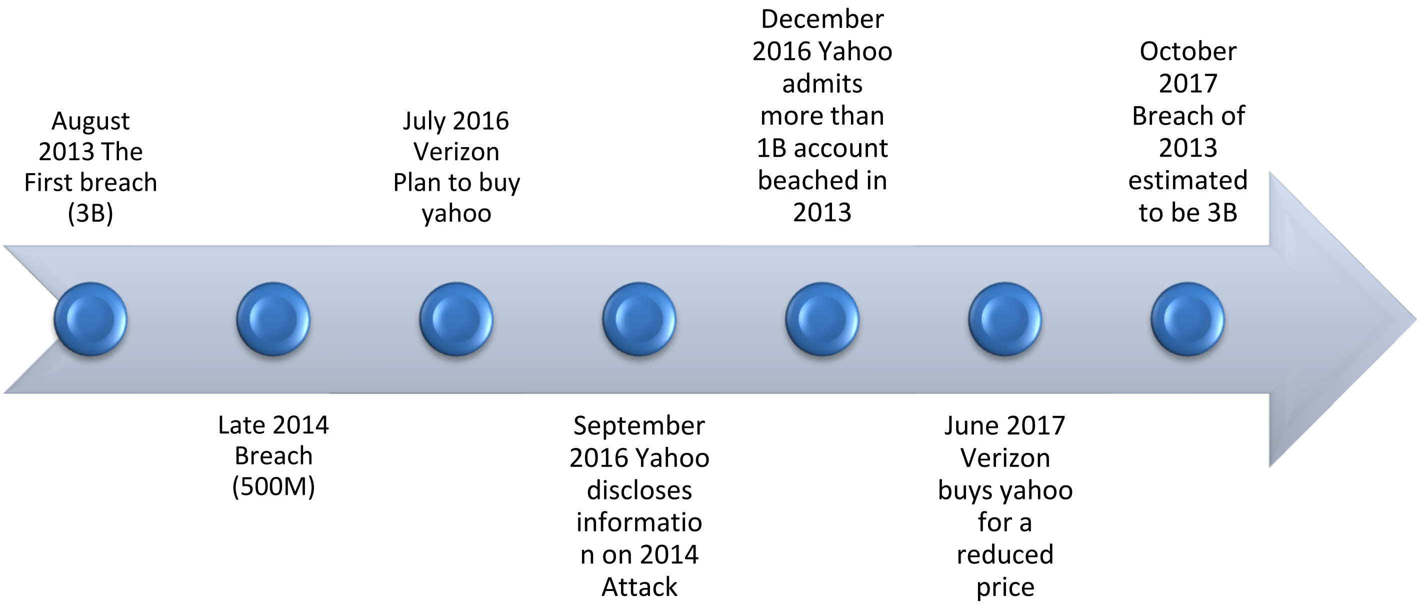
1. Introduction-Yahoo Data Breach

In a world with ever growing internet technologies securing the data and ensuring confidentiality plays a long way in retaining a solid customer base and trust. Yet Another Hierarchically Organized Oracle (acronym: YAHOO) is a leading internet service provider which is owned by Verizon right now. Its founders were Jerry Yang and David Filo. Yahoo had a data breach twice, once on August 2013 and another during late 2014. The 2013 attack compromised 3 billion yahoo accounts and then the 2014 attack about 500 million user accounts was compromised. The details stolen during the breach includes names, email address and password but not financial information.

“This is the biggest data breach ever,” said well-known cryptologist Bruce Schneier.


August 2013 The First breach (3B)
Late 2014 Breach (500M)
July 2016 Verizon Plan to buy yahoo
September 2016 Yahoo discloses information on 2014 Attack
December 2016 Yahoo admits more than 1B account beached in 2013
June 2017 Verizon buys yahoo for a reduced price
October 2017 Breach of 2013 estimated to be 3B

Breach 1 – August 2013

The first breach in August 2013 was one of the worst breach of this decade.A total of 3 billion account was compromised during the hack. At that time this was equivalent to the total account present.Yahoo did not know that their system were compromised until third-party evidence was presented to the company by law enforcement in 2016. When Yahoo was pressed on how it failed to recognize that 3 billion account was compromised, former Yahoo CEO Marissa Mayer admitted that the specifics of the attack remain unknown.

