Nervous System #6: How the AIDS Trojan Makes You WannaCry

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 bimonthly blog 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.*

For years, ransomware has been one of the easiest and most profitable computer crimes: a criminal or criminal organization maneuvers secret software onto a victim's computer, which encrypts the victim's data until a ransom is paid in exchange for the decryption key. Not only is it inexpensive to deploy such a scheme, but the people and organizations hit by such attacks are often highly motivated to pay to regain access to their files. For various reasons, the rate of ransomware attacks is gradually declining, but the government officials in Atlanta who spent a harrowing six days without functioning computer systems will tell you that these attacks can still be devastating. In May 2017, a wave of attacks involving a breed of ransomware called "WannaCry" affected hundreds of thousands of computers in over a hundred countries.

Surprisingly, the granddaddy of ransomware was released on December 19, 1989, at a time when email and computer networks were still such novelties that this piece of malware had to be physically mailed to victims through the postal service on a 5.25-inch floppy diskette. In order to be victimized by it, you had to make a conscious decision to insert the diskette into your computer and run the installer.

The people who opted to install it on their computers did so because it was labeled "AIDS Information." Many of the victims were delegates to the 1988 World Health Organization's International AIDS Conference in Stockholm, and were delighted to receive free AIDS research unbidden. This blind faith was rewarded, in part, because the label was accurate—the diskette did actually contain genuine AIDS research data. However, it also contained software that, after a certain number of reboots, encrypted the hard disk. The ransomware then prompted the user to turn on their printer, which it used to print an invoice for a $189 "license fee" to be paid to a post office box in Panama.

It is worth noting that there was no subterfuge here—the package containing the diskette also contained a letter explaining the license agreement: "In case of breach of license, PC Cyborg Corporation reserves the right to use program mechanisms to ensure termination of the use of these programs. These program mechanisms will adversely affect other programs on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement. Warning: do not use these programs unless you are prepared to pay for them."

In other words, every victim was warned in advance, although one assumes few either read the letter or paid it much mind. The reason the scheme worked was that large numbers of computer users in 1989 were completely willing to take at face value a strange diskette mailed to them out of the blue—and this very behavior points to an essential fault line in the world of computer security and the nature of hackers.

At the first Hackers Conference in 1984, counterculture tech visionary Stewart Brand legendarily told Apple cofounder Steve Wozniak, "On the one hand, information wants to be expensive, because it's so valuable. The right information in the right place just changes your life. On the other hand, information wants to be free, because the cost of getting it out is getting lower and lower all the time."

The phrase "Information Wants to Be Free" has become something of a mantra for a particular philosophy of information technology that argues people should be able to retrieve information freely. It is a utopian philosophy, advocating for greater transparency and wider access. Viewed from an information security perspective, "Information Wants to Be Free" can trend towards the unwanted disclosure of proprietary, confidential, or sensitive information. Taken to extremes, a philosophy that says information should be "liberated" leads to pirating of intellectual property or the disclosure of documents on sites like WikiLeaks.

The criminals who deploy ransomware, however, operate from a completely different stance. The threat posed by ransomware is not unwanted disclosure, but its *exact opposite*—authorized users unable to access their own data. "Information Wants to Be Free" is a political ideology; most ransomware traces back to people who are just in it for a buck.

The AIDS Trojan had real victims—medical institutions and scientific research establishments that were deprived of essential data. Some reacted to the attack on their data systems by deleting what they feared was now compromised information. One Italian organization allegedly deleted ten years' worth of its research. Yet all of these victims took a strange package received in the mail and trustingly installed its contents on their computers.

The mastermind behind the AIDS Trojan was eventually caught, under circumstances as least as surprising as the crime he committed. Security officers at an Amsterdam airport were called in to investigate when a passenger on a flight from Nairobi discovered the phrase "Dr. Popp has been poisoned" had been written on his luggage. Weirdly, the man who wrote this was the "Dr. Popp" in question. Dr. Joseph L. Popp was a Harvard PhD and evolutionary biologist who had conducted AIDS research in Africa for the World Health Organization—and when airport police discovered that his bags contained a company seal for "PC Cyborg Corp," Dr. Popp was soon arrested and extradited to the UK on ten counts of blackmail and criminal damage.

He was never prosecuted, though. The odd behavior that led to his capture intensified—he put condoms on his nose and a cardboard box on his head; he put curlers in his beard to repel radiation. The judge found him unfit to stand trial.

Dr. Popp's AIDS Trojan was not an especially sophisticated attack. His software was kludgy and easily defeated—decryption disks were made available for free to reverse the encryption. In fact, many modern ransomware attacks are equally unsophisticated. The WannaCry virus contained a built-in "kill switch," making it possible for a twenty-two-year old tech blogger named Marcus Hutchins to step in and singlehandedly stop the spread of the virus.

While the curious case of the AIDS Trojan has many peculiar details, at its heart it is a story of this basic schism in the hacker communities. PC Cyborg destroyed the data of many goodhearted and trusting scientists because "Information Wants to Be Free" is an inadequately cautious worldview. Today's computer users may have learned to be a little more cautious, but the mindset and philosophy of those early computer pioneers is baked in too much of our modern information systems. Malware commits mischief by exploiting software vulnerabilities, and the technological solution is to fortify the software and patch the vulnerabilities. But malware spreads in part by also exploiting social vulnerabilities, preying on the unskeptical or incautious attitudes of users. These are much harder to patch.

Legaltech® news

This article was originally published in Legaltech News on July 9, 2018.