YAHOO DATA BREACHES:

CASE STUDY

Sowmyashree Bevur Mandya Venkatesh

Foundations of Information Assurance

22nd April 2021

ABSTRACT

Yahoo! is a web services provider, acquired by Verizon Communications in 2017 was a victim of one of the biggest data breaches in 2013 and 2014. The incident that happened in 2014 was concluded to be a state-sponsored attack and indicted 4 people, 2 out of which were Russian Intelligence Officers while the 2013 incident by an unauthorized third-party.

The first breach was publicly announced in September 2016 which exposed 500 million user accounts in 2014. The investigation of this incident led to the discovery of an earlier breach happened in 2013 that was initially assumed to have exposed 1 billion user accounts and announced about in December 2016. Later Yahoo confirmed in 2017 that all its user accounts were exposed due to these breaches.

The following sections of the paper focus on the detailed description of the attacks and the business, social and financial impact it had on the company.

INTRODUCTION

Yahoo was a victim of two data breaches that compromised every single user account it held back in 2013 (approx. 3 billion). The compromised data contained PII like name, email, hashed password, security questions and answers however associated financial details of the users were not compromised. Not only the registered accounts were compromised, also the accounts people had in Flickr, BT, Sky, and Fantasy due the merger/acquisition made by Yahoo!. Although Yahoo! declared that they securely stored the passwords decreasing the chances of them being recovered, significant number of passwords were known to be stored using a weak encryption algorithm that can be easily cracked. If the users had reused the compromised passwords elsewhere and/or other sites were linked to this account, even those were found to be affected due to these attacks.

The attack that happened in 2014 was a state-sponsored and four people were indicted for this crime. Two Russian agents named Dmitry Dokuchaev and Igor Sushchin hired the hackers Aleksey Belan and Karim Baratov to target specific personnel working for Russian government, US government and Swiss bitcoin wallet company. This attack compromised 500,000 user accounts and 6,500 accounts were of which was accessed.

DESCRIPTION OF THE BREACH

Yahoo's security team and senior executives were aware that copy of their data backup was stolen back in 2014 and they believed it to have exposed what they thought of 26 user accounts. They even disclosed in their filing that they took remedial actions to secure these accounts and implemented new security features to protect against further attacks.

Upon investigation of the incident by the Federal Bureau of Investigation for nearly two years, the actual depth and implication of the attack was revealed. About 500,000 user account was exposed as result. The FBI said the attack started with email spear phishing attack against the employers of the company. Using the compromised employee's account, the hacker was able to get his hands on the user database and account management tool. The user database held information about the user's personal details like names, phone numbers, security questions and answers (encrypted and unencrypted), password recovery emails and a unique cryptographic value called as Nonces. For persistent access to this database, he installed a backdoor on the Yahoo server. He then later copied a copy of the database onto his personal computer. The state-sponsored hackers then used the recovery emails to target specific user accounts and the nonces to forge access cookies to login without having to require a password.

While investigating this attack, they discovered another attack that took place in 2013 when they found a chunk of their data being sold on the Dark Web. However, Yahoo disclosed that they are unable to indict the attackers and that it was done by "unauthorized third party". They found that this data was bought by 3 entities (2 were spammers and 1 was alleged to be a spy). They soon discovered that all their 3 billion user data was compromised. Though they claimed that most of the passwords of the users were securely stored using bcrypt encryption algorithm, significant user's password was stored using a weaker encryption called MD5.

MITR ATT&CK MAPPING

Reconnaissance:

- Gather Victim Identity Information
- Gather Victim Organization Information

Resource Development

- Compromise accounts
- Develop capabilities

Initial Access

- Phishing
- Compromise accounts

Execution

- User Execution

Persistence

- Event-triggered Execution (Accessibility feature: backdoor)

Credential Access

- Steal Web Session Cookies

Collection

- Data from network shared drive

RESPONSE, RECOVERY ACTIONS AND IMPACT

Yahoo disclosed the data breach incident in September 2016, two years later than it originally occurred. Since the security team knew about the possible theft back in early 2014, further investigations and analysis of the incident in the early stages of detection could have prevented the impact much significantly. Yahoo identified the technique used to be forged cookies and invalidated the use of them. The security questions answers used to reset the password was previously stored unencrypted and these were invalidated for further usage. Yahoo notified and urged its user to reset their passwords.

Yahoo was in the middle of merger with Verizon Communications amidst this. It presented false spreadsheets claiming it was aware of only four minor data breaches and only disclosed about these major breach two days prior to the public disclosure. As a result, Yahoo lost $350 million USD in this merger. And its stock price dropped by 3% the after the announcement. Yahoo was fined a penalty of $35 million for failing to disclose known cyber incidents in its fillings another 11 million towards its legal cost. And was made to pay settlement amounting to $117,500,500 according to the final judgement made on July 22, 2020. The lack of security liability insurance costed them 16 million USD towards incident expenses.

The FBI indicted four people including two Russia Federal Security (FSB) workers and prosecuted one who later pled guilty. He was sentenced to 5 years in prison and was fined with $2.25 million USD in May 2018.

The huge loss associated is not just because the breach happened, it was more about how the company handled it and the security mechanisms in place prior to it. Ensuring that a good security plan is in place and is revised regularly is important for companies. Since the attack was

initiated with the phishing attack, the employees must be regularly trained to ensure that they do not become a victim to such social engineering attacks. In addition, they can install phishing filter on email gateways. They need to regulate and remove (wherever necessary) the access rights of the employees to company resources from time to time. Promote/enforce stronger password policy usage among employees and users is another good practice. It was revealed that the company used MD5 hashing algorithm for significant number of users if not for majority. This needs to be replaced bcrypt for every user account. One of the major comments received by Yahoo was that the delay in response and negligence shown in not investigating and securing the infrastructure better when they were aware of the breach initially. Well-trained Incident Response team is required to handle such incidents better. Investing in cyber liability insurance would help with financial impact of such attacks in the future.

CONCLUSION

The IT industry witnessed one of the biggest Data Breaches ever. It was clear that these breaches' impact could have been significantly reduced if not prevented entirely had the company invested more funds annually to improve the security of its infrastructure (based on the claim made by CISO Alex Stamos on being denied the grant to implement stronger security measures). The result of these negligence in handling and reporting the incidents costed Yahoo not only a huge financial lose but also its reputation and trust it holds amongst the users and additional 3rd party companies globally. However, post these incidents the now owner Verizon Communications have invested nearly 306 million USD towards security improvement which is commendable. These incidents can serve as an example for enterprises the need to prioritize security as such attempts will continue to be prevalent in future.

REFERENCES

"Yahoo! Data breaches", Wikipedia. https://en.wikipedia.org/wiki/Yahoo!_data_breaches

Marty Williams, "Inside the Russian Hack of Yahoo: How they did it", CSO Online. https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html

"Analysis of the Yahoo! Data Breaches", Uk Essays. https://www.ukessays.com/essays/computer-science/analysis-of-the-yahoo-data-breaches.php

United States District Court Northern District of California San Jose Division Case No. 5:16-MD-02752-LHK "Yahoo! Inc. Customer Data Security Breach Litigation Settlement", Heffler Claims Group. https://yahoodatabreachsettlement.com/en

Edward J. McAndrew, "The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far)", The National Law Review. https://www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far

MITR ATT&CK, https://attack.mitre.org/