Method:

Most of this information were protected with outdated easy-to-crack encryption according to academic experts. Yahoo had made a official confirmation that hackers used its propriety code on how to forge cookies, which would allow an intruder to access user accounts without a password.

Initial estimates for the 2013 breach were 1 billion but the merger with Verizon put the breach at about 3 billion which is the largest data breach in history. [1]

"During integration, the company recently obtained new intelligence and now believes, following an investigation with the assistance of outside forensic experts, that all Yahoo user accounts were affected by the August 2013 theft,"[2] a Verizon official statement on its website states.

2014 hacks:

In late 2014 about 500 Million yahoo account was compromised. Reports suggests that there were 4 attackers of which 2 of them are Russian spies. The hackers were found to be Dmitry Dokuchaev (Russian),Igor Sushchin (Russian),Alexsey Belan and Karim Baratov.

[1] Read the complete 2013 attack- https://www.cnbc.com/2017/10/03/yahoo-every-single-account-3-billion-people-affected-in-2013-attack.html

[2] Read https://www.cnbc.com/2017/06/13/verizon-completes-yahoo-acquisition-marissa-mayer-resigns.html for complete Verizon deal Details

[3]

Method:

This is one of the most ingenious hacks to happen. The attackers began sending phishing emails to yahoo employees in early 2014. How the employees were chosen is unknown but once any employee clicks on the link the attacker was able to get into the system.

Alexsey Belan, a Latvian hacker was hired by the Russians and the only thing which he looked for in the system was the user database and Account Management Tool which is used to edit the database.

The database contained names, phone numbers, password challenge questions and answers, password recovery emails and a unique hash for each account.

To not lose access, Belan installed a backdoor on the server and took a backup copy of the user database.

The attackers used recovery email address to identify the targets and used cookies to access the account without the need for passwords. It is reported that of the 500M accounts hacked, Belan and his accomplice used only about 6500 cookies to get into important account of people. One particular technique used by the attacker to keep the user logged in without the need to reenter password is a process called as “cookie minting”. This process allowed the attackers to appear to the yahoo servers as those which have already been logged in using a secure username and

[3] Image Source - https://www.eurasiareview.com/16032017-us-indicts-russian-fsb-officers-over-2014-yahoo-hack/

password thus denying the need for username and password again. Initially the cookies were generated in the yahoo server but by August 2015 they have gained access to yahoo’s cookies minting code which allowed them to go through the process on their own machines.

The hackers used the information to target other online properties belonging to the same user, such as Hotmail, Gmail, and other services. They could also send fraudulent emails to the users to fool them into revealing passwords for other accounts, or install malware on their computers.

Yahoo initially estimated that only 26 accounts were hacked at that time and approached the FBI for help. It was only after the revelation did yahoo get to know that about 500 Million accounts were compromised.

The target chosen were several Russian journalists ,employees of a Russian cybersecurity company and officials working in the ministry of sports. It also included 14 employees of a Swiss Bitcoin banking firm, a Nevada gaming official, a senior officer of a major U.S airline , a Shanghai based managing director of a U.S private equity firm and the CTO of a French transportation company.

Once the attacker chose a specified target they would next target the wives and children of the specified target to obtain more personal information

Baratov used the same technique used by Belan to launch similar spear phising attack, gaining access to at least 80 email accounts, including at least 50 google account.

Belan is also said to have used his access to Yahoo accounts for personnel gains. He searched the account for gift cards ,credit card numbers and login information for financial services such as Paypal.

Throughout the attack FBI has alleges that the hackers "attempted to hide the nature and origin of their internet traffic" so that they will not be detected by their victims and law enforcement officers. They used Virtual Private Networks(VPN), servers from different countries and multiple false accounts.

Consequence

The initial estimate to buy yahoo was about 5.12 Billion US dollars. However after the breach was exposed yahoo and Verizon reworked the deal to about 4.48 Billion, Yahoo losing about $350 Million due the breach. Marissa Meyer, the former CEO walked away with 23 Million

2. IR recommendation

2.1 Pre incident Prep-

Identifying Risk:

Critical Assets:

The most critical assert for yahoo is its user popularity and its loyal fans considering at a time when giants like Google and Microsoft were taking over the Internet world. Also the most valuable asset for yahoo was its revenue generated through Advertisement through the source of E-Mail.

