HACKERS ARE EVERYWHERE

A Global Overview of 10 Famous Cyberattacks

LOS ANGELES TRAFFIC LIGHT HACK (2006)

Los Angeles, California, United States

During a strike by unionized traffic engineers in Los Angeles, two of the striking employees took their protest to the next level. Bypassing safeguards put in place prior to the strike, Kartik Patel and Gabriel Murillo reprogrammed the traffic signals at four key Los Angeles intersections — just four, out of more than 4,000 — causing four days of delays, massive congestion, and general chaos.

MAFIABOY DDOS ATTACKS (2000)

Quebec, Montreal, Canada

Using a homemade application he dubbed Rivolta (the Italian word for "rebellion"), Canadian teenager Michael "MafiaBoy" Calce launched distributed denial-of-service (DDoS) attacks against a series of high-profile U.S. corporations, including Yahoo!, Buy.com, eBay, CNN, Amazon, and Dell. U.S. and Canadian authorities zeroed in on Calce after he boasted about the success of the attacks online.

CITIBANK HACK (1994)

St. Petersburg, Russia

Russian mathematician Vladimir Levin broke into several corporate accounts at U.S.-based Citibank and stole $10.7 million. Citibank recovered most of the money, but Levin, arrested in England and extradited to the United States, spent three years in jail and paid nearly $250,000 in restitution. Self-proclaimed accomplices later alleged that Levin had misrepresented certain elements of his account of the hack.

STUXNET WORM (2010)

Natanz, Iran

Entering through computers running Microsoft's Windows operating system, Stuxnet famously stalled out uranium enrichment at a massive nuclear facility near the city of Natanz in Iran's Isfahan Province. Specifically, the worm disrupted the operating speed of gas centrifuges at the plant. Stuxnet, the first known purpose-designed cyberweapon, is believed to have been created by the combined intelligence forces of the United States and Israel.

OFFICE OF PERSONNEL MANAGEMENT (OPM) HACK (2015)

China

Perhaps the most infamous cyberattack ever perpetrated against the United States targeted the Office of Personnel Management in Washington, D.C. Hackers, widely believed to have been sponsored by the Chinese government, looted personal information connected to as many as 22.1 million individuals, including 5.6 million sets of fingerprints.

CHASE MANHATTAN BANK HACK (1985)

Escondido, California, United States

One of the largest FBI raids in California history was organized to shut down the activities of ... a 14-year-old trying to find computers powerful enough to run a C compiler. Calling himself "Lord Flathead," savvy teen Tom Anderson perpetrated a successful war dialing attack against Chase Manhattan Bank and threatened to destroy its data. Authorities seized Anderson's computer (which was never returned) and he agreed to probation. In 2003, Anderson founded MySpace.

AIDS TROJAN (1989)

Panama

Evolutionary biologist Joseph Popp perpetrated one of the first known ransomware attacks. Popp used the postal service to send floppy disks labeled "AIDS Information Introductory Diskette" to unsuspecting peers. Each disk contained a trojan that would lock up the user's computer and demand that a payment of $189 be sent to a P.O. Box in Panama.

TRACK2 CREDIT CARD RESELLER (2014)

Kanifushi Island, Maldives

Russian hacker Roman "Track2" Seleznev famously caused more than $169 million in damages to businesses and financial institutions by stealing and reselling credit card data. The United States Secret Service worked for years to identify and track Seleznev before he was finally arrested while vacationing at a posh resort in the island nation Republic of Maldives. In 2016, Seleznev was given a 27-year prison sentence, the longest ever handed down by a U.S. court for a hacking conviction.

NASA WORM (1989)

Melbourne, Australia

NASA and the U.S. Department of Energy were targeted by this playful protest hack, which propagated through linked computer networks and would announce itself with the following message: "Worms Against Nuclear Killers / WANK / Your System Has Been Officially WANKed / You talk of times of peace for all, and then prepare for war." Hackers based in Melbourne, Australia, possibly including an 18-year-old Julian Assange, are believed to have been responsible.

SONY PICTURES HACK (2014)

North Korea

Weeks before the widely publicized release of the comedy movie *The Interview*, hackers calling themselves "Guardians of Peace" used a Server Message Block (SMB) worm to infiltrate Sony Pictures and steal a giant cache of data. The cause? *The Interview* is built around a highly unflattering portrait of North Korean dictator Kim Jong-un ... and North Korea is generally believed to have directly sponsored the attack.