Paul Polsinelli

Jun 20, 2020

IFT 302 - Lab 5

Current Event 1

Title: Australia is All But Accusing China of a Months-Long Cyberattack on its Government Systems and Major Companies

Author: Kieran Corcoran

Publication Date: Jun 19, 2020

Link: <https://www.businessinsider.com/australia-all-but-accuses-china-cyberattack-government-companies-2020-6> 

Summary: Though they didn’t say on record, sources close to the government were cited as blaming a months-long cyberattack on China. All levels of government, industry, political organizations, education, health, essential service providers and operators, and other critical infrastructure were targeted. China denied involvement. Some methods used exploited weaknesses in code and phishing. The attacks were not categorized as sophisticated but effective as their targets were poorly defended.

Analysis: This is a case of a large number of essentially small security flaws adding up to a very large problem. The issue here is scale. This type of sustained attack can wear down the productivity of a country and overwhelm its ability to handle so many attacks in a timely and coordinated manner.

Proposed Resolution: PSA’s on phishing attacks would be an efficient way to reach a large portion of the population in a short period of time. Critical infrastructure must be a priority focus and any additional resources, if any and when available, should be dedicated to training corporate trainers to address the issue so their manpower can help disseminate the remedy.

Current Event 2

Title: ‘Ripple20’ Flaws in Medical Devices: The Risks

Author: Marianne Kolbasuk McGee

Publication Date: Jun 18, 2020

Link: <https://www.databreachtoday.com/interviews/ripple20-flaws-in-medical-devices-risks-i-4713>



Summary: 19 ‘Ripple 20’ vulnerabilities were revealed from a TCP/IP software library in Cincinnati named Treck. They make software for networking protocols in embedded systems. The flaws were not just limited to healthcare devices but also industrial control systems. The flaw could allow an attacker full control of the devices including the ability to shut them off.

Analysis: The potential impact is enormous. Gaining access to the devices through their internet protocols is not only hazardous to the equipment containing the flawed software, but it could act as a gateway to whatever network it is on, multiplying the effect of a cyber-attack. Just having the vulnerability could allow hackers to plant malicious software throughout networks they are connected to which could silently spread and perhaps be activated at a time of an attackers choosing to cause maximum damage.

Proposed Resolution: According to Elad Luz of CyberMDX, the first critical step is to identify all the potentially impacted equipment. “Imagine you're a hospital with thousands or tens of thousands of connected devices. You have to find out if you have certain affected models. And you want to know about every one of them because even if it's only 10 devices out of tens of thousands, it's those 10 devices that are the weakest link."