MICROSOFT WINDOWS DEFENDER AND FIREWALL

Introduction

In today’s interconnected world, the security of our digital assets is paramount. With the ever-increasing prevalence of cyber threats, safeguarding our systems against malicious attacks has become concern. To address this challenge, the implementation of robust security measures is essential. The “Windows defender and firewall” project aims to explore, analyse and optimize the built-in security features offered by Microsoft’s Windows operating system.

Windows Defender, the default antivirus and antimalware software integrated into windows, servers as the first line of defence against a wide range of threats, including viruses, spyware and other malicious software. Concurrently, the Windows Firewall acts as a protective barrier, monitoring and controlling inbound and outbound network traffic to prevent unauthorized access to our systems.

This project delves into functionality, configuration, and performance of Windows Defender and Firewall, aiming to enhance their effectiveness in safeguarding user systems and data. By conducting comprehensive evaluations, implementing best practices, and potentially customizing configurations, this project seeks to fortify the security posture of Windows based environments, mitigating the risks posed by cyber threats and enhancing user confidence in their digital security.

Throughout the project lifecycle, we will explore various aspects of Windows Defender and Firewall, including their features, settings, performance impact, and integration with other security tools. Additionally, we will examine strategies of proactive threat detection, incident response, and continuous improvement to ensure the resilience and adaptability of our security infrastructure.

Features and Functionality:

Windows Defender and Windows Firewall are integral components of the Microsoft Windows operating system, designed to provide security against various threats and unauthorized access. Here are the key features and functionalities of each:

Windows Defender:

1. Real-time Protection: Windows Defender offers real-time protection against malware, viruses, spyware, and other malicious software. It continuously monitors system activities and files to detect and block threats as they occur.

2. Cloud-based Protection: Windows Defender leverages cloud-based protection to enhance threat detection and response. It utilizes Microsoft's cloud infrastructure to analyse suspicious files and behaviours, providing additional layers of defence against emerging threats.

3. Automatic Updates: Windows Defender automatically updates its malware definitions and engine to ensure that it can detect and mitigate the latest threats. This feature helps keep the system protected against newly discovered vulnerabilities and malware variants.

4. Scheduled Scans: Users can schedule periodic scans with Windows Defender to check for malware and other potentially unwanted software. Scheduled scans can be customized to run at specific times and frequencies, helping maintain the security of the system without manual intervention.

5. Quarantine and Remediation: When Windows Defender detects a threat, it quarantines the malicious file or software, preventing it from causing harm to the system. Users can then review and take action on quarantined items, such as removing or restoring them.

6. Browser Protection: Windows Defender includes browser protection features that help block malicious websites and phishing attempts. It integrates with web browsers to provide real-time protection while browsing the internet, reducing the risk of malware infection and online scams.

7. Security Dashboard: Windows Defender provides a centralized security dashboard where users can view the security status of their devices, access scan results, and manage security settings. The dashboard offers insights into recent activities, detected threats, and recommended actions to improve security.

Windows Firewall:

1. Inbound and Outbound Traffic Filtering: Windows Firewall monitors both inbound and outbound network traffic, controlling access to and from the system based on predefined rules. It allows users to specify which applications and services are allowed to communicate over the network, enhancing security by preventing unauthorized access.

2. Rule-based Configuration: Users can create custom firewall rules to define how incoming and outgoing traffic should be handled. Firewall rules can be based on various criteria, such as port numbers, protocols, IP addresses, and applications, giving users granular control over network access.

3. Network Profile Management: Windows Firewall supports different network profiles, including public, private, and domain networks. Users can configure firewall rules and settings separately for each network profile, allowing for tailored security configurations based on the network environment.

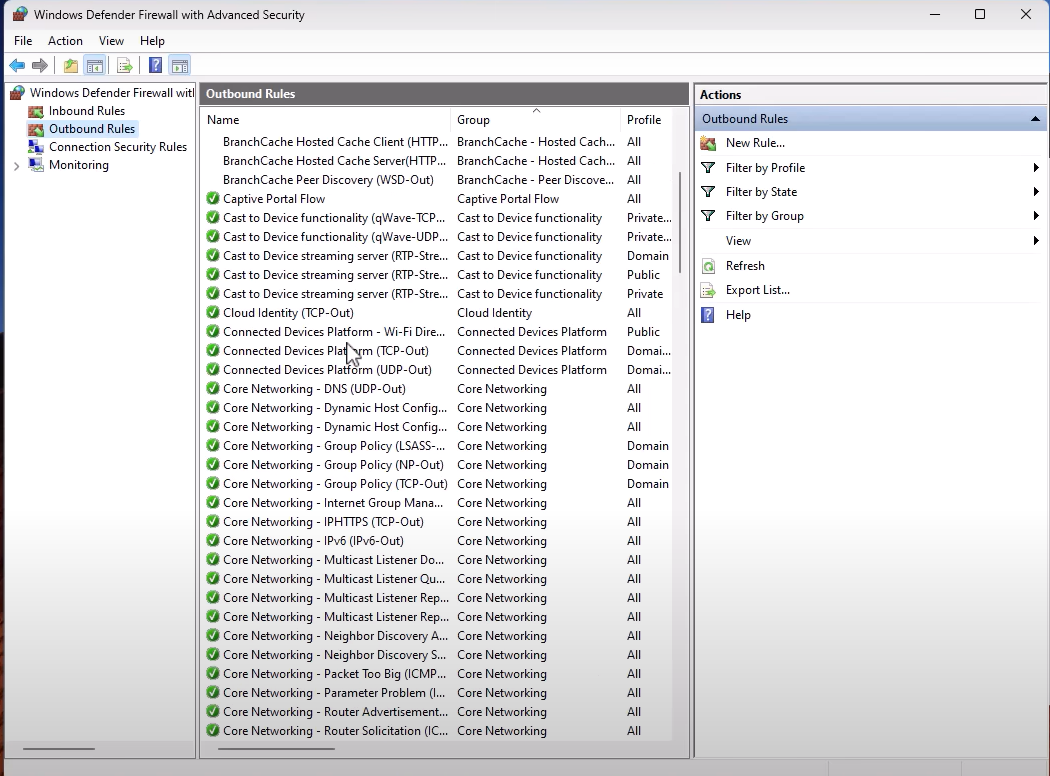
4. Stealth Mode: Windows Firewall includes a stealth mode feature that helps make the system less visible to unauthorized network scans and probes. In stealth mode, the firewall silently drops incoming network traffic that doesn't match any allowed rules, making it harder for attackers to identify and target the system.

