Five notorious cyberattacks that targeted governments

September 2 2024, by Rachael Medhurst

Credit: Pixabay/CC0 Public Domain

Warfare is no longer confined to physical battlefields. In the digital age, a new front has emerged—cyberspace. Here, countries clash not with bullets and bombs, but with lines of code and sophisticated malware.

One of the most recent examples came to light in May this year, when an estimated 270,000 payroll records belonging to the UK's armed forces were found to have been exposed in a data breach. Though not explicitly named by the UK government, several ministers told the press they believed China to be responsible. The Chinese government has denied any involvement.

Of course, this wasn't the first time that governments, their institutions and employees were targeted by cyberattackers. Here are five prominent examples.

1. Stuxnet, 2010

In 2010, the first known major cyberweapon was unleashed. Stuxnet was a sophisticated computer worm (a program that replicates itself in order to spread to other computers) that targeted Iran's nuclear program. Unlike typical malware, Stuxnet was engineered to infiltrate and sabotage Iran's uranium enrichment facilities by causing centrifuges to spin uncontrollably while sending false data to monitoring systems. This made the damage invisible to the people overseeing the systems.

The attack set a new precedent in cyberwarfare, demonstrating how digital tools could cause physical destruction. Believed to be a joint operation by the US and Israel, Stuxnet delayed Iran's nuclear ambitions, but it also brought about new fears about the future of global cybersecurity.

The discovery of the worm highlighted the vulnerability of critical infrastructure worldwide. It also sparked debates over the ethics and dangers of state-sponsored cyberattacks.

2. WannaCry, 2017

In May 2017, the WannaCry ransomware attack wreaked havoc across the globe, locking up hundreds of thousands of computers in more than 150 countries. Ransomware is a malicious type of software that locks your files or computer and demands payment to unlock them.

Exploiting a vulnerability in Microsoft Windows, WannaCry encrypted users' files and then demanded a ransom payment in Bitcoin for their release. The attack hit numerous important sectors, including health care. The NHS was badly hit, with the attack affecting at least 81 health trusts. It forced hospitals to cancel appointments and divert emergency services, and it's estimated to have cost the NHS £92 million.

The rapid spread of WannaCry was stopped by a security researcher who discovered a "kill switch" in the malware, but the damage had already been done. Blamed on North Korean hackers, the attack showed the severe risks posed by outdated software.

3. NotPetya, 2017

Also in 2017, Ukraine was hit by a devastating cyberattack known as NotPetya, which quickly spread beyond its borders, damaging various companies and institutions worldwide.

Initially disguised as ransomware, NotPetya encrypted victims' data, demanding a ransom that could never be paid. It primarily targeted Ukraine's government, financial sector and energy companies, and brought vital services to a halt.

But the malware spread and ended up affecting companies across the globe, including the shipping and logistics company Maersk and the pharmaceutical company, Merck. It cost billions in damages. The White House described NotPetya as the "most destructive and costly cyberattack in history."

Unlike traditional ransomware, NotPetya's purpose was destruction rather than financial remuneration. It has been widely attributed to Russian state-sponsored hackers, who were aiming to destabilize Ukraine, though the Kremlin denied any involvement.

4. SolarWinds hack, 2020

As the world ground to a halt because of COVID-19, several US federal government agencies were targeted by the SolarWinds hack in 2020.

Hackers had infiltrated SolarWinds, a tech company providing IT network management software. They injected malicious code into the company's Orion platform, which is widely used in the public and private sectors. This allowed them to spy on an array of sensitive information across multiple government departments, including the Treasury and Homeland Security.

The breach went undetected for months and showed how vulnerable even the most secure government systems can be. The attack was attributed to Russian state-sponsored hackers, which Russian government officials have denied.

5. OPM data breach, 2015

Five years before the SolarWinds hack, the US Office of Personnel Management (OPM) was rocked by a massive data breach that exposed the personal information of more than 21 million federal employees and contractors.

It was widely believed that state-sponsored hackers from China accessed sensitive data including social security numbers, fingerprints and confidential information from employee background checks. It was a

devastating blow to national security and personal privacy, revealing vulnerabilities in the management of US government data.

It took months for investigators to uncover the full extent of the damage, which sparked a nationwide reassessment of data protection methods. Chinese government officials denied any involvement at the time.

Provided by The Conversation

Citation: Five notorious cyberattacks that targeted governments (2024, September 2) retrieved 2 September 2024 from https://techxplore.com/news/2024-09-notorious-cyberattacks.html