Medicon Engineering Themes
Volume 6 Issue 6 June 2024
Article Type: Research Article
ISSN: 2834-7218

What Influences a Hacker to be a Black Hat?

Bishal Poudel[1]* and Satish Kumar Karna[2]

[1]Department of Computer Engineering, Nepal College of Information, Technology, Balkumari, Lalitpur

[2]Department of Electrical and Electronics Engineering, Nepal College of Information Technology, Balkumari, Lalitpur

***Corresponding Author:** Bishal Poudel, Department of Computer Engineering, Nepal College of Information, Technology, Balkumari, Lalitpur.

Received: April 29, 2024; **Published:** May 31, 2024

DOI: 10.55162/MCET.06.215

Abstract

Hacking used to be linked with computer enthusiasts making positive improvements. But now, it has split into two sides: ethical and unethical practices. Originating from MIT's hacker culture, the paper examines the mindset, motivations, and influences behind the transition of hackers, in unauthorized and harmful activities, known as "black hat" hacking. Hackers, initially driven by a dream to enhance human life through computers, became divided into black hats and white hats, separated by a fuzzy gray line. While both possess technical expertise, black hats engage in bad activities driven by motivations such as financial gain, revenge, ideology, curiosity, ego, and enjoyment. Money and ego emerge as primary influencers leading hackers towards the black hat path. The study emphasizes the interplay of technical skills, human vulnerabilities, and hacking methods. Despite the negative impact, black hat activities unintentionally contribute to technological progress. The paper concludes by highlighting the importance of understanding the human aspect of hacking in the evolving digital landscape.

Keywords: hacker; black hat; white hat; mindset; motivation; influence

Introduction

The word hacker is very famous in this digital age of technology. With the initiation of hackers and their hacking activities, there formed a subculture called hacker culture [1]. People often don't realize that hacker culture can be a source of inspiration. This happens because the media often portrays hackers in a biased and overly simplistic way [2]. Person who belong to Information Technology and who know about hacking and technological stuffs describe the term hacker in their own way like they are villains and in a way media shows them—a hacker is a bad guy, he did all the bad stuffs sitting on a dark room wearing a black hat and hoodie behind a black and blue terminal with a mask. But hackers actually started the computer revolution and created the information society before big companies took charge of developing technology [2]. The shadow used to describe a hacker by the public is actually a black hat hacker. Hackers are more than villains and thieves in the digital age. Motivating factors for a normal hacker to involve in illegal and unauthorized activities are discussed in this paper.

Defining The Terms

Hack

The hack is a way of understanding what is possible, sensible and ethical in the twenty-first century [3]. There are many meanings of the term hack, simple is short for hacker. Hack might be characterized as an appropriate application of ingenuity. The hack involves alternating a pre-existing situation to produce something new; to hack is to produce differences, the differences in any field of study and experiment [3]. At MIT the word hack usually refers to a clever, benign, and ethical prank or practical joke, which is both challenging for the perpetrators and amusing to the MIT community and sometimes even the rest of the world [4].

Hacker

The Jargon File contains a bunch of definitions of the term 'hacker', most having to do with technical adeptness and a delight in solving problems and overcoming limits. There is a community of expert programmers and networking wizards that traces its history back through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments. A member of this culture originated the term hacker. However hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics, music, arts and science. There is another group of people who loudly call themselves hackers, but aren't. Real hackers call these people crackers. The basic difference is this: hackers build things, crackers break them [5].

The hacker is a person who enjoys learning the details of computer systems and how to stretch their capabilities, as opposed to most users of computers, who prefer to learn only the minimum amount necessary [6]. To use a computer science metaphor, the word "hacker" acts as a pointer to three different groups of people, the expert programmers, the black hats, and the white hats. The first verifiable modern source of the word hacker is linked to 1959 at MIT [7]. Hacker communities are socially and mentally separated into two groups—white hat and black hat with a fuzzy gray line that separates the two [8].

