Malware deadline passes, very few knocked offline

July 9 2012, by BARBARA ORTUTAY

Webroot's SecureAnywhere Complete 2012 software for computer security on display at Best Buy in Mountain View, Calif., Friday, July 6, 2012. Despite repeated alerts, tens of thousands of Americans may lose their Internet service Monday unless they do a quick check of their computers for malware that could have taken over their machines more than a year ago. The warnings about the Internet problem have been splashed across Facebook and Google. Internet service providers have sent notices, and the FBI set up a special website. (AP Photo/Paul Sakuma)

(AP) — If you're reading this online, you're fine. The day that was supposed to see thousands of people knocked off the Internet has arrived, but only a few people were affected.

Thousands of Internet users across the U.S. and beyond waited too long or simply didn't believe warnings that they would lose access to the Internet just after midnight because of malware that took over

computers around the world more than a year ago.

At 12:01 a.m. (0401 GMT) on Monday, the FBI turned off Internet servers that were functioning as a temporary safety net to keep infected computers online for the past eight months. A court order the agency had gotten to keep the servers running expired, and was not renewed.

FBI officials have been tracking the number of computers they believe still may be infected by the malware. As of Sunday night, there were about 41,800 in the U.S., down from 45,600 on July 4. Worldwide, the total is roughly 211,000 infected. An estimated 2.3 billion people around the world use the Internet, according to Internet World Stats.

Considering that there are millions of Internet users across the country, several thousand losing access isn't a big deal — unless you are one of them.

As the deadline approached, Internet service providers such as AT&T Inc. and Time Warner Cable Inc. set up their own safety nets to allow the affected computers to continue to access the Internet.

AT&T said only a "small percentage" of its customers were affected by the virus. To make sure they can continue to access the Internet, the company will maintain legitimate Internet servers for them through the end of the year.

This, said spokesman Mark Siegel, gives people "adequate time" to remove the virus from their computers and avoid service interruption.

Time Warner Cable would not say how many of its customers were affected by the virus, but spokesman Justin Venech said the company also set up its own servers to ensure they can get online. Time Warner has no specific deadline, but the company will notify people who are

affected so they can fix their computers.

Verizon Communications Inc. said it will "continue to provide extended support to our customers during the month of July - while continuing to instruct them on the necessary actions they must take to resolve the issue on their computers."

The company added that it has notified affected customers "using a variety of methods, including email, phone calls, and postal mail correspondence."

In South Korea, there were no reports from affected computers Monday. As many as 80 computers there are believed to be infected with the malware that may cause problems in Web surfing, down from 1,798 computers in February, according to the government.

"The impact will be limited," said Lee Sang-hun, head of network security at the Korea Communications Commission, a government body. The government and private broadband providers opened helplines and issued warnings. They also asked users to check if their computers were infected and to download antivirus software. South Korea is one of the most wired countries in the world, with more than 90 percent of households connected to broadband Internet.

The problem began when international hackers ran an online advertising scam to take control of more than 570,000 infected computers around the world. When the FBI went in to take down the hackers late last year, agents realized that if they turned off the malicious servers being used to control the computers, all the victims would lose their Internet service.

In a highly unusual move, the FBI set up the safety net. They brought in a private company to install two clean Internet servers to take over for the malicious servers so that people would not suddenly lose their

Internet.

And they arranged for a private company to run a website, www.dcwg.org, to help computer users determine whether their computer was infected and find links to other computer security business sites where they could find fixes for the problem.

From the onset, most victims didn't even know their computers had been infected, although the malicious software probably slowed their web surfing and disabled their antivirus software, making their machines more vulnerable to other problems.

Efforts to solve the issue have been hindered a bit by a few factors: Many computer users don't fully understand how their computers work. The cyber world of viruses, malware, bank fraud and Internet scams is often distant and confusing, and warning messages may go unseen or unheeded.

And other people simply don't trust the government, and believe that federal authorities are only trying to spy on them, or take over the Internet, by pushing solutions to the infection. Blogs and other Internet forums are riddled with postings warning of the government using the malware as a ploy to breach American citizens' computers — a charge the FBI and other security experts familiar with the malware quickly denounced as ridiculous.

There is an underlying sense that this has been much ado about nothing — like the hoopla over Y2K, when the transition to the year 2000 presented technical problems and fears that some computers would stop working because they were not set up for the date change. In the end, as in this case, there were very few problems.

Rep. Jim Langevin, who co-founded the cybersecurity caucus in

Congress, said computer users have a responsibility to practice good hygiene and make sure their computers have not been infected or hijacked by criminals.

"These types of issues are only going to increase as our society relies more and more on the Internet, so it is a reminder that everyone can do their part," he said.

Chester Wisniewski, senior security adviser at computer security firm Sophos, said it would have been better to turn off the safety net earlier, so that people can clean up their computers.

"There is only so much responsibility the American government has to continue to run this stuff," he said. "If you still have this virus it's likely that you have others."