Yahoo Data Breach Attack Case Study

Company/Affected Parties: Yahoo!

Prepared By:
Cynara Justine

ttack ategory: hishing

Description of the Attack Category to teach the reviewer about the attack.

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site. Phishing is an example of social engineering techniques used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators. Phishing was the top initial infection vectors seen in X-Force IRIS engagements in 2019 (31 percent).

Research (Sources):

- Wikipedia
- X-Force Threat Intelligence Index 2020
- Internet
- Blogs

npany description:

oo! is an American web services provider founded by Jerry Yang and David Filo in January 1994 and was incorporate
March 2, 1995. **Yahoo** was one of the pioneers of the early Internet era in the 1990s. It provides/provided a Web port
rch engine and related services including advertising, online mapping, video sharing, fantasy sports, and its social
dia website. Once one of the largest Internet companies, Yahoo slowly declined starting in the late 2000s, and in 20
zon Communications acquired most of Yahoo's Internet business for $4.48 billion,excluding its stakes in Alibaba Gro
Yahoo! Japan, which were transferred to Yahoo's successor company Altaba.Despite its decline from prominence,
oo domain websites are still among the most popular, ranking 10th in the world according to the Alexa rankings as
ober 2019

nmary of the security incident and data breach

oo announced in September 2016 that in 2014 it had been the victim of what would be the biggest data breach in
ory. The attackers, which the company believed we "state-sponsored actors," compromised the real names, email
resses, dates of birth and telephone numbers of 500 million users. Yahoo claimed that most of the compromised
swords were hashed.

n in December 2016, Yahoo disclosed another breach from 2013 by a different attacker that compromised the name
es of birth, email addresses and passwords, and security questions and answers of 1 billion user accounts. Yahoo
sed that estimate in October 2017 to include all of its 3 billion user accounts.

timing of the original breach announcement was bad, as Yahoo was in the process of being acquired by Verizon,
ch eventually paid $4.48 billion for Yahoo's core internet business. The breaches knocked an estimated $350 million
value of the company

meline

o Attack

1 The hack began with a spear-phishing email sent in early 2014 to a Yahoo company employee. The attacker, Aleksey Belan, installed a backdoor on a Yahoo server that would allow him access

2 In December 2014, the attacker stole a backup copy of Yahoo's user database and transferred it to his own computer

3 Yahoo first approached the FBI in 2014, it went with worries that 26 accou had been targeted by hackers

4 In 2015 and 2016, the hackers used stolen cryptographic values called "nonce generate access cookies through a script installed on a Yahoo server which g them free access to a user email account without the need for a password

5 In August 2016, the full scale of the breach began to become apparent and the FBI investigation significantly stepped up

6 In December 2016, Yahoo went public with details of the breach and advised hundreds of millions of users to change their passwords.

ulnerabilities

Overall Summary:

The 4 important vulnerabilities in the case of Yahoo breach were:

1. Centralized storage of sensitive account information
2. Centralized access tokens
3. Administrator access
4. Web application vulnerability

Vulnerability #1

Centralized storage of sensitive account information: The Yahoo UDB is a centralized database of all users' account information that was stored on Yahoo's servers. While passwords were encrypted, a lot of other personal information was not.

Vulnerability #2

Centralized access tokens: Whe a user logs in to Yahoo, the serve sends the user's browser a token based on a nonce, which is then stored locally on the browser. Th corresponding nonce is stored in the UDB. When a user connects t Yahoo later, their token is sent to the server and, if the token is consistent with the nonce in the UDB, the user does not have to l in again.

Vulnerability #3

Administrator access: The attackers got into Yahoo's centralized administrative program, the Account Management Tool. This allowed them to reset a user's password and then, using a minted nonce, connect to Yahoo and change it, thus taking control of the user's account.

Vulnerability #4

Web application vulnerability: A report indicated that the "dat is in SQL format, meaning it was server-side dump", and therefor the hackers who breached Yaho "likely did so by exploiting a web application vulnerability to gain access to the user database".

Costs

3 billion user accounts were compromised

The breaches knocked an estimated $350 million off the value of the company

Yahoo has been fined ($35 million) by the Securities and Exchange Commission for filing statements that failed to disclose known data breaches.

Attorneys' fees up to $35 million

Estimated cost of settlement is $117.5 million

Prevention

- Employee awareness education and training
- Early detection
- Full Encryption
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Critical patches (eg: this could have avoided the web application vulnerability)