TASK-1

AI FOR CYBER SECURITY

P. MONISH

21BCE9517

23-08-2023

- Top 10 most notorious hackers of all time inthis internet world

1. kevin mitnik

- A seminal figure in American hacking, Kevin Mitnick got his career start as a teen. In 1981, he was charged with stealingcomputer manuals from Pacific Bell.
- In 1982, he hacked the North American Defense Command (NORAD), an achievement that inspired the 1983 film *WarGames*.
- In 1989, he hacked Digital Equipment Corporation's (DEC) network and made copies of their software. Because DEC was a leading computer manufacturer at the time, this act put Mitnickon the map.
- He was later arrested, convicted and sent to prison.

- During his conditional release, he hacked Pacific Bell's voicemail systems.Throughout his hacking career, Mitnick never exploited the access and data he obtained.
- It's widely believed that he once obtained full control of Pacific Bell's network simply to prove it could be done.
- A warrant was issued for his arrest for the Pacific Bell incident,but Mitnick fled and lived in hiding for more than two years. When caught, he served time in prison for multiple counts of wire fraud and computer fraud.

Although Mitnick ultimately went white hat, he may be part of theboth-hats grey area. According to Wired, in 2014, he launched "Mitnick's Absolute Zero Day Exploit Exchange," which sells unpatched, critical software exploits to the highest bidder.

2. Anonymous

- Anonymous got its start in 2003 on 4chan message boards in anunnamed forum.
- The group exhibits little organization and is loosely focused onthe concept of social justice.
- For example, in 2008 the group took issue with the Church of Scientology and begin disabling their websites, thus negatively impacting their search rankings in Google and overwhelming itsfax machines with all-black images.
- In March 2008, a group of "Anons" marched passed Scientology centers around the world wearing the now-famous Guy Fawkesmask.

- As noted by The New Yorker, while the FBI and other law enforcement agencies have tracked down some of the group'smore prolific members, the lack of any real hierarchy makes italmost impossible to identify or eliminate Anonymous as a whole

- Anonymous" is not an individual hacker but a loosely organized and decentralized collective of hacktivists. They are known for their hacktivist activities, which include various forms of online protests, hacking, and digital activism.
- Anonymous doesn't have a specific ranking of "2 hacker" or any such formal structure. Instead, they operate as a collective with various individuals participating in their actions, often under the "Anonymous" banner.

Here's some information about Anonymous:

1. Anonymous Origins: The origins of Anonymous can be traced back to online imageboards like 4chan, where users would post anonymously and often engage in online pranks and activism.
2. Decentralized Structure: Anonymous does not have a centralized leadership or membership list. Instead, anyone can claim to be part of Anonymous by participating in their activities or adopting their iconic Guy Fawkes mask symbol.
3. Hacktivist Activities: Anonymous is known for conducting various forms of hacktivist activities. These actions have included Distributed Denial of Service (DDoS) attacks, website defacements, data breaches, and leaking sensitive information. They often target organizations or individuals they perceive as engaging in unethical or oppressive behavior.

It's important to note that due to its decentralized nature, Anonymous is not led by a single "2 hacker" but

rather a collective of individuals with diverse skills and motivations. While they have been involved in various high-profile actions over the years, their activities have also led to legal consequences for some of their participants.

3. Adrian-lamo

- In 2001, 20-year-old Adrian Lamo used an unprotected content management tool at Yahoo to modify a Reuters article and add a fake quote attributed to former Attorney General John Ashcroft.
- Lamo often hacked systems and then notified both the press and his victims. In some cases, he'd help clean up the mess to improve their security.
- As Wired points out, however, Lamo took things too far in 2002, when he hacked The New York Times' intranet, added himself to the list of expert sources and began conducting research on high-profile public figures.
- Lamo earned the moniker "The Homeless Hacker" because he preferred to wander the streets with little more than a backpack and often had no fixed address.

4. Albert Gonzales

- According to the New York Daily News, Gonzalez, dubbed "soupnazi," got his start as the "troubled pack leader of computer nerds" at his Miami high school.
- He eventually became active on criminal commerce site Shadowcrew.com and was considered one of its best hackers and moderators.
- At 22, Gonzalez was arrested in New York for debit card fraud related to stealing data from millions of card accounts.
- To avoid jail time, he became an informant for the Secret Service, ultimately helping indict dozens of Shadowcrew members.

- During his time as a paid informant, Gonzalez continued his incriminal activities.

- Along with a group of accomplices, Gonzalez stole more than 180 million payment card accounts from companies including OfficeMax, Dave and Buster's and Boston Market.
- The New York Times Magazine notes that Gonzalez's 2005 attack on US retailer TJX was the first serial data breach of credit information.
- Using a basic SQL injection, this famous hacker and his team created back doors in several corporate networks, stealing an estimated $256 million from TJX alone.
- During his sentencing in 2015, the federal prosecutor called Gonzalez's human victimization "unparalleled."