Types of Exposure:

One major concern is the employee are untrained to handle security vulnerability which may result in exposure of the system.

Yahoo potentially had a huge security gap after which it decided to change its security policies which were based on MD5 hash. In 2008, Carnegie Mellon University's Software Engineering Institute issued a public warning to security professionals through a U.S. government-funded vulnerability alert system: MD5 "should be considered cryptographically broken and unsuitable for further use."[4] This was a major risk considering that yahoo knew about the risk for long and did not act on it for 5 whole years. The company began migrating to newer algorithm in late 2013.

2.2 Preparing the IR team:

Mission:

- Provide a overall management of system security and ensure prevention of unauthorized usage of data for customer
- Provides information and assistance to the staff of hosting company to reduce the risks of computer security incidents as well as responding to such incidents when they occur.
- Ensure to provide proper guidance to the host company when an incident occurs.

Policies:

Intrusion attempts, security breaches, theft or loss of hardware and other security related incidents perpetrated against the Yahoo,Inc must be reported to the Chief Information security officer Alex Stamos. People with knowledge, or a reasonable suspicion, of an incident which violates the confidentiality, integrity, or availability of data leak, will make an immediate report to the following e-mail address: ciso@yahoo.com

[4] Refer : http://www.businesstimes.com.sg/technology/yahoo-security-problems-a-story-of-too-little-too-late

The Director of Networks, Security and Systems, in collaboration with other appropriate staff with the CTO shall determine if a reported incident IS or IS NOT a confidential information Security Incident.

Communication Procedures:

All internal communication between the IR team must be encrypted. Proper labelling and documentation must be done All external communication have to be reported on a weekly bases. Notification is passed on to the 3rd party using SSH communication. Yahoo CEO Marissa Mayer handles the final public disclosure. Penalties for non-compliance includes arrest,criminal and non-criminal charges, suspension, severance of benefit packages and termination without benefits depending on the severity of the non-compliance.

2.3 Resources For IR Team:

Storage Used: WD Blue PC Mobile Hard Drive – FAT – Volume Encryption.

Software For IR:

Software used to analyze is OpenIOC. Boot Disk -Kali. Disk Imaging Tool – FTK, Forensic examination Tool – Nuix.

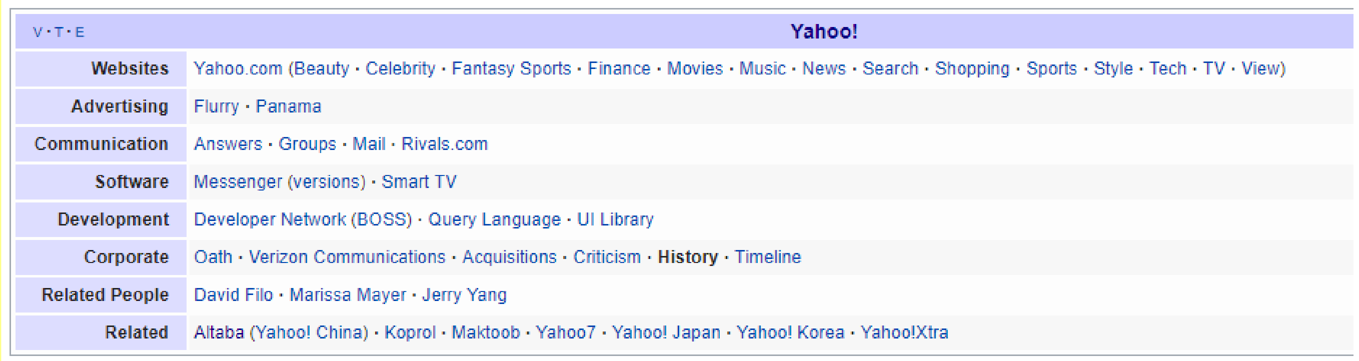
Network monitoring Platforms: Fiber Channel with over 24 ports. SAN support with HBA.

