

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:



Network Topology & Critical Vulnerabilities



Traffic Profile



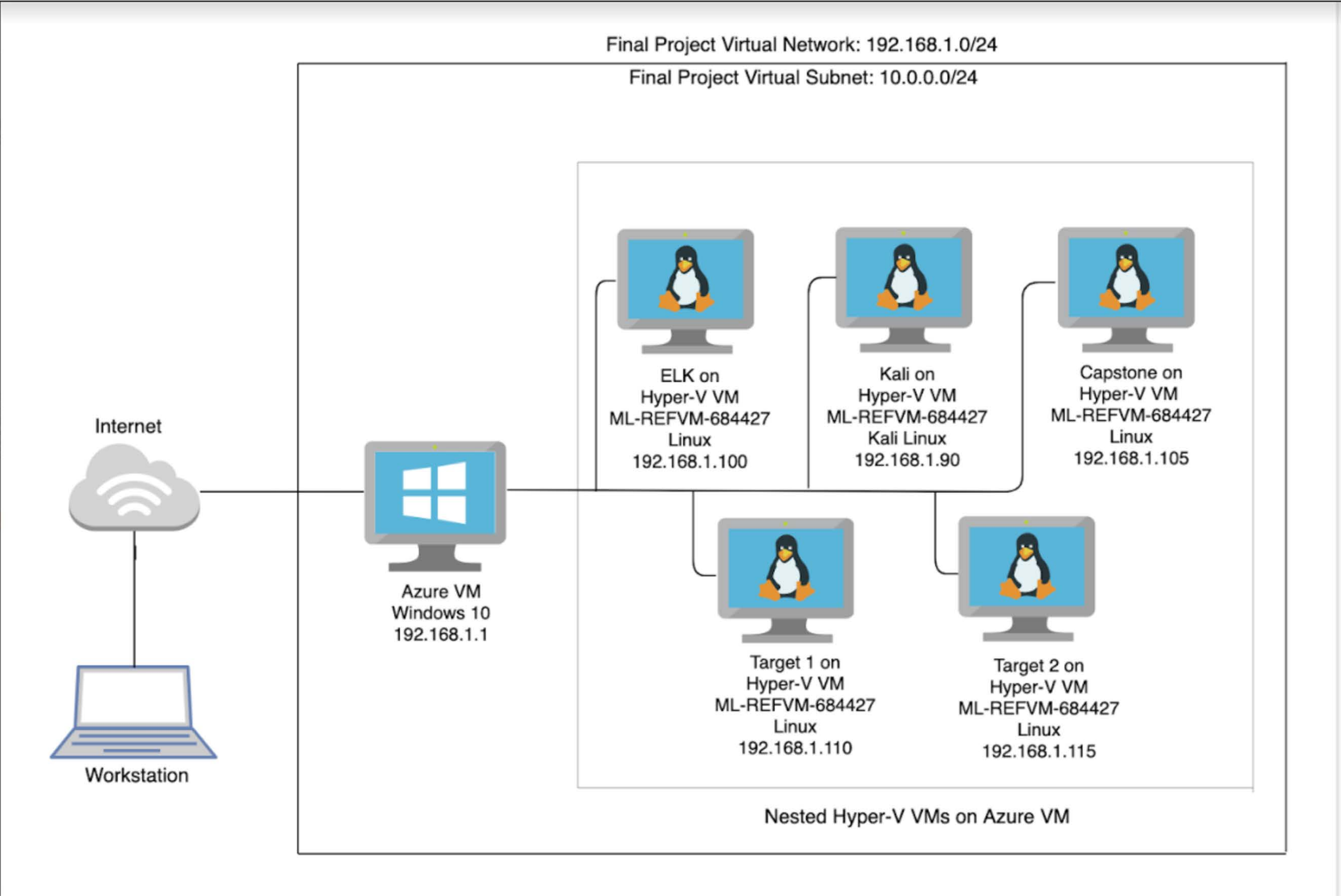
Normal Activity



Malicious Activity

Network Topology & Critical Vulnerabilities

Network Topology



Network Address
Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.1
OS: Windows 10
Hostname: Azure VM
ML-REFVM-684427

