TITLE PAGE

DIGITAL REGENESYS

CYBERSECURITY FULLSTACK COURSE

[BATCH 29]

CYBERSECURITY FUNDAMENTALS

INSTRUCTOR

[Dr. Saquib Ahmad Khan]

RESEARCH WORK
SUBMITTED

BY
DANIEL ZADVA JNR.
[DREG008502]

FEBRUARY 2025

INTRODUCTION

This research work aims at discussing common cybersecurity threats, actors that perpetrate those threats and further discuss a case of cybersecurity scandal “Facebook and Cambridge Analytica data breaches Scandal”.

CYBERSECURITY THREATS

According to Computing Technology Industry Association (CompTIA) cybersecurity threats refers to any malicious activity or potential danger that aims to steal, damage or disrupt digital data or systems including actions like data breaches, computer viruses, denial of service attacks, and other forms of cyber-attacks aimed at compromising the integrity or availability of information within a network or system; essentially, it is a potential danger posed by cybercriminals to your digital environment. The following section will discuss most common cybersecurity threats that threaten digital systems and online security.

Malware

The term malware is derived from “malicious + software”, mal+ware -> malware. Malware is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the users’ computer security and privacy. Popular examples of malware are: trojans, spyware, adware, rootkits, bots, worms etc.

Phishing

Phishing is a cyberattack that involves tricking people into sharing sensitive information or money. Attackers often pose as a legitimate organization or person in emails or text messages.

Social Engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Man in the Middle Attack (MitM) Attacks

A "Man in the Middle" (MitM) attack is a cybercrime where a hacker secretly positions themselves between two communicating parties, intercepting and potentially altering their data exchange without either party realizing, allowing the attacker to steal sensitive information like login credentials, financial details, or personal data by eavesdropping on their communication.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

A Denial of Service (DoS) attack is a cyber-attack where a malicious actor attempts to make a computer or network resource unavailable to legitimate users by overwhelming it with traffic, while a Distributed Denial of Service (DDoS) attack is a more severe version where multiple compromised devices (often forming a botnet) are used to launch the same overwhelming traffic against a target, significantly increasing the attack's power and impact.

Zero-Day Exploits

A zero-day exploit is a cyberattack vector that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware. "Zero day" refers to the fact that the software or device vendor has zero days to fix the flaw because malicious actors can already use it to access vulnerable systems.

SQL Injection

In computing, SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Cross-Site Scripting (XSS)

Cross-site scripting (XSS) is a security flaw that allows attackers to inject malicious scripts into a website's code. The scripts are then executed by the user's browser.

Ransomware

According to the US National Cybersecurity Center Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption.

Insider Threat

An insider threat is a cybersecurity risk that comes from someone who has access to an organization's data and systems. This could be a current or former employee, contractor, or other business associate.

THREATS ACTORS

A "cybersecurity threat actor" refers to an individual or group that intentionally attempts to compromise computer systems, networks, or data with malicious intent, often by exploiting vulnerabilities to steal information, disrupt operations, or cause financial damage; essentially, anyone who actively seeks to harm a digital system or organization through cyber-attacks. Most popular actors include:

Nation States

Cyber-attacks by a nation can inflict detrimental impact by disrupting communications, military activities, and everyday life.

Criminal Groups

Criminal groups aim to infiltrate systems or networks for financial gain. These groups use phishing, spam, spyware, and malware to conduct identity theft, online fraud, and system extortion.

Hackers

Hackers explore various cyber techniques to breach defenses and exploit vulnerabilities in a computer system or network. They are motivated by personal gain, revenge, stalking, financial gain, and political activism. Hackers develop new types of threats for the thrill of challenge or bragging rights in the hacker community.

Terrorist Groups

Terrorists conduct cyber-attacks to destroy, infiltrate, or exploit critical infrastructure to threaten national security, compromise military equipment, disrupt the economy, and cause mass casualties.

Hacktivists

Hacktivists carry out cyberattacks in support of political causes rather than for financial gain. They target industries, organizations, or individuals who do not align with their political ideas and agenda.

Malicious Insiders

97% of surveyed IT leaders expressed concerns about insider threats in cybersecurity. Insiders can include employees, third-party vendors, contractors, or other business associates who have legitimate access to enterprise assets but misuse that access to steal or destroy information for financial or personal gain.

Corporate Spies

Corporate spies conduct industrial or business espionage to either make a profit or disrupt a competitor's business by attacking critical infrastructure, stealing trade secrets, and gaining access.