5. Logging and Monitoring: Windows Firewall logs network activity and security events, providing visibility into incoming and outgoing connections. Users can review firewall logs to track network traffic, identify potential security incidents, and troubleshoot connectivity issues.

6. Advanced Security Features: Windows Firewall includes advanced security features such as connection security rules, which enable encryption and authentication for network traffic, and Windows Defender Firewall with Advanced Security, which offers additional configuration options and management capabilities.

**Implementing Robust Protection with Windows Defender and Firewall:**

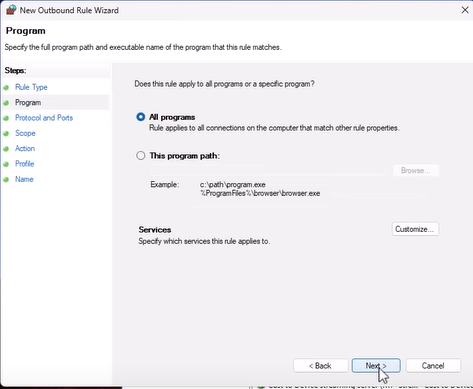
First of all, we may not realize windows firewall has a lot of rules and what it’s doing is it’s filtering some of the traffic coming in and out of our system, which is why an application connects to the internet in a non-standard way it typically has to create an exception within Windows Firewall to allow that type of connection. However, these rules are quite generic and they don’t really do any kind of blacklisting. So, if there is a random malware IP the Windows Firewall is most likely not going to block that. However, there is a way to extend that functionality into Windows Firewall, we can actually use it to block a host of the most dangerous Botnets out there.

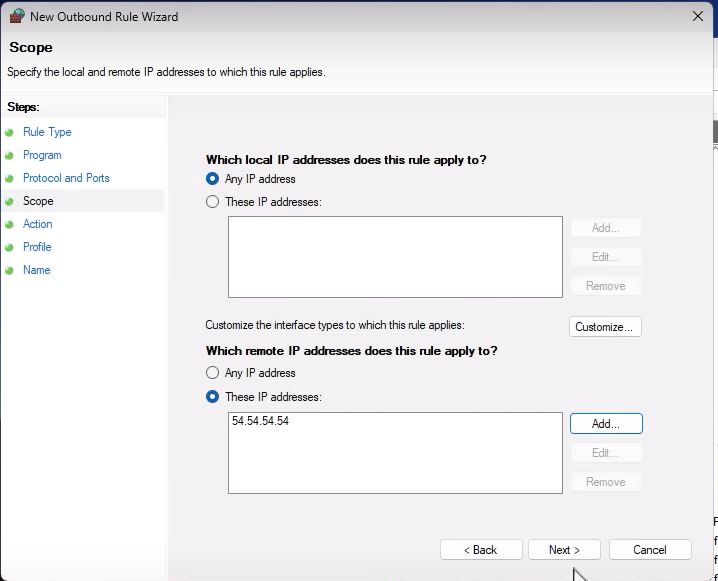


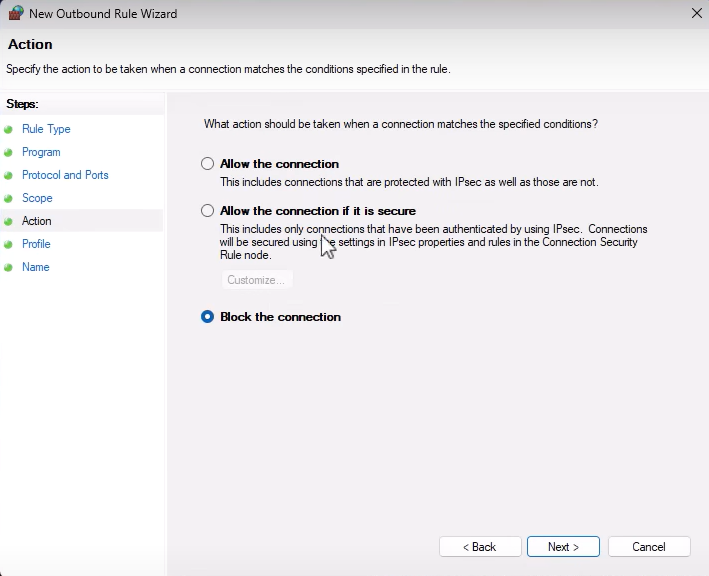
In order to do this we are going Windows Firewall’s ability to create rules.

