CXOtoday.com
IT Perspective for Decision Makers

DNSChanger: Not a Major CIO Threat

by Sohini Bagchi Jul 09, 2012

DNSChanger malware has already created ripples across the globe and thousands of internet users in India are expected to lose access as the Federal Bureau of Investigation (FBI) shuts down temporary domain name system (DNS) servers. According to a report, with over 20,000 infected IP addresses, India is among the third largest DNSChanger malware-infected country. The US tops the list with 65,000 infected IPs, followed by Italy with over 26,000 infected IPs. In such a scenario, security experts and FBI warned enterprises and general PC users across the world to ensure that their systems are not infected.

As rogue servers were used by cyberspace criminals to reroute traffic from the infected PCs, FBI planned the shutdown so that the infected PCs cannot access the Internet. Most Indian enterprises however opined that DNSChanger is going to have minimal impact on corporate network.

Less Impact on Corporate Network

Most business and technology leaders believe that the DNSChanger malware is mostly targeted to the end-

user consumer PCs, although roughly 50 Fortune 500 companies have been found to have DNSChanger on some of their computers.

Several Indian CIOs/IT managers said that they are equipped to deal with the malware as they remain vigilant and monitor their systems and networks closely.

“Our company uses several layers of security to defend against DNSChanger and other security threats. However, there was no indication of DNS Malware,” said Arindam Acharya, Head - Technical Services at Madras Cements.

“We have tested our computers to make sure they are safe. We use a powerful security system that easily spot and remove malware. Our entire IT and support team is also on alert if something has gone undetected,” asserted Anil Kuril, AGM IT, Union Bank of India.

Tamal Chakravorty, CIO at Ericsson India Pvt Ltd however said even though it is not a major threat for CIOs, the need of the hour is to remain agile. “The IT team should back up their data before determining if a computer is infected. They should also take immediate action if they find systems getting infected, instead of delaying the issue further.”

“The impact of DNSChanger would be minimal on corporate networks due to the sheer fact that large networks have their own set of DNS Servers deployed in their own premises. However, we cannot rule out the existence of an infected DNS server within the premises as most of the DNS servers use the DNS entry present in the OS for “DNS look-up queries” and DNSChanger bot does exactly the same. Hence, CIOs should ensure that the security solutions deployed in the network are updated,” said Govind Rammurthy, CEO & MD, eScan.

CIOs On Alert

To combat the DNSChanger and associated viruses, the FBI has come up with a fixed guideline through which enterprises and general PC users can identify whether their computer system is affected by the DNSChanger or not. The DNSChanger Working Group also has a list of free removal tools from major computer security firms including Kaspersky, McAfee, Symantec, e-Scan and Trend Micro which CIOs can use if some computers are found to have DNSChanger malware.

But Acharya of Madras Cements suggests that before you use any of these tools, you need to backup your personal files. It is also important to reformat your hard drive and reinstall your OS. Chakravorty of Ericsson believes that robust scanning of your PC can remove the virus completely.

According to Information Security Analyst Kiran Belsekar, “Enterprise technology decision makers need not panic because their security systems are generally well monitored. Moreover, with various antivirus firms and working groups combating this menace, block will be only on internet access of PCs that are infected.

Ramamurthy believes if corporates do not adhere to security policies, they might be at a higher risk. Hence, DNS related helpdesk calls should be treated with high priority. Belsekar added that DNSChanger will have minimal effect among Indian enterprises, even though CIOs should – as part of their task - be constantly on alert.