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali
IPv4: 192.168.1.100

OS: Linux
Hostname: ELK
IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Wordpress Vulnerability	Wordpress Content Management plugins for username, password makes it vulnerable. Enumeration attack on this vulnerability gives out usernames.	Helps hacker with reconnaissance in collecting usernames on the system.
Weak password Policy	Weak password allows user to select easy password which are cracked easily. Using username as password or password length with short length. No mix of uppercase and special characters makes system vulnerable.	Easy passwords are very dangerous for giving out system information as whole system becomes available to hacker. Michael's account has access to database information. Steven's account has special privileges.
Secure Shell Port Open	Open secure shell service is serious attack surface. Hacker can easily brute force on this to gather user account information.	Breaking down user account access is like giving keys to the kingdom.
CWE-307: Brute Force attacks	Allows hacker to specialized tools to crack passwords.	Once password is cracked, User has good access to the system.

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
Wordpress wp-config.php vulnerability	Database root password was stored in an application configuration file	This has a high impact because the threat can gain access to machine, the password will be easily available and they can quickly gain access to the database.
Privilege escalation by sudo python (CVE-2006-0151)	Allows a local users to gain privileges by using a Python script	provides root escalation this is very dangerous and impactful because it provides root to the threat actor
Directory Listing Vulnerability	Directory listing vulnerability displays directory contents.	The attacker was able to browse through directory and files and obtained phpmailer
PHPMailer Vulnerability	PHPMailer version user had several exploits. Metasploit listed several of those exploits.	This exploit allowed hacker to edit .pl file to upload PHP file. Creating an executable file and running it can give hacker shell access on the system.
Mysql UDF dynamic library Privilege escalation	A well documented exploit is available ready to compile that allows an unprivileged user to gain root	This allowed the attacker to jump from the www-data user to root

Traffic Profile

Traffic Profile

Feature	Value	Description
Top Talkers (IP Addresses)	185.243.115.84 (green.mattingsolutions.co) 172.16.4.205 (Rotterdam-PC) 10.6.12.203 (Ted n Frank Laptop) 23.43.62.169 (Akamai Server) 172.16.4.4 (Mind-hammer-DC) 10.0.0.201 (Blanco-Desktop) 10.11.11.11 (okay-boomer-dc)	Machines that sent the most traffic.
Most Common Protocols	SSL, HTTP, TCP UDP, DNS, DHCP, LDAP, Kerberos, SMB, ARP	Most common protocols on the network.
# of Unique IP Addresses	808	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.
	Betty Boop on the Reservations.avi	

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Web browsing, Web Blogging, DNS queries, DHCP requests

