7/30/2021

Audit Report on “xyz.pcap” file

Amy Leung | 803921
SAIT | ITSC - 321A

Table of Contents

Table of Tables

Table of Figures

Abstract

No one wants a security scandal, however they happen daily to any company no matter the size; companies like Facebook [1], Hearing Care Network [2], Volkswagen [3], Royal Military College [4], etc. are not immune to targeted attacks. Facebook had a major **data leak** where over 533 million Facebook users had their phone numbers, IDs, full names, locations, birthdates, email addresses were leaked online to a forum [1]. Hearing care network had a **security breach** where an individual hacked into its provider of the hearing care network, Amazon Web Services and deleted information for 3.3 million patients [2]. Volkswagen had a **data breach** accessed by a leak exposed previously, the individual who attacked Volkswagen leaked 3.3 million peoples data found in the Volkswagen database [3]. The Royal Military college in Canada had a data breach where personal data was leaked in a cyberattack, not only did they take student information they also stole private institution information [4].

Security leaks, data breaches are incredibly important especially, when one takes into account the considerable fees. For example, the legal fees required to address the situation, cost to repair a network, cost to upgrade/purchase a security solution, etc. is costly to all targets no matter how big or small. To prevent such costly practices, it is important to get a systematic security audit. Avoiding data leaks and misuse of data is important for any company, and it is becoming even more important as services and access to network resources become more important to a company.

Background

A security audit is an evaluation of a company's network, when done a security audit will help protect critical data, identify security vulnerabilities, and present an effective security strategy. Regular systematic security audits can prevent potential security breaches, data leakage, protect user data, ensures company's and their employees stick to security practices, and catch new vulnerabilities found in the network. The client has asked us to complete an audit report and a risk assessment for its systems.

The client has provided a file named "xyz.pcap" this file is important for us to identify the malicious incident. The major concern for the client is the issues that is associated to the bandwidth, because there is a limited amount of bandwidth available this is a crucial concern.

Audit Objectives

The objectives for this audit are:

- Provide a assessment of the clients network
- Identify the malicious incident that is causing the bandwidth problem
- Provide potential areas of improvement

Glossary

CryptoJacking Or Cryptomining	-	A form of exploit where the attacker uses the resources on the target device to mine for digital currency, also known as malicious crypto mining. [5]
Botnet	-	Network of computers that automate attacks (data theft, server crash, malware, etc.). [6]
IP address	-	A unique address that identifies a device on the internet/local network.
Cryptocurrency	-	A decentralized digital currency with little to no central authority (laws). [7]
Blockchain	-	A database for cryptocurrency. [8]
http.request	-	An action (request) to be performed for a resource.
Uniform Resource Locater (URL)	-	Identifier used to locate a resource on the internet. EX. www.google.ca
Packet	-	Small segment of data, used for Handshakes and analysis.
Port	-	A number used to uniquely identify a transaction over a network. EX. Port 443 is for HTTPS
User-Agent	-	A request header used to identify application, OS, and Vendor.
JSON-RPC	-	A remote procedure call for JSON files. [9]
Hashrate	-	The measuring unit for processing power on the bitcoin network. [10]
Ufw (uncomplicated firewall)	-	Default firewall application for Linux OS.
Firewalld	-	Similar to the ufw. However, is more popular and has a friendlier interface.
Intrusion Detection System (IDS)	-	A software solution that monitors the network for malicious activity.
pfsense	-	A firewall/router that is more advanced, has a lot of features.
pfblocker	-	A package that allows the client to add a IP block list.

IP Block List **or** **Feeds**	-	A list of IPs that filter out malicious activity from accessing the client's network.
Server.xml	-	File that contains server configuration.
Apache Tomcat	-	Open source Server.
Active Directory	-	Microsoft Server.

Details of Finding

Identification of the malicious traffic

The Malicious incident seems to be a **cryptojacking botnet** that has been downloaded from the device with the **IP address** 172.16.253.129. Cryptojacking or malicious **cryptomining** is an exploit where malware uses the devices' resources such as the graphics processing unit (GPU) or central processing unit (CPU) to mine digital/virtual currency (**cryptocurrency**). [5] The reason why this company is having bandwidth issues is due to the malicious malware from the Trojan, the Trojan sends the data to the attacker when mining with the **blockchain**. The main indicators of compromise found are the IP, user-agent, domain name, hostname, reconstructed files, and a few patterns I found.

