MIT World Peace University

Attack Research and Documentation
Fourth Year B. Tech, Semester 8

Incidence Report for an Incident

Lab Assignment 5
Incidence Report

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 15

April 3, 2025

Contents

Chapter 1

Yahoo Data Breach (2013-2014)

1.1 Executive Summary

- **Date of Incident:** August 2013 (first breach); November/December 2014 (second breach)
- **Reported By:** Yahoo, disclosed publicly in September 2016
- **Affected Systems:** Yahoo user account database and servers
- **Impact:** 3 billion accounts affected in 2013, 500 million in 2014; exposure of sensitive user data
- **Status:** Resolved, with legal settlements and enhanced security measures post-Verizon acquisition

1.2 Incident Details

1.2.1 Detection & Analysis

- **Date & Time of Detection:** Likely in 2016, exact time unspecified
- **Detection Method:** Unclear; possibly identified during security audits
- **Attack Vector:**
  - 2013: Unknown
  - 2014: Exploitation of vulnerabilities in cookie creation for unauthorized access
- **Indicators of Compromise (IoCs):** Circulation of stolen data on underground forums
- **Root Cause:** Inadequate security practices and funding; possible state-sponsored involvement (suspected Russian hackers)

1.3 Containment, Eradication & Recovery

- **Containment Measures:** Required all users (affected and unaffected) to change passwords
- **Eradication Steps:** Likely included patching system vulnerabilities; details not widely documented

- **Recovery Actions:**
  - Increased cybersecurity spending post-Verizon acquisition
  - Verizon committed $306 million (2019-2022) to security enhancements
  - IT staff expanded fourfold to address ongoing risks

1.4 Impact Assessment

- **Number of Affected Customers:** 3 billion in 2013; 500 million in 2014
- **Data Exposed:**
  - Names, email addresses, phone numbers, birth dates
  - Encrypted passwords
  - Security questions in some cases
- **Regulatory Compliance Impact:**
  - SEC fines for delayed disclosure
  - Shared legal liabilities with Verizon post-acquisition
- **Financial Impact:**
  - $350 million reduction in Yahoo's sale price to Verizon
  - $117.5 million settlement for affected users

1.5 Reporting & Notification

- **Internal Report:** Breach disclosed by Yahoo in September 2016
- **Regulatory Authorities:** Reported to SEC, resulting in fines
- **Customers:** Notified post-disclosure; advised to change passwords
- **Third-Party Vendors:** Verizon shared liabilities and took over security enhancements

1.6 Lessons Learned & Recommendations

- Importance of **timely disclosure** to regulators and the public
- Need for **robust cybersecurity funding** and proactive security measures
- Implementation of **regular security audits** to detect vulnerabilities early
- Strengthening **password security policies** and multi-factor authentication
- Organizations should **invest in advanced detection systems** and security awareness programs

Chapter 2

Facebook Data Leak (2019)

2.1 Executive Summary

- **Date of Incident:** Before August 2019
- **Reported By:** Facebook, initially disclosed in 2019, with further details emerging in April 2021
- **Affected Systems:** Contact importer feature
- **Impact:** 533 million users affected globally, exposing personal data
- **Status:** Resolved, vulnerability patched by September 2019

2.2 Incident Details

2.2.1 Detection & Analysis

- **Date & Time of Detection:** Likely in 2019, exact time unspecified
- **Detection Method:** Security audits, identification of abnormal scraping activity
- **Attack Vector:** Exploitation of the contact importer tool for automated data scraping
- **Indicators of Compromise (IoCs):** Stolen dataset appeared on dark web in April 2021
- **Root Cause:** Inadequate security measures in the contact importer feature, allowing large-scale automated data collection

2.3 Containment, Eradication & Recovery

- **Containment Measures:**
  - Patched the vulnerability by September 2019
  - Modified the contact importer feature to block automated software uploads
- **Eradication Steps:** Confirmed issue was resolved; ensured scraping method could no longer be exploited