Suspicious Activity

- Malware download,
- Surfing Malware Infected Site,
- Torrent downloads,

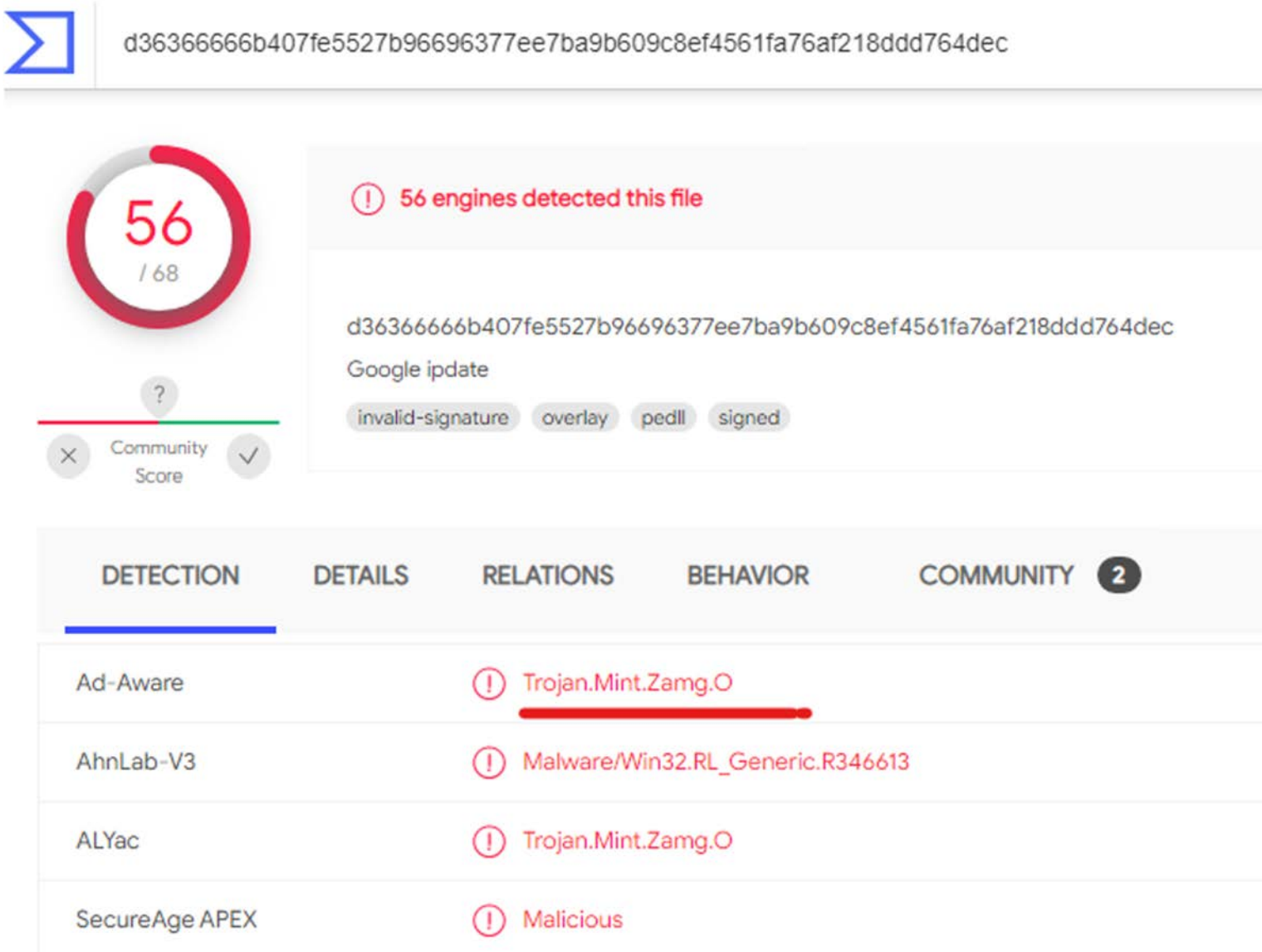
Public Domain Movies

Betty Boop - Rythm on the Reservation

Categories: [animation](#)
User rating: ⭐⭐⭐



1. Click “Start Now”
2. Download Now
3. Get Quick Access To Popular Templates





Normal Activity

[Browsing / Downloading]

- Significant amount of traffic was for browsing and downloading using SSL, HTTP, TCP UDP, DNS, DHCP, Kerberos, SMB
- Some of the User visited Sites are : Public Domain Torrents and Sabetha Community Hospital, Word Press Website, Time.com and iPhone Hacks, Watching You Tubes.

ip.addr == 168.215.194.14

No.	Time	Source	Destination
67264	752.320941200	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com
67265	752.322008800	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com
67266	752.322921500	files.publicdomaintorrents.com	BLANCO-DESKTOP.dogoftheyear.net
67267	752.323790800	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com
67268	752.331198600	BLANCO-DESKTOP.dogoftheyear.net	files.publicdomaintorrents.com
67269	752.332066200	files.publicdomaintorrents.com	BLANCO-DESKTOP.dogoftheyear.net
67270	752.332983400	files.publicdomaintorrents.com	BLANCO-DESKTOP.dogoftheyear.net

> Flags: 0x40, Don't fragment

Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x0d54 [validation disabled]

[Header checksum status: Unverified]

Source Address: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201)

Destination Address: files.publicdomaintorrents.com (168.215.194.14)

HOME LOG IN
SIGNUP

1TB Harddrive
with ALL 900+
divx PD movies
Only - \$550!

SMOOTH RIDE
Air Adjustable
Shocks

RENT ME!
Over 120,000
Unique Visitors
See This Spot
Every Month.
(Click Here)

Public Domain Torrents

Movies that made History...Sort of...

Download Movies - Classic Movies and B-Movies For FREE!

