Online Security Flaw Exposes Millions of Passwords

ANICK JESDANUN, AP Technology Writers MICHAEL LIEDTKE, AP Technology Writers

San Francisco (AP) — An alarming lapse in Internet security has exposed millions of passwords, credit card numbers and other sensitive bits of information to potential theft by computer hackers who may have been secretly exploiting the problem before its discovery.

The breakdown revealed this week affects the encryption technology that is supposed to protect online accounts for emails, instant messaging and a wide range of electronic commerce.

Security researchers who uncovered the threat, known as "Heartbleed," are particularly worried about the breach because it went undetected for more than two years.

Although there is now a way to close the security hole, there are still plenty of reasons to be concerned, said David Chartier, CEO of Codenomicon. A small team from the Finnish security firm diagnosed Heartbleed while working independently from another Google Inc. researcher who also discovered the threat.

"I don't think anyone that had been using this technology is in a position to definitively say they weren't compromised," Chartier said.

Chartier and other computer security experts are advising people to consider changing all their online passwords.

"I would change every password everywhere because it's possible something was sniffed out," said Wolfgang Kandek, chief technology officer for Qualys, a maker of security-analysis software. "You don't know because an attack wouldn't have left a distinct footprint."

But changing the passwords won't do any good, these experts said, until the affected services install the software released Monday to fix the problem. That puts the onus on the Internet services affected by Heartbleed to alert their users to the potential risks and let them know when the Heartbleed fix has been installed so they can change their passwords.

"This is going to be difficult for the average guy in the streets to understand, because it's hard to know who has done what and what is safe," Chartier said.

Yahoo Inc., which boasts more than 800 million users worldwide, is among the Internet services that could be potentially hurt by Heartbleed. The Sunnyvale, Calif., company said most of its most popular services — including sports, finance and

Tumblr — had been fixed, but work was still being done on other products that it didn't identify in a statement Tuesday.

"We're focused on providing the most secure experience possible for our users worldwide and are continuously working to protect our users' data," Yahoo said.

Heartbleed creates an opening in SSL/TLS, an encryption technology marked by the small, closed padlock and "https:" on Web browsers to signify that traffic is secure. The flaw makes it possible to snoop on Internet traffic even if the padlock had been closed. Interlopers could also grab the keys for deciphering encrypted data without the website owners knowing the theft had occurred, according to security researchers.

The problem affects only the variant of SSL/TLS known as OpenSSL, but that happens to be one of the most common on the Internet.

About two-thirds of Web servers rely on OpenSSL, Chartier said. That means the information passing through hundreds of thousands of websites could be vulnerable, despite the protection offered by encryptions. Beside emails and chats, OpenSSL is also used to secure virtual private networks, which are used by employees to connect with corporate networks seeking to shield confidential information from prying eyes.

Heartbleed exposed a weakness in encryption at the same time that major Internet services such as Yahoo, Google, Microsoft and Facebook are expanding their usage of technology to reassure the users about the sanctity of their personal data. The additional security measures are being adopted in response to mounting concerns about the U.S. government's surveillance of online activities and other communications. The snooping has been revealed during the past 10 months through a series of leaked documents from former NSA contractor Edward Snowden.

Despite the worries raised by Heartbleed, Codenomicon said many large consumer sites aren't likely to be affected because of their "conservative choice" of equipment and software. "Ironically, smaller and more progressive services or those who have upgraded to (the) latest and best encryption will be affected most," the security firm said in a blog post.

Although it may take months for smaller websites to install the Heartbleed fix, Chartier predicted all the major Internet services will act quickly to protect their reputations.

In a Tuesday post announcing it had installed the Heartbleed fix, Tumblr offered its users some blunt advice.

"This still means that the little lock icon (HTTPS) we all trusted to keep our passwords, personal emails, and credit cards safe, was actually making all that private information accessible to anyone who knew about the exploit," Tumblr said. "This might be a good day to call in sick and take some time to change your passwords everywhere — especially your high-security services like email, file

storage, and banking, which may have been compromised by this bug."

___

Jesdanun reported from New York.