International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 12
ISSN: 2454-4248
97 – 101

History & Impression of Hacking on the Society

Abhishek Gupta
Department of Computer Science,
AISECT UNIVERISTY
Village Mendua,Raisen,Bhopal,M.P
Abhishekgupta141983@gmail.com

Dr. Jatinder Manhas
Sr. Asstt. Professor,
University of Jammu
Jammu, India

Abstract: The hackers have been widespread throughout the IT world. The main categories of Hackers have evolved: the Open Source and Free Software group and the Security Hackers group these both groups are function differently and there concept and method are differ from each other . In this paper we are discussed on some of the more noteworthy groups and individuals of each 'category' of hackers, the effects of hacking on society, as well as conferences and publications that they are responsible for that have contributed to the modern hacking world. Hacking is just like a cancer that has very dangerous effects on the society. Today in this modern world, where measures have been taken to improve the security level in the distributed systems ,hackers have found a way to crack into systems and take away information. In this paper, we will explain you few aspects of hacking, tools and technique used by hackers that has caused of its existence and few techniques through which we can minimize this.

Keywords: *Hacker,Ethical Hacker,Red Hat,White Hat,Grey Hat,Security*

*****

I. INTRODUCTION

The hacker philosophy began in the 1960s and 1970s as an cogent movement: exploring the unknown, documenting the secret, and doing what others cannot. Many hacker subcultures developed independently and in parallel at various universities throughout the United States: Stanford, MIT, CalTech, Carnegie Mellon, UC Berkeley, and many others. The completion of the ARPANET linked these campuses and they were able to share their collective experiences, their knowledge, humor and skills. Together, they formed the first hacker culture. Many hackers began as expert programmers: programming master like Richard M. Stallman, founder of the Free Software Movement, and Linus Torvalds, creator of the Linux kernel. These programmers were able to found new loosely-connected organizations that would push the boundaries of accepted software engineering, and also technology. These figures serve to popularize the efforts of hacking to a society increasingly focused on computing. In the realm of computer security, with the advent of global networking, a distinction began to form between two groups: the so-called black hat and white hat hackers. Both maintain a connection to the hacker ethic, but focus on different aspects and explanations. The black hat culture is known for infringement authority and embracing lawlessness, committing acts of mischief and spite and knowingly breaking and entering secured systems—these are the hackers most often seen in the news and popular culture. The white hats, the "ethical hackers", focus on other aspects of the hacker ethic: they seek to understand, to satisfy curiosity, and to inform. A compelling aspect of the history of hackers lies in the history of the word itself. To fully understand how and why these often mutually disparate groups happened to be called the same name, we have to examine how the computer security definition sprang from its common English definition and how it evolved to identify these different communities. While it is intractable to provide even a definite definition of "hacker" due to the constant merging and fracturing of the English language, we will at the very least, attempt to provide a chronicle of the word's new definitions from their birth to their entry into standard American English.

Hacking Organizations & Laws

Creation Year	Organization or Law	Description
1984	Computer Fraud & Abuse Act	Laws passed with the intent of reducing "hacking" of computer systems.
1985	FSF- Free Software Foundation	Non-profit corporation founded to support Free Software Movement.
1987	Computer Security Act	Congresses attempt at improving the security and privacy of sensitive information in Federal computer systems. Designates the National Institute of Standards and Technology (NIST) as the lead government agency for computer security standards.
1988	CERT CC- Computer Emergency Response Team Coordination Center	Created by DARPA, it is the major coordination center in dealing with internet security problems.
1992	NCCS- FBI's National Computer Crime Squad	Investigates violations of the Federal Computer Fraud and Abuse Act of 1986.

 ISSN: 2454-4248
97 – 101

1996	National Information Infrastructure Protection Act	Amended the Computer Fraud & Abuse Act.
1998	Presidential Directive PDD-63 (CIP-Critical Infrastructure Protection)	National program to assure the security of vulnerable and interconnected infrastructures of the US.
2001	US Patriot Act	Increased the scope of the penalties defined in the Computer Fraud & Abuse Act.
2004	CAN-SPAM Act	Establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them.