Analysis steps taken to identify the malicious traffic.

The first step I took was to find the device communicating on the network, and this can be found in the xyz.pcap using the **http.request** filter. A HTTP request is made by a client to a host on a server, the client device uses the **Uniform Resource Locator (URL)** to request access to a resource on the server. A HTTP **packet** can provide information such as **port** used/accessed, GET/POST methods, etc. http.request can also be used to find the operating system (OS) of a device. To find the OS we need to follow the TCP stream, by following the TCP stream we can see an abundant of information. To find the Device connected to the network I filtered by http.request, http.request tells us which device is making outgoing connections. Based on the http.request filter, we find that the only device making outgoing connections is 172.16.253.129 or DellXT because only one device is making outgoing connections we can infer that the DellXT device is the one having issues with bandwidth.

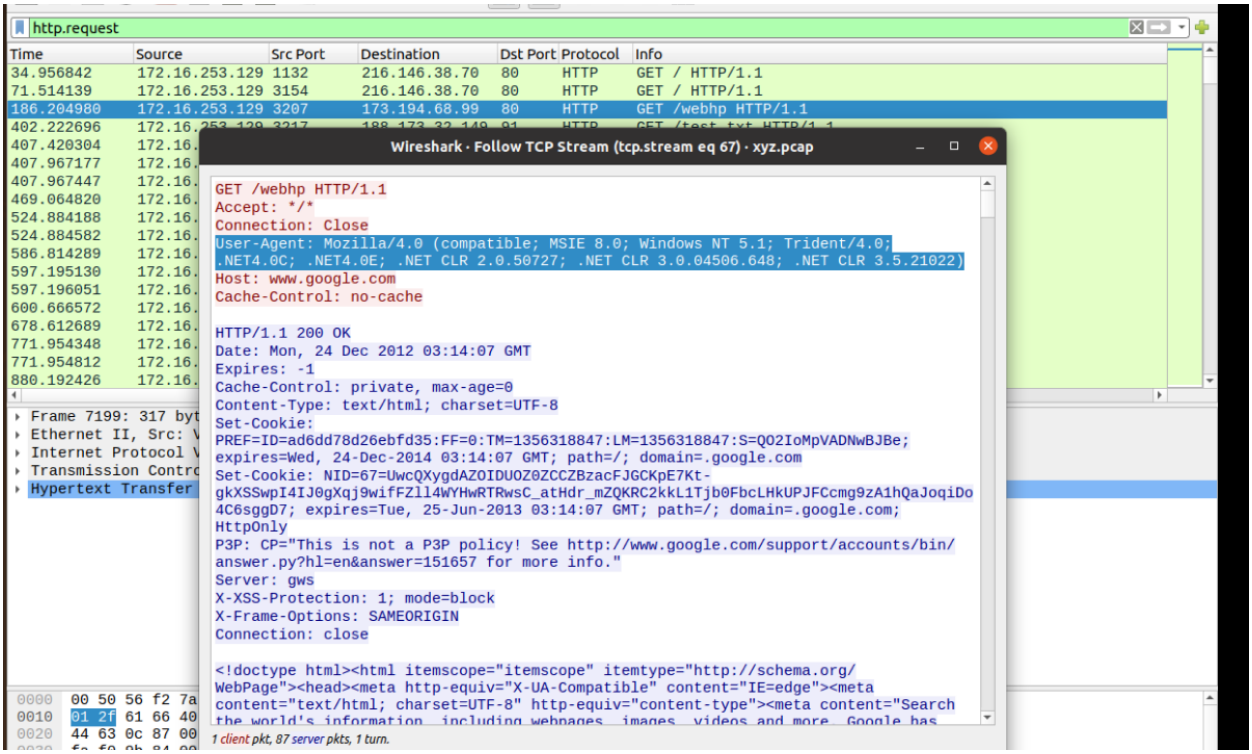


Figure 1: Example of a TCP stream of the HTTP packet from 172.16.253.129 (DellXT)

