CYBER CRIME

Common Stages & Patterns

There are a number of attack models that describe the stages of a cyber-attacks, and the majority have four common stages. Whilst some of these will meet their goal, others may be blocked by firewalls and various security measures.

An attack, particularly if it is carried out by a persistent adversary, may consist of repeated stages. The attacker would continuously probe your defences for weaknesses that if exploited, will take them closer to their ultimate goal. Understanding these stages will help you to better defend yourself and your organisation.

We have provided a simplified model in this document that describes the four main stages present in most cyber attacks, *The Cyber Kill Chain® produced by Lockheed Martin* is a popular example.

Stage I

CYBER SURVEY

Investigating and analysing available information about the target in order to identify potential vulnerabilities. Attackers will use any means available to find technical, procedural or physical vulnerabilities which they can attempt to exploit.

Stage II

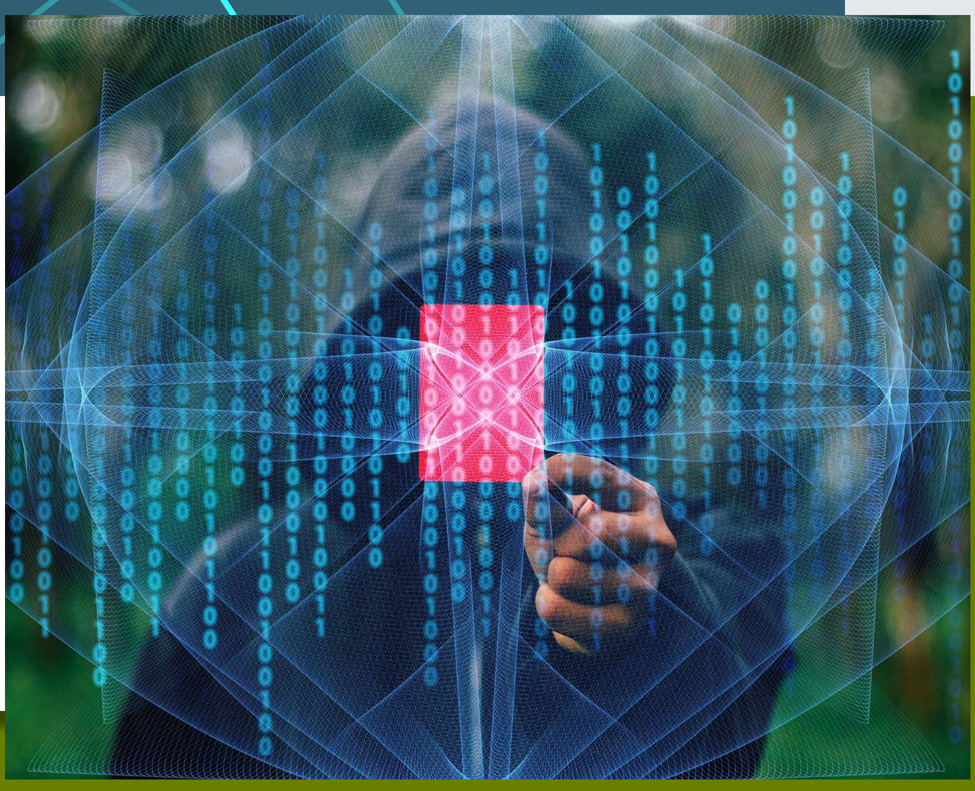
CYBER DELIVERY

Getting to the point in a system where a vulnerability can be exploited. During the delivery stage, the attacker will look to get into a position where they can exploit a vulnerability that they have identified, or they think could potentially exist.

Stage III

CYBER BREACH

Exploiting the vulnerability / vulnerabilities to gain some form of unauthorised access. It may allow them to make changes that affect the system's operation, gain access to online accounts, and achieve full control of a user's computer, tablet or smartphone.



Stage IV

CYBER AFFECT

This could be in the form of retrieving information they would otherwise not be able to access, such as intellectual property or commercially sensitive information, or making changes for their own benefit, such as creating payments into a bank account they control or changing insurance policies.

The Internet can be a hostile environment. The threat of attack is ever present as new vulnerabilities are released and commodity tools are produced to exploit them. Doing nothing is no longer an option; protect your organisation and your reputation by establishing some basic cyber defences to ensure that your name is not added to the growing list of victims.

“INTELLIGENCE THAT WORKS”

SOURCE: https://www.ncsc.gov.uk/white-papers/common-cyber-attacks-reducing-impact

#OrganisedDisruption