

# **Incident Response**

## **Analysis of a Vulnerable Network**

Presented by:  
Edward Cruz and Clement Yang

# Table of Contents

---

This document contains the following resources:



**Traffic Profile**



**Normal Activity**



**Malicious Activity**

# Traffic Profile

# Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205, 185.243.115.84, 166.62.111.64, 172.16.4.205	Machines that sent the most traffic.
Most Common Protocols	TCP (87.7%) UDP (12.2%) TLS (11.5%)	Three most common protocols on the network.
# of Unique IP Addresses	810	Count of observed IP addresses.
Subnets	10.6.12.0/24 172.16.4.0/24 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	1 (june11.dll)	Number of malware binaries identified in traffic.

# Behavioral Analysis

---

## Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

### **“Normal” Activity**

- Browsing blogs, reading the news, checking emails

### **Suspicious Activity**

- Setting up an private Active Directory to watch YouTube videos at work, downloading malicious Trojan malware, and torrenting illegal/copyrighted content.

The background of the slide is a dark gray, almost black, field filled with a complex, repeating pattern of geometric shapes. These shapes include squares and triangles of various sizes, some of which are slightly lighter or darker than the background, creating a subtle, textured effect. The overall impression is one of a modern, minimalist design.

# Normal Activity



# Normal Activity: Browsing Blogs

Summarize the following:

- Normal web browsing behavior was observed by filtering through HTTP traffic.
- In one example, the user was browsing a blog site called “mysocalledchaos.com,” which is a blog site run by a mother and lifestyle blogger named Angie.
- An examination of http traffic revealed GET requests for image files named “Bloggging-Tips-1.png,” “Good-Eats-1.jpg,” “Crafty.jpg,” and “HomeDecor.jpg,” suggesting that the blog covers lifestyle topics such as food and home decorations.

http							
Destination	Protocol	Length	Destination Port	SSID	WPA Version	BSS Id	Info
172.16.4.205	HTTP	241	49189				HTTP/1.0 400 Bad request (text/html)
172.16.4.205	HTTP	918	49202				HTTP/1.1 200 OK (JPEG JFIF image)
172.16.4.205	HTTP/XML	1018	49198				HTTP/1.1 200 OK
166.62.111.64	HTTP	395	80				GET /wp-content/uploads/2018/02/Bloggging-Tips-1.png HTTP/1.1
166.62.111.64	HTTP	391	80				GET /wp-content/uploads/2018/02/Good-Eats-1.jpg HTTP/1.1
166.62.111.64	HTTP	386	80				GET /wp-content/uploads/2018/02/Crafty.jpg HTTP/1.1
166.62.111.64	HTTP	389	80				GET /wp-content/uploads/2018/02/HomeDecor.jpg HTTP/1.1
172.16.4.205	HTTP	104	49201				HTTP/1.1 200 OK (JPEG JFIF image)
166.62.111.64	HTTP	386	80				GET /wp-content/uploads/2018/02/Family.jpg HTTP/1.1
172.16.4.205	HTTP	1336	49199				HTTP/1.1 200 OK (PNG)

[Bytes in flight: 341]  
[Bytes sent since last PSH flag: 341]  
TCP payload (341 bytes)

▼ Hypertext Transfer Protocol

> GET /wp-content/uploads/2018/02/Bloggging-Tips-1.png HTTP/1.1\r\nHost: mysocalledchaos.com\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0\r\nAccept: image/webp,\*/\*\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nDNT: 1\r\nConnection: keep-alive\r\nReferer: http://mysocalledchaos.com/\r\n

7



# Normal Activity: Reading the news

Summarize the following:

- Normal browsing activity such as reading the news was detected by filtering for and examining HTTP traffic.
- One user was reading a TIME magazine article and photo essay covering ancient Roman ruins in Libya under Muammar Gaddafi
- An examination of http traffic revealed GET requests for image files including “libya\_ruins\_01.jpg”



