Types of Cyber Crimes
Case Study

(Author: Soham Helekar)

1. Summary

This document delves into various cybercrimes, such as malware attacks, phishing, identity theft, and cyberstalking, presenting detailed case studies. Each case explores how cybercriminals exploited vulnerabilities in systems, causing significant damage to individuals, organizations, and public trust. Notable incidents like the WannaCry ransomware attack, the Equifax data breach, and the ILOVEYOU virus are discussed, emphasizing the widespread impact on different sectors, including healthcare, finance, and personal privacy.

The document also outlines the responses and measures taken by affected entities to prevent future attacks, including strengthening security protocols, implementing new cybersecurity technologies, and increasing awareness. These actions not only helped mitigate the immediate damage but also contributed to enhancing overall cybersecurity practices, ensuring a more resilient defense against evolving cyber threats.

2. Malware Attacks (Ransomware, Rootkit, Virus, Trojan)

WannaCry Attack

Incident: In May 2017, a ransomware attack known as WannaCry spread rapidly across the globe, affecting over 200,000 computers in 150 countries. The malware encrypted files on infected computers, demanding ransom payments in Bitcoin to unlock them.

Impact: The attack hit various sectors, including healthcare, where the UK's National Health Service (NHS) was severely disrupted, causing appointments and surgeries to be canceled. Organizations worldwide faced significant downtime and financial losses.

Response: The cybersecurity community quickly identified a kill switch in the ransomware's code, which halted the spread. However, many organizations had to restore data from backups and strengthen their cybersecurity defenses.

3. Malvertising

Yahoo! Ad Network Attack

Incident: In 2015, Yahoo!'s ad network was compromised by cybercriminals who inserted malicious advertisements. These ads redirected users to websites that delivered malware, including ransomware and banking trojans, without the users' knowledge.

Impact: Millions of Yahoo! users were exposed to the malicious ads over the span of a week. The attack affected users worldwide, leading to potential data breaches, financial losses, and compromised personal information.

Response: Yahoo! quickly removed the malicious ads and collaborated with cybersecurity firms to track down the source of the malvertising campaign. They also implemented stricter security measures in their ad network to prevent similar incidents in the future.

4. Phishing Attacks

ILOVEYOU Virus

Incident: In May 2000, the ILOVEYOU virus, a computer worm, spread through email systems worldwide. It arrived as an email attachment with the subject line "ILOVEYOU," enticing recipients to open it.

Impact: The virus infected millions of computers, causing billions of dollars in damage by overwriting files, stealing passwords, and spreading itself to every contact in the infected users' email address books. It disrupted businesses, government agencies, and personal users.

Response: Organizations and individuals were urged to update their antivirus software and avoid opening suspicious email attachments. The incident led to increased awareness about email security and the importance of having robust cybersecurity measures in place.

5. Misuse of Personal Information (Identity Theft) and Cyberstalking

Equifax Data Breach

Incident: In 2017, Equifax, one of the largest credit reporting agencies in the US, suffered a data breach that exposed the personal information of approximately 147 million people. Hackers exploited a vulnerability in a web application to gain access to sensitive data, including Social Security numbers, birth dates, addresses, and driver's license numbers.

Impact: The breach led to widespread identity theft, as the stolen information was used to open fraudulent accounts, apply for loans, and commit other forms of financial fraud. Victims faced long-term repercussions, including damaged credit scores and financial losses. The incident also caused significant public outcry and loss of trust in Equifax.

Response: Equifax offered free credit monitoring and identity theft protection services to affected individuals. The company also faced numerous lawsuits and regulatory scrutiny, leading to a settlement that included financial compensation for victims. Equifax implemented enhanced security measures and hired a new Chief Information Security Officer (CISO) to oversee cybersecurity efforts.

The Case of Shannon Sharpe

Incident: In 2021, Shannon Sharpe, a former NFL player and TV personality, was targeted by a cyberstalker who repeatedly sent him threatening messages and made false accusations on social media. The stalker created multiple fake accounts to harass Sharpe and his family, causing significant distress and fear for their safety.

