

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

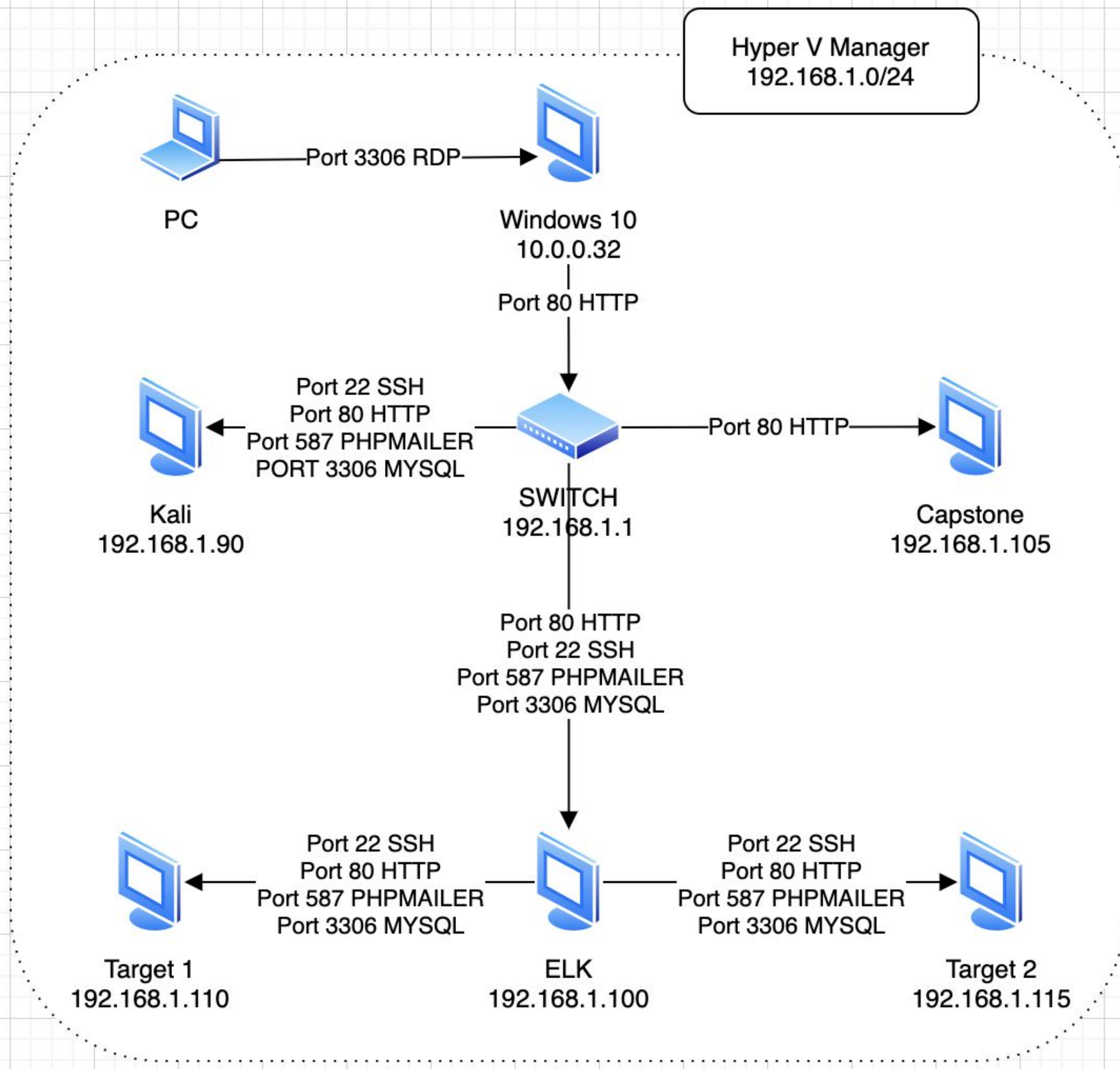


Malicious Activity

Network Topology & Critical Vulnerabilities



Network Topology



Network

Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.110
OS: Linux
Hostname: TARGET1

