Global Cyber Risk Threats Intensify in the Wake of War in Ukraine

Experts advise Russia's cyber-attacks on Ukraine could spread worldwide, and all organizations should prepare immediately

Overview

- Russia's millitary assault on Ukraine has a significant cyber component including distributed denial of service (DDoS) attacks, ransomware, and destructive wiper malware destroying data.
- Spread of decoy ransomware and destructive wiper malware used to attack Ukraine remains possible as escalation continues.
- Governments and cyber security experts warn, "Every organization, large and small, must be prepared to respond to disruptive cyber activity."

Staying Informed

As organizations around the world continue to monitor developments in Russia & Ukraine and assess the potential for escalation of cyber-attacks, remaining informed is essential. While information and guidance are rapidly evolving, the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") and the Canadian Centre for Cyber Security ("Cyber Centre") remain two of the most credible sources for timely and actionable intelligence.

Intelligence and Threat Bulletin Sources:

CISA

- Shields Up - https://www.cisa.gov/shields-up
- Russia Cyber Threat Advisories - https://www.cisa.gov/uscert/russia

Cyber Centre

- Reports and Assessments - https://cyber.gc.ca/en/reports-assessments
- Alerts and Advisories - https://cyber.gc.ca/en/alerts-advisories

In addition to cyber readiness, organizations of all sizes are also encouraged to remain aware of foreign influence operations attempting to use mis-, dis-, and malinformation (MDM) tactics to disrupt and undermine democratic interests.

Mis-, Dis-, and Malinformation Awareness:

- https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf

Guidance

At present, guidance from CISA is predicated on the following position: “While there are no specific or credible cyber threats … at this time, Russia’s unprovoked attack on Ukraine, which has involved cyber-attacks on Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region, particularly in the wake of sanctions.”

For All Organizations:

- Reduce the likelihood of a damaging cyber intrusion
- Take steps to quickly detect a potential intrusion
- Ensure that the organization is prepared to respond if an intrusion occurs
- Maximize the organization’s resilience to a destructive cyber incident

For Corporate Leaders and CEOs:

- Empower Chief Information Security Officers
- Lower incident reporting thresholds
- Participate in a test response of plans
- Focus on continuity for critical business activities
- Plan for a potential worst-case scenario

Steps Individuals Can Take to Protect Themselves

- Implement multi-factor authentication (MFA) on all accounts
- Update software and turn on automatic updates
- Think carefully before clicking on any hyperlink or opening an unsolicited attachment
- Use strong passwords and/or a password manager

For full descriptions of each bulletin point listed above visit the Shields Up page.

Free Cyber Security Services and Tools

CISA has compiled a list of freely available cybersecurity tools and services to help organizations further advance their security capabilities. This active repository includes cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community.

- https://www.cisa.gov/free-cybersecurity-services-and-tools

If you are in need of support managing this complex risk, the Organizational Resilience practice within HUB’s Risk Services Division provides consultative services to help prepare for and manage a wide array of cybersecurity, fraud, and continuity risks. Now may also be a good time to evaluate and understand your options for transferring risk through cyber insurance coverages.