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, and we are going to talk about the first data breach today. The first announced breach had occurred sometime in late 2014, and affected over 500 million Yahoo user accounts. The late 2014 breach is considered the largest discovered cyber attack in the history of the Internet. Specific details of material taken include names, email addresses, telephone numbers, encrypted or unencrypted security questions and answers, dates of birth, and hashed passwords. Further, Yahoo reported that the late 2014 breach likely used manufactured web cookies to falsify login credentials, allowing hackers to gain access to any account without a password.

Attack:
Security experts noted that the majority of Yahoo's passwords used the bcrypt hashing algorithm, which is considered difficult to crack, with the rest using the older MD5 algorithm, which can be broken rather quickly.

Such information, especially security questions and answers, could help hackers break into victims' other online accounts. Computer security experts cautioned that the incident could have far-reaching consequences involving privacy, potentially including finance and banking as well as personal information, including information pulled from any other accounts that can be hacked with the gained account data. Experts also noted that not only current Yahoo users were affected but also millions of people with Flickr, Sky and/or BT accounts who do not realize that they indirectly have a Yahoo account as a result of past acquisitions and agreements made with Yahoo.

Yahoo reported the breach to the public on September 22, 2016 and it believes the breach was committed by "state-sponsored" hackers, but did not name any country(Russia). Yahoo affirmed the hacker was no longer in their systems and that the company was fully cooperating with law enforcement.

Yahoo believed the data breach had been conducted through a cookie-based attack that allowed hackers to authenticate as any other users without their passwords. Yahoo and its outside security analysts confirmed this was the method of intrusion in their December 2016 announcement of the August 2013 data breach (which is a previous attack), and had invalidated all previous cookies to eliminate this route at last.

Lessons learned from this 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. In fact, the Yahoo fact pattern shows that the Russian intelligence services have been doing so since at least 2014.
3. Compromises of one online account (such as a Yahoo account) often lead to compromises of other accounts tied to targeted individuals. Credential sharing between accounts and the failure to employ multi-factor authentication makes these compromises very easy to execute.

Sources:

- https://www.cshub.com/attacks/articles/incident-of-the-week-multiple-yahoo-data-breaches-across-4-years-result-in-a-1175-million-settlement#:~:text=In%202014%2C%20hackers%20directly%20targeted,passwords%2C%20phone%20numbers%20and%20birthdays.
- https://www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far
- https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-hackers-stole-data-from-500-million-accounts-in-2014-idUSKCN11S16P
- https://en.wikipedia.org/wiki/Yahoo!_data_breaches
- https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html