INTRODUCTION TO HACK

2021

MOJTABA MALEKI

Introduction
To
Hack

Mojtaba maleki

ISBN:

TO MY FATHER WHO IS MY ONLY HERO DURING MY LIFE.

AND

MY MOTHER WHO ALWAYS ENCOURAGED ME WITH COMPASSION.

MY DEAR AND KIND PARENTS THANK YOU VERY MUCH FOR BEING MY FRIEND AND SUPPORTER AT ALL STAGES OF MY LIFE, AND I DEDICATE THE FIRST RESULT OF AN EFFORT OF MY LIFE TO YOUR KINDNESS.

CONTENTS

ACKNOWLEDGMENTS

Special thanks from my best friend Mr.Afshari, who supported me in all stages of my life.

1 INTRODUCTION

“Introduction to hack” is a book that includes some information that all hackers must know. The focus of it is the theory of hack. It is a kind of navigator and stand’s out what to do to become a hacker. It illustrates the Dark Web, the hacker’s tools, the most famous techniques, and it will answer some beginner hacker’s questions. Some people want to be a hacker but they don’t care about some basics of it. On the other hand, finding these pieces of information on the Internet is very hard. So this book gathered all of that information in one short book to navigate you into one of the most exciting subjects. This book contains some biography of the most famous hackers and their meetings. If you want to be a hacker but don’t know how to start, you choose the right book. Now that we have the introductions out of the way, continue onto the first chapter to start learning about what is the hack?

2 WHAT IS THE HACK?

Most people even don’t know what is the Hack? In general, hack means, doing something with one object which is not designed for. For example, using a microwave to make a cup of coffee, is one type of hack and the person is a hacker because a microwave has been invented to cook food, not to make coffee. In the computer world, hack means using a different kind of elements to have access to something which is locked for people. This action happens for many reasons and it could be very dangerous sometimes.

One of the reasons is political activity. When a country wants to know about the secrets of other countries they try to hack them in the use of politics. In this case, mostly, the government will gather very professional people to do this for them. Being a hacker and work for the government is a top-secret job and nobody doesn't knows these hackers.

The other reason for hack could be personal advantages. For example, someone has some problems with another person or even a company, etc. He wants to get revenge on the person or company. The other type is hacking a server or personal account of someone and ask them for money instead of sharing their data.

There is one other type of hacker that is good. Maybe you are asking how could a hacker be good? In this case, a hacker hacks a website, server, etc to warn them this system is not safe enough and give them clues to fix it. This type of hacker has benefits. One of the benefits is that place will be safe and other hackers and cannot take advantage of it. The other benefit is, tech companies pay good money to these people. Because they helped them to make their servers more secure.

3 HISTORY OF THE HACK

The term hacking dates back to the 1970s. In 1980, the term hacker was used in an article in the journal Psychology Today. This article dealt with the addictive nature of computers. In 1982, a sci-fi film titled Tron was released, with the protagonists seeking to infiltrate and hack into one of the companies' computer systems. The character in another film, WarGames (1983), is a teenager who infiltrated the North American Aerospace Defense System (NORAD). In the film, hackers are presented as a threat to national security. Thus, art became a prelude to reality.

In 1983, a group of teenage hackers infiltrated U.S. and Canadian computer systems, including Los Alamos National Laboratory and Sloan Kettering Cancer Center, and Pacific Security Bank. Shortly after, an article was published in Newsweek magazine with a cover photo of one of the teenage hackers, and the word hacker was first used in this article. After the events, Congress stepped in and passed laws on computer crimes. In the 1980s, numerous hacker groups were formed in the United States and elsewhere, seeking to attract enthusiasts for some missions. Some of these missions were safe and others dangerous.

From the 1980s onwards, many attacks and intrusions into institutional and government computers, followed by numerous laws to combat hacking, were passed, and many people active in the field were arrested. However, popular culture accepted hacking and hackers in the form of specialized videos and books, and magazines.

4 WHO IS A HACKER?

Hacker is a person who has high familiarity with equipment which he or she uses and can do several things which those tools were not designed to use in that way.

Hacker in the computer science world means a person who has complete familiarity whit the computers and knows how they work, so he or she can do many things which others can’t, because others are not that familiar with

those tools.
From this introduction for hackers, we can understand that all of the hackers know how computers work and also this means most of the hackers (not all of them) are well educated and they know computers from scratch.
A hacker must be professional in the software and hardware of computers. He or she has to know how to work with programming languages. Programming is one of the most important things in the hack. No hacker in the world could say they can hack into something without programming. Programming is the basic of the computers and all of the hackers must be professional in that. This book covered all of the basic data about programming languages.

