**ITSC 305 group assignment**

Here is a log of my individual contributions:

March 28 – April 1: research for the assignment

April 2: set up of streamyard account to perform the broadcast.

I listed my general script I prepared for the recording on the next page, note that I did not necessarily follow it exactly as it is a rough draft and we wanted to keep the podcast more conversational.

YouTube link for recording: <https://www.youtube.com/watch?v=HDc-SNMnLgk>

**Research/script:**

IoT security refers to the methods of protection used to secure internet-connected or network-based devices. The term IoT is incredibly broad, and the term has only become broader. From watches to thermostats to everything in-between, nearly every technological device can interact with the internet, or other devices, in some capacity.

Now with these systems becoming more widespread, so too does the existence of malicious software, or malware, that will attempt to exploit these devices. In the last few years malware attacks on IoT devices has increased tremendously. It is reported that there were 1.5 billion IoT breaches in 2021, which is a drastic increase from 639 million in 2020.

IoT malware is used to perform a variety of attacks, such as DDoS attacks, port scanning for possible entry and brute force attacks also to gain entry. These are the most common reported malware attacks. Some examples of IoT malware families are: Bashlite, Mirai, and Linux.Darlloz. These examples are used to create botnets, which Raymond goes more in depth about.

* Bashlite targets linux-based systems to preform a DDoS attack by exploiting a flaw in the bash shell. It is estimated that over 1 million devices have been infected, creating a powerful botnet.
* Mirai targets IoT devices to create a botnet by scanning for IP addresses and attempting to brute force its way in by using common default usernames and passwords.
* Linux.Darlloz is a worm which targets linux embedded systems exploiting a PHP vulnerability.

This malware relies on vulnerabilities which for the most part can be fixed. For one, ensure that in your devices you do not use default usernames and passwords, and use standard password security, also use two factor authentication where possible. Second, ensure that when designing IoT systems that data encryption is a high priority. Third, make sure to close any unused ports and limit internet connectivity wherever possible.

However, these steps are not 100% foolproof, because as time goes on the malicious programmers create malware that becomes more sophisticated and new vulnerabilities are discovered that we did not consider before. That is why malware analysis is important in preventing future attacks.

Both developing malware and performing malware detection and dynamic analysis is incredibly difficult due to the wide range of differences there are between IoT systems and their architecture. Dynamic analysis consists of monitoring the executable functions while running and attempting to detect abnormal behavior. Besides regular issues that are faced when performing dynamic analysis, there are specific limitations that are present when analysing possible infected IoT and embedded systems. Such as:

* It is difficult to properly sandbox an infected embedded system as it can often require the whole network to be able to properly function, which would allow the malware to spread.
* Diverse architectures present in these systems mean that malware can behave differently, or not at all, on different systems.
* Resource constraints within these systems mean that it is very difficult to run the required software to debug and analyze the malware.

To get around the restrictions mentioned, it would require configuring a system that is vastly different then the actual system used, which many modern malware is adept at detecting and so will attempt to hide and not perform their malicious functions, making it next to impossible to perform the analysis.

In contrast, static analysis is used to analyze malware without it running. Using this method, we can explore all paths of execution that are possible in a malware sample without necessarily having to consider the differences in the systems architecture. Static analysis can provide features such as Op codes, strings, and the file structure to help determine if a binary file is malicious or not.

However, this basic method of analysis is still limited in its functionality, leading to advances in new methods of malware analysis, most of which are far to advanced for me to comprehend properly right now. (Such as graph-based analysis).

Anyways that concludes my talk on malware in IoT devices, over to you, (NEXT PERSON)