BRACEWELL

INSIGHTS

Cyber Siren Warning - When State Actors Attack

February 25, 2022

By: ***Seth D. DuCharme***

Russia began a physical invasion of Ukraine Wednesday night, and as the United States responded with sanctions, the threat of cyberattacks against American companies became more acute. Major American businesses – from banks to critical infrastructure companies – are preparing for possible cyberattacks after Russia ***threatened*** "consequences" for nations interfering with its invasion of Ukraine. This follows recent ***warnings*** from United States officials that companies should harden their network defense against potential cyberattacks due to growing tensions with Russia. While cyberattacks are typically financially motivated, recent cyberattacks from Russia and other nation-states are being conducted for a nefarious and political purpose: to disrupt and destroy networks. With the threat of war in Europe looming, companies should review their incident response plans to ensure they are current, realistic, and account for a variety of cyberattacks.

As cyberspace becomes a new battleground for competing powers to confront one another, cyberattacks are less about money and more about wreaking havoc on an adversary's networks. Instead of ransomware, politically motivated hackers, such as those currently ***conducting*** attacks on Ukranian systems, typically use data-wiping malware and distributed denial-of-service ("DDoS") attacks.[1] These types of attacks can be more dangerous than cash-grab ransomware attacks because in many cases, the initially accessed system is not the final target. Instead, the target systems are attacked because they play a role in critical infrastructure, such as airport and power grid management. Russian cyberattacks often include disinformation campaigns which can cause confusion regarding the scope or consequences of an attack. Internet news sources should be scrutinized for reliability, and companies should identify reliable information streams now.

Mandiant, a cybersecurity company that tracks nation-state cyber activity, ***warned*** that although the consequences of cyberattacks can be devastating for companies, the main goal of nation states launching offensive cyber activity is to create worry and uncertainty. The U.S. Cybersecurity and Infrastructure Security Agency echoed this sentiment, ***warning*** Americans that as Russia continues its advances against Ukraine, cyberattacks may lead to collateral supply chain impacts. Because there is little slack in the world's supply chains to absorb disruptions, disruption to the supply chain would certainly fulfill a primary goal of wartime cyberattacks: to cause panic and frustration.

As NATO-aligned countries respond to Russia's invasion of Ukraine and brace for retaliatory cyberattacks, organizations should be assessing supply chain risks, patch management plans, and other cyber hygiene protocols. Companies should ensure all software is up-to-date,

especially ***Log4j vulnerabilities***, and prioritize applying critical patches. Companies should also consider running tabletop exercises to ensure that employees understand the plan and their role, and then test different scenarios to make sure the plan works for different types of cyberattacks. Bracewell attorneys are ready and able to help companies prepare for and respond to cyberattacks of all kinds.

---

1. DDoS attacks render websites unreachable by flooding them with junk data.