CYBER TEC
SECURITY

SUPPLY CHAIN ATTACKS

2013

TARGET DATA BREACH

In the first major supply chain attack to hit the media, hackers stole up to 40 million credit and debit card details from those shopping at the American store, by compromising a third-party refrigeration contractor. A phishing email allowed hackers to install banking trojan, Citadel, onto computers and gain credentials to access Target's internal network. The breach cost Target around $202 million.

JUNE 2017

NOTPETYA

Hackers initially targeted Ukraine in the famous NotPetya (an advanced variant of Petya ransomware) attack by infiltrating the server of a third-party accounting software vendor. After injecting malicious code into the software update, it was pushed out and subsequently installed by Ukrainian businesses, government agencies and individuals. NotPetya was especially dangerous because it was able to spread on its own after compromising the original software package.

SEPTEMBER 2017

EQUIFAX

The Equifax crisis began in early 2017 when attackers exploited a vulnerability in an open-source development framework for creating Java applications that Equifax was using. The company's consumer complaint web portal was affected, allowing hackers to access Equifax's network and extract data, as well as encrypting it so it would be harder for the breach to be discovered. Unfortunately, Equifax themselves made a number of mistakes like failing to patch and renew public-key certificates, contributing to the severity of the attack.

AUGUST 2018

BRITISH AIRWAYS

Affecting around 380,000 customers, hackers modified a JavaScript file on BA's website so it included a credit card logging script that would steal customers' payment information. Customer data was stolen from those making payments on both the website and app. Magecart, the hacking group this attack was attributed to, was also responsible for similar supply chain attacks on Ticketmaster and Cancer Research UK earlier in the year.

2020

SOLARWINDS ATTACK

Hackers compromised a piece of software called Orion, produced by major IT firm SolarWinds, by injecting malware into an update that was due to be rolled out, giving the hackers a backdoor into others' internal systems. Among those affected were US agencies such as the Department of Homeland Security and the State Department as well as major private companies like Microsoft, Cisco, Intel, and Deloitte. Microsoft described the breach as the "largest and most sophisticated attack the world has ever seen".

FEBRUARY 2021

NOVEL ATTACK UNCOVERED BY ETHICAL HACKER

Security Researcher, Alex Birsan, demonstrated a new kind of Supply Chain attack involving the injection of malicious code in tools used to install dependencies for developer projects. This malware can then spread through the target company's systems, wreaking havoc. The vulnerability was found by Birsan in over 35 companies, including the likes of Apple, Netflix, Microsoft and PayPal.