Яхю! Взломанный 2016
A Big Yikes @ Yahoo

Rohit Mareddy, Ari Margolin, Robert Hall, Tory Lipsey, & Tiffannie MacDonald

Yahoo has had a years-long history of data breaches:

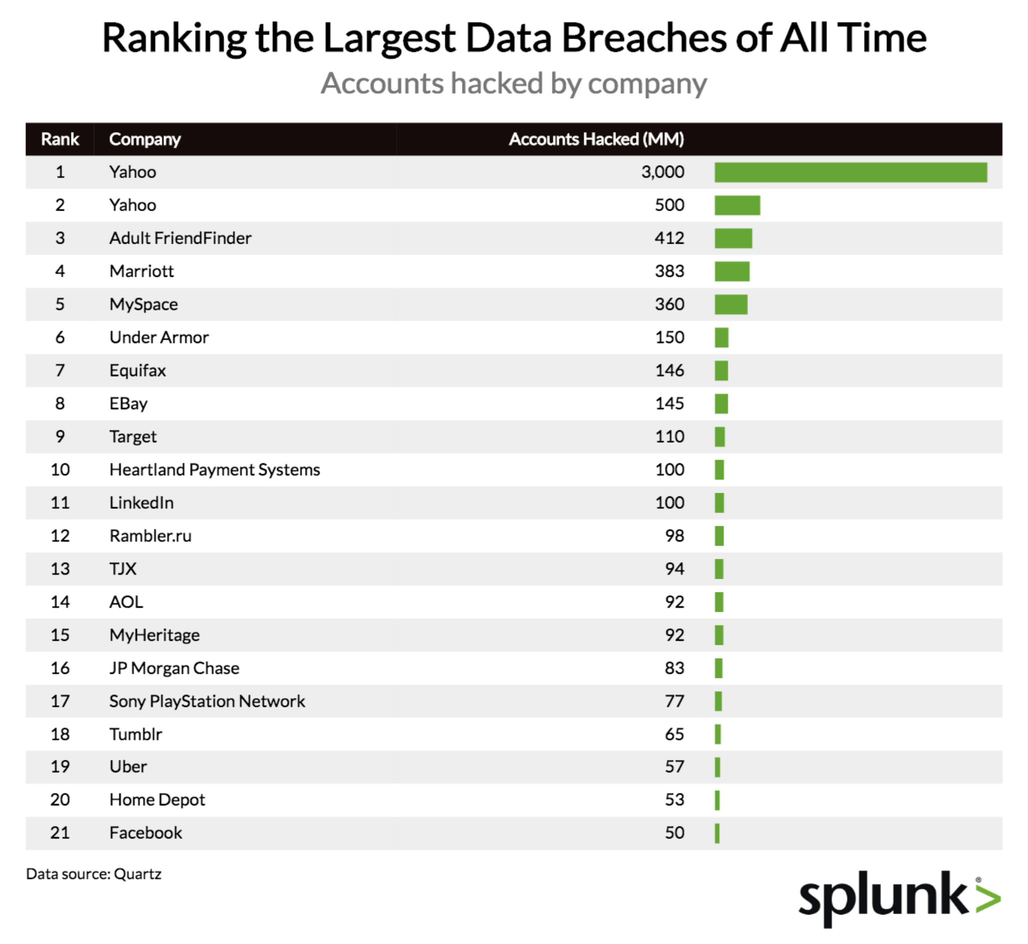
July 2012: E-mail addresses and encrypted passwords stolen from Yahoo Voices.

2013: Phishing attacks.

Jan 2014: Customer e-mail account details hacked.

Sept. 22, 2016: 500 million user accounts hacked.

Dec. 14, 2016: 1 billion user accounts breached by Russian-sponsored hackers over 2-year period.



Ranking the Largest Data Breaches of All Time

Accounts hacked by company

Rank	Company	Accounts Hacked (MM)
1	Yahoo	3,000
2	Yahoo	500
3	Adult FriendFinder	412
4	Marriott	383
5	MySpace	360
6	Under Armor	150
7	Equifax	146
8	EBay	145
9	Target	110
10	Heartland Payment Systems	100
11	LinkedIn	100
12	Rambler.ru	98
13	TJX	94
14	AOL	92
15	MyHeritage	92
16	JP Morgan Chase	83
17	Sony PlayStation Network	77
18	Tumblr	65
19	Uber	57
20	Home Depot	53
21	Facebook	50

Data source: Quartz

How it was done

2013 Data Breach (Discovered 2016)

2014 Data Breach (Discovered 2016)

2013 Data Breach

Russian hacking collective offered up the account information for sale.

