KSG

KREBS STAMOS GROUP

KSG Security Advisory: Crisis in Ukraine

Issue Date: February 11, 2022

Distribution: KSG Clients and Colleagues

Version: 1.0

Executive Insights: Your Risk and How to Manage It

Statements by U.S. and western government officials and Russian government actions point to the likelihood that Russia will launch military operations in Ukraine within days. Considering Russia’s historical use of combined cyber, information operations, and military capabilities, we are advising our clients and partners to take immediate steps to reduce their cyber-risk profile and to prepare for possible human and business impacts.

This KSG Security Advisory is intended to provide actionable guidance for executives and network defenders to help them better understand and manage their risk exposure in the coming days.

Expected Impact

Russian operations will likely limit intentional impacts to targets in Ukraine that align with Russian military operational objectives. That includes Ukranian government and key infrastructure targets. It is unlikely that Russian state-sponsored cyber actors will take direct intentional action against U.S. or western businesses located outside of Ukraine.

There are circumstances, however, where entities outside Ukraine could be indirectly or incidentally impacted. Those circumstances include poor design or operational control of deployed malware, or corporate network configurations that allow for movement from Ukrainian networks to systems outside the country.

Following any western response to Russian hostilities, including sanctions, diplomatic actions, or additional lethal aid support to Ukraine, Russian cyber actors could use deniable and reversible actions (including ransomware) against western targets. Accordingly, an effective risk management strategy optimizes for an adversary’s mistakes as much as their precision.

Identifying Your Risk

Direct Operational Risk: Organizations with personnel, assets, or operations in Ukraine, Belarus, or Russia should take these developments very seriously and should take the most aggressive defensive steps. In some cases, those steps will include extracting personnel, isolating network connections, or idling operations.

Dependency Risk: Organizations with dependencies (e.g., outsourced software services in Ukraine) are next highest priority.

Indirect Risk: U.S. or western-based businesses in critical industries such as finance, energy, transportation, and water should consider themselves potential targets for follow-on actions or responses to western sanctions against Russian interests.

It is important to note that up until the very moment hostilities begin, any decisions to further escalate tensions are reversible by the Kremlin. Expect western national security leaders to continue to provide opportunities for Moscow to de-escalate tensions.

Executive-Level Actions

1. Organizations should immediately activate crisis management cells and incident response plans. Ensure plans are up to date, verify contact information, establish a regular coordination cadence, and remind responsible parties of their duties. Consider conducting a tabletop exercise or rehearsal of duties drill.
2. Hold emergency board committee meetings and receive briefings from management and security teams on contingency planning and staff protection plans.
3. Confirm any connections or dependencies on systems or operations in Ukraine, Belarus, and Russia. Verify or implement segmentation of networks and access and confirm ability to isolate network on short notice. Consider isolating operations in Ukraine from rest-of-world operations by opening of business Monday, February 14, 2022.
4. Review cybersecurity posture across the organization, and where possible, tune controls to stricter settings. Similarly, reduce thresholds for investigation of anomalous or suspicious activity.
5. Verify critical systems are patched from known exploited vulnerabilities (see the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerability catalog here).
6. Confirm critical systems and data are backed up, stored offline, and tested to ensure recoverability.
7. Report any incidents or suspicious activity to CISA (central@cisa.gov) or to your local FBI office.

Risk Environment: Actors and Actions

The buildup of Russian military forces along the border with Ukraine over the past several months have reached[1] a crucial inflection point this week. As of the morning of February 11, western defense officials have reportedly[2] concluded that Russian forces are poised for a renewed, further military incursion into Ukrainian territory to begin as early as next week. A flurry of inconclusive diplomatic engagements from the United States[3] and European Union[4] over the past several weeks leave in doubt the prospects for a peaceful offramp, while several western nations, including the U.S., have begun to minimize their diplomatic footprint and advise their citizens to depart Ukraine.[5] For businesses, the time to take emergency measures to protect your assets—from personnel to physical and digital—is now.