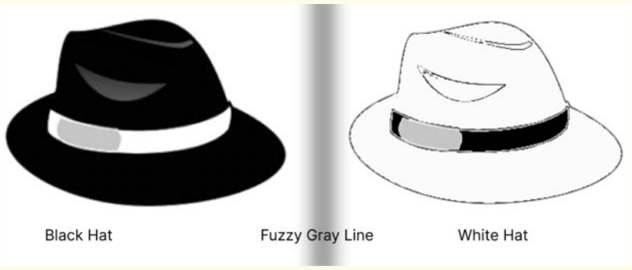

Figure 1: Black and White hat hacker.

White Hat Hacker

White hat hackers are also called an ethical hacker. The practice of ethical hacking has recently been the focus of much debate among computer security professionals [7]. They are good hackers. They shape the technology using their hacking skills and are considered as never destroying the system.

Black Hat Hacker

Black hat hackers are those who want to steal information, break the system or cause damage. For large numbers of people, hackers refer to black hat hackers. The name comes from the old westerns—the movies, dramas, and novels in which bad guys such as bank robbers wear black hats and heroes wear white hats [6]. Script kiddies, state sponsored, spy hackers, cyber terrorists, and malicious insiders fall under this category [4].

Both black and white have deep knowledge of computers and networks but they apply their knowledge for different purposes. Sometimes hacker and cracker are used synonymous but a cracker is a person who breaks into or otherwise violates the system integrity of remote machines, with malicious intent [7, 9].

Hacking

Hacking is what a hacker does. It is not only a skill set, it is a mindset and a mentality not just about computers but about taking something from A to B. Hacking is doing something in a way that is not supposed to be done in that way. It is thinking outside the box and is freedom [1]. In a detail way, it can be defined either by attributes such as questioning social norms, finding a way and never accepting no for an answer, persistence, organization, workaholic, creativity, problem solving or by attitude of hacker such as the world is full of fantastic problems to be solved, no problem should ever have to be solved twice, freedom is good, think bad and do good [1, 5].

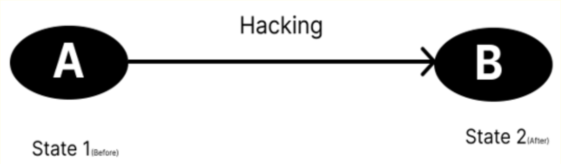

Figure 2: Hacking (taking something from A to B).

While talking about hacking, the ethics of hackers and the dream of early hackers should be considered. All information should be free, computer can change your life for the better, you can create art and beauty on computer, not damage anything, be safe, hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position are the hacker ethics and the betterment of human life through computer was the hacker dream [1, 10]. There is a mindset that defines both the black and white hat hackers but the mindset of black hat hackers is more about destroying the infrastructure.

Methodology

The methodology for this paper involves a comprehensive review and synthesis of existing literature, qualitative analysis and case studies.

Literature Review

A comprehensive review of relevant literature was conducted to gain insights into the historical context of hacker culture, motivations, methodologies, evaluation and current context.

Case Studies

Most popular hacking incidents such as the Target cyber breach and activities of notable hackers like Kevin Mitnick and Anonymous, were analyzed to identify common patterns and strategies employed by black hat hackers.

Behavioral Analysis

Psychological and motivational factors driving black hat hacking were examined through behavioral analysis, focusing on themes such as financial gain, revenge, ideology, curiosity, ego, and enjoyment.

Ethical Considerations

Throughout the research, ethical considerations were prioritized, ensuring that the focus remained on understanding and preventing unethical hacking rather than promoting it.

Literature Review

Origin of hacker culture

In the 1950s, the term “hack” originated from MIT, and its meanings have changed over time. Before the 1970s, it wasn’t commonly used in written form. At MIT, students used “hacking” to describe various activities to avoid studying, like goofing off, playing bridge, chatting with friends, or going out. Even playing pranks was seen as a form of hacking, but it was just one aspect of a broader definition [10].

