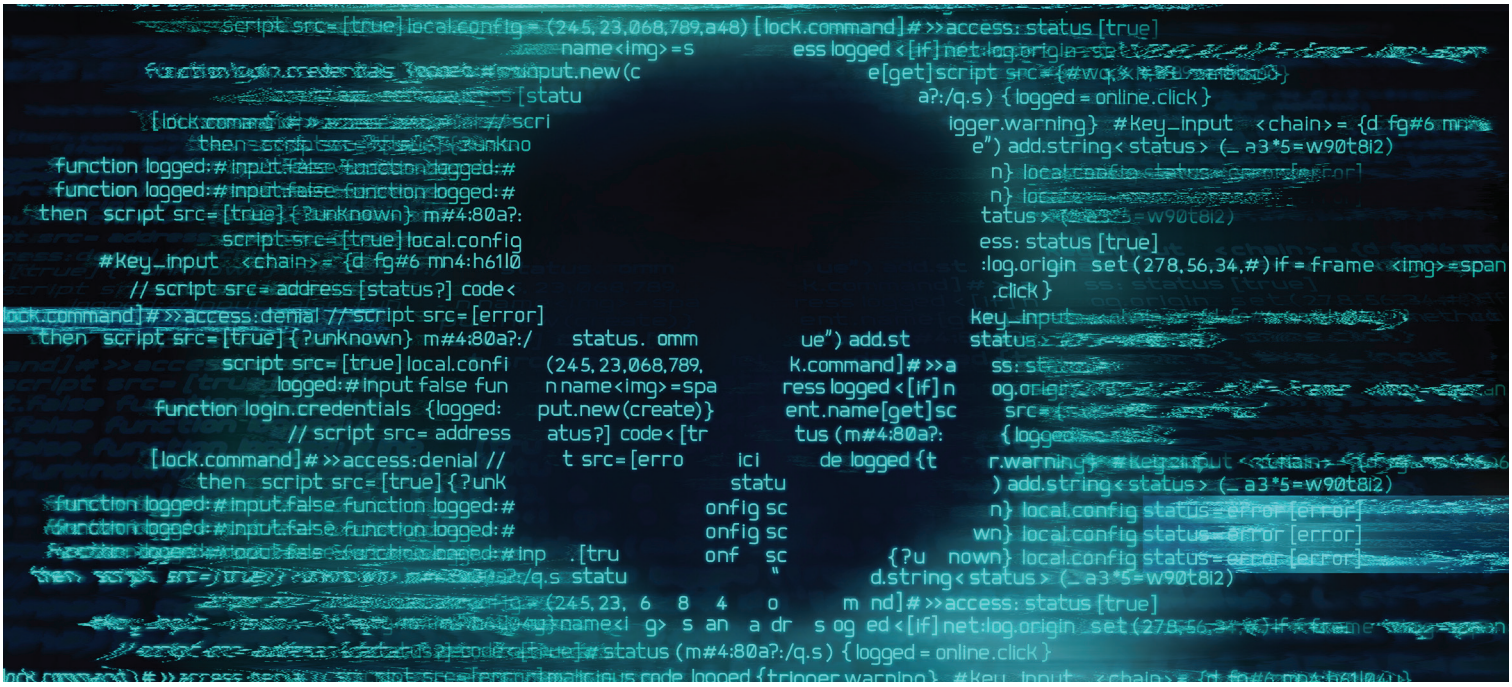

Nervous System: The Virus That Wasn't

BY DAVID KALAT

With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have been with us longer than we remember.

Nervous System *is a monthly series that approaches issues of data privacy and cyber security from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.*

It began with a warning posted to online bulletin boards. Below the subject line "Really Nasty Virus," user Mike RoChenle explained how this terror had deleted his data and corrupted his hard drives. The author called it "the world's worst computer virus yet" and speculated that the malware was distributing its infection through the subcarrier used in 2400-baud modems. "Probably the best thing to do now is to stick to 1200 baud until we figure this thing out," he concluded.

Modern-day modems are commonly classified by how many bits (or megabits) they transmit per second. Back when connecting to the internet meant converting computer signals into something that could be transmitted over telephone wires, the term "baud" denoted how many times per second the modem sent a new signal.

Understanding this is utterly incidental to understanding how the so-called "2400 Baud Modem Virus" worked. The virus, you see, was not a piece of software at all. It never infected a single computer. Instead, it spread through the minds and habits of computer users. Some people who passed along the warnings of "Mike RoChenle" believed the hoax and thought themselves to be acting in the community's interest. Others saw through the absurd claims of Mr. "Micro Channel" and merely wanted to warn others not to fall for them. Both types of people, however, passed along the message—and that is how it spread.

When the hoax first appeared in October 1988, the community of computer users was beginning to wake up to the risks of information security in a networked world. Although the threat posed by the 2400 Baud Modem Virus was fanciful and technologically implausible, it was not wholly outside the realm of possibility. Barely a month after the post first surfaced, and while online bulletin board users were still passing it around and debating whether such a virus was possible, a real virus actually was spreading.

Unleashed on November 2, 1988, the malware later identified as the Morris Worm began to propagate across connected computers at an unprecedented speed. The worm did not damage files, but its hijack of system resources to self-replicate slowed computer networks to a crawl. The scope of the damage has never been quantified definitively, but estimates range between $100,000 into the tens of millions.

The 2400 Baud Modem Virus might seem quaint by contrast, but it was not harmless. It and other virus hoaxes, like the Good Times Virus, exploited the gullibility of users to spread a story to one another. Some speculated at the time that "Mike RoChenle" was trying to spook people into not using their modems, to free up bandwidth for his own use. The identity and motivation of the prankster have never been determined.

Virus hoaxes have real-world consequences, as frightened computer users delete their own files and unplug critical system components in the belief they are protecting themselves. Even users who see through the hoaxes waste their time and energy debunking these myths. Similar hoaxes persist, although their nature has evolved. Recently, a viral Facebook meme offered seemingly plausible but actually catastrophic "advice" on what to do if one were stranded with a dying phone battery. Various official search and rescue authorities struggled to keep pace with the meme, because their lifesaving message was not as compelling as the phony one.

On November 21, 1988, in response to the virus hoaxes, a user named Robert Morris III posted a warning to an online message board. Under the subject line "VIRUS ALERT," Morris urged readers to avoid using *any* kind of power—direct wire or battery—and to avoid interacting with any data, software, or hardware. He concluded by cautioning people against using "running water, writing, fire, clothing or the wheel."

The facetious posting about an obviously nonsensical threat was meant to be provocative and remind users of the forum not to take postings at face value. However, it was passed around among users, shared, and recirculated just as much as the "real" hoaxes it parodied.

Although online "bulletin board" postings of this type were meant to be ephemeral, and this particular one was posted long before the popularization of internet culture, Morris' "VIRUS ALERT" has a special place in the history of information security.

Nineteen days before posting his comical "VIRUS ALERT," Morris had created the worm that was eating its way through computer networks. The damage his worm caused was so severe that intrepid computer detectives immediately began investigating the origins of the malware—and quickly traced it back to Morris. Mere days after the worm was released, the *New York Times* reported that it had been created by a twenty-three-year-old graduate student at Cornell University who was the son of a prominent Bell Labs researcher. An extra wrinkle: the elder Bob Morris was at that time employed by the National Security Agency as its chief computer scientist, which did not become known until much later.

The younger Morris was investigated by the FBI. Ultimately, he was tried and became the first person convicted for violating the Computer Fraud and Abuse Act for his role in engineering and releasing the Morris Worm.

Legaltech® news

This article was originally published in Legaltech News on November 30, 2021.