



## CROSS-SECTOR

20 February 2022

LIR 220220002

### Threat of Russian Advanced Persistent Threat Cyber Activities While Tensions with Russia are Heightened

*References in this LIR to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the FBI.*

The FBI Cyber Division, in coordination with the FBI's Office of Private Sector (OPS), prepared this LIR to inform the private sector about the threat of Russian state-sponsored advanced persistent threat (APT) cyber activities, while tensions with Russia are heightened. The FBI is engaging in efforts to support the U.S. response and to secure the Homeland from any Russian actions; historically, Russian state-sponsored APT cyber activities increase when tensions are high with Russia. This LIR should be read in conjunction with Joint Cyber Security Advisory, AA21-350B, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, as well as DHS, Intelligence in Brief, DHS-IA-IB-2022-01498, *Russian Online Malign Influence Increasing in Response to Ukraine Crisis*.





- Russian APT actors have used spear phishing and brute force cyber network attacks (CNA), while exploiting known vulnerabilities against accounts and networks with weak security. Russian APT actors have targeted a variety of U.S. and international critical infrastructure, including entities in the Defense Industrial Base, Healthcare and Public Health, Energy, Telecommunications, and Government Facilities Sectors. Finally, Russian malign influence actors have and continue to use social media accounts, overt and covert media connections, and message amplification to articulate narratives designed to exclude or isolate groups from one another.
  - Russian APT actors targeted and successfully compromised state, local, tribal, and territorial (SLTT) governments and aviation networks, September 2020 through at least December 2020.
  - Russian-tied APT actors, using specifically crafted spear phishing emails, target current and former USG-affiliated individuals through personal email accounts. The emails contain a malicious link that directs to a website that prompts the reader to enter their login credentials.

Due to the increased threat of Russian military action, the security situation in Ukraine could deteriorate with little notice. The United States, along with its Allies and partners, has underscored its readiness to impose significant costs on Russia if it takes further military action against Ukraine, potentially further increasing the volume/severity of Russian APT cyber activities.

OPS's Information Sharing and Analysis Unit disseminated this LIR; please direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: <https://www.fbi.gov/contact-us/field-offices>.



**Traffic Light Protocol (TLP) Definitions**

Color	When should it be used?	How may it be shared?
<p><b>TLP:RED</b></p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p><b>TLP:AMBER</b></p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>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. <b>Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</b></p>
<p><b>TLP:GREEN</b></p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p><b>TLP:WHITE</b></p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>