CYBERCRIME NEWS

ISSUE 16 • AUGUST 2025

RECONNAISSANCE

THE FIRST STAGE OF RANSOMWARE ATTACKS

RECONNAISSANCE IS OFTEN THE FIRST STAGE OF A RANSOMWARE ATTACK.

It involves gathering information about a target before an attack is carried out. Think of it like burglars scoping a property before breaking in – They will identify weaknesses, opportunities, and valuable assets.

KEY RECONNAISSANCE TECHNIQUES

SEARCHING OPEN OR CLOSED WEBSITES/SOURCES:

Attackers search for public information about an organisation, such as names of staff, email addresses, or network infrastructure. This helps them identify potential entry points or targets for phishing emails. Criminals may also acquire information from closed sources such as leaked credentials from data breaches.

GATHERING NETWORK INFORMATION:

Criminals will seek out technical details about the network, such as IP addresses, domain names, and Virtual Private Network (VPN) gateways. This assists them in planning their method of entry and movement once inside the system.

WHY DOES RECONNAISSANCE MATTER?

1. **PREPARATION IS KEY FOR CRIMINALS:**

   Effective reconnaissance means the difference between a failed phishing email, and a catastrophic ransomware deployment that effects the entire organisation.

2. **MAXIMISING FINANCIAL GAIN:**

   By identifying high-value data and critical systems, attackers can choose targets that will cause the most damage to their victim, allowing them to demand higher ransoms.

3. **STAYING UNDER THE RADAR:**

   Reconnaissance can be passive, meaning attackers can gain information without alerting the victim.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

DORSET POLICE

PRODUCED BY DORSET OPCC AND DORSET POLICE

DEFEND AGAINST RECONNAISSANCE

LIMIT PUBLICLY SHARED INFORMATION

Reduce unnecessary details about your staff, technology, and processes from your website or social media. For example, avoid sharing detailed organisational charts or naming specific software and versions used in your systems.

CHECK FOR OPEN PORTS AND UNNECESSARY SERVICES

Attackers often scan networks to find open ports that indicate running services. Ports on a network are like doors that let different types of traffic in and out. Each door has a specific job, such as:

- Port 80 – for web traffic
- Port 25 – for email
- Port 3389 - for remote desktop (often targeted for unauthorised remote access)

Regularly review which ports are open to the internet and close those that are not required. For more information on this, please see the Further Information section at the end of this newsletter.

MONITOR FOR SUSPICIOUS BEHAVIOUR

Utilise threat intelligence and network monitoring tools to detect suspicious behaviour on your network. For instance, multiple failed login attempts from the same IP address, or port scanning activity.

EDUCATE STAFF

Train staff to be vigilant with their personal and financial information. Education on reducing what we share publicly, and maintaining a secure online presence is crucial in reducing the effectiveness of reconnaissance efforts.

We can help with this – The Dorset Police Cyber Crime Unit offer free Cyber Awareness sessions, covering topics such as Ransomware and Social Engineering.

FURTHER INFORMATION

THE SOUTH WEST CYBER RESILIENCE CENTRE (SWCRC)

https://www.swcrc.police.uk/

The SWCRC is a police-led, not-for-profit partnership that helps businesses and organisations improve their cyber-security. They provide free guidance and updates on emerging threats to help keep your systems and data safe.

NATIONAL CYBER SECURITY CENTRE – RANSOMWARE

https://www.ncsc.gov.uk/ransomware/home

For further information on Ransomware, the National Cyber Security Centre provide clear, practical advice on how to protect your organisation from ransomware, and what to do if you are attacked.

DORSET POLICE

Dorset Police

Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

E cybercrimeprevention@dorset.pnn.police.uk
www.dorset.police.uk

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

Office of the Dorset Police & Crime Commissioner

Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

T 01202 229084
E pcc@dorset.pnn.police.uk
www.dorset.pcc.police.uk