Yahoo! Data Breaches

Amanda Robinson and Matt Duff

What Happened?

August 2013: 3 billion users leaked

Late 2014: 500 million users leaked

December 2016: Yahoo! announces the 500 million user leak.

September 2016: Yahoo! announces 1 billion users leaked, later updates to all 3 billion users

Who Was Responsible?

Who else but Russian Hackers!

Marissa Mayer, Yahoo CEO, said in testimony: “We now know that Russian intelligence officers and state-sponsored hackers were responsible for highly complex and sophisticated attacks on Yahoo’s systems.”

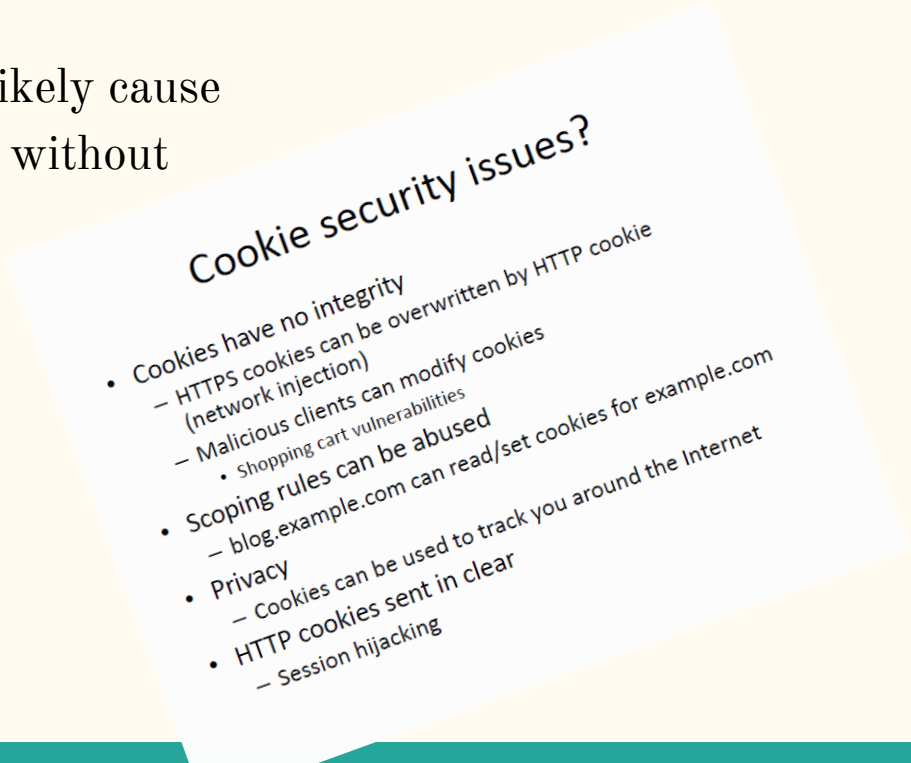
Aleksey Belan: Latvian/Russian Hacker, one of FBI’s most wanted

$100,000 reward for information leading to arrest

The Attack Vector?

For the 500 million user leak:

- Web cookie falsification is the most likely cause
- Allowed hackers to log into accounts without passwords
- Sound familiar?



The Attack Vector?

The current most likely order of events for the 3 billion user leak:

1. Spear phishing attack targeting specific Yahoo Employees
2. Hacker(s) found Yahoo's user database and the Account Management Tool (used for editing the database)
3. Pulled entire user database including: names, phone numbers, password challenge questions and answers, password recovery emails and a cryptographic value unique to each account
4. Used this information to target specific users

What Did We Learn?

- Side channel attacks are incredibly effective
- State sponsored attacks are a very real threat

What Did Yahoo Learn?

- Lost $350M during Verizon buyout
- Hired a Chief of Security Officer, Alex Stamos
- Reportedly have underfunded security portion of company
- Took over a year after announcement to force password changes
- So, essentially nothing

Bibliography

https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html

https://techcrunch.com/2017/11/08/yahoo-senate-commerce-hearing-russia-3-billion-hack/

https://en.wikipedia.org/wiki/Yahoo!_data_breaches

https://www.wired.com/2016/12/yahoo-hack-billion-users/

https://www.washingtonpost.com/news/the-switch/wp/2016/11/10/yahoo-discovered-hack-leading-to-major-data-breach-two-years-before-it-was-disclosed/?utm_term=.45702e0ac103

https://www.fbi.gov/wanted/cyber/alexsey-belan