CTOFORUM
Technology for Growth and Governance

Apple's Siri is a Big Threat

21 June 2012 13:07 pm , Varun Aggarwal

In a conversation with Varun Aggarwal, Govind Rammurthy, CEO & Managing Director, eScan shares insights into Anonymous operations in India and the state of security in the country

What evidence do you have to support the fact that Anonymous attacks on the Indian government were undertaken by their Indian recruits?

Though Anonymous is a global idea but identification of local government sites and organizations can be done effectively by the active support of local hackers. In the past, when individual countries were being targeted, it was done by their own netizens with a little help from outside. Incidentally, the language / slang used by the @opindia_revenge suggest that it is managed and operated by an Indian or a group of Indian hackers.

Do you see the recent spurt of targeted attacks in India as purely hacktivism attacks or there seems to be some other motivation?

Hacktivism in India is related to;

1: Recognition by the peers within Indian hacking circle and globally too.

2: Recognition and the ability to make the voice heard by thousands, if not millions.

3: Staying anonymous, yet being a part of a rebellion and the thrill which it provides coupled with the access and implementation of destructive power over the Internet that is not possible under normal real-world circumstances.

4: Most of the Indians are of the belief that as long as no human / animal / property was physically hurt/destroyed, it is not called a destruction. Hence, in most of the recent Anonymous attacks on Indian installations, we have observed this trend - web-pages are added with a message that nothing was deleted only a page with the message was added.

For past few years, the new generation has been watching in apathy the political trend and the helplessness of everyone around them, but they have also see the rise of Anonymous and the effect Anonymous has over others. #Occupy movement has inspired many youngsters and has turned hacking into a culture or a religion.

India is geographically far away from USA but on internet, they are neighbours and many hacktivists share common ideologies. Geography just does not come into picture.

Do you see any business impact of Android malware for an enterprise? Please explain.

Yes. Not only Android based-malware but also certain legit services e.g. Siri

(Apple's iPhone voice activated personal assistant) have wide range implications for the Enterprises. BYOD (Bring Your Own Devices) at work culture is a dangerous concept as most of the devices fall in the category of mobile devices (Smartphones, Tablets) which are internet enabled. This is a security hazard with respect to Transfer of confidential files, Photos being taken, etc. In case of Siri, every spoken command is sent to the servers of Apple for processing, but the terms and conditions of Apple speak about data sharing and using data for enhancing user experience. This is harmful for an organization as confidential data may land up on Apple servers.

An infected android device may act as Botnet or may even steal the login credentials for your corporate mail logon. Whether an android malware or a legit app such as Siri - both have direct implications on the security of an enterprise and its business.

What according to you is the state of PCI-DSS compliance in India? Do you see online merchants flouting the compliance norms and storing more personal data than required?

PCI-DSS is all about storing of CC related data and its secure transmission over open and public networks. However, connectivity between the POS and the back-end server is a concern. Many of the high end-attacks e.g. TJX happened at the server level by way of MITM - in-transit data packets were sniffed. How many organizations follow PCI-DSS compliance is one aspect, what type of data security is being deployed to ensure safe transmission of data, within LAN/WAN is the second aspect and the last aspect is where-else and how-much of this data is shared.

Retail malls do store personal data including the entire CC number and other details. It is quite evident from the fact that they swipe the card on two different systems - first one is the POS and second is the merchant POS. e.g. Star Baazar, try asking the attendant to swipe the card only once (merchant POS provided by bank) and they will simply refuse citing Company Policy and account audit.

However, when it comes to online merchants, it is difficult to ascertain about the storage of personal data and nothing can be said about the payment gateways processors. In addition, amount of much information is shared between the Payment Processor and the merchant is difficult to ascertain.

IT Rules clearly mention that organisations need to notify on their website what personal data they are storing. Do you see Indian organisations following this so far? Has the government so far failed to enforce the law?

None of the sites analyzed during our research have provided any type of information about what they are storing and how they are storing the data, even if it is stored then it was not within the reach of a normal search.

FAME-Cinema's online site, stores the user password in their database in PLAIN TEXT. We arrive at this result by knowing what information we are providing i.e. address, contact numbers while filling up the registration form or while using the ‘Forgot Password’ feature.

Failure by websites to notify their users about the information being stored and in what manner is a dead-give-away about the failure of government to enforce the law.