TECHNOLOGY

The Computer Virus That Haunted Early AIDS Researchers

The first-ever ransomware attack was delivered on a floppy disk.

KAVEH WADDELL MAY 10, 2016

Computers like this 1980s-era Amiga 1000 were the state of the art when the first-ever ransomware virus was released. (BLAKE PATTERSON / FLICKR)

After booting up their computers one day in late March, scores of employees at MedStar, a sprawling health-care system with ten hospitals in the Washington-Baltimore area, were greeted with a menacing ransom note. Their computer systems had been taken over, the note said, and vital files had been locked away. “You have just 10 days to send us the Bitcoin,” the hackers wrote, after demanding about 19,000 dollars’ worth. “After 10 days we will remove your private key and it’s impossible to recover your files.”

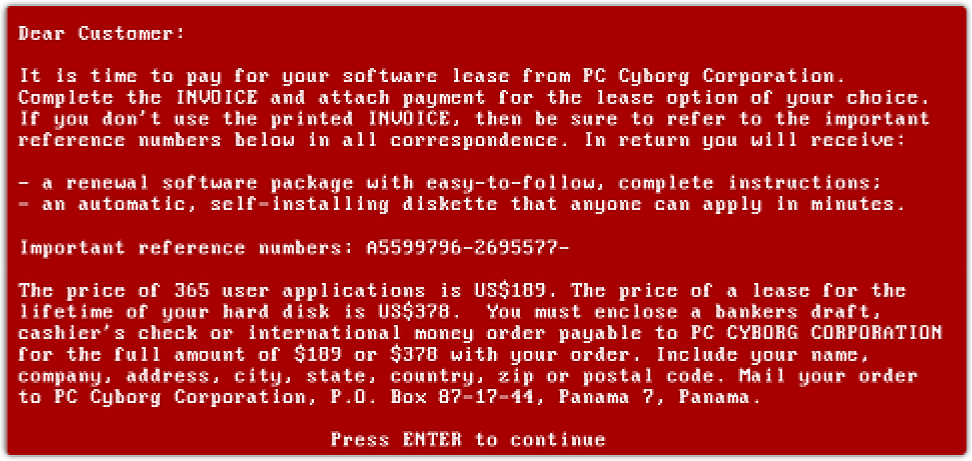
MedStar’s systems had been infected by ransomware, a type of computer virus that encrypts a victim’s files with a private key and demands payment to unlock them. It took the rest of the week for the health-care system to recover its files. MedStar was able to do so without paying the ransom, but a hospital in Los Angeles wasn't so lucky: In February, Hollywood Presbyterian Medical Center sent hackers 17,000 dollars in Bitcoin in order to regain access to its records.

Since the pair of high-profile attacks, hospitals have been called the next frontier for ransomware infections. Indeed, they're an ideal target for hackers: Access to lifesaving patient-record information is mission-critical and time-sensitive, so administrators might be more willing to pay to get them back after an attack.

But in fact, ransomware that targets the health-care sector is just returning to its roots. A research paper on ransomware from Palo Alto Networks, a cybersecurity company, shows that the first-ever ransomware attack went after AIDS researchers—and it was distributed on 5.25-inch floppy disks.

The year was 1989, and the AIDS epidemic was in full swing. The number of reported AIDS cases had hit 100,000 for the first time. An evolutionary biologist named Joseph Popp came up with a computer-based questionnaire he said would help determine patients' risk of contracting AIDS, and he distributed 20,000 copies of it to researchers in 90 countries.

But the surveys on Popp's floppy disks were a ruse. When participating scientists loaded the disk, their computers became infected with what would come to be known as a digital version of the AIDS virus. It lay dormant for a while: For the next 89 times the computer was turned on, everything would seem normal. But on the 90th boot, an angry red message splashed across the screen.



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                         Press ENTER to continue
```

(PALO ALTO NETWORKS)

The virus scrambled the contents of the victims' computers and offered to unlock them only in return for a "licensing fee." It worked by encrypting filenames, a relatively primitive attack that still rendered most computers unusable.

Soon, security researchers produced antidotes that would recover the files locked away by the virus. The development of those tools, plus the difficulty of actually paying the ransom—it required sending a cashier's check or an international money order to a P.O. Box in Panama—kept Popp from profiting much from his trick.

The biologist was soon arrested and charged with blackmail in the U.K. He claimed in court to have planned to donate the spoils of his caper to AIDS research, but *The Guardian* reported that his stunt was a reaction to being rejected for a job at the World Health Organization. He was eventually ruled mentally unfit to stand trial (the journalist Alina Simone found British reports citing his propensity for wearing condoms on his nose and curlers in his beard to protect from radiation) and was deported to the U.S., where he remained free until his death in 2007.

Now, nearly 30 years later, ransomware generally falls into two camps—and both draw on elements of Popp's early virus.

The first type of modern ransomware, known as scareware, relies on computer users' unfamiliarity with the inner workings of important software—and their profound fear of breaking their machines. Bandying about phrases like "SYSTEM WARNING" and "CRITICAL ERROR," this type of malware tries to convince the user that something is horribly, terribly, wrong with their computer with insistent alerts and frightening splash screens, and then promises to sell just the tool to fix the problem for a bargain: a sum usually under 100 dollars. Once the unsuspecting user pays up, the alerts go away. (In one version, the scareware imitates the FBI, demanding a fine for the fictitious child pornography found on your laptop.)

A good understanding of how operating systems work, or what computer problems usually look like, can help users avoid falling into a scareware trap. But the second, more complex branch of ransomware is far more insidious, and can stump even the most capable victims.

Known as crypto ransomware or cryptoware, this newer breed of virus takes Popp's idea—using encryption to render files inaccessible without a specific cryptographic key—and infuses it with state-of-the-art cryptography. Modern cryptoware attacks can encrypt entire file systems with such sophistication that even the FBI has been repeatedly unable to unscramble the files. And unlike the tools that could reverse the effects of Popp's "AIDS virus," nothing short of the attacker's private key—available for purchase, of course, for anywhere between a hundred and thousands of dollars—will save an infected computer or server.

CryptoLocker began the wave of largely unbreakable cryptoware in 2013. Today, Palo Alto Networks tracks 30 different types of cryptoware, which it says "all follow very similar playbooks" to the one CryptoLocker wrote. These viruses are prolific, and they don't differentiate between victims: They've taken down home PCs, school computers, and police-department servers, let alone the likes of MedStar.

And soon, their repertoire may expand beyond computers and servers. As I've written before, hackers are experimenting with ransomware tailored to smartphones, smartwatches, and even Internet-connected TVs. As household appliances and security systems begin talking to one another on the Internet as well, it may not be long before they start getting ransomed, too. And just as attackers asked for higher ransoms from desperate hospitals, a hacker who compromises a refrigerator or front-door lock may be able to ask for far more than a few hundred dollars to relinquish control.

And unlike the virus made by Popp, an evolutionary biologist moonlighting as an enterprising hacker, modern ransomware is produced by hackers who have learned from decades of virus development and who can lean on industry-standard cryptography to create truly frightening viruses.

We want to hear what you think about this article. Submit a letter to the editor or write to letters@theatlantic.com.