits/s
192.168.99.10	224.0.0.251	46	4.5 KB	46	4.5 KB	0	0 B	72.69371	3300.11899	11.2 bits/s	0 bits/s
192.168.99.10	224.0.0.252	12	900 B	12	900 B	0	0 B	72.69512	3300.11688	2.2 bits/s	0 bits/s
192.168.99.55	52.184.216.174	99	22.1 KB	54	7.7 KB	45	14.4 KB	76.04455	2764.97145	22.9 bits/s	42.5 bits/s
192.168.99.55	192.168.99.1	24	8.2 KB	12	4.2 KB	12	4 KB	83.289505	3300.689294	10.4 bits/s	9.9 bits/s
192.168.99.55	224.0.0.22	60	3.2 KB	60	3.2 KB	0	0 B	83.29637	3301.17603	7.9 bits/s	0 bits/s
192.168.99.55	224.0.0.251	40	3.9 KB	40	3.9 KB	0	0 B	83.30082	3300.72088	9.7 bits/s	0 bits/s
192.168.99.55	224.0.0.252	17	1.2 KB	17	1.2 KB	0	0 B	83.303055	3300.720945	3.1 bits/s	0 bits/s
192.168.99.51	239.255.255.250	84	57.3 KB	84	57.3 KB	0	0 B	83.4507	3467.6483	135.3 bits/s	0 bits/s
192.168.99.51	224.0.0.22	60	3.5 KB	60	3.5 KB	0	0 B	85.57264	3299.59016	8.7 bits/s	0 bits/s
192.168.99.51	224.0.0.251	24	2.3 KB	24	2.3 KB	0	0 B	85.5965	3299.3583	5.8 bits/s	0 bits/s
192.168.99.51	224.0.0.252	11	825 B	11	825 B	0	0 B	85.59905	3299.35745	2 bits/s	0 bits/s

The beaconing behavior of the Backoff malware



Summary of update requests to and responses from the C2 server



Stream	Request	Frame	Response	Frame	Total Time	Object
1	GET	13	200 OK	15	0.048900	
4	GET	81	200 OK	83	0.049755	
5	GET	124	200 OK	127	0.047291	
7	GET	270	200 OK	272	0.058102	
8	GET	332	200 OK	335	0.046788	
9	GET	369	200 OK	371	0.046575	
10	GET	405	200 OK	407	0.048826	
11	GET	448	200 OK	450	0.048503	
12	GET	482	200 OK	484	0.049808	
13	GET	543	200 OK	545	0.050083	
14	GET	584	200 OK	586	0.046367	
15	GET	646	200 OK	648	0.052463	
16	GET	677	200 OK	679	0.047765	
17	GET	791	200 OK	793	0.047672	
18	GET	853	200 OK	855	0.050738	
19	GET	891	200 OK	893	0.046104	
20	GET	926	200 OK	928	0.045621	
21	GET	971	200 OK	974	0.049001	
22	GET	1013	200 OK	1015	0.046306	

SILENTTRINITY

Threat Simulation

To investigate and analyze for silenttrinity malware, I will create customized alerts that would send notifications as soon as a condition is triggered. The said malware uses a command-and-control server to communicate consistently with its hosts. As such, I will monitor the communications that existed between two IP addresses. the IP address 10.0.0.65 established a 3-way handshake with the host 157.230.93.100. Consistent communication took place after a successful handshake from different ports on 10.0.0.65 to the same port on 157.230.93.100 (port 8443). By using the graph, I will monitor the interval at which these two nodes communicated. I realized that both addresses communicated at regular intervals and exchanged almost the same number of packets every 5 seconds. Using the ladder diagram, I identified that a total of 1432 packets were exchanged between these, the highest on the chart. I tried following the communications with the "Follow Stream" and "Follow TLS" tools; however, they were encrypted. Malware steals sensitive information by using encryption and compression to reduce file sizes to avoid network transfer threshold alerts and evade detection. As such, I will equally analyze all packets within a day of the event to scout for patterns and potential actions executed by the malware. Due to the nature of this malware, I will assign a high criticality level. I will use the graphs and protocol ladder views to follow communications. A post-incident report will be written to document the event and the company's threat intel and attack signatures will be updated.

2. Business Impact

The silenttrinity malware can be used to steal sensitive information from a network. Short-term risks include information theft, the stolen information can be used by attackers to commit fraud, and possible ransomware attacks. Long-term risks are legal actions and data protection compliance issues with Compliance Authorities, tarnish business reputation, huge financial loss, and loss of customer trust.

3. Remediation

The network will be monitored in real-time to detect any uncommon data flow. Intrusion Prevention Systems utilize deep reinforcement learning will be employed to detect new silenttrinity malware variants, educate employees on safe online practices, block any IP address with consistent communications to an external address on port 8443, and monitor for any suspicious file.