Hackers must know how the hardware of computers works. Hackers must know all of the detail of the hardware part of a computer such as RAM and CUP, etc (this book covered some basics of how computer hardware works in “how the

hardware of computer works”).
Based on what a hacker wants to do, he must know about Deepweb and Darkweb which are both covered in the “DARKEWB AND DEEPWEB” chapter.
One of the most important things about hackers is to have hacker's behavior. This means that, be in the computer atmosphere which means find other people who are interested in computer (or even hack) find each other and learn from each other about how computers work, how all world are connected, etc.
Another tip is to think like a hacker which this book covered some tips in the “How to think like a hacker?” chapter.

5 WHAT TYPE OF HACKERS ARE THERE?

White hat hackers:

Hackers who work for government and companies are White hat hackers. White hat hacker's duties are cybersecurity. All of the governments and big companies such as Google have cybersecurity engineers to protect their data and keep them safe. For example, the duties of Instagram cybersecurity engineers are protecting your personal information such as passwords from other people.

Black hat hackers:

Black hat hackers are another category of types of hackers that come in front of white hat hackers. Black Hat hackers, which also include crackers, usually pursue profitable goals and seek to create unauthorized access to systems. The activity of this group of hackers is completely illegal and usually causes heavy damage to their targets.

The Black Hat hacker is like a scientist who benefits from his knowledge for criminal purposes. Typically, the targets of this type of hacker are unauthorized access to classified information, breach of privacy, damage to systems, damage to networks, and access to bank accounts.

Gray hat hackers:

Grey hat hackers are another category of hacker types that fall between white hat hackers and black hat hackers. In order to entertain or enhance their experience, these hackers usually discover vulnerabilities and declare them so that the owners of the attacked service can fix that vulnerability.

The difference between this category of hackers and the White Helmets is that these people infiltrate without the permission of the service owner. But compared to black hat hackers, they don't commit subversive acts and don't manipulate information.

Script kiddies:

The kiddie script, commonly referred to as novice hackers, is a class of hackers who don't have much knowledge of what they're doing. This category of hackers, also known in the world of hacking and security as "hacker chicks," usually use tools and resources already made by others to hack.

Since there is not much need for

knowledge for this type of hack, a very large number of hackers fall into this category. It can be said that the kiddy script stage is one of the early stages to become a hacker, in which only a series of basic concepts are known.

Green hat hackers:

The Green Beret hacker, also known as Neophyte or Newbie, is told those who have no familiarity with the hack and are recently planning to log in. In fact, the Green Caps are a lower category than the Kiddies script, and they need a long way to go to become a hacker.

Blue hat hackers:

Blue helmet hackers can be considered a bunch of White Helmets hackers, except that they do not work within the framework of certain company security rules. Blue Hat hackers usually work as a project, and programs are usually provided before launch to be examined for bugs and flaws. These hackers check apps and services and declare their vulnerabilities to the owner.

Red Hat Hackers:

Red hats are another category of hackers whose activity falls between white hat hackers and black hats. The targets of these hackers, who have a very high level of knowledge, are usually government agencies and intelligence agencies of countries, and generally seek to hack services that deal with sensitive information.

6 WHAT JOB A HACKER COULD HAVE?

There are a lot of computers related jobs available which a hacker can do, but in this chapter, we will cover some jobs which match the hacker's feelings.

One of the impactful jobs in the computer world is cybersecurity. Cybersecurity engineers watch servers all the time to keep them safe.
 This very hard and effective job is one of the jobs which is sutable for hackers. In this job, employees have to be very

responsible and careful about every single details. If you want to be a cybersecurity engineer, you have to prepare yourself for office midnight callings.

This job is similar to work in the emergency section of a hospital, you have to take care of servers like patients.

The salary for this job depends on many elements such as country, level of experience, resume, etc. but the average annual salary for cybersecurity engineers in New York is around 125,000$.

