Journal of Engineering and Applied Sciences 8 (7): 225-229, 2013
ISSN: 1816-949X

Hacking and Cyber Crimes: A Preventive Guide

[1]Akram Moustafa, [2]Mohammed M. Al-Shomrani,
[1]Abdusamad Al-Marghirani and [3]Ahmad A. Al-Rababah
[1]Northern Border University, KSA, Arar, Saudi Arabia
[2]Department of Mathematics, King Abdulaziz University,
21589 Jeddah, Saudi Arabia
[3]Hail University, KSA, Hail, Saudi Arabia

Abstract: Network and web security are continuously evolving subjects in both industry and research. Both sides and players of security (i.e., attackers and controllers) continuously try their best to find new ways and techniques to access or protect. This talk will include some of the new trends in web and network security in terms of detection and prevention. The importance of security in IT field and the unawareness of most of the users in hacking techniques which make them victims of cyber attacks had been discussed in this study. This study analyses, the important types of cyber crimes like hacking, Denial of Service (DoS) attack, virus dissemination, digital piracy, IRC crime, credit card fraud, spamming, phishing, spoofing, salami attack, net extortion, social engineering attack and propose various techniques of countermeasures. It is required to categorize, the cyber criminals to several groups to better match their respective goals is to examine the destructive phenomena in cyberspace, mainly the use of modern information and communication technologies for hostile and criminal purposes. Therefore, researchers will consider such phenomena as cyber war.

Key words: Online criminals, cyber criminals, cyber crimes, hackers, intruders

INTRODUCTION

The information society has a significant positive impact on the future of each country in particular at the level of the development of transport, financial and technological areas to accelerate economic and social development, strengthening national defense and security. But, the development of information gives rise to complex and adverse effects. Scientific and technological progress on the one hand allows the creation of computer and telecommunications systems, stunning used both in daily human activities and the special branches of such activities and on the other hand, the same system can be subject, destructive activities, such as computer crime. In addition modern information society reached a level of development when one of the main forms of war beginning of the 3rd millennium, as it is not sad is an information war is global or regional scope increased use of global information infrastructure in all spheres of state and public life resulted in the formation of a new field of activity for criminals. Such concepts as cyber crime offences in the sphere of high technologies, computer crime you can select the following types of cyber crimes and illegal acts in the field of computer information (Mathew *et al.*, 2010):

- Violent or other potentially harmful, infringing upon the physical safety, human life and health
- Cyber crimes, in violation of the confidentiality of data floating around in the information and telecommunication systems of different objects (such crimes aimed at disclosing sensitive information without its destruction, modification, destruction, reorder)
- Cyber crimes, in violation of the integrity of the data, their availability to legitimate users and administrators (denial of service) which can disrupt the established modes of information and telecommunication systems of various purpose (such crimes could cause property damage but they are not linked to the theft of sensitive information, data, money)
- Cyber crimes against property, property rights and the ownership of the information and copyright
- Cyber crimes against public morals
- Cyber crimes against public security
- Other cyber crimes

These include traditional crimes infringing on various objects protected by law but by using information and telecommunication systems. This group includes the

Corresponding Author: Mohammed M. Al-Shomrani, Department of Mathematics, King Abdulaziz University, 21589 Jeddah, Saudi Arabia

crime, a sign of which is that they can all be done without the use of information and telecommunication technologies that play a supporting role. The most likely direction of cyber crime is related to:

- The ability to access high-speed wireless violators including using WiMAX, 4 g, etc., to the full range of current and future internet services at affordable prices and anywhere in the world (in space and time)
- The emergence of new forms of abuse (computer crime) and improvement of known-phishing, SMS fraud, fake-antivirus, fake mailing information from friends emails with interesting attachments, create zombie networks, including to carry out attacks on various sites (Schaeffer *et al.*, 2009)

MATERIALS AND METHODS

Types of cyber crime

Phishing: Phishing is the criminally fraudulent method of attempting to acquire perceptive data, such as user names, passwords and credit business card details. Phishing often directs users to go in details in a fake website who's URL, look and seem are almost identical to the legitimate one. Even, when utilizing SSL with strong cryptography for server authentication, it is practically tough to notice that the website is fake. Phishing is an the user will see and used by phishing, to deceive users. Can be divided into two parts. Cover the content which is made to look as an organization, usually notify the user of problems with their accounts (Stuttard and Pinto, 2011).

