ORF ISSUE BRIEF

SEPTEMBER 2011 ISSUE BRIEF # 32

Virtual Alarm: Social Engineering Attacks Imperil Cyber Security

Rahul Prakash

Cyber security threats have amplified significantly in the last decade, creating security concerns across the globe. Media reports during this period on illegal cyber activities have highlighted how information network systems have been exploited by cyber criminals—as well as States—on numerous occasions for espionage and intelligence gathering.

Even as "experts" on cyber warfare find ingenious ways of conducting their operations, what perhaps makes it easier for them is our sheer dependence on the Internet for everyday communication. Moreover, social networking makes us highly vulnerable to cyber attacks that are carried out by a simple but highly effective technique called "Social Engineering"—a technique where deception or persuasion is used to gain access to information.

According to Symantec, a cyber security firm, the social engineering technique was used in some of the most successful cyber attacks in 2010. In this, the role played by targeted individuals is a crucial factor and needs to be examined. Despite having security mechanisms in place, it has been found that social engineering techniques have tricked individual targets to reveal vital information resulting in serious consequences such as facilitating a cyber intrusion into the network system used by the individual. In a broader sense, Social Engineering methods can be used for gaining information by deceiving victims through other means as well, such as telephone calls and also direct interaction. However, this paper will focus on cyber security concerns related to Social Engineering. The following sections will examine the concepts of Social Engineering and Zero-Day Vulnerability and

give a few instances where a combination of both resulted in "compromise" of confidential information, raising security concerns for nations.

Social Engineering

In a Social Engineering attack, the attacker does in-depth research about the victim on the Internet and maps his/her virtual life (often with the help of social networking websites). Information regarding the victim's close friends, likes and dislikes, habits and social life are observed over a period of time. This general information, which one considers harmless, plays a critical role in facilitating an attack. This information helps the attacker to bond with the victim at a personal level and then gain further information enabling him to launch an attack. The United States Computer Emergency Readiness Team (US-CERT) defines Social Engineering as a technique:

"(When) an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility."[1]

Zero-Day Vulnerability

This is a vulnerability in a software, which has not yet been discovered by its developers. The hacker finds the flaw in the software before the software developing company finds it and since the attack begins before the first day of the developer's awareness about the vulnerability, it is called a "Zero-Day" vulnerability attack. When combined with a well-crafted social engineering technique to know the target computer's defences, the attacker gets access to the information stored in the target computers. Upon discovering further vulnerabilities in the network systems, the attacker can access computers connected to the initial target and remains undetected for a long time until the Zero-Day Vulnerability is discovered.

The most prominent example of the exploitation of a "Zero-Day" vulnerability is the case of the "Stuxnet" attacks, which used four different Zero-Day vulnerabilities. The attacker used the unknown vulnerabilities in the protection systems and infiltrated deep into the target systems which allegedly crippled the Iranian nuclear programme. In 2010, 14 new Zero-Day vulnerabilities were found in most commonly-used software such as Internet Explorer, Adobe Reader and Adobe Flash Player.[2]

Another factor abetting cyber crime is the availability of "attack tool-kits" on the Internet which are accessible to "underground" hackers. Once a vulnerability is discovered, attack tool-kits are made to exploit loopholes along with tools to customise, deploy and automate widespread attacks. A key feature offered by some of these kits is the Command and Control System which makes it easy for the hacker to launch and control the attack. In fact these kits also come with a facility to update the versions of tools, which actually improve the marketability of the product. Such kits are

advertised and sold in what is called the online underground economy (black market for cyber criminals).

The Role of Social Networking Websites

Today more than a billion people are connected to an array of social networking websites. They put their trust in these websites with information about themselves. They are, thus, are a favourite hunting ground for cyber attackers. Facebook, by far the most popular of these sites, has been widely criticised for its lax security settings which enable malicious applications to access the personal information of users.

During Operation Aurora, a high profile cyber attack, hackers sent links to malicious websites using social networking websites such as Facebook and then used the Zero-Day Vulnerability in Internet Explorer to download the malware into the target's system.[3] In the light of these events, social networking websites have tried to address concerns of users by strengthening their security and privacy features.