7 IS A HACKER A WELL-EDUCATED PERSON?

This is a very common question among people who are attracted to hack. The answer is yes and no at the same time. When someone wants to hack a place, he needs to know computers and how to work with them, then how to attack them. This high amount of knowledge is achievable without going to the university and studying computers (in as much as other majors) but learning these things are much harder than something which a normal person can figure it out by themselves. When someone goes to university, he will meet other high-knowledged people such as professors who have lots of experience to share. University only does not mean that going to one place and studying some books and get a certificate. Smart people use those areas to find other people like them and try to make a connection. One of the most important things in university is making a good connection.

On the other hand, if someone wants to be a hacker need to have experience. One of the most important experiences is finding a related job. For finding related jobs, most of the places need your degree for hiring so you have to have it to get hired.

The other important thing about getting hired is being updated. When you are hired by one company, you will be in their meetings and you will see the technology development so you always update to the new technology and you know how they work, you know their strong points, you know their weakness so you can hack them.

All in all, a hacker is not necessarily a high-educated person but he needs to have knowledge. One of the best and easiest ways to be knowledgeable is going to university. The other point of going to university is meeting other highly educated people. Finding jobs and being update is one of the other advantages of going to university.

8 HOW TO BECOME A HACKER?

This chapter of the book covered two main elements to be a hacker which are Software and Hardware. Hardware is like a piano and Software is like music.

Software:
Software means the area of computers which you cannot touch. All of the programs and applications are in this section.
Programming is the alphabet of the hack. The first step of hack and become

a person who can talk about software is programming. There are lots of programming languages such as python, java, C, C++ , etc.

Computers cannot talk and they would not understand what we mean. By programming, we tell computers what to do. For example in the next picture, we tell the computer if the user gives you an even number tell him or her “Hello” but if he or she give you an odd number tell her or him “bye”. This is a very simple code which we are talking with computer and we are telling it what to do and what not to do.

The hacker must know how to work with all of them but most hackers use python for hacking. One of the most important reasons for using Python is Python has a lot of libraries that you can use to complete your process faster.

A Python library is a reusable chunk of code that you may want to include in your programs/ projects. Making these libraries from scratch is so time-consuming because in most projects hackers use libraries several times. Besides the importance of programming in software, knowing how to use an app is important too. When a person becomes a programmer, he or she will see other applications in technical ways. He or she knows how this app works so when they know how it works so they know how to use is too. When you get that point of view, you will see all of the detail of the app so you will see what others cannot see then you will use it in those ways.

Hardware:
“Hardware” refers to the physical part of the computers. Computers have several parts such as CPU, RAM, Hard Drive.

CPU:

- CPU is the short form of Central Processing Unit
- CPU job is to act like brain and follow the instruction in the code
- Image, networking, math, calculating, all happened on the CPU

- Modern CPU chips have multiple “cores”.
- Each core is a semi-independent core.

RAM:

- RAM is the short form of Random Access Memory
- It acts like a Whiteboard
- RAM storage both data and code
- When you open many tabs on your browsers each tab data is on the RAM and after closing them it like it will be clear from the whiteboard, this happened for other programs too

Hard Drive:

- High pitch spinning sound you may hear is from Hard Drive
- Persistent storage of bytes

When someone knows how these and other parts of computers work in detail, he can use them to hack (or anything else).

9 HOW TO THINK LIKE A HACKER?

Thinking like a hacker is as important as knowledge. Hackers look at what they have, they know their tool in detail. When a hacker wants to hack a place, he makes a blueprint. He says for example for hacking a web site which sends a lot of advertisement:

- This web site must be written in HTML
- The designer put some code in HTML so I can see this ad

- What systems do I need?
- He has to get access to the codes
- He is knowledgeable in designing websites so he knows how to get access to the codes.
- He revies the codes
- Find the part which is responsible for showing ADs.
- Disable the code

The main steps of the hack are:

- goal
- Pick the tools which you need
- Analysis your target
- Follow the steps one by one
- Be patient if you lost and do the steps again

By following these steps you can hack whatever you want.

10 WHAT ARE THE TOOLS?

Knowing what are the best tools you need for a different type of hack is one of the essential elements.

Hackers should be familiar with computer accessories, especially network accessories and devices.
Because you can hack something when you fully understand it and know how it works.
NOTE: based on what hacker want to hack , obviously tools are different.