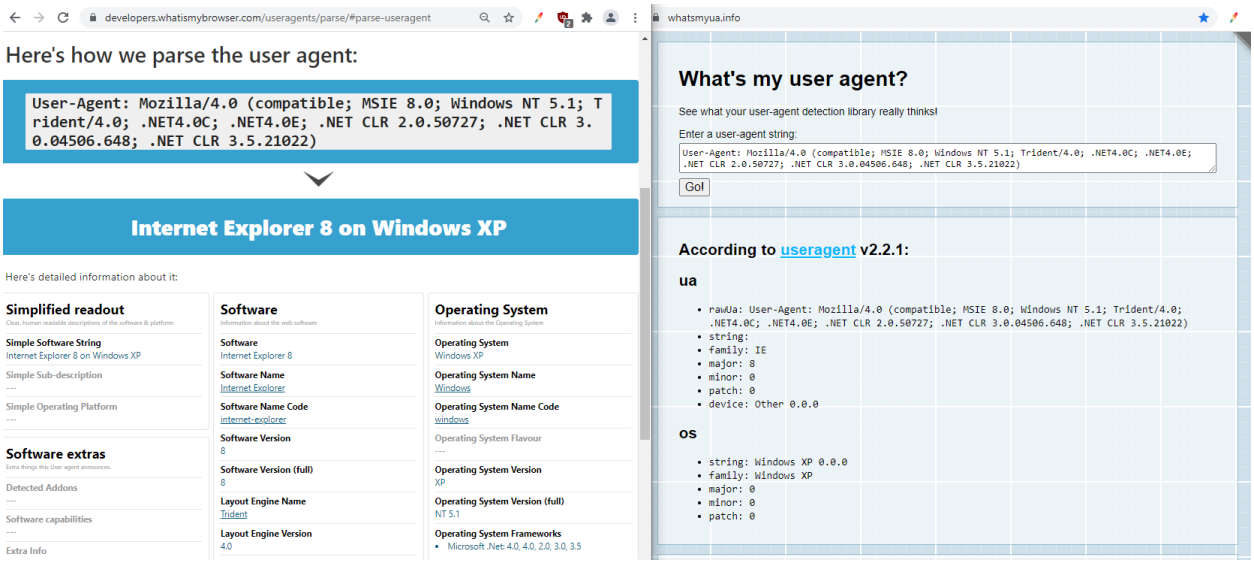
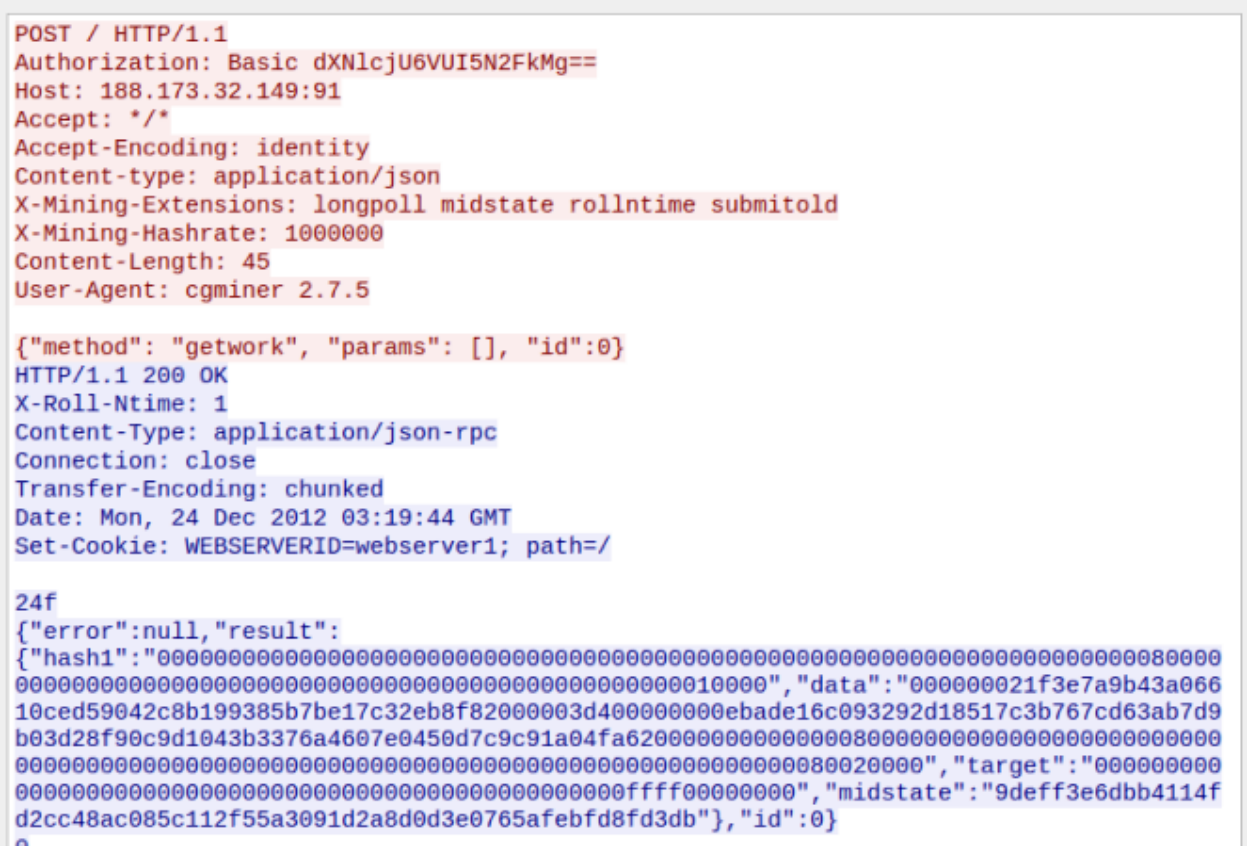


