CNR Network Reporting

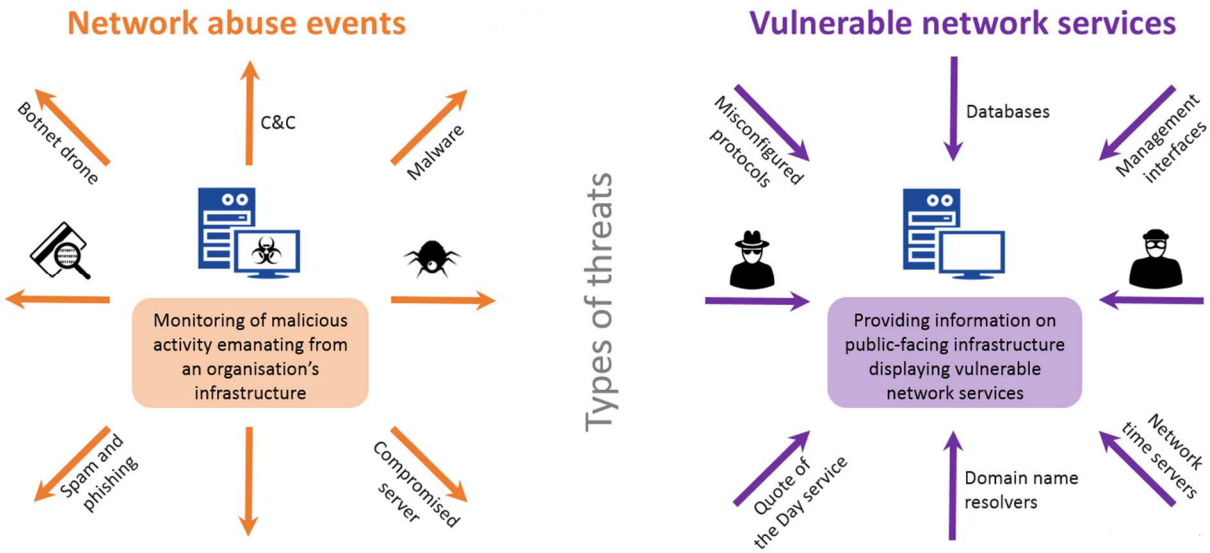
National Cyber Security Centre

The National Cyber Security Centre (NCSC) offers a free network abuse management reporting service called "CNR Network Reporting" (CNR) to Cyber-Security Information Sharing Partnership (CiSP) members to help them secure and protect their corporate IT infrastructure.

We process actionable threat information to establish indicators of malicious activity and compromise as well as identify known vulnerable network services. This threat information is gathered from a range of information security forums and initiatives who collect data passing across the public Internet. Our abuse management system ingests data feeds from public, commercial and trusted sources (including several privileged feeds not available elsewhere but made available to the NCSC in its position as the national CERT) to notify subscribing organisations.

Our CNR service is free-of-charge to subscribing organisations. There are two elements in CNR reports:

(i) **network abuse events**, which provide indicators of cyber threats and malicious activity from within an organisation's network; and
(ii) **vulnerable network services**, an outline of which Internet-facing infrastructure network services are vulnerable from outside.



The CNR service is not a replacement for any existing intrusion detection systems or protection already in place; it should be viewed as another tool in an organisation's arsenal. We process a vast amount of information on various types of malicious network activity, but this is not intrusive and we cannot see inside a corporate network.

Despite this, there are instances of organisations with mature cyber defences finding that only the NCSC services identify events that would not otherwise have been picked up.

The reports

We ingest open source, commercial and privileged feeds from a range of sources (including Shadowserver, Team Cymru, Abuse.CH, OpenPhish, Daniel Gerzo's BruteForceBlocker, and NCSC-FI, among others). This data is de-duplicated, harmonized, augmented, and filtered automatically. The system processes millions of events per day related to malicious network activity and vulnerable network services.

It is important to understand the NCSC neither monitors nor scans your network. The CNR service ingests data feeds and uses this information to generate its tailored and specific reports.

The CNR reports provided for subscribers include the following types of events:

Network abuse events

- Infected hosts (e.g. bots communicating with sinkholes)
- Indicators derived from malware analysis
- Botnet infrastructure (e.g. command and control)
- Compromised hosts that are serving malware
- Web server defacements
- Attacking IPs (hosts inside a network observed conducting brute force attacks)
- Sources of spam and phishing

Vulnerable network services

- Services that can be abused for amplification (DDOS) attacks and should be closed or restricted to trusted IPs:
    - CharGEN
    - DNS Open Resolver
    - MS-SQL
    - NetBIOS
    - Network Time Protocol (NTP)
    - Quote of the Day (QOTD)
    - Simple Network Management Protocol v2 (SNMP)
    - Simple Service Discovery Protocol (SSDP)
    - Steam Protocol
- Protocols that are misconfigured and should not be exposed or accessible by non-trusted IPs:
    - Cisco Smart Install
    - CWMP
    - DB2
    - Elastic Search
    - Hadoop
    - LDAP
    - mDNS
    - MemCached
    - MongoDB
    - Portmapper
    - RDP
    - REDIS
    - SMB
    - TFTP
    - Telnet
    - VNC
    - XDMCP
- Protocols that are vulnerable:
    - ISAKMP
    - Netcore/Netis Router
    - Synful Knock

Reports are sent as CSV files to nominated addresses of the organisation's choosing.

What do I need to provide?

The CNR service does not require any hardware or software installation or modification. There is nothing to implement on your side, and nothing is installed on your network. You only need provide details of your external public-facing IP addresses or ranges, and/or registered domain name(s).

How do I sign up for CNR?

If your organisation is already a CiSP member, please email cnr@ncsc.gov.uk for an application form. However, if your organisation is not already a member of CiSP, you can subscribe to the free reporting services at the same time as applying to join CiSP via https://www.ncsc.gov.uk/cisp/

Further information

Should you have further queries or questions about CNR, please email us at **cnr@ncsc.gov.uk**

2018-08-28