National Cyber Security Centre

2202101415-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Advisory

Cyber Risk Assessment and Advice Regarding Ongoing Ukraine Situation

2022-02-17

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Impact on Ireland from Ukrainian-targeted Cyber Operations

Due to ongoing tension in the Ukraine region NCSC-IE is releasing an advisory to highlight any potential impact on Ireland or Irish-based entities should the current situation continue to escalate. **NCSC-IE currently assesses the risk to Irish entities from a targeted nation-state attack relating to current events in Ukraine as low**, however there remains a potential for entities to be affected by events downstream of any primary targets in the region. Increased cyber criminal activity should also be anticipated, as threat groups may seek to profit from the tensions.

- NCSC-IE would particularly advise organisations with operations based in Ukraine and Russia to take time to analyse/audit third-party supply contracts, test their incident response plan and to harden their organisations security posture.

Previous state-backed cyber operations in the region have caused significant disruption to some Irish-based entities in the past. Nation State APT groups focused on Eastern Europe have previously demonstrated an ability to conduct aggressive cyber operations. In recent years threat actors have exploited weaknesses in third-party software and managed services to access and attack their intended targets.

- The NotPetya attack in 2017 is a useful example of these threat groups targeting global and local supply chains. This attack was conducted primarily against businesses working in Ukraine by a Nation State APT group. It exploited MeDoc application widely used in Ukraine, whereby the software update process was hijacked to deploy malicious updates that eventually installed a wiper malware. The resulting attack caused several billion euros of damage globally.
- In 2020, Solarwinds, a supplier of network management tools was targeted by APT groups. These attackers chose to deploy additional tools to, according to reporting, less than 0.5% of the 50,000 firms that they had access to, but demonstrated a significant technical skill set in again compromising an update process in the software.

An additional risk factor to be considered is the constraint on commercial cyber security expertise in the event of an incident similar to those mentioned above. Many Irish organisations resource their incident response plans from specialist companies. Therefore constituents should consider such a risk in any response plans and take additional steps to mitigate these risks.

At this time NCSC-IE has no specific information relating to the current Ukraine situation to indicate any direct threats to Irish interests, however we do advise that all organisations take time to assess their individual exposure to cyber security risks. We would also remind entities to report any cyber incidents directly to the NCSC-IE incident response team (see contact details below).

Recommendations

Some actions organisations can take now are :

- Review Access Control
- Review Your Network Defences
- Review Vulnerability Management
- Review Backups
- Incident Response Plan
- Monitoring and Logging
- Raise Awareness Among Employees

(Please see the NCSC-IE Cyber Vitals Checklist for more information on these points)

NCSC-IE recommends that affected organisations as a minimum:

- Scan for unpatched systems and services
- Fully assess their third party MSP and supply chain contracts
- Secure Active Directory (AD) - see the Microsoft guidance for hardening AD here
- If your organisation uses Microsoft 365 review their advice on ways to secure your setup
- Ensure your organisation has an up-to-date Incident Response Process. The NCSC-IE Baseline Standards document includes a Cyber Incident Response Plan Checklist (see Annex 3)
- Review the NCSC-IE Cyber Vitals Checklist
- Review the CERT-EU\ENISA joint publication “Boosting your Organisations Cyber Resilience”

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie