Russia? China? Who hacked Yahoo, and why?

September 23 2016, by Guy Jackson, Laurence Benhamou

US internet giant Yahoo is under pressure to explain how it sustained a massive breach in 2014, which possibly affected 500 million accounts

Yahoo's claim that it is the victim of a gigantic state-sponsored hack raises the question of whether it is the latest target for hackers with the backing of Russia, China or even North Korea, experts say.

The US internet giant was under pressure Friday to explain how it

sustained such a massive breach in 2014, which possibly affected 500 million accounts.

Yahoo said the stolen information may have included email addresses and scrambled passwords, along with both encrypted or unencrypted security questions and answers that could help gain access to victims' other online accounts.

Sometimes the link between the target of a hack and a particular state may suggest itself easily.

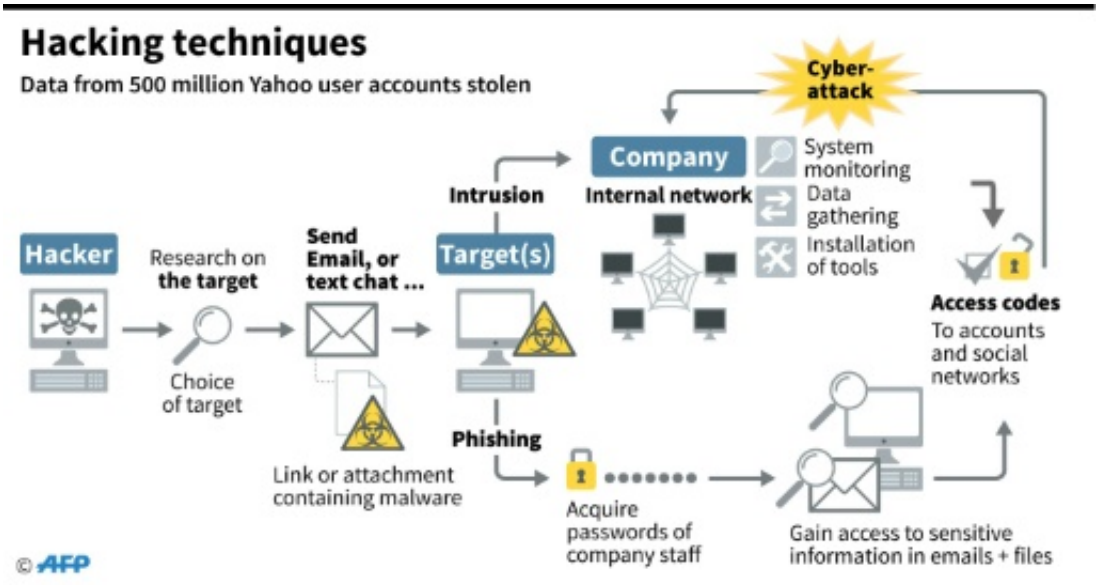
One of the highest-profile hacks came when North Korea is thought to have targeted entertainment titan Sony in 2014, apparently in revenge for producing the comedy film "The Interview" about a CIA plot to assassinate leader Kim Jong-Un.

More recently, a mysterious group calling itself Fancy Bears hacked the medical records of athletes held by the World Anti-Doping Agency (WADA). It is still dripping the information out.

Commercial motives

Many experts believe that cyberattack was carried out by Russia after its track and field athletes were banned from the Olympics and its entire Paralympics team turfed out of their Games over evidence of state-sponsored doping.

While motivation for those cyberattacks seems clear, it might initially appear less obvious why countries such as Russia, North Korea or even China would target a company like Yahoo.



Yahoo hacked: how it is done

Chinese hackers have been accused of plundering industrial and corporate secrets and of orchestrating a breach of US government files on its employees that affected more than 21 million people and reportedly led to the hasty withdrawal of US intelligence operatives from China to protect their lives.

But political motives can be as strong as commercial ones, analysts note.

"Would, for example, Russian intelligence wish to conduct a large-scale hack on a major internet company like Yahoo? Absolutely they would," Shashank Joshi, senior research fellow at the London-based Royal United Services Institute, told AFP.

"It is an incredibly valuable commodity. The ability to access email addresses for US persons, perhaps a Russian dissident—any intelligence agency worth its salt would want that sort of data, although it is very hard to use because of the encrypted passwords," he said.