In the later part of the 1950s, members of the Tech Model Railroad Club added new meanings to the term “hack.” The Tech Model Railroad Club (TMRC) was a student organization established at the Massachusetts Institute of Technology (MIT) in 1946-1947. The club was known for its pioneering work in computer technology, particularly in the field of artificial intelligence, and for its elaborate model railroad layout which featured advanced automation and control systems. The club’s legacy has had a lasting impact on the development of computing technology and hacker culture. When computers came in they basically transferred that hacker culture into computing from model railroads. As the TMRC people used the word, there was serious respect implied. They called it a mere hack for some extraordinary work; it would be understood that to qualify as a hack, the feat must be imbued with innovation, style, and technical virtuosity [1]. There was a computer on the second floor of building 26, received from Lincoln Lab called TX-0 and it was one of the transistor’s running computers in the world. The TMRC hackers, who soon referred to themselves as TX-0 hackers, changed their lifestyle to accommodate the computer.

They spend most of their time on a computer, they called themselves hackers they were just crazy about computers and did unbelievable and amazing things. Graduate students, working on the IBM machines, on the first floor of building 26, didn’t embody the hacker culture—they would call them losers. Sometimes losers would prove themselves and earn the status of hacker—that was only through really really hard work, tenacity, and really not giving up. Hacker culture spawned out of that they were creatures of the night, hacking your own body, and hacking your own life, without pharmaceuticals. The hackers are just not limited to software and programming; they are math hackers, game hackers and hardware hackers. Later the culture was spread outside MIT, all around the world. Richard Greenblatt, Bill Gosper, Lee Felsenstein, and John Harris are the spirit and soul of computing itself [1]. Development of Spacewar, Chess game, John Conway’s game of life, Project MAC, and ARPAnet were examples of some early hacks [1].

Evolution of Hackerism

As change is the law of the universe, there are many changes that can be seen in the evolution of hackerism. Strong evidence of the origin of this culture was found in MIT [1, 10]. But it is just not limited to it, it evolved and sub culture was established in different places around the world such as Cambridge, Russia, Israel, China etc. Hacker shaped the technology with the development of projects like Unix, C programming language, BASIC, World Wide Wave (WWW), the internet, Linux, Windows in case of programming. Also they developed modern hardware for computer systems. Some ideas like Windows and MacOS were commercialized while others like GNU, Linux, LibreOffice, Emacs are running under hacker philosophy. The philosophy is about freedom—freedom to run, copy, distribute, study, change, and improve. There was a free software movement started in 1983 by computer scientist Richard M. Stallman [11]. Teaching new users about freedom became more difficult in 1998, when the community decided to stop using free software instead of open source. The concept of open source is the software development pattern focuses on the potential to make high quality, powerful software with distributing the source code. The root of that concept is found to be linked with MIT, where the code was available to anyone and could modify according to them—this is what the hackers want for betterment and improvement [1, 11]. The development of artificial intelligence is also connected with the MIT AI lab.

There were hardware hackers in the 1970s, they focused on advancement of hardware technology and owning self hardware. They created Homebrew Computer Club which was a community of like minded hackers. Also there were game hackers in the 1980s [1]. In the generation of game hackers, the term hacking has become associated with criminal behavior. They were involved in the breaking of copyright protection codes thus enabling the games programs to be refined or altered, or simply to facilitate the pirating of the games. In 1988, Robert Morris, a student at Cornell University, unleashed the first Internet worm. The worm replicates itself at a rate higher than Morris intended, resulting in an Internet shut down. Morris became the first person to be indicted under the Computer Fraud and Abuse Act [8]. Between the end of the 1990s and the 2000s, the hacker community became sociologically separated into two groups—black and white separated by gray line. As technology has become an important component to the human way of life, hacking has manifested itself in the form of two industries—an underground industry that is based on greed, theft, chaos, and human trafficking, and a business industry that survives based on its ability to combat that of the underground.

