Issued 3/18/17

HOW IT TOOK JUST ONE-CLICK TO EXECUTE BIGGEST DATA BREACH IN HISTORY

In the digital world, it just takes one click to get the keys to the kingdom. Do you know spear-phishing was the only secret weapon behind the biggest data breach in the history?

It's true, as one of the Yahoo employees fell victim to a simple phishing attack and clicked one wrong link that let the hackers gain a foothold in the company's internal networks.

You may be familiar with phishing attacks — an attempt to steal user credentials or financial data — while, Spear-phishing is a targeted form of phishing in which attackers trick employees or vendors into providing remote-access credentials or opening a malicious attachment containing an exploit or payload.

Here's how the Yahoo's massive data breach was traced back to human error and who were the alleged masterminds behind this hack.

On March 15th the US government charged two Russian spies and two criminal hackers in connection with the 2014 Yahoo hack that compromised about 500 million Yahoo user accounts.

While the indictment provided details on the 2014 Yahoo hack, the FBI officials recently gave a fresh insight into how the two officers from the Russian Federal Security Service (FSB) hired two hackers to gained initial access to Yahoo in early 2014.

Here's How the Yahoo Hack Initiated:
The hack began with a "Spear Phishing" e-mail sent to a "semi-privileged" Yahoo employees and not the company's top executives early in 2014.

Although it is unclear how many Yahoo employees were targeted in the attack and how many emails were sent by the hackers, it only takes one employee to click on either a malicious attachment or a link, and it gave attackers direct access to Yahoo's internal networks.

Once in, Alexsey Belan, who is already on the FBI's Most Wanted Hackers list, started poking around the network and, according to the FBI, discovered two key assets:

Yahoo's User Database (UDB) – a database containing personal information about all Yahoo users.

The Account Management Tool – an administrative tool used to edit the database.

Belan used the file transfer protocol (FTP) to download the Yahoo database, containing usernames, phone numbers, security questions and answers, and, what's worse, password recovery emails and a cryptographic value unique to each Yahoo account.

Recovery emails and unique cryptographic values enabled Belan and fellow hacker Baratov to access the accounts of certain users requested by the Russian spies.

Since the Account Management Tool did not allow for simple text searches of usernames, the hackers began identifying targets based on their recovery email address.

Once identified, the hackers then used stolen cryptographic values called "nonces" to generate forged access cookies for specific user accounts,

giving both the FSB agents and Belan access to users' email accounts without the need for any password.

According to the FBI, those cookies were generated many times between 2015 and 2016 to access "more than 6,500 Yahoo accounts," out of the roughly 500 million accounts.

Victims Targeted by the Russian Spies:
According to the indictment, among other foreign webmail and Internet-related service providers, the Russian spies accessed the Yahoo accounts belonging to:
- An assistant to the deputy chairman of Russia.
- An officer in Russia's Ministry of Internal Affairs.
- A trainer working in Russia's Ministry of Sports.
- Russian journalists.
- Officials of states bordering Russia.
- U.S. government workers.
- An employee of a Swiss Bitcoin wallet company.
- A U.S. airline worker.

A FBI special agent told a news conference that Yahoo first approached the bureau in 2014, regarding the hack and was "great partners" during its investigation.

However, the company took two years to go public in December 2016 with details of the data breach and advised hundreds of millions of its customers to change their passwords.

Baratov was arrested on Tuesday by the Toronto Police Department, while Belan and the two FSB officers are in Russia. The United States has requested all the three to be handed over to face charges, but the US has no extradition treaty with Russia.