IPv4: 192.168.1.115
OS: Linux
Hostname: TARGET2

Critical Vulnerabilities: Target 1

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

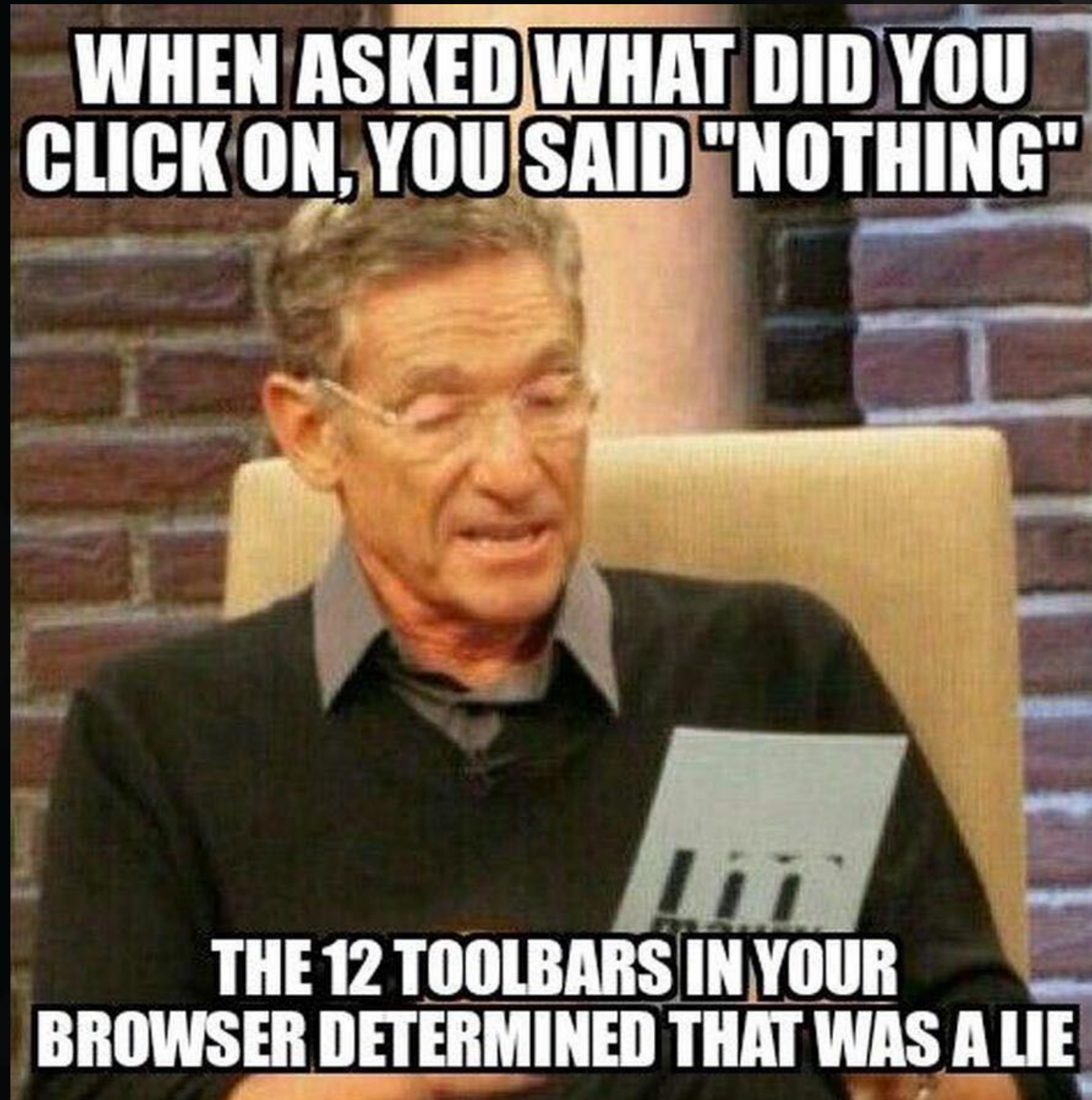
Vulnerability	Description	Impact
WordPress Site Enumeration	Use of WordPress Security Scanner (wpscan) against server (192.168.1.110) reveals sensitive information	The WordPress Security Scanner reveals the usernames: “michael” and “steven”
Brute Force Attack (michael)	By using Metasploit’s ssh_login module, user michael’s password can be cracked on the target	Malicious attackers can ssh into the TARGET1 server as user michael
wp-config.php readability	wp-config.php reveals sensitive information about root password for MySQL database	Vulnerable user michael has access to viewing wp-config.php which reveals root password for MySQL
John the Ripper (steven)	Using John on a hashed password for Steven found in MySQL	User steven’s hashed password cracked and obtained
Privilege escalation with Python	Exploit steven’s sudo permissions on python to gain root access of system: sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’	Steven’s sudo permissions with Python can be leveraged to gain root access of the system

Critical Vulnerabilities: Target 2

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

Vulnerability	Description	Impact
Wordpress Scan	<ul style="list-style-type: none">● WPScan Tool to scan a server's Wordpress database for any vulnerabilities.● Can also be done using an nmap script.	<ul style="list-style-type: none">● Hidden folders such as "manual" and "vendor" were revealed in the scan.● Accessing "vendor" folder and the VERSION page leads to a single flag.
PHPMailer 5.2.16	<ul style="list-style-type: none">● Exploitdb search revealed an RCE vulnerability for PHPMailer versions below 5.2.18	<ul style="list-style-type: none">● Uploading a unique PHP script into the server and calling on it will send a shell to the attacker machine.
MySQL Root Access	<ul style="list-style-type: none">● Access to server's MySQL database as 'root' allows the attacker to administer the database.	<ul style="list-style-type: none">● Attacker can create tables and functions that can allow the attacker to take control from MySQL.

