Potential for Imminent Russian Cyber-attacks Against SLTTs

January 2022 • SFAR-2022-1
TLP: AMBER – Distribute within your organization and with vetted partners.
Purpose of document – Educational for executive and technical staff.

Executive Summary

The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) Cyber Threat Intelligence Team and Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) assess with high confidence that SLTTs, election offices, and critical infrastructure are at a significantly heightened risk from cyber-attacks if Russian aggression against Ukraine persists and elicits a U.S. response. U.S. President Joseph R. Biden publicly stated that if Russia invades Ukraine, there would be a "swift, severe, and united response" from the United States.[1] Possible responses discussed publicly include economic sanctions targeting specific sectors of the Russian economy/government and suggestions of reactive cyber operations.[2] These actions would increase the risk of cyber-attacks against SLTTs, elections infrastructure, and critical infrastructure. SLTTs should continue to monitor the situation and follow the recommendations at the end of this report.

Substantive Analysis

U.S. actions taken to punish Russia for renewed incursions into Ukraine will likely lead to a response from Russia. Retaliatory offensive cyber operations represent options Russia would pursue, as stated by Russian President Vladimir Putin in December 2021.[3] In this scenario, SLTTs likely would see an increase in cyber-attacks that aim to disrupt operations or destroy systems. It is also possible that Russian cyber-attacks against Ukraine, as part of a larger operation, could quickly spread beyond Ukraine's borders and impact entities around the globe.

The level of possible offensive cyber operations against SLTTs would be driven by the severity of U.S. responses enacted. Possible avenues for a Russian response include increased Russian cybercriminal activity, nation-state activity, or both. Previous Russian-orchestrated cyber campaigns involved the use of destructive malware, and the widespread use of dis/misinformation.

Russian Destructive Malware

Russia deployed various destructive malware campaigns in the past, such as ransomware from Russian cybercriminal groups; nation-state malware, such as NotPetya; and a current Master Boot Record (MBR) wiper malware campaign. The 2017 NotPetya deployment against Ukraine represents a relevant example. NotPetya quickly spread globally, in part due to leaked National Security Agency (NSA) exploits like EternalBlue crippling entities, such as global shipping company Maersk.[4]

More recently, on January 13, 2021, Microsoft Threat Intelligence Center (MSTIC) identified a (MBR) wiper malware campaign named WhisperGate, which spans multiple government, non-profit, and information technology organizations, all based in Ukraine.[5] This malware disguises itself as ransomware, leaving a fake ransom note while actually wiping data from the infected system.

Russian Cybercriminal Activity

Reports detailing the Russian government leveraging cybercriminal entities dates back to the late 90s when the FSB (Federal'naya Sluzhba Bezopasnosti), Russia's domestic intelligence and security service, coerced cybercriminals to act as internal proxies to deface pro-Chechen websites.[6] More recently, commodity malware and

cybercriminal groups have emerged, such as Dridex operated by a group known as Evil Corp. A growing body of evidence showcases some cybercriminals can also serve as an extension of Russian state interests on occasion, making it more unlikely that these specific individuals will face justice in Western courts unless they travel to a country willing to arrest and extradite them, such as Alla Witte in 2021[7]or Dridex administrator Andrei Ghinkul in 2014.[8&9] When Russia is confronted about harboring cybercriminals within its borders, Russian officials often exercise plausible deniability and deflect blame citing the West's role in enabling cybercrime.[10]

In January 2022, the FSB stated it dismantled ransomware criminal group REvil at the request of the U.S. This is in response to the Colonial Pipeline cyber-attack in May 2020. [11] It is likely that Russia will use this sudden cooperation as a bargaining tool during U.S.-Russian diplomatic responses to Ukraine, as the arrest took place shortly after Russia began amassing military equipment and personnel along the Ukrainian border. Cybercriminals will likely hesitate to conduct any operations of their own unless Russia moves forward with an invasion, capitalizing on the uncertainty of the situation with phishing lures associated with the activity.

Russian Disinformation Campaigns

Russian mis/disinformation campaigns were well documented during the 2016 U.S. Presidential election.[12]These campaigns leveraged social media to push false information, cast doubt on legitimate information, and inflame tensions. It is likely that any Russian incursions into Ukraine would employ disinformation campaigns in an attempt to shift narratives. There is evidence that Russia already launched disinformation campaigns, with the United States announcing on January 20th, that it was sanctioning four individuals in Ukraine for spreading Russian disinformation.[13]

Analytic Confidence

Analytic confidence in this assessment is moderate. Source reliability is high with minimal conflict among sources. The analysts used circleboarding and multiple scenarios generation techniques in this analysis.

For questions or comments, please contact us at intel@cisecurity.org.

Recommendations

Take the following actions to prepare for a potential increase in cyber-attacks.

- Implement the CIS Critical Security Controls to harden environments and maximize protection.
- Review and implement the CISA Insight on implementing cybersecurity measures now to protect against potential critical threats.
- For further recommendations on protecting against destructive malware review Mandiant's white paper on Proactive Preparation and Hardening to Protect Against Destructive Attacks.
- Develop an emergency response plan and be prepared to communicate what actions you are taking in the event of a cyber-attack.
- Exercise caution when sharing information found online. If you identify misinformation about your office/organization please send it to misinformation@cisecurity.org.
- Continue to monitor for confirmed information from the MS/EI-ISAC and CISA.

References

1. https://apnews.com/article/antony-blinken-jen-psaki-vladimir-putin-sergey-lavrov-congress-1df536e9a832830dc3bae2e89aef4116
2. https://www.nytimes.com/2022/01/08/us/politics/us-sanctions-russia-ukraine.html
3. https://www.cbsnews.com/news/russia-ukraine-war-news-putin-retaliatory-military-technical-measures/
4. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
5. https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
6. https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499
7. https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization
8. https://www.post-gazette.com/news/crime-courts/2018/12/06/Moldova-Andrey-Ghinkul-Smilex-sentenced-time-served-Bugat-malware-case-deported-Pittsburgh/stories/201812060131
9. https://www.justice.gov/usao-wdpa/pr/moldovan-sentenced-distributing-multifunction-malware-package
10. https://www.reuters.com/technology/murkiness-russias-ransomware-role-complicates-biden-summit-mission-2021-06-14/
11. https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/
12. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
13. https://www.reuters.com/world/europe/us-imposes-sanctions-four-ukraine-it-says-spread-disinformation-russia-2022-01-20/

MS-ISAC®
EI-ISAC®

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

TLP: AMBER

Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
https://www.cisa.gov/tlp