Expected Russian Cyber-Enabled Actions

Judging from Moscow's domestic state-run media[6] and western insights[7], the Kremlin is likely to seize upon any pretext—from genuine to contrived—as the spark for kinetic activity. However, cyber operations appear to already be underway—defacing Ukrainian government websites[8] and disrupting Western European oil and gas transit in Germany[9] and Belgium[10]. Several aspects of Russian state-backed offensive cyber operations should be expected. Lessons from 2007[11], 2008[12], 2014[13], and 2017[14] are useful to guide expectations:

- Attacks aimed at confusing and demoralizing the Ukrainian public, discrediting the Ukrainian government, and sowing uncertainty within Ukrainian markets—including DDOS, website defacements, and social media campaigns.
- Operations aimed at crippling critical infrastructure such as telecommunications, internet connectivity, and energy transmission.
- Espionage intrusions aimed at both prepositioning for later disruption, as well as ascertaining Ukrainian, NATO, and U.S. plans and intentions.
- Exploitations in retaliation for likely sanctions and export curbs prepared by the U.S., EU, and NATO member-states.

[1] IN11806 (congress.gov) Russian Military Buildup Along the Ukrainian Border
[2] Nick Schifrin on Twitter: "NEW: The US believes Russian President Vladimir Putin has decided to invade Ukraine, and has communicated that decision to the Russian military, three Western and defense officials tell me." / Twitter
[3] FACT SHEET: U.S. Diplomatic Engagement with European Allies and Partners Ahead of Talks with Russia | The White House
[4] EU diplomatic outreach in the context of security challenges by Russia - European External Action Service (europa.eu)
[5] Ukraine Travel Advisory (state.gov)
[6] The Armed Forces of Ukraine began a massive shelling of Donetsk - MK
[7] First on CNN: US intelligence indicates Russia preparing operation to justify invasion of Ukraine - CNNPolitics
[8] Brief on Russia/Ukraine Cyber Conflict: CVE-2021-32648, WhisperGate (paloaltonetworks.com)
[9] Explainer: How a German 'climate' fund set out to help Russia dodge U.S. sanctions | Reuters
[10] European Oil Port Terminals Hit By Cyberattack | Barron's (barrons.com)
[11] Estonian denial of service incident https://www.cfr.org/cyber-operations/estonian-denial-service-incident
[12] Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace (justsecurity.org)
[13] Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict (usf.edu)
[14] Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes - The Washington Post

Known Russian Cyber Capabilities

While factoring for the wide array of unknowns in this scenario, precautionary measures should be guided by key assumptions:

- Russian state-sponsored actors use cyber capabilities across the spectrum of conflict—they can precede, support, or serve as an offramp to conventional warfare. This means that, irrespective of political or conventional military developments, **the risk from these operations is likely to remain elevated through the next year or more**.

- Prior Russian aggression, in both cyberspace and through kinetic military action, in Eastern Europe and Western Asia have had cascading effects outside the technical domain, disrupting business operations and supply chains globally. Companies with a presence anywhere in Eastern Europe **should plan for technical and business disruptions stemming directly from Russian state-backed cyber operations**. Cyber offensives and counter-offensives between state-backed actors in this crisis—from military to intelligence to law enforcement—will also almost certainly leverage and impact private interests.

- Russian state-backed cyber actors like the GRU[15], SVR[16], and FSB—known by industry monikers like Sandworm, APT29, and BerserkBear, respectively—are **highly sophisticated, determined, and likely to succeed in some measure against their targets**. Even so, the malware and exploits they may deploy against discrete targets **could spiral out of their operational control**, with potentially devastating, unintended consequences. This was the case in 2017 with the NotPetya infection—widely attributed to the GRU—costing up to tens of billions in damages and temporarily crippling global supply lines.

- Against this backdrop, recent crackdowns[17] by Russian authorities against Russia-based ransomware actors and cybercriminals hint at Russia finally cooperating with western governments to reduce the amount of uncontrolled criminal cyber activity. While this could be indicative of a newfound cooperative approach in Moscow, it may also reflect an effort to **consolidate state-level control of deniable ransomware** that could be used as leverage against Ukraine and its western supporters.

