Date: 2/21/2021

To: CISO for the ITN 295 Gateways to Dark Web

From: Afeefah Manzoor

Subject: Data Connectors’ Ohio Virtual Cybersecurity Summit Writeup

The Data Connectors Ohio Virtual Cybersecurity Summit had three major topics that were breaking authentication, real-time asset visibility and security for everyday devices, endpoint management and security, and Mitre attack for assessing and mitigation. The overall topic of this summit was discussing different exploits and ways to mitigate them.

The broken authentication lecture briefly explained the different types of attacks that can be used, for example- credential stuffing, password spraying, injection attacks, session hijacking and session ID URL rewriting. The few ways users can prevent or deter these attacks are multifactor authentication, not shipping with default credentials, enforcing strong passwords and using a breached password detection.

The real-time assets visibility and security for everyday devices lecture, it explained the types of technologies that we have in two-way, traditional devices which are devices that people will first think of like laptops, servers, tablets, etcetera and newer devices which include Iot, IoMT, and OT which will make up about 50 billion devices in 2025. The reason these new devices pose a threat is that users may not know of legacy devices they may have been deployed, are difficult to scan and patch, have no security agents, and the sheer volume of these newer devices. The reason we must worry about these newer devices are because users have already been affected by the Miria botnets, the hacking of ST Jude Cardiac devices, Ripple20 vulnerabilities, and Solarwind vulnerabilities. Possible mitigation techniques include passive discovery being used verses active scanning, real-time and granular device content, knowing exactly how devices behave, network segmentation, a flexible segmentation approach, and connected device security requiring collaboration.

The endpoint management and security lecture discussed the effect from COVID-19 and consequences from working from home. Many devices in the offices have not been used for months causing these devices to be behind in updates creating vulnerabilities in their systems. Since COVID-19 has started, cyberattacks and phishing has quadrupled. Now that many offices have started to open up, the devices in their offices need to be updated as soon as possible to prevent attacks on their systems that could have been prevent, patch up, update and encrypt other devices that will be used from home to mitigate any other risk.

In the lecture for Mitre attack for assessing and mitigation, it was discussed the benefit of looking for the tactics used by hacker instead of their techniques. By looking for known techniques the company or user will always be one step behind the attacker. When trying to mitigate these attacks it is best to try to shift this prioritization to improve risk reduction assessment. Some of these techniques include asset hardening, IT hygiene attack surface reduction, disabling functionality, and zero-trust technologies and policies which includes zero-trust execution.

In the Data Connectors’ Ohio Virtual Cybersecurity Summit, they went over mitigation techniques for broken authentication, fore everyday devices including newer technologies, working from home and returning to offices, and offensive mitigation techniques instead of defensive mitigation techniques.