The hacking is associated with security, securing the system from malicious intent. An entire sub-industry has emerged around security products and services, consisting of information security professionals are tasked with defending against, tracking, and pursuing black hats – while staying within the rules of the law. Today, the most common hacks come in the form of web application attacks, denial of service, malware, advanced persistent threats (APT), and social engineering [8]. There are hacking groups like Anonymous and Lulzsec, they usually target governments, corporations, or social groups that have wronged others. The Anonymous group was founded in 2003. Since the group is decentralized, it has no real structure or hierarchy. By the time many cyberattacks like Melissa virus in 1999, Sony's Playstation network attack in 2011, 2014 cyber attack on Yahoo, WannaCry ransomware 2017 were done by hackers and they were stopped by the hackers. In the 2020s, kids want to be hackers—ethical hackers, the hacker culture is going on—maybe in a different way than how it started. Universities such as Massachusetts Institute of Technology, Carnegie Mellon University, University of California, University of Cambridge are providing the syllabus for hacking and Cybersecurity to the students.

The Motivation of a Black Hat Hacker

There is a reason or motivation behind any activities. Human beings are influenced by the motivation to do what they do. Hackers also have their motivation and reason behind hacking. Behavioral science plays a complementary role in cybersecurity, helping develop a stronger understanding of why hackers do what they do, because hackers are, at the end of the day, still humans. Different types of hackers have their own motivation and strategies. Generally black hat hackers are motivated by financial gain, revenge, and ideology [12].

In the digital era, data has become one of the most critical components of an enterprise. Hackers are motivated to expose this confidential information to unauthorized parties and it is called data breach—one of the methods of cyberattack. Data leakage poses serious threats to organizations, including significant reputational damage and financial losses. An illustrative example is the case of Yahoo, which faced two major data breaches in 2016. The first incident involved hackers compromising up to 500 million user accounts in late 2014, while the second cyber attack, discovered in December 2016, affected more than 1 billion user accounts compromised in August 2013, separate from the first breach. Another notable instance occurred between November 27 and December 18, 2013, when cyber criminals breached the data security of Target Corporation, leading to the theft of personal information, including names, addresses, phone numbers, email addresses, and financial details, affecting up to 70 million customers [13, 14]. The major motivation behind data breach was found to be desire to steal money along with espionage and ideology.

Another type of cyber attack frequently used by hackers is malware attack. A software S is malware by definition if and only if S damages a non-damaging software system or software system that damages malware [15]. Worms, viruses, ransomware, rootkits etc are fully under the category of malware. These attacks are carried out for entertainment, peer recognition, revenge, infrastructure damage etc. Some examples of malware attacks are: WannaCry ransomware in 2017, Stuxnet computer worm in 2010, IloveYou virus in 2000 etc.

Motivation of hack carried out by black hat hacker can be categorized into following themes:

Financial gain

Money is an essential part of our life in order to live in this universe. Hackers hack to seal or earn money. This can be done through misusing data, data breach and selling data on the dark web—it is the dark side of the internet, which is not indexing from google search engine and normal browser, selling malware, ransom demand, pirating software etc. Target Cyber breach is an example of this motive. In 2013, a group of hackers stole the credit and debit card information of millions of Target customers during the holiday shopping season. The attack went undetected for several weeks, during which time the hackers were able to steal the data of approximately 40 million customers. The attack resulted in losses of over $200 million for Target. The attackers were later identified as a group of hackers based in Russia and Ukraine, who were believed to have sold the stolen data on the black market for millions of dollars [16].

Taking personal revenge

Some hackers hack any person or company for revenge and either they use data for the wrong purpose or damage infrastructure. In 1994 Kevin Mitnik—once he was the world's most famous hacker, now he is a speaker, cybersecurity consultant, and a global authority on social engineering—hacked into the computer systems of Shimomura Security, a company owned by security expert Tsutomu Shimomura for revenge. Mitnick had a personal grudge against Shimomura, who had helped the FBI track down Mitnick and eventually led to his arrest [17]. Password cracking and compromising social media accounts are the common example of this motive.

Ideology

This is the set of beliefs and values that motivate hacking. Anonymous' hacking occurred in 2011 is ideology driven hacking. The group launched a series of attacks against the websites of government agencies, corporations, and organizations that opposed the whistleblowing site WikiLeaks. Anonymous was motivated by the belief that governments and corporations were suppressing information and infringing on people's right to free speech [18].