5. Matthew Bevan and Richard Pryce

- Matthew Bevan and Richard Pryce are a team of British hackers who hacked into multiple military networks in 1996, including Griffiss Air Force Base, the Defense Information System Agency and the Korean Atomic Research Institute (KARI).
- Bevan (Kuji) and Pryce (Datastream Cowboy) have been accused of nearly starting a third world war after they dumped KARI research onto American military systems.
- Bevan claims he was looking to prove a UFO conspiracy theory, and according to the BBC, his case bears resemblance to that of Gary McKinnon.
- Malicious intent or not, Bevan and Pryce demonstrated that even military networks are vulnerable.

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 curious about the use of bots—software-based robots that can infect and ultimately control computer systems.
- Using a series of large-scale "botnets," he was able to compromise more than 400,000 computers in 2005.
- According to Ars Technica, he then rented these machines out to advertising companies and was also paid to directly install bots or adware on specific systems.
- Ancheta was sentenced to 57 months in prison.
- This was the first time a hacker was sent to jail for the use of botnet technology.

7. Michael Calce

- In February 2000, 15-year-old Michael Calce, also known as "Mafiaboy," discovered how to take over networks of university computers.
- He used their combined resources to disrupt the number-one search engine at the time: Yahoo.
- Within one week, he'd also brought down Dell, eBay, CNN and Amazon using a distributed-denial-of-service (DDoS) attack that overwhelmed corporate servers and caused their websites to crash.
- Calce's wake-up call was perhaps the most jarring for cybercrime investors and internet proponents.
- If the biggest websites in the world—valued at over $1 billion—could be so easily sidelined, was any online data truly safe? It's not an exaggeration to say that the development of cyber crime legislation suddenly became a top government priority thanks to Calce's

hack.

8. Kevin Poulsen

- In 1983, a 17-year-old Poulsen, using the alias Dark Dante, hacked into ARPANET, the Pentagon's computer network.
- Although he was quickly caught, the government decided not to prosecute Poulsen, who was a minor at the time.
- Instead, he was let off with a warning.
- Poulsen didn't heed this warning and continued hacking.
- In 1988, Poulsen hacked a federal computer and dug into files pertaining to the deposed president of the Philippines, Ferdinand Marcos.
- When discovered by authorities, Poulsen went underground. While he was on the run, Poulsen kept busy, hacking government files and revealing secrets.
- According to his own website, in 1990, he hacked a radio station contest and ensured that he was the 102nd caller, winning a brand new Porsche, a vacation, and $20,000.
- Poulsen was soon arrested and barred from using a computer for three years.
- He has since converted to white hat hacking and journalism, writing about cyber security and web-related socio-political causes for Wired, The Daily Beast and his own blog Threat Level.
- Paulson also teamed with other leading hackers to work on various projects dedicated to social justice and freedom of information.
- Perhaps most notably, working with Adam Swartz and Jim Dolan to develop the open-source software SecureDrop, initially known as

DeadDrop.

- Eventually, Poulsen turned over the platform, which enabled secure communication between journalists and sources, to theFreedom of Press Foundation.

9. Jonathan James

- Using the alias cOmrade, Jonathan James hacked several companies. According to the New York Times, what really earned James attention was his hack into the computers of the United States Department of Defense.
- Even more impressive was the fact that James was only 15 at the time. In an interview with PC Mag, James admitted that he was partly inspired by the book *The Cuckoo's Egg*, which details the hunt for a computer hacker in the 1980s.
- His hacking allowed him to access over 3,000 messages from government employees, usernames, passwords and other sensitive data.

James was arrested in 2000 and was sentenced to a six months house arrest and banned from recreational computer use. However, a probation violation caused him to serve six months in jail.

- Jonathan James became the youngest person to be convicted of violating cyber crime laws.
- In 2007, TJX, a department store, was hacked and many customer's private information were compromised.
- Despite a lack of evidence, authorities suspect that James may have been involved.
- In 2008, James committed suicide by gunshot.
- According to the Daily Mail, his suicide note stated, "I have no faith in the 'justice' system. 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 differs from the others on this list in that he has never been publicly identified.
- However, according to the Daily Mail, some information has been released about ASTRA.
- Namely that he was apprehended by authorities in 2008, and at that time he was identified as a 58-year-old Greek mathematician.
- Reportedly, he had been hacking into the Dassault Group, for almost half a decade.
- During that time, he stole cutting edge weapons technology software and data which he then sold to 250 individuals around the world.
- His hacking cost the Dassault Group $360 million in damages.
- No one knows why his complete identity has never been revealed, but the word 'ASTRA' is a Sanskrit word for 'weapon'.