[15] https://attack.mitre.org/groups/G0007/

[16] https://attack.mitre.org/groups/G0016/

[17] https://www.wsj.com/articles/what-the-russian-crackdown-on-revil-means-for-ransomware-11642188675

Recommendations: Next Steps for Risk Managers

The immediacy and intensity of the risks described above require responsible organizations to respond with a level of aggressiveness well outside of business-as-usual.

Corporate Risk Management and Partnership

- **Align Goals and Plans from Top to Bottom** – Communicate calmly but urgently the mitigation steps that must be taken immediately across the organization.
  - Schedule emergency meetings of audit or risk committees for briefings on current risk assessments and planning by senior management.
  - Reassure the employee base that the executive team is actively responding to potential risks. Underscore that the priority will be to prevent against urgent risks, including potential loss of life or human suffering.
  - Prepare business unit leads for full cooperation with the emergency actions taken by their CISO and CIO, even if they cause short-term business disruption.
  - Activate security teams to full readiness and align on a plan of action that considers the potential responses outlined below.
- **Activate Crisis Cell –** Activate the corporate emergency response function and convene an executive emergency committee immediately.
  - Prepare an executive-level briefing leveraging information from government and industry partners, and internal resources.
  - Schedule daily, regular meetings with incident response lead(s) and emergency executive committee throughout the weekend.
  - Establish a situation report cadence with leadership and board members.
- **Activate Business Continuity/ Disaster Recovery Plans** – Activate business continuity and disaster recovery plans immediately to reduce the operational impact in case of military conflict.
  - Ensure plans anticipate the loss of important utilities and infrastructure, including internet connectivity.
  - Plan for disruption to staff, data-hosting, product development, equipment, HR, service providers, and financial transactions.
- **Review supplier and customer dependencies –** Identify all customer and supplier dependencies, especially key relationships with critical infrastructure and government.
  - Activate mitigation measures to enable global operational continuity and security in the case of trade restrictions or disruption to telecommunications.
- **Communicate with Stakeholders in Government and Industry –** Review existing memoranda of understanding and information sharing pathways with the appropriate industry, private, and public sector information sharing partners.
  - Establish connection points to specific Information Sharing and Analysis Centers (ISACs) and government partners, e.g., CISA, ENISA, NCSC, others.

  - Identify internal points of contact for routine information sharing versus reporting critical events.

- **Pre-Position Assets to Support Potentially Targeted Customers –** Identify high-risk, critical infrastructure customers in the affected region to:
  - Ensure outbound and inbound contact information is up to date and that internal points-of-contact are properly briefed on communication and escalation procedures.
  - Prepare the necessary people and assets to support an incident response or recovery operation.
  - Minimize external dependencies for support activities by pre-downloading required documentation and software packages, applying important updates to corporate systems, and charging battery packs.

- **Prepare for Long-term Economic Restrictions in the Region** – Military action will likely portend long-term increases in economic & trade restrictions in the region. Begin assessing the impact of sanctions and trade restrictions on operations to maintain operational agility in the case of market or operational losses.

Staff Protection

- **Establish Contact -** Organizations should plan to establish contact with, and ensure support for, those who will shelter-in-place during the likely conflict. Protection should extend to ex-pats and citizens directly at risk in Ukraine and to non-citizens living in or visiting Belarus and Russia. These groups will likely be cut off from commercial travel. Visible executives may be used as leverage in a combined physical/cyber conflict.

- **Address Immediate Physical Threat –** Activate any existing incident response plans for employees in the conflict region as soon as possible[18]. As hostilities commence, commercial air travel is likely to cease. Already, flights from Kyiv have become rare and expensive. Companies should plan for a best-case scenario of evacuating families via commercial options where possible.

Proactive Technical Risk Mitigation

- **Reduce the Attack Surface -** Reduce internet exposure of all services, applications, and assets in Eastern Europe and Central Asia. Pay special attention to assets that are connected to internal corporate networks. Lock down sensitive ports and protocols, such as RDP, to make initial compromise more difficult.

- **Segment Networks** – Limit network access to and from states in Eastern Europe and Central Asia where Russia maintains significant influence and technical capacity, including Belarus, Kazakhstan, and Ukraine itself. This should include client VPNs, site-to-site VPNs, and WAN links.

[18] State Department Statement on Citizens in Ukraine

- Layer-3 access to production services outside of these countries should be extremely curtailed or eliminated, to reduce the risk of both automated and manual malicious movement across the network.
- Communications with employees should be maintained with cloud services accessed over the public internet.
- Any management software required to maintain critical services, networks or systems in region should be deployed physically into the region as soon as possible. This deployment will ensure team members can access this software in the event internet or WAN access is limited.

- **Review and Reduce Insider Access** – Review administrative and privileged access accounts in affected regions. Remove and temporarily limit administrative access for non-critical users located in those regions. Conduct an access review for members in mission-critical environments and, where possible, remove local administrative access for these populations. Consider limiting access to both self-hosted and cloud-based line-of-business systems and critical intellectual property.
- **Perform Controlled Shutdowns** – Begin graceful shutdowns of non-critical systems and services in impacted regions. Focus especially on systems hosting sensitive customer and employee data, which should be backed up and then wiped before shutdown.
- **Manage Third-Party and Supply Chain Dependencies** – Prepare for the potential disruption of goods and services currently provided by these regions.
    - Review critical suppliers and third parties with access to sensitive assets to understand their presence and exposure within these regions and identify alternate suppliers.
    - Restrict or closely monitor access for service providers with exposure within the region. Securely transfer critical digital assets hosted by third parties in the impacted region to alternate providers.

Incident Response and Threat Hunting

- **Implement Incident Response Plan** – Prepare for impending action.
    - Brief all incident response stakeholders on the emerging crisis and review response plans, policies and procedures, as well as roles and responsibilities.
    - Designate a primary and secondary incident commander responsible for guiding an incident to closure.
    - As soon as practicable, exercise the incident response plan, focusing on executing key activities and maintaining operational coordination. The incident response plan must include potential impact to OT environments with thresholds for required shutdowns.
    - Begin regular status meetings this weekend to discuss preparations and to keep all teams aligned on the short- and medium-term response plans.

- **Increase Detection Capabilities –** Enterprises without the ability to search for rogue processes across their server and workstation fleet, to isolate all network traffic per region, or to perform remote forensics on their far-flung employee base will not be able to react quickly enough to intrusions by Russian state actors. Crash deployments of EDR agents and rushed projects to direct logging to cloud SIEM providers are warranted, even if they pose some risk of helpdesk or operational impact.
- **Shift Teams Towards Threat Hunting** – Orient qualified security resources towards proactively hunting for persistent threats in your corporate network(s). Criminal and nation-state threat actors routinely wait weeks or months after achieving initial access before acting towards their objective. Cyberattacks that coincide with the regional instability are likely to leverage access that has already been achieved, so a focus on persistent mechanisms and command-and-control channels is advised.
- **Review/reduce dependencies between OT and IT environments** – There is currently an increasing pattern of utilizing vulnerabilities in the IT environment, such as insecure credentials or phishing campaigns, to gain access to the OT environment. This pattern was observed most recently with Ryuk ransomware attacks[19] and Colonial Pipeline[20]. The attacks stemmed from insufficient separation between IT and OT networks.
  - Review and document dependencies between the OT and IT environment.
  - Review potential areas where dependencies may have been overlooked, such as shared OT/IT data aggregation.
  - Prioritize dependencies by criticality to eliminate non-critical dependencies and increase segmentation.

Additional Resources

UK NCSC Guidance: Actions to Take When the Cyber Threat is Heightened

CISA/NSA/FBI Joint Cybersecurity Advisory: Understanding Mitigating Russian Cyber Threats to U.S. Critical Infrastructure

Mandiant Proactive Preparation and Hardening against Destructive Attacks

Microsoft: Destructive Malware Targeting Ukrainian Organizations

About Krebs Stamos Group

Krebs Stamos Group drives progress toward a better, safer, and more secure technological future. We use our expertise in technology and geopolitics to deliver insights into an increasingly complicated technology risk landscape, and to help clients develop strategies to address technology-centric safety and security challenges.

[19] Ryuk Ransomware Hit Multiple Oil & Gas Facilities, ICS Security Expert Says (darkreading.com)
[20] Hacking regrets: The Colonial Pipeline and lessons to be learned. (The Hill)