For example :

Hard external:

- it is Hard Disk Drive (HDD) or Solid-state Drive (SSD) which need to be connected to the computer
- The disadvantages of these drives are they are much slower and more expensive than SSD or HDD
- Hacker use HDD and SDD in the way of Hard external because speed plays effective rule

Raspberry pi:

- A complete mini computer
- So powerful compare to the size
- So Fast
- So cheap

UberTooth one:

- A gadget for hacking via Bluetooth
- You can find online
- Open-source development board
- It looks like a naked Bluetooth USB

dongle, it can do a lot more than that

Ardiuno MKR1000:

- This device is specifically designed for projects that allow you to connect your devices to the internet.
- can be connected to your Wi-Fi network without using any Wi-Fi shield And that’s as a web server
- This device can also act as a human interface device like a USB mouse or Keyboard which can send keystrokes to the computer which is connected to it.

11 MOST FAMOUS TECHNIQUES?

Fake WAP:

One of the simplest ways to stealing personal data is setting a fake free WIFI that has no password and it seems to be safe. Once they are connected to the router, the hacker can monitor and even change the internet connection to steal data or force them to download malware onto their device.

Bait and switch:

In this type of hack, hackers show you an advertisement, and users by clicking on them would be hacked. By doing so, the hacker can use several other attacks like downloading malware, clickjacking, or browser locking, to compromise your system.
Always try not to click on ads which sources are not verified.

Wordlist:
Hacking via wordlist is also one of the most popular techniques of hacking. Hackers make a list of words in which your password is included. the number of the words in that word list sometimes could be very large, for example, a simple wordlist which is 8 characters long, containing only numbers, has 100000000 elements. But another faster way is guessing the person's password with our knowledge about them.
For example, someone's name is Judy, she was born in 2002 and her dog name is Poppy.
Wordlist for this person is similar to this:

- Judy20022002
- Ju2002dy
- Judylovepopy2002
- Judy02popy
- Popy2002judy
- Popyandjudy
- Etc.

This method may sound silly, but it’s the most common way to hack a password. So think more, before choosing a password!

These are just three, common ways of hacking; depending on the situation, methods will change.

12 DARKWEB AND DEEPWEB

What is DeepWeb?

DeepWeb simply refers to a part of the web that search engines and guest users cannot access, for example, websites that you need to login to your account to access, such as the university unit selection page, your email account, the communities and sites in which you need to have an account to view their content, the content management systems pages of websites, website databases, Social networking profiles and...

All of these are examples of DeepWeb, as you can see, we deal with a lot of these things on a daily basis, and in fact, we've all ever logged in and used deepweb.

So with these deepweb interpretations in itself is not a dangerous nature, many people confuse DeepWeb with DarkWeb, follow along with us to thoroughly review DarkWeb and tell you everything you need to know about it.

What is DarkWeb?
A network of websites is called out of the public's reach and can only be accessed using certain tools since it is almost untraceable, any crime such as dealing guns and drugs, harassing human beings, supplying false documents, trafficking human organs, soliciting the murder of a human being, asking for the hacking of a person and any other illegal activity. To think about it can happen.
Since these networks are established in

completely isolated environments and no information is available from their operators, it is somewhat impossible for governments to track these individuals, although there are also instances of police arrests of these individuals.

DarkWeb is a safe environment for criminals, they can expand their illegal activities and make more money, dealing on such websites is usually done through Bitcoin so that it cannot be tracked and tracked.

What is the story of Red Room in Darkweb?

WARNING: The text you read below is somewhat disturbing, please refer to the next section of the article if you have certain conditions, pregnancy, or heart problems, without reading this section, the information that has been circulated online about darkweb red rooms, rumors, and the purpose of these people is only to exploit people's curiosity and receive money, so far no valid document has been found about the existence of a red room in darkweb.

The first thing we remember when we hear the name of the Red Room is pain, torture, and bloodshed, but is it true? Perhaps you've also heard that in darkweb's red rooms, people pay to watch live, eat human flesh, cut limbs, murder, torture, rape children and harass others! But you should know, the existence of such a thing on DarkWeb is only a rumor, and the public red room has not done anything after receiving the money, no torture, no live broadcasts! The only purpose behind these websites is to exploit people's curiosity and steal the money they pay.

ATTENTION: Again, we recommend that you do not enter the dark web environment as much as possible as, in addition to the risks on this network, illegal and inhumane activities are also carried out in

which viewing them will only make you uncomfortable and relaxed!!