ORANGEWORM

Threat Simulation

The first step to take is to create a network alert to notify you when suspicious activity is detected. After the notification, I will start analyzing packets captured within 4 days before the alert was triggered and the activities within 24 hours after the event. By filtering the packets, I will analyze all packets that are associated with the C2 server. I will then monitor for any uncommon communications that will exist between two IP addresses. From the packet capture, multiple communications were discovered from address 35.221.46.24 to different hosts. However, there was consistent communication between the said address on port 443 and the address 192.168.99.52 on different ports. From the capture, it was evident that close to the same number of packets was communicated at different but regular time intervals. This behavior deviates from normal user actions. it could represent structured communication between the C2 and its compromised hosts since both parties need to be in regular touch for matching orders or commands. Using the Zeek Logs panel, I discovered that all the packets that were communicated between 35.221.46.24 and 192.168.99.52 have the same orig_ip_bytes (payload byte) of 1449 bytes. Having different packets with the same payload size indicates suspicious or programmed activity. Orangeworm can create backdoors and targets critical infrastructure such as hospitals to steal information. Due to this, I will assign a high criticality level. I used the Zeek logs and graph panel to analyze the packets. A detailed report will be written on the incident and threat intel will be updated.

2. Business Impacts

Orangeworm malware can be used to steal sensitive information, create backdoors for future exploitation, and launch ransomware attacks with the stolen information. The business can incur huge financial losses from ransomware, face legal battles, and deal with compliance issues.

3. Remediation

The network must be monitored and analyzed in real-time for anomalies, advanced Intrusion Prevention Systems must be deployed, and efficient and trusted antivirus should be installed. In addition

Backoff

Threat Simulation

To address the backoff malware, I will first create an alert to send a notification to the security team as soon as an abnormal traffic flow or activity is detected on the network. I will then analyze all network traffic within a 120-hour timeframe. This will help investigate potential pre-alert malware activities. The network traffic will be refined by filtering with IP addresses to determine any strong and consistent connections between two hosts and look out for any jitters that could be introduced by the malware authors to avoid detection. After that, I will apply additional filters to search for packets that may contain executable files (.exe) with the hex signature "4D 5A" which may have been downloaded by users. From the packet capture, it was evident that the host 192.168.99.55 sent packets from different ports to the IP address 157.245.128.27 on port 80, a total of 1331 packets were communicated at regular intervals within an hour. By using the graph dashboard, I will be able to monitor the rate at which the communication was done and the jitter rate to be able to determine if the behavior is normal or unusual – it was abnormal in this case. Since Backoff uses HTTP GET requests, I will use the "follow HTTP stream" panel to analyze the HTTP packets to search for any malicious user-agent stings. I identified a user-agent string "Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0" – which a malicious agent that is used by the Backoff malware. I will draft a report on this event and update the company's incident response plan. I will equally update our threat intel and signatures. The threat assessment panel indicated that there were 126 packets with high severity. As such, I will assign a high criticality level to this malware. The dashboards to be used are the threat assessment panel, zeek logs, follow stream, and ladder diagram.

Business Impact

The malware is used to steal sensitive user information. Short-term impacts are potential ransomware attacks and financial loss. The reputation of the business could be destroyed, and the company can be battling legal and PCI compliance issues in the long term.

Remediation

To address this incident, it is important to constantly monitor the network for any suspicious behavior. In addition, implement ACLs to restrict access to the network - only allowed ports will be able to communicate with my network, block all unnecessary ports and services, ensure end-to-end encryption

on every system, employ data exfiltration systems, and implement MFA to restrict access to the company's remote desktops.

References

Medium (May 19, 2019). Silent Trinity – Research Report. Retrieved February 27, 2023 from https://medium.com/@threathuntingteam/silent-trinity-research-report-7df7ab88f78c

Vivekananda, V (May 12, 2017). Dissecting TLS using Wireshark. Retrieved February 27, 2023 from https://www.catchpoint.com/blog/wireshark-tls-handshake.

MITRE (October 17, 2018). Exfiltration. Retrieved February 27, 2023 from https://attack.mitre.org/tactics/TA0010/

CISA (September 30, 2016). Backoff Point-of-Sale Malware. Retrieved February 27, 2023 from https://www.cisa.gov/news-events/alerts/2014/07/31/backoff-point-sale-malware

Chew, K (October 1, 2020). Malware of the Day – Backoff. Retrieved March 6, 2023 from https://www.activecountermeasures.com/malware-of-the-day-backoff/

Chew, K (June 10, 2020). Malware of the Day – Orangeworm. Retrieved February 27, 2023 from https://www.activecountermeasures.com/malware-of-the-day-orangeworm/

Symantec (April 23, 2018). New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia. Retrieved February 27, 2023 from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia