Famous Cybercrimes

The Melissa Virus

What Happened?

One of the earliest and biggest cyber threats came from the Melissa Virus in March, 1999 by programmer David Lee Smith. He sent users a file to open via Microsoft Word, which held a virus.

Once opened the virus activated causing severe damage to hundreds of companies, including Microsoft, Intel Corp, and the United States Marine Corps.

Approximately one million email accounts were disrupted and Internet traffic in some locations slowed to a crawl. It is estimated it cost $80 million to repair the affected systems.

How He Got Caught

Authorities traced the electronic fingerprints of the virus to Smith, who was arrested in northeastern New Jersey on April 1, 1999.

Smith pleaded guilty in December 1999, and in May 2002, he was sentenced to 20 months in federal prison and fined $5,000. He also agreed to cooperate with federal and state authorities.

After-Effects

After Smith was caught, the FBI put in place its new national Cyber Division, which focused exclusively on online crimes.

This virus also made many new Internet users aware of the dangers of opening unsolicited emails and attachments.

Research the Melissa Virus

Use Google to research the impact that the Melissa Virus had on computer systems and end users. Answer the questions on the following slides about the virus.

Melissa Virus Questions

What impact did the Melissa Virus have on computer systems?

The virus caused widespread disruptions in computer systems, leading to overloaded email servers and slowdowns. It infected many computers, resulting in data loss, email system crashes, and disruption of network services.

Melissa Virus Questions

How did the Melissa Virus spread so quickly?

The virus propagated by sending infected email attachments to the first 50 email addresses found in the victim's Microsoft Outlook address book.

Melissa Virus Questions

What advice would you have given users in 1999 to avoid being victims of the Melissa Virus?

Answers will vary, but could include:

- Regularly updating antivirus software
- Being cautious with email attachments

NASA Cyber Attack

What Happened?

In 1999, 15-year-old James Jonathan hacked the Defense Threat Reduction Agency (DTRA). This division is responsible for nuclear and chemical special weapons. During the hack, Jonathan installed a backdoor on the computer server which allowed him to intercept over 3,300 emails as well as usernames and passwords of department users.

Later, he visited the Marshall Space Flight Center in Huntsville and, while there, was able to hack into and download data worth $1.7 million.

Because of the intrusion and hacking, NASA had to shutdown their computers for 21 days! Fixing Jonathan’s damage cost the organization around $41,000 in repairs.

How He Got Caught

Jonathan stated that he didn't believe he was doing anything wrong so he made no effort to hide his true identity when hacking into the systems and downloading information.

The FBI was quickly able to trace the source of the hacks back to Jonathan.

After-Effects

Jonathan pleaded guilty and served six months in a detention facility.

As a condition of his guilty plea, he was required to write letters of apology to the Department of Defense and NASA and also agreed to public disclosure of information about the case.

NASA Cyber Attack Questions

What measures could have been taken by NASA to prevent James Jonathan from hacking into their systems?

Answers will vary.

Sample answer:

The attack could have been prevented by implementing regular security audits on NASA's cyber systems and strong access controls. Employee's should have received more training in how to keep their online systems secure, and data should have been encrypted.


Darkode Cyber
Criminal Forum

What was the Darkode Forum?

It was, in effect, a one-stop, high-volume shopping venue for some of the world's most prolific cyber criminals. Called Darkode, this underground, password-protected, online forum was a meeting place for those interested in buying, selling, and trading malware, botnets, stolen personally identifiable information, credit card information, hacked server credentials, and other pieces of data and software that facilitated complex cyber crimes all over the globe.

How the Forum Worked

The Darkode forum, which had between 250-300 members, operated very carefully—not just anyone could join. Fearful of compromise by law enforcement, Darkode administrators made sure prospective members were heavily vetted.

Similar to practices used by the Mafia, a potential candidate for forum membership had to be sponsored by an existing member and sent a formal invitation to join. In response, the candidate had to post an online introduction—basically, a resume—highlighting the individual's past criminal activity, particular cyber skills, and potential contributions to the forum. The forum's active members decided whether to approve applications.

Once in the forum, members—in addition to buying and selling criminal cyber products and services—used it to exchange ideas, knowledge, and advice on any number of cyber-related fraud schemes and other illegal activities. It was almost like a think tank for cyber criminals.

How it Was Taken Down

The FBI infiltrated this communication platform and began collecting evidence and intelligence on Darkode members.

The Department of Justice and the FBI—with the assistance of departments in 19 other countries around the world—announced the results of Operation Shrouded Horizon, a multi-agency investigation into the Darkode forum.

Among those results were charges, arrests, and searches involving 70 Darkode members and associates around the world; U.S. indictments against 12 individuals associated with the forum, including its administrator; the serving of several search warrants in the U.S.; and the Bureau's seizure of Darkode's domain and servers.

Criminal Forum Questions

Why do you think the Darkode Forum was created? What need did it fill?

Answers will vary.

Sample answer:

The criminal forum was created in an effort to facilitate collaboration between like-minded individuals who all had the same goal: to steal personal information. Some of these individuals just wanted the challenge to see if they could be successful while others wanted to use the stolen information for more nefarious purposes.

Role of Dark Web Questions

What role does the Dark Web play in facilitating cybercrime?

Answers will vary.

Sample answer:

The dark web provides a place for criminals to exchange stolen data or sell their illegal services and skills. It also serves as a place for knowledge exchange between criminals.

Other Cyberattacks

Activity

Research one of the following cyberattacks:

- The Sony Pictures Hack (2014)
- The DarkSide Ransomware Attack on Colonial Pipeline (2021)
- The TJX Companies Data Breach (2007)
- The Stuxnet Worm (2010)

For the attack that you have chosen, answer the questions on the following slides.

Cyberattack Research Questions

Which cyberattack did you choose to research?

Answers will vary.

Cyberattack Research Questions

Briefly explain what happened during this cyberattack. Who were the victims? What happened during the attack (system shutdown, data leak, etc.)?

Answers will vary.

Cyberattack Research Questions

Briefly explain the impact of this cyberattack. In other words, did companies or victims lose money? Were any major systems disrupted? What happened as a result of this cyberattack?

Answers will vary.

Cyberattack Research Questions

Who was responsible for the cyberattack? Or was the perpetrator never caught?

Answers will vary.

Cyberattack Research Questions

Identify two valuable lessons (online safety, cybersecurity, awareness, etc.) that could be learned from this attack. Explain.

Answers will vary.