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 10.0.0.201	Machines that sent the most traffic.
Most Common Protocols	DNS, HTTP, TCP	Three most common protocols on the network.
# of Unique IP Addresses	809	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	2	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 inconspicuous websites such as Instagram, or purchasing toys

Suspicious Activity

- Trojan, Malware and Illegal downloads via Torrent

Normal Activity



MySoCalledChaos

- Through ordinary HTTP traffic we are able to see that the user browses the site mysocalledchaos rather regularly, a blog for mothers that also sells niche products through Amazon
- A quick check via VirusTotal.com shows that the site and its plugins are not malicious

6707	95.145293200	172.16.4.205	166.62.111.64	HTTP	409	GET /wp-content/uploads/2018/11/AdventCalendarFillers-400x600.jpg HTTP/1...
6824	97.016631600	172.16.4.205	166.62.111.64	HTTP	413	GET /wp-content/uploads/2018/11/12-Days-of-Christmas-Swap-400x600.jpg HT...
6910	98.434702000	166.62.111.64	172.16.4.205	HTTP	255	HTTP/1.1 200 OK (JPEG JFIF image)
6936	98.697789700	172.16.4.205	166.62.111.64	HTTP	394	GET /wp-content/uploads/2018/02/footer-218x300.png HTTP/1.1
6996	99.454591000	54.230.89.184	172.16.4.205	HTTP	432	HTTP/1.1 200 OK (text/html)
7084	101.005103500	166.62.111.64	172.16.4.205	HTTP	1223	HTTP/1.1 200 OK (JPEG JFIF image)
7091	101.020430200	172.16.4.205	166.62.111.64	HTTP	598	GET /wp-content/plugins/instagram-feed/img/small-logo.png HTTP/1.1
7455	106.200700200	166.62.111.64	172.16.4.205	HTTP	456	HTTP/1.1 200 OK (PNG)

Request URI: /wp-content/uploads/2018/11/AdventCalendarFillers-400x600.jpg

Request Version: HTTP/1.1

Host: mysocalledchaos.com\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n

Accept: image/webp,*/*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

DNT: 1\r\n

Connection: keep-alive\r\n

Referer: http://mysocalledchaos.com/\r\n

\r\n

[Full request URI: http://mysocalledchaos.com/wp-content/uploads/2018/11/AdventCalendarFillers-400x600.jpg]

Cardboard Spaceship Toys

- Through HTTP Get protocols we are able to see additional normal behaviour such as an invoice for a purchase at Cardboard Spaceship Toys
- As shown below, and with further inspection via VirusTotal.com, the invoice file holds no malicious activity

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
57913	652.341073200	172.93.120.242	10.6.12.157	HTTP	561	HTTP/1.1 302 Found (text/html)
58748	658.621258400	10.6.12.203	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
58750	658.630781400	205.185.125.104	10.6.12.203	HTTP	542	HTTP/1.1 302 Found
Frame 57913: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface eth0, id 0						
Ethernet II, Src: Cisco_29:41:7d (ec:c8:82:29:41:7d), Dst: Intel_68:42:d3 (00:11:75:68:42:d3)						
Internet Protocol Version 4, Src: 172.93.120.242, Dst: 10.6.12.157						
Transmission Control Protocol, Src Port: 80, Dst Port: 49728, Seq: 1, Ack: 460, Len: 507						
Hypertext Transfer Protocol						
HTTP/1.1 302 Found\r\n						
Date: Fri, 12 Jun 2020 17:14:45 GMT\r\n						
Server: Apache\r\n						
Location: https://cardboardspaceshiptoy.com/logs/invoice-86495.doc\r\n						
Content-Length: 241\r\n						
Keep-Alive: timeout=5, max=100\r\n						
Connection: Keep-Alive\r\n						
Content-Type: text/html; charset=iso-8859-1\r\n						
\r\n						
[HTTP response 1/1]						
[Time since request: 0.022311200 seconds]						
[Request in frame: 57901]						
[Request URI: http://cardboardspaceshiptoy.com/logs/invoice-86495.doc]						
File Data: 241 bytes						

