PSNI CYBER CRIME CENTRE

Information Sheet – 07/08/2020

This information sheet has been compiled by the Police Service of Northern Ireland Cyber Crime Centre and is intended to raise awareness of current threats and available guidance: **Contact us:** cyberprotect@psni.pnn.police.uk

The return of EMOTET

Over recent weeks, security blogs across the Internet have reported a noticeable rise in Emotet activity after what has been described as a distinctly quiet few months. Your first thought may be, well what is it?

Emotet is a piece of malware primarily distributed by malicious emails using the contact list of a compromised organisation. In a typical attack, a user opens an attachment or clicks a link leading to the deployment of Emotet and exposure to additional malware Emotet is associated with such as Trickbot.

Designed as a banking Trojan, Emotet is known for its ability to use a victim's email contact list to distribute itself and to use genuine email subject lines to entice the recipient to click the link. The current campaign however has revealed a new side to Emotet. It can now apparently capture and use genuine attachments, meaning you could receive an email from a contact you know, which contains attachments you created and sent, something that may reassure some that the email is genuine and the link or extra attachment is something that can be opened safely.

Advice

Staff Awareness

As with most phishing-based campaigns, Emotet distribution concentrates on enticing the end user to click a link or open an attachment. Educating staff on current trends, encouraging users to challenge email attachments / links and promoting a positive reporting environment, are crucial steps in preventing Emotet getting a foothold in your network. NCSC SME guidance

Protect your accounts

Whether it is an email account or RDP, stolen credentials linked to an organisation are of value and as a result, they can be traded amongst organised crime gangs specialising in attacks such as ransomware. Protect your accounts with strong passwords and just as importantly, 2FA / MFA to minimise the risk of outside parties gaining unauthorised access. NCSC Malware Mitigation Advice

Patch your end points

Described by the NCSC as 'the single most important thing you can do to secure your technology', ensuring your organisation undertakes this basic step will help prevent malware exploiting known vulnerabilities. Are your end points are up to date with the latest Microsoft patches and software updates? NCSC Patching Guidance

IN THE NEWS

New CEO for the NCSC

The NCSC have announced that NI born Lindy Cameron will become its new Chief Executive Officer, a role that will see Ms Cameron leave the Northern Ireland Office and replace current CEO Ciaran Martin (who also hails from NI!). We wish both well in their new roles.

NCSC - Cyber Insurance Guidance

Is cyber insurance right for you? The National Cyber Security Centre has released their first guidance document in respect of Cyber Insurance. Focusing on the cyber security aspects of cyber insurance, the guidance aims to support any organisation considering this option by discussing questions they may wish to consider in advance. The guidance also outlines the roll the NCSC Cyber Essentials scheme can play in assisting an organisation protect itself.

Never too young to report

What would your child do if they spotted a suspicious email or sms? This week a keen eyed 14yr old in NI reported a phishing attempt containing a link to a spoofed banking webpage indistinguishable from the genuine article. A great piece of detective work which lead to steps being taken to block access to the webpage.

Suspicious emails can be reported to the NCSC Suspicious Email Reporting Service - report@phishing.gov.uk

Useful websites

www.actionfraud.police.uk
www.cyberaware.gov.uk
www.nicybersecuritycentre.gov.uk

Social Media

@PSNIBelfast
@cyberawaregov
@NICyberSC

we care · we listen · we act