On the other hand the word hacker is the agent of hack or hacking and it was defined as a person who enjoys accessing files whether for fun, imposing power or the interest related to the accessed files or. While Marotta has a negative view of the hacker as a data lord, a barbarian who takes what he wants. Himanen defines hacker as any person who performs illegal actions whether they were related to computer or not which means the usage of a device apart from its functionality. Seems hacking according to Himanen is related to any illegal or unauthorized action.

II. WHO IS THE HACKER?

The Hacker can be anyone who has knowledge of things; he can be a graduate or a computer professional working at a multinational company. He can be one amongst us. A is part of the society, a computer professional who wants to use technology for his own benefit . Hackers are experts and professional people who first enjoy the technology and through research and development they gain more interest and you never know when this curiosity of technology changes into crime. People must realize that the technology is good lest it is used for the countries benefit, but it has adverse affect when things turn upside down, that the hackers learn this technique in order to gain profits for themselves through illegal ways. Levy described hackers in regard to the history; she divided the life history of hackers into three generations: the first generation of hacking was made of experts of computer programming who never stopped improving their skills then misuse them, the second generation was made of computer hardware developers who found hacking and accessing data and information for free as an appealing idea while the third generation included developers of games architecture . And I think the fourth generation of developers are those who know about computers and have just enough knowledge about computer programming.

The classification of hackers depends on the functionality, in other words the classification depends on the way hacker interacts with what is being hacked. Hackers were classified into three different types; the first type is called In-house hacker. An in-house hackers actually works inside the company, who knows the system security, has access to all the features. His motivation to hacking might be because he wasn't recognised as a potential candidate for promotion or because he was betrayed by his fellow colleagues. The second type of hackers is a super hacker who doesn't interact with the system, but remotely monitors all the movements or the data transactions that are going on and depending on the situation and the amount of money that is being transferred he then changes that transaction into his account. And finally, comes the professional hacker, he is very strong and capable of getting any type of data from anywhere, he has the ability to manipulate things and change them to his benefit, programming Trojans and software that get installed on the system through hidden window and then sits on the system.

III. MOTIVATIONS BEHIND HACKING

Hacker's psychology and the fuel that encourages him/her to perform such illegal activities, also because hackers view about what they are doing is far different from our views as victims , in this paper Halting the hacker, says "the challenging part of the hacker's personality as the biggest motivation; this means that the hacker feels the joy and excitement when hacking systems that are provided with the almost perfect security tools" . One of the main reasons for hacking is excitement where hackers find adrenalin rush to break the law, to find an easy access to earn money by hacking crucial information of the customers by creating unreal shopping websites and obtaining payment details, credit card details.

Furnell judged hackers "depending on the harm they cause whatever was their motivation, because hacking is a disease and should be removed so that the effect of hacker attacks will be minimized". The motivations behind hacking are an issue that is discussed heavily due to the importance of understanding the hacking.

An ethical hacker attempts to duplicate the intent and actions of malicious hackers without causing harm. Ethical hackers conduct penetration tests to determine what an attacker can find out about an information system, whether a hacker can gain and maintain access to the system, and whether the hacker's tracks can be successfully covered without being detected. The ethical hacker operates with the permission and knowledge of the organization they are trying to defend and tries to find weaknesses in the information system that can be exploited.

In some cases, to test the effectiveness of their information system security team, an organization will not inform their team of the ethical hacker's activities. This situation is referred

 ISSN: 2454-4248
97 – 101

to as operating in a double blind environment. To operate effectively, the ethical hacker must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support the ethical hacker's efforts.

A. Hacker and Ethical Hacker Characteristics and Operation

Hackers can be categorized into the three general classes of black hats, gray hats, and white hats. A black hat hacker or cracker has the necessary computing expertise to carry out harmful attacks on information systems. A gray hat is a hacker with a split personality. At times, this individual will not break the law and, in fact, might help to defend a network. At other times, the gray hat hacker reverts to black hat activities. The white hat individual usually has exceptional computer skills and uses his or her abilities to increase the security posture of information systems and defend them from malicious attacks. This individual might be an information security consultant or security analyst.

