CS50 CYBERSECURITY

SNAPPFOOD Data Breach in Iran
Dec 2023

By: Rasool Hashemi

Final Project Presentation

Analyzing the Snappfood Hack in Iran

- **Name:** Rasool Hashemi
- **edX username**: rhawshemi
- **GitHub username**: hawshemi
- **Date of Recording**: 25/Jan/2024
- **Topic**: Focusing on the Snappfood hack in Iran, a significant incident in recent Iran's cybersecurity history.

Snappfood Data Breach Overview

Comprehensive Incident Analysis

- **Breach Overview**: In late 2023, Snappfood, a leading Iranian online food delivery service, experienced a significant data breach. The cybercriminals, operating under the alias 'irleaks', disclosed the breach on various platforms including Breach Forums and Telegram.
- **Scope of Data Compromised**: The breach involved over 3TB of data, affecting over 20 million user profiles, 240,000 vendors, 600,000 payment records, 180 million devices, 880 million product orders, 360 million orders, 35,000 bikers and riders details, and 130 million trip records.
- **Response and Negotiation**: Snappfood acknowledged the breach and engaged in negotiations with 'irleaks'. An agreement was reportedly reached, preventing the sale or leakage of the data online.
- **Context of Incident**: This breach is part of a disturbing trend in Iran's cybersecurity landscape, with several high-profile companies falling victim to similar incidents.

Technical Aspects of the Snappfood Breach

In-Depth Analysis of the Cyberattack

- **Method of Attack:** Likely involved advanced network penetration techniques, such as exploiting unpatched vulnerabilities or spear-phishing, followed by lateral movement within the network and data exfiltration using encrypted channels.
- **Type of Data Compromised:** Breach extended to sensitive customer data (personal and payment information), indicating a compromise of database security, possibly through SQL injection or inadequate access controls.
- **Security Measures in Place:** The breach's scale suggests potential gaps in network security, such as inadequate real-time monitoring, endpoint protection, and possibly flawed implementation of data encryption protocols.
- **Response to the Breach:** Involved immediate acknowledgment and collaboration with Iran's Cyber Police for forensic analysis, alongside direct negotiations with 'irleaks' to prevent further data leakage.

Impact of the Snappfood Breach

Consequences and Implications

- **Immediate Impact on Snappfood:** The breach likely led to immediate operational disruptions and security overhauls, alongside significant customer trust issues, potentially impacting user retention and company valuation.
- **Long-term Implications for Users:** Exposed users face heightened risks of identity theft and financial fraud, given the sensitive nature of the compromised data, necessitating ongoing vigilance against fraud and phishing attempts.
- **Reputational Damage:** The scale and nature of the breach likely resulted in considerable reputational harm to Snappfood, potentially affecting customer loyalty and attracting scrutiny from investors and regulators.
- **Wider Industry Implications:** This incident highlights the escalating cybersecurity risks within the digital economy, underscoring the need for enhanced industry-wide data protection and cybersecurity measures.

Legal and Regulatory Responses

Consequences and Compliance

- **Legal Actions and Compliance:** The incident may lead to legal scrutiny under data protection laws, with Snappfood potentially facing fines and mandatory compliance measures to safeguard user data.
- **Industry-Wide Regulatory Impact**: The breach could catalyze a reassessment of data security regulations in Iran, potentially leading to stricter enforcement and enhanced cybersecurity mandates for digital platforms.
- **Snappfood's Internal Measures**: Post-breach, Snappfood would likely need to implement rigorous security upgrades, undergo regular audits, and possibly restructure its data governance to align with enhanced regulatory requirements.
- **Global Perspective on Data Breach Responses:** The Snappfood incident contributes to the global dialogue on cybersecurity, emphasizing the need for robust international standards and coordinated efforts to protect digital data.