Curiosity and ego

Hackers are problem solvers and creative by nature. Individuals or a group of such hackers use their skill to show up how powerful they are, or sometimes they want to be popular for their task so they perform hacking. Gary McKinnon, a British hacker who carried out what has been described as the "biggest military computer hack of all time." In 2002, McKinnon was accused of accessing and damaging computer systems belonging to the US Army, Navy, Air Force, and NASA. He claimed that he was searching for evidence of UFOs and extraterrestrial technology. McKinnon's motivations for carrying out the hacks were reportedly to gain recognition as a skilled hacker and to prove that the US government was covering up evidence of extraterrestrial life.

Enjoyment

Some black hats hack the organization or people only for fun and enjoyment. They found themselves happy by watching the trouble of the people. Mostly Distributed Denial of Service (DDoS) attacks are done to achieve that motive.

Many authors explained about motivation factors that why individuals turn to hacking. These factors include addiction, curiosity, entertainment, money, power/ego/recognition, ideology, and revenge [19].

How do they hack?

Hacking is not the task of fewer minutes. It may require planning, patience and research. There is no hard and fast rule but all of the hackers follow a similar process. The phases included in this process are information gathering, scanning, gaining access, maintaining access, and covering tracks. This is often called phases of ethical hacking [20].

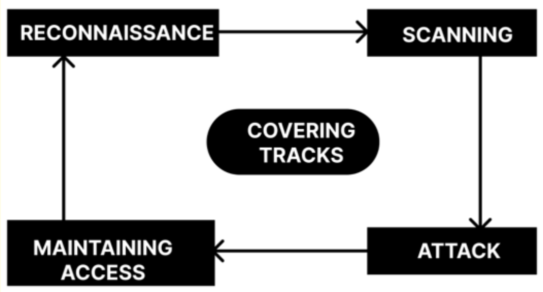

Figure 3: Hacking methodology.

Information Gathering/Reconnaissance

This step involves the collection of information as much as possible about the target. Active and passive reconnaissance are the techniques involved in information gathering. Passive refers to collection of information indirectly whereas active refers to indirect collection of information.

Scanning/Enumeration

It is done to identify live systems, open ports, services, and potential vulnerabilities. This includes network scanning, port scanning and vulnerability scanning.

Gaining Access/Attack

The objective of this stage is to exploit identified vulnerabilities to get unauthorized access to the target system.

Maintaining Access

It ensures the continuous access of the target system without detection. It can be done through Rootkit, Backdoor etc.

Covering Tracks

Throughout the phases, needed to remove the evidence of hacking activities to avoid detection. Some techniques used include clearing history, removing logs.

A skill by which an unknown person gains the trust of someone and this leads one step forward in hacking. This skill is called social engineering, hackers attack on the weakest link—humans. This might be a non technical skill but the technical skill for hacking is exploiting vulnerabilities. Most of the hacks use the combination of social engineering and technical hacking skills [13, 16]. At this point the hacking is connected with human psychology.

Findings

Hacking is a mindset more than a skill so it is connected with human psychology. Hackers are smart and highly skillful people, both black and white hats have in-depth knowledge but the difference is black hats are using their skills illegally like they didn’t learn any wisdom with knowledge. Being such illegal activity and unethical, normal hackers are influenced by materialistic things like financial gain, revenge, enjoyment, ideology etc. and start becoming black hats. Some hackers are transformed into black hats due to their compulsion like shortage of money, some are driven by powerful people or black hats, and some fall into the circle of such black hats unknowingly. A hack is accomplished through two types of factors namely influencing and achieving factors. Influence factor leads to excitement, whereas achieving factors leads to execution.

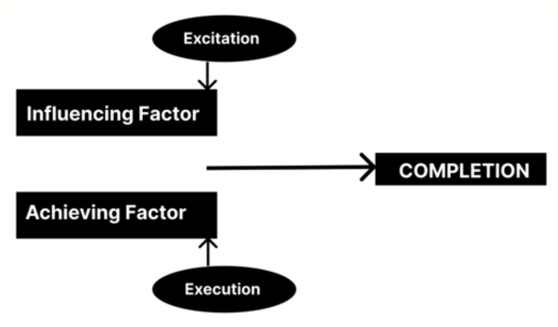

Figure 4: Influencing and Achieving factor in hacking.