Source	Destination	Protocol	Length	Destination Port	SSID	WPA Version	BSS Id	Info
3.33.255.25	10.11.11.179	HTTP	477	50235				HTTP/1.1 200 OK (application/javascript)
0.11.11.179	143.204.29.89	HTTP	450	80				GET /time/rd/trunk/www/web/feds/j/showLinks.js HTTP/1.1
0.11.11.94	52.218.228.130	HTTP	558	80				GET /core/scripts/lrs/tin-can.min.js?_=1573510907652 HTTP/1.1
43.204.29.89	10.11.11.179	HTTP	71	50234				HTTP/1.1 200 OK (text/css)
43.204.29.89	10.11.11.179	HTTP	71	50233				HTTP/1.1 200 OK (text/css)
43.204.29.89	10.11.11.179	HTTP	1343	50237				HTTP/1.1 200 OK (application/javascript)
0.11.11.179	143.204.29.89	HTTP	430	80				GET /time/js/photoessay.js HTTP/1.1
0.11.11.179	143.204.29.89	HTTP	448	80				GET /time/assets/js/frequency_capping.min.js HTTP/1.1
0.11.11.179	143.204.29.89	HTTP	457	80				GET /time/rd/trunk/www/web/feds/j/mobileExperience.js HTTP/1.1
43.204.29.89	10.11.11.179	HTTP	769	50236				HTTP/1.1 200 OK (application/javascript)
0.11.11.179	143.204.29.89	HTTP	460	80				GET /time/rd/trunk/www/web/feds/j/MobileCompatibility.js HTTP/1.1
43.204.29.89	10.11.11.179	HTTP	78	50232				HTTP/1.1 200 OK (application/javascript)
43.204.29.89	10.11.11.179	HTTP	71	50231				HTTP/1.1 200 OK (application/javascript)
0.11.11.179	143.204.29.89	HTTP	445	80				GET /tii/omniture/h/config/time_s_code.js HTTP/1.1
0.11.11.179	143.204.29.89	HTTP	519	80				GET /time/photoessays/2011/libya_ruins/libya_ruins_01.jpg HTTP/1.1
43.204.29.89	10.11.11.179	HTTP	71	50234				HTTP/1.1 200 OK (application/javascript)

[Bytes sent since last PSH flag: 453]

TCP payload (453 bytes)

▼ Hypertext Transfer Protocol

▼ GET /time/photoessays/2011/libya\_ruins/libya\_ruins\_01.jpg HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /time/photoessays/2011/libya\_ruins/libya\_ruins\_01.jpg HTTP/1.1\r\n]

Request Method: GET

Request URI: /time/photoessays/2011/libya\_ruins/libya\_ruins\_01.jpg

Request Version: HTTP/1.1

Host: img.timeinc.net\r\n

Connection: keep-alive\r\n

Accept: image/png,image/svg+xml,image/\*;q=0.8,video/\*;q=0.8,\*/\*;q=0.5\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_1) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Safari/605.1.15\r\n

Accept-Language: en-us\r\n

Referer: http://content.time.com/time/photogallery/0,29307,2077702,00.html\r\n

Accept-Encoding: gzip, deflate\r\n

\r\n

[Full request URI: http://img.timeinc.net/time/photoessays/2011/libya\_ruins/libya\_ruins\_01.jpg]

[HTTP request 3/4]



# Malicious Activity



# Malicious Activity: Frank-n-Ted Server creation

Summarize the following:

- When observing activity from 10.6.12.12, we saw SMB2 protocols where they requested a Session Setup and Created a Tree Connect Request Tree \\Frank-n-Ted-DC.frank-n-ted.com\\sysvol
- These sessions identify that this user was creating a server for the site frank-n-ted.com.

