Case Study: AIDS Trojan Ransomware

Marlese Lessing | Studios Editor

The first ransomware attack, launched in December 1989, was called PC Cyborg, or AIDS Trojan. It was distributed by one Dr. Joseph L. Popp, an evolutionary biologist, to some 20,000 individuals and medical institutions.

While the malware itself was weak, and easily removable with decryption software, the attack set the stage of over 20 years of ransomware and virus attacks, and highlighted the need for data security measures.

AIDS Trojan: Delivery

Popp's malware was delivered in a fairly unorthodox manner, with the internet still being in its infancy. Popp mailed every victim an infected floppy disc, labeled as "AIDS Information Introductory Diskette," using hijacked mail subscriber lists to the World Health Organization AIDS conference and *PC Business World* magazine in December 1989.

The software contained a questionnaire about the AIDS virus, disguising itself as a survey. The disc was stamped with a logo for the "PC Cyborg Corporation."

In reality, the floppy disk would deliver its payload of encryption malware onto the computer, making it one of the earliest pieces of Trojan malware.

AIDS Trojan: Methodology

The disc contained two files, both written in QuickBASIC 3.0. One contained the "survey" while the other contained the installer for the malware.

Once in the system, the malware did not encrypt the files immediately. Instead, it infected the C: drive of the computer and hijacked AUTOEXEC.BAT in the root directory. AUTOEXEC.BAT was the startup file used for

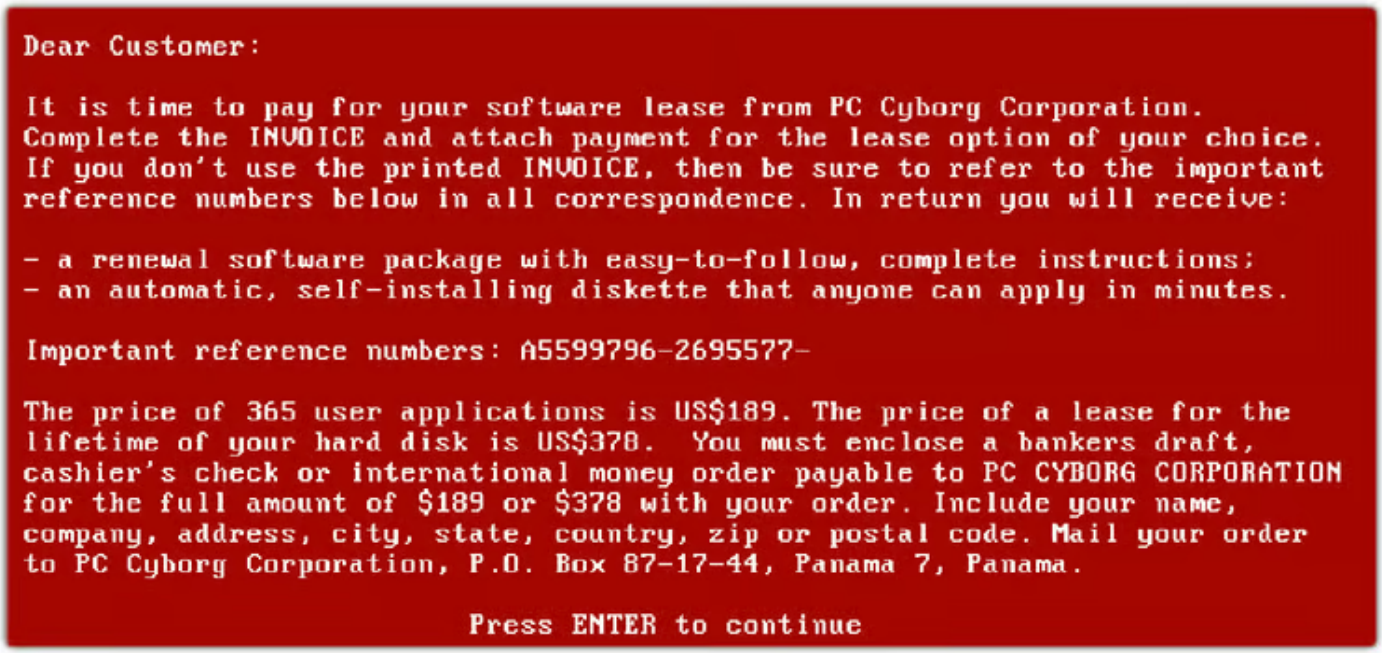
the Windows operating system at the time. The operating system executed it with each boot.

While the virus did not affect the boot itself, it instead counted the number of times the file was executed. After a certain number of times (typically 90, though it varied) the malware would trigger, encrypting the names of all the files within the C: drive using symmetrical encryption.

While the files themselves were not affected, the encryption would alter the extension names and prevent them from being executable.