Malicious Activity

AAAAAAA

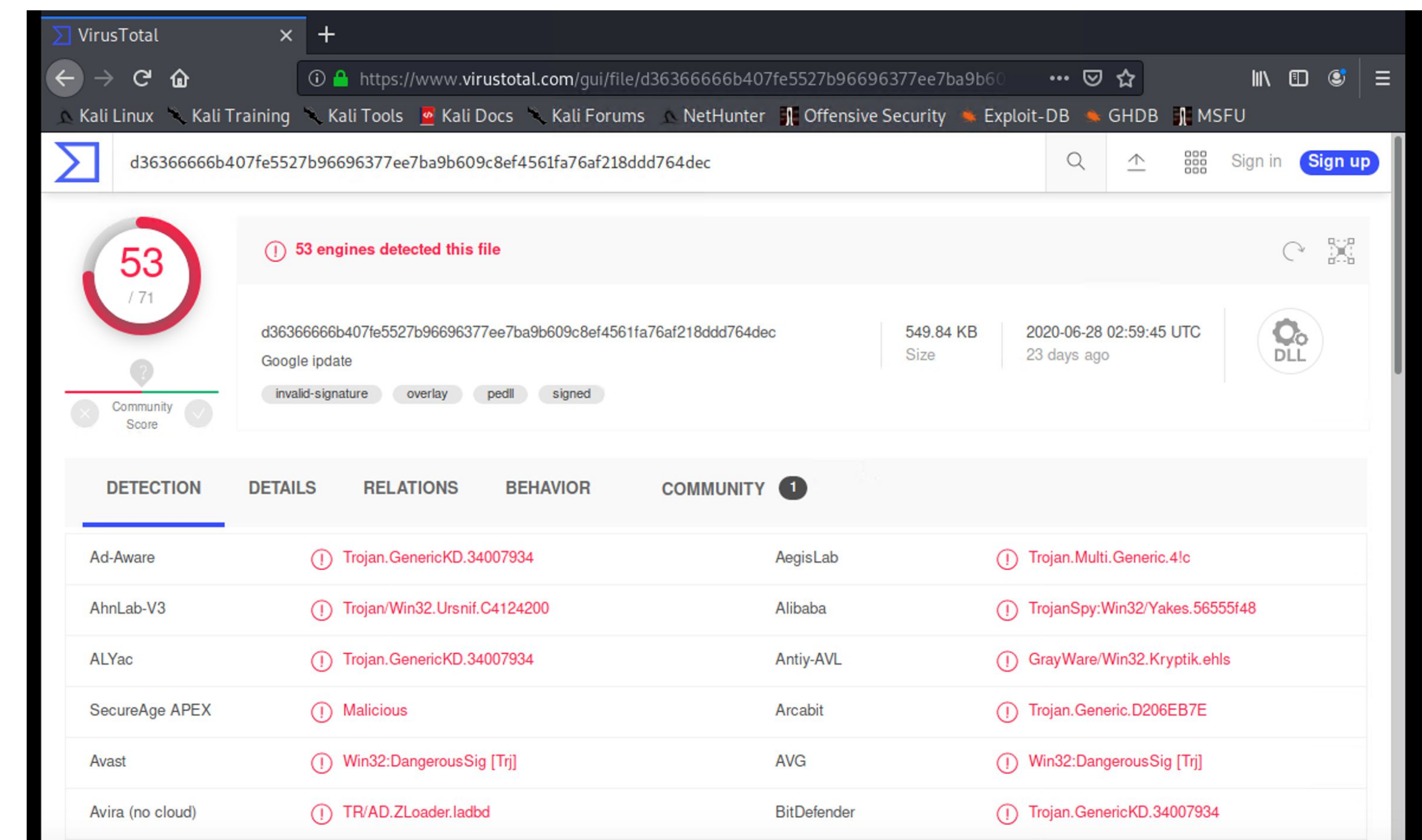
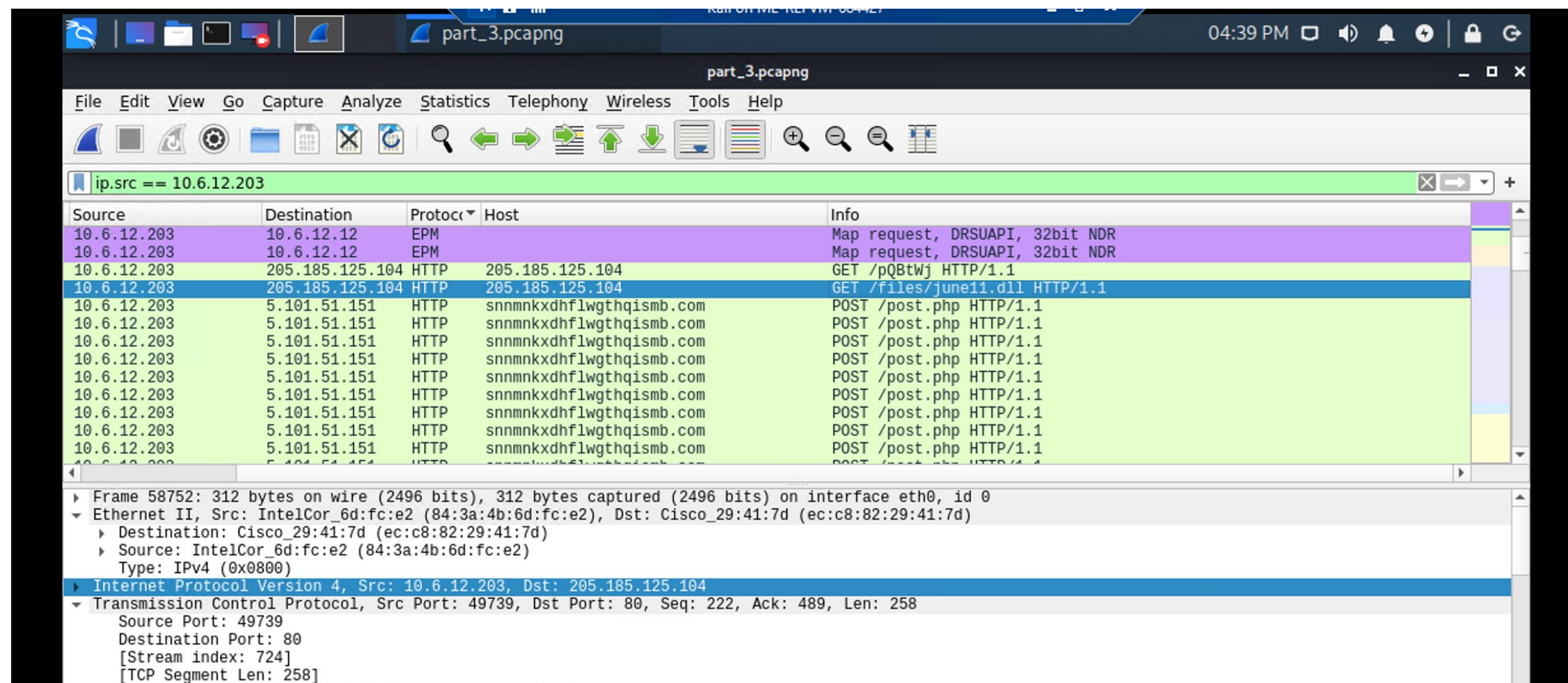
AA AAAAAAAAAA AA AAA AAAAAA AA AAA:AAAAAAA AA AAA AAA AAA(AA) +
AAAAAAA. AAA AAA AAAAAA AAA AAA:AAAAAAA AA AAA AAAAAAAA(AA) +
AAAAAAA. AA AAA AA AAAAAA AA AAAAAA AAAAAA.