2.4 Infrastructure preparation:

Yahoo was started in January 1994 by Jerry yang and David Filo at Stanford University. Yahoo grew exponentially in the dot com bubble and became a corporate company on March 2nd 1995 with its headquarters located at Sunnyvale, California. Yahoo offers a webportal service to its user where all information from diverse sources like emails, search engines and forums are brought together.

Yahoo Business Unit and Applications:

Yahoo owes many businesses as shown below:

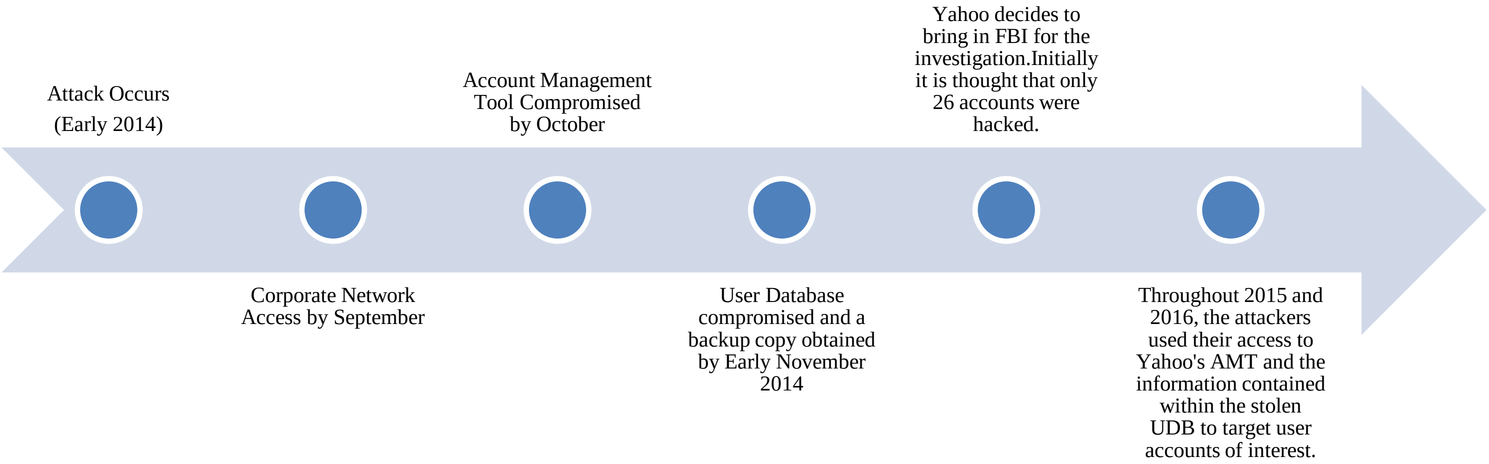


V · T · E	Yahoo!
Websites	Yahoo.com (Beauty · Celebrity · Fantasy Sports · Finance · Movies · Music · News · Search · Shopping · Sports · Style · Tech · TV · View)
Advertising	Flurry · Panama
Communication	Answers · Groups · Mail · Rivals.com
Software	Messenger (versions) · Smart TV
Development	Developer Network (BOSS) · Query Language · UI Library
Corporate	Oath · Verizon Communications · Acquisitions · Criticism · **History** · Timeline
Related People	David Filo · Marissa Mayer · Jerry Yang
Related	Altaba (Yahoo! China) · Koprol · Maktoob · Yahoo7 · Yahoo! Japan · Yahoo! Korea · Yahoo!Xtra

5

2.5 Collecting initial Facts:

The attacker timeline is as following:



Attack Occurs (Early 2014)

Corporate Network Access by September

Account Management Tool Compromised by October

User Database compromised and a backup copy obtained by Early November 2014

Yahoo decides to bring in FBI for the investigation.Initially it is thought that only 26 accounts were hacked.

Throughout 2015 and 2016, the attackers used their access to Yahoo's AMT and the information contained within the stolen UDB to target user accounts of interest.

