LEAD SOCIETY

INTERNET DOOMSDAY TO HIT INDIAN USERS

DNScharger is a malware (malicious software created to gather sensitive information) that changes the domain name system (DNS) settings on the compromised computer (see box for details). DNS is an internet services that allows computers to talk to each other.

According to estimates from US government agencies, about 250,000 computers are still infected with the malware world-wide and only 64,000 of those computers are in the US.

The problem is that when the malware infested the systems it changed the users DNS server IP address (this is unique to each user). While FBI did put clean servers, these DNS server IP addresses have not been changed. Hence, on Monday, an infected system will not be able to access the internet. There are tools that McAfee has provided for users if there systems is infected. Before that, they can also find out if their system is infected as well, said Vinoo Thomas, product manager, McAfee Labs.

The blackout will not only impact Windows systems, but also Mac users and people who have set up home routers.

The internets doomsday event is almost two years old. In 2007, a group of hackers had operated an online advertising scam to take control of 570,000 infected computers around the world. The hackers were able to manipulate internet advertising to generate at least $14 million in illicit fees.

When FBI decided to take down these hackers a year before, they realised that turning off the malicious servers would mean the users losing their internet services. FBI initiated lsquo;Operation Ghost Click and took over the DNS infrastructure of the Botnet and replaced it with legitimate or clean servers.

But this act by FBI was legally bound with a specific time-frame, which was set to expire on March 8, 2012. FBI later had set July 9 as the deadline to clean the DNSChanger malware. Hence, on Monday, July 9, a large number of internet users across the world, who are still infected by the malware, will not be able to access internet.

Govind Rammurthy, chief executive officer and managing director, eScan Microworld, explained all systems infected with the malware would be affected by the blackout on Monday, that will begin from 9.31 am in India. About a minimum of a quarter million people in the world will be affected by this. The only way to ensure that ones device is not affected is to ensure that an Antivirus to detect and clear the DNSChanger malware, he said.

What is internet blackout all about?

Domain name systems (DNS) is an internet service that converts user-friendly domain names into the numerical IP addresses that computers use to talk to each other. When you enter a domain name into your web browser address bar, your computer contacts DNS servers to determine the IP address for the website.

Internet doomsday to hit Indian users

By changing a computers DNS settings, malware authors can control what websites a computer connects to on the internet and can force a compromised (infected) computer to connect to a fraudulent website or redirect the computer away from an intended website. To do that, a malware author needs to compromise a computer with malicious code, which in this case is DNSChanger.

If your computer is still using DNS entries that are pointing to the FBI servers on July 9, you will lose total access to the internet.

Solution: Websites have been created by security solutions provider and by a task force called DNSChanger Working Group (DCWG). Users can use any of the links below to check whether their systems are infected.

www.dcwg.org
http://www.dcwg.org./detect
www.mcafee.com/dnscheck