Figure 2: Example of using the User-Agent to get OS information



```
POST / HTTP/1.1
Authorization: Basic dXNlcjU6VUI5N2FkMg==
Host: 188.173.32.149:91
Accept: */*
Accept-Encoding: identity
Content-type: application/json
X-Mining-Extensions: longpoll midstate rollntime submitold
X-Mining-Hashrate: 1000000
Content-Length: 45
User-Agent: cgminer 2.7.5

{"method": "getwork", "params": [], "id":0}
HTTP/1.1 200 OK
X-Roll-Ntime: 1
Content-Type: application/json-rpc
Connection: close
Transfer-Encoding: chunked
Date: Mon, 24 Dec 2012 03:19:44 GMT
Set-Cookie: WEBSERVERID=webserver1; path=/

24f
{"error":null,"result":
{"hash1":"00000000000000000000000000000000000000000000000000000000000000800000
0000000000000000000000000000000000000000000010000","data":"000000021f3e7a9b43a066
10ced59042c8b199385b7be17c32eb8f82000003d400000000ebade16c093292d18517c3b767cd63ab7d9
b03d28f90c9d1043b3376a4607e0450d7c9c91a04fa62000000000000008000000000000000000000000
0000000000000000000000000000000000000000000000080020000","target":"000000000
0000000000000000000000000000000000000ffff00000000","midstate":"9deff3e6dbb4114f
d2cc48ac085c112f55a3091d2a8d0d3e0765afebfd8fd3db"},"id":0}
```

Figure 3: TCP stream of a packet it has got certain data by accessing the json application

The **User-Agent** from Figure 1 can be then entered into another tool like whatsmyua.info or developers.whatismybrowser.com (Figure 2) that can identify the OS from the user-agent. Figure 3 has an X-mining-Extensions header this means that someone is using this device to mine using an http transport. The “getwork” method in figure 3 is a “**JSON-RPC** method sent over a HTTP transport” [6]. Notice that x-mining-hashrate = 100000 this means that **hashrate** is high, that means there is a higher processing power in the network. Based on Table 1 and Figure 3, this packet is telling us that it will continually mine and submit data to the server, due to that bandwidth will continually be used as it needs to submit data at intervals when a new valid block has been generated. This is the reason as to why the client is having bandwidth issues.

Table 1: x-mining-extensions [6]

Extension name	Purpose
Longpoll	Notifies the miner(in this case the device) when a valid block has been generated and added to the blockchain.
Midstate	The initial hash of the first half of the data, after will be used as an input for the second half.
Rollntime	Time extension for mining
Submittold	Requires longpoll to work, submits the data mined to the server. After begins working on the new data.

