ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

A real understanding of Hacking and its consequences in real world

Dr. KAMMILI JAGAN MOHAN[1], Dr. PENMETSA VAMSI KRISHNA RAJA[2]

Professor, Dept of CSE, Periyar Maniammai University, Thanjavur, TN, India[1]

Professor, Dept of CSE, JNTU, Kakinada, AP, India[2]

Abstract: It is very much necessary to know how the process of hacking takes place in the area of network security. There are various kinds of hacking techniques available that would affect the users/internet-customers by harming their financial accounts in un-authorized ways. In this technical paper, we would like to explain how the innocent internet user gets affected by hackers and lose their money electronically. The definition of a hacker is made in the beginning and the fraud made by Krishna Karpal's email is explained as an example and the necessary URL is also provided to give the awareness to all the internet-users. Then the basic terminology used in network security is made available for the better understanding of the learners. Thereafter, the concept of Phishing and the necessary precautions to be taken by the internet-users is clearly mentioned. Our objective through this technical paper is to give awareness to internet-users not to respond to greedy advertisements which come through un-known emails for making more money in less time and not to divulge their user-id and password in any web-page except in an authorized web site.

Keywords: Hacker, Online theft, firewall, networking software, network operating systems, shared network applications, client-server network programs, sibling domains, Phishing.

I. INTRODUCTION

In the context of computer network security, a **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge.
A hacker may belong to any one of the following two kinds:
A person who work to provide security against hacking in a known community of a computer network. They can be referred to as computer security experts or white hats.

A computer criminal that attacks computer networks for hacking the accounts of customers of a bank by identifying their user-id and passwords for making online theft in banking transactions etc. They can be referred to as crackers or black hats.

In general, to hack any data in a computer network, a black hat works thoroughly on the following areas which include – the type of the firewall, networking software, operating system in use, host lists, network connection (point to point / Multipoint connection), sibling domains, target network, collection of user-Ids and passwords from users through unauthorized advertisements like Krishna Karpal's email to user accounts to earn more US dollars in a month. (To know more details about how this email misleads the users and cheat them by online theft of amounts from user accounts, please logon to http://www.jobs8home.com/krishna-karpal-is-the-name-of-biggest-work-from-home-scam.htm) in the internet that attracts and cheats the users etc. Several people from different countries lost so much of their money in this international scam. Even nationalized banks (Example: IOB) also unable to trace the fraud made by them internationally. Even the police and central government of India are not taking steps to control such frauds even though it is being informed properly by the victims. Hence, we like to give awareness to the public through this technical paper about online fraud along with hacking.

II. BASIC TERMINOLOGY

Firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on a rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted. A firewall is a network device for controlling network security and access rules. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.

There are different types of firewalls exists depending on where the communication is taking place, where the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

communication is intercepted and the state that is being traced.

Networking software is software that facilitates, enhances or interacts with a computer network. One type of networking software allows computers to communicate with one another, while another type of networking software provides users access to shared programs. Networking software is a key component of today's computer networks, including the Internet. Understanding the types of networking software is the first step in understanding how the computer network really works.

Various network-software may have various features. Some network software can perform accounting tasks. Some create a communication path between computers, other networks or individual users. Some of these programs store large amounts of data and distribute it to users or to other programs.

Network Operating Systems can be embedded in a router or hardware firewall that operates the functions in the network layer (layer 3) of the OSI model. Example: JUNOS, used in routers and switches from Juniper Networks.

In a peer to peer**_network** operating system users are allowed to share resources and files located on their computers and access shared resources from others.
Example: Windows for Workgroups used for networking peer-to-peer windows computers.

Network Operating Systems can be based on a **client/server** architecture in which a server enables multiple clients to share resources. Examples include Novell Netware, Windows Server.

Shared network applications are another type of computer networking software. These are applications that are stored on a central server, but run from the individual client computers. Examples include certain types of database applications such as Oracle.
Client-Server Network Programs are the programs that have one component that's stored on the server, and another component that's stored on the client workstation. Microsoft Exchange is an example of this type of network program.

Sibling domain is an exact replica of a primary domain, in all respects except the name of the domain itself. The primary domain and the sibling domain must have the exact same mail host, email account lists, aliases, spam filtering settings, and so forth. For example, yourcompany.com may be a primary domain while yourcompany.net may be a sibling domain -- in which case, when the filter receives any message to an address at yourcompany.net, it will treat the message exactly as if the message was sent to the same an address at yourcompany.com. The sibling domain can be added in the Domains section of the control panel.

III. PHISHING

Phishing is a common form of Internet piracy. It is deployed to steal user's personal and confidential information like bank account numbers, net banking passwords, credit card numbers, personal identity details etc. Later the perpetrators may use the information for siphoning money from the victim's account or run up bills on victim's credit cards. In the worst case one could also become the victim of identity theft. A few customers of some other Indian banks have been affected by the attempt of phishing in early 2006 and it is being continued even on today also because of lack of awareness of users/customers of a bank about Phishing.

Phishing Methodology:

- Phishing attacks use both social engineering and technical subterfuge to steal customers' personal identity data and financial account credentials.
- Customer receives a fraudulent e-mail seemingly from a legitimate Internet address.
- The email invites the customer to click on a hyperlink provided in the mail.
- Click on the hyperlink directs the customer to a fake web site that looks similar to the genuine site.
- Usually the email will either promise a reward on compliance or warn of an impending penalty on a non compliance.
- Customer is asked to update his personal information, such as passwords and credit card and bank account numbers etc.
- Customer provides personal details in good faith. Clicks on 'submit' button.
- He gets an error page.
- Customer falls prey to the phishing attempt.

