CTC #11: Ransomware

<https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/>

<https://www.youtube.com/watch?v=4gR562GW7TI>

This Cisco advertisement does not actually explain the anatomy of a ransomware attack but shows a fictitious example of how a hacker might perform the open source research and social engineering before executing an attack. It is a good example of the power of social engineering which exploits the natural trust between human beings. If an attacker can make their targets feel like their social engineering attack (phone call, phishing email, or information request) seems natural and expected, they will have a greater amount of success. One explicit strategy employed by the fictitious hacker to enhance her attack is *deception* and *misdirection.* The hacker executes a ransomware attack which draws the attention of the company and the media. This allows the hacker to exfiltrate of the company’s customer and financial data which was the real target. The money and the payout ($100,000 in this case) was just icing on the cake. This video also shows (although not in detail) how easy it is for criminals to execute this type of attack because of the available tools. Information about ransomware and what to do in the case of an infection (attack) can be found in an introductory article by Wired titled “What is Ransomware? A Guide to the Global Cyberattack’s Scary Method” (https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/). This article includes a short video that provides the basics of the attack and a discussion about the history and current trends (from 2012 – 2017). Ransomware, also called cryptocurrency attacks, seem to be popular with cyber criminals because they provide almost immediate monetization of cyberattacks. Instead of stealing information such as account credentials and credit card numbers, which must either be sold for money or be exploited in another way for money, ransom payments go directly to the attacker’s cryptocurrency account. Additionally, because cryptocurrency accounts provide anonymity, the money can be quickly transferred to another bank, and does not have to laundered via another method. Essentially, ransomware provides cyber criminals a very short kill chain, cutting out several other steps compared to other attacks.

CTC# 12: Computer Network Defense

This is a very interesting article from Lyu Janghua, a retired colonel from the Chinese People’s Liberation Army. Her researched has focused on cybersecurity and China-U.S. relations. She provides this article as an analysis of the recent cyber strategy released by the DoD and China’s public cyber policies. She focuses on the U.S.’s shift to a cyber strategy of “defending forward” used in the 2018 DoD Cyber Strategy released on 18 Sep 2018. This term is more aggressive than, active cyber defense, the term used in the previous strategy released in April of 2015. Defending forward portrays the idea of taking cyber defense to the source to protect the United States’ military advantage. Defending forward also targets threats that fall below the level of armed conflict. This strategy provides a lot more flexibility, than previous strategies, to meet cyber threats wherever they may be in the world if there is a significant threat to the nation’s military advantage. This article shows that the US is increasingly concerned about China as a general threat, but also, specifically, a cyber threat. One interesting insight in this article is that cyberspace connects countries that do not share physical boundaries. This can encourage cooperation and trust, but also conflict. This is a new reality in the age of cyber conflict. In this domain, if borders are defined, they touch the border of every other country.

CTC #13:

Design Thinking:

This article in Forbes magazine provides a simple definition of design thinking and how it can help make cybersecurity more effective. Design thinking is important because it puts the user at the center of the problem and the potential solutions. Design thinking consists of three principles: (1) begin with empathy for the end user, (2) focus on the solution, not the problem, and (3) iterate. Beginning with the user is essential because the user continues to be the weakest link in the chain of cyberspace and the most easily exploited. The second principle, helps us to figure out how to think long-term while deploying solutions that will add to the long-term solution. This is important, especially for the Air Force, as our solutions must be massive because we are operating on a massive network and trying to fulfill hundreds of different missions across the world. I believe this thinking is already present in the “pathfinder” mentality of Air Force Space Command over the past 10 years, but it needs to be reflected in how we acquire systems as well. The third principle of “iterate” is also needed in the Air Force and DoD. Rajat Mohanty writes, “design thinking teaches how to act small and fast. To build small prototypes. To refine what’s working. To break what isn’t. To embrace experimentation to prove (or disprove) ideas quickly and to constantly adjust to user feedback.” This iterative process will help the DoD to quickly figure out what is working, what is not working, and how to bring viable solutions to the warfighter.