2.6 Incident Detection Summary Checklist:

The date the incident was reported was on August 2014. Affected resources include Database Server’s, Host systems, compromise of the Hashing algorithm, Account Management Tools (AMT), end users and software’s used for Database Servers. Incident Detected through 3rd party help. Current Knowledge regarding hack known to the CEO Marissa Mayer, Jacqueline Reses EVP People And Development and CISO Alex Stamos

[5] Source Wikipedia - Refer Wikipedia.com for a complete list of Yahoo Business unit

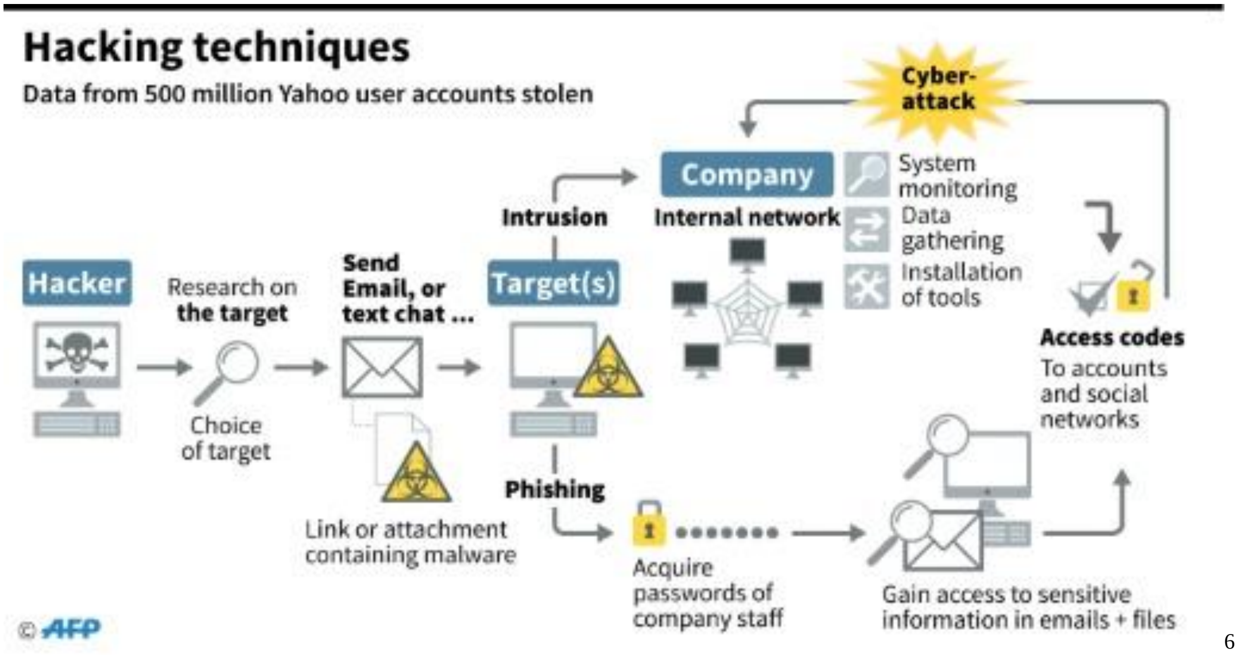
2.7 Incident Detection Checklist:

The initial investigation reveal that the incident was not revealed by internal intern but by external sources which claimed that the information of about 280 million yahoo user databases was on sale in the black market by a hacker. Joseph Cox, a reporter with the technology news site Motherboard,emailed Yahoo on July 30 regarding the leaked Data sale. This was when Yahoo began its investigation on the breach in a broad perspective.

On conducting an internal investigation initially, the team found nothing to support the claim. But on further detailed, broader deep dive review, it was found that the compromise was true and about 5 million accounts has been compromised. The date and time were noted regarding the compromised and the necessary contact person including the CEO was notified of the lapse in security.The incident was detected due to a manual check performed.

At the breach meeting the decision to make this breach a public matter was deferred until further investigation were conducted.

