

### Top security trends to watch for in 2012

India will emerge as the largest hub of Botnet and anonymous proxy services by the end of 2012, says Govind Rammurthy of eScan

By Govind Rammurthy , eScan, January 17, 2012



Tweet

The year 2011 was one of the landmark years for high-profile cyber attacks. As the trend is said to continue in 2012 with more sophisticated and targeted attacks, security is a major concern for the IT users of all the segments from Home Users to SMB to Enterprise.

The year 2012 will build the foundation for India's future IT-related crimes. Hactivism will gain momentum. Anonymous, which is mostly active in European Countries and the US, will be seen making active inroads into Asian Countries, especially in India in 2012. India will see a sharp rise in both money mules related activities and credit card-related crimes. As the list of petty criminals is huge in India, the activities of money mules will be outsourced to the country.

The number of data thefts has tripled in the past five years and the graph tends to rise with every passing year. Right from the Government, corporate, data centres and small to medium-sized companies, all have been targeted. With the introduction of IT consumerization, issues such as managing and supporting consumer devices and securing data from criminals, malware and other threats have emerged. Mobility in enterprise sector brings new challenges for managing data, as well as the wide range of devices in the network.

Social engineering attacks pose great risk to large amounts of valuable data that SMBs hold due to lack of data security budgets. Hence, the need to look beyond the basics of policy and procedure development to more advanced technologies such as network monitoring, data leakage prevention, and log file analysis arises. Social engineering tactics on social media that drive its users to disclose sensitive information and download malware are skyrocketing with its increasing popularity, especially amongst the SOHO users.

Used for various tasks from launching DDOS attacks to spamming, and recently being used to provide paid anonymous browsing proxy services, Botnets have always been a pain to organizations and security researchers worldwide. In 2012, India will be the largest host for such services.

Unauthorized access coupled with data pilferage is generally termed as hacking, and generally organizations treat these cases quite seriously. But when unauthorized processes are not leaking out the organization's data but are utilizing their resources then it is termed as a virus/malware/Trojan or simply a failure of the organization to deploy a proper AV solution. Well no matter if there is a hack or an infection, every unauthorized resource access is to be dealt and handled. Bandwidth availability on the other hand is increasing exponentially while the cost to avail the bandwidth is decreasing.

Though corporates may take these issues seriously, however, security awareness is taken seriously when it comes to SMBs and home users. Based on this perception, we believe that

India will be the largest hub of Botnet and anonymous proxy services by the end of 2012. We have recently seen IP addresses of SMBs and home users with broadband being used by paid anonymous proxy services.

Stuxnet and Duku require access to the internal networks but with freely available service like ShodanHQ being made available and the latest telnet exploit making rounds in the security circles, it would not be a surprise to find an automated attack on embedded devices, which are exposed on Internet, being taken over by rogue entities. Rogue entities/states having their own database of vulnerable IPs, similar to ShodanHQ are just waiting to be exposed. And if this exposure ever takes place, it is going to raise a lot of questions, especially related to espionage.

In the past, we have seen non-compliance of PCI-DSS by some of the top-most organizations, whether it was Sony or STRATFOR or Heartland. And in the year 2012 such threats will intensify with the increasing number of shopping malls that store entire credit card and debit card data on their personal servers and their employees are encouraged to swipe the card into their own POS along with the one provided by the banks. It is only a matter of time until someone hacks into these and finds a treasure trove of information.

Phishing will never cease to exist. Until, email servers and domains are non-compliant to at least one industry standard i.e. DKIM or SPF with strict enforcement, phishing is not going to stop. According to Mayan calendar, there is no 2013. This will lead to lots of phishing mails/scams, especially in the first half of November/December. Phishing mails with malware attachments, malware laced URLs, or plain data stealing website clones can always be expected. Hence as a security vendor, we will be enhancing our content scanning and detection of phishing/malware sites to combat the ever increasing database of URLs.

India has seen a jump in sales of smartphones and the cheaply available Android-based tablets for less than Rs 3,000 i.e. approx 56 USD. Hence, the market of mobile malware is now evenly balanced with the conventional version. When a particular piece of technology/hardware is available so cheaply, it garners extreme interest in all the circles and in turn grabs a huge market share.

Tablets provide computing power as well as mobility, and add a new segment of IT users but nothing much can be said about their security awareness. Premium rate SMS/Call hacks, Premium Image downloads will occur along with this data-harvesting and tracking apps will increase. Not only Indians but the rest of the smartphone / tablet users will be at risk. Long URLs have already proved to be excellent USP for phishing syndicates, QR codes for long URLs won't be much far behind. After all, the display screen size and font size does matter. QR codes often do not accompany the visually displayed links, which they are supposed to represent. This is one big flaw and can / will be exploited.

Last year we saw rise of a handful of fake antivirus software that were capable of tricking the users to believe that their computer is at risk or is already infected. Such fake security software are one of the most common and dangerous threats on the Internet today.

In addition, the increasing use of Mac products has created more opportunities for cybercriminals. Malware targeted solely at Mac users are increasing at the rate of approximately 10 percent each month. In 2012, the number of malware specimens for Mac will continue to grow.

We realise that year 2012 is expected to be more explosive in terms of threat landscape. With this, the demand of security software that remains ever Argus-eyed and gives proactive unparallel protection to the networks, applications and data arises. eScan, as a security vendor will be concentrating on creating new technologies that ensure effective security and data integrity of IT users and thereby, adding confidence to their computing experience.

*The author is MD&CEO, eScan*

