University of Essex

Principles of Digital Forensics and Cyber Law January 2022

Unit 9 – Mid-Module Assignment 2: Blog Post

Criminals often disguise themselves as companies and trick victims into using malicious websites or installing malware on their devices. They will send thousands of emails to multiple targets simultaneously, as with phishing scams. People can have their sensitive personal information stolen through these kinds of scams. Criminals collect enough data about victims and verify their identities to commit fraud. For example, personal information may be used to open new bank accounts and obtain passports or driver's licenses.

Criminals can use the Internet to commit fraud and make counterfeit products. Furthermore, They can disguise websites as legitimate retailers or create a fake site that sells counterfeit goods. Intellectual property crime is when someone streams copyrighted material online without permission. These criminals often include movie releases or live sports broadcasts that are scheduled on TV networks like NBC Sports and ABC/ESPN Soccer Plus in advance of their broadcast dates.

As cybercrime increases at an unprecedented scale and pace, law enforcement and prosecutors' level of expertise should be increased to match current and anticipated future trends. Along with this, the new Cybercrime Act should be as technically neutral as possible -both now and in the future- to prevent any updates needed or limit investigation abilities.

Several practise and challenges could limit cyber-identity theft. One of them is the loss of data. For example, some European countries cannot obtain the data from private companies like the Internet Service Provider when other countries can. In addition, current data retention frameworks put undue pressure on investigators to prioritize operational activities instead of high-value goals. (Europol, 2019) As an open issue, Need for a new legislative framework regulating data retention for law enforcement purposes at EU-level.

However, with anonymous networks, cybercriminals can encrypt data to disguise their ISP address when connecting to the Internet and hide various activities or locations. For example, The Dark Web can be reached through decentralized, anonymized nodes on a number of networks including Tor (short for The Onion Router) or I2P (Invisible Internet Project). (Finklea, 2017)

Another obstruct is strong encryption. Strong cryptography is an integral part of digitized democracy and helps protect the most basic human rights and the security of the digital economy. Nevertheless, it is also the best opportunity for criminals to hide the crime data. Traceback illegal activities may take some time, depending on the creator's knowledge and abilities. The amount of time it takes depends on how well they disguise their identity and activities. Traceback occurs after a

cybercrime has occurred or when it is detected (Pihelgas, 2013). As a solution, law enforcement should be provided with the latest technologies to help them counter cryptography criminals.

The theft of personal information is rapidly growing, causing significant financial damage to millions of people. According to Finanso.se data, In 2018 and 2019, it was found that about half of Europeans had experienced at least one type of fraud. Nearly half of all identity theft attacks have occurred through email in European countries, while 39% came by phone calls. Statistics show that 25% of Europeans exposed to any type of fraud suffered financial damage and a total loss of €24 billion between 2018-2019. (Ilic, 2021)

References:

- Europol (2019) common challenges in combating cybercrime, https://www.europol.europa.eu/publications-events/publications/common-challenges-in-combating-cybercrime [Accessed 04 March 2022].
- Finklea, K. (2017) Dark Web. Available from: https://www.unodc.org/e4j/data/_university_uni_/dark_web.html?lng=en&match=Dark%20Web. [Accessed 19 March 2022].
- Pihelgas, M. (2013) Back-Tracing and Anonymity in Cyberspace. *Peacetime Regime for State Activities in Cyberspace*, pp.31-60. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.645.1982&rep=rep1&type=pdf#page=66. [Accessed 17 March 2022].
- Ilic, J (2021) One in five European Have Experienced Identity Theft Fraud in the Last Two Years. Available from: https://finanso.se/one-in-five-europeans-have-experienced-identity-theft-fraud-in-the-last-two-years/ [Accessed 21 March 2022].