Joshua Reed
Cyber Security Bootcamp
September 24th, 2020

Network Security Analysis

An investigation of several security risks

Table of Contents

Introduction

The network was monitored with the program Wireshark, a packet capture tool used to view network packets going in and out of the system after the SOC team observed odd behavior coming from multiple IP addresses and downloads. After investigating multiple packets requested from specific IP addresses, several security discrepancies were observed and were reported on. These discrepancies were:

- DNS server (Domain Name Service) discovered on the company network
- A malicious download discovered containing a trojan horse malware
- Illegal torrent downloads violating copyright laws

Time Thieves

Two users were discovered by the SOC team wasting time on YouTube. Although the IT department usually doesn't concern themselves with this kind of behavior, it was noticed that these two individuals had created a web server on the company's network, draining company resources. The security team was given the following information for further investigation:

- An Active Directory Network was created
- The individuals constantly watch YouTube
- The IP addresses investigated were on the subnet range 10.6.12.0/24

During the investigation, the name of the webserver was discovered to be "frank-n-ted.com" on the IP 10.6.12.12. A download was discovered containing a malicious file on the network IP 10.6.12.203. The name of this file was "june11.dll." An archive of this file was uploaded to "VirusTotal.com" revealing this file to be a trojan horse that had infected the machine on 10.6.12.203. The infected machine will be taken down and serviced to repair any damage done and to prevent the virus from spreading laterally across the network.

Vulnerable Windows Machine

The security team received reports that a windows host machine had been infected on the network. The SOC team provided the following information to be investigated further:

- The infected machine was in the IP range of 172.16.4.0/24
- The domain “mind-hammer.net” is associated with the infected computer
- The domain controller is on the IP 172.16.4.4
- The network has a standard gateway and broadcast addresses

The Wireshark team filtered out the network traffic to reveal an IP address of 172.16.4.205 that was communicating with the “mind-hammer.net” domain. The infected Windows machine’s information was then gathered:

- Host Name: Rotterdam-PC
- IP Address: 172.16.4.205
- MAC Address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
- Username: matthijs.devries

With this information, the IT department was able to shut the infected host down and Mr. Devries was given security training to prevent any future malicious downloads from occurring.

In order to prevent the same download from happening, the Wireshark team also found the offending IP address (185.143.115.84) and saved it to the company blacklist. This IP was also released to certain online IP blacklists for others to use as well.

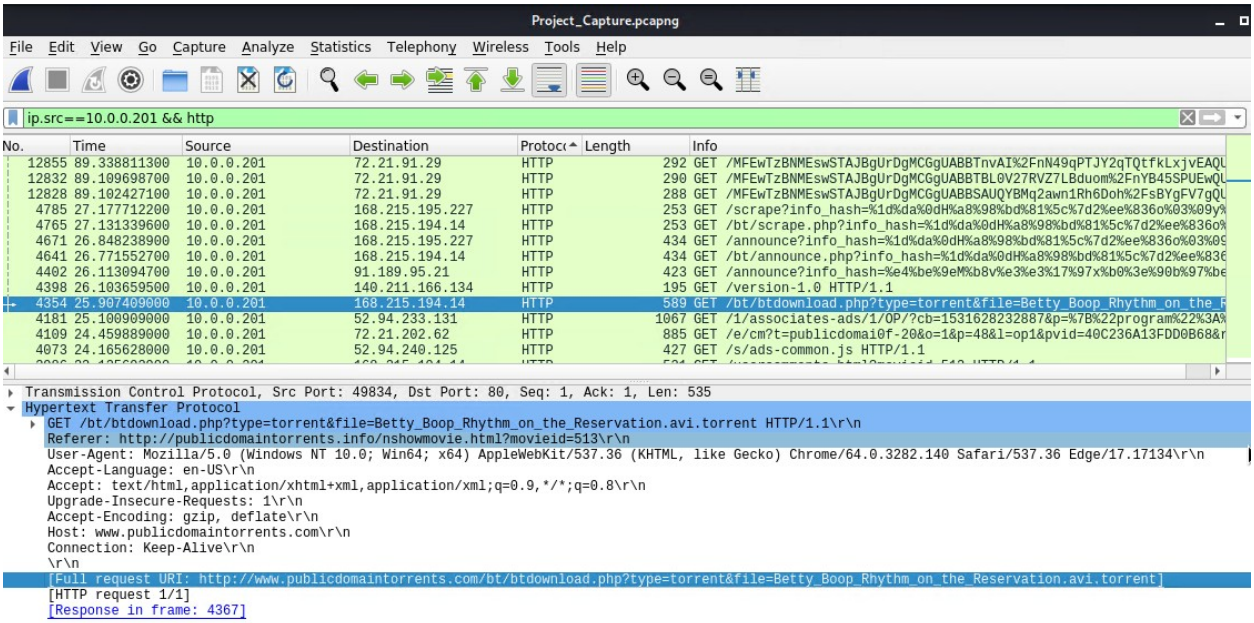
Illegal Downloads

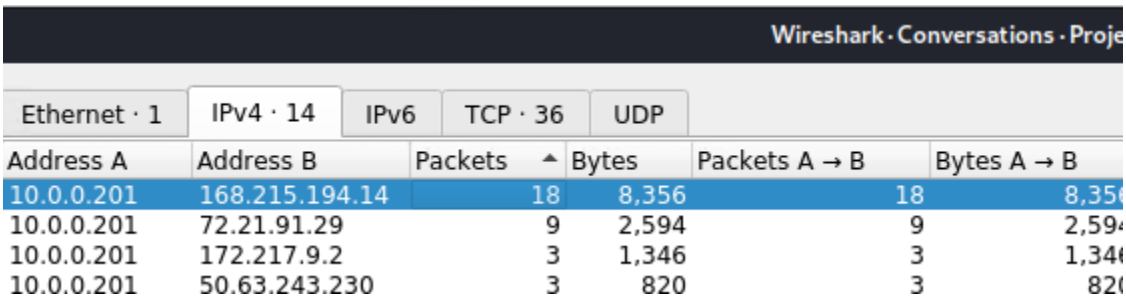
IT informed the security team that a user was torrenting Copyright protected media over the company network. Torrenting files are not strictly prohibited by company policy to allow employees to access legitimate files. However, this user was violating Copyright laws. IT handed over the following information to be investigated.

- Torrents downloaded on the IP range 10.0.0.0/24
- The domain controller is on 10.0.0.2
- The domain is associated with “dogoftheyear.net”

The torrent traffic was filtered through in Wireshark, and the machine located on IP 10.0.0.201 was discovered. By filtering for HTTP GET requests, the illegal torrent was discovered along with the host site the torrent was downloaded from. The following images

contain the torrent and torrent size





With the torrent found, the Wireshark team investigated who the individual was that downloaded the torrent. The following was discovered:

- MAC Address: MSI_18:66:c8 (00:16:17:18:66:c8)
- Windows Username: elmer.blanco
- OS version: Windows NT 10.0

Human Resources was notified of what Mr. Blanco has done, and will be deciding on further actions.