TechXplore

Cyberattacks: Bigger, smarter, faster

May 25 2021

A cyberattack in mid-May paralysed Colonial Pipeline, one of the largest US oil pipeline operators.

From paralysing the internet in Estonia to a $4.4-million ransom being paid last week after the shutdown of a major US pipeline, we take a look back at 15 years of cyberattacks.

Cyberwars begin

The Baltic nation of Estonia was the first state hit by a massive cyberattack in 2007, paralysing key corporate and government web services for days.

Estonia blamed Moscow, with which it was mired in a diplomatic conflict, but the Kremlin denied the charge.

First industrial target

A powerful computer virus called Stuxnet attacked Iran's nuclear facilities in 2010 in an apparent bid to cripple the country's atomic programme.

Stuxnet hit the functioning of Iranian nuclear sites, infecting several thousand computers and blocking centrifuges used for the enrichment of uranium.

Tehran accused Israel and the US of being at the origin of the cyberattack, the first to target an entire industrial system.

Yahoo hacking

A 2013 hack that affected all three billion accounts at Yahoo is believed to be the biggest cyberattack in history.

Another attack on the web services provider, blamed on Russia, affected some 500 million accounts in 2014, with stolen data including usernames, email addresses and birthdates.

It was only revealed five years later and resulted in a fine of $35 million.

Sony

Sony Pictures Entertainment became the target of a major cyberattack in 2014 linked to its North Korea-set satire "The Interview".

Washington blamed Pyongyang for the hacking, a claim it denied—though it had strongly condemned the film, which features a fictional CIA plot to assassinate its leader Kim Jong Un.

Islamic State

A group declaring support for Islamic State jihadists hacked into the social media accounts of US Central Command (CENTCOM) in 2015, an embarrassing setback for Washington in its war against IS in Syria and Iraq.

Two months after the attack a group calling itself the "Islamic State Hacking Division" published what they said were the names and addresses of 100 military personnel and urged supporters to kill them.

US vote meddling

In the run-up to the 2016 US presidential election, emails of Democratic Party candidate Hillary Clinton's campaign staff were published online.

After Donald Trump was elected to the White House, the US intelligence community alleged that Moscow influenced the outcome of the vote, resulting in a snowballing probe, sanctions and expulsion of diplomats.

US intelligence agencies accused Moscow of being behind hacking entities Fancy Bear and Cozy Bear which carried out cyberattacks on the

Democratic Party.

WannaCry's ransomware

In 2017, scores of world organisations and companies were hit by a massive cyberattack that spread rapidly using a security flaw in an older version of Microsoft's Windows XP operating system.

The attacks were launched via WannaCry, a type of malware called ransomware that encrypts files on an infected computer and demands money via virtual currency Bitcoin to unlock them.

It affected 300,000 computers in 150 countries. Among its victims were Britain's National Health Service, a factory belonging to French carmaker Renault and Spanish phone operator Telefonica.

SolarWinds breach

In the first of a recent trio of cyberattacks against the US, security software company SolarWinds was hacked in late 2020 in an attack lasting months and affecting up to 18,000 clients and more than a hundred US companies.

Washington announced economic sanctions against Russia and accused it of being responsible for the attack.

Huge Microsoft hack

In March, a hack exploiting flaws in Microsoft Exchange service affected at least 30,000 US organisations including local governments and was attributed to an "unusually aggressive" Chinese cyberespionage campaign.

DarkSide shuts US pipeline

A cyberattack in mid-May paralysed Colonial Pipeline, one of the largest US oil pipeline operators and the biggest in the east of the country, operating a system that serves 50 million consumers.

Washington identified the Russia-based DarkSide as the group which produced the ransomware used in the attack.

A few days later Colonial Pipeline admits that it has paid a ransom of $4.4 million (3.6 million euros).

Citation: Cyberattacks: Bigger, smarter, faster (2021, May 25) retrieved 23 April 2024 from https://techxplore.com/news/2021-05-cyberattacks-bigger-smarter-faster.html