Can be found deception depends only on the cover because the grammar is incomplete or spelling errors which is rare in legitimate messages. Over time, Album covers used in phishing and more the complex to the point where they even warn users to protect their passwords and avoid scams.

And the sting was part of the content the victim take corrective measures. It usually takes the form of interactive URL that directs the victim to a fake website sign in to your account or any other personal data. Reserchers call it sting, as part of the content. In flicts pain or other financial loss unwanted after the victim enter their data on the website, typically sting hidden using HTML to display legitimate looking email address instead of the fake website (Shinder and Cross, 2008).

URL obsifucation: Using different URL obfuscation methods, depending upon how they are classified as: Obfuscation, which is a URL, the host name-encoded URL obfuscation and cross site URL obfuscation and mixed.

Pharming: In a classic phishing attacker distributes email messages among users of social networks, online banking, email, web services, trapping on fake sites users have become a victim of fraud in order to obtain their usernames and passwords. Many users actively use modern web services not once had such cases of phishing and cautious to suspicious messages. In the classic phishing basic weak link, determining the effectiveness of the scheme is dependent on user-believe it or not Fischer. However, over time increase the awareness of users about phishing attacks. Banks, social networks and other web services have warned about various fraudulent tricks using social engineering techniques. All this reduces the number of responses in a phishing scheme-less users manage to entice fraudulently on the fake site. So, they invented a mechanism hidden redirect users to phishing sites called Pharming which is derived from the word phishing and English. Farming is a farming, livestock. An attacker spreads to your users computers special malware that after starting the computer forward to specified sites on fake sites. This ensures high stealth attack and user participation is minimal-just wait until the user decides to visit an attacker's sites of interest. Malware that pharming attack use two basic techniques for Stealth redirection to fake sites to manipulate the HOSTS file or DNS change (Halder and Jaishankar, 2011). The popular methods of pharming attacks:

- Edit the HOSTS file
- Modifying the HOSTS file along with the change of its location
- Modification of DNS server settings
- Registration of a DHCP server

Social engineering

The process of the social engineering attack: The main purpose of social engineers like other hackers and crackers is to gain access to secure systems in order to steal information, passwords, credit card data, etc., the main difference from the standard cyber attacks is that in this case, the object of attack is not a machine and its operator that is why all the methods and techniques of social engineering based on the weaknesses of the human factor that is considered to be extremely destructive, as the attacker receives the information for example by using a regular phone call or enter your organization disguised as her servant. To protect against this type of aware of the most common types of fraud, understand that actually want and organize suitable crackers security policy.

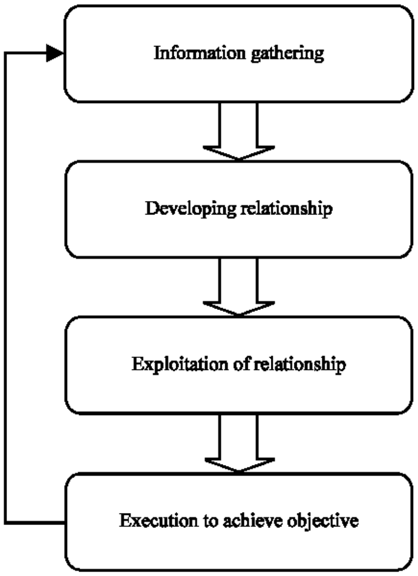

Fig. 1: The social engineering process attacks

Social engineering attacks can be performed in different ways by many common patterns has emerged, according to Gartner. This template is analyzed and divided into four general steps that occur in a social engineering attack. Each step is independent completion and the success of the previous steps, so their position during a fixed this; Fig. 1 shows these steps.

Social engineers uses various methods to collect information on specific target information is then used to build relations with a view to establishing a relationship. The attackers put themselves in a position of trust which can then be used. The attacker targeted information this information or actions may be objective function or can be used to stage the next attack/phase attack. An attacker can be executes this process many times to achieve the ultimate goal is often the attack includes a number of these cycles to achieve the end. Iteration of the arrow in Fig. 1, show that this process can be repeated several times until the attacker has collected the information needed to run a more serious attack. Thus, an attacker reaches sufficient information about the organization and its staff to be able to, for example act as an employee of the organization in such a way that an attacker could convince the target to disclose necessary information to compromise the security of your organization (Janczewski and Colarik, 2008).