Data Security Vulnerabilities in Snappfood's Infrastructure

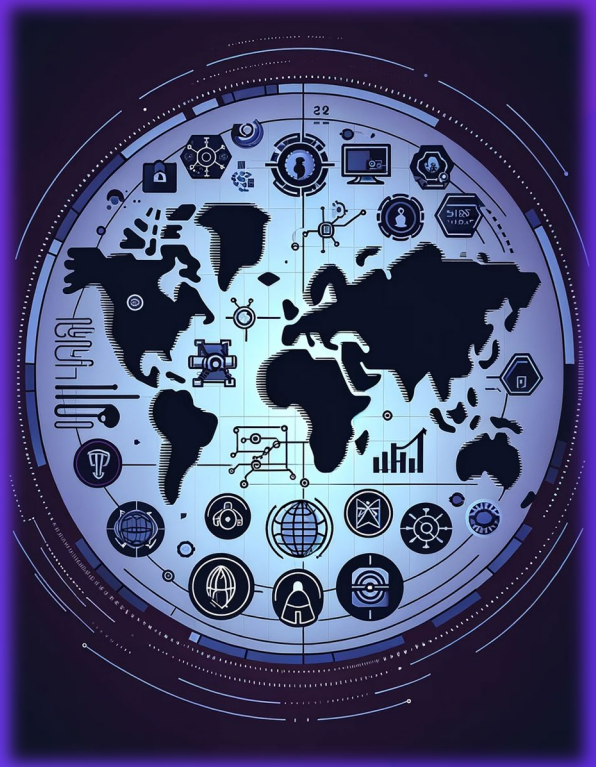
Analyzing Potential Weaknesses

- **Identifying Vulnerabilities**: Analysis suggests potential exploitation of unpatched system vulnerabilities, possibly within Snappfood's server infrastructure or through its API endpoints. Vulnerabilities might include SQL injection, cross-site scripting, or server misconfigurations.
- **Impact of Vulnerabilities**: The breach indicates possible weaknesses in data encryption at rest and in transit, along with inadequate access control mechanisms. The lack of robust encryption protocols like AES-256 or TLS for data transmission could have been a factor.
- **Improvement Measures**: The scale of data accessed points to possible lapses in endpoint security, suggesting that internal systems might have been compromised, possibly through phishing attacks or exploiting zero-day vulnerabilities.

Global Context of Cybersecurity Breaches

Comparative Analysis

- **Global Breach Incidents**: Comparing the attack vectors used in the Snappfood hack with global incidents, like the Marriott and Equifax breaches, suggests similarities in exploiting system vulnerabilities and lateral movement within the network.
- **Learning from Global Breaches**: The breach highlights the need for compliance with global cybersecurity frameworks like ISO/IEC 27001 and adherence to protocols outlined in frameworks such as NIST.
- **International Cybersecurity Standards**: Considering the sophistication of the attack, it's plausible that an APT group might have been involved, using advanced techniques like spear-phishing, backdoors, and rootkits for prolonged and undetected access.



User Data Protection: Best Practices

Securing Digital Services

- **Key Data Protection Practices**: Best practices would include the implementation of end-to-end encryption using protocols such as AES-256, RSA, or ECC, especially for sensitive user data.
- **Implementing Robust Security Measures**: Conduct frequent and thorough security audits and penetration testing to identify and address vulnerabilities before they can be exploited.
- **Educating Users and Employees**: Implementing robust IAM policies, including the use of multi-factor authentication and least privilege principles, to control access to sensitive systems and data.