13 DEF CON

DEF CON is one of the most important and significant hacker gatherings in the world, held annually in Las Vegas, Nevada. DEF CON’s first event took place in June 1993, and today many of its participants include computer security professionals, journalists, lawyers, federal government employees, security researchers, students, and hackers interested in software, computer architecture, hardware modification, and anything that can be "hacked." The event includes several lecture sections on computer-related topics — and hacking — as well as cybersecurity challenges and competitions.

The competitions held during the event vary greatly, from creating the greatest connection distance of a device to Wi-Fi to finding the most effective way to cool a beer in the Nevada heat. But perhaps the most important competition is the Flag Capture Event (CTF), in which teams of hackers must defend or attack computers and networks that are provided with certain hardware, software, and architecture.

14 MOST FAMOUS HACKERS

Kevin Mitnick

Kevin Mitnick, who is a key figure in hacking American systems, began his career as a teenager. In 1981, he was charged with stealing computer booklets from Pacific Bell Telephone Company. In 1982 he hacked the North American Defense Command (NORAD), an achievement that inspired the 1983 film War Games. In 1989 he hacked the Digital Equipment Corporation (DEC) network and copied copies of their software. Since DEC was a leading computer manufacturer at the time, this practice put Mitnick at the center of attention. He was later arrested and convicted and sent to prison. He hacked Pacific Bell's voicemail systems during parole.

During the hacking Mitnick never used access to the systems and data obtained. The general public says he once gained full control of the Pacific Bell network simply, only to prove it was doable. A warrant was issued for the Pacific Bell incident, but Mitnick escaped and lived in secret for more than two years. When caught, he was imprisoned on several counts of computer fraud.

Although Mitnick eventually continued his career as a White Helmets hacker, he may be part of the gray area wearing both hats. In 2014, he launched "Mitnick's Absolute Zero Day Exploit Exchange", which sells unofficial and important software interests to the highest buy offer, according to Wired magazine.

Image courtesy: Mikhail Romanenko

Anonymous
Launched in 2003 on 4chan message boards in an unnamed forum. This organizing group shows little of itself

and is more focused on the concept of social justice. In 2008, for example, the group clashed with the Scientology Church and dismantled their websites.

So this negatively affected their search rankings on Google, and fax machines covered them with completely black images. In March 2008, a group of "Annus" wearing the famous Guy Fawkes mask passed through Scientology centers around the world.

As The New Yorker magazine noted, while the FBI and other law enforcement agencies have tracked down some of the group's most labored members, identifying all members of the group can't be done because they have left no identities.

Adrian Lamo

In 2001, Adrian Lamo, in the age of 20, used an unprotected content management tool at Yahoo to correct a

Reuters article and add fake quotes attributable to former Attorney General John Ashcroft. Lamo often hacked systems and then informed both the press and his victims.

In some cases, he could help clean up their problems to improve their security. As Wired magazine noted, Lamu added himself to the list of expert sources in 2002 when he hacked the New York Times intranet and began investigating prominent public figures. Lamo Manicer was nicknamed "The Homeless Hacker" because he preferred to patrol the streets with a backpack and often had no specific address.