Great power comes with more responsibility, but after getting such great power of knowledge, some want to show off their knowledge to destroy things. After certain unethical tasks, some become slavery to their own habits. By following the rule of the more you have, the more you want, normal hackers want to earn more and more money and they want power, they can go into any situation to make themselves powerful so unknowingly or knowingly they are transformed into a black hat. They generally use the most widely used techniques of social engineering and technical hacking to break into the system. So the most vulnerable factor is human weakness and the influencing factor is their motivation.

Conclusions

The hacker culture originated from the TMRC at MIT. There was a hacker dream, the betterment of human life through a computer. There was not any concept of damaging the infrastructure and destroying the network, nor the concept of black hat hackers. Hackers used their skills to improve the computer system. Through the evolution of this culture the dark side is separated from the white side and the concept of the black hat is generated. They were using their skills in an illegal way, they are selling breached data into the darknet. Some hackers are transformed into the black hat to get their motivation and some are transformed forcefully.

Like two parts of a coin, there are two sides of hacker which are clearly separated, one is using their skills for betterment but another is using them for the opposite. Black hat hackers are criminals while white hats are ethical hackers. New generations are becoming more aware of such hacking groups and they want to become an ethical hacker. Really the ethical hackers doing and flowering the hacker culture seed by the TX-0 hackers. In spite of the destruction, black hats also support the advancement of technology and creative thinking so that computer systems are evolving and are the way of advancing in technology.

References

1. Levy S. “Hackers: Heroes of the computer revolution”. Garden City, NY: Anchor Press/Doubleday; (1984).
2. Sune D Müller and F Ulrich. “The Competing Values of Hackers: The Culture Profile that Spawned the Computer Revolution”. ResearchGate (2015): 2-5.
3. Jordan T. “Hacking: Digital media and technological determinism”. Polity (2008).
4. Nasr E., et al. An Analytical Approach to Psychological Behavior of Hackers’ Motives.
5. Raymond ES. “How to become a hacker”. Database and Network Journal 33.2 (2003): 8-9.

6. Turgeman-Goldschmidt O. “Meanings that hackers assign to their being a hacker”. International Journal of Cyber Criminology 2.2 (2008).
7. “History & Impact of Hacking: Final Paper”. History of Computing 5-6.
8. TC Summers. “How Hackers Think: A Mixed Method Study of Mental Models and Cognitive Patterns of High-Tech Wizards”. (2015): 11-16.
9. G Vishnuram, K Tripathi and A Kumar Tyagi. “Ethical Hacking: Importance, Controversies and Scope in the Future”. 2022 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India (2022): 01-06.
10. Bender E. “Nightwork, updated edition: A History of Hacks and Pranks at MIT”. Mit Press (2011).
11. Stallman RM. What is free software. Free Society: Selected Essays of (2002).
12. Chng S., et al. “Hacker types, motivations and strategies: A comprehensive framework”. Computers in Human Behavior Reports 5 (2022): 100167.
13. Cheng L, Liu F and Yao D. “Enterprise data breach: causes, challenges, prevention, and future directions”. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 7.5 (2017): e1211.
14. Daswani N., et al. “The Yahoo Breaches of 2013 and 2014”. Big Breaches: Cybersecurity Lessons for Everyone (2021): 155-169.
15. Kramer S and Bradfield JC. “A general definition of malware”. Journal in computer virology (2010): 105-14.
16. Finkle J and Skariachan D. “Target cyber breach hits 40 million payment cards at holiday peak”. Reuters (2013).
17. J Littman. “The Fugitive Game: Online with Kevin Mitnick”. Houghton Mifflin (1997).
18. G Coleman. “Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous”. Verso Books (2014).
19. McBrayer J. “Exploiting the digital frontier: hacker typology and motivation”. The University of Alabama (2014).
20. Juneja GK. “Ethical hacking: A technique to enhance information security”. International Journal of Innovative Research in Science, Engineering and Technology 2.12 (2013): 7575-80.

Volume 6 Issue 6 June 2024