The History of Cyber Attacks

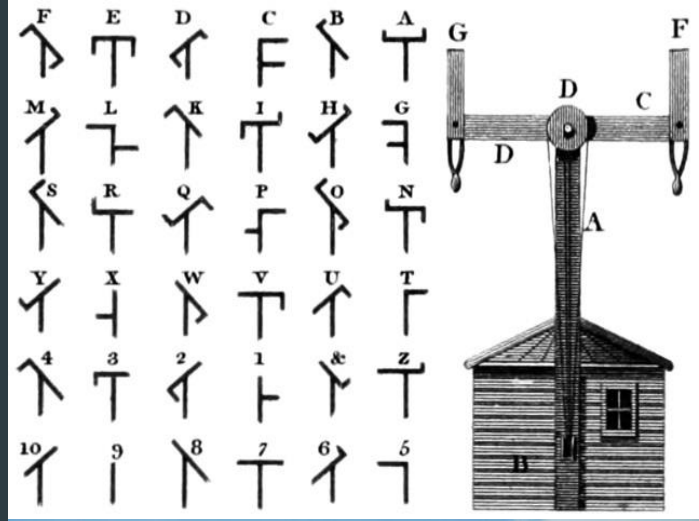
By: Patrick Hurley

Table of Contents

France 1834

The optical telegraph was created by the Chappe brothers, and was used to transmit data across large distances through visuals.

Two brothers named Francois and Joseph Blanc would bribe the operators to send information about the stock market to another person in Bordeaux. The information sent in these telegraphs would take less time to go from Paris to Bordeaux, than the information sent by mail coach.



General Information

What is a Cyber Attack?

- According to IBM, “A cyber attack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device.”

- According to NIST it is, “Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.”

Different Types of Hackers

- Black hat:

A cybercriminal that will illegally infiltrate systems. They will use many different types of methods. Will usually do this out of financial gain, or for some other reason.

- White hat:

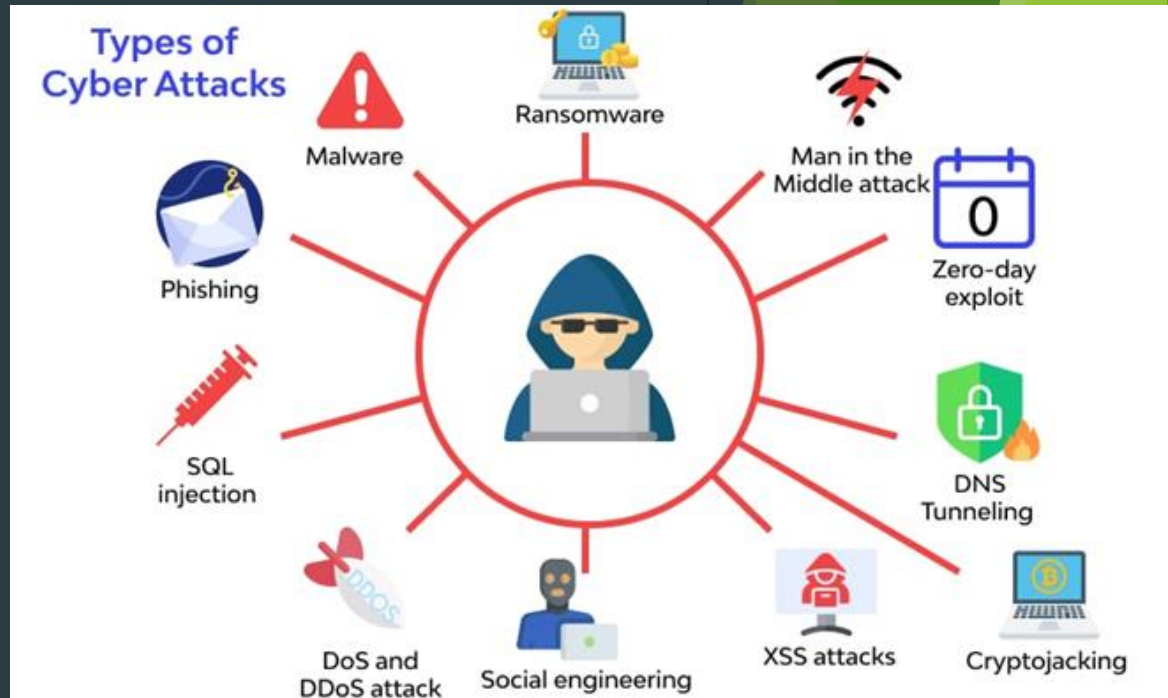
Someone who is given permission by an organization to try to penetrate their systems. Usually trying to find out weaknesses in the organizations systems. Also know as an ethical hacker.