ip.src == 10.6.12.203						
	Time	Source	Destination	Protocol	Length	Info
60077	657.853978	10.6.12.203	10.6.12.12	TCP	1514	49697 → 88 [ACK] Seq=1 Ack=1 Win=262656 Len=1460 [TCP segment of a reasse.
60078	657.855357	10.6.12.203	10.6.12.12	KRB5	81	TGS-REQ
60082	657.882985	10.6.12.203	10.6.12.12	TCP	54	49697 → 88 [ACK] Seq=1488 Ack=1517 Win=262656 Len=0
60083	657.883842	10.6.12.203	10.6.12.12	TCP	54	49697 → 88 [FIN, ACK] Seq=1488 Ack=1517 Win=262656 Len=0
60086	657.909819	10.6.12.203	10.6.12.12	TCP	1514	49680 → 445 [ACK] Seq=4287 Ack=1617 Win=2102272 Len=1460 [TCP segment of .
60087	657.934090	10.6.12.203	10.6.12.12	TCP	1514	49680 → 445 [ACK] Seq=5747 Ack=1617 Win=2102272 Len=1460 [TCP segment of .
60088	657.943708	10.6.12.203	10.6.12.12	SMB2	603	Session Setup Request
60091	657.952889	10.6.12.203	10.6.12.12	SMB2	208	Tree Connect Request Tree: \\Frank-n-Ted-DC.frank-n-ted.com\\sysvol
60093	657.963130	10.6.12.203	10.6.12.12	SMB2	502	Create Request File: frank-n-ted.com\\Policies\\{31B2F340-016D-11D2-945F-00.
60095	657.972610	10.6.12.203	10.6.12.12	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: frank-n-ted.c.
60097	657.977857	10.6.12.203	10.6.12.12	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: frank-n-ted.c.
60099	657.983607	10.6.12.203	10.6.12.12	SMB2	171	Read Request Len:22 Off:0 File: frank-n-ted.com\\Policies\\{31B2F340-016D-1.
60101	657.993257	10.6.12.203	10.6.12.12	SMB2	446	Create Request File: frank-n-ted.com\\Policies\\{31B2F340-016D-11D2-945F-00.
60103	658.001892	10.6.12.203	10.6.12.12	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: frank-n-ted.c.
60105	658.009029	10.6.12.203	10.6.12.12	SMB2	260	Find Request File: frank-n-ted.com\\Policies\\{31B2F340-016D-11D2-945F-00C0.
60107	658.027486	10.6.12.203	10.6.12.12	SMB2	470	Create Request File: frank-n-ted.com\\Policies\\{31B2F340-016D-11D2-945F-00.
60109	658.036410	10.6.12.203	10.6.12.12	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: frank-n-ted.c.



# Malicious Activity: Downloading Trojan/Malware

Summarize the following:

- When observing traffic from 10.6.12.203, we noticed HTTP traffic where they requested to download a file from 205.185.125.104.
- The file in question was the called 'june11.dll', which when run through Virustotal.com, showed it was malicious.
- The Trojan found is named: Trojan.Mint.Zamg.O

ip.src == 10.6.12.203						
	Time	Source	Destination	Protocol	Length	Info
62458	670.147220	10.6.12.203	10.6.12.12	EPM	222	Map request, DRSUAPI, 32bit NDR
69339	754.003140	10.6.12.203	10.6.12.12	EPM	222	Map request, DRSUAPI, 32bit NDR
69356	754.089149	10.6.12.203	10.6.12.12	EPM	222	Map request, DRSUAPI, 32bit NDR
62534	670.436447	10.6.12.203	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
62538	670.451853	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
63583	681.719142	10.6.12.203	5.101.51.151	HTTP	713	POST /post.php HTTP/1.1

53  
/ 67

Community Score

53 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764de

c

Googleipdate.exe

invalid-signature overlay pedll signed

549.84 KB

Size

2022-01-18 21:59:14 UTC

2 days ago

DLL

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O



# Malicious Activity: Infected Traffic

Summarize the following:

- We observed a large amount of suspicious HTTP and TCP traffic communicating with 172.16.4.205.
- The users PC was infected and requesting several POST methods and ACK flags, which is not normal activity within a short timespan.

activity within a short timespan.

ip.addr == 172.16.4.205

Packet details ▾

Narrow & Wide ▾

☐ Case sensitive

String ▾

	Time	Source	Destination	Protocol	Length	In
33249	473.020614	172.16.4.205	31.7.62.214	HTTP	282	PI
33251	473.025995	172.16.4.205	31.7.62.214	HTTP	282	PI
33253	473.031365	172.16.4.205	31.7.62.214	HTTP	282	PI
33314	473.276545	172.16.4.205	31.7.62.214	HTTP	282	POST
33316	473.281913	172.16.4.205	31.7.62.214	HTTP	282	POST
33318	473.287452	172.16.4.205	31.7.62.214	HTTP	282	POST
33392	473.548596	172.16.4.205	31.7.62.214	HTTP	282	POST
33417	473.658167	172.16.4.205	31.7.62.214	HTTP	282	POST
33421	473.667066	172.16.4.205	31.7.62.214	HTTP	282	POST
33423	473.672432	172.16.4.205	31.7.62.214	HTTP	282	POST
33425	473.677804	172.16.4.205	31.7.62.214	HTTP	282	POST
33427	473.683203	172.16.4.205	31.7.62.214	HTTP	282	POST
33429	473.688564	172.16.4.205	31.7.62.214	HTTP	282	POST
33431	473.693945	172.16.4.205	31.7.62.214	HTTP	282	POST
33433	473.699545	172.16.4.205	31.7.62.214	HTTP	282	POST
33435	473.704696	172.16.4.205	31.7.62.214	HTTP	282	POST
33437	473.710064	172.16.4.205	31.7.62.214	HTTP	282	POST
33439	473.715443	172.16.4.205	31.7.62.214	HTTP	282	POST