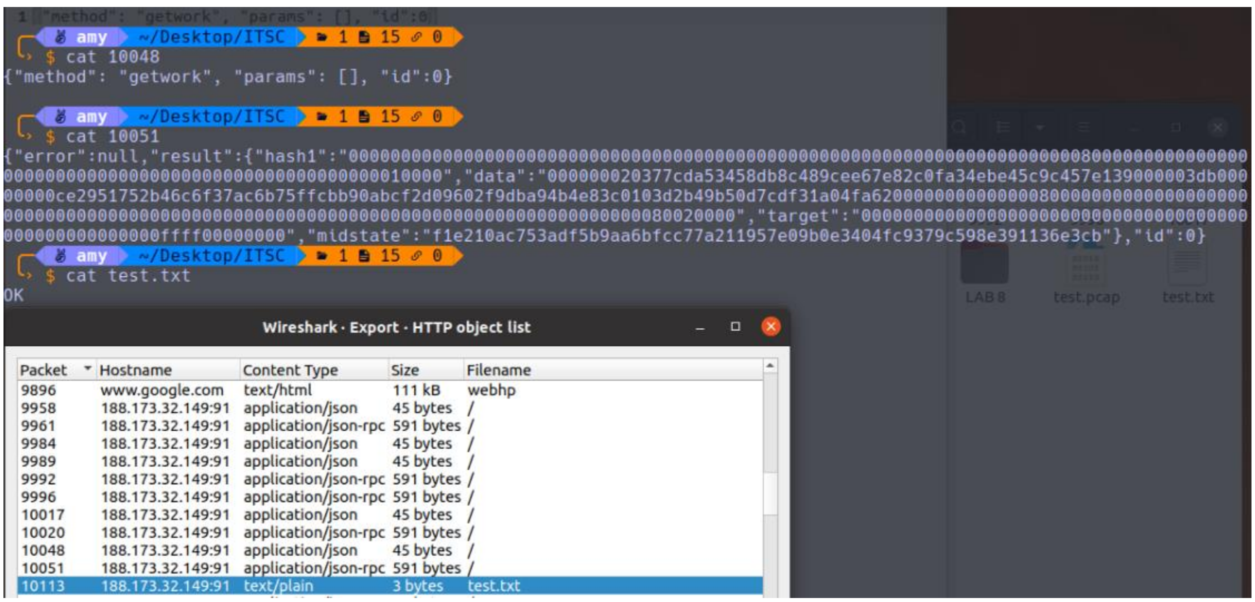


Figure 4: Export HTTP object list

As an extra area of interest, the json-rpc application can also be rebuilt from the pcap file. From figure 4 we can see that there is a series of progression, first what needs to happen is that the client device (DellXT) needs to access the “webhp” site from www.google.com, then a json application runs. After, the json-rpc application runs during this time the device is being used to mine data.

1. Client DellXT device access webhp
2. Packet 10048 shows that a getwork template request is being sent to the DellXT device

3. Packet 10051 shows that in response use this hash algorithm, operate using this data, to a certain target, perform first half of data.

4. Test.txt means that it has been successfully sent to the server

From packet No. 9754 -> 10124 took approximately 3 minutes, the duration of a single mine exchange based on the pcap file can be as long as ~3-20 minutes.

Risk analysis of threats to company assets

Based on the pcap file and the packet analysis, I have identified 4 vulnerabilities/risks in the client's network. The following risks were found:

1. Client is using a older Windows XP device

   This risk was found when finding the OS of the device, from table 2 we can see that the client device accessing the network is an older device, running windows XP. This is a security risk because Microsoft has discontinued with providing support for devices running windows XP [7]. The end of support means that the device is more vulnerable to security risks, malware, viruses, and will struggle performance wise because the support and security packs are no longer being updated.

2. Open Ports

   From figure 5 we can see that DellXP is being accessed by ports from 1132 – 3398. This means that there are way more ports than necessary being open and accessed to 172.16.253.129. Open **TCP ports** means there are more likely to be taken advantage of. One could exploit the device by accessing a backdoor. One could also introduce malware and/or malicious code to grab data. Open ports are hotspots for attacks, and attackers can use these ideal ports to find execute exploits.

   Attackers can use a fingerprint scan like nmap to report the client's software and applications being run. Port 1132-3398 are ports that are not assigned/controlled which means that an attacker can temporarily use the port to execute an attack [8].