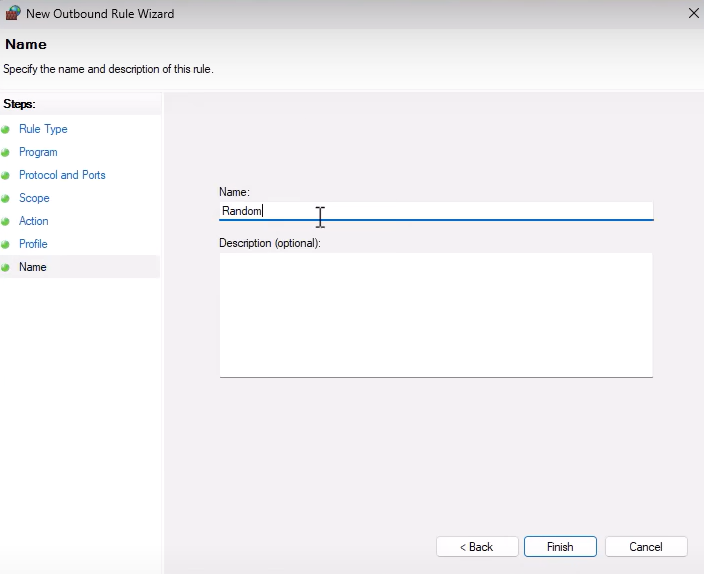


With using a GUI it is pretty straight forward, we can select any type of rules. So, for example if we want to filter any specific program, we select “Program”. If we want to block a port we select “Port”, “Predefined” or “custom”. We are gonna go custom and essentially what we want to do is for all programs blacklist a specific remote IP address.



