Cascading effect: One attack led to another at Yahoo

March 15 2017, by Anick Jesdanun, Michael Liedtke And Mae Anderson

This Jan. 14, 2015, file photo shows a sign outside Yahoo's headquarters in Sunnyvale, Calif. In an indictment Wednesday, March 15, 2017, announcing charges against four Russians, U.S. officials describe how Russian hackers working with Russian intelligence officials broke into Yahoo's network, stole information on Yahoo user accounts and ultimately gained entry into other services used by individuals they were targeting. (AP Photo/Marcio Jose Sanchez, File)

Russian hackers working with Russian spies didn't crack Yahoo security

all at once.

Instead, according to an account offered by U.S. officials, they methodically made their way deeper into Yahoo's network over the space of months—maybe years. That allowed them to forge technological skeleton keys that would unlock many Yahoo accounts, steal personal information and then use that data to break into other email services used by their targets, U.S. officials said in announcing charges against four Russians .

The hackers' primary targets were Russian and U.S. government officials, Russian journalists and employees of financial companies and other businesses. But the attackers also used access to Yahoo's network for financial gain, according to Wednesday's indictment.

The severity of that breach, the second worst in internet history, was most likely magnified by the fact that it took some two years for Yahoo to disclose the initial attack. Had Yahoo taken more aggressive steps—for instance, asking users to change their passwords, or even expiring the passwords and forcing users to enter new ones—it might have prevented some of the damage.

Here's a look at how the breach occurred, according to U.S. officials.

USER ACCOUNTS

Hackers got their initial access to Yahoo's network around early 2014, although it's not clear exactly how. By the end of the year, they had made two valuable finds.

The first was a backup copy of Yahoo's user database, current as of early November 2014. That database contained information that could be used to reset passwords and gain entry to Yahoo accounts, including phone

numbers, answers to security questions and recovery email addresses. Using the latter, services like Yahoo can send password reset links.

The database also contained cryptographically scrambled versions of user passwords, which Yahoo uses to verify users as they log in.

The second was an internal tool Yahoo used to access and edit information in the user database. Together, they allowed hackers to start unlocking Yahoo accounts at will.

FOOL ME ONCE, FOOL ME TWICE

In effect, hackers created a Yahoo skeleton key by fooling the service into thinking they had already signed into particular accounts, even if they didn't know their passwords. Web service providers typically use bits of data called cookies to let you stay signed into an account via a web browser. This is how you keep Gmail, for instance, open even if you close your browser and restart it.

The hackers used malware and the scrambled passwords in the user database to manufacture fake cookies. To Yahoo, it then appeared that the hacker was the authorized user, who was already logged in without entering a password.

That method worked so long as users didn't change their passwords after early November 2014. Hackers used this technique to target more than 6,500 user accounts.

BEYOND YAHOO

The hackers targeted employees of specific companies by searching the database for recovery emails that used employer domains, according to the indictment. For instance, if hackers had looked for employees from

The Associated Press, they'd have searched for email addresses ending with ap.org.

Hackers also searched emails for the existence of other accounts controlled by the same user. Some were at Yahoo, others at Google's Gmail and other companies. The hackers could then send emails designed to dupe recipients into installing malware or providing passwords for those other accounts.

MAKING MONEY

While Russian intelligence officials were interested only in a limited number of accounts, hackers used access to Yahoo's network for their own financial gain.

For instance, they manipulated servers so that searches for erectile dysfunction medications generated a link that took users to an online pharmacy that was paying commissions to the hackers.

Hackers also searched users' email accounts for credit card information and electronic gift cards. Hackers also searched emails for contact information of friends and colleagues; such data enabled spam that appeared to originate from those friends and colleagues, making it more likely that the recipient would open the message.

THE OTHER BREACH

The 2014 breach was the second of two major breaches at Yahoo and involved at least 500 million user accounts. Yahoo later revealed that it had uncovered a separate hack in 2013 affecting about 1 billion accounts, including some that were also hit in 2014. Wednesday's indictment didn't address the 2013 breach.