The Role of Regulatory Bodies in Data Security

Ensuring Compliance and Protection

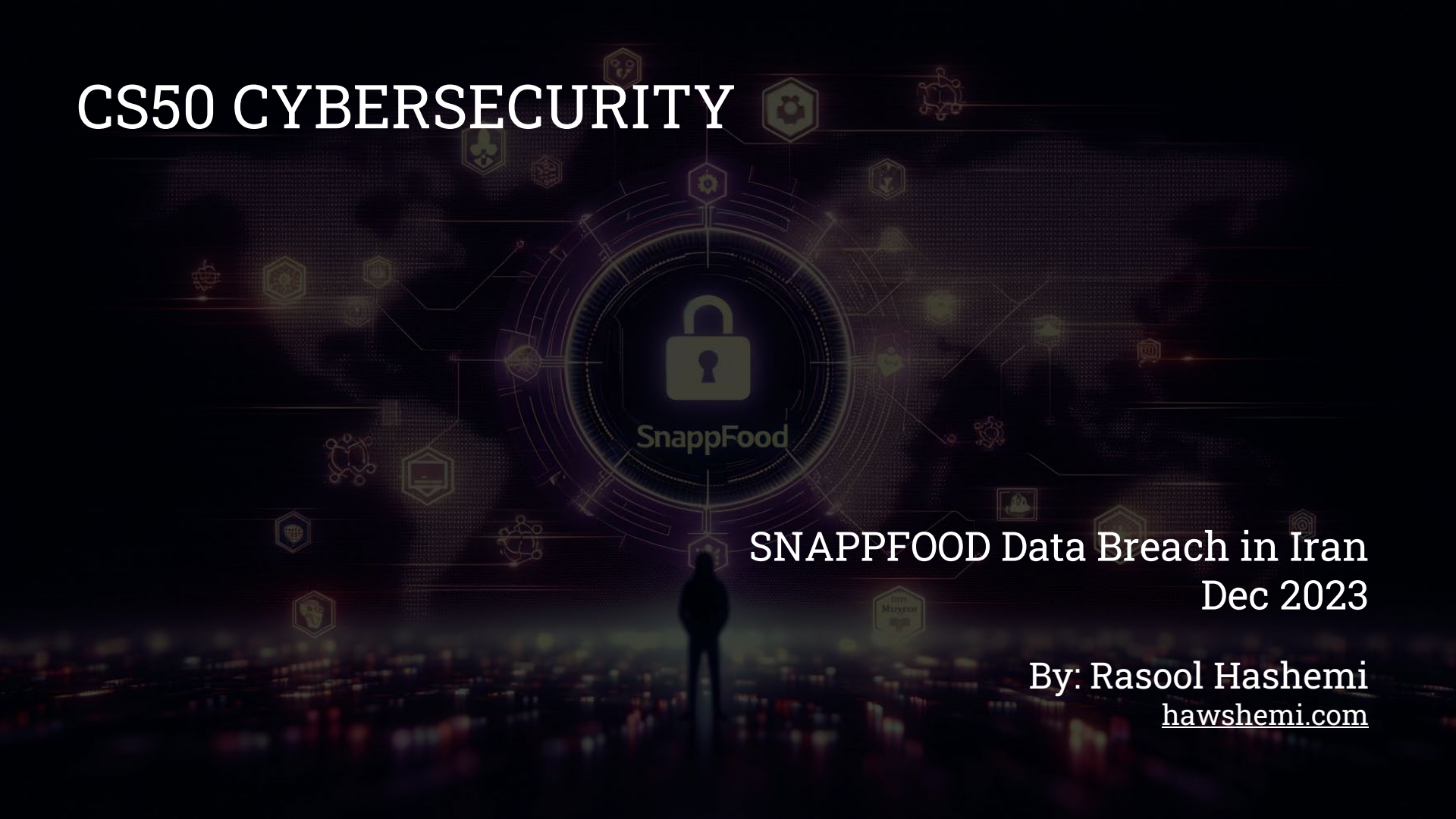
- **Regulatory Oversight**: In the context of the Snappfood hack, regulatory bodies may enforce compliance with data protection laws like GDPR, which mandates strict data protection and privacy measures.
- **Compliance and Enforcement**: Regulatory bodies may require mandatory incident reporting within a stipulated timeframe, along with adherence to specific compliance measures post-breach.
- **Impact of Regulations on Snappfood**: Introducing regular compliance audits, certifications, and mandatory cybersecurity training as part of the regulatory framework to ensure ongoing adherence to data protection standards.

Future Implications and Preventive Strategies

Mitigating Risks in the Digital Age

- **Proactive Threat Intelligence and Monitoring**: Emphasizing the need for proactive cybersecurity measures, including real-time threat intelligence, monitoring, and the use of SIEM (Security Information and Event Management) systems.
- **Adoption of Zero Trust Architecture**: Moving towards a Zero Trust security model, which assumes no implicit trust and verifies every request as though it originates from an open network.
- **Investment in AI and Machine Learning for Security:** Investing in AI and machine learning technologies for predictive analytics and advanced threat detection, enhancing the ability to identify and respond to cyber threats swiftly.

CS50 CYBERSECURITY



SNAPPFOOD Data Breach in Iran
Dec 2023

By: Rasool Hashemi
hawshemi.com