   Open ports are a security risk that once can easily reduce.

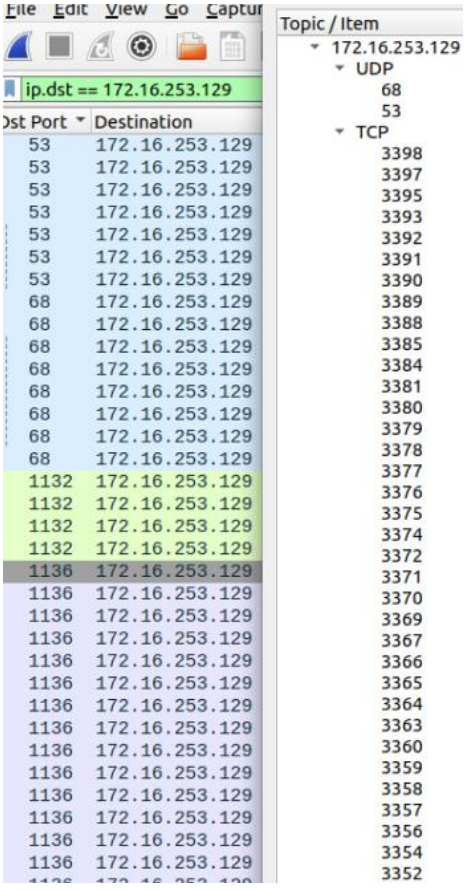


Figure 5: Destination ports to 172.16.253.129

3. No malware detection

Client Device 172.16.253.129 does not have a malware detection system. If there was one than it is most likely that it would have found the potential risks in the json-rpc application. From figure 4 based on the HTTP export list we can see multiple application json files, this is indicative of the fact that there is little to no malware/virus detection.

An example of this would be the December 2019 incident when a "Cryptocurrency-mining bot use[d] a image of Taylor Swift to hide malware [in its] payload" [9] this is similar to this. Instead of a Taylor Swift image it uses a webhp file.

4. Client device accessed sites with port 80

Port 80 is the assigned HTTP port, accessing sites using port 80 means that there is no **SSL** when accessing the site. The http is used for unencrypted communication, this means that transferred data can be intercepted and be read in plain text. A problem with this attackers can read essential and high priority information like username/passwords. DellXL used port 80 to access IP 216.146.38.70 a total of 10 times, IP 173.194.68.99 a total of 139 times, and accessed IP 173.194.68.104 a total of 68 times.