Hacking Diagram:


Hacking techniques
Data from 500 million Yahoo user accounts stolen
Cyber-attack
Company
Internal network
System monitoring
Data gathering
Installation of tools
Intrusion
Hacker
Research on the target
Choice of target
Send Email, or text chat ...
Target(s)
Link or attachment containing malware
Phishing
Acquire passwords of company staff
Gain access to sensitive information in emails + files
Access codes
To accounts and social networks
© AFP

[6]

[6] Image source : https://phys.org/news/2016-09-russia-china-hacked-yahoo.html

Additional Details:

System Details:

Critical information stored on the system includes the user database. Compromised information includes username, passwords, giftcard details and personal information.The system including the data server is connected to online to the server so that we can identify the source of the intrusion. Remediation steps currently in progress includes isolation of the database server and web server, analyzing the source of the attack to know more in detail about the malware

Network Details:

Various domains have been involved in the attack. Current process to decrypt them is undergoing. Attackers used VPN’s and spoofing technique to launch the attack and access the data. All incoming and outgoing traffic are monitored and a special network analyzing team has been formed. Remediation steps followed is the enhancement of the network security and hashing algorithm used along with Two-factor Authentication

Malware Details:

The malware present here is a cookie though which the attacker was able to gain access to the system.The internal cookie responsible for tracking user logging and help them in logging in without the requirement for username or password was compromised. Attackers used a fake cookie to trick the web server to think it was a valid cookie thus helping them gain access to the UDB. Remediation work include a IOC is now in preparation to prevent these types of cookies. End-clients are now made to reset the password for the account, Cookie tracking is enabled to find the details of the attack.

2.8 Leads:

An online website ‘Peace’ which contained information pertaining to about 280 Million user database.

2.9 IOC Creation:

OpenIOC was used to detect the malware based on the cookie and an IOC was created. IOC was host and network based. The suspected system was identified, and the evidence was collected. The data from the system was analyzed and the IOC is now further improved. This is an iterative process. OpenIOC is used to document the changes made to the infected host's file system and registry configurations; kernel and other program hooks; network protocols and ports. With this information, network, and the host IPS could be configured for containment and eradication.

Recommendations:

Having a Prepared Incident Team – Of the Analysis performed we found that Yahoo does not have a fully functional Incident Handling Team. Financial allocation to the team is minimum. This must be increased.

Consult with Legal Departments – Yahoo has delayed in its approach to the legal department by first waiting for a complete Analysis. The Analysis proved to be futile since it was only able to determine 26 accounts were hacked initially with its technology. This could have been easily averted if Yahoo has approached the Legal Team on a earlier date.

Updating of Latest Technology – Yahoo has made use of an antique encryption technique which was known to have security vulnerability. Updating of Latest technology and staying with the current market trend is necessary as new technologies emerge in the market.

Sharing of Information – Yahoo must make sure that the Senior Management team is willing to share its information with the other members so that it would lead to formation of ideas and tacking of any security breach up to a certain point.

Limiting Access to Privilege Data – Access the user database must be limited and monitored along with the change of credentials for application components to protect it from unauthorized exposure.

Point Of Entry - Prevention – A multifactor authentication would prevent the attacker from accessing user data easily. This must be implemented.

Employee Security Education – All Employee must be educated to handle vulnerable issues such as an email from an unknown sender, pen drive injection, unauthorized access on one’s system, browsing of unsecure sites etc.

References:

Indictment – Department Of Justice - https://www.justice.gov/opa/press-release/file/948201/download

A History of Yahoo Attacks - https://www.technologyreview.com/s/603157/a-history-of-yahoo-hacks/

Why Does Yahoo keep getting Attacked - http://www.kcra.com/article/why-does-yahoo-keep-getting-hacked-cybersecurity-experts-weigh-in/8879255

Did Yahoo do enough to prevent the massive hack? - http://money.cnn.com/2016/09/23/technology/yahoo-hack-timeline/index.html

Who the Russian hackers targeted when they stole Yahoo emails- http://money.cnn.com/2017/03/16/technology/yahoo-hackers-targeted-erectile-dysfunction/index.html?iid=EL

Yahoo hack: What you need to know about the biggest data breach in history - https://www.telegraph.co.uk/technology/2016/12/15/yahoo-hack-need-know-biggest-data-breach-history/

Computer Security Incident Handling Guide - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Keys to Successful Incident Response Teams - https://www.symantec.com/connect/articles/keys-successful-incident-response-teams

Storage Incident Handling - https://www.sans.org/reading-room/whitepapers/incident/guide-encrypted-storage-incident-handling-33059

Checklists - https://www.sans.org/score/checklists/

Incident Response Fight Back - https://www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342