PSNI CYBER CRIME CENTRE

Ransomware – 22/07/2020

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

Ransomware

Over 2020, it is true to say that those behind ransomware attacks have become increasingly selective about who they target. Multinationals such as Travelex or public sector bodies such as Redcar & Cleveland Council are often in our headlines and incidents increasingly involve the combined threat to leave data encrypted or to release data stolen before the attack unless payment is made.

The experience in Northern Ireland, as elsewhere across the UK, shows that quite often it is SMEs based in local manufacturing or the service sector who can find themselves falling victim to ransomware and attackers do not avoid small family firms or charities.

Over the past week, the Cyber Crime Centre has been alerted to two local ransomware attacks both of which have resulted in significant impact to the organisations involved.

As reflected in the experience of many local cyber security providers, the NCSC and law enforcement, there is no way to completely protect your organisation against this type of attack, but with defence in depth and crucially the right back ups, it is possible to increase the chances your organisation will avoid, detect or successfully recover from the impact a ransomware attack.

```
Not your language? Use https://translate.google.com
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
-----
What happens to your files?

It's clear, your files encrypted with [RSA-2048] algorithm which the
decryption key is in our hands.
Don't worry, you can return all your files to the original state if you'll be
a little generous!

- To decrypt your files you should contact with @[redacted] user in Telegram
messenger (https://telegram.org)

*** Don't waste your time and money on forensics or recovery techniques to
restore files, it may take your files to an unrecoverable state.
*** To ensure your data is safe you can decrypt 3 files that don't have
important info and ready to recover for free.
*** Remember, the entire payment and decryption tool delivery process done by
a stupid automated bot, so don't beg on it!

*** From today [07/16/2020] you have 5 days to contact our bot and pay the
requested amount.
    after 5 days for each day, you should pay an extra $2,000, and finally,
after 5 days (10 days in total),
    the bot stops responding to you and the negotiate is the final option for
you which costs a lot.

*** The bot need below information to decrypt your files, so don't remove or
modify it ***
-----BEGIN PUBLIC KEY-----
```

Summary of NCSC Ransomware Tips

Tip 1 – Make Regular Backups
The key action to take to mitigate ransomware. Make regular backups, keep at least one copy offline and do not rely on a single cloud syncing service.
Test your backups

Tip 2 – Prevent malware being delivered to devices
Use email filtering & software tools to reduce the impact of phishing emails and ensure services such as remote access are secured against brute force attack.
Authenticate using MFA

Tip 3 – Prevent malware from running on devices
Ensure end user devices are correctly configured, use the latest OS versions and keep software up to date. Protect against malicious Microsoft Office macros
PROMOTE STAFF AWARENESS

Tip 4 – Limit the impact and enable rapid response
Segregate obsolete platforms, regularly review permissions and limit the use of administration accounts.
Use 2FA to protect against compromised accounts

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