TASK-1

K. Naveen Abhiram

21BCE7357

Explore Top 10 notorious Hackers in the world and summarize into their categories. (White Hat, Grey Hat, Black Hat)

1. Kevin Mitnick

Kevin Mitnick, a prominent figure in the world of American hacking, embarked on his career as a teenager. His journey began in 1981 when he faced charges for pilfering computer manuals from Pacific Bell. In the subsequent year, he accomplished a significant feat by hacking into the North American Defence Command (NORAD), an event that served as an inspiration for the 1983 film "War Games."

In 1989, Mitnick made a noteworthy intrusion into Digital Equipment Corporation's (DEC) network and replicated their software. This act catapulted him to notoriety, as DEC was a prominent computer manufacturer at the time. However, his actions didn't involve exploiting the access and data he obtained. It is widely believed that he once gained full control of Pacific Bell's network solely to demonstrate its vulnerability. Although a warrant was issued for his arrest in connection with the Pacific Bell incident, Mitnick decided to go into hiding, where he remained concealed for more than two years. Eventually, he was apprehended and subsequently served a prison sentence for multiple counts of wire fraud and computer fraud.

Mitnick's transition to a "white hat" hacker was marked by a degree of ambiguity. In 2014, he launched "Mitnick's Absolute Zero Day Exploit Exchange," a platform that auctions unpatched critical software exploits to the highest bidder, as reported by Wired.

It's essential to note that Kevin Mitnick's hacking career has been marked by both illicit activities and a later shift toward ethical hacking, blurring the lines between "black hat" and "white hat" in the world of cybersecurity.

2. Anonymous

Anonymous emerged in 2003 within the confines of an unspecified forum on 4chan message boards. The group operates with minimal organizational structure and loosely centres its activities around the idea of social justice. Notably, in 2008, Anonymous targeted the Church of Scientology, initiating cyberattacks that disrupted the church's websites and tarnished their search engine rankings, while also inundating their fax machines with all-black images.

In a notable display of protest, a collective of "Anons" donned the iconic Guy Fawkes mask and marched in front of Scientology centres worldwide in March 2008. The New Yorker has pointed out that while law enforcement agencies, including the FBI, have identified and apprehended some of the group's more active

participants, Anonymous' lack of a formal hierarchy renders it exceptionally challenging to pinpoint or dismantle the collective as a whole.

3. Adrian Lamo

In 2001, a 20-year-old named Adrian Lamo gained unauthorized access to an unprotected content management tool at Yahoo. During this incident, he made unauthorized changes to a Reuters article and inserted a fabricated quote, falsely attributing it to former Attorney General John Ashcroft. Lamo was known for frequently hacking into computer systems and had a unique approach of notifying both the affected parties and the press. Surprisingly, in some instances, he would assist in resolving the security vulnerabilities he discovered to enhance their security measures.

However, as Wired magazine points out, Lamo crossed ethical boundaries in 2002 when he infiltrated The New York Times' intranet. During this breach, he not only added himself to the list of expert sources but also conducted unauthorized research on prominent public figures. Due to his unconventional lifestyle and nomadic tendencies, Lamo earned the nickname "The Homeless Hacker" as he often wandered the streets with little more than a backpack and lacked a fixed address.

4. Albert Gonzalez

According to reports from the New York Daily News, Albert Gonzalez, known by his online alias "soupnazi," initially gained notoriety as a leader among computer enthusiasts during his time at a Miami high school. Unfortunately, he took a dark turn and became involved in criminal activities on the Shadowcrew.com platform, where he established himself as a skilled hacker and moderator. At the age of 22, Gonzalez faced arrest in New York for debit card fraud, linked to the theft of data from millions of card accounts. In an attempt to avoid imprisonment, he cooperated with the Secret Service as an informant, contributing to the indictment of numerous members of the Shadow crew.

Shockingly, while acting as an informant, Gonzalez continued his criminal endeavours. Teaming up with a group of associates, he orchestrated the theft of over 180 million payment card accounts, targeting companies such as OfficeMax, Dave and Buster's, and Boston Market. Notably, Gonzalez's 2005 breach of US retailer TJX marked a significant milestone as the first large-scale data breach of credit information. Using a relatively straightforward SQL injection technique, this infamous hacker and his team exploited vulnerabilities in various corporate networks, resulting in an estimated $256 million stolen from TJX alone. At his 2015 sentencing, federal prosecutors described the extent of human victimization caused by Gonzalez's actions as "unprecedented."

5. Matthew Bevan and Richard Pryce

Matthew Bevan and Richard Pryce, known as "Kuji" and "Data stream Cowboy" respectively, formed a British hacking team in 1996. They gained notoriety for infiltrating various military networks, including Griffiss Air Force Base, the Defence Information System Agency, and the Korean Atomic Research Institute (KARI). Their actions raised concerns about the potential for international conflict when they deposited KARI research onto American military systems. Bevan claimed his motive was to uncover a UFO conspiracy theory. This case drew parallels to that of Gary McKinnon. Whether driven by malicious intent or not, Bevan and Pryce exposed vulnerabilities in military networks, highlighting the need for improved cybersecurity measures.