However, hackers have found ways to infiltrate even these by exploiting the negligence of users. While general users face common cyber attacks threatening their privacy, users who work on confidential matters, whether in a corporation or government agency, are more vulnerable targets because of the nature of their work or employment.

Recent Attacks

There have been numerous cases where victims willingly gave information regarding Internet security which only facilitated the cyber attacks that followed. During the cyber attack on US government officials' Google email IDs in June 2011, the attacker identified the targets well before launching the operation.

The attacker used social engineering techniques to identify the close friends and colleagues of the target and then sent emails using spoofed email IDs pretending to be a close friend of the target. The target, trusting the person sending the malicious email, clicked the link which redirected him to a fake Gmail page requiring Gmail Id and password. It is said that the page already had the email ID field filled with the target's email ID, making it look legitimate. Once the target entered the email ID and password, the attacker accessed the email account and tweaked the account to automatically forward the incoming and outgoing mails to an email ID which the attacker could access. This gave the attacker the ability to closely monitor the target's email communication leading to compromise of information.

The US government denied the compromise of any confidential data but issued an advisory asking its employees to avoid using personal email accounts to discuss official matters. This shows the damage that was done by a well-executed social engineering plan which could have potentially led to compromise of classified documents. The cyber attack was traced to Jinan, China—a base for one of People's Liberation Army's Technical Reconnaissance Bureaus.[4]

The alleged Chinese cyber attack on several companies, including Google, which was exposed in January 2010 also used social engineering for reconnaissance of employees working in these

companies.[5] According to Verisign iDefense Security Intelligence Services, these attacks were "unusually sophisticated" and access was gained to company networks by sending targeted emails to employees whose systems contained malicious PDF documents. A Zero-Day vulnerability in Adobe's Acrobat Reader was exploited to gain access to information networks of targeted companies. Apparently the malicious code installed in the target computer was transferring massive amount of data to a server that received the stolen information.[6]

Another interesting example of how social engineering can be used to access network systems of companies was provided by an organisation called Social-Engineer.org. With the clearance from the Federal Bureau of Investigation, Social-Engineer.org organised a competition wherein participants were allotted American companies as targets and the task to extract vital information using social networking techniques, with an aim to expose the weaknesses in the security systems of these companies. In a report, the organisation stated, "when employees do not have clear guidelines set in place to a given situation, they will default to actions that they perceive as being helpful. This natural response was what was utilised in every instance where contestants obtained high scores." The report also pointed out that social media was a low effort vector for information gathering that very few organisations were addressing. The common sources of information used by almost all contestants included Google, Facebook and LinkedIn.[7]

As highlighted in the above sections, a well-orchestrated social engineering attack could lead to compromise of vital information. If it is followed with a Zero-Day vulnerability attack, it could prove to be even more damaging. The utilisation of these methods by State actors is another factor which qualifies it as a major threat. The alleged use of this technique by certain States against government agencies and officials of rival States shows the level of threat it poses. India has been one of the targets and faced a number of cyber attacks, some of which have had Chinese fingerprints.

The social engineering attack, where the victim's role is often the most crucial one, is a simple but at the same time very sophisticated attack. Due to the growing popularity of social networking it has become even easier for hackers to catch a prey. Symantec's Internet Security Threat Report, 2010 stated that, it wasn't necessarily a senior employee who was targeted, even a junior level employee could hold the key to gain crucial information.

A breach using a low level employee's negligence can give attackers an opportunity to launch additional attacks using the credentials of the compromised user. Organisations have taken preventive steps like blocking access to social networking websites at workplaces but this doesn't secure the employee from being a likely a target as he /she could very well be attacked during after-work hours. Even if we put in place advanced security systems, the ultimate responsibility would rest with the user.

With both government and private sector organisations as targets, national security and economic concerns are paramount. It can be assumed that vital government networks are protected more than a private firm's networks due to the nature of information that is being dealt with.

But the question that arises is: how informed are the people who deal with such information and how vulnerable do they remain to cyber attacks even outside their office premises.

Cyber attacks are traced to different parts of the world, making it difficult to punish the culprits. The alleged involvement of States in such activities makes it even more difficult to decide the course of action to be taken to deal with such issues. However, it is essential that at a macro level, a country needs to have a cyber strategy in place and create appropriate agencies that can deal with such threats.