Once the files had been encrypted, the malware would then launch the ransom message. The message claimed that the lease for software from the PC Cyborg Corporation had expired, and the user must pay to renew it. The fees were $189 for a year's "lease" or $378 for a lifetime "lease." When adjusted for inflation, this comes out to roughly $400 and $800, respectively. Victims were instructed to mail their money to a PO box in Panama.

The user was continuously bombarded with this message; if they attempted to reboot, the process would simply start over again with the hijacked AUTOEXEC.BAT file.



The ransom note that the malware displayed to users, demanding money for a software "lease." Source: Wikimedia Commons

AIDS Trojan: Impact

Partly due to the unusual ransom paying method, Popp did not receive much of a payout. However, the damage was done. Panicked users wiped their hard drives; some research and medical organizations lost years of work in the process.

AIDS Trojan was not a particularly widespread, advanced, or profitable piece of malware. However, it introduced and popularized the concept of using malware as leverage. Previous viruses such as Creeper

introduced and popularized the concept of using malware as leverage. Previous viruses such as Creeper would inconvenience the user by filling up their hard drive or destroying users' files. AIDS Trojan, however, took it a step further by coercing users into paying money, preying on the world's increased reliance on computers to store and edit data as well as the victims' ignorance. This approach attacks set the stage for more invasive ransomware like Archievus or Reveton.

Ransomware has exploded since then, resulting in over $1 billion in revenue for attackers in 2018, with that number expected to rise exponentially as attacks continue to increase, according to a study conducted by security company SafeAtLast. The average cost of a ransomware attack on a business is $133,000 according to that same report. More cases are being reported every day.

The Aftermath of AIDS Trojan

As for the attacker himself, Popp was arrested in the Netherlands in January 1990 after a nervous breakdown at an Amsterdam airport. Police found equipment labeled with "PC Cyborg Corp." in his baggage. Authorities sent him back to the US, where the FBI arrested him. New Scotland Yard then extradited him to Britain on the charges of blackmail.

However, the court declared Popp mentally unfit to stand for trial in 1992. He apparently took to wearing curlers in his beard to protect himself against radiation and "microorganisms," sporting a condom on his nose, and repeatedly putting a cardboard box on his head.

The malware itself was fairly easy to resolve. Jim Bates, editorial advisor for *Virus Bulletin,* authored the programs AIDSOUT and CLEARAID in January 1990. The programs, respectively, removed the malware from the computer and decrypted the files, making them usable again.

AIDS Trojan Ransomware: Key Takeaways

- The Trojan AIDS/PC Cyborg virus was the first known ransomware attack.
- It gained access to users' computers through a mailed floppy disc disguised as a survey program.
- The malware encrypted C: drive file names, preventing users from accessing their files.
- It used symmetric encryption, making it fairly easy to remove and decrypt.

Updated September 2020 by Ashley Wiesner

Read Next

Case Study: Archievus Ransomware

Definitions | Marlese Lessing

Case Study: Reveton Ransomware

Definitions | Marlese Lessing

Definitions | Marlese Lessing

Case Study: WannaCry Ransomware

Definitions | Marlese Lessing

Cloud Security Basics — Definition

Definitions | Connor Craven

Data Security in the Cloud Best Practices

Definitions | Connor Craven

Data Security Regulations – an Overview

Definitions | Scott Raynovich

How Does Ransomware Work?

Definitions | Marlese Lessing

How to Protect Against Ransomware

Definitions | Marlese Lessing

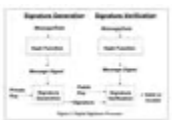
Keeping a Telecommuting Workforce Safe Online

Definitions | Connor Craven

What are the Data Privacy Fundamentals?

Definitions | Marlese Lessing

Deepen Your Knowledge

1 

What Does it Mean To Be FIPS Compliant?

2 

What is SASE? Its benefits, features and challenges

3  **Case Study: WannaCry Ransomware**

4  **The advantages of quantum computing**

5  **What is the cloud? Technology, advantages and disadvantages**

Related Terms

Client-Server Model

Information and Communication Technology

Federal Information Processing Standard

Open Systems Interconnection

Shor's Algorithm

CRYSTALS-Kyber

Webinars

Whitepaper: Security fabric reimagines enterprise protection

In the News

1 

Palo Alto Networks moves to SASE 3.0

2  **Verizon, AT&T, T-Mobile fined for selling location info**

Related Security Advisories

CISA Releases Eight Industrial Control Systems Advisories

Cisco Releases Security Updates Addressing ArcaneDoor, Vulnerabilities in Cisco Firewall Platforms

CISA Releases Two Industrial Control Systems Advisories

Cisco Releases Security Advisories for Cisco Integrated Management Controller

Industry News

More

Ververica Achieves ISO 27001 Certification, Bolstering Data Security

GEOINT 2024: Vibrint to Showcase Latest National Security Innovations in Artificial Intelligence, Cloud, LiFi and Quantum Computing, Booth 2131

Eaton highlights cybersecurity education, skilled workforce training programs at White House Cyber Workforce event