National Cyber Security Centre

General Security Advisory

GSA-2022-2940

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

18 February 2022

The Traffic Light Protocol (TLP) marking is used to ensure that sensitive information is shared with the correct audience. Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine

Summary:

The National Cyber Security Centre (NCSC) encourages Aotearoa New Zealand's nationally significant organisations to consider and strengthen their cyber security readiness in response to heightened tensions between Russia and Ukraine.

Malicious cyber activity in Aotearoa New Zealand reflects international trends. Alongside heightened tensions, there is an increased potential for cyber attacks. These may have serious impact, even for countries and organisations not directly targeted. Previous examples of this include the NotPetya cyber-attack in 2018 and more recently the compromise of SolarWinds Orion software in 2020.

Aotearoa New Zealand has previously condemned the widespread disruption resulting from indiscriminate cyber campaigns conducted by Russia.

In light of the global threat environment, the NCSC recommends nationally significant organisations consider their security posture, exercise readiness, and monitor for relevant cyber security developments.

Recommendations:

International partners have produced a range of advice to ensure readiness for specific cyber threats in the context of Russia-Ukraine tensions. For Aotearoa New Zealand, organisations may find this advice useful to consider:

Cybersecurity & Infrastructure Security Agency (CISA): *Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats*.

Cybersecurity & Infrastructure Security Agency (CISA): *Understanding and Mitigation Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*.

Canadian Centre for Cyber Security (CCCS): *Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity.*

The NCSC can be contacted by email via ***incidents@ncsc.govt.nz*** *or by phone on:* ***04 498 7654****.*
We encourage you to contact us at any time if you require any further assistance or advice.