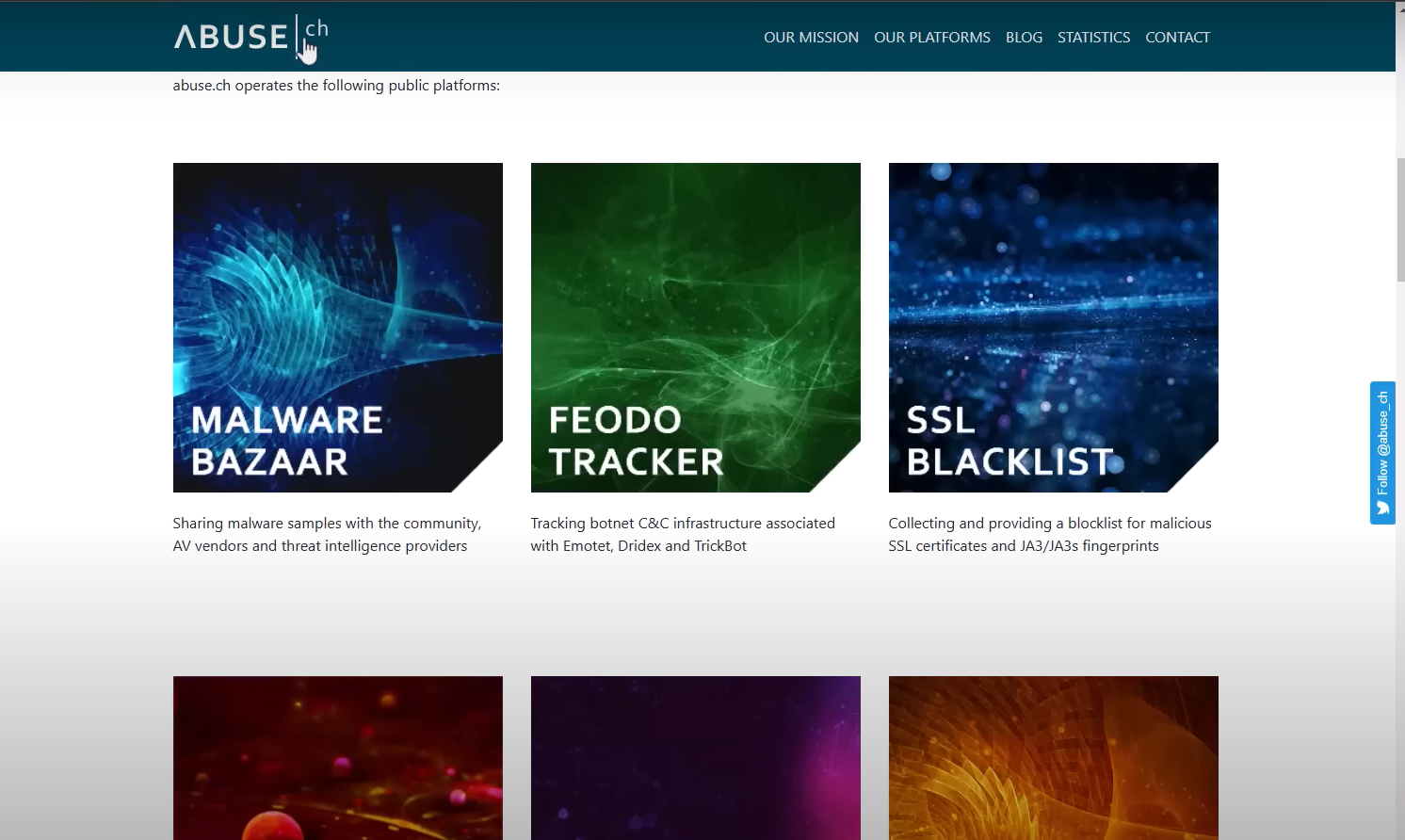


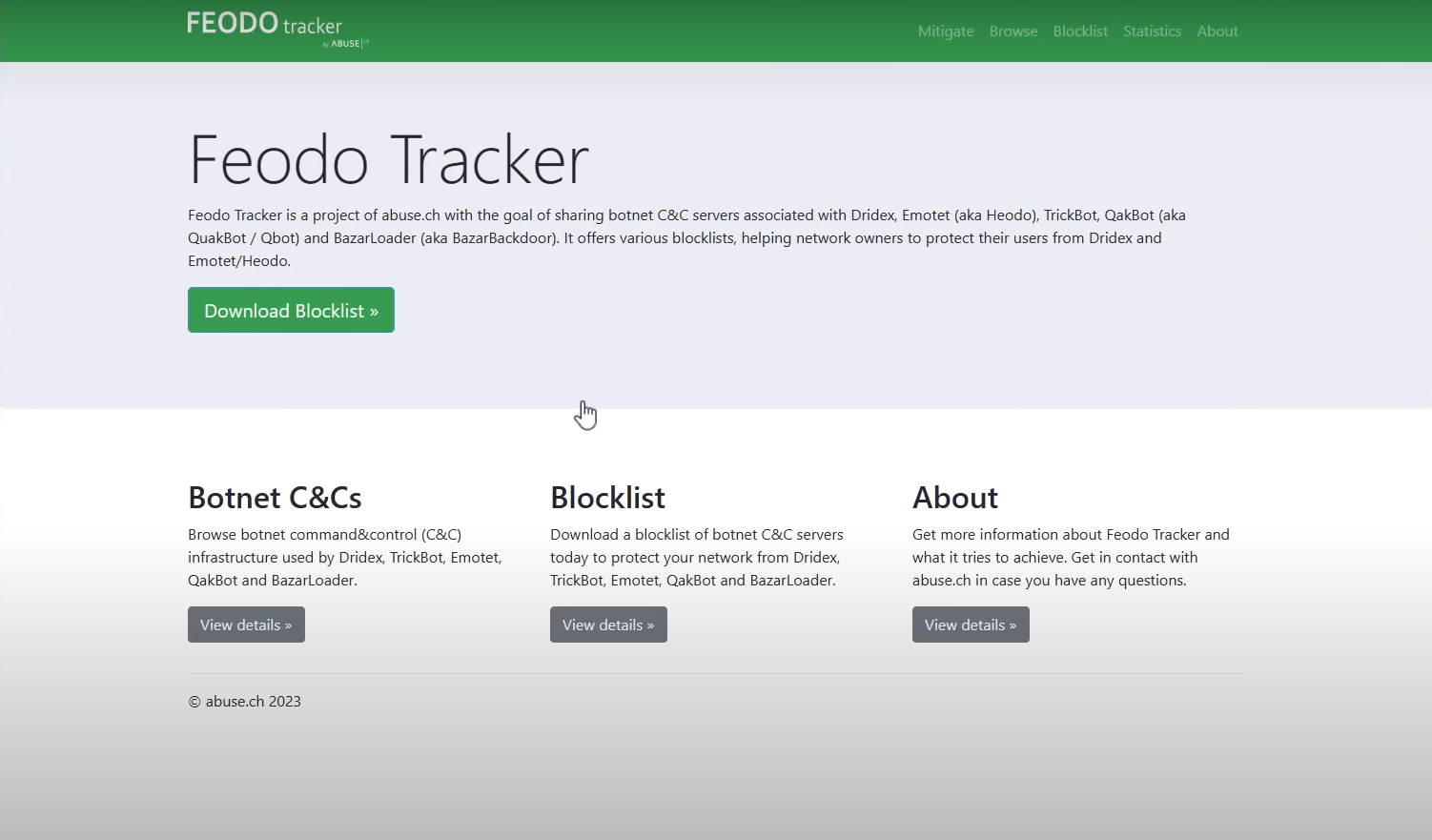




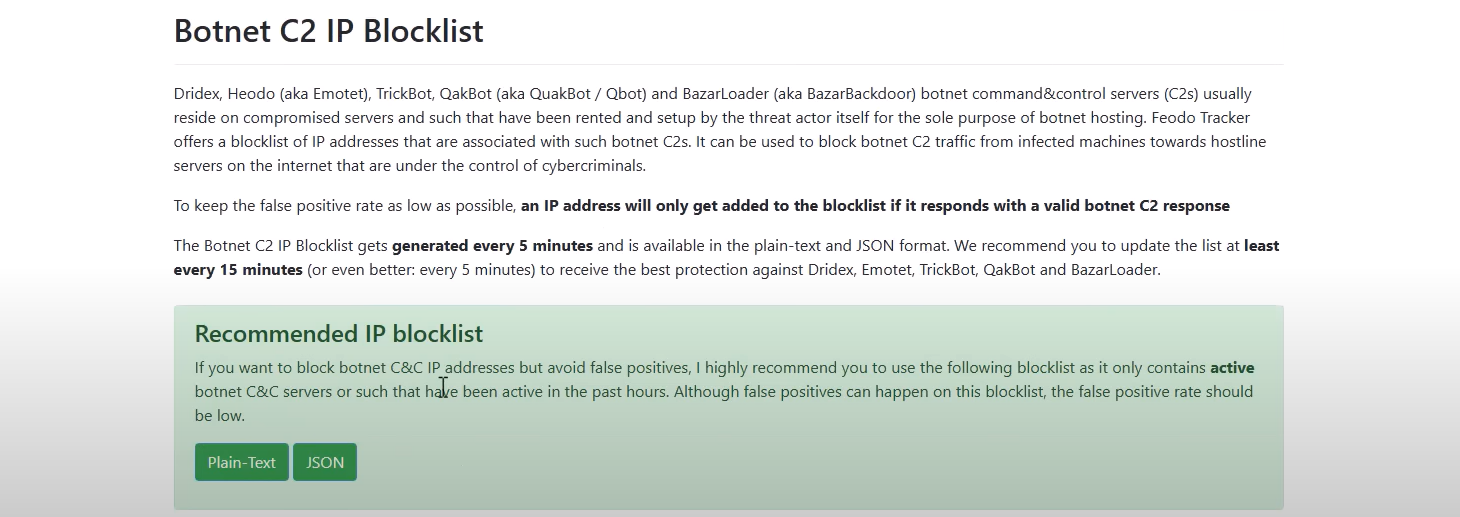
But that’s just one IP it’s not very useful. What we want to do is have a list of the most malicious IPs and update that list every day and that’s exactly what we are doing.

So, to start off how we are going to get the list of malicious IPs , for starters we could go to “abuse.ch” and check out their botnet tracker and this is going to give us a list of bad servers they are hosting command and control infrastructure for attackers trickbots emotat whatever and we can actually access this for free.