IV. SAFETY INSTRUCTIONS

Don't do the following:

Do not click on any link which has come through e-mail from an unexpected source. It may contain malicious code or could be an attempt to 'Phish'.
Do not provide any information on a page which might have come up as a pop-up window.
Never provide your password over the phone or in response to an unsolicited request over e-mail.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Always remember that information like password, PIN, TIN, etc are strictly confidential and are not known even to employees/service personnel of the Bank. One should therefore, never divulge such information even if asked for.

Do the following:

- Always logon to a site by typing the proper URL in the address bar.
- Give your user id and password only at the authenticated login page.
- Before providing your user id and password please ensure that the URL of the login page starts with the text 'https://' and is not 'http:// '.The 's' stands for 'secured' and indicates that the Web page uses encryption.
- Please also look for the lock sign ( ) at the right bottom of the browser and the VeriSign certificate.
- Provide your personal details over phone/Internet only if you have initiated a call or session and the counterpart has been duly authenticated by you.
- Please remember that the bank would never ask anyone to verify their account information through an e-mail.

V. AN ONLINESBI EXAMPLE

What to do if you have accidentally revealed password/PIN/TIN etc:

- If you feel that you have been phished or you have provided your personal information at a place you should not have, please carry out the following immediately as a damage mitigation measure.
- Please lock your user access immediately using 'Lock User Access' option given on the home page of www.onlinesbi.com
- Report to the bank by clicking on the link Report Phishing
- Check your account statement and ensure that it is correct in every respect.
- Report any erroneous entries to the bank.
- Use the other compensatory controls provided by the bank like setting the limits for demand draft and trusted third parties to zero, enabling high security, etc to minimize the risk.

VI. RECOMMENDATIONS

- Newer version of Operating System with latest security patches.
- Latest version of Browsers (IE 7.0 and above , Mozilla Firefox 3.1 and above, Opera 9.5 and above, Safari 3.5 and above, Google chrome,etc.)
- Firewall is enabled.
- Antivirus signatures applied
- Scan your computer regularly with Antivirus to ensure that the system is Virus/Trojan free.
- Change your Internet Banking password at periodical intervals.
- Always check the last log-in date and time in the post login page.
- Avoid accessing Internet banking accounts from cyber cafes or shared PCs.

VI. CYBER CRIME CASES IN INDIA

Cyber crime cases in the country registered under the IT Act last year rose by about 61% to 2,876 with Maharashtra recording the most number of cases. The country had witnessed 1,791 cases registered under the Information Technology (IT) Act in 2011, Minister of State for Communication and IT Milind Deora said in a written reply to Rajya Sabha.

As per the cyber crime data maintained by National Crime Records Bureau (NCRB), a total of 288, 420, 966, 1,791 and 2,876 cyber crime cases were registered under IT Act during 2008, 2009, 2010, 2011 and 2012, respectively.

State Name	No. of cyber crime cases registered in 2012
Maharashtra	471
Andhra Pradesh	429
Karnataka	412
Kerala	269
Uttar Pradesh	205

To address the growing threat of cyber crimes/incidents in the country, government has issued an advisory to state governments and union territory administrations advising them to build adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes.

CONCLUSION

This technical paper is explained all the necessary precautions to be taken while working with internet not to divulge the important information like user-id and password in any other website other than the intended website. Also explained the online-fraud made by Krishna Karpal's email to mislead the internet-users thereby affecting their banking accounts and the comments made by the victims can also be seen through the URL mentioned. Hence, we can conclude

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

that this technical paper would be helpful to the internet-users as well as the future technocrats who want to excel in the field of software development by providing security to their online applications by taking necessary precautions particularly in the field of internet-hacking.

ACKNOWLEDGMENT

We here by wish to acknowledge OnlineSBI and other contributors for developing and maintaining the important governing rules for the public awareness in order to get rid of the problem of hacking.

REFERENCES

[1] Cryptography and Network security --- Stallings, Fifth Edition.
[2] The Complete E-Commerce book ----Janice Reynolds
[3] http://www.jobs8home.com/krishna-karpal-is-the-name-of-biggest-work-from-home-scam.htm
[4] www.en.wikipedia.org
[5] www.garykessler.net
[6] www.williamstallings.com
[7] http://cybercellmumbai.gov.in/
[8] http://cybercrimeindia.org

BIOGRAPHIES

Dr. Kammili Jagan Mohan had been awarded his first PhD(Computer Science) from Golden State University, Wyoming State, USA., Second PhD (Computer Science & Engineering) from CMJ Universty, Meghalaya State, India and M.Tech(I.T) from Allahabad Agricultural Institute Deemed University, U.P, India. His research areas include Network Security, Cryptography, Intrusion Detection, Databases, Data Mining & Data warehousing, and Software Engineering.

Dr. Penmetsa V. Krishna Raja did his PhD from JNTU, Kakinada. He received his M.Tech (CST) from A.U, Visakhapatnam, Andhra Pradesh,India. His research areas include Network Security, Cryptography, Intrusion Detection, Neural networks, Data Mining and Software Engineering.