* AAAAA AAA AAA AA AAAAA AA AAAAAA.
* AAAAA AAA+AAA+AAAA AA AAAAA AAA AAAAAA. AAA AAA
AAA AAA AAAAA AAAAAAAA AA AAA AAAAAA.

AAAA AAA AAA AA AAAAAA

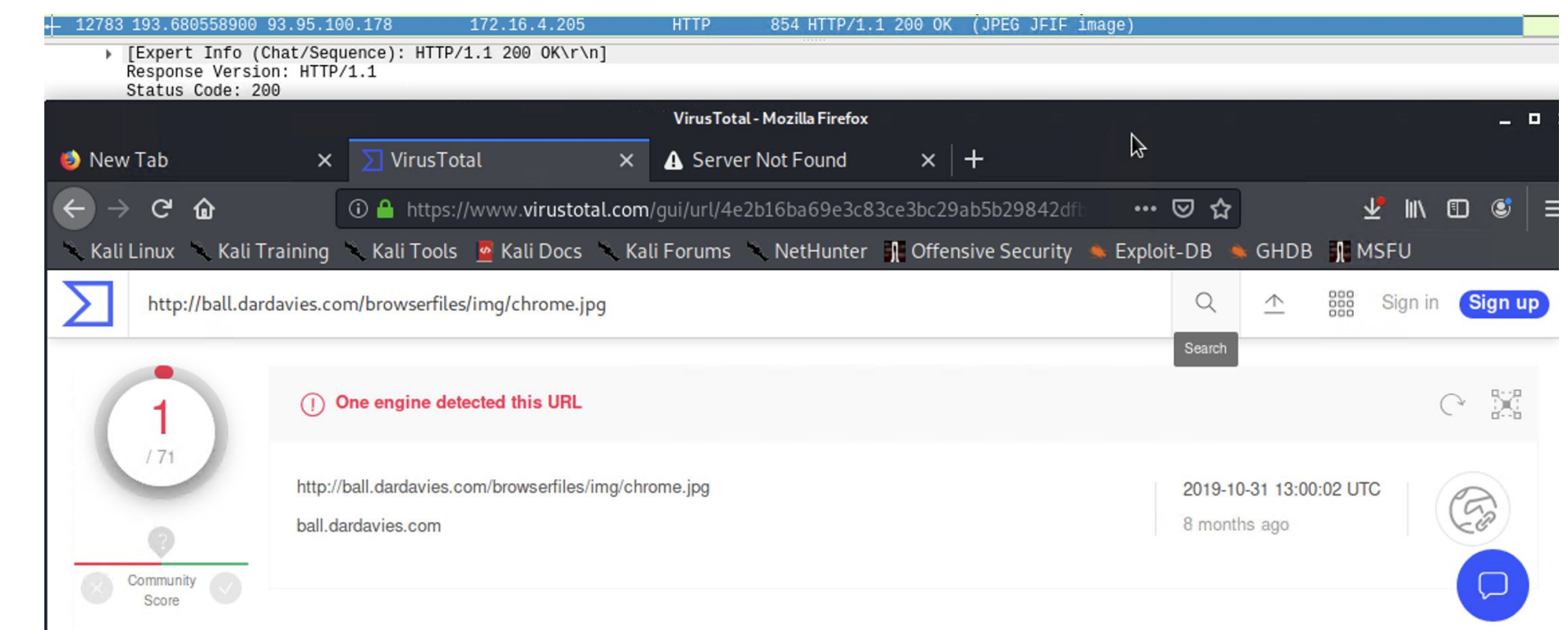
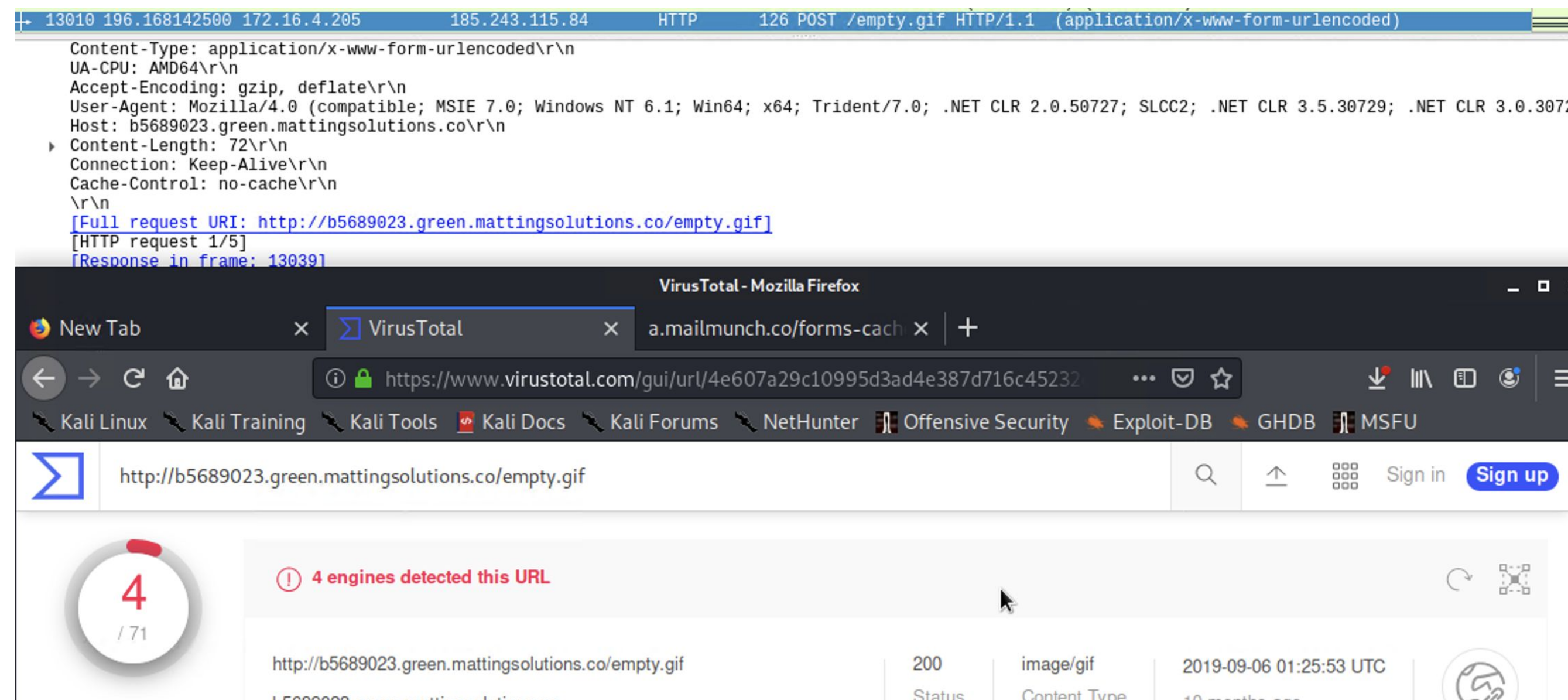
Time Thieves

- Via a custom site, frank-n-ted.com, two users were able to watch Youtube videos during work hours
- A Domain Controller (DC) with an IP of 10.6.12.12 on their custom Active Directory (AD) Network was established
- Trojan Malware named june11.dll was downloaded on 10.6.12.203
- Using VirusTotal.com we are able to determine that the file has 53 engines

