Malware may knock thousands off Internet on Monday

July 5 2012, by LOLITA C. BALDOR

This undated handout image provided by The DNS Changer Working Group (DCWG) shows the webpage resulting from not having the DNS malware. It will only take a few clicks of the mouse. But for hundreds of thousands of computer users, those clicks could mean the difference between staying online and losing their connections. Tens of thousands of Americans may still lose their Internet service Monday July 9, 2012 unless they do a quick check of their computers for malware that could have taken over their machines more than a year ago. (AP Photo/DNC Changer Working Group, FILE)

Despite repeated alerts, tens of thousands may still 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.

According to the FBI, the number of computers that probably are infected is more than 277,000 worldwide, down from about 360,000 in April. About 64,000 still-infected computers are probably in the United States.

The Canadian Internet Registration Authority said about 25,000 of the computers initially affected by the malware were in Canada, but now only about 7,000 machines remain infected there, according to Canadian Internet Registration Authority spokesman Mark Buell.

He said his organization, together with Public Safety Canada and the Canadian Radio-television Telecommunications Commission, has developed an online site where computer users can check their computers for the malware.

People whose computers are still infected Monday will lose their ability to go online, and they will have to call their service providers for help deleting the malware and reconnecting to the 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 a 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 while it was the first time they'd done something like that, FBI officials acknowledged that it may not be the last, since authorities are

taking on more of these types of investigations.

The temporary Internet system they set up, however, will be shut down at 12:01 a.m. EDT (0401 GMT) Monday, July 9.

Most victims don't even know their computers have been infected, although the malicious software probably has slowed their online surfing and disabled their antivirus software, making their machines more vulnerable to other problems.

But popular social networking sites and Internet providers have gotten more involved, reaching out to computer users to warn of the problem.

According to Tom Grasso, an FBI supervisory special agent, many Internet providers are ready for the problem and have plans to try to help their customers. Some, such as Comcast, already have reached out.

The company sent out notices and posted information on its website. Because the company can tell whether there is a problem with a customer's Internet server, Comcast sent an email, letter or Internet notice to customers whose computers appeared to be affected.

Grasso said other Internet providers may come up with technical solutions that they will put in place Monday that will either correct the problem or provide information to customers when they call to say their Internet isn't working. If the Internet providers correct the server problem, the Internet will work, but the malware will remain on victims' computers and could pose future problems.

In addition to individual computer owners, about 50 Fortune 500 companies are still infected, Grasso said.

Both Facebook and Google created their own warning messages that

showed up if someone using either site appeared to have an infected computer. Facebook users would get a message that says, "Your computer or network might be infected," along with a link that users can click for more information.

Google users got a similar message, displayed at the top of a Google search results page. It also provides information on correcting the problem.

To check whether a computer is infected, users can visit a website run by the group brought in by the FBI: www.dcwg.org .

The site includes links to respected commercial sites that will run a quick check on the computer, and it also lays out detailed instructions if users want to actually check the computer themselves.

Citation: Malware may knock thousands off Internet on Monday (2012, July 5) retrieved 20 March 2024 from https://phys.org/news/2012-07-malware-thousands-internet-monday.html