6. Jeanson James Ancheta

Jeanson James Ancheta had no interest in hacking systems for credit card data or crashing networks to deliver social justice. Instead, Ancheta was intrigued by the potential of bots—software-based robots capable of

infecting and ultimately controlling computer systems. Through the deployment of extensive "botnets," he managed to compromise over 400,000 computers in 2005. According to Ars Technica, he proceeded to lease these machines to advertising companies and also received payment for directly installing bots or adware on specific systems. Ancheta received a 57-month prison sentence, marking the first instance of a hacker being incarcerated for employing botnet technology.

7. Michael Calce

In February 2000, a 15-year-old individual named Michael Calce, who later became known as "Mafia boy," made a significant discovery in the realm of computer networks. He found a way to take control of networks of university computers and harnessed their combined resources to disrupt the operations of prominent online entities, including the leading search engine at that time, Yahoo. In just one week, he successfully executed distributed-denial-of-service (DDoS) attacks, overwhelming corporate servers and causing the websites of major companies like Dell, eBay, CNN, and Amazon to crash. This incident sent shockwaves through the world of cybercrime and the internet itself.

The magnitude of the disruption caused by Calce raised pressing questions about the security of online data. It prompted a fundamental shift in priorities for both cybercrime legislation and internet security efforts. The realization that even the largest and most valuable websites, collectively worth billions of dollars, could be easily incapacitated underscored the urgency of enhancing cybersecurity measures and enforcing stricter cybercrime laws.

This event served as a wake-up call, leading governments to recognize the critical need for robust cybersecurity strategies and legislation to protect digital assets in an increasingly interconnected world.

8. Kevin Poulsen

In 1983, a 17-year-old Kevin Poulsen, using the pseudonym Dark Dante, gained unauthorized access to ARPANET, the computer network used by the Pentagon. Although he was swiftly apprehended, Poulsen, being a minor at the time, was not prosecuted by the government but rather cautioned.

Poulsen, however, disregarded this warning and continued his hacking activities. In 1988, he infiltrated a federal computer system and accessed files linked to the deposed president of the Philippines, Ferdinand Marcos. Upon being discovered by authorities, Poulsen went into hiding. During his time on the run, he engaged in further hacking, targeting government files and exposing confidential information. According to his own account, in 1990, he manipulated a radio station contest to become the 102nd caller, winning a new Porsche, a vacation, and $20,000.

Subsequently, Poulsen was arrested and prohibited from using a computer for three years. Over time, he transitioned to ethical hacking (white hat hacking) and journalism. Poulsen began writing about cybersecurity and web-related socio-political issues for publications such as Wired, The Daily Beast, and his own blog, Threat Level. He also collaborated with fellow hackers on various projects dedicated to social justice and the free flow of information. Notably, he worked with Aaron Swartz and Jim Dolan to develop the open-source software SecureDrop, initially named DeadDrop. Eventually, Poulsen transferred the platform, which facilitated secure communication between journalists and sources, to the Freedom of the Press Foundation.

9. Jonathan James

Jonathan James, known by the alias "comrade ," gained notoriety as a hacker who breached several companies, but his most significant hack was into the United States Department of Defence when he was just 15 years old. Inspired in part by the book "The Cuckoo’s Egg," which chronicled the pursuit of a hacker in the

1980s, James infiltrated the Department of Defence's computers, gaining access to over 3,000 messages, usernames, passwords, and sensitive data.

In 2000, James was arrested and sentenced to six months of house arrest, during which he was banned from recreational computer use. However, a probation violation led to a subsequent six-month jail sentence. He became the youngest person to be convicted of violating cybercrime laws. In 2007, a major data breach occurred at TJX, a department store, compromising many customers' private information. While lacking concrete evidence, authorities suspected James's involvement.

Tragically, in 2008, James took his own life with a gunshot. In his suicide note, he expressed a lack of faith in the justice system and a desire to regain control over his life, stating, "Perhaps my actions today, and this letter, will send a stronger message to the public. Either way, I have lost control over this situation, and this is my only way to regain control."

10. ASTRA

This hacker stands out from others on this list due to the fact that their identity has never been publicly disclosed. Nonetheless, according to reports from the Daily Mail, some details have emerged regarding this individual, who goes by the pseudonym ASTRA. It has been reported that ASTRA was apprehended by authorities in 2008, and at that time, he was identified as a 58-year-old Greek mathematician. Allegedly, he had been engaged in hacking activities targeting the Dassault Group for nearly five years. During this period, he illicitly obtained cutting-edge weapons technology software and data, which he subsequently distributed to 250 individuals worldwide. The consequences of his hacking were substantial, resulting in $360 million in damages to the Dassault Group. The reasons behind the secrecy surrounding his complete identity remain unknown, but it is noteworthy that 'ASTRA' is derived from the Sanskrit word for 'weapon'.