2014 Yahoo data breach

Background

The Internet service company Yahoo was subject to the largest data breach on record. Two major data breaches of user account data to hackers were revealed during the second half of 2016

1. **August 2013 breach**
2. **Late 2014 breach**

We are going to talk about the Late 2014 breah today

Background

In 2014, hackers directly targeted Yahoo's user database, affecting about 500 million people. The cybercriminals reportedly got account details such as people's names, email addresses, passwords, phone numbers and birthdays.

Attack

Passwords hashed in two ways:

1. bcrypt hashing algorithm - difficult to crack
2. MD5 algorithm - can be broken quickly

Victims:

1. Current Yahoo users
2. User accounts that have indirect connect to Yahoo

Who did this and how?

Yahoo believes the breach was committed by "state-sponsored" hackers.

Russia? We don’t know.

Data breach had been conducted through a cookie-based attack that allowed hackers to authenticate as any other users without their passwords.

Same as August 2013 breach.

What we learned from the attack?

1. Cybercrime as a service is growing substantially.
2. Nation-state cyber actors are using criminal hackers as proxies to attack private entities and individuals.
3. Compromises of one online account (such as a Yahoo account) often lead to compromises of other accounts tied to targeted individuals.