WANTED
Adrian Lamo
DEAD OR ALIVE
© 2010 CBS Interactive

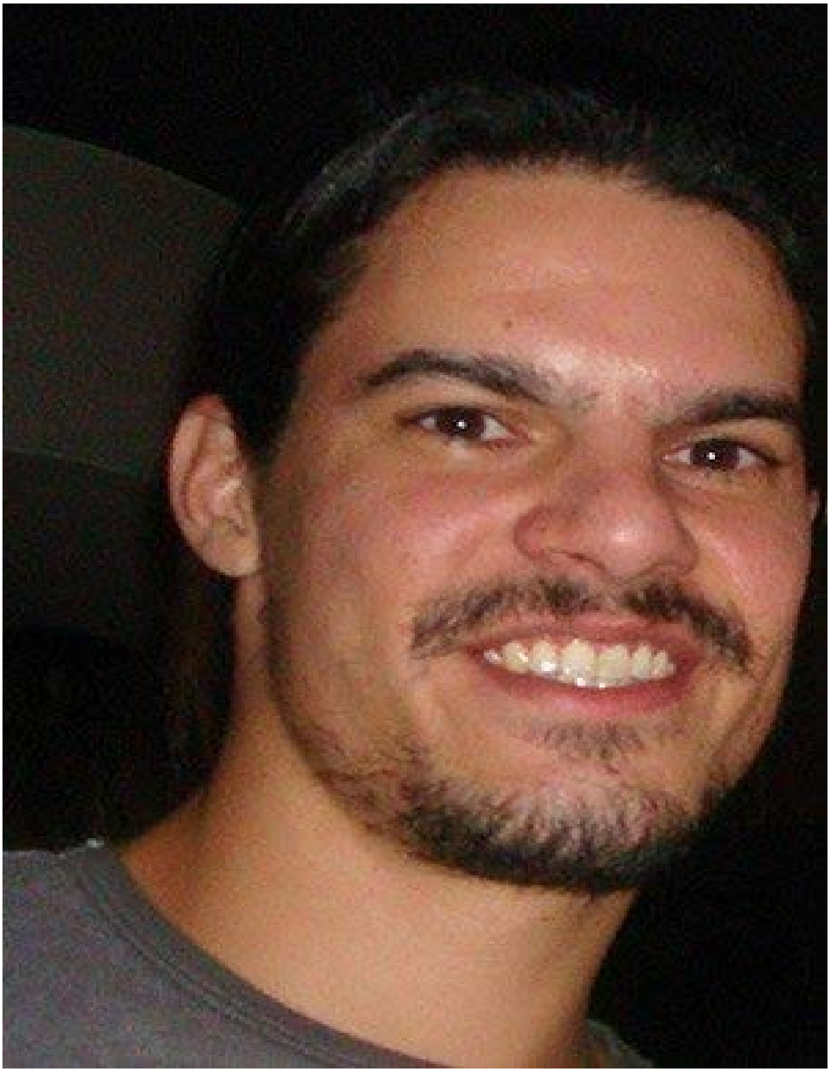
Albert Gonzalez

Gonzalez, one of the world's biggest hackers, was dubbed "Sopanazi," according to the New York Daily News. He began his career as a "leader of the Computer Troublers Group" at a high school in Miami. He was eventually activated on the criminal trading site Shadowcrew.com and was considered one of the best hackers and executors.

At 22, Gonzalez was arrested in New York for credit card fraud related to the theft of information from millions of bank accounts. To avoid imprisonment, he became a Secret Intelligence Service informant and eventually helped in issuing indictments to Shadowcrew members.

Gonzalez continued his criminal activities during his career as a paid informant. Along with a group of collaborators, Gonzalez stole more than 180 million payments from companies such asOfficiceMax, Dave and Buster's, and Boston Market.

The New York Times Magazine noted that Gonzalez's 2005 attack on U.S. retailer TJX was the first breach of bank account information. He was a serial offender and using SQL, this famous hacker and his team created a way in several corporate networks. They stole about $256 million from TJX alone. During Gonzalez's 2015 punishment, the federal prosecutor called Gonzalez's crimes "unparalleled."



Matthew Bevan and Richard Pryce

Matthew Bevan and Richard Pryce are a team of the biggest hackers in the UK and even the world who attacked several military networks in 1996, including Raf Griffith Air Base, the Defence Intelligence Agency, and the Korea Institute for Nuclear Research (KARI).

Bevan (kuji) and Pryce (Datastream Cowboy) have been accused of starting World War III after putting KARI research on U.S. military systems. Bevan claims he sought to substantiate the UFO conspiracy theory. According to the BBC, his case bears much resemblance to that of Gary McKinnon. Bevan and Pryce's crimes showed that even military networks are vulnerable.

