NCSC
National Cyber Security Centre

2011091057-NCSC

A part of **Department of the Environment, Climate & Communications**

# NCSC Flash Alert

## Increased Emotet Activity
**2020-11-09**

*https://www.ncsc.gov.ie/*

*certreport@decc.gov.ie*

**Status:** TLP-WHITE

NCSC

## Threat Type

The NCSC has observed a recent notable increase in Emotet activity targeting Irish organisations. The purpose of this NCSC Flash Advisory is to provide organisations with some context on what Emotet is, and some basic steps you can take to reduce your chances of exposure to an Emotet infection.

**What is Emotet?**
Emotet is a Trojan malware that is usually spread through email. It is an infostealer and its goal is for the victim to click-on/open the infected content of an email - usually either a macro enabled document (usually an Office document or a PDF) or a link to a malicious site.

Emotet's objective is to steal content such as passwords, credit card details, emails and other personal information. It can also lead to further malware being downloaded and run on a system; Emotet is a known dropper for the Trickbot Trojan which steals information and downloads Ryuk Ransomware. After infecting a device, Emotet will use the victims contact list to spread itself to more potential victims.

## Recommendations

CSIRT-IE advises organisations to consider the following mitigation steps:

- Make sure AV signatures are updated on all devices.
- Promote user training and awareness campaigns - a training programme and periodic awareness campaigns should be utilised. Advise users on how to recognise phishing/malspam mail - email attached Microsoft Office files (.doc, .docm, .docx, .xls, .xlsm, .xlsx) with a Macro embedded are a favourite vector of the Emotet authors.
- Do not allow Macros embedded in Microsoft Office products to run automatically. Advise users to not enable content for Macros when presented with the option and to report it to their IT Security department.
- Vulnerability Management and Patching - Deploying security patches to fix vulnerabilities in software and systems is the most effective way of preventing systems from being compromised.
- Passwords are often the only barrier between you and your personal information. They need to be strong, secure, random and managed appropriately.
- Use Multi-Factor Authentication (MFA) on all email accounts.
- Implement DMARC which can help you establish where your email has come from, helps protect against email spoofing, improves trust and simplifies email processing.
- Install a Web Filter. Users clicking on links or visiting malicious sites inadvertently is still one of the major threats to network security.
- Users can find a list of latest IOCs associated with Emotet here. This site is updated regularly with information on recently identified Emotet campaigns.