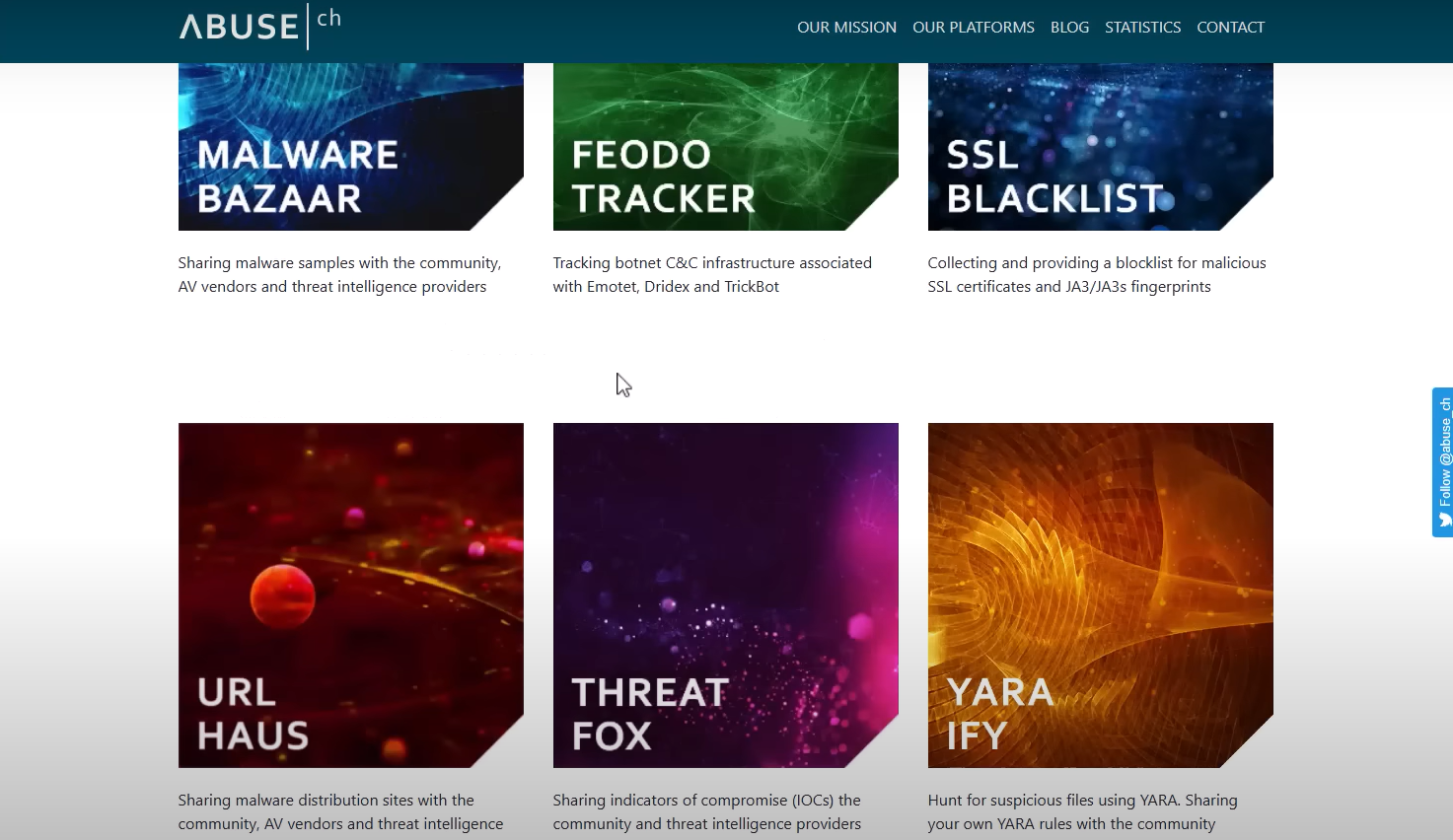


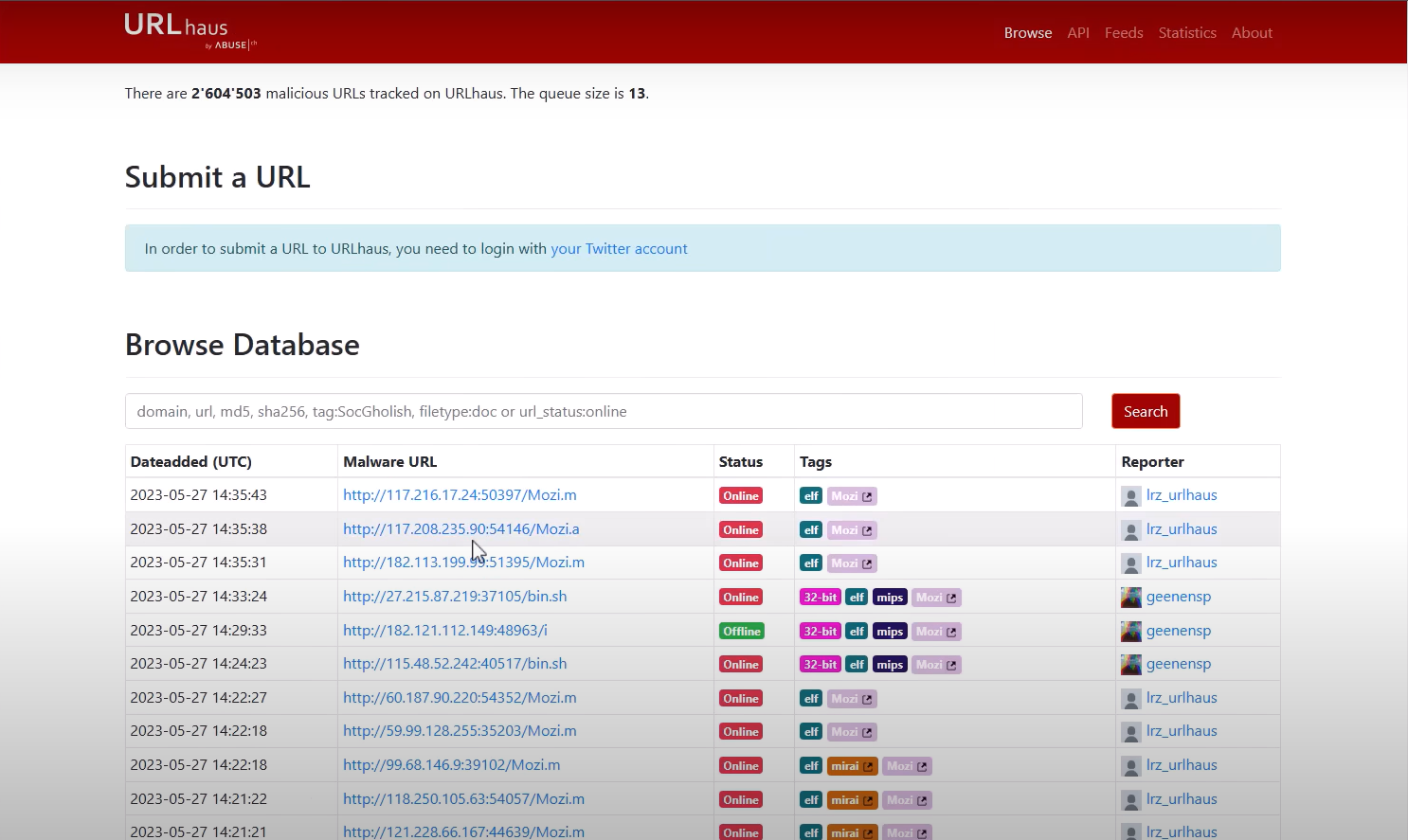


* And as we can see the Botnet C2 IP Blocklists get generated every 5minutes and is available in Plain-Text and JSON.

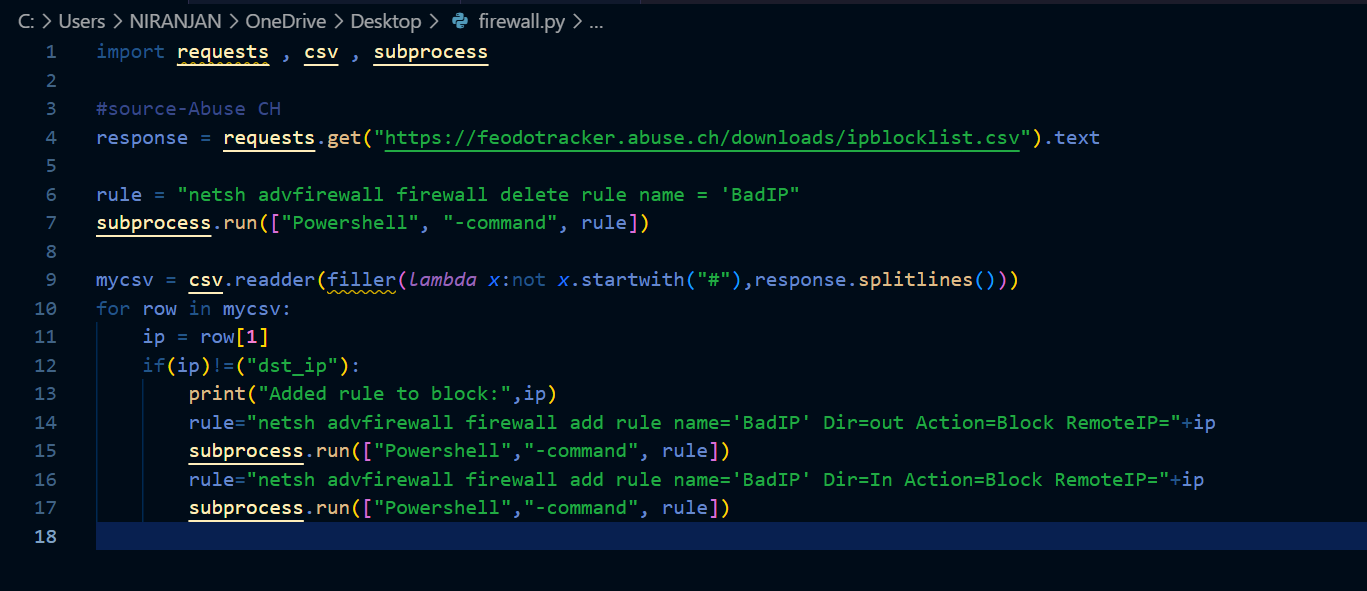


* We could also use to blocklist outgoing connections to malware domain. If we go to “URLhaus” for example we can see the list of Malware URLs and again we could totally Blocklists this IP. So, that our computer would not be able to connect to them and download the Malware.

