January 29, 2022

Russia possibly preparing cyber countermeasures if challenged in Ukraine.

Reports and discussions in forums reveal that Russia is potentially planning a cyber-attack on the U.S. to limit the American response in case of a Russian invasion of Ukraine. A DHS memo last Sunday warned that Russia is set to target U.S. national infrastructure via Cyber-attacks to cripple a probable U.S. response in the event of a Russian invasion of Ukraine. Private cyber industry firms are on the alert for possible Russian hacking activity. Russian hacktivist groups have spent years targeting and gaining access to critical infrastructure in the United States. For example, in one campaign back in 2016, Russian hackers compromised U.S. Energy networks, conducting reconnaissance and collecting the information needed to gain control of the systems if they wanted to.

CISA, through the Joint Cyber Defense Collaboration, identified that Russian state-sponsored hacking groups already established long-term persistence in various U.S. systems, allowing them to execute numerous cyberattacks such as DDoS, Ransomware, Malware delivery, Espionage, and other types of cyber-attacks. For example, in May 2021, the colonial pipeline ransomware attacks credited to Russian state-sponsored hacking groups led to gas shortages in all of the east coast of the U.S., signifying Russian capabilities to root harm to the U.S. homeland without a single soldier. In 2020, the SolarWinds breach, another campaign led by Russian hackers, exhibited the capacity to penetrate over ten U.S. government agencies and fifty Fortune 500 companies.

U.S. agencies and companies are vigilant through CISA Joint Cyber defense collaboration. They will continue to monitor suspicious activity that could indicate a real cyber threat to the U.S. homeland if the U.S. decides to act with its NATO partners to counter a possible Russian invasion of Ukraine. In that case, Russian retaliation via cyber operations is expected to directly impact the critical infrastructure of the U.S. and NATO allies.

Sources:

Johnson, B. (2022, January 28). *DHS intelligence brief warns of potential Russian cyber-retaliation against U.S. critical infrastructure - H.S. Today*. Hstoday. Retrieved January 30, 2022, from https://www.hstoday.us/federal-pages/dhs/dhs-intelligence-brief-warns-of-potential-russian-cyber-retaliation-against-critical-infrastructure/

*DHS is a U.S. government organization

Vladimir Isachenkov, T. A. P. (2022, January 27). *Russia threatens retaliation if Ukraine's demands not met*. Defense News. Retrieved January 30, 2022, from https://www.defensenews.com/flashpoints/2022/01/26/russia-threatens-retaliation-if-ukraine-demands-not-met/

*non-bias U.S. Military and defense news outlet

Morgan, R. (2022, January 25). *Russia could cyberattack us to distract from Ukraine invasion, DHS warns*. American Military News. Retrieved January 30, 2022, from https://americanmilitarynews.com/2022/01/russia-could-cyberattack-us-to-distract-from-ukraine-invasion-dhs-warns/

*non-bias military news outlet

Meyer, J. (2022, January 25). *Homeland Security warns that Russia could launch cyberattack against U.S*. USA Today. Retrieved January 30, 2022, from https://www.usatoday.com/story/news/2022/01/24/homeland-security-russia-cyberattack-us/9202949002/

*USA today is a politically left-leaning news outlet