MARCH 09, 2022

Russia/Ukraine – Geopolitical Tension Cyber Update

IESO Information Security

Traffic Light Protocol (TLP): WHITE – able to be shared broadly

ieso
Connecting Today. Powering Tomorrow.

Threat Landscape: Russia/Ukraine

- The geopolitical tension continues to escalate between Russia and Ukraine in both military and cyber warfare domains
- There are no known direct threats observed towards the Ontario electricity sector at this time
- Multiple attacks reported against Ukrainian IT systems, but not in their electricity sector
- Russia has shown prior capability to execute destructive cyber attacks against critical infrastructure

What we are seeing in the sector:

- Increased amount of perimeter probing & scanning attributed to Russia or Russian-backed threat actors

Guidance: Russia/Ukraine

- Test backup sets, disaster recovery, and business continuity plans
- Inventory and monitor VPN and business to business connections, establish criteria for disconnection if malicious activities are detected
- Assess supply chain vendors to identify and mitigate direct and spill over risks from this geopolitical tension
- Review, update, and practice, incident/crisis response plans
- Ensure strong cyber controls are in place and adopt cyber security guidance provided by reputable authorities:
    - CCCS (Canadian Center for Cyber Security), CISA (Cyber Security & Critical Infrastructure Security Agency), E-ISAC, Technology & Cyber Security Vendors

Resources:

- Canadian Center for Cyber Security
  - https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadian-critical-infrastructure-operators-raise
- Cyber & Infrastructure Security Agency
  - https://www.cisa.gov/shields-up
  - https://www.cisa.gov/uscert/ncas/alerts/aa22-011a
- Sentinel One Labs
  - https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/