- Grey hat:

A person who will intentionally infiltrate a system without any consent, and then report any weakness to the organization. Sometimes they will also seek out financial gain in return.

Common Types of Attacks

- Phishing, Whale Phishing
- Malware
- Ransomware
- Denial of service (DoS and DDoS)
- Corporate Account Takeover (CATO)
- Trojan Horses



The History

1903 – The First Instance of Modern Hacking

- John Ambrose Flemming was demonstrating Guglielmo Marconi's "secure" wireless telegraphy machine to the public. This machine was able to send morse code using electromagnetic waves. This machine was also able to send the signals out several kilometers. During the demonstration, 300 miles away there way another man who was going to send signals to Marconi's machine.

- Nevil Maskelyne was able to intercept the message, and he was able to start sending his own messages. The first message that Nevil sent was "rats." He then went on to start mocking Marconi by sending other messages making fun of him.

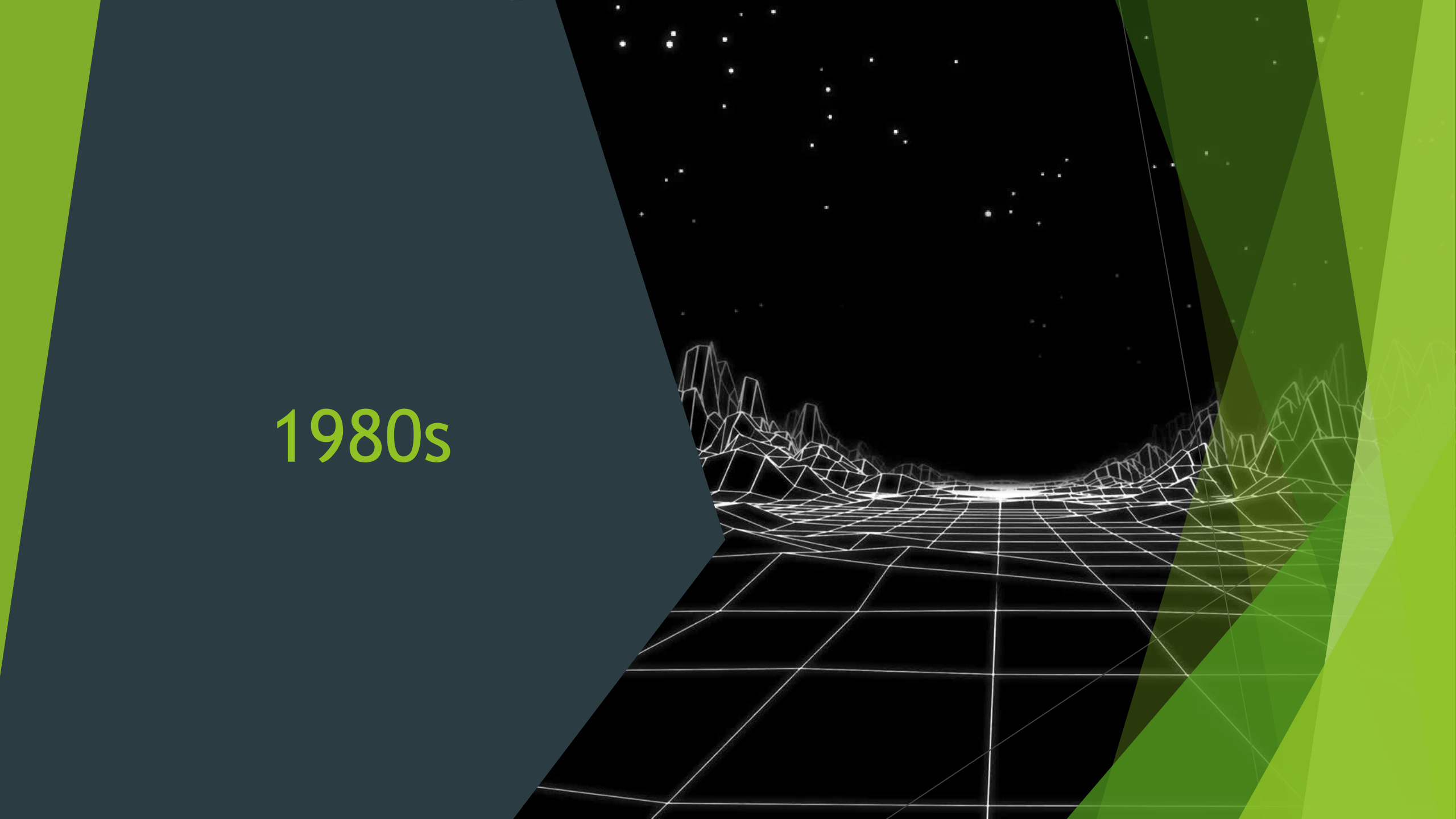
1943 – The First Ethical Hacker

- René Carmille is known to be one the very first ethical hackers, and was a expert on punch card systems.
- In WW2 a punch card system was widely used in Germany to track various information about jews. René was able to sabotage this information collecting by purposely slowing down speed at which they processed information.
- His team of double agents purposely did not process the punch cards as fast as they could. Camille even hacked his own machine to reprogram them to not punch in the last column of information.

Late 1950s, 1960s and 1970s - Phreaking

- Phreaking, was an illegal manipulation of the telephone signals to get free phone calls.
- People figured out that, if you could create a pitch at 2600 MHz to mimic the phone routing signal, then you would be able to make free phone calls