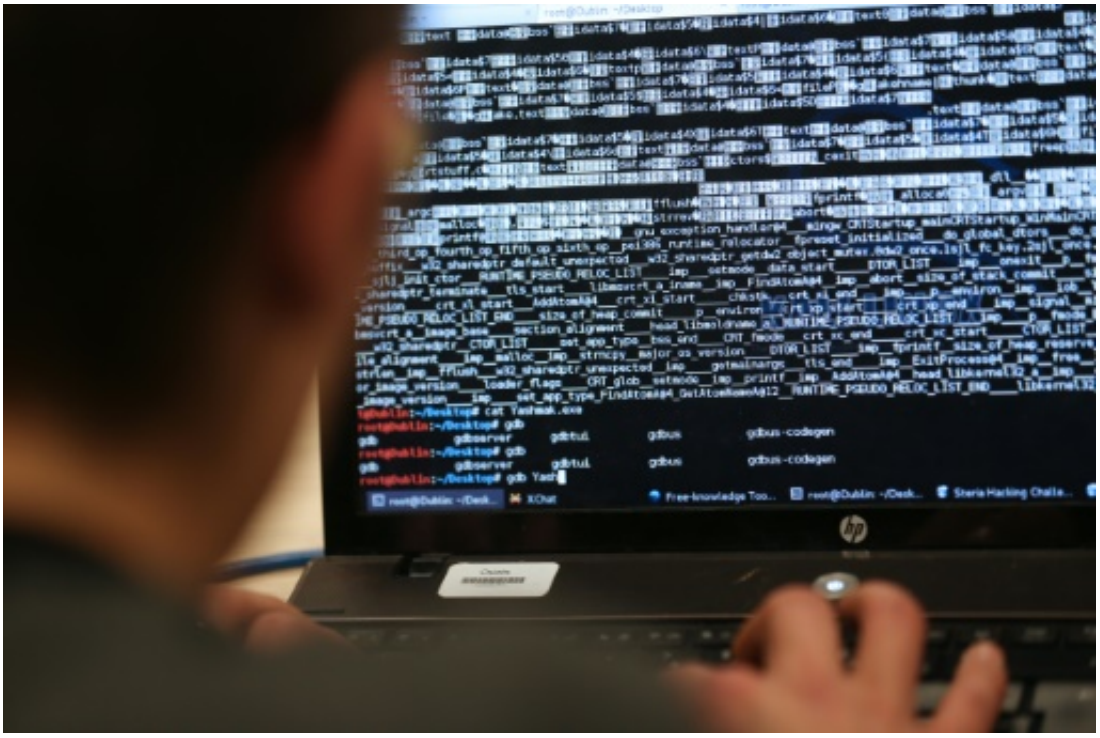
Julien Nocetti, of the French Institute of International Relations (IFRI), said the hack was too big for an independent group to carry out.

"Given the scale of the revelations about Yahoo, it indicates that a lot of resources, technical equipment and coordination were required—this definitely comes from a state," he said.

Given the tensions between Russia and the United States over the Syrian war "you could put forward the theory that this could be a Russian attempt to test the Americans' cyber defences", he said.

Finding the source

Yahoo has so far given no evidence to support its claim that it has been targeted by a state.



Yahoo says information stolen through a hack may have included email

addresses and scrambled passwords, along with both encrypted or unencrypted security questions and answers that could help gain access to victims' other online accounts

RUSI's Joshi said finding the source "is the most fundamental problem when it comes to cyber-attacks".

"This completely bedevils even the most well-resourced people," he said.

However, he believes Yahoo would only have pointed the finger at state involvement if it had some evidence.

"The way you identify responsibility for a hack is to look for signatures that correspond to earlier known facts and then see what you know about them," he said.

For example, in case of the hacking of Democratic National Committee (DNC) emails this year which exposed bias within the party in favour of Hillary Clinton, cyber-security experts found evidence of a so-called Advanced Persistent Threat (APT).

"That is a code word for state hackers who were clearly operating in a system and matched up with earlier such hacks" carried out by Russia's state and military intelligence agencies, Joshi said.

But in Russia, so often accused of state-sponsored hacking, one expert said it was naive to immediately blame a state and scoffed at the suggestion the hackers were sophisticated spies.

"Anyone could have hacked a database of users like Yahoo because it's a classic commercial server," said Oleg Demidov, a consultant at the

Moscow-based independent think-tank PIR Center.

"At the moment, this looks like a traditional hack aimed at making money or carving out a reputation by selling a load of personal data," he added.

Yahoo hack is latest major cyber-attack

The massive hacking attack on Yahoo revealed Thursday is one of biggest thefts of online users' personal information ever, affecting some 500 million accounts.

For Tanguy de Coatpont, head of the French and North African divisions of Kaspersky Lab, a computer security company, it is "the biggest in history involving a single company".

Michael Bittan, a risk manager at Deloitte, cautioned that it was "the biggest to be made public. There have possibly been others that were bigger".

At any rate, it is far from the first, and here are other notable major corporate hacks of recent years:

Taking aim at Target

US retail giant Target was hit by a computer attack in December 2013 that affected 110 million clients. Seventy million might have lost personal data including names, addresses, phone numbers and e-mail accounts, while 40 million bank accounts and credit cards were also put at risk.

South Korea scramble

- In January 2014, South Koreans scrambled to stop money being siphoned from their bank accounts after it emerged that data on 20 million credit cards had been stolen over several years.

The data was swiped by an employee from the personal credit ratings firm Korea Credit Bureau, who then sold it to telemarketing companies.

Password plunder

- In August 2014, online data protection firm Hold Security claimed that Russian hackers had accessed 1.2 billion passwords linked to 420,000 internet sites around the world, from corporate giants to individual accounts. Hold Security pointed to a group of hackers called "CyberVor", which it said had potentially gained access to 500 million e-mail accounts.

Too hot to handle

In August 2015, hackers calling themselves The Impact Team published nearly 30 gigabytes of files including the names and credit card data of people who had signed up with Ashley Madison, a website for those who wanted to have extra-marital affairs.

The company's boss stepped down as several suicides were linked to the revelations.

Ashley Madison had earlier offered to delete users personal data for a modest fee, but did not, resulting in the launch of a class-action lawsuit estimated at Can$760 million (US$578 million).

Apple in crosshairs

In September 2015, computer security experts discovered a virus dubbed "KeyRaider" that targetted Apple iPhones and iPads, and which had already affected 225,000 Apple accounts.

The virus intercepted communications with Apple's iTunes music store, stealing information as purchases were made. Users in 18 countries were affected.

© 2016 AFP

Citation: Russia? China? Who hacked Yahoo, and why? (2016, September 23) retrieved 2 May 2024 from https://phys.org/news/2016-09-russia-china-hacked-yahoo.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.