Entities that perform ethical hacking functions for organizations usually fall into one of three categories: white hats, former black hats, and independent consulting organizations. The white hat ethical hacker has the appropriate computer skills and understanding of the black hat hacker mentality and methods. This person might be an independent consultant hired to perform ethical hacking activities. The former black hat hacker is, we might hope, reformed and brings actual black hat experience to his or her work. There is a concern about this individual in that you can never be certain that he or she will not revert to their former malicious activities. The third category of ethical hacker is taken by consulting companies that perform a variety of services for organizations including accounting, auditing, and information system security.

Related Types of Computer Crime and attack:

Different kind of hacking attacks are considered as computer crimes. The following is the list of crimes which are committed frequently:

Password Hacking.

Hackers find a way to illegally hack into the passwords of users of federal bureau, banks in order to gain benefits from them.

Network intrusions.

Malicious Trojan, worms and viruses to gain access into the information systems.

Cheat.

Illegal use of people identities such as credit card details.

Software piracy.

Illegal copying and use of software

Viruses.

Viruses, Trojan horses and worm cause the computers to become more vulnerable and susceptible to hardware damage.

IP address spoofing.

Disguising the IP address and using that to gain illegal access into countries most confidential files.

Money Laundering

Illegally acquiring funds through the manipulation and falsification of financial statements and illegal transactions.

Data-modification.4 -

The modifying all the data.

Smuggling of files.

Gain illegal access of confidential files including bodies like military/government networks, communication systems, power grids, and the financial community

There is number of hacking attacks that are most commonly used in breaking system and causing disruption and damage for services. These attacks can be summarized as following :

Software piracy is a criminal offense. Many hackers have indulged in making copies of software and selling them to gain profits on their own. The companies who develop these software will have to bare all the losses only because of someone who is illegally misusing software. Stealing confidential files through illegal access of the companies most confidential files. Hackers have many such motives, few of them like denial of services to the user and to make hardware conflict, making unwanted popup, causing trouble, terrorism.

The main characteristics of hacking attacks in three points :

Simplicity: means that the attack should be simple in appearance but the effects are impressive and the results will be as pleasing to the hacker as what he planned for. It means that do your job in a smart and easy way.

Mastery: the methods used in hacking contain sophisticated knowledge which is difficult for anyone to understand. The reason behind mastery is to make sure that the hacker is the only one who can solve the problem being caused.

IV. HACKERS IMPRESSION ON SOCIETY

Hackers have been responsible for both good and bad incidents in society. As a result of White Hat hackers we have foundations such as the Free Software Foundation that have made it possible for computer users to use, study, copy, modify, and redistribute computer programs freely. Grey Hat hackers have also had positive effects on society by working to find vulnerabilities in popular software products with the intentions of notifying the creators so they can fix the problems before a Black Hat hacker can come along and exploit the flaw. However during the prime time of hacking in the mid 90's Black Hat hackers caused all sorts of rumpus. "The NY Times reported that in 1997, there were more than 1900 hacker websites and more than 30 hacker publications." In 1998, 418 cases were given to federal prosecutors. That was 43% more than the previous year. In the first & second quarter of 1999, businesses were said to have lost $7.6 billion as a result of viruses. Also in 1999, corporations spent $7.1 billion on security and were estimated to spend a total of $17 billion

 ISSN: 2454-4248
97 – 101

in a matter of four years. Over 1400 web hacks were reported as of July 1999. One can assume that from 1999 to 2007, these numbers have more than doubled. Table 7 below lists the organizations & laws that have come about as a result hacking in society. Some of the most expensive and prolific victims of hacking have been businesses. Businesses are many times targeted for their customers' personal and financial data and often are targeted by their own employees, whether resentful or just devious. Businesses lose billions of dollars yearly as a result of hacking and other computer breaches. Many times, the true cost cannot be evaluated because the effects of a security breach can delay for years after the actual attack. Companies can lose consumer confidence and in many cases are held legally responsible for any loss to their customers.

