PSNI CYBER CRIME CENTRE

INFORMATION SHEET – 13/05/20

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. Advice and information is changing daily as we all navigate our way through the current COVID19 pandemic so please ensure you only take information from reputable sources.

Alongside our counterparts within the UK Cyber Protect network, the Cyber Crime Centre are supporting the issuing of notifications to organisations who are possibly at risk to the recently published Sophos XG Firewall vulnerability. We would encourage anyone using this product to ensure advice from the vendor on mitigating the risk is followed. For more information and advice, see: **NCSC statement: Sophos Vulnerability**

Updates

Action Fraud

The latest update from Action Fraud (07/05/2020) indicates a total of £2,996,252 has been reported lost in the UK by 1,467 victims of coronavirus related scams.

Suspicious Email Reporting Service

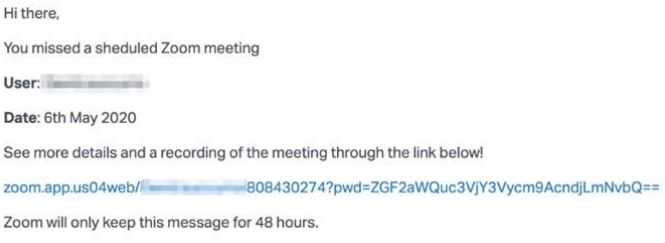
The NCSC report that as of 07/05/2020, over 160,000 suspect emails have been reported to the new reporting system (**report@phishing.gov.uk**). These reports have helped lead to the take down of over 300 fake websites. This reflects a great take up by the public and a real positive step forward in the battle against phishing.

Ransomware update

In their regular ransomware update, **Bleeping Computer** report that current ransomware variants such as Sodinokibi and Ryuk have helped raise the average ransom demand to $111,000, a 33% rise on the previous quarter. These increased demands and being made in conjunction with the threat of having data stolen prior to the attack released online.

As seen elsewhere in the UK, locally we have seen attackers move from issuing demands on encryption in favour of having a victim contact them by email to ascertain how much they need to pay. In one recent incident in which attackers were able to encrypt onsite backups, a local company received a demand for over $30,000 for decryption keys.

NCSC Malware & Ransomware Advice


Hi there,

You missed a sheduled Zoom meeting

User: [redacted]

Date: 6th May 2020

See more details and a recording of the meeting through the link below!

zoom.app.us04web/[redacted]808430274?pwd=ZGF2aWQuc3VjY3Vycm9AcndjLmNvbQ==

Zoom will only keep this message for 48 hours.

Fujitsu have observed a phishing campaign centred on alleged missed Zoom meetings. A platform many of us may not have heard of before the current pandemic, anyone clicking this link would have been taken to a fake Microsoft login webpage looking to steal your credentials.

NCSC Suspicious Email Reporting Service – forward suspicious emails to report@phishing.gov.uk
Did you know you can report spam sms on your phone to 7726 (SPAM)

Useful websites
www.actionfraud.police.uk
www.ncsc.gov.uk/cyberaware
www.nicybersecuritycentre.gov.uk

Social Media
@PSNIBelfast
@cyberawaregov
@ncsc