Q&A: Experts warn of Bash Bug, what are the risks? (Update)

September 25 2014, by Barbara Ortutay

In this Feb. 22, 2010 file photo, a student uses an Apple MacBook laptop in his class in Palo Alto, Calif. New warnings are emerging of a security flaw known as the "Bash" bug, which cyber experts say may pose a serious threat to computers and other devices using Unix-based operating systems such as Linux and Mac OS X. (AP Photo/Paul Sakuma, File)

Internet security experts are warning that a new programming flaw known as the "Bash Bug" may pose a serious threat to millions of computers and other devices such as home Internet routers. Even the

systems used to run factory floors and power plants could be affected.

So, is it time to panic? Here are some common questions and answers about the latest security scare.

—

Q. What is the Bash Bug, and why is it a big deal?

A. The bug, also known as "Shellshock," is in a commonly used piece of system software called Bash. Bash has been around since 1989 and is used on a variety of Unix-based systems, including Linux and Mac OS X.

Devices that use Unix in some form include many servers, routers, Android phones, Mac computers, medical devices and even the computers that create bitcoins. Systems running power plants and municipal water systems could also be affected by the bug, though security experts already recommend that these systems remain disconnected from the Internet to avoid opening them to such risks.

Bash is a command shell—"the thing you use to tell your computer what you want it to do," explains Christopher Budd, global threat communications manager at security firm Trend Micro. Thus, exploiting a security hole in Bash means telling your computer, or other systems, what to do.

—

Q. Why are people saying it's worse than "Heartbleed," the flaw that exploited security technology used by hundreds of thousands of websites?

A. While Heartbleed exposed passwords and other sensitive data to hackers, Bash Bug lets outsiders take control of the affected device to install programs or run commands.

On the other hand, Bash Bug might be harder to exploit. Heartbleed affected any system running OpenSSL, a common Web encryption technology. With Bash Bug, your system actually has to be using Bash, Budd said. There are multiple types of command shells, so even if Bash is installed, the system could actually be using a different one.

___

Q. It's been a quarter century since Bash came out, so why is the bug a threat now?

A. That's because someone—Stephane Chazelas of Akamai Technologies Inc. to be specific—just found it.

Heartbleed was around for more than two years before it was discovered.

___

Q. Should you be worried?

A. For now, the Bash Bug appears to be more of a potential nuisance than a major threat.

It's a more vexing problem for Mac owners. The Bash Bug makes it easy for hackers to take control of a Mac running on a public Wi-Fi network, such as one in a coffee shop or airport, said Chris Wysopal, chief technology officer of computer security firm Veracode.

At home, a hacker who takes control of an Internet router could

consume so much bandwidth for online mischief that the owner gets hit with a huge bill from service providers that impose monthly data caps, said Dave Lewis, Akamai Technologies' global security advocate.

Another possible security problem: A hacker who seizes control of a vulnerable Web server might collect online passwords stored in databases, said Joe Siegrist, CEO of LastPass, a service that stores and protects passwords. The threat doesn't appear to be as high as with Heartbleed, however.

The Bash Bug could cause massive damage if it's used to create an Internet "worm"—lines of malicious computer coding that wiggle from one vulnerable server to the next. A worm that reaches pandemic proportions could bog down the Internet and even render some services inaccessible. At this point, a worm feeding on the Bash Bug looms as a theoretical threat.

___

Q. What can you do about it?

A. Everyday users can't do much right now, except to wait for manufacturers to release fixes for their products. Budd recommends applying the patches for routers, Macs and other devices as they come out.

Even if a fix is developed, getting it could be another matter. Budd expects that to be an issue with Android phones, because their manufacturers and carriers are often slow to push out the system updates that Google provides.

Of course, it always helps to run up-to-date security software on your devices.

—

Q. Should these recurring security breakdowns cause people to reassess society's ever-increasing dependence on the Internet?

A. Probably, given that the revelations about Bash Bug and Heartbleed surfaced within six months of each other. What's especially troubling about Bash Bug is that it's been hiding in plain sight for the past two decades, even as millions of more machines came online to widen the threat.

Furthermore, these risks are likely to escalate as people store more documents, photos, videos and even medical records over the Internet. At the same time, technology is expected to make it possible to plug just about everything imaginable into the Internet, be it coffee machines or automobiles.

We'll just have to live with technological risks. As Lewis noted, "We are already too far down the road to take a step back."