6-Reuters-Yahoo security problems

By Joseph Menn , Jim Finkle , Dustin Volz

7 Min Read

SAN FRANCISCO/BOSTON/WASHINGTON (Reuters) - In the summer of 2013, Yahoo Inc launched a project to better secure the passwords of its customers, abandoning the use of a discredited technology for encrypting data known as MD5.

A photo illustration shows a Yahoo logo on a smartphone in front of a displayed cyber code and keyboard on December 15, 2016. REUTERS/Dado Ruvic/Illustration

It was too late *[Disappointment]*. In August of that year, hackers got hold of more than a billion Yahoo accounts, stealing the poorly encrypted passwords and other information *[Disappointment]* in the biggest data breach on record. Yahoo only recently uncovered the hack and disclosed it last week.

[Disappointment]

The timing of the attack might seem like bad luck, but the weakness of MD5 had been known by hackers and security experts for more than a decade *[Disappointment]*. MD5 can be cracked more easily than other so-called “hashing” algorithms, which are mathematical functions that convert data into seemingly random character strings.

In 2008, five years before Yahoo took action *[Disappointment]*, 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.”

Yahoo's failure to move away from MD5 in a timely fashion was an example of problems in Yahoo's security operations *[Disappointment]* as it grappled with business challenges, according to five former employees and some outside security experts. Stronger hashing technology would have made it more difficult for the hackers to get into customer accounts after breaching Yahoo's network, making the attack far less damaging, they said.

"MD5 was considered dead long before 2013," said David Kennedy, chief executive of cyber firm TrustedSec LLC. "Most companies were using more secure hashing algorithms by then *[Disappointment]*." He did not name specific firms.

Yahoo, which has confirmed it was still using MD5 at the time of the attack, disputed the notion that the company had skimped on security.

[Disappointment]

"Over the course of our more than 20-year history, Yahoo has focused on and invested in security programs and talent to protect our users," Yahoo said in a statement to Reuters. "We have invested more than $250 million in security initiatives across the company since 2012."

[Reinforce]

COMPETING PRIORITIES

The former Yahoo security staffers, however, told Reuters the security team was at times turned down when it requested new tools and features such as strengthened cryptography protections, on the grounds that the requests would cost too much money, were too complicated, or were simply too low a priority.

[Disappointment]

Partly, that reflected the internet pioneer's long-running financial struggles: Yahoo's revenues and profits have fallen steadily since their 2008 peak while Alphabet Inc's Google, Facebook Inc and others have come to dominate the consumer internet business.

“When business is good, it’s easy to do things like security,” said Jeremiah Grossman, who worked on Yahoo’s security team from 1999 to 2001. “When business is bad, you expect to see security get cut.”

To be sure, no system is completely hack-proof. Hackers have managed to break into passwords that were encrypted using more advanced technologies than MD5. Other Internet companies, such as LinkedIn and AOL, have also suffered security breaches, though none nearly as large as Yahoo’s.

“This could happen to any large corporation,” said Tom Kellermann, a former World Bank security manager and security industry executive.

Kellermann, now CEO of investment firm Strategic Cyber Ventures, said he was not surprised that it had taken Yahoo several years to identify the massive attacks. “Hackers often have a capacity to burrow deeper than we thought into a system and remain for years,” he said.

[Positive]

Reuters could not determine how many companies besides Yahoo were using MD5 in 2013. Google, Facebook and Microsoft Corp did not immediately respond to requests for comment.

According to another former security veteran at Yahoo, even when the company was growing quickly, security sometimes took a back seat as the company focused on system performance to keep up with the growth.

Then, when growth stalled, senior security staff left for other companies and the chances of getting approval for expensive upgrades dropped further, the person said.

“Any changes to the user database took forever because they were understaffed, and it’s an ultra-critical system - everything depends on it,” said the former Yahoo employee.

Yahoo declined to comment on details of its security practices, but said it routinely conducted drills to test and improve its cyber defenses and

highlighted campaigns such as a “bug bounty” program in which it pays hackers to find security flaws and report them to the company.

[Reinforce]

TWO BIGGEST BREACHES

Last September, Yahoo disclosed a 2014 cyber attack that affected at least 500 million customer accounts, the biggest known data breach at the time.

Following last week’s news of the even bigger 2013 breach, U.S. federal investigators and lawmakers said they are scrutinizing Yahoo’s security practices, and Verizon Communications Inc is seeking to renegotiate a July deal to buy Yahoo’s internet business for $4.8 billion. *[Legal Action]*

The former Yahoo employees said the company’s security problems began before the arrival of Chief Executive Marissa Mayer in 2012 and continued under her tenure *[Disappointment]*. Yahoo had suffered attacks by Russian hackers for years, two of the former staffers said.

In 2014, Yahoo hired a new security chief, Alex Stamos, and one of the security crews he led - known internally as ‘The Paranoids’ - thought they were making headway against the hackers, former employees said. In 2015, when the security crew discovered a hidden program attached to Yahoo’s email servers that was monitoring all incoming messages, their first thought was that the Russian hackers had come back.

It turned out that the program had been installed by Yahoo’s email engineers to comply with a secret surveillance order requested by a U.S. intelligence agency, as Reuters previously reported. Stamos and some of his staff left Yahoo soon after that, creating further disruptions to security operations.

This week, in addition to disclosing the 2013 hack, Yahoo said someone had accessed its proprietary computer code to learn how to forge “cookies,” which would allow hackers to access an account without passwords. Yahoo said it connected some cookie-forging activity to the same state-sponsored actor it believed was responsible for the 2014 data theft.

“They burrowed in and got access to everything,” said Dan Guido, chief executive of cyber security firm Trail of Bits.

On Thursday, Germany’s cyber security authority criticized Yahoo for failing to adopt adequate encryption techniques and advised German consumers to switch to other email providers.

[Anger]

Yahoo told Reuters it was committed to keeping users secure by staying ahead of new threats. “Today’s security landscape is complex and ever-evolving, but, at Yahoo, we have a deep understanding of the threats facing our users and continuously strive to stay ahead of these threats to keep our users and our platforms secure.”

[Reinforce]

Reporting by Joseph Menn in San Francisco, Jim Finkle in Boston and Dustin Volz in Washington; Editing by Jonathan Weber and Bill Rigby