FACEBOOK–CAMBRIDGE ANALYTICA DATA SCANDAL

Background

In the 2010s, personal data belonging to millions of Facebook users was collected by British consulting firm Cambridge Analytica for political advertising, without the informed consent of users. The data was collected through an app called "This Is Your Digital Life", developed by data scientist Aleksandr Kogan and his company Global Science Research in 2013. The app consisted of a series of questions to build psychological profiles on users and collected the personal data of the users' Facebook friends via Facebook's Open Graph platform. The app harvested the data of up to 87 million Facebook profiles. Cambridge Analytica used the data to assist the 2016 presidential campaigns of Ted Cruz and Donald Trump. Cambridge Analytica was also accused of interfering with the Brexit referendum, although the official investigation recognized that the company was not involved "beyond some initial enquiries" and that "no significant breaches" took place.

In 2018, Christopher Wylie, a former Cambridge Analytica employee, disclosed information about the data misuse. In response, Facebook apologized for their role in the data harvesting, and CEO Mark Zuckerberg testified in front of Congress. In July 2019, Facebook was fined $5 billion by the Federal Trade Commission for privacy violations. In October 2019, Facebook agreed to pay a £500,000 fine to the UK Information Commissioner's Office. In May 2018, Cambridge Analytica filed for Chapter 7 bankruptcy.

Other advertising agencies have been implementing various forms of psychological targeting for years, and Facebook had patented a similar technology in 2012. Cambridge Analytica's methods and their high-profile clients brought the problems of psychological targeting to public awareness. The scandal sparked increased public interest in privacy and social media's influence on politics. The online movement #DeleteFacebook trended on Twitter.

Overview

Aleksandr Kogan, a data scientist at the University of Cambridge, was hired by Cambridge Analytica to develop an app called "This Is Your Digital Life". Cambridge Analytica arranged an informed consent process for research in which several hundred thousand Facebook users agreed to complete a survey for payment that was only for academic use. However, Facebook allowed this app to collect personal information from survey respondents and their Facebook friends, leading to the acquisition of data from millions of Facebook users.

The collection of personal data by Cambridge Analytica was first reported in December 2015. Reports followed in 2016 and 2017, detailing how Cambridge Analytica used data harvested from millions of Facebook accounts without consent. In his 2016 presidential campaign, Trump paid Cambridge Analytica for data on Americans and their political preferences.

In March 2018, whistleblower Christopher Wylie revealed more information about the data breach. The Guardian and The New York Times published articles simultaneously, leading to significant public and political backlash. Facebook's market capitalization dropped by over $100 billion, and CEO Mark Zuckerberg agreed to testify in front of Congress.

Data Characteristics

- **Numbers:** The data set included information on up to 87 million Facebook users, with 70.6 million from the United States. California, Texas, and Florida were the most affected states.
- **Information:** The data included users' public profiles, page likes, birthdays, current cities, and sometimes News Feed, timeline, and messages. This data was used to create psychographic profiles for targeted political advertising.

Data Use

- Ted Cruz Campaign: In 2016, Ted Cruz hired Cambridge Analytica for his presidential campaign, paying $5.8 million for services. The data was used to create tailored advertisements to sway voters.
- Donald Trump Campaign: Trump's 2016 campaign used the data to build psychographic profiles and micro-target voters with customized messages. Ads were segmented based on support levels and swing votes, with different visuals and messages for each group.

Alleged Usage

- **Russia:** In 2018, the UK Parliament questioned Cambridge Analytica's connections with Russian oil company Lukoil. Concerns were raised about the company's data being used to target American voters.
- Brexit: Cambridge Analytica was allegedly hired by Leave.EU and the UK Independence Party to support Brexit. Internal emails suggested involvement, but the official investigation found no significant breaches.

Responses

- **Facebook:** CEO Mark Zuckerberg apologized for the situation, calling it a breach of trust. Facebook implemented changes to prevent similar breaches and established Social Science One in response. The company faced fines and legal actions from various governments.
- **Governmental Actions:** The UK fined Facebook £500,000, and the FTC fined Facebook $5 billion. The FTC also sued Cambridge Analytica's CEO and the app developer, leading to administrative orders and the destruction of collected data. Facebook agreed to pay $100 million to settle with the SEC for misleading investors.

Impact on Facebook Users and Investors

Since April 2018, user activity on Facebook decreased by almost 20%, although user growth increased by 1.8% during the final quarter of 2018. Facebook's stock fell by about 24% after the story broke but recovered by May 2018.

#DeleteFacebook Movement

The public reacted to the data privacy breach by initiating the #DeleteFacebook campaign to boycott Facebook. The co-founder of WhatsApp joined the movement, and the hashtag was tweeted almost 400,000 times within 30 days. Despite concerns, a survey found that about 48% of Facebook users wouldn't cut back on their usage. Mark Zuckerberg commented that the company hadn't seen a significant number of people deleting Facebook.

