CYBER MEDIA
CIOL
MAKING IT YOUR ADVANTAGE

DNS Changer causes minimal damage to India

Top security vendors observed that the impact of the Internet malware DNS Changer is minimal in India compared to the US and other countries

Pankaj Maru

Tuesday, July 10, 2012

MUMBAI, INDIA: The much talked about and discussed Internet doomsday on 9 July, 2012, has finally fizzled out without much of an impact in contrast to what many security experts had expected globally.

India, like the US, was among the many countries, that were expected to be hit by the DNS Changer malware; however, according to top security and anti-virus firms, the nation with over one billion population and growing Internet users, reported a minimal damage with some unconfirmed instances.

According to Govind Rammurthy, eScan CEO and MD, India is amongst the top 5 countries to suffer from the infection due to DNS Changer malware and about 19,991 computers were affected due to Internet shut down on 9 July; however, the impact was minimal in India compared to the USA, which had more than 50,000 infected machines.

“Majority of the ISPs had already configured substitute DNS servers, while many had taken precautions to ensure that their customers do not suffer from any hindrance in the services. DNS Cache of the affected PCs is still in effect, hence only after the cache expires, will the true picture be revealed,” added Rammurthy.

Also read: DNS Changer: Indian ISPs say alls fine

"As of now various unconfirmed reports indicate that few thousand machines have been infected in India due to the DNS Changer and its variants. Clean-up is going on, backed by leading industry aggregated members, including ISPs and security firms and the infection numbers are getting reduced,” said Altaf Halde, managing director, Kaspersky Lab- South Asia.

“Noteworthy is that this particular malware (DNS Changer) and its variants like Shadowbot have been in existence since 2007. Much of cleaning up activity has already happened and now the infections have drastically come down. The 'Internet Blackout' may impact the still-infected machines,” Halde added.

Users with pirated software programs and operating systems along with computer devices running without any security tools have been impacted by DNS Changer.

However, many Internet Service Providers (ISPs) had taken precautionary steps to counter the malware and safeguard their users and customers in India. This helped in reducing the expected damage that FBI had announced back in November 2011.

"We predicted that there will be minimal impact of this shutdown on 9 July, due to

timely and sustained awareness campaign by all stakeholders, the investigators (FBI and other agencies), the ISPs especially in the US, the security vendors and lot of media hype and buzz around across social media, blog posts, etc.," said Baburaj Varma, Trend Micro's head – Technical Services for India and SAARC.

"Our support center in India received very few calls mostly pertaining to enquiry on the subject rather than real support issues due to this shutdown," Varma pointed out.

Trend Micro's back-end threat research team found that there was no general Internet meltdown but rather a loss of connectivity by certain individuals and corporations that were compromised by the botnet.

Further it found that the scope of the compromise is not that promiscuous and the counter measures and information drives put into place by various groups had lessened the impact of the attack.