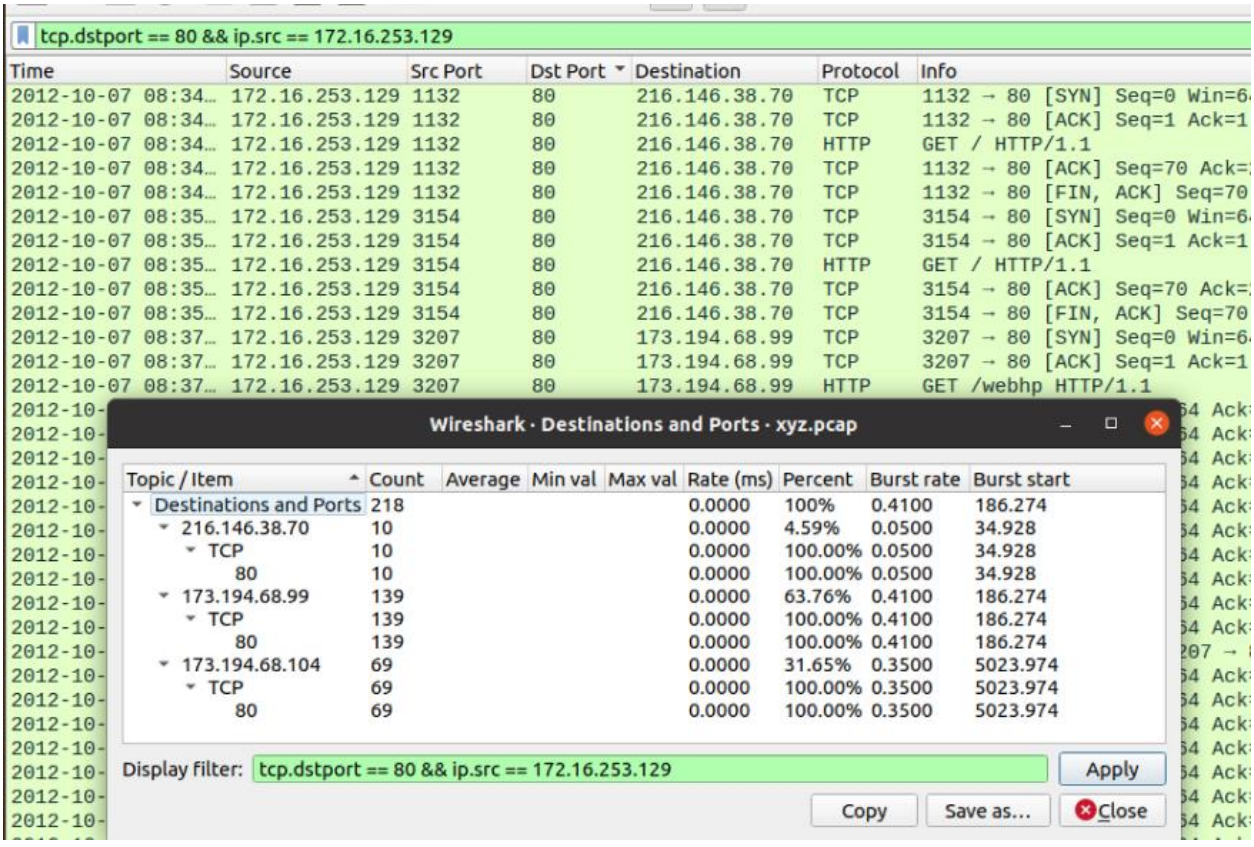


Figure 6: 172.16.253.129 (DellXL) accessing sites via port 80 based on the destination IP

Recommendations for prevention of this malicious traffic

Based on the packet analysis and risk assessment I think there are multiple things one can do to improve the security of the network. For the risks previously stated, I believe that this would be the best course of action.

1. Upgrade OS, and if necessary machine

   In response to a client machine running an older OS. I would like to recommend an upgrade to a better, more modern system that is still being supported. Windows 10 or Linux are both great OS's that would improve the business. They also have services and features that have been upgraded and no longer contain outdated drivers/services. If money is a concern, that the Linux OS what is open source is an excellent choice. If the client lacks the capital to upgrade the hardware itself, than I recommend thrifting and buying second-hand components or fully built computers.

2. Close open ports

   An easy way to make sure that no foreign attackers can access your ports is to close them. There are a few ways to go about this:

   - Windows OS: one could use the built-in windows firewall console (Windows Defender Firewall). The fire wall rules can be edited to make sure that no one can access port 1132-3389 or 1132-65535, likewise they can be edited to allow a port through when/if necessary.
   - Linux OS: one could use the **ufw** or **firewalld** to deny or block ports 1132-3389 or 1132-3389. Likewise, they can also be opened to allow a port through when necessary.

3. Install a Malware Detection

   Malware and virus detection software needs to be able to detect the incident in question, to ensure that there is a higher chance of it being caught I would install 2 or more software. Kapersky, is a good tracker for inter security, Malwarebytes is a popular choice as well. An **Intrustion Detection System (IDS)** can be implemented onto the current server. For example installing **pfsense** and downloading the **pfblocker** extension to download an **IP block list** that blocks access to certain IPs. Pfblocker can be used to download multiple **feeds** to provide additional protection against foreign IPs.

The client can install pfsense onto the existing security framework, and then pfsense can log all potential bad traffic.

4. Deny access to port 80

There are a few ways to deny access to port 80.

Table 2: Table of options to deny access to port 80

Client Side	Server Side
Use iptables/ufw/firewalld to block access to port 80	Change the **server.xml** file for **tomcat**
Use windows Defender firewall to add a rule to block remote port 80 (block access to port 80)	Use **active directory** to add a security access rule to block access to port 80

Table 3: List of all Assets, the devices listed are based on the wireshark endpoint statistics, filters and the resolved addresses statistics.

