6 STAGES OF AN ATTACK

DATA EXFILTRATION STAGE

06

RECONNAISSANCE STAGE

01

Six Stages Attack

DELIVERY STAGE

02

LATERAL MOVEMENT STAGE

05

COMMAND AND CONTROL STAGE

04

03

INSTALLATION STAGE
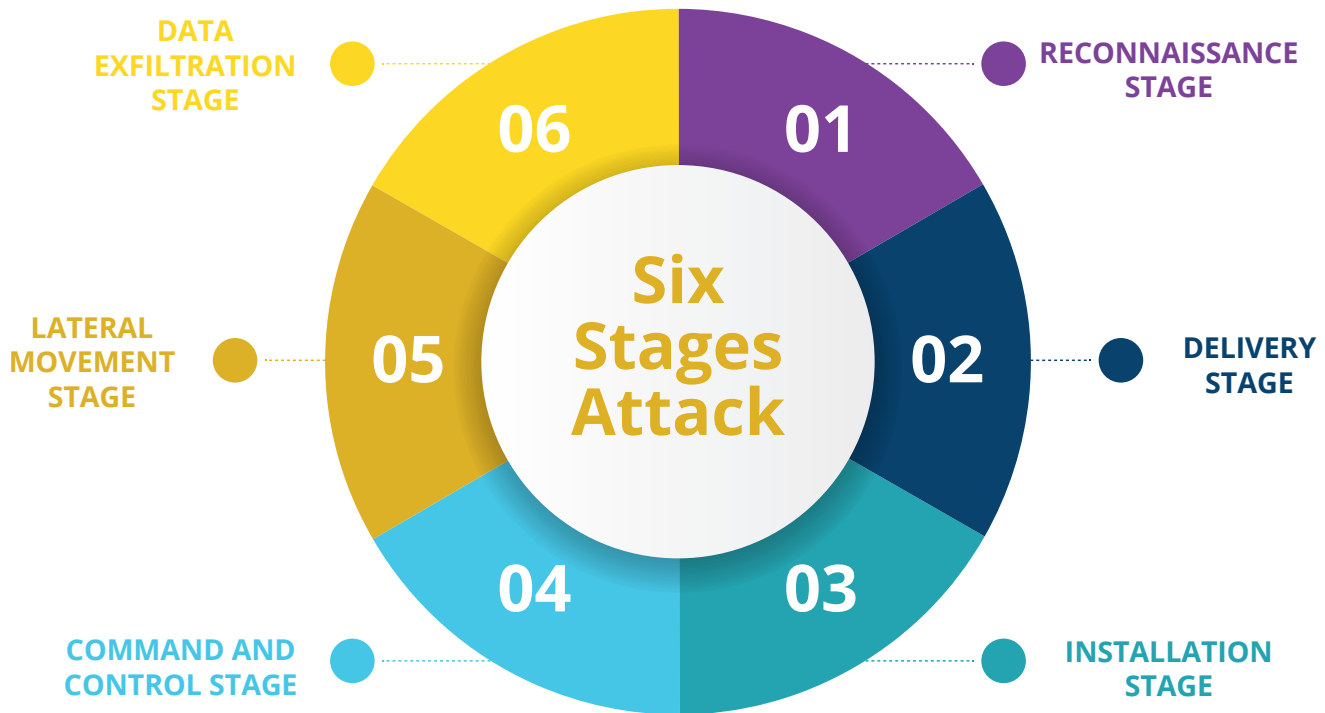
Stage 1 is the Reconnaissance stage in which the attacker gathers information before an attack to find a vulnerable point in the network. This includes threats such as spam email.

Stage 2 is the delivery stage in which the attacker delivers a malicious package to gain access to a network. This includes threats like communication to a malicious website over proxy.

Stage 3 is the installation stage in which the attacker finds a vulnerable point of entry into the network and gains access. This includes threats like an unusual process on a host in the operating system events.

Stage 4 is command and control. In this stage, the malicious package is sending traffic to a malicious web server to escalate access. This includes malware beaconing over proxy.

Stage 5 is lateral movement. In this stage, the attacker has escalated access to execute the attack using admin privileges.

Finally, **stage 6** is data exfiltration. This is the stage in which the attacker moves freely around the network and can access or remove any sensitive 9 data at will. This is detected through an observed spike in the number of bytes out over proxy.