Internet doomsday virus appears to fizzle

July 9 2012, by Rob Lever

The so-called Internet doomsday virus with the potential to black out tens of thousands of computers worldwide appeared to pose no major problems Monday after a temporary fix expired.

Security firms reported no significant outages linked to the DNS Changer virus, as many Internet service providers have either implemented a fix or contacted customers with steps to clean their computers.

The problem stems from malware known as DNS Changer, which was created by cybercriminals to redirect Internet traffic by hijacking the domain name systems (DNS) of Web browsers.

The ring behind the DNS Changer was shut down last year by the US Federal Bureau of Investigation (FBI), Estonian police and other law enforcement agencies, after infecting some four million computers worldwide.

Some 210,000 computers worldwide remained infected as of Sunday, including more than 41,000 in the United States, according to a working group monitoring the problem.

On Monday, temporary servers set up by the FBI to direct Internet traffic normally, even for infected computers, were shut down.

But security specialists said most Internet users and providers have had time to work around or fix the problem.

"Although it's not completely over, I think we can count case DNS Changer as a success story, said Mikko Hypponen, chief research officer at the Finland-based firm F-Secure, in a Twitter message.

"Many global operators are keeping their DNS Changer victims online, even after FBI stopped," he said in a separate tweet.

Johannes Ullrich of the SANS Security Institute said that for computers running Windows, the computer "may actually revert to the default settings once the DNS server is turned off."

He added, that "if you used the bad DNS server, chances are that various entities tried to notify you. Google for example should have shown you a banner."

Additionally, Ullrich said the malware is "old enough where antivirus, if you run any, should have signatures for it."

Six Estonians and a Russian were charged in Estonia in November with infecting computers, including NASA machines, with the malware as part of an online advertising scam that reaped at least $14 million.

Because the virus controlled so much Internet traffic, authorities obtained a court order to allow the FBI to operate replacement servers until July 9.

The FBI, as well as Facebook, Google, Internet service providers and security firms have been scrambling to warn users about the problem and direct them to fixes.

A DNS Changer Working Group has been monitoring and educating people about the malware, with a website www.dcwg.org.

FBI spokeswoman Jenny Shearer said the temporary servers were indeed halted and that the agency had no reports of outages.

"I'm not aware of any problems," she told AFP.

"If members of the public are not able to use their Internet they should contact their Internet service providers."

The working group website said traffic directed to the servers that were under temporary control "will be monitored by several service providers and security organizations to insure they are not maliciously hijacked."

Experts said that if a computer is infected, they could still access the Internet by reconfiguring the way they access the domain name system.

Instead of entering an address such as ebay.com, they could use the underlying address, which is a series of numbers, said Marco Preuss of the Russian security firm Kaspersky on the company's Securelist blog.

"If you know the address of the server you can still use it instead of the name, e.g. 195.122.169.23 is 'securelist.com' but this is not an easy solution," he said.

Others with more technical savvy can also reprogram their computer's network settings, to access public DNS servers such as one operated by Google.