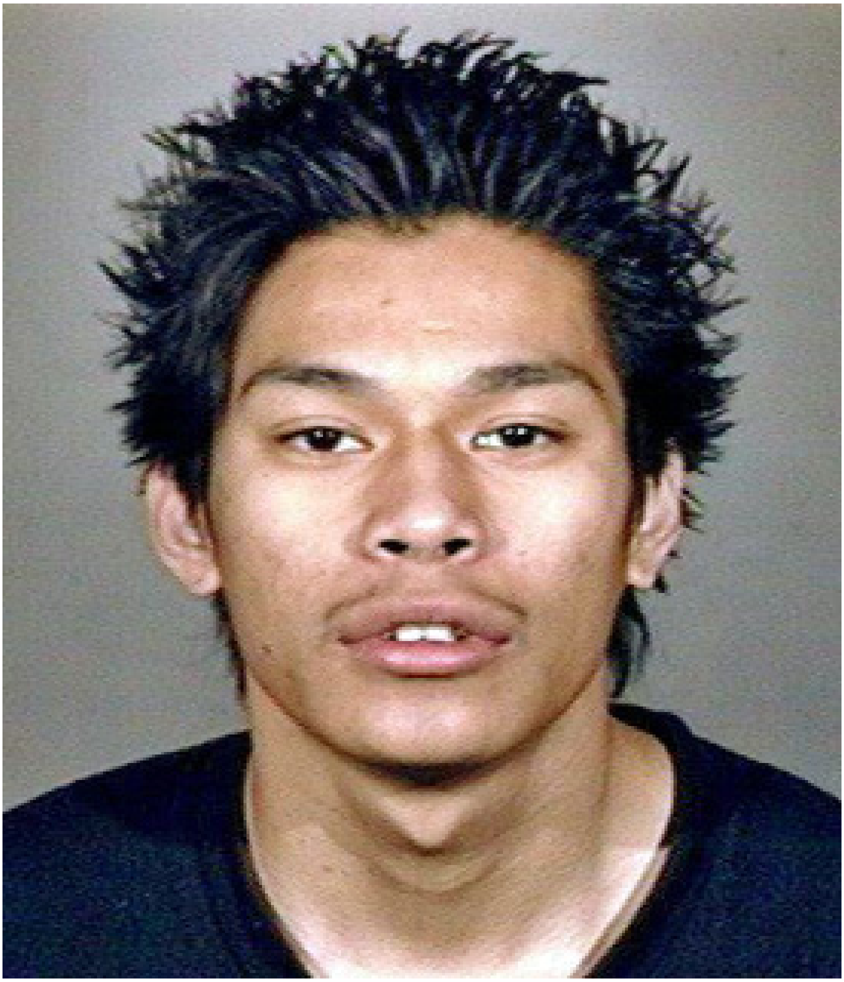
891 A
Adelaide

Jeanson James Ancheta

Jeanson James Ancheta was not interested in hacking bank accounts or sabotaging networks to realize social justice. Instead, Ancheta was curious about the use of robots, software-based robots that can infect and control computer systems.

Using a large-scale "botnet" series, he was able to compromise more than 400,000 computers in 2005. According to Ars Technica magazine, he rented these machines to advertising companies and was also paid to install robots or advertising software directly on specific systems.

Ancheta was sentenced to 57 months in prison. It was the first time a hacker had been sent to prison for using botnet technology.



Michael Calce

In February 2000, 15-year-old Michael Kalles, known as "Mafiaboy," discovered how to take over the university's computer networks. He used their combined resources to disrupt the number one search engine at the time (Yahoo). Within a week, he overthrew Dell, eBay, CNN, and Amazon companies using distributed attacks and denial of service (DDoS), causing corporate servers to be overthrown and their websites broken.

Kals' wake-up move was perhaps the most troubling move for cybercrime leaders and internet advocates. If the world's largest websites, worth more than $1 billion, could simply be marginalized by hackers, would online data be safe all over the world? It is no exaggeration to say that the development of the CyberCrime Act suddenly became a top government priority thanks to the Kals hack.

Kevin Poulsen

In 1983, 17-year-old Poulsen, nicknamed Dark Dante, hacked the Pentagon's computer network ARPANET. Although he was caught quickly, the government decided not to prosecute Poulsen, who was a minor at the time. Instead, he was fired with a warning.

Poulsen did not heed the warning and continued to hack. In 1988, Poulsen hacked a federal computer and uncovered files related to the deposed Philippine President Ferdinand Marcos. Poulsen stepped on the run when he was identified by authorities.

As he fled, Poulsen was busy hacking government files and revealing secrets. According to his website in 1990, he hacked a radio station contest and announced he was the 102nd caller, winning a Porsche, a vacation trip, and $20,000.

Poulsen was arrested early and banned from using a computer for three years. He has since turned to White Helmets hacking and journalism, writing about cybersecurity and web-related social-political reasons for Wired and Daily Beast magazines and his blog Threat Level.

Paulson also worked with other prominent hackers to work on a variety of projects dedicated to social justice and freedom of information. Perhaps most importantly, his collaboration with Adam Swartz and Jim Dolan was to develop secureDrop's open-source software, originally known as DeadDrop. Paulsen eventually handed over to the Press Freedom Foundation a platform that enabled secure communication between journalists and sources.

