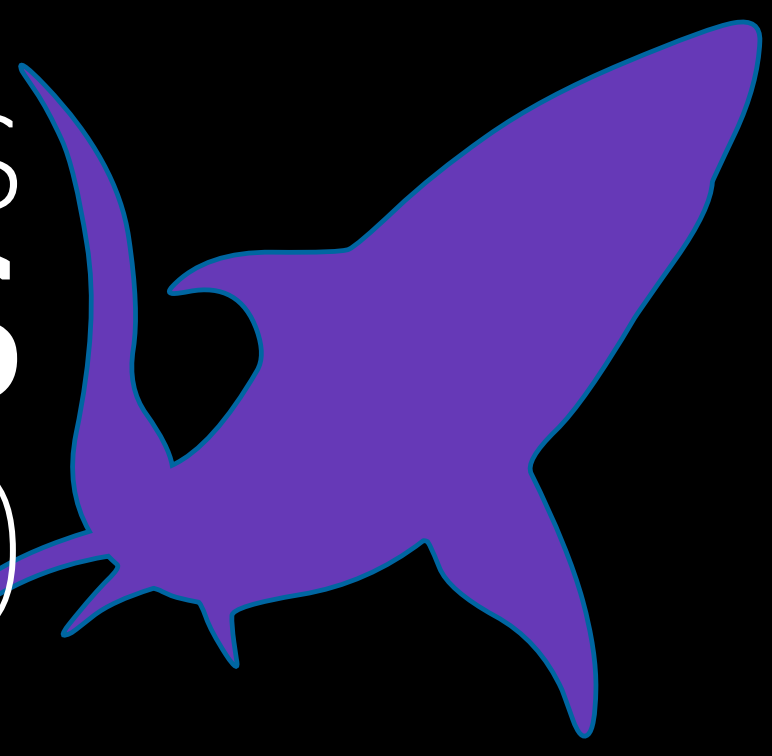
Did you know?

10 CYBER THREATS & ATTACKS EXPLAINED



1 Lone hacker website attack

In July 2019, an attack targeting vulnerabilities within part of a large financial organisation's website resulted in a data breach that affected around 100 million credit card customers in the US and six million in Canada. While it's unlikely that the data was used for fraud, the cost to the company was around $150 million.

2 Magecart

Originally thought to be one group, Magecart is now considered to be a number of cybercriminal organisations, some in competition with each other. They are commonly engaged in card-skimming and formjacking, using malicious code to steal credit card details and other information from payment forms on e-commerce sites. Two recent Magecart attacks hit the ticketing and airline industries in the UK in 2018.

3 Largest Denial of Service attack

A Denial of Service (DoS) attack in February 2018 rendered an online code management service used by millions of developers temporarily unavailable. DoS attacks often flood the targeted machine or resource with superfluous requests in an attempt to overload systems. The organisation called in assistance to reroute the traffic to its site while removing and blocking malicious data.

4 & 5 Meltdown & Spectre

These are two related examples of vulnerabilities within modern central processing units (CPUs) that stem from code designed to accelerate processing, but which can be maliciously exploited for unauthorised access to data. In 2018, researchers found over 130 samples of malware that tried to exploit Meltdown and Spectre vulnerabilities, although most appeared to be tests rather than live attacks. Since Meltdown and Spectre, new sets of vulnerabilities like 'Zombieload', 'fallout' and 'RIDL' have emerged which steal sensitive data from CPUs and cloud environments.

6 NotPetya

NotPetya started in June 2017 and targeted machines initially through updates to popular financial software after its source code was compromised. It affected companies in Ukraine and global companies with subsidiaries there, with costs totalling hundreds of millions of pounds; one company alone reported £100 million lost revenue.

7 Large scale unpatched software attack

In an attack on unpatched software, a global information solutions company that enables access to credit suffered a data breach in May 2017 that affected over 145 million US customers and over 15 million UK customers. Costs totalled $1.4 billion by May 2019, including legal and investigative costs, costs to improve security and shield customers from fraud, and a $700 million settlement with the US Government agencies.

8 WannaCry

WannaCry was a high-profile example of attacks that exploit vulnerabilities in software. Normally, when vulnerabilities come to light, software vendors write additional code called 'patches' to cover up the security 'holes'. WannaCry was a self-replicating ransomware attack that started in May 2017 and targeted unpatched Microsoft Windows environments. It affected over 200,000 machines in 150 countries, with collateral damage to public and private sector organisations and potentially hundreds of millions of pounds in operational losses.

9 Cloud Hopper

Cloud Hopper attacks infiltrate managed service providers, usually via a spear phishing email to trick employees into downloading malware or giving away their passwords. Attackers then use the cloud infrastructure to 'hop' from one target to another, gaining access to sensitive data. The original Operation Cloud Hopper, which started back in 2014, or possibly even earlier, hit a wide range of government and industrial entities in healthcare, manufacturing, finance and biotech in at least 12 countries; its costs are unknown.

10 Shamoon

Shamoon is an example of wiper malware, which is designed first to exfiltrate data and then to cover its own tracks and wipe the data from the machine, either by deleting it or overwriting it with garbage data. Shamoon specifically deletes the master boot records of a PC and renders it unable to start. While Shamoon dates back to a 2012 attack on national oil companies of Saudi Arabia, more recently it has affected other oil and gas organisations.

Trusted partner for your **Digital Journey**

Atos