Clarence V Kimbrell Jr
2/16/23

No One is Safe!

Tens of millions of people are in danger!

Medjacking

All corners of the internet are targets for hackers. The medical industry is a high-value target because subsequently, it contains highly classified information. This is because over the years information technology has been incorporated into the medical field more and more. Medical centers have some of the latest technology advancements added to them to help patients. Most of this comes at a cost connected to the internet and computer algorithms.

Equipment

Many of the equipment in medical centers are no longer just physical tools. They are connected to the local networks and have operating systems. Like many devices, they need periodic updates. If equipment is not updated periodically, it can become a big and easy target for hackers. Then when hackers have found a target, they can use the medical device or equipment as a staging ground to further cause disruption.

TrapX

TrapX is a cyber security company based out of Israel. They are leading the charge in deception technology and are found in countless reports across the globe. This includes ones in the medical field. TrapX can emulate real assets in computers with their deception technology decoys. These types of hacks are conducted to improve security. Their main goals in the medical device hijacking field are to show that medical records can be stolen, that devices in hospitals can be used as threat actors, and finally that there is a large demand for classified medical-related

information. Any of these can be devastating to a company or a medical center; this is why TrapX is trying to better educate everyone on the potential of these events.

Live Scenario

TrapX was the first to create a counterintelligence cyber deception operation. They were able to do this by creating a fake hospital network. Then hacking into it with some of their deception devices and techniques. In one of their operations, they planted malware inside VLANs of the medical device network and others. After some time passed the decoys were incorporated into the network. The first device that was compromised was an MRI device that was connected to a desktop. MRIs are used for things like radiology and require a lot of large computer-based machines. This began the main part of the attack because it became the staging ground to send off more malware to every other device connected to the network. After spreading the malware was able to find an administrative device that was using an older operating system. Then gained full access to nearly everything, and it used this device to send out more payloads of malware to the remaining equipment. It was noted that the malware stored itself in the resident memory. This is important because some devices could be restored but could pose a threat at a later date. Before the situation got too out of hand TrapX deployed some of their security team to stop the attack and to stop further damage.

Conclusion

TrapX's real-time simulation needs to be a foundation in many counterintelligence operations. Situations like what they conducted are happening around the globe daily. It is important to understand the step-by-step process of the attack to be able to mitigate the losses. TrapX is a leading company in cyber security and what it created needs to be practiced by everyone.

Clarence V Kimbrell Jr
2/16/23

Sources

Nair, Mano J. “Welcoming Trapx to the Commvault Family.” *Commvault*, 1 Feb. 2022, https://www.commvault.com/blogs/welcoming-trapx-to-the-commvault-family.

TrapX Research Labs, “MEDJACK.4 Medical Device Hijacking” *TrapX*, 2018, TrapX%20-%20Medical%20Device%20Hijacking%20(1).pdf