The cost of recovering from an attack can spread quickly: legal fees, investigative fees, stock performance, reputation management, customer support, etc. Companies, and more recently, consumers, are investing more and more money into preventing an attack before it actually happens. Businesses that hold stores of consumer's personal and financial data are especially taking extra steps to insure the data's safety. Microsoft's online group, MSN/Windows Live, requires that no single group store personally identifiable information without explicit consent from an internal security group. Security reviews occur frequently for groups that do store consumers' data and the security

group performs its own personal security review by actually attempting to hack into the sites. Sites have actually been withheld from releasing to the web due to flaws found through this method. Other businesses that are more limited in technical areas employ outside security experts to assist

them with their security. ScanAlert.com boasts of working with over 75,000 secure ecommerce sites, including many famous brands like FootLocker, Restoration Hardware and Sony. The ecommerce sites host a "Hacker Safe" logo, stating that the site is tested daily and is effectively preventing 99.9% of hacker crime. The ScanAlert disclaimer though appears far less confident: This information is intended as a relative indication of the security efforts of this web site and its operators. While this, or any other, vulnerability testing cannot and does not guarantee security; it does show that [the eCommerce Site] meets all payment card industry guidelines for remote web server vulnerability testing to help protect your personal information from hackers. HACKER SAFE does not mean hacker proof. HACKER SAFE certification cannot and does not protect any of your data that may be shared with other servers that are not certified HACKER SAFE, such as credit card processing networks or offline data storage, nor does it protect you from other ways your data may be illegally obtained such as non-hacker "insider" access to it. While ScanAlert makes reasonable efforts to assure its certification service is functioning properly, ScanAlert makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that ScanAlert shall be held harmless in any event. Businesses, in recent years, have also had to deal with a specialized and more challenging type of hacking. Social engineering is a way of defrauding a user into providing you with information not normally available to you, whether it be a password, access code or other piece of information necessary in hacking into a computer system. Similar to phishing, social engineering relies on tricking a person or group of people in order to be successful. While not normally the tactics associated with a hacker, famous hackers like Kevin Mitnick have used it in their crimes and claim it to be one of the most effective means of hacking.

V. CONCLUSION

Hackers were considered to be mastermind because they helped in many ways in the development of computers and internet technology as such, but in this modern world where personal benefit has played a major importance in one's life, people are often involved to things they can do and gain through illegal entry into people privacy and using for their own benefits. Different inspirations and thoughts have been discussed in this paper, but if we consider them as a person they are a live example of sensation because of their abilities of doing the farfetched and inaccessible by getting more involved into the programming and understanding the loop holes in the security systems. I think because of these, scientists and researchers have spent lots of technology to improve the systems security and make them more secure so that no illegal access can be gained. In my own view understanding the different standpoint of a hacker, we can develop a much more secure and much more sophisticated atmosphere and provide a safer world for transactions. The bad things of them should be taken into good only to benefit our country and its progress. A hacker has always been someone who pushes the bounds of technology. Based on history we see that newer fields of computing are generally the places where hackers have the largest impression. This would lead to the conclusion that the impression of hackers will be felt most in the developments to do with the Internet in the short term, and in the medium term it would seem predictable that other newer fields of computing would attract the interest of hackers, we see more and more activity: spyware, viruses, spam. But as the number of malicious black hats increases, we can expect a corresponding increase of security works and white hats.

VI. REFERENCES

[1]. Banks, Michael A. (1997), 'Web psychos, stalkers, and pranksters: How to protect yourself online'. Arizona (USA).
[2]. Chakrabati, Anirban and Manimaran, G. (2002), 'Internet infrastructure security: A Taxonomy', IEEE Network, November/December 2002, P.13.
[3]. CNET (2001), FBI "hack" raises global security concerns

 ISSN: 2454-4248
97 – 101

[4]. Crucial paradigm (2003), Hacking attacks-How and Why.
[5]. Darlington, R (2001), Crime on the net
[6]. Furnell, Steven. (2002), Cybercrime: Vandalizing the information society, Boston; London: Addison-Wesley.
[7]. Himanen, Pekka. (2001), The hacker ethic and the spirit of information age, Great Britain.
[8]. Levy, Hacker: Heroes of the computer revolution, Hackers: Crime in the digital sublime.
[9]. Hackers: Crime in the digital sublime
[10]. Halting the hacker: A practical guide to computer security
[11]. Taylor, Paul A. (1999), "Hackers: Crime in the digital sublime", London.
[12]. https://courses.cs.washington.edu/courses/csep590a/06au/projects/hacking.pdf