Name: Ronit Singh **CDAD** **Date:** 19 September, 2021

CYBERWARFARE

Week 4 Reading Summary

The three readings for this week, *"Hackers Profiled — Who Are They and What Are Their Motivations?", "Issues of Implied Trust in Ethical Hacking", and "The Risk Propensity and Rationality of Computer Hackers",* explain the concept behind hackers and their different levels, motives, and their origins by comparing them with our current stereotypical view of them, and how they have evolved over time to pose a serious threat to organisations and people.

The first article*"Hackers Profiled — Who Are They and What Are Their Motivations?",* broadly classifies the cybercriminals into three main types i.e. **Script Kiddies, Hackers, and Crackers**. Script Kiddies are curiosity-driven teenagers or beginners who pose a lesser threat to highly secure infrastructures due to their limited skills, experience, capabilities, and resources. However, due to the availability of very powerful tools on the internet to perform attacks nowadays, they can be dangerous at times if misdirected. With gradual experience and guidance, they can progress to the second level called 'hackers'. Due to their extensive knowledge of programming languages and the inner workings of the internet, they have the capability to write their own exploits and scripts, and in turn perform more sophisticated attacks. They are also purely curiosity-driven and like to challenge themselves to penetrate a system to see what lies behind. Crackers are just hackers (have similar capabilities), but are purely malicious and hack for personal or monetary gains or to spread a particular political agenda. Moreover, the article also mentions various motivations behind hacking such as curiosity, vandalism, hacktivism, industrial espionage, extortion and fraud, and information warfare.

The second article, *"Issues of Implied Trust in Ethical Hacking",* dives deep into the ethical hacking world and its increasing implementation in the corporate sector. The author argues whether 'ethical' really means ethical? This is because more often, ethical hackers use unethical means in order to simulate the hacker mindset to gain information about the organisation they are supposed to attack and find vulnerabilities in the system to report. Moreover, the author questions whether it is really safe for the ethical hackers to be given full access to sensitive and confidential parts of the system, in the long term. If so, then how are ethical hackers supposed to follow the guidelines and not disclose anything, and thus **maintain trust between them and the client**. According to the author, "Trust plays an important role when organizations engage the services of ethical hackers." (Thomas, 4). Hence, the article goes over this issue to suggest a solution i.e. **code of ethics and conduct**. It lists out various organizations like ACS, CREST, EC-Council, ISACA, ISC2 etc. that give out several kinds of cybersecurity certifications, which include the study of ethics as well. However, these are organisation-dependent, and are not uniformly followed. Hence, there is a need for a mandatory and uniform code of conduct and ethics for cybersecurity professionals around the world.

In the third article, *“The Risk Propensity and Rationality of Computer Hackers”,* the author presents a research study done on hackers at one of the largest hacker conventions in Washington D.C. i.e. **ShmooCon** in 2008. With the help of a survey, he studied the mindset of more than hundred hackers present there. “The involvement in hacking activities was measured in three different categories: (1) technical intrusions, (2) social engineering attacks, and (3) malware distributions.” (Bachmann, 645). The author came to the conclusion that people with a hacker mindset are more thoughtful and are likely to delve into challenging tasks willingly, make quick decisions, try something out many times and not give up easily, and have more risk appetite than the general public. In the end, the article also raises concern over the challenges and limitations of combating cybercrimes in today's world. This has reduced the fear among hackers because “despite the annually increasing number of cybercrimes, only a relatively few high profile cybercrime cases are presently successfully tried, many of them without swift or severe punishments.” (Brenner, 2006). Hence, the author suggests that “more effective response by the criminal justice system is an urgent need—because it would increase the number of convicted cybercriminals and more importantly, because it would also have a preventive deterrence effect on the illegal parts of the hacking community.” (Bachmann, 653).

What surprised me?

I was surprised by this particular statement, “The average time it takes to detect a breach is reported to be between 99 and 172 days depending on the region” (Mandiant, 2017). That’s a lot of time, according to me. I feel if this is the case, then there’s a severe need to have a system such that the attacks or breaches are detected in real time or at least in a matter of weeks. This would help in implementing immediate security measures and prevent another attack during the time the breach is yet to be discovered. Moreover, the concept of ‘get out of jail free card’ was new to me. According to the article, it is a written authorization for ethical hackers to conduct an attack into the organization’s systems with permission and report the vulnerabilities, without getting convicted for doing so.

Questions?

1. Since the article mentions that the research study was “one step toward the establishment of cyber criminology as a distinct subfield of criminological research”, do you think this would deter hackers from breaking into the system?
2. Why do you think unemployed cybersecurity professionals are more likely to become malicious hackers than the employed ones?
3. How does the personality of an individual influence his/her hacking involvement?

References

- Barber, Richard. (2001). Hackers Profiled — Who Are They and What Are Their Motivations? Computer Fraud & Security. 2001. 14-17. 10.1016/S1361-3723(01)02017-6.
- Bachmann, Michael. "The Risk Propensity and Rationality of Computer Hackers." International Journal of Cyber Criminology, vol. 4, no. 1, 2010, pp. 643-656. ProQuest.
- Thomas, Georg & Burmeister, Oliver & Low, Gregory. (2017). Issues of Implied Trust in Ethical Hacking.