- This information was bought by 3 entities, two of the entities were ‘spammers’ and other appears to be interested in espionage purposes.

Still unclear how hackers were able to steal 1 billion Yahoo accounts.

Yahoo was able to trace the sale of 1 billion accounts for a quarter million dollars.

- Traced with the help of law enforcement and outside security firm

Due to the nature of the breach, authorities believe that the 2013 hack was a state-sponsored incident

2014 Data Breach

Additional 500 million accounts were hacked.

A Latvian hacker gained access to Yahoo’s User Database and account management tool.

- The hacker used spear-phishing campaign that specifically targeted Yahoo employees.
- Once inside the user database, hacker installed a backdoor on a Yahoo server where he later stole a backup copy of the user database onto his personal computer

On March of 2017, the Department of Justice indicted four individuals for the hack. Two of the individuals indicted were Russian intelligence officers.

Once hackers identified accounts of interest, the hackers used stolen cryptographic values, “nonces”, to generate access cookies through a script that was installed on a Yahoo server

- Authorities said the stolen information was used to spy on a range of targets in the US.

Technical Technics

1. Session Hijacking
2. Spear-phishing / DNS Spoofing

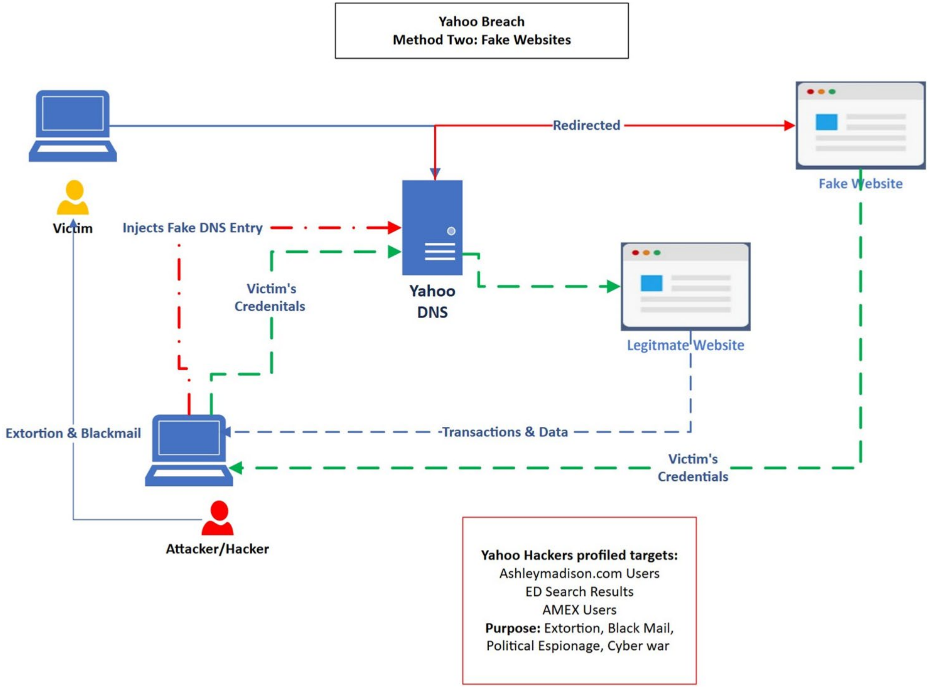
Method One: Spear-phishing, Fake Websites & DNS Spoofing

Hackers used spear-phishing to gain access to Yahoo’s servers.

The Hackers targeted several Yahoo employees unaware that one click on phishing email that would result in a breach of 1 billion users by 2016.

The hackers through several methods were able to gain access to the account management too, which didn't allow for simple text searches of usernames, so instead the hackers turned to recovery email addresses. Sometimes they were able to identify targets based on their recovery email address, which the hacker used to extort several of their victims.

There was a strategy behind the targets they selected for extortion. This ultimately gave the hackers influence via political espionage all of which was financially backed by the Russian Government. Source: Northern District Court of California.