Conclusion

According to the Symantec Internet Security Threat Report, the total number of web attacks increased by 93 percent in 2010 with Symantec alone encountering more than 286 million variants of malware. The number of targeted attacks on companies and governmental organisations continued to grow in 2010; Operation Aurora and Stuxnet being the most prominent. These figures clearly indicate the likelihood of more sophisticated attacks in the future.

As India improves its Internet connectivity, the dependence on the Internet will also increase. From 2000 to 2010, the number of Internet users in India increased from approximately 5 million to 100 million.[8] The total number of Facebook users in India has reached 25 million in 2011.[9] Hence, a significant increase in cyber attacks using Social Engineering or other means is quite possible. Indian national security establishments have been favourite targets in a number of cyber attacks that were traced to other countries, including China.

As a counter measure by India, the Computer Emergency Response Team (CERT – IN) has been setup as a nodal agency for responding to computer security incidents. From a larger perspective, there is a need to enhance the cooperation between different agencies that exist within the country to counter these threats.

Also, a cyber strategy needs to be put in place which clearly defines the role played by various organisations dealing with such issues and defines the stance India takes on cyber offences. Such a move will strengthen the existing mechanisms and send a strong message to the international community about India's seriousness in dealing with such issues. The US recently announced its cyber strategy which views cyber attacks as a domain of warfare; it subsequently announced its cooperative cyber strategy with Australia.

There is need for an international Code of Conduct on cyber activities. Recently China, Russia, Tajikistan and Uzbekistan have jointly submitted a Code of Conduct for Information Security in the United Nations. They have requested UN Secretary General Ban-Ki-Moon to circulate the code during the 66th session of the General Assembly. However, a consensus may prove elusive. As the cyber world has no international boundaries, international cooperation between countries is highly important to tackle the issue of cyber security.

Lastly, since there is a lack of awareness about dealing with such issues at the individual level in many departments of the government, education of the individual becomes the most crucial element in countering such threats, especially in the case of Social Engineering related threats. In fact, Social-

Engineer.com's report states that security through education is the foundation of every solution. In the cyber world, it's said, there exists no patch for human negligence.

ABOUT THE AUTHOR
Rahul Prakash is a Research Assistant at Observer Research Foundation, New Delhi.

Endnotes

1. Mindi McDowell, Avoiding Social Engineering and Phishing Attacks, *Cyber Security Tip ST04-014 US-CERT*, available at http://www.us-cert.gov/cas/tips/ST04-014.html (accessed on September 15, 2011).
2. Symantec Corporation, Symantec Internet Security Threat Report: Trends for 2010, April 2011.
3. Kim Zetter, "Google Hack Attack was Ultra Sophisticated, New Details Show," *Threat Level,* January 14, 2010, available at http://www.wired.com/threatlevel/2010/01/operation-aurora/ (accessed on September 12, 2011).
4. Amir Efrati and Siobhan Gorman, "Google Mail Hack Blamed on China," *The Wall Street Journal*, June 02, 2011, available at http://online.wsj.com/article/SB10001424052702303657404576359770243517568.html (accessed on September 16, 2011).
5. Warwick Ashford, "Social Engineering was Key to Google Hack," *Computer Weekly*, January 26, 2011 available at http://www.computerweekly.com/Articles/2010/01/26/240062/Social-engineering-was-key-to-Google-hack.htm (accessed on September 16, 2011).
6. Kim Zetter, "Google Hackers Targeted Source Code of More Than 30 Companies," *Threat Level*, January 13, 2010, available at http://www.wired.com/threatlevel/2010/01/google-hack-attack/ (accessed on September 17, 2011)
7. Social-Engineering.org, Social Engineering: Capture the Flag Results – Defcon 18, Social-Engineering.org, 2010.
8. Internet World Stats, India: Internet Usage Stats and Telecommunications Market Report, available at http://www.internetworldstats.com/asia/in.htm (accessed on September 17, 2011).
9. "Facebook has 25 million users in India," *IBN Live*, April 29, 2011, available at http://ibnlive.in.com/news/facebook-has-25-million-users-in-india/150696-11.html (accessed on September 17, 2011).

Observer Research Foundation,
20, Rouse Avenue, New Delhi-110 002
Phone: +91-11-43520020 Fax: +91-11-43520003
www.orfonline.org email: orf@orfonline.org