East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Wednesday 24 June 2020

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

Today's topic is Denial of Service (DoS)

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.

Solutions

- 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.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.
Forward suspicious emails to report@phishing.gov.uk.
Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).