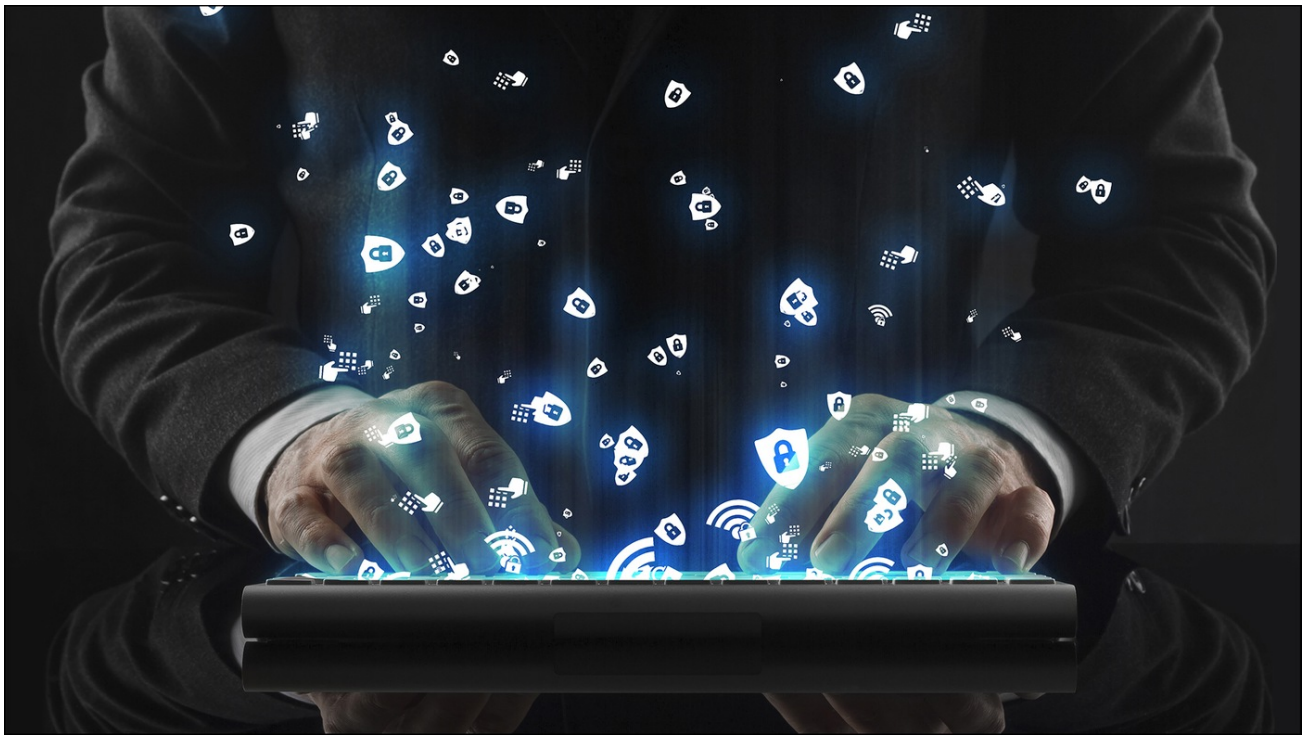
March 25, 2019

The Melissa Virus

An $80 Million Cyber Crime in 1999 Foreshadowed Modern Threats



Two decades ago, computer viruses—and public awareness of the tricks used to unleash them—were still relatively new notions to many Americans.

One attack would change that in a significant way.

In late March 1999, a programmer named David Lee Smith hijacked an America Online (AOL) account and used it to post a file on an Internet newsgroup named “alt.sex.” The posting promised dozens of free passwords to fee-based websites with adult content.

When users took the bait, downloading the document and then opening it with Microsoft Word, a virus was unleashed on their computers.

On March 26, it began spreading like wildfire across the Internet.

The Melissa virus, reportedly named by Smith for a stripper in Florida, started by taking over victims' Microsoft Word program. It then used a macro to hijack their Microsoft Outlook email system and send messages to the first 50 addresses in their mailing lists. Those messages, in turn, tempted recipients to open a virus-laden attachment by giving it such names as "sexxxy.jpg" or "naked wife" or by deceitfully asserting, "Here is the document you requested ... don't show anyone else ;-)." With the help of some devious social engineering, the virus operated like a sinister, automated chain letter.

The virus was not intended to steal money or information, but it wreaked plenty of havoc nonetheless. Email servers at more than 300 corporations and government agencies worldwide became overloaded, and some had to be shut down entirely, including at Microsoft. Approximately one million email accounts were disrupted, and Internet traffic in some locations slowed to a crawl.

Within a few days, cybersecurity experts had mostly contained the spread of the virus and restored the functionality of their networks, although it took some time to remove the infections entirely. Along with its investigative role, the FBI sent out warnings about the virus and its effects, helping to alert the public and reduce the destructive impacts of the attack. Still, the collective damage was enormous: an estimated $80 million for the cleanup and repair of affected computer systems.

Finding the culprit didn't take long, thanks to a tip from a representative of AOL and nearly seamless cooperation between the FBI, New Jersey law enforcement, and other partners. 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.

The Melissa virus, considered the fastest spreading infection at the time, was a rude awakening to the dark side of the web for many Americans. Awareness of the danger of opening unsolicited email attachments began to grow, along with the reality of online viruses and the damage they can do.

Like the Morris worm (https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218) just over a decade earlier, the Melissa virus was a double-edged sword, leading to enhancements in online security while serving as

inspiration for a wave of even more costly and potent cyberattacks to come.

For the FBI and its colleagues, the virus was a warning sign of a major germinating threat and of the need to quickly ramp up its cyber capabilities and partnerships.

Fittingly, a few months after Smith was sentenced, the Bureau put in place its new national Cyber Division focused exclusively on online crimes, with resources and programs devoted to protecting America's electronic networks from harm. Twenty years later, with nearly everything in our society connected to the Internet, that cyber mission (https://www.fbi.gov/investigate/cyber) is more crucial than ever.

Resources

- Cyber Crime (https://www.fbi.gov/investigate/cyber)