Criminal Profile

Trenesia Hurkes

[Institutional Affiliation(s)]

Author Note

Criminal Profile

# Profile

Joe is a 38 years old male. Joe came from a lower income family of hard-working parents who had saved to pay for his college education. Joe had a degree in Network Security and found a placement at IBM. He wanted to travel and managed to acquire a scholarship in a Chinese university, and decided it would be a good opportunity to explore a different part of the world. Here he enrolled into a Master’s degree in information systems, which is where he met Liu who introduced him to an organized group of cybercriminals which enticed him through offering an exciting life and financial benefits, which also gave him a sense of power. Continuing his degree, he would work in this cybercriminal organization disguised as an SME in Shanghai, China that operated as a highly organized enterprise. Joe continued to stay in Shanghai and told his family that he was working for an established multi-national organization.

# Fact Pattern: Crime

For Joe and the organization he belongs to, criminal activities were not just confined to hacking accounts. The organization had developed its own expertise in several areas of exploitation and hacking which involved data breaches of large organizations, industrial espionage, as well as providing hacktivism services to those who wish to prove a political point. For Joe, it was not just about thrills but rather a serious industry that has its own veterans (Saroha, 2014).

Psychologist’s profile Joe’s participation in cybercrime and hacking to be motivated from primarily an enjoyment of the feeling of power, peer recognition, feelings of addition, as well as to engage politically through subversive ways (Lickiewicz, 2011). Personality profile reveals that Joe demonstrated aspects of extroversion, neuroticism, agreeableness, and conscientiousness. Moreover, some traits exhibited aggressiveness, psychopathy as a lack of personal integrity (Bada, 2016).

Joe does not operate like a lone-wolf attacker. The organization he belongs to employs a range of tools and strategies in organized ways by combining forces to initiate highly coordinated cyber-attacks. They also own underground marketplaces where stolen identities and information can be purchased. They operate like an SME employing 90 people in which all management, deputies, heads and line managers’ work in different compartments such as belonging to production, marketing, operations and so on.

Joe and the organization he works for conduct a range of operations, which involve spyware/adware planting, industrial espionage, online extortion, developing virus technologies, dialers, and in particular ransomware attacks. They are also underground traders and sell of data and services to a range of individuals who need to threaten an individual or business with some trouble, financial hardship or to settle a personal vendetta. Moreover, they engage in social engineering through legitimate looking applications on the internet (Lusthaus, 2018).

# Fact Pattern: Ultimate Crime

An ultimate crime in which Joe was directly involved was hitting Rebecca, a celebrity model, with a ransomware attack. He managed to hack into her personal computer and network, to access personal data and encrypted some key data through malware that was nearly impossible to break through. The ransomware had a feature to allow the victim to communicate with Joe in which he threatened her with locking the important data forever unless she pays to obtain her important files back. Due to the critical nature of the data, that involved her various portfolios and work, she decided to pay Joe the demanded amount as ransom. Initially, Joe charged her with 1000$ for the first batch of data and subsequently 2500$ for the next batch. The payment was done through the Bitcoin service that Rebecca was initially not familiar with. A delay in payment led Joe to increase the Ransomware payment by 2000$ further to provide her the encryption key to unlock her data. The ransomware attack had caused Rebecca $15000 of losses.

# References

Bada, M. (2016, April 18). *Profiling the Cybercriminal*. Retrieved January 6, 2019, from CyberSecurity Capacity Portal: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/profiling-cybercriminal

Lickiewicz, J. (2011). Cyber Crime psychology-proposal of an offender psychological profile. *Problems of forensic sciences, 2*(3), 239-252.

Lusthaus, J. (2018). *Industry of anonymity: inside the business of cybercrime.* Cambridge, Massachusetts: Harvard University Press.

Saroha, R. (2014). Profiling a Cyber Criminal. *International Journal of Information and Computation Technology, 4*(3), 253-258.