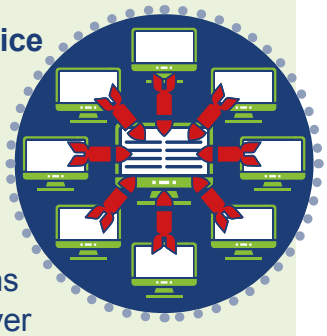
Denial of Service (DOS) Attack

Denial of Service (DOS) attack is a targeted attack that causes disruption to the network by overwhelming a system with requests until it can no longer cope and crashes. DOS attacks involve a single device flooding a system but this method is easily noticed and traceable.

Distributed Denial of Service (DDOS) attacks send requests from multiple devices and are far harder to detect. A DDOS is performed by combining several software applications that run automated tasks over the Internet, known as a Botnet, making it difficult to pinpoint the origin for the attack.



Through the likes of Social Engineering, vulnerabilities, insider threats, etc. a criminal will compromise many internet connected devices to create a Botnet. A Botnet allows a criminal to simultaneously control the devices to co-ordinate a DDOS attack.

Devices that may facilitate a Botnet include computers, printers, smart assistants, smart fridges, smart doorbells. In fact, any device connected to the internet, referred to as IOT (Internet of Things), can be used.

To prevent your devices from becoming part of a Botnet and facilitating this attack, follow our recommended best practices, which can also be found on our Advice Page:

Change default passwords

Default passwords are easily guessed or obtainable online.

Use strong, unique passwords for all devices and online accounts

Prevent criminals from accessing your devices and taking control.

Use 2 Factor Authentication (2FA)

For an extra layer of security protecting your account.

Update all software and Operating Systems

Ensure they are supported by the vendor: criminals take advantage of vulnerabilities to infect a system with malware. Unsupported software will not receive the latest release of updates when needed.

Switch on a Firewall

Prevent unauthorised connections to the network.

Install AntiVirus

To detect and remove malware.

Train staff to identify and report potential threats (phishing, insiders, ransomware, DOS)

Knowing the signs of an attack can reduce your response time, which will greatly reduce the impact it has on your business. Often attacks (especially DOS) noticeably slow systems down.

Manage user privileges and removable media

Prevent any opportunity for malware to infect your whole network.

For advanced technical solutions that reduce the impact of DOS attacks, speak with Technical Support, your Internet Service Provider, your web provider and any other service providers you use. Nonetheless, following best practice will greatly reduce the risk and impact of an attack:

Create an Incident Response Plan and Disaster Recovery Plan

Being prepared for a DOS attack will ensure a speedy recovery. The sooner this attack is identified, the quicker you can respond and reduce the impact it has on your business.

Backup your Data

DDOS renders your systems unusable. Using clean backups, you can continue business as usual.

Update all software and Operating Systems

Vulnerabilities make it easier to carry out an attack.

Manage user privileges and segment the network

Contain the spread of the attack so part of your network is spared. Importantly, ensure admin capabilities are separate from everyday activity. It is difficult to recover if the admin accounts are compromised.

Switch on a Firewall

Prevent unauthorised connections to the network.

Use a VPN

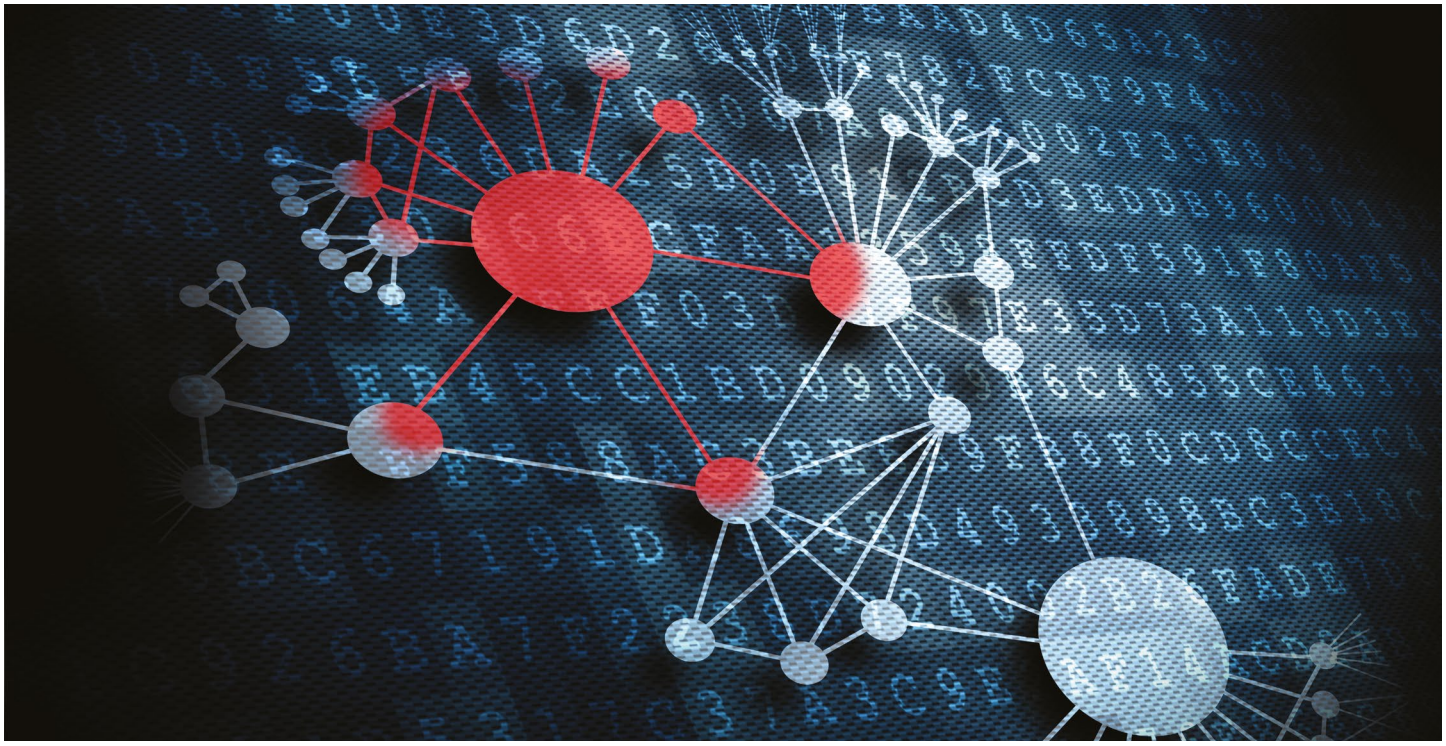
To hide your IP (Internet Protocol) address from sight. DOS attacks target IP addresses.

Use the cloud

Cloud providers have the software in place to handle DDOS attacks. It also makes it much harder for criminals to target a specific business.

Know your business infrastructure

Identify the parts of your business infrastructure that has potential to be overloaded and who is responsible for it so you can action appropriately, whether it's yourselves or your supplier.



For more detailed guidance visit the NCSC website:
https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

PDSC
POLICE DIGITAL SECURITY CENTRE