Ethernet · 75

IPv4 · 880

IPv6

TCP · 1046

UDP · 1827

Address A	Address B	Packets	Bytes	Packets A → B
172.16.4.205	185.243.115.84	18,324	16 M	9,753
166.62.111.64	172.16.4.205	11,597	11 M	8,327

ip.addr == 172.16.4.205

Packet details ▾

Narrow & Wide ▾

☐ Case sensitive

String ▾

	Time	Source	Destination	Protocol	Length	Info
31773	450.160798	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31774	450.183396	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31778	450.208564	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
25852	357.658324	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31779	450.231143	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31780	450.253727	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31781	450.276423	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31782	450.299010	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31783	450.321495	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31784	450.344087	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31785	450.366605	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31786	450.389180	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31788	450.412586	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31789	450.435192	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
25853	357.680927	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31791	450.458617	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31792	450.481224	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]
31795	450.527261	172.16.4.205	185.243.115.84	TCP	1411	49249 → 80 [ACK]

12



# Malicious Activity: Torrenting Copyrighted File

Summarize the following:

- When observing traffic from 10.0.0.201 we noticed HTTP and BitTorrent traffic.
- The user was requesting to download an AVI.Torrent file from <http://www.publictorrents.com>

ip.addr == 10.0.0.201 and http							
Packet details		Narrow & Wide		<input type="checkbox"/> Case sensitive	String	GET	Find
No.	Time	Source	Destination	Protocol	Length	Username	Info
73647	777.231622	10.0.0.201	168.215.194.14	HTTP	500		GET /grabs/bettybooprythmonthereservatio
73688	777.640590	172.217.9.2	10.0.0.201	HTTP	696		HTTP/1.1 200 OK (text/javascript)
73694	777.653160	10.0.0.201	168.215.194.14	HTTP	465		GET /divxi.jpg HTTP/1.1
73711	777.743640	50.18.44.131	10.0.0.201	HTTP	239		HTTP/1.1 404 Not Found (application/x-j..
73789	778.673023	10.0.0.201	52.94.240.125	HTTP	415		GET /s/ads.js HTTP/1.1
73916	779.400505	10.0.0.201	168.215.194.14	HTTP	531		GET /usercomments.html?movieid=513 HTTP/..
73988	780.365376	168.215.194.14	10.0.0.201	HTTP	464		HTTP/1.1 200 OK (JPEG JFIF image)
73992	780.373220	52.94.240.125	10.0.0.201	HTTP	375		HTTP/1.1 200 (text/javascript)
73994	780.393372	168.215.194.14	10.0.0.201	HTTP	1212		HTTP/1.1 200 OK (GIF89a)
73998	780.425367	168.215.194.14	10.0.0.201	HTTP	865		HTTP/1.1 200 OK (JPEG JFIF image)
74006	780.440429	10.0.0.201	52.94.240.125	HTTP	427		GET /s/ads-common.js HTTP/1.1
74028	780.699086	52.94.240.125	10.0.0.201	HTTP	1227		HTTP/1.1 200 (text/javascript)
74038	780.717874	168.215.194.14	10.0.0.201	HTTP	59		HTTP/1.1 200 OK (text/html)
74042	780.734693	10.0.0.201	72.21.202.62	HTTP	885		GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=..
74051	780.879490	72.21.202.62	10.0.0.201	HTTP	1310		HTTP/1.1 200 OK (text/html)
74114	781.375722	10.0.0.201	52.94.233.131	HTTP	1067		GET /1/associates-ads/1/OP/?cb=153162823..
74174	781.491043	52.94.233.131	10.0.0.201	HTTP	254		HTTP/1.1 200 OK (GIF89a)
74287	782.182166	10.0.0.201	168.215.194.14	HTTP	589		GET /bt/btdownload.php?type=torrent&file..
74300	782.331449	168.215.194.14	10.0.0.201	HTTP	59		HTTP/1.1 200 OK (application/x-bittorre..
74331	782.378466	10.0.0.201	140.211.166.134	HTTP	195		GET /version-1.0 HTTP/1.1
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 168.215.194.14							
Transmission Control Protocol, Src Port: 49834, Dst Port: 80, Seq: 1, Ack: 1, Len: 535							
Hypertext Transfer Protocol							
GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n							
[Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]							
[GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]							
[Severity level: Chat]							