Articles + Publications | May 16, 2022

Russian Threats and the Need to Protect Critical Infrastructure

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox

U.S. authorities have increased warnings of threats to critical infrastructure from Russian sources and have laid the groundwork for 72-hour reporting requirements for critical infrastructure organizations. At the end of April 2022, the Cybersecurity and Infrastructure Security Agency ("CