Heartbleed bug causes major security headache (Update 3)

April 9 2014, by Anick Jesdanun

A confounding computer bug called "Heartbleed" is causing major security headaches across the Internet as websites scramble to fix the problem and Web surfers wonder whether they should change their passwords to prevent theft of their email accounts, credit card numbers and other sensitive information.

The breakdown revealed this week affects a widely used encryption technology that is supposed to protect online accounts for a variety of online communications and electronic commerce.

Security researchers who uncovered the threat are particularly worried about the lapse because it went undetected for more than two years. They fear the possibility that computer hackers may have been secretly exploiting the problem before its discovery. It's also possible that no one took advantage of the flaw before its existence was announced late Monday.

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.

Canada's tax agency isn't taking any chances. Citing the security risks posed by Heartbleed, the Canada Revenue Agency shut off public access to its website "to safeguard the integrity of the information we hold," according to a notice posted on its website Wednesday. The agency said it hopes to re-open its website this weekend. The lockdown comes just three weeks from Canada's April 30 deadline for filing 2013 tax returns.

The U.S. Internal Revenue Service said in a statement Wednesday that it's not affected by the security hole.

TurboTax, the most popular U.S. tax preparation software, also issued a Wednesday statement reassuring people that its website is now protected against Heartbleed.

Computer security experts are still 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."

Google is so confident that it inoculated itself against the Heartbleed bug before any damage could be done that the Mountain View, California, company is telling its users they don't have to change the passwords they use to access Gmail, YouTube and other product accounts. More than 425 million Gmail accounts alone have been set up worldwide.

Facebook, which has more than 1.2 billion accountholders, also believes its online social network has purged the Heartbleed threat. But the Menlo Park, California, company encouraged "people to take this opportunity to follow good practices and set up a unique password for your Facebook account that you don't use on other sites."

Online short messaging service Twitter Inc. and e-commerce giant Amazon.com Inc. say their websites weren't exposed to Heartbleed. Ebay Inc., which runs the PayPal payment service as well as online shopping bazaars, says most of its services avoided the bug.

Changing passwords on other online services potentially affected by Heartbleed won't do much good, security experts said, until the problem is patched. The trouble-shooting software was released Monday.

So far, very few websites have acknowledged being afflicted by Heartbleed, although the bug is believed to be widespread.

"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. and Google are among the most prominent Internet services to say they have already insulated most of the most popular services from Heartbleed.

At Yahoo, the repairs have been made on a list of services that includes its home page, search engine, email, finance and sport sections, Flickr photo-sharing service and its Tumblr blogging service. In a Wednesday blog post, Google said it had applied the Heartbleed patch on its search engine, Gmail, YouTube, Wallet and Play store for mobile apps and other digital content.

Yahoo is advising its users to "rotate their passwords" and add a backup mobile number to the account. That number can be used to verify a user's identity if there are problems accessing the account because of hacking.

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 that 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.

Fixing the Heartbleed flaw still doesn't guarantee people's online data wasn't compromised, said Nathaniel Couper-Noles, principal security consultant at Neohapsis. "The horse may already be out of the barn, so to speak, if passwords or SSL keys were compromised before the patch

was in place," Couper-Noles said. "It may take a considerable amount of effort and money to re-establish a nominal security level."

In a Tuesday post announcing it had installed the Heartbleed patch, 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."

More information: Read: Heartbleed bug find triggers OpenSSL security advisory