Jonathon James

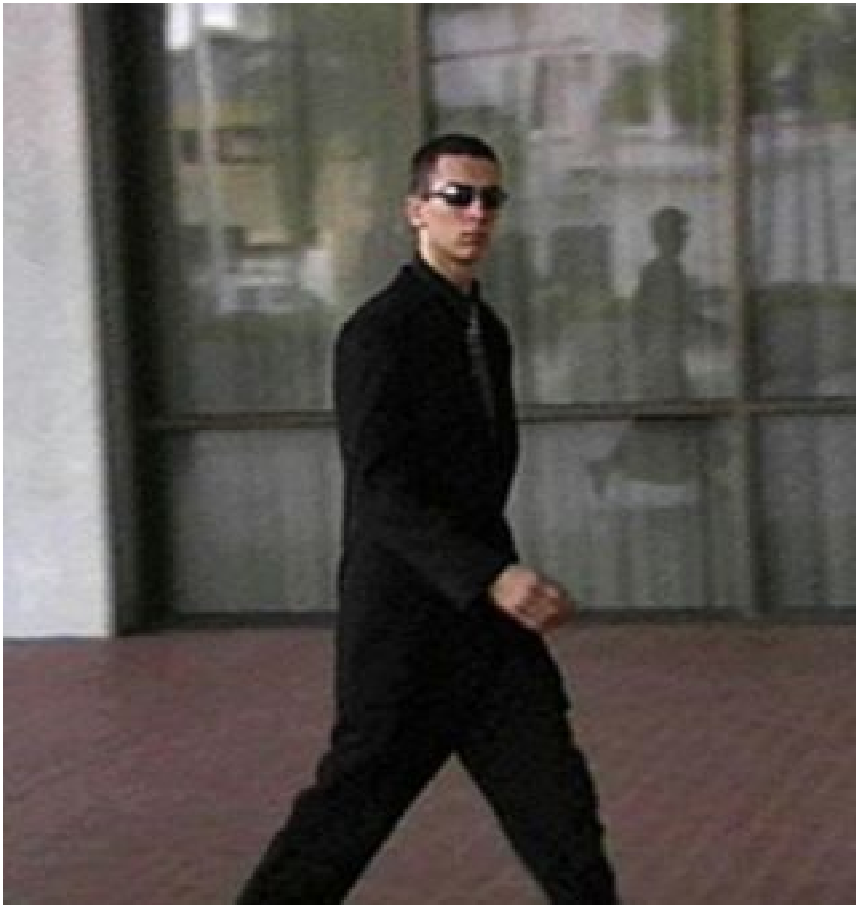
Jonathan James hacked several companies using the pseudonym cOmrade. According to the New York Times Magazine, what caught James' attention on the hacking was his attack on U.S. Department of Defense computers. Even more impressive was the fact that James was only 15 at the time.

In an interview with PC Mag magazine, James admitted that he was partly inspired by The Cuckoo's Egg, which detailed a hacking computer hacker in the 1980s. The hacking gave him access to more than 3,000 messages from civil servants, their usernames, passwords, and other sensitive information.

James was arrested in 2000 and sentenced to six months of house arrest and a ban on computer use. However, a probation violation caused him to be in prison for six months. Jonathan James, one of the world's largest hackers, became the youngest person found guilty of violating cybercrime laws.

In 2007, TJX was hacked and much of customers' private information was compromised. Despite the lack of evidence, authorities suspect James was involved.

In 2008, James committed suicide by firing a shot. "I have no faith in the "justice" system," he said in his suicide note, according to the Daily Mail. Perhaps today's actions of me and this letter will send a stronger message to the public. Either way, I've lost control of this situation and that's my only way to regain power.



ASTRA
The hacker was allegedly hacking the Dassaou group for almost half a decade. At the time, he stole advanced weapons software and data and then sold it to 250 people worldwide. His hacking damage for dassauds group was $360 million. No one knows why his full identity has never been revealed. But the word 'ASTRA' is a Sanskrit word meaning "weapon."

Some of these world's biggest hackers were planning to make the world a better place. Others wanted to prove UFO theories. Some wanted money and others famed. All of these people played a key role in the evolution of the Internet and cybersecurity.

ABOUT THE AUTHOR

Mojtaba Maleki is a computer science student at the University of Debrecen in Hungary. He is interested in continuing his study on Machine Learning for his master. He decided to share his knowledge by publishing several books related to computer science. Meanwhile, he is in a professional area and has a good connection whit his professors.