NISOS
Webinar Brief

Threats to Retail Sector and Update on Russia/Ukraine Conflict

Main Takeaways

Russia is not likely to use a sophisticated cyber weapon through state-sponsored efforts (GRU, SVR, and FSB) to cause mass disruption. Instead, they are likely to target businesses that leave Russia through the proxy use of cybercriminal gangs via ransomware and denial of service attacks. Organizations must use threat intelligence to prioritize defense strategies in disinformation, identity and access management, insider threat, training and awareness, adversary simulation, and denial of service protection.

Russia and Ukraine Predictions

Any multinational company likely has equities in Russia or Ukraine. Threat intelligence has been more important than ever to inform the proper risk posture and response. Intelligence informs not only through defense strategy from cyber attacks, but from overall business continuity. The top areas of concern over the last month have been:

- **Vendor Response:** Diligence to ensure vendors are following the law with regard to sanctions and business connections in Russia.

- **Insider Threat:** A lot of Russia and Ukraine-based individuals are exposed to western thought and have access to large enterprise networks. They may have a negative sentiment towards the United States, and the Russian government may attempt to recruit these individuals because of this. Intelligence, investigations, and response to each of these problem areas need a different solution.

- **Direct Threat in the Cyberwar Landscape:** While Russia has been soft on the response toward western enterprise, security leaders and board members are on edge for what could happen next. Cybercrime organizations like Conti want to come after large firms with their support to the West and Russian state-sponsored APT efforts may be more aggressive from a theft and disruption perspective. Regardless, it's believed that Russia

won't use sophisticated tools like Solarwinds exploits to cause mass disruption due to the long research and development efforts needed for those tools.

However, if Russian state sponsors or crime affiliates gain access to POCs against applications like Not-Petya, they likely would use these tools if backed into a corner in the conflict. Organized cybercrime syndicates may result in lawlessness since jobs are being taken from Russian citizens.

- **Business continuity:** Since Russia has been slow to respond with cyber attacks, businesses are focused on pushing through the supply chain and ensuring products can be delivered without interference from Russia. Roughly 374,000 businesses worldwide rely on Russian suppliers with 90% of these businesses based in the U.S. and roughly 241,000 businesses rely on Ukrainian suppliers with 93% based in the U.S. according to a recent Dunn and Bradstreet study.[1]

  Russia and Ukraine lead the global production of natural gas, utilities, crude oil, industrial metals, and agri-commodities (wheat and grain). While natural gas, utilities, crude oil, industrial metals, and agri-commodities are most important to Russia, we assess Russia will not necessarily limit its targeting of other businesses by industry and thus would target any sector that supports Ukraine in a show of force to combat a growing impression the war is not going well for Russia.

  The use of a wiper malware called HermeticWiper is an example of a disciplined attack with an associated destructive ransomware component used against Ukrainian government institutions the day before the invasion on 24 February. This attack is similar in method to Whispergate, NotPetya, and other operations credited to Russian APT actor Sandworm.[2]

[1]https://www.forbes.com/sites/edwardsegal/2022/03/06/ukraine-crisis-creates-new-strains-on-global-supply-chains/?sh=51ff1ac610af
[2]https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/

Defending Against Cyber Attacks in Geo-Political Sensitive Times

The volume of attacks are increasing and controls are important to protect enterprise. Threat Intelligence is more critical than ever to inform these controls and outcomes. Enterprise must be able to defend against a pro-Ukrainian employee or group as much as a pro-Russian group. Common defense strategies emanating from threat intelligence could include:

- **Continuous Penetration Testing and Threat Intelligence:** Organizations should receive threat intelligence and run constant penetration testing exercises at a similar volume as the attacks are coming.

- **Disinformation:** Reviewing with increased scrutiny how your platform can be used for spreading propaganda.

- **Denial of Service Protection:** Protecting against denial of service attacks is critical.

- **Identity and Access Management:** Enterprises need to have the ability to terminate access to contractors and employees in troubled areas who may pose risk.

- **Training and Awareness:** Human resources and open communications with employees are critical. Enterprises should implement a "see something say something" policy to ensure political opinions do not escalate to violence against the enterprise. It's not as simple as banning and blocking content like Parler and Gab similar to fallouts from the 06 January 2021 Capitol attacks. Employees could be conscripted to military service for example. Therefore any keyword searches using machine learning on alerts need to be placed into context.

About Nisos

Nisos is the Managed Intelligence[SM] company. Our services enable security, intelligence, and trust & safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset delivering smarter defense and more effective response against advanced cyberattacks, disinformation, and abuse of digital platforms. For more information visit: **www.nisos.com**

This briefing is not legal advice and is provided for general informational purposes only.