30 JUNE 2020
WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK
WWW.WMCYBER.ORG

West Midlands | Regional Cyber Crime Unit

# DoS/DDoS Information Guide

The very first DoS attack, way back in 1999, occurred when a network of 114 computers at the University of Minnesota were infected with a malicious script called “Trin00”. Twenty years later, and DoS attacks are now one of the most common and most difficult types of attacks to address.

## How does it work?

A DoS attack floods a target with so much traffic that it simply cannot respond or crashes, preventing access for legitimate users. Affected services include email, websites, online accounts, and remote working services and for this reason, DoS attacks cost organisations both time and money.

## The most common attacks include

- **SMURF ATTACK:** The adversary asks the target machine whether they are experiencing any communication problems and whether data is being received in a timely manner. This is known as an ICMP or ‘ping’ request. The attack is successful because the adversary generates hundreds of these ping requests from fake systems and the targeted machine crashes when trying to reply to them all.
- **SYN FLOOD:** The adversary asks the target machine whether it is happy to connect. The connection process requires 3 distinct steps (known as the 3-way handshake), but the attacker’s machine never completes these steps. Instead, it sends more and more requests to connect, leaving the server in limbo and unavailable for legitimate requests.

## What is a Distributed Denial-of-Service attack (DDoS)?

A DDoS attack occurs when there are many machines (called bots) working together to attack a targeted system. These bots represent hijacked computers, these may be vulnerable machines within your organisation. In this case, these hijacked machines are as much a victim as the target of the DDoS.

Cyber criminals also hire bots to perform these attacks, if they lack the necessary skill to set up their own botnet. DDoS allows for exponentially more requests to be sent to the target, increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

## How do you know if an attack is happening?

Symptoms of a Denial of Service (DoS) can resemble a network availability or other non-malicious availability issues. Typical symptoms are:

- Unusually slow network performance (opening files or accessing websites),
- Unavailability of a particular website, or an inability to access any website.

The best way to detect and identify a DoS attack would be via network traffic monitoring and analysis. Network traffic can be monitored via a firewall or an intrusion detection system.

## Mitigation Advice

· Enrol in a DoS protection service that detects abnormal traffic flows and redirects traffic away from your network. The DoS traffic is filtered out, and clean traffic is passed on to your network.
· Contact your ISP to ask if there is an outage on their end or even if their network is the target of the attack and you are an indirect victim. In either case, they may be able to give advice.
· It is possible for administrators to monitor network traffic to confirm the presence of an attack, identify the source, and mitigate the situation by applying firewall rules and dropping traffic that meet a certain criteria
· Create a disaster recovery plan to ensure successful and efficient communication, mitigation, and recovery in the event of an attack.

It is also important to take steps to strengthen the security posture of all of your internet-connected devices in order to prevent them from being compromised, such as installing anti-virus and using good patch management. Attackers may use a DoS attack to deflect attention whilst another type of attack is launched.

## Make Positive Cyber Choices:

Did you also know that if someone conducts a DDoS attack, or make, supply or obtain stresser or booter services, they could receive a prison sentence, a fine or both? Often people don’t realise that one pathway into cyber crime can come from “modding or cheating” in gaming by using these services. Booting someone offline whilst playing online games may seem like a harmless joke, but is still illegal. Find out more at https://www.nationalcrimeagency.gov.uk/?view=article&id=243:ddos-attacks-are-illegal&catid=2 or www.cyberchoices.uk

## OTHER USEFUL RESOURCES:

**Denial of Service (DoS) guidance:**
https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

**Guidance: A minimal Denial of Service (DoS) response plan:** https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/a-minimal-denial-of-service-response-plan

**Infographic: Preparing for a DoS Attack**
https://www.ncsc.gov.uk/files/Preparing-for-DoS-attacks-infographic.pdf