- There were some people who could produce this by whistling, like Joe Engressia (Joybubbles). He became known as the Whistling Phreaker.
- A friend of Joe, named John Draper, discovered that a whistle prize in Captain Crunch ceral was able to produce this sound. This man later earned the nick name “Captain Crunch.”
- Later people started developing blue boxes, which were also able to produce these sounds
- In the early 1980s, phone lines were upgraded to separate the signaling from the voice line. This was what marked the end of phreaking.

1980s



1981 – Chaos Computer Club

- Founded in Europe in the year 1981.
- Provide information about social issues regarding information and technology, such as surveillance, privacy, freedom of information, and hacktivism.
- This group thinks that all information should be free and every should have access to computers.
- They think that criteria such as degrees, age, and race are “bogus,” and that you should be judged by your “acting.”

Chaos Computer Club History

- 1984 – BTX
- Mid 1980s – Karl Koch
- 1998 & 2008– Project Blinken Lights

1986 – Computer Fraud and Abuse Act

- Passed in 1986

- This bill addresses cyber crime, such as accessing a protected computer without authorization.
- The bill also addresses when you access certain parts of a network that you do not have access to.

1988 – Morris Worm

- On November 2, 1988, Robert Tappan Morris released one of the first worms that infected the internet from the Massachusetts institute of technology.
- This worm was a self-replicating virus that would utilize a defect in email protocols.
- The worm would replicate itself indefinitely until the infected systems memory as filled up, and the machine would not be able to operate anymore.
- At the peak of the worm, nearly 6000 computers were compromised and were inoperable until a fix came.
- This event was sort of a wake-up call to the nation on how important cybersecurity is.

