CERTJE
The Cyber Security Centre for Jersey

27th February 2022

Invasion of Ukraine – Raised Cyber Threat

Jersey's Cyber Emergency Response Team CERT.JE has been closely monitoring recent developments in Ukraine including a series of cyber attacks in January and February 2022. These attacks have included both Distributed Denial of Service attacks (DDoS) and malware designed to render information systems inoperable. Several of these attacks have been attributed by UK and US authorities to Russia's Main Intelligence Directorate (GRU).

Whilst there is no evidence of a specific threat to Jersey organisations, there has been an historical pattern of cyber attacks on Ukraine with international consequences and local organisations are asked to prepare for an increase in malicious cyber activity. Similar warnings have been issued by other national cyber authorities including NCSC (UK) and CISA (USA).

Such attacks are likely to be followed by an increase in criminal or hacktivist (cyber activist) led cyber attacks. We are currently tracking follow-on cyber activity targeted primarily at government bodies, financial services, critical infrastructure and their direct supply chains.

The situation is increasingly unpredictable and this raised threat level is likely to persist.

Jersey based organisations operating in the **financial services**, **government and public services**, **professional services** and **critical infrastructure** sectors are therefore strongly encouraged to take the following immediate steps to minimise the risk of a successful cyber attack. The below advice is also appropriate for organisations outside these sectors as cyber attacks can be indiscriminate.

Awareness and Alerting

1. Register for NCSC's Early Warning Service. We have confirmed that NCSC will make this service available to all Jersey based organisations. This provides alerts when intelligence suggests your network or systems may be compromised.
2. Register for NCSC's Cyber Information Sharing Portal (CiSP) – Channel Islands Node to receive and share intelligence on potential or actual attacks. CERT.JE will sponsor applications for CiSP from Jersey based organisations following a request to hello@cert.je.
3. Register for updates from CERT.JE via our newsletter or social media (twitter and LinkedIn) so we can inform you quickly if the situation develops.
4. Inform CERT.JE of any unusual cyber activity via CiSP (Channel Islands Node) or alternatively via email to incidentreports@cert.je.

Operation of Critical Cyber Security Controls

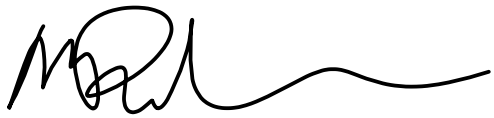
1. Ensure that good cyber hygiene practices are followed consistently and internal controls are assessed against a recognised framework such as CyberEssentials Plus, NIST CSF, NCSC's Common Assurance Framework or ISO 27001.
2. Follow guidance from NCSC on actions to take when the threat level is heightened.

3. Ensure patching is up to date on all systems including device firmware, with a particular focus on core IT infrastructure and externally facing systems.
4. Ensure externally facing services such as websites are protected from Distributed Denial of Service (DDoS) attacks, for example by implementing cloud-based DDoS protection services.
5. Implement multi-factor authentication (MFA) for all accounts and operate additional controls to secure highly privileged accounts.
6. Ensure employees are aware of good cyber hygiene practices, including use of multifactor authentication for personal accounts.

Incident Readiness & Response Planning

1. Ensure cyber incident response plans are reviewed and tested on a regular basis.
2. Ensure back up data is effectively segregated and undertake test restores on a regular basis.

Further advice and assistance is available from local cyber security providers and from CERT.JE.



Matt Palmer

Director, CERT.JE
The Cyber Security Centre for Jersey
hello@cert.je
01534 500 050