Jersey Financial Services Commission

Press Statement **30 June 2017**

JFSC issues guidance following recent Petya/NotPetya cyber attack

The Jersey Financial Services Commission (JFSC) is aware of the recent ransomware campaign which first appeared on 27 June 2017. The global reach and considerable impact of the current Petya/NotPetya ransomware outbreak bears remarkable similarities to the WannaCry attack of just a few weeks ago.

The JFSC has been monitoring the threat, further reviewing its own systems' security measures, while liaising with partner organisations and using intelligence to constantly assess the risk posed.

We would encourage local financial service providers to contact us if they have been affected and are already working with a number of firms who have fallen victim to this latest threat.

The Petya/NotPetya ransomware is designed to encrypt the file system of an infected Windows system, denying you access to data. It will also replace the master boot record of the computer with code to display a ransom demand for $300 in bitcoins. The ransomware is also designed to spread aggressively within your local network environment.

The JFSC has been informed of further variants of the malware entering circulation locally, distributed by phishing emails. Companies can undertake the following simple steps to help protect their organisation, please note that this is not an exhaustive list but the best advice that we have at this time:

- Most importantly for ransomware, **back up the data** that matters to you and test the backups. These should be kept disconnected or offline so they can't become infected. You should then be able to recover your data without paying a ransom
- Ensure that ransomware cannot spread to backup systems. Ransomware can take time to encrypt large volumes of files, particularly across a network share. It is imperative to ensure your back-up window is long enough to go back before any infection began and that the backups themselves are immutable once written
- Keep your organisation's **security software patches** up-to-date and deploy immediate security upgrades. Every organisation must ensure its IT systems are regularly updated. Microsoft released a security update back in March which addresses the vulnerability that Wannacry exploited and that Petya/NotPetya also appears to exploit. For those companies who have not yet applied the security update, it is recommended you should immediately deploy Microsoft Security Bulletin MS17-010. If you are using a legacy, now unsupported version of Windows, you should consider upgrading immediately.

Emma Mathew
Head of Communications
T + 44(0)1534 822166
E e.martin@jerseyfsc.org
Jerseyfsc.org

- **Network hardening** - good security practice dictates removing or disabling unnecessary network services to reduce the potential attack surface. Since Petya/NotPetya has spread quickly by abusing vulnerabilities in the Server Message Block network protocol this should be an area of immediate focus. Unless you have a very good reason not to, disable the SMBv1 protocol on your network, while also ensuring needed SMB services cannot be directly accessed from the internet. Also, disable or block other legacy protocols on your network that you are not using. Leaving them available leaves them available for malicious actors to leverage
- Use **up-to-date antivirus software** services
- **Do not download files or programs** from unknown websites or sources. Even if you know the source, get authorisation from your IT department before downloading software to the company network
- **Think before you click – exert extreme caution** regarding emails, links or untrustworthy websites that may allow dangerous viruses or malware onto the network
- Reduce access rights and control to authorised personnel only
- **Given the nature of ransomware, we suggest that you report but do not forward any suspicious emails, to your IT or Security Departments**
- **Be vigilant when opening attachments**, as viruses can be embedded in files. Take extra care when opening these files and only open them if you know they are genuine. Where possible disable automatic execution of macros – attachments/links should not open up automatically
- **Report anything suspicious** whether it is an email, link or website, to your IT or Security Departments
- Phishing emails are designed to look like authentic messages to lure you into clicking them. Trust your instincts. If an email seems suspicious or isn't quite right, even if it's from someone you know, do not open it and report it
- Accidents happen - if you do open an email or click a link you think is suspicious, inform your Security Team or IT immediately
- We advise local companies to never succumb to the pressure to pay the ransom to regain access to their applications and data. There is no guarantee that cybercriminals can or will unlock files and payment only further motivates and finances attackers to expand their ransomware campaigns. The key advice for a ransomware defence is to always be in a position where you don't even need to consider paying the ransom
- **Be alert. Think before you click.**

For further security guidance the National Cyber Security Centre website has a wide range of materials including the most up-to-date advice on how to protect your business against ransomware please visit the National Cyber Security Centre (NCSC) website:
https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance

We also suggest that companies sign up to be members of the Cyber Security Information Sharing Partnership (CiSP). CiSP is a secure joint industry and UK Government initiative for exchanging cyber-threat information. Membership gives full access to the UK Financial Services Cyber Incident Response Framework and provides vital threat information.

Ends.