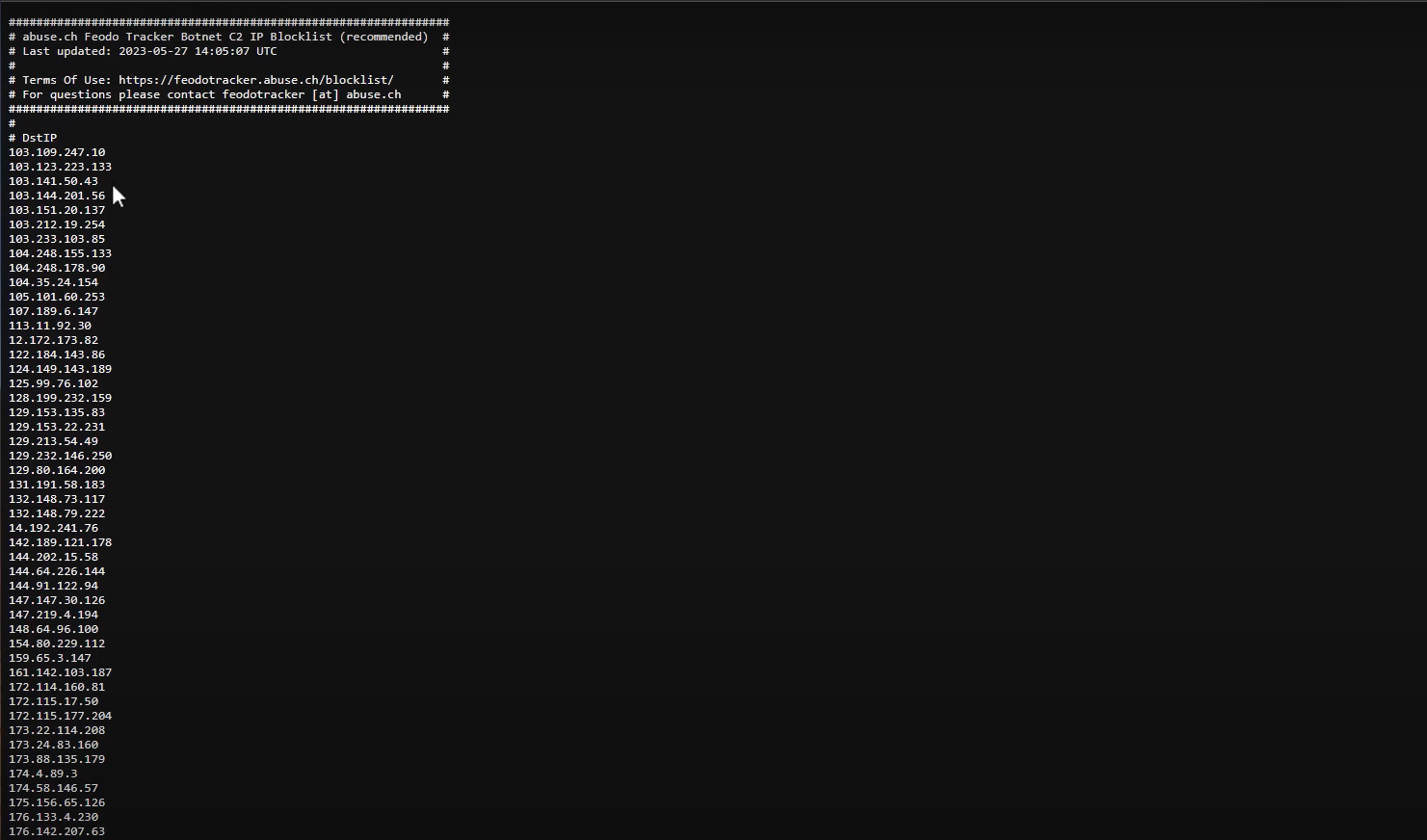




And the question is How are we going to automate that and get the list up-to-date everyday and actually it’s not that hard, as we can see, I have written a script for that.

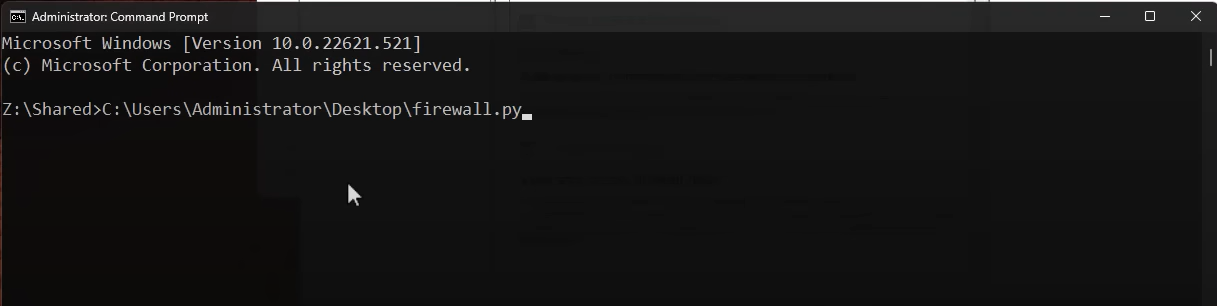


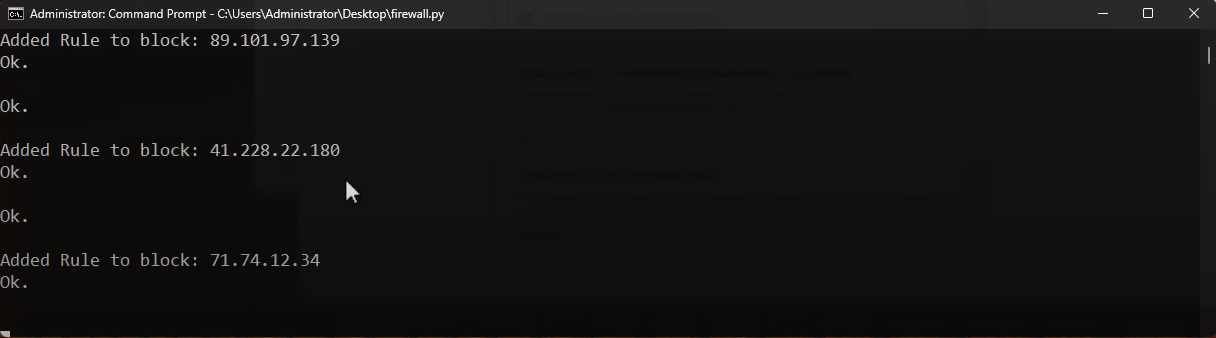
* So first we are going to import “requests”, “CSV”, “subprocess” these are just some libraries that we’re going to use to make our job easier.
* Then we are basically going to download the CSV file containing all of the IP addresses and just so it’s not intimidating, I’m going to show you what that actually looks like manually. So, we take a look at the plain-text this is what it looks like. So, we have got destination IP and then IP addresses.