- **Recovery Actions:**
  - Ongoing monitoring for scraping behaviors
  - Efforts to remove leaked data from online sources
  - Recommendations for users to update privacy settings on Facebook

2.4 Impact Assessment

- **Number of Affected Customers:** 533 million users across 106 countries
- **Data Exposed:**
  - Phone numbers, full names, locations, birthdates, Facebook IDs
  - In some cases, email addresses
- **Regulatory Compliance Impact:** 277 million Dollar fine by Irish Data Protection Commission (DPC) in 2022
- **Financial Impact:** At least 277 million Dollars in regulatory fines, with additional costs in legal and security measures

2.5 Reporting & Notification

- **Internal Report:** Disclosed internally in 2019
- **Regulatory Authorities:** Notified later, resulting in a 277 million Dollar fine under GDPR
- **Customers:** No individual notifications issued, raising transparency concerns
- **Third-Party Vendors:** Regulatory oversight shared with the FTC and Irish DPC

2.6 Lessons Learned & Recommendations

- Strengthening security for platform features that handle user data
- Enhancing automated detection systems to prevent large-scale data scraping
- Ensuring compliance with GDPR and other global data protection regulations
- Implementing proactive disclosure and notification practices to maintain user trust
- Conducting regular security audits to identify and mitigate potential vulnerabilities

2.6.1 Glossary

The following terms are defined to provide clarity on technical concepts referenced in the reports for the Yahoo Data Breach (2013-2014) and the Facebook Data Leak (2019).

- **Attack Vector**: The method or pathway used by an attacker to gain unauthorized access to systems or data (e.g., cookie exploitation in Yahoo 2014, contact importer in Facebook 2019).
- **Containment Measures**: Immediate actions taken to limit the spread or impact of a breach (e.g., password resets for Yahoo, patching for Facebook).
- **Data Scraping**: The automated extraction of data from a website or application, often maliciously (e.g., Facebook's contact importer exploit).
- **Indicators of Compromise (IoCs)**: Evidence or clues that a security breach has occurred (e.g., stolen data on the dark web for both breaches).
- **Regulatory Compliance**: Adherence to laws and regulations governing data protection (e.g., GDPR for Facebook, SEC requirements for Yahoo).
- **Root Cause**: The underlying reason or vulnerability that allowed the breach to occur (e.g., inadequate security practices in Yahoo, feature misuse in Facebook).

Bibliography

[1] Wikipedia, “Yahoo! Data Breaches,” https://en.wikipedia.org/wiki/Yahoo_data_breaches, Accessed April 03, 2025.

[2] The New York Times, “All 3 Billion Yahoo Accounts Affected by 2013 Attack,” https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html, Published October 03, 2017, Accessed April 03, 2025.

[3] Reuters, “Yahoo says all three billion accounts hacked in 2013 data theft,” https://www.reuters.com/article/technology/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82NV/, Published October 03, 2017, Accessed April 03, 2025.

[4] Medium, “Yahoo Data Breach: An In-Depth Analysis,” https://shellmates.medium.com/yahoo-data-breach-an-in-depth-analysis-of-one-of-the-most-sig Accessed April 03, 2025.

[5] NPR, “After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users,” https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users, Published April 09, 2021, Accessed April 03, 2025.

[6] Facebook Blog, “Facts on News Reports About Facebook Data,” https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/, Published April 2021, Accessed April 03, 2025.

[7] NPR, “Facebook to Pay $5 Billion to Settle FTC Privacy Case,” https://www.npr.org/2019/07/24/741282397/facebook-to-pay-5-billion-to-settle-ftc-privacy-case, Published July 24, 2019, Accessed April 03, 2025.

[8] NordVPN, “Facebook Data Breaches: Investigating Top Data Leaks,” https://nordvpn.com/blog/facebook-data-breach/, Accessed April 03, 2025.

[9] Have I Been Pwned, X Post, “65% of the Facebook data was already in previous leaks,” https://x.com/haveibeenpwned/status/1378554902100635659?s=20, Published April 03, 2021, Accessed April 03, 2025.