#OwnYourData Campaign

Brittany Kaiser coined the hashtag #OwnYourData to push for increased transparency on Facebook. She also created the Own Your Data Foundation to promote digital intelligence education.

The Great Hack

The 2019 Netflix documentary "The Great Hack" covered the Facebook–Cambridge Analytica data scandal, providing background information and personal journeys of individuals involved, including David Carroll and Brittany Kaiser.

Witness and Expert Testimony

The United States Senate Judiciary Committee held two hearings on the data breach and data privacy. Mark Zuckerberg testified, apologizing for the breach and acknowledging his responsibility. Experts like Eitan Hersh and Mark Jamison testified about voter targeting and data usage.

Aftermath

Following the downfall of Cambridge Analytica, related companies like Emerdata Limited and Auspex International were established. Emerdata acquired Cambridge and SCL, but did not inherit their data or assets. In 2021, NPR revisited the scandal, noting Facebook's lack of responsibility. In 2022, Meta Platforms agreed to pay $725 million to settle a class-action lawsuit related to improper data sharing.

REFERENCES

ABC News. (2018, April 5). Facebook says 300,000 Australians may have had their data 'improperly shared'. Retrieved from https://www.abc.net.au

BBC. (2019, October 30). Facebook agrees to pay Cambridge Analytica a fine in the UK. Retrieved from https://www.bbc.com

BBC. (2020, October 7). Cambridge Analytica 'not involved' in Brexit referendum, says watchdog. Retrieved from https://www.bbc.com

Business Insider. (n.d.). PolitiFact - Trump campaign used Cambridge Analytica in final months of campaign. Retrieved from https://www.politifact.com

Cadwalladr, C. (2017, February 26). Revealed: How US billionaire helped to back Brexit. The Observer. Retrieved from https://www.theguardian.com

Cadwalladr, C. (2017, May 7). The great British Brexit robbery: How our democracy was hijacked. The Guardian. Retrieved from https://www.theguardian.com

Chan, R. (2021). The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections. Business Insider. Retrieved from https://www.businessinsider.com

Chen, B. X. (2018, March 21). Want to #DeleteFacebook? You can try. The New York Times. Retrieved from https://www.nytimes.com

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The scandal and the fallout so far. The New York Times. Retrieved from https://www.nytimes.com

Davies, H. (2015, December 11). Ted Cruz campaign using a firm that harvested data on millions of unwitting Facebook users. The Guardian. Retrieved from https://www.theguardian.com

Funk, M. (2016, November 19). Cambridge Analytica and the secret agenda of a Facebook quiz. The New York Times. Retrieved from https://www.nytimes.com

Graham-Harrison, E., & Cadwalladr, C. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. Retrieved from https://www.theguardian.com

Kaminska, I. (2020, October 7). Cambridge Analytica probe finds no evidence it misused data to influence Brexit. The Financial Times. Retrieved from https://www.ft.com

Krogerus, H. G., & Mikael, M. (2017, January 28). The data that turned the world upside down. Vice. Retrieved from https://www.vice.com

Ma, A., & Gilbert, B. (2021). Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Business Insider. Retrieved from https://www.businessinsider.com

Matz, S., Appel, R., & Kosinski, M. (2020, February). Privacy in the age of psychological targeting. Current Opinion in Psychology, 31, 116–121. https://doi.org/10.1016/j.copsyc.2019.08.010

Meredith, S. (2018, April 10). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. CNBC. Retrieved from https://www.cnbc.com

National Cyber Security Centre. (n.d.). Ransomware guidance. Retrieved from https://www.ncsc.gov.uk/ransomware/home

Reuters. (2018, May 18). Cambridge Analytica files for bankruptcy in the U.S. following the Facebook debacle. Retrieved from https://www.reuters.com

Schwartz, M. (2017, March 30). Facebook failed to protect 30 million users from having their data harvested by a Trump campaign affiliate. The Intercept. Retrieved from https://theintercept.com

Smith, A. (2020). There's an open secret about Cambridge Analytica in the political world: It doesn't have the 'secret sauce' it claims. Business Insider. Retrieved from https://www.businessinsider.com

StealthLabs. (n.d.). Cyber security threats: All you need to know. Retrieved from https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/

The Georgia Straight. (2019, April 17). British investigative journalist Carole Cadwalladr sticks it to the gods of Silicon Valley in Vancouver TED talk. Retrieved from https://www.straight.com

The Guardian. (2019, July 12). Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports. Retrieved from https://www.theguardian.com

The Guardian. (n.d.). Cambridge Analytica did work for Leave. EU, emails confirm. Retrieved from https://www.theguardian.com