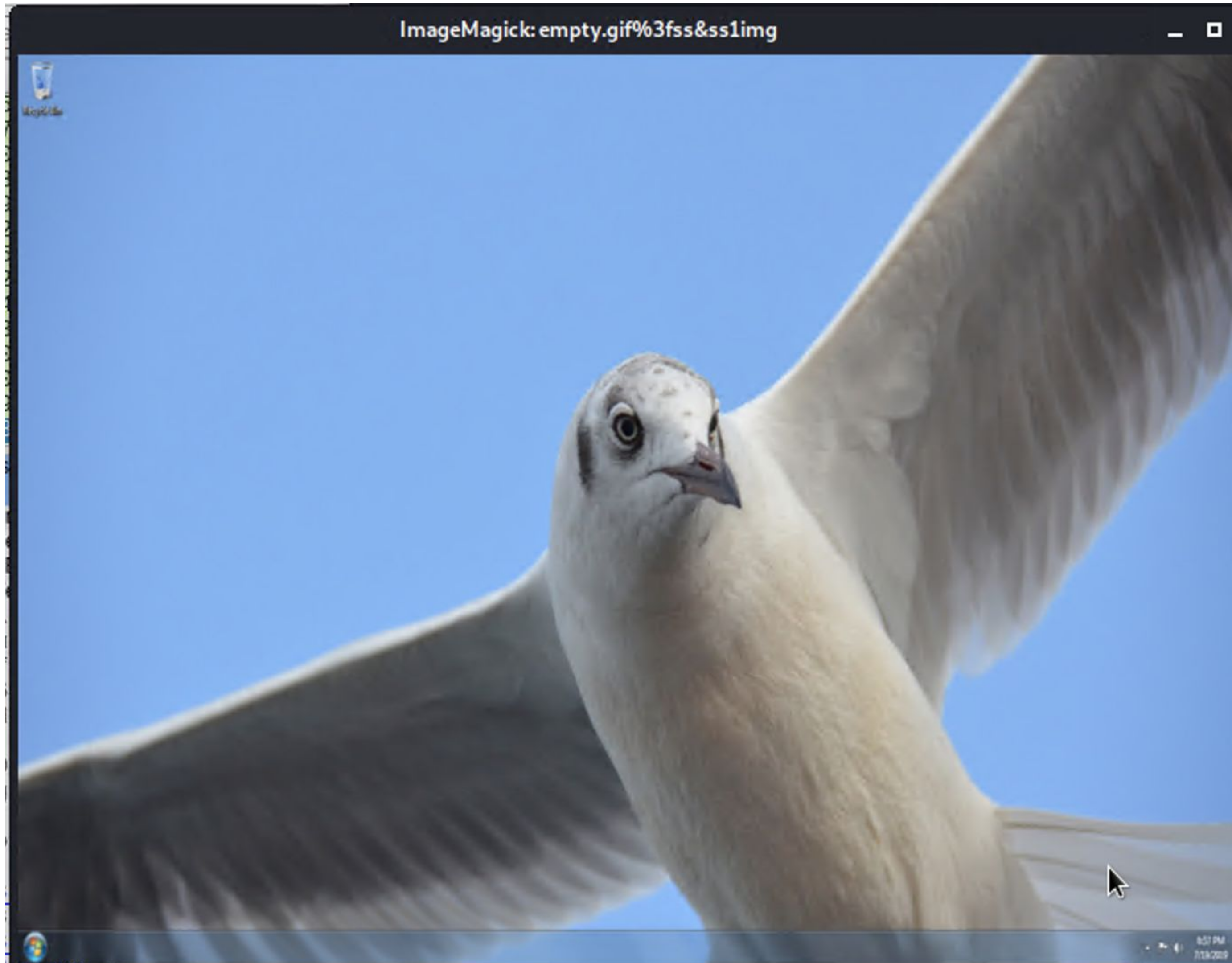


Malware

- The infected Windows machine on the network is Rotterdam-PC with an IP address of 172.16.4.205 and a MAC address of 00:59:07:b0:63:a4
- The user name of the Windows user with the infected machine is matthjis.devries
- IP addresses involved in the infection traffic include 185.243.115.84, 93.95.100.178



Hidden Desktop Background



Illegal Downloads via Torrent

- Web traffic via HTTP Get protocol was used to torrent Betty Boop Rhythm on the Reservation.avi.torrent
- The offending party under the involved was elmer.blanco with a Windows NT 10.0 OS and a MAC address of (00:16:18:66:c8)

