# **Determine Bad Actors**

Ryan Briggs

University of Maryland Global College

CYB 670 – Capstone in Cybersecurity

Professor Yurek Hinz

October 7, 2021

## Determine the bad actors

There are many ways to determine bad actors and just as many ways to hide as bad actors. For example, a basic bad actor may be coming from their current country with no obfuscation. Whereas a more advanced bad actor may obfuscate their location by using another countries Internet Protocol (IP) address as redirection, this is known as IP obfuscation. “IP obfuscation -- also known as geo-spoofing, masking or anonymization -- refers to the process of concealing a user’s geographic location. Keeping one’s whereabouts and identity concealed, especially when connecting from untrusted locations, can be challenging” (Smith, 2018). Knowing this is important because the list of IPs listed in table 1, may not be the actual location of the malicious activity. Shown in table 1, is a list of IP addresses and their respective Whois location information, which was provided for possible defense and remediation actions. Shown below in figure 1, is the list of local IP addresses and the remote IPs they are connecting out too, as well as the process, process path, and the username.

The first criteria for attribution would be the location of the remote IP addresses. As shown in table 1, all IP addresses going to a remote IP that is not a part of the Five Eyes Alliance (FVEY), should be remediated. Unless there is a specific requirement for those IP addresses to have access, they should be blocked from the Summit’s network. This then leaves 8 IP addresses, 7 United States and 1 New Zeeland, to be further investigated. One of the United States IP addresses will need to be investigated a bit more thoroughly because it had a location mismatch. The next criteria however should then be investigating is the owners of each of the IP addresses. For example, the first United States IP address, 7.26.42.136, has a whois owing organization of the Department of Defense (DoD). This probably is a legitimate IP address for the Summit’s network to be talking out too.

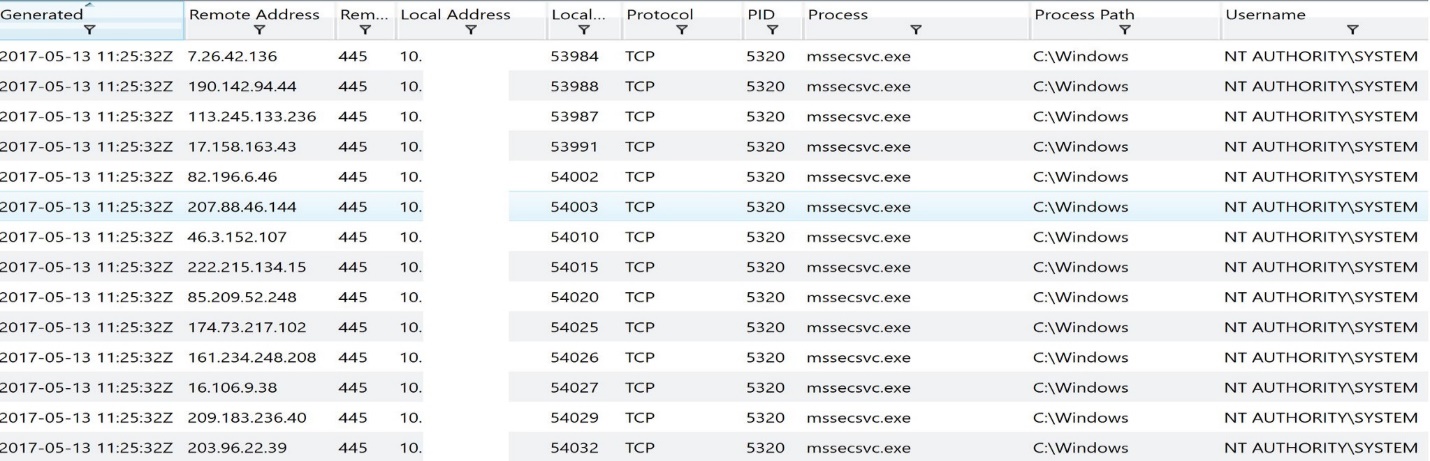
However, after investigating all of these IP addresses, another issue with Summit’s network maybe needs to be addressed. This issue involves all of these local addresses attempting to access Transmission Control Protocol (TCP) port 445 from across the Internet. According to thewindowsclub.com, TCP:

Port 445 is ‘SMB over IP’. SMB stands for ‘Server Message Blocks’. Server Message Block in modern language is also known as Common Internet File System. The system operates as an application-layer network protocol primarily used for offering shared access to files, printers, serial ports, and other sorts of communications between nodes on a network. (thewindowsclub.com, 2020)

This protocol allows networked computer to access resources that other systems have shared. This is typically done within a network and not across the internet. This is extremely odd behavior from these local addresses to attempt to access SMB resources from across the Internet. Microsoft states that “It is unlikely that any SMB communication originating from the internet or destined for the internet is legitimate” (Microsoft.com, n.d.). The other portion of this issue is the local system’s process name, the process location, and the user running these connections, as shown below in figure 1.

**Figure 1**

*Provided List of IPs*



When researching this process and it’s running location, it was found that this could possibly be the WannaCry Ransomware. From spyware.com,

Mssecsvc.exe is an executable that is running in the background and can be seen in the Task Manager during the operation of the PC. The process can be found in Windows XP, 7, 8, and 10 and is usually located in C: \Windows. (Hall, 2019)

This could be extremely worrying because the “Mssecsvc.exe virus was proliferated with the help of the EternalBlue exploit” (Hall, 2019). This “exploit that allows cyber threat actors to remotely execute arbitrary code and gain access to a network by sending specially crafted packets. It exploits a software vulnerability in Microsoft’s Windows operating systems (OS) Server Message Block (SMB) version 1 (SMBv1) protocol” (cisecurity.org, 2019). Since this virus uses a similar process name and location, and an SMB exploit as well as these connections are using TCP port 445, which is typically associated with SMB, these local systems should be quarantined immediately. Once they have been quarantined, remediation should begin to determine why these systems were trying to reach remote IP addresses using TCP port 445 and if these systems are infected with the WannaCry virus. Additional remediation should be conducted against

**Table 1**

*Table showing IP registration locations*



## References

cisecurity.org. (2019, January). Eternalblue Security Primer. Retrieved October 9, 2021, from <https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf>

Hall, G. E. (2019, June 13). MSSECSVC.EXE is a part of notorious wannacry - delete it immediately. Security and spyware news. Retrieved October 9, 2021, from <https://www.2-spyware.com/file-mssecsvc-exe.html>

Microsoft.com. (n.d.). Preventing SMB traffic from lateral connections and entering or leaving the network. Microsoft Support. Retrieved October 9, 2021, from <https://support.microsoft.com/en-us/topic/preventing-smb-traffic-from-lateral-connections-and-entering-or-leaving-the-network-c0541db7-2244-0dce-18fd-14a3ddeb282a>

Smith, G. (2018, December 14). The benefits and practicalities of IP obfuscation. Attila. Retrieved October 9, 2021, from <https://www.attilasec.com/blog/geo-spoof-your-location>

thewindowsclub.com. (2020, January 10). What is an SMB port? what is Port 445 and Port 139 used for? The Windows Club. Retrieved October 9, 2021, from <https://www.thewindowsclub.com/smb-port-what-is-port-445-port-139-used-for>