

ATTACK!

ACCORDING TO THE UK NATIONAL CYBER SECURITY CENTRE THERE ARE FOUR STAGES TO A CYBER ATTACK:



SURVEY

Identify potential vulnerabilities



DELIVERY

Exploit a vulnerability



BREACH

Gain unauthorised access



AFFECT

Carrying out activities within a system that achieve the attacker's goal

CYBER CRIMINALS' TOOLKIT

Threat actors employ a wide range of tools to meet their objectives:

» **PHISHING** is sending emails to people asking for sensitive information (such as bank details) or encouraging them to visit a fake website - around 135 million phishing attacks are attempted every day.

» **SPEAR-PHISHING** is a personalised and targeted version of phishing. Here threat actors use social engineering to present themselves as trusted individuals or information sources as it is often easier to exploit an individual's weaknesses than a system's.

» **DENIAL-OF-SERVICE (DOS)** attacks aim to flood a target with fake requests, so as to exhaust server resources, whereas **distributed denial-of-service (DDoS)** attacks are launched from multiple devices, distributed across the internet and are generally harder to deflect due to the volume of devices involved. Each can be used as a smokescreen while threat actors conduct more invasive attacks in the background.

» **MALWARE** is malicious software designed to be harmful to a computer user and could include spyware (programs that spy on your online activities), viruses (programs that corrupt other programs) and Trojan horses (programs that look OK but hide something nasty).

» **RANSOMWARE** is malware that takes the victim's computer hostage by making it unusable and demanding payment to release it.

» **CLONING/WATER HOLING** involves setting up a fake website or compromising a real one to exploit visiting users - like a crocodile in a water hole, waiting for a thirsty buffalo, threat actors wait for unsuspecting users to visit the affected website where they attack either through stealing information or injecting malware into the user's systems.

WHAT BOARDS NEED TO KNOW IN THE EVENT OF A CYBER BREACH...

- 1 How did the firm learn about the breach? Was it notified by an outside agency or was the breach found internally?
- 2 What was affected by the breach? Was anything stolen?
- 3 Does the breach require prompt disclosure to authorities? If so, is the firm's legal team prepared for such notifications? Who else should be notified about this breach?
- 4 What steps are being taken by the response team to ensure the breach is under control and the hacker no longer has access to the firm's internal network? Is the crisis response plan working as planned?
- 5 Does the firm believe the hacker was an internal or external actor?
- 6 What weaknesses in the firm's system allowed the breach to occur and what steps can the firm take to make sure this type of breach does not happen again?