* We are going this file in a CSV format convert it to text and then just automate typing in the command to add this to Windows Firewall.
* First of all though I’m deleting every rule that already exist with the name of “BadIP”, because what we are going to do is we are going to use this name to create rules to Block Malicious IPs and I wanted to set it up so that everyday it’s going to delete everything and then get the new list of IPs and that’s important because malware IPs don’t always stay the same sometimes an IP any be malicious because the attacker is controlling legitimate infrastructure so it has to be dynamic. So, first we are going to delete everything so that every time the script runs, we have new set of rules and the old rules don’t just there.
* We are going to use CSV reader, a Lambda filter-what this going to do is basically just filter out lines that do not start with hash because that is a comment line and if we go back to our actual, we can see that there of a heading that has the whole hash structure in it, So, we don’t want these lines to be included in our rules.
* And then for each row within that list we’re going to assign the variable IP to row one that’s because of the format of the CSV and there is an additional check over here, because sometimes we don’t have a hash before the column name if the text not destination IP which would be the heading of the column, we’re going to grab that IP.
* And then it is just going to print what IP it is going to block; it’s going to run a command and this command is basically going to add a rule call it BadIP the direction is outbound in this case. Obviously, we want to add inbound as well if we are trying to block botnets from connecting to us and prevent things like DDOS attack this just an example, the action is block and remote IP equals and then we’re just passing the variable here.
* Then subprocess start run, this going to run the thing and powershell.

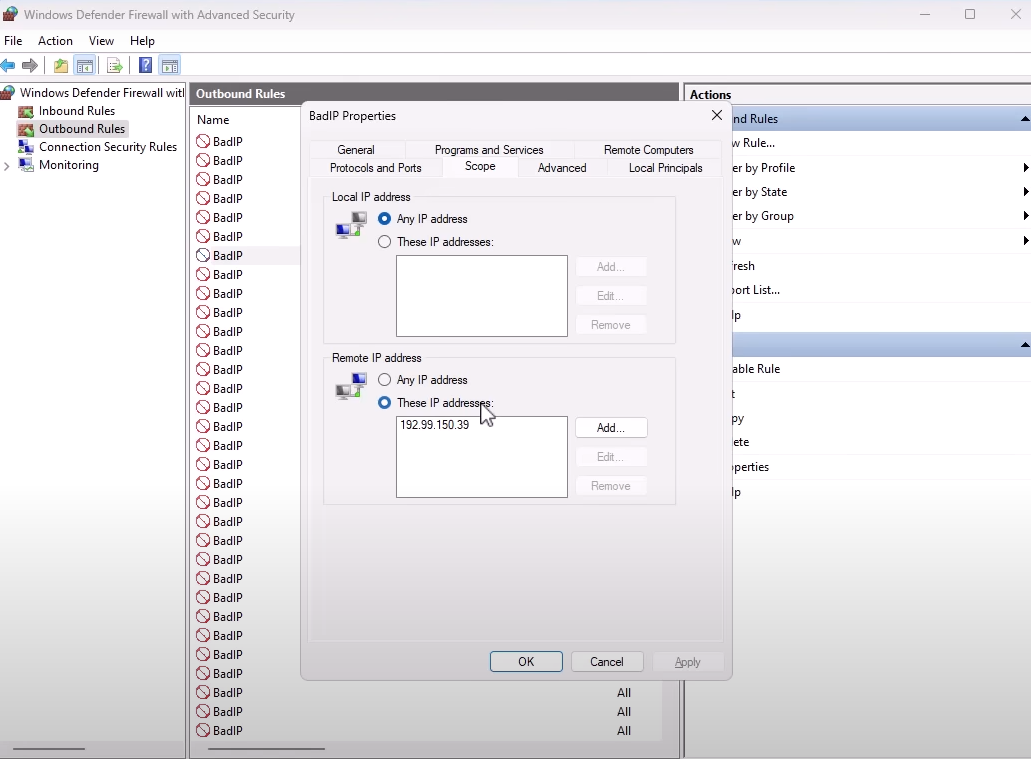
Now let’s see it in action. So, I’m going to open up regular command prompt, remember you have to do this as an administrator, just going to drag my script in we’re going to run it





* And this going to add rules for each of this IPs as we can see.
* And once the script completes, all of those rules going to be in here.
* 

So, as we see for outbound we have lot of BadIPs already and if we open we are going to see that the scope says that these IP addresses which we got from blocklist derived from abuse reports open source and now we are actively blocking it in our system.



We can of course use similar kind of workflow on any kind of firewall software.

**Conclusion:**

In conclusion, the "Windows Defender and Firewall" project has provided a comprehensive exploration of the built-in security features offered by Microsoft's Windows operating system. Throughout this project, we have delved into the functionality, configuration, and effectiveness of Windows Defender and Firewall in safeguarding systems against a wide range of cyber threats.

Windows Defender, with its real-time protection, cloud-based security intelligence, and automatic updates, serves as a robust defence mechanism against malware, viruses, and other malicious software. Its integration with the Windows operating system and seamless user experience makes it a valuable asset in maintaining the security posture of Windows-based environments.

Similarly, Windows Firewall plays a crucial role in controlling network traffic and preventing unauthorized access to systems. With its rule-based configuration, network profile management, and advanced security features, Windows Firewall empowers users to customize security settings according to their specific requirements and network environments.

Throughout the project, we have explored various aspects of Windows Defender and Firewall, including their features, settings, performance impact, and integration with other security tools. By implementing best practices, optimizing configurations, and staying vigilant against emerging threats, users can enhance the security of their Windows systems and mitigate the risks posed by cyber-attacks.

As technology continues to evolve and cyber threats become increasingly sophisticated, maintaining robust security measures remains essential. Windows Defender and Firewall serve as foundational components in this endeavour, providing users with the tools and capabilities needed to defend against evolving threats and protect their digital assets.

In conclusion, by leveraging the capabilities of Windows Defender and Firewall and adopting a proactive approach to cybersecurity, users can strengthen the security posture of their Windows-based systems, ensuring a safer and more secure computing environment in today's interconnected world.