Threat Intelligence Advisory

Russian Escalations in Cyberspace

Executive Summary

Following the invasion of Ukraine by the Russian Federation, the risk of cyber-attacks has increased. The Russian Federation has been widely considered to possess mature cyber espionage and offensive cyber operations capabilities. They hold the capability and intent to deliver destructive malware in furtherance of full-spectrum operations in Ukraine.

While most cyberspace operations are expected to be directed at Ukraine, the risk of collateral damage is high. Further, the risk of a response in the cyber domain remains high following the announcement of sanctions against Russian Federation interests and potential additional future responses from the United States and its allies. Organizations in the financial, energy, and public sectors are at especially high risk given Russia's demonstrable actions in past conflicts. However, as this has the potential to unfold in unpredictable ways, all organizations deemed critical infrastructure should remain in a heightened state of readiness.

There is an increased risk of opportunistic attacks carried out by unaffiliated malign cyber actors using the conflict for financial gain. It is important to note, however, that these actors will employ more familiar tactics such as ransomware and business email compromise (BEC). While there is no current indication or threat of attack, the situation remains fluid as the situation develops.

Analysis

The Russian Federation has developed significant capability in the cyber domain, which has steadily evolved from Distributed Denial of Service (DDoS) attacks in 2007, to the use of destructive malware targeting Ukrainian energy infrastructure as early as 2015. The attack against Ukrainian energy infrastructure in 2017 is particularly noteworthy due to the fact that while the malware itself was destructive in nature, the attack was designed to disrupt and ultimately cripple Ukraine's energy infrastructure.

As previously mentioned, Russia is capable of developing sophisticated malware, and as such special attention should be paid to avoid a singular focus on signature based detection. It is unlikely that Russia

will redeploy compromised toolsets and the use of new Zero-Day exploits is expected to rise in the coming weeks.

Monitoring of the Dark Web largely suggests that the bulk of activities are directed inward toward Ukraine with a specific focus on government infrastructure. However, our analysis also revealed alleged capability and access to deliver effects against organizations in the energy, agricultural, and financial sectors. This is largely consistent with Russian offensive military operations in the past.

It is the assessment of the Verizon Threat Research Advisory Center (VTRAC) that an in-kind response from the Russian Federation should be expected, resulting from worldwide punitive response. Further, those organizations aligned with Critical Infrastructure and Key Resources (CIKR) are at an especially high risk. Separately, there is also elevated risk of opportunistic attacks against small and medium sized businesses as a means to cause marked impact to the economy.

VTRAC is closely monitoring the military conflict in Ukraine and will continue to follow any cyber related impacts that may affect our customers globally. Customers of Verizon cybersecurity services are reminded that they may engage Verizon's security consulting services to conduct a detailed assessment of their networks and systems. This due-diligence review will help to identify and mitigate possible malicious activities affecting critical services that can result in data loss and degradation of system integrity. For more information or further assistance, please contact your Verizon Account Representative. Rapid Response Retainer customers are encouraged to contact their dedicated Investigative Liaison for any questions or support.

Recommendations

Nation-State Cyber Actors often deploy capabilities months or even years prior to exploitation and/or attack, therefore it is highly-likely that any capabilities would have been staged at some unknown point in the past. With that in mind, we suggest that organizations consider some or all of the below actions.

- Conduct proactive threat hunting starting against business critical assets and ensure that proper backups of the same are taken and kept for an extended period of time. This should be followed-up with hunting against systems capable of interacting with those business critical assets. Next, work outward from the assets most critical to business continuity to those with external access. Hunting activity should be focused more on identification of employed TTPs rather than a singular focus on signature based detection.

- Revisit Incident Response (IR) capabilities and actions to be taken upon positive identification of a possible incident. This includes reviewing play/run books and existing policy, with special emphasis on determining scope, remediation, and recovery. Nation-State actors possess exceptionally sophisticated persistence mechanisms, which can make incident handling especially tricky if not properly prepared.

- Review Acceptable Use Policies and consider re-evaluating short term social media and non-business email usage for a limited time. Though, at the very least, organizations should ensure that externally sent emails are marked in several conspicuous areas to alert the user to the potential risk.

- To further mitigate the risk of opportunistic exploitation, we recommend that phishing and social engineering drills be performed at a heightened level. Additionally, we strongly recommend that end-users understand how and what to report and why.

- Revisit rules and/or signatures for any detection and prevention platforms. We recommend, where possible, consider alerting and/or blocking known commercial Virtual Private Network (VPN), Proxy, and Tor exit nodes to prevent anonymized attacks from known infrastructure.

- For those organizations with Industrial Control Systems (ICS) /Supervisory Control and Data Acquisition (SCADA), and Programmable Logic Controller (PLC), review safety checks and controls in the event of an incident.

- You may also consider reaching Verizon's Rapid Response Retainer (RRR) group to assist with any forensic investigation within your networks..

Recommended Reading and Resources

- We recommend reviewing the alert published by the US Cybersecurity and Infrastructure Security Agency (CISA) advisory AA22-011A (*Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure). Available at the link below --*

  https://www.cisa.gov/uscert/ncas/alerts/aa22-011a

- For those organizations with ICS, SCADA, and PLC related infrastructure, we recommend reviewing the MITRE ATT&CK® framework for industrial control systems. Available at the link below.

  https://collaborate.mitre.org/attackics/index.php/Main_Page