TestOut

HACKERS GET INTO EVERYTHING

If something — anything — is out there, then a hacker has probably tried to mess with it

YOUR E-MAIL

Yahoo! Attack (2013)

Most hackers could not care less about actually reading your messages, but e-mail accounts are often linked to names, birthdates, phone numbers, and other valuable personally identifying information (PII). Hackers cracked the servers of internet portal Yahoo! in 2013 and stole data connected to more than 1 billion user accounts. Two subsequent attacks plundered data from 750 million user accounts.

YOUR CREDIT PROFILE

Experian Attack (2015)

Credit monitoring agencies like Experian (based in Ireland) maintain complex, data-rich profiles of individual consumers from countries around the world. In 2015, hackers stole data connected to 15 million different people from Experian, which turned out to be merely prelude to larger breaches in 2020 (24 million profiles exposed) and 2021 (220 million profiles exposed).

RETAIL STORES

Target Attack (2013)

Point of sale (POS) credit card processing is what lets you swipe a card and walk out of a store with everything from breakfast cereal to flat-screen TVs. After breaching the internal network of retail giant Target — using access credentials stolen from an HVAC contractor — in advance of the Black Friday shopping weekend in November 2013, hackers stole credit card data from thousands of POS terminals.

DIGITAL INFRASTRUCTURE

SolarWinds Attack (2020)

IT resource management software helps computer systems function smoothly. Hackers added malicious code to one such program, Orion — managed by Texas-based SolarWinds — turning it into a backdoor to sensitive computer networks, including those at a number of U.S. government agencies. The list of suspects includes Russian espionage agency SVR and the Russian hacker group Cozy Bear.

GOVERNMENT SECRETS

U.S. Department of Defense and NASA Attack (2001)

Plenty of people believe that national governments hide advanced technologies and other information from citizens. Scottish hacker Gary McKinnon actually did something about it in 2001, hacking 97 different U.S. military and NASA computers looking for energy technology secrets and suppressed evidence of UFOs. British authorities later blocked an attempted extradition of McKinnon to the United States.

HOME IS WHERE YOU HANG YOUR HACK

Houzz Attack (2019)

Interior design and decoration is a hot topic for millions of people who want to know (for example) the top paint color for the coming year. How many millions of people? Hackers turned home improvement platform Houzz into a house of pain by stealing data from more than 48 million user accounts. In addition to usernames and passwords, hackers stole profile data linking site users to their cities of residence.

SOCIAL MEDIA

Twitter Attack (2020)

Everyone knows — or at least most people *think* — that individual Twitter accounts get "hacked" all the time. Post something stupid? Claim you were hacked. Twitter users found out firsthand what a real hack looks like on July 15, 2020, when high-profile accounts for a handful of public figures (130 accounts were targeted; 45 were successfully hacked) briefly shared a message inviting followers to make charitable donations in Bitcoin and receive back double the value of their original donation.

GAMES PEOPLE PLAY

Nintendo Attack (2020)

Video game consoles have come a long way since the 1980s heyday of one-button joysticks and 8-bit graphics, and gamers are now linked by global networks. Hackers raided gaming titan Nintendo in early 2020, stealing data from more than 300,000 user accounts. In addition to personally identifying information (PII) like names, birthdates, and e-mail addresses, hackers also stole credit card data and PayPal data.

STOCK MARKETS

Nasdaq Attack (2010)

The Nasdaq stock exchange, one of the biggest in the world, lists thousands of different stocks every day. The 2010 attack on Nasdaq (alleged to have been attempted by state-sponsored Russian hackers) is possibly the most famous failed hack in history. U.S. government officials from the NSA, CIA, and Department of Homeland Security detected a so-called "digital bomb" before it could be activated.

PHYSICAL INFRASTRUCTURE

Colonial Pipeline Attack (2021)

Physical systems are often guided by computers. A criminal hacking group known as DarkSide caused six days of panic and chaos with a ransomware attack that forced Texas-based Colonial Pipeline to temporarily freeze its transmission operations, bottling up supplies of gasoline and jet fuel. Colonial Pipeline paid a ransom of 75 bitcoin (about $4.4 million) to restore its internal network.

Become the Next Certified Cyber Defender. www.TestOut.com