Thousands risk Internet shutdown as US fix expires

WASHINGTON, US: Tens of thousands of people around the world whose computers were infected with malware may lose their Internet access on Monday after the expiry of a US government fix, security experts said.

However, no trouble was reported in the early hours of Monday. The problem stems from malware known as DNS Changer, which was created by a gang of cybercriminals to redirect Internet traffic by hijacking the domain name systems of Web browsers.

The ring behind the DNS Changer virus, discovered in 2007, was shut down last year by the US Federal Bureau of Investigation (FBI), Estonian police and other law enforcement agencies.

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 US$14 million.

Because the virus controlled so much Internet traffic, authorities obtained a court order to allow the FBI to operate replacement servers that allow traffic to flow normally, even from infected computers.

Shutdown

However, those replacement servers were to have been shut down at 0401 GMT, when some experts say infected computers could face an "Internet doomsday." "DNS Changer is an insidious form of malware affecting everyone from the everyday consumer to a large chunk of the Fortune 500," said Lars Harvey, the chief executive of security firm Internet Identity.

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. According to a working group set up by experts, more than 300 000 computers remained infected as of 11 June.

The largest number were in the United States (69 000), but more than a dozen countries, including Australia, Britain, Canada, France, Germany, India and Italy, are also believed to have infected computers. Security experts say it is not clear how many of those computers are active.

"Reaching victims is a very hard problem, and something we have had issues with for years," said Johannes Ullrich, a researcher with the SANS Security Institute. However, he said he expected the impact to be "minimal" because many of these systems are no longer used or maintained.

Test your PC

Internet Identity said last week that at least 58 of all Fortune 500 companies and two out of 55 major government entities had at least one computer or router that was infected with DNS Changer. That compares with figures in January, when half of Fortune 500 companies and US federal agencies were infected.

IID said the malware also compromises computers by preventing antivirus software updates, thereby exposing infected machines to even more malicious software. Users who think they are infected may perform a test at the DNS Changer Working Group's website http://www.dcwg.org/ or others operated by various security firms.

For computers affected, the blackout will be total, experts say. "Connectivity will be lost to the Internet PERIOD," said a blog posting from the security firm Symantec. The virus was designed by six Estonians, whose arrest was announced by the FBI in November.

According to the bureau, the gang used the DNS Changer to infect about four million computers in more than 100 countries in a scam launched in 2007. There were initially about 500 000 infections in the United States, including computers belonging to individuals, businesses, and government agencies such as NASA, the FBI said.

Source: *AFP* via I-Net Bridge