Internet security threats and solutions: Table 1 shows the relationship between the various methods of attack and their respective internet solutions.

Table 1: Attack methods and internet solutions

Computer security attributes	Attack methods	Technology for internet security
Confidentiality	Eavesdropping, hacking, phishing, DoS and IP spoofing	IDS,Firewall,Cryptographic, Systems IPSec and SSL
Intergrity	Viruses, worms, trojans, eavesdropping, DoS and IP spoofing	IDS, Firewall, Anti-Malware Software, IPSec and SSL
Privacy	Email bombing, spamming, hacking, DoS and cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL
Availibilty	DoS, email, bombing, spamming and systems boot record infectors	IDS, Anti-Malware Software and Firewall

Hacking: Hackers can be people who have a career criminal. They are competent and highly skilled in the use of computers after they analyze and detect a leakage in the target system, they will find ways to get access to and attack the system. They can use different kinds of attacks or even develop their own ways to attack your computer. For example, they can gain access to the system and create bogus information or try to create a flow of information. They can also break through the web servers to access or information theft.

IP spoofing attacks: A malicious attacker can gain entry spoofing the IP address of the source packets that are sent to the firewall. A firewall can let if the address uses the identity of the trusted site. To avoid such attacks responsible information management is important. In addition, this type of attack is typically combined with other kinds of attack to hide the identity of crackers and makes the detection and prevention of hard. Unfortunately with current technology, it is impossible to eliminate spoofed IP packets. However, you can reduce the number of fake IP packets in and out of private networks. One method of reducing such attacks is to install a filtering router which rejects the incoming packets the external interface has address internal source or uses the reserved private network or other/incorrect addresses. Besides outgoing packets that have a source address that differs from your internal network should be blocked to prevent the source IP spoofing attack from originating from your site. These filters will not stop all attacks because fake out attackers can forge packets from any outside the network and internal malicious users can send internal address spoofing attacks (Carr, 2012).

Secure Socket Layer (SSL): Secure Socket Layer (SSL) is a protocol suite that actually uses many different standards for key exchange, authentication and encryption for your work that's settled. The server typically provides regular Web http services on port 80 and SSL-encrypted https Web traffic through port 443.

SSL is the standard way to achieve good the level of security between web browser and the Website. SSL is designed to create a secure channel or tunnel between the web browser and web server so that the secure exchange of information within the secured tunnel. SSL is a good choice to add end-to-end application protection, it guards against hijacking, session hijacking and Trojan servers' can be applied to online security and privacy, authentication, integrity, confidentiality and non-repudiation. SSL provides authentication of the clients to the server using certificates. Clients are from the certificate to the server in order to verify your identity.

RESULTS AND DISCUSSION

Detection: The software will identify the face within the range of a video camera, 2010 International Conference on Networking and Information Technology.

Alignment: It automatically adjusts the alignment to store the details of the position, size of the detected face.

Normalization: The software will try to normalize and to fix the image by correcting the size or to rotate the image of the detected head with the proper background.

Representation: All the nodal points of the face are represented as a unique number.

Matching: The new collected-detected data are compared with the database for matching. The image is retained as an 84 byte face print document and could be contrasted to other face prints in a gigantic database. The softwarecan compare 6 million face prints min^{-1} from the memoryor 1.5 million min^{-1} from the hard disk. Faces are utilized, as passwords to go in into restricted areas or any location where a password is required (Carr, 2012; Vacca, 2009).

Identify and block phishing in time: If researchers, can spot the phishing websites in time, researchers can prevent and avoid phishing scams. It is relatively easy to (manually) determine if the location of the phishing site or not but it's hard to find these phishing sites in time. Here, researchers register 3 methods to determine the location of phishing (Oriyano and Gregg, 2011).