Impact: The cyberstalking caused emotional and psychological harm to Sharpe and his family. It also damaged his reputation and created a hostile online environment. The relentless harassment highlighted the challenges of addressing cyberstalking and the limitations of existing legal frameworks.

Response: Sharpe reported the incidents to law enforcement and worked with cybersecurity experts to identify and block the stalker's accounts. Social media platforms were also notified, leading to the removal of the offending accounts. Sharpe used his platform to raise awareness about cyberstalking and advocate for stronger legal protections for victims. Additionally, increased efforts were made to enhance online safety and privacy measures.

6. Creating Fake Profiles

The Case of LinkedIn Scammers

Incident: In 2018, LinkedIn users were targeted by scammers creating fake profiles to connect with professionals, often impersonating legitimate executives or recruiters. These fake profiles were used to gain trust and extract sensitive information, such as personal details, financial information, or confidential company data.

Impact: Many LinkedIn users were deceived into sharing personal and professional information, leading to identity theft, financial fraud, and corporate espionage. The trust in LinkedIn's platform was undermined, causing concern among users about the legitimacy of connection requests and the safety of their data.

Response: LinkedIn took steps to identify and remove fake profiles by enhancing its automated detection systems and employing more rigorous verification processes. The platform also provided guidelines to help users recognize and report suspicious profiles. LinkedIn worked closely with cybersecurity firms to track down and mitigate the activities of these scammers. Users were educated about the risks of sharing sensitive information online and advised to verify the authenticity of connection requests.

7. Web Defacement

Bangladesh Bank Website

Incident: In January 2021, the official website of Bangladesh Bank was defaced by hackers. The attackers replaced the homepage with their own messages, which included political statements and criticism of the bank's security measures. The defacement disrupted the bank's online presence and caused embarrassment.

Impact: The defacement damaged the reputation of Bangladesh Bank, highlighting vulnerabilities in its cybersecurity infrastructure. The incident raised concerns among stakeholders about the security of sensitive financial data and the bank's overall ability to protect its digital assets. It also led to a temporary loss of trust among the bank's customers and partners.

Response: Bangladesh Bank quickly took down the defaced website and restored it to its original state. They launched an investigation to identify the perpetrators and understand how the attack was carried out. The bank also collaborated with cybersecurity experts to strengthen its defenses and prevent future attacks. Public statements were made to assure customers and stakeholders that the breach did not affect financial transactions or sensitive data. Additionally, Bangladesh Bank conducted an internal review of its cybersecurity policies and implemented more stringent security measures.

8. Web Jacking

The New York Times Website Incident

Incident: In August 2013, the website of The New York Times was hijacked by the Syrian Electronic Army (SEA), a hacker group known for supporting the Syrian government. The attackers redirected visitors to a SEA-controlled page by compromising the DNS records of The New York Times.

Impact: The web jacking incident caused significant disruption as visitors to The New York Times website were unable to access news content and were instead greeted with a message from the hackers. The attack not only impacted the newspaper's reputation but also raised concerns about the security of online media outlets. It highlighted the vulnerability of DNS systems and the potential for widespread misinformation.

Response: The New York Times worked with its DNS provider and cybersecurity experts to regain control of its DNS records and restore access to its website. The company implemented additional security measures, including two-factor authentication for DNS account access and regular monitoring of DNS records for suspicious activity. The incident also prompted other organizations to review and strengthen their DNS security practices to prevent similar attacks.

9. Juice Jacking

Los Angeles Charging Stations

Incident: In November 2019, the Los Angeles County District Attorney's Office issued a warning about the risk of juice jacking at public charging stations in airports, hotels, and other locations. Juice jacking occurs when malware is installed on a device via a compromised charging port or cable, potentially leading to data theft or device hijacking.

