horizontal line

**Plus971 Cybersecurity**

The Significance of Understanding Cyber Crimes for Cyber Forensic Analysts

**14th August 2023**

**Cyber crimes and their types:**

1. Hacking: gaining unauthorized access to a computer system or network with malicious intent such as to steal info, disrupt operations, cause damage etc.
   1. EXAMPLE: SolarWinds Hack (2020): A sophisticated cyber espionage operation allegedly backed by a nation-state that affected multiple US government agencies and companies.
2. Malware: Distributing malicious software to gain access to networks or systems with malicious intent, malware can be trojans,, spyware etc.
   1. EXAMPLE: The WannaCry ransomware attack in 2017 affected over 200,000 computers in 150 countries, demanding ransom for data decryption.
3. Phishing: sending emails pretending to be a legitimate source such as a bank and asking for PI(Personal information) or SPI(sensitive personal information) or providing an attachment that is embedded with malware, which when opened can compromise a system
   1. EXAMPLE: The phishing attack on John Podesta's email account during the 2016 U.S. presidential election.
4. Identity Theft: stealing PI or SPI’S of a person to impersonate them and do malicious acts such as fraud, credit card fraud or using the individuals name only to cheat people.
   1. EXAMPLE: The breach of Target's customer data in 2013 exposed credit card information of over 40 million customers
5. Online Fraud: a form of social engineering where users are tricked into sending personal information(PI) or SPI such as credit card info for saving a person from imprisonment.
   1. EXAMPLE: Nigerian 419 scams where victims are promised large sums of money in exchange for small upfront fees.
6. Cyber Bullying: Harassment, threats, offensive words or slurs are types of bullying and when done over social media or internet it then becomes cyber bullying.
   1. EXAMPLE: teenagers facing relentless online harassment, leading to severe psychological impact.

**Impact of Cyber Crimes**

**Financial Loss:**

money is stolen from people or organizations, and in the case of credit card fraud the person cant get a loan or many times cant even open a bank account.

EXAMPLE: 81 million was stolen from bangladesh bank in 2016

**Data Breaches:**

sensitive info is stolen from organizations or people.

EXAMPLE: 50 Million Credit Cards Data Stolen from Home Depot’s System (2014)

**Reputation Damage:**

if sensitive information comes out or is leaked it could lead to the reputation of the person in shambles

EXAMPLE: Hillary Clinton's campaign manager John Podesta’s emails were leaked where he said phrases like “Needy Latinos” which lead to a drop in his popularity.

**Disruption of Services:**

an attack that leaves a service unavailable

EXAMPLE: in june 2023 microsoft claimed that a ddos attack left the microsoft office suite unusable

**Psychological impact:**

the impact on humans who were victims of a cyber attack

EXAMPLE: A person might experience anger, fear, and sadness, or events like nightmares and flashbacks. This is commonly found in videogame chat rooms such as vr char which is a place where preying adults can influence young children who play the game.

**National Security:**

when a cyber attack comprises a nation's secrets or causes a financial loss for the country and its residents.

EXAMPLE: In May 2021, Colonial Pipeline temporarily halted the operations of the pipeline due to the ransomware attack. DarkSide, a Russian hacking group, was responsible . It was the largest cyberattack on an energy infrastructure target in US history. This caused many homes to lose power.

**Role and responsibility of cyber forensic analysts:**

1. **Contextual Understanding:**
   1. Analysts need to comprehend the TTP,s (tactics, techniques and procedures) of many different attacks and their motivations, this will greatly increase their understanding of an attacker's MO.
   2. And will also help the analyst come up with preventative measures against future threats.
2. **Accurate evidence Gathering/handling:**
   1. Investigating cyber crimes preserving information, gathering the info and analyzing the info.
   2. This helps analysts with knowing where to look for information, how to look for evidence and how to handle it without compromising the integrity of the machine which leads to loss of potential case breaking information. It also adds to their own investigative capabilities so that they can find exploits themselves and patch them.
3. **Ethical and legal considerations:**
   1. Analysts must adhere to the laws of their particular region and have ethical standards as the evidence they collect will be used in court to determine a verdict.
   2. And thus must know legal procedures, search and seizure laws, data privacy regulations and rules for presenting data in court.
4. **Malware analysis:**
   1. Understanding how mallware operates, spreads and interacts with a machine is crucial in understanding how to defend against them
   2. Analysts should be able to dissect a malware and understand what it is doing, where the malicious part lies, what vulnerabilities it's exploiting etc. by doing this they gain insight into more vulnerabilities that can be patched and can add to the library of IOC’s
5. **Network Forensics:**
   1. Cyber forensics analysts should familiarize themselves with network protocols, vulnerabilities in the TCP/IP stack for instance. This helps them look at and analyze a networks traffic and determine whether it is malicious or not
6. **Incident Response:**
   1. Whether it is responding to a incident or investigating a crime, the analyst should use a methodical process where every step is documented in a playbook, not only for backtracking and avoiding repetition but for future analysts who might encounter a similar attack, it gives them a good headstart/starting point
7. **Report Writing:**
   1. An analyst needs to get their points across with clear and concise language to present findings to non technical people, often judges in court and thus must also use appropriate legal terms, a balance between showcasing the technical side of the case and maintaining understandability needs to be present when writing the report.
8. **Continuous Learning:**
   1. An analyst needs to be constantly kept up to date with the latest developments in cyber security as new vulnerabilities are found everyday. By analyzing previous attacks they can patch existing vulnerabilities while also reducing their response time the next time an attack happens, reducing downtime and quickening the investigation.
9. **Professional growth**
   1. The greater an analyst's knowledge the greater their reputation in the cyber forensics field, this will allow them to write papers, look into more difficult attacks etc.