Increase the security for your website the enterprise world wide websites, such as the websites of banks can take on new methods to ensure the security of your personal information. One procedure to improve security is to use a hardware device. To demonstrate the Barclays Bank is hand-held business card reader for users. Before buying online, users are required to give the borrowing business card into the reader and enter their PIN (Personal Identification Number) and then business card reader will produce a one-time password security, users can perform the operation only after the correct password. Another method is to use biometric data attribute (for example, voice, fingerprints, Iris, etc.) to authenticate the user. To show the Paypal has worked to restore the password verifier lonely voice recognition to increase security in the world website. With these procedures, suspected completes its work even after they have received a portion of the data. However, these techniques added hardware to recognize authentication between users and websites who will thus increase the value and to allocate certain inconveniences. So, it takes time for these methods are widely accepted (Davidoff and Ham, 2012).

Installing the online anti phishing software on users computers. Despite all efforts, the overhead is still likely for the user to visit a fraudulent websites around the world, as the last defense against, users can install the anti phishing devices in their computers. Anti phishing devices used today are classified as: Black/white based on the registers.

Blacklist/white list: When a customer visits a page on the (world wide web) anti-phishing tool to find the address of this site to the blacklist is stored in the database. If you have visited a site is on the list, the anti-phishing device then alert users. Although, the developers of these electronic media that they might reconsider the black in time, they do not prevent attacks from the freshly launched (unknown) phishing sites that often appear on the Internet (Brenner, 2010).

CONCLUSION

Cyber crime evolving a serious security risk which determinants loss of sensitive facts and figures like passwords, internet safety and security of users of the internet becomes an integral part of the development of new services, as well as the government in politiki 34. Deter cyber crime is an integral part of the national cyber security and critical infrastructure protection strategy to impact the integrity of critical national infrastructures. At the national level, it is a shared responsibility which requires concerted action by government organizations, the private sector and citizens to help prevent, prepare, respond and recover from incidents. At the regional and international level, this involves cooperation with relevant partners. Thus, the development and implementation of the national strategy for cyber security and requires a comprehensive approach.

Cyber security strategy, for example the development of technical protective systems and training users on how to avoid becoming victims of cybercrime can help reduce the risk. Development and support of cyber security strategy is an important element in the fight against cyber crime.

REFERENCES

Brenner, S.W., 2010. Cybercrime: Criminal Threats from Cyberspace. Pentagon Press, Santa Barbara, ISBN-13: 9788182746145, Pages: 294.

Carr, J., 2012. Inside Cyber Warfare. 2nd Edn., O'Reilly Media, Inc., Sebastopol, CA., Pages: 318.

Davidoff, S. and J. Ham, 2012. Network Forensics: Tracking Hackers through Cyberspace. Prentice Hall, USA, ISBN-13: 9780132564717, Pages: 576.

Halder, D. and K. Jaishankar, 2011. Cyber Crime and the Victimization of Women: Laws, Rights and Regulations. Idea Group Inc (IGI), Hershey, PA, USA, ISBN-13: 9781609608309, Pages: 267.

Janczewski, L.J. and A.M. Colarik, 2008. Cyber Warfare and Cyber Terrorism. Idea Group Inc. (IGI), USA., ISBN: 9781591409922, Pages: 532.

Mathew, A.R., A. Al Hajj and K. Al Ruqeishi, 2010. Cyber crimes: Threats and protection. Proceedings of the International Conference on Networking and Information Technology, June 11-12, 2010, Manila, pp: 16-18.

Oriyano, S.P. and M. Gregg, 2011. Hacker Techniques, Tools and Incident Handling. Superior Solutions, Inc., Houston, ISBN-13: 9780763791834, Pages: 400.

Schaeffer, B.S., H. Chan, H. Chan and S. Ogulnick, 2009. Cyber crime and cyber security: A white paper for franchisors, licensors and others. http://business.cch.com/franlaw/cybercrime_whitepaper.pdf.

Shinder, D.L. and M. Cross, 2008. Science of the Cybercrime: Computer Forensics Handbook. Syngress Publishing Inc., USA.

Stuttard, D. and M. Pinto, 2011. The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaw. 2nd Edn., John Wiley and Sons, Inc., New York.

Vacca, J.R., 2009. Computer and Information Security Handbook. Morgan Kaufmann, Burlington, MA., ISBN-13: 9780080921945, Pages: 928.