Impact: The warning highlighted the potential risks to travelers and the general public who rely on public USB charging stations. While specific incidents were not publicly detailed, the awareness campaign underscored the dangers of using unsecured charging stations, which could lead to personal data theft, unauthorized access to sensitive information, and compromised device functionality.

Response: Following the warning, individuals were advised to use personal charging accessories, such as USB data blockers, portable power banks, and AC chargers. Public awareness increased regarding the risks of using public USB ports, leading to more cautious behavior among device users. Organizations also started to take steps to secure their public charging stations and educate their employees and customers about safe charging practices.

10. Distributed Denial of Service Attacks (DDoS)

GitHub

Incident: In February 2018, GitHub, a popular code hosting platform, experienced a powerful DDoS attack that disrupted its services for several minutes. The attack targeted GitHub's engineering team pages and caused intermittent outages for users worldwide.

Impact: The DDoS attack temporarily disrupted access to GitHub, affecting developers and organizations relying on the platform for code collaboration and project management. While GitHub quickly mitigated the attack, the incident raised concerns about the resilience of major online services against large-scale DDoS attacks.

Response: GitHub responded by implementing additional layers of DDoS protection and scaling up its infrastructure to handle future attacks more effectively. The platform also improved its incident response protocols and communication strategies to keep users informed during service disruptions. The incident prompted GitHub and other tech companies to enhance their DDoS mitigation strategies and invest in robust cybersecurity defenses.

11. Software Piracy

The Case of Adobe Photoshop

Incident: Adobe Photoshop, a widely used software for image editing, has been a frequent target of software piracy. Various versions of Adobe Photoshop have been illegally distributed through online platforms, torrent websites, and peer-to-peer networks without proper licensing or authorization from Adobe.

Impact: Software piracy of Adobe Photoshop has resulted in significant financial losses for Adobe Systems Incorporated. The unauthorized distribution of software versions deprives Adobe of potential revenue from legitimate sales and software subscriptions. It also undermines the company's efforts to maintain control over its intellectual property rights and software distribution channels.

Response: Adobe has implemented several measures to combat software piracy, including digital rights management (DRM) technologies, software activation mechanisms, and legal actions against distributors of pirated software. Adobe also offers subscription-based licensing models, such as Adobe Creative Cloud, which provides users with legal access to Adobe Photoshop and other Adobe software products through a monthly or annual subscription fee. Additionally, Adobe engages in public awareness campaigns to educate consumers and businesses about the risks and consequences of using pirated software.

12. Form jacking

British Airways Data Breach

Incident: In 2018, British Airways experienced a form jacking attack where malicious code was injected into the airline's payment page. The attackers intercepted and stole payment card details, including names, addresses, and credit card information, from customers making bookings on the British Airways website.

Impact: The form jacking attack affected approximately 380,000 transactions, compromising sensitive financial information of British Airways customers. The stolen data was used for fraudulent transactions, leading to financial losses and potential identity theft for affected individuals. The incident also damaged British Airways' reputation and resulted in regulatory scrutiny over the airline's cybersecurity practices.

Response: British Airways quickly detected and mitigated the form jacking attack by removing the malicious code from its website and enhancing security measures. The airline notified affected customers and offered them free credit monitoring services as a precautionary measure. British Airways also faced legal consequences, including a £183 million fine imposed by the UK's Information Commissioner's Office (ICO) under the GDPR regulation for failing to protect customers' personal data adequately.

13. Conclusion

In conclusion, this document highlights the evolving landscape of cybercrimes, showcasing how attackers continuously adapt their tactics to exploit vulnerabilities. By examining real-world case studies, it emphasizes the far-reaching consequences of these crimes on individuals, businesses, and public institutions. The responses to these incidents reflect the importance of proactive cybersecurity measures, collaboration among organizations, and the need for constant vigilance to safeguard digital assets. As cyber threats become more sophisticated, it is crucial to stay informed, implement robust security protocols, and cultivate a culture of cybersecurity awareness to protect against future attacks.