Yahoo Breach
Method Two: Fake Websites

Yahoo Hackers profiled targets:
Ashleymadison.com Users
ED Search Results
AMEX Users
Purpose: Extortion, Black Mail, Political Espionage, Cyber war

Method Two: Cookie/Session Hijacking

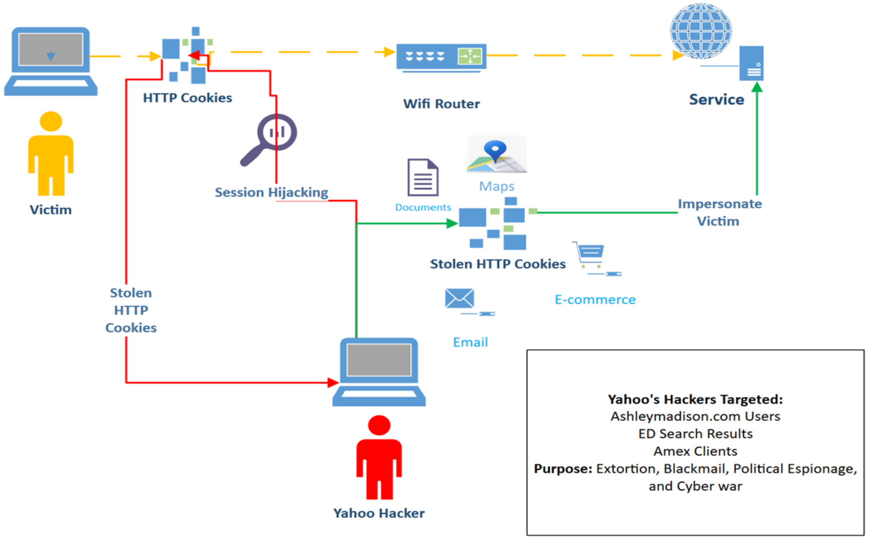
Cookies have many benefits, such as remembering your password each time you visit.

Cookies can also remember what happened last in a series of screens leading to purchases and authentication to to other sites external to Yahoo's network..

When cookies record too much sensitive information about you, they become spyware. Cookies are not Trojan horses because they are legitimately generated by the victim. This breadcrumb trail allowed hackers access other sensitive data outside of Yahoo's network that was used for blackmail.

These cookies, which were generated many times throughout 2014 - 2016, gave hackers free access to influence the lives of their victim.

Yahoo Breach
Method One: Cookie Hijacking



Yahoo's Hackers Targeted:
Ashleymadison.com Users
ED Search Results
Amex Clients
Purpose: Extortion, Blackmail, Political Espionage, and Cyber war

Fallout

1. VERIZON DEAL
2. SETTLEMENT
3. LONG-TERM RAMIFICATIONS
4. HOW TO AVOID

Verizon Deal

In July 2016, Verizon announced plans to buy Yahoo for about $4.8 billion.

Following the breaches going public, Verizon investigated the situation to decide on how they should proceed.

Following their investigations, the offer was lowered by $350 million.