Fast Online Custom Print Shop & Printing
Services | 4OVER4.COM

SHOP NOW

LAST 5 Movie Comments/Ratings (Downloads are free, but to rate or leave comments you must sign up)

http.req

No.	Time	Source	Destination
38778	506.424691800	DESKTOP-B49J3FD.local	www.sabethahospital.com
38931	508.011584300	DESKTOP-B49J3FD.local	www.sabethahospital.com
38932	508.019456400	DESKTOP-B49J3FD.local	www.sabethahospital.com
38933	508.027351400	DESKTOP-B49J3FD.local	www.sabethahospital.com
38936	508.036784400	DESKTOP-B49J3FD.local	www.sabethahospital.com
38937	508.044390000	DESKTOP-B49J3FD.local	www.sabethahospital.com
38941	508.067091600	DESKTOP-B49J3FD.local	www.sabethahospital.com

Sabetha
Community
Hospital

14th & Oregon Street |

Employee E-mail

Home About Us Sabetha Hospital Family Practice Clinic Home Health & Hospice Monthly Health Topics

The Wound Care Center
at Sabetha Community Hospital

Open Now

Click For More Info

11

[Blogging / Domain Controller Traffic]

- Good amount of blogging traffic using HTTP Protocol POST Method. User was going to mysocalled Chaos.com website.
- Significant amount of traffic between a machine and its Domain Controller using RPC_NETLOGON Protocol. Domain Controller responds to Security Authentication Requests.



rpc_netlogon				
No.	Time	Source	Destination	Protocol
32415	463.600178400	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind-hammer.net	RPC_NETLOGON
32416	463.617045500	mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	RPC_NETLOGON
32595	464.191398200	Gilbert-Win7-PC.okay-boomer.info	okay-boomer-dc.okay-boomer.info	RPC_NETLOGON
32596	464.192832300	okay-boomer-dc.okay-boomer.info	Gilbert-Win7-PC.okay-boomer.info	RPC_NETLOGON
32600	464.200892800	Gilbert-Win7-PC.okay-boomer.info	okay-boomer-dc.okay-boomer.info	RPC_NETLOGON
32601	464.202483300	okay-boomer-dc.okay-boomer.info	Gilbert-Win7-PC.okay-boomer.info	RPC_NETLOGON
32610	464.227248300	Gilbert-Win7-PC.okay-boomer.info	okay-boomer-dc.okay-boomer.info	RPC_NETLOGON

Malicious Activity

Download Malicious Data


Summarize the following:

- Frank-n-Ted downloaded June.dll using HTTP GET request.
- VirusTotal.com showed June.dll containg Trojan Virus.

malicious files and accessing malicious sites such as green.mattingsolutions.com.

- Include screenshots of packets justifying your conclusions.

ip.addr == 10.6.12.203 && http				
No.	Time	Source	Destination	Info
58748	658.621258400	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	GET /pQBtWj HTTP/1.1
58750	658.630781400	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP/1.1 302 Found
58752	658.636633700	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	GET /files/june11.dll
59388	668.197470500	205.185.125.104	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP/1.1 200 OK
59680	669.903931800	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgtqismb.com	POST /post.php HTTP/1
59682	669.911770400	snnmnkxdhflwgtqismb.com	LAPTOP-5WKHX9YG.frank-n-ted.com	HTTP/1.1 200 OK (tex
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258				
Hypertext Transfer Protocol				
GET /files/june11.dll HTTP/1.1\r\n				
Accept: */*\r\n				
Accept-Encoding: gzip, deflate\r\n				
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n				
Host: 205.185.125.104\r\n				
Connection: Keep-Alive\r\n				
Cookie: _subid=3mmhfd8jp\r\n				
\r\n				
[Full request URI: http://205.185.125.104/files/june11.dll]				
[HTTP request 2/2]				



d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

56

/ 68

Community Score

56 engines detected this file

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Google ipdate

invalid-signature overlay pedll signed

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 2

Ad-Aware

Trojan.Mint.Zamg.O

AhnLab-V3

Malware/Win32.RL_Generic.R346613

ALYac

Trojan.Mint.Zamg.O

SecureAge APEX

Malicious

Torrenting

- Good amount of Torrenting activity was observed using BitTorrent Protocol
- Significant amount of traffic coming from files.publicdomaintorrents.com to BLANCO-DESKTOP.dogoftheyear.com and some traffic from fcmatch.youtube.com.
- We observed a download from download.deluge-torrent.org, DNS query from router.bittorrent.com and files.publicdomaintorrents.com



Public Domain Movies

Betty Boop - Rythm on the Reservation

Categories: [animation](#)

User rating: ★★☆☆

START NOW

1. Click "Start Now"
2. Download Now
3. Get Quick Access To Popular Templates



The End