ip.addr == 10.0.0.0/24 && ip.src == 10.0.0.201 && http contains torrent						
No.	Time	Source	Des	Protocr	Len	Info
69142	765.263272500	10.0.0.201	1...	HTTP	4...	GET /yellow-star.gif HTTP/1.1
69150	765.279673000	10.0.0.201	1...	HTTP	4...	GET /pagead/show_ads.js HTTP/1.1
69155	765.290109300	10.0.0.201	5...	HTTP	4...	GET /tools/diggthis.js HTTP/1.1
69167	765.416418700	10.0.0.201	1...	HTTP	5...	GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
69213	765.837950500	10.0.0.201	1...	HTTP	4...	GET /divxi.jpg HTTP/1.1
69298	766.857868300	10.0.0.201	5...	HTTP	4...	GET /s/ads.js HTTP/1.1
69347	767.585292600	10.0.0.201	1...	HTTP	5...	GET /usercomments.html?movieid=513 HTTP/1.1
69434	768.625230500	10.0.0.201	5...	HTTP	4...	GET /s/ads-common.js HTTP/1.1
69470	768.919511100	10.0.0.201	7...	HTTP	8...	GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FD00B68&ref-url=http%3A//publicdom...
69542	769.560506300	10.0.0.201	5...	HTTP	1...	GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C%22tag%22%3A%22p...
69706	770.366956400	10.0.0.201	1...	HTTP	5...	GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HT...
69750	770.563257500	10.0.0.201	1...	HTTP	1...	GET /version-1.0 HTTP/1.1
69754	770.572697300	10.0.0.201	9...	HTTP	4...	GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97be%5c%8d%be&peer_id=-DE13F0...
69980	771.231145500	10.0.0.201	1...	HTTP	4...	GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe&peer_id=-D...
Frame Number: 69706						
Frame Length: 589 bytes (4712 bits)						
Capture Length: 589 bytes (4712 bits)						
[Frame is marked: False]						
[Frame is ignored: False]						
[Protocols in frame: eth:ethertype:ip:tcp:http]						
[Coloring Rule Name: HTTP]						
[Coloring Rule String: http tcp.port == 80 http2]						
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)						
0000	00 09 b7 27 a1 3e 00 16 17 18 66 c8 08 00 45 00	...>...f...E				
0010	02 3f 76 d1 40 00 80 06 0c 39 0a 00 00 c9 a8 d7	?v@...9.....				
0020	c2 0e c2 aa 00 50 97 b7 b1 25 75 99 6b 48 50 18P...%u.kHP				
0030	ff ff 31 06 00 00 47 45 54 20 2f 62 74 2f 62 74	..1...GE T /bt/bt				
0040	64 6f 77 6e 6c 6f 61 64 2e 70 68 70 3f 74 79 70	download.php?type				
0050	65 3d 74 6f 72 72 65 6e 74 26 66 69 6c 65 3d 42	e-torren t&file=B				
0060	65 74 74 79 5f 42 6f 6f 70 5f 52 68 79 74 68 6d	etty_Boo p_Rhythm				
0070	5f 6f 6e 5f 74 68 65 5f 52 65 73 65 72 76 61 74	_on_the_ Reservat				
0080	69 6f 6e 2e 61 76 69 2e 74 6f 72 72 65 6e 74 20	ion.avi. torrent				
0090	48 54 54 50 2f 31 2e 31 0d 0a 52 65 66 65 72 65	HTTP/1.1 . Refere				
00a0	72 3a 20 68 74 74 70 3a 2f 2f 70 75 62 6c 69 63	r: http: //public				
00b0	64 6f 6d 61 69 6e 74 6f 72 72 65 6e 74 73 2e 69	domainto rrents.i				
00c0	6e 66 6f 2f 6e 73 68 6f 77 6d 6f 76 69 65 2e 68	nfo/nsho wmovie.h				
00d0	74 6d 6c 3f 6d 6f 76 69 65 69 64 3d 35 31 33 0d	tml?movi eid=513				
00e0	0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a	.User-Ag ent: Moz				
00f0	69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77	illa/5.0 (Window				
0100	73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34	s NT 10. 0; Win64				

No.	Time	Source	Destination	Protocol	Length	Info
67262	752.318346900	10.0.0.201	10.0.0.2	DNS	85	Standard query 0x307d A publicdomaintorrents.info
69700	770.351745800	10.0.0.201	10.0.0.2	DNS	88	Standard query 0xdee1 A www.publicdomaintorrents.com
69729	770.525334900	10.0.0.201	10.0.0.2	DNS	81	Standard query 0xe7bb A router.bittorrent.com
69735	770.535832000	10.0.0.201	10.0.0.2	DNS	79	Standard query 0x7b0e A router.utorrent.com
69736	770.537226500	10.0.0.201	10.0.0.2	DNS	87	Standard query 0xbf76 A download.deluge-torrent.org
69745	770.555788300	10.0.0.201	10.0.0.2	DNS	78	Standard query 0x69b2 A torrent.ubuntu.com
69974	771.214457800	10.0.0.201	10.0.0.2	DNS	90	Standard query 0xee1a A files.publicdomaintorrents.com
70002	771.289020100	10.0.0.201	10.0.0.2	DNS	92	Standard query 0xb99f A tracker.publicdomaintorrents.com

65617	744.239448800	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
65625	744.255672900	10.0.0.201	10.0.0.2	KRB5	381	AS-REQ
65636	744.319236900	10.0.0.201	10.0.0.2	KRB5	292	TGS-REQ
65648	744.380721700	10.0.0.201	10.0.0.2	KRB5	95	TGS-REQ
Frame 65617: 301 bytes on wire (2408 bits), 301 bytes captured (2408 bits) on interface eth0, id 0						
Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Dell_f4:3b:96 (00:12:3f:f4:3b:96)						
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 10.0.0.2						
Transmission Control Protocol, Src Port: 49682, Dst Port: 88, Seq: 1, Ack: 1, Len: 247						
Kerberos						
Record Mark: 243 bytes						
0... .. = Reserved: Not set						
.000 0000 0000 0000 0000 0000 1111 0011 = Record Length: 243						
as-req						
pvno: 5						
msg-type: krb-as-req (10)						
padata: 1 item						
PA-DATA PA-PAC-REQUEST						
req-body						
Padding: 0						
kdc-options: 40810010						
cname						
name-type: KRB5-NT-PRINCIPAL (1)						
cname-string: 1 item						
CNameString: blanco-desktop\$						



The End