The Final sale price was $4.48 billion

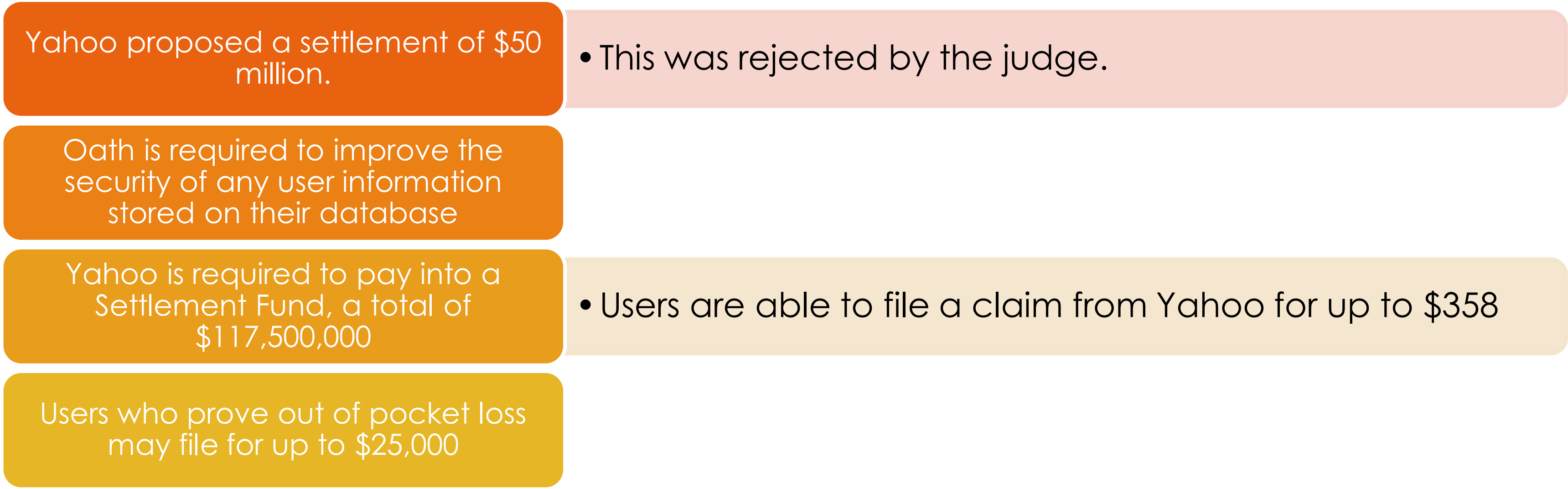
Verizon Deal Pt II

With the new agreement, "Yahoo and Verizon will split cash liabilities… Yahoo, however will continue to be responsible for liabilities from shareholder lawsuits and SEC investigations." (Athavaley,/Shepardson, 2017)

Yahoo CEO Marissa Mayer resigned, receiving $23 million in the deal

Yahoo was combined with AOL brands and rebranded as Oath (Kharpal, 2017)

Settlement



- Yahoo proposed a settlement of $50 million.
  - This was rejected by the judge.
- Oath is required to improve the security of any user information stored on their database
- Yahoo is required to pay into a Settlement Fund, a total of $117,500,000
  - Users are able to file a claim from Yahoo for up to $358
- Users who prove out of pocket loss may file for up to $25,000

Long-Term Ramifications

Companies will need to be more diligent in identifying and disclosing data breaches to their users and their shareholders

Companies cannot spare expenses when it comes to security. Outdated security will not be acceptable when a data has the information of 3 billion user accounts

There will be a larger spotlight on these companies going forward by the government and other investigative agencies in order to protect their users

How to avoid

If you don't want attackers to tear you or your company "limb by limb"

WATCH OUT FOR PHISHING EMAILS!

- Don't open emails from suspicious emails
  - Don't recognize the sender?
  - The sender has a weird address
    - Don't click any links!
- If an unknown email address emails you asking for information, don't respond providing the wanted information!
- When you're at work – DON'T CLICK ON ERECTILE DYSFUNCTION WEBSITES!

Цитаты

Athavaley, A., & Shepardson, D. (2017, February 21). Verizon, Yahoo agree to lowered $4.48 billion deal Following cyber attacks. Retrieved March, 2020, from https://www.reuters.com/article/us-yahoo-m-a-verizon/verizon-yahoo-agree-to-lowered-4-48-billion-deal-following-cyber-attacks-idUSKBN1601EK

Condliffe, J. (2016, December 15). A brief history of Yahoo hacks. Retrieved March 1, 2020, from https://www.technologyreview.com/s/603157/a-history-of-yahoo-hacks/

Kharpal, A. (2017, June 13). Verizon completes its $4.48 billion acquisition of Yahoo; Marissa Mayer leaves with $23 million. Retrieved March, 2020, from https://www.cnbc.com/2017/06/13/verizon-completes-yahoo-acquisition-marissa-mayer-resigns.html

Rivero, N. (2018, November 30). The biggest data breaches of all time, ranked. Retrieved March 1, 2020, from https://qz.com/1480809/the-biggest-data-breaches-of-all-time-ranked/

Yahoo! Inc. Customer Data Security Breach Litigation Settlement. (2019). Retrieved March, 2020, from https://yahoodatabreachsettlement.com/

Williams, Martyn. “Inside the Russian Hack of Yahoo: How They Did It.” CSO Online, CSO, 4 Oct. 2017, www.csoonline.com/article/3180762/data-breach/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

Boyle, R. J., & Panko, R. R. (2013). *Corporate computer security: Randall J. Boyle, Raymond R. Panko*. Boston: Pearson.

U.S v DMITRY DOKUCHAEV, v ALEXSEY BELAN, v IGOR SUSHCHIN, v and KARIM BARATOV Et Al Indictment (2017) https://www.justice.gov

Вопросы ?