Asset List						
Time when Table was Recorded	IP Address	Machine Name (Host Name)	Device Operating System (OS)	MAC Address	MAC Vendor	Server
2021-07-27 10:09 PM MST	172.16.253.129	DellXT	Windows XP	VMware_7b:a8:da (00:0c:29:7b:a8:da)	VMware, Inc.	
2021-07-27 11:05PM	173.194.68.99			VMware_f2:7a:09 (00:50:56:f2:7a:09)	VMware, Inc.	Gws
2021-07-27 11:07PM	173.194.68.104			VMware_f2:7a:09 (00:50:56:f2:7a:09)	VMware, Inc.	Gws
2021-07-27 11:15PM	188.173.32.149			VMware_f2:7a:09 (00:50:56:f2:7a:09)	VMware, Inc.	
2021-07-27 11:25PM	216.146.38.70			VMware_f2:7a:09 (00:50:56:f2:7a:09)	VMware, Inc.	

References

[1] A. Holmes, "533 million Facebook users' phone numbers and personal data have been leaked online," Business Insider, 3 April 2021. [Online]. Available: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4. [Accessed 27 July 2021].

[2] J. Davis, "Data of 3.3M 20/20 Hearing Care Patients Hacked From Cloud Database," Health IT Security, 3 June 2021. [Online]. Available: https://healthitsecurity.com/news/data-of-3.3m-20-20-hearing-care-patients-hacked-from-cloud-database. [Accessed 27 July 2021].

[3] D. Shepardson, "VW says data breach at vendor impacted 3.3 million people in North America," CTV News, 11 June 2021. [Online]. Available: https://www.ctvnews.ca/autos/vw-says-data-breach-at-vendor-impacted-3-3-million-people-in-north-america-1.5466903. [Accessed 27 July 2021].

[4] C. Freeze, "RCMP investigating after soldiers' personal data leaked in cyberattack at RMC," The Globe and Mail, 19 August 2020. [Online]. Available: https://www.theglobeandmail.com/canada/article-rcmp-investigating-after-soldiers-personal-data-leaked-in-cyberattack/. [Accessed 27 July 2021].

[5] R. Sovers, "What Is Cryptojacking? Prevention and Detection Tips," Varonis, 29 January 2021. [Online]. Available: https://www.varonis.com/blog/cryptojacking/. [Accessed 27 July 2021].

[6] Kapersky, "What is a Botnet?," Kapersky, [Online]. Available: https://www.kaspersky.com/resource-center/threats/botnet-attacks. [Accessed 28 July 2021].

[7] K. Ashford and J. Shmidt, "What Is Cryptocurrency?," Forbes, 18 December 2020. [Online]. Available: https://www.forbes.com/advisor/investing/what-is-cryptocurrency/. [Accessed 28 July 2021].

[8] L. Cinway, "Blockchain Explained," Investopedia, 1 June 2021. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. [Accessed 28 July 2021].

[9] Wikipedia, "JSON_RPC," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/JSON-RPC. [Accessed 30 July 2021].

[10] bitcoin, "Some Bitcoin words you might hear," bitcoin, [Online]. Available: https://bitcoin.org/en/vocabulary#:~:text=The%20hash%20rate%20is%20the,10%20trillion%20calculations%20per%20second.. [Accessed 30 July 2021].

[11] bitcoin, "Getwork," Bitcoin Wiki, 1 April 2015. [Online]. Available: https://en.bitcoin.it/wiki/Getwork. [Accessed 27 July 2021].

[12] Microsoft, "Windows XP support has ended," Microsoft, 2021. [Online]. Available: https://support.microsoft.com/en-us/windows/windows-xp-support-has-ended-47b944b8-f4d3-82f2-9acc-21c79ee6ef5e. [Accessed 27 July 2021].

[13] iana, "Service Name and Transport Protocol Port Number Registry," Internet Assigned Numbers Authority, 27 July 2021. [Online]. Available: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt. [Accessed 27 July 2021].

[14] C. Cimpanu, "Cryptocurrency-mining botnet uses a Taylor Swift image to hide malware payloads," ZDNet, 19 December 2019. [Online]. Available: https://www.zdnet.com/article/cryptocurrency-mining-botnet-uses-a-taylor-swift-image-to-hide-malware-payloads/. [Accessed 27 July 2021].