1990s

Late 1989 to 1990 – AIDS Trojan

- Created by Dr. Joseph Popp, who was an evolutionary biologist.
- Regarded as the first ransomware virus.
- Dr. Popp mailed 20,000 floppy disks to different medical professionals in many countries.
- The floppy disks had a label of a fake corporation, and when inserted into a drive would infect the system.
- When a system is booted 90 times, all the user files would become encrypted. To unlock them, you would have to send $189 to a Panamanian post office box.

1994 - Citibank

- A Russian software engineer stole account information and had stolen over ten million dollars. The money was put into accounts that were stored around the world.
- According to Citibank, they had recovered all the money, but $400,000.

2000s to Present Day

2000 – ILOVEYOU Virus

- On May 4th, a young man named Onel de Guzman created a worm that infected emails and overwrote random files.
- This email worm was able to infect about 45 million Windows computers in just one day and had also caused billions of dollars in damages.
- Because there were no laws against his actions, he was let free.
- Because of this man, the Philippines started to take the internet more seriously, and wrote laws that forbid his actions.

Other notable attacks

- 1998 – Yahoo! “logic bomb”
- 1999 – Melissa Virus.
- 1999 – 15-year-old who hacked NASA.
- 2003 - hacker group Anonymous was formed.
- 2009 – Conficker worm.
- 2010, April 17 – PlayStation servers were brought offline.
- 2010 – Stuxnet worm
- 2013 – Adobe Cyber attack.
- There are many more!

The Results of Cyber Crime

- While most of the time, the only thing that comes out of cyber crime is money, a message that wants to be sent, or just general chaos, there are also some good things that have resulted from cyber crime.
- In general, as cyber crime started to become more and more prevalent, We have started to see a higher need for cyber security professionals.
- For the US, the government has implemented a system called EINSTEIN. There are also two versions of it called EINSTEIN 1 and EISTEIN 2.
- This system monitors the flow of traffic in and out of the federal government.

Conclusions

- Cyberattacks has grown a lot of the Years
- There are a lot of attacks that are happening constantly all over the world.

References

- https://en.wikipedia.org/wiki/Optical_telegraph
- https://www.ibm.com/topics/cyber-attack
- https://www.britannica.com/technology/telegraph
- https://www.bbvaopenmind.com/en/technology/visionaries/nevil-maskelyne-vs-marconi-a-hacker-in-1903/
- https://medium.com/@silicondomme/hacking-the-holocaust-abcd332947ae
- https://www.britannica.com/topic/phreaking
- https://www.justice.gov/jm/jm-9-48000-computer-fraud
- https://www.ccc.de/en/hackerethik
- https://en.wikipedia.org/wiki/Chaos_Computer_Club

References

- https://www.britannica.com/technology/computer-worm
- https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218
- https://www.gocertify.com/articles/historic-hacks-of-the-1990s-part-1
- https://www.latimes.com/archives/la-xpm-1995-08-19-fi-36656-story.html
- https://www.computermuseumofamerica.org/2023/02/07/i-love-you-virus/
- https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/
- https://en.wikipedia.org/wiki/List_of_security_hacking_incidents#2010s
- https://www.cisa.gov/einstein#:~:text=an%20incident%20occurs.-,EINSTEIN%202,is%20an%20intrusion%20detection%20system.

References

- https://www.avast.com/c-hacker-types
- https://www.mass.gov/info-details/know-the-types-of-cyber-threats
- https://germanhistory-intersections.org/en/knowledge-and-education/ghis:document-22
- https://hcommons.org/deposits/objects/hc:48732/datastreams/CONTENT/content
- https://search-guard.com/hall-of-fame-karl-Koch/
- https://en.wikipedia.org/wiki/Chaos_Computer_Club
- http://blinkenlights.net
- https://csrc.nist.gov/glossary/term/cyber_attack

References

I had used Quotes from these two websites in Slide 5

- https://csrc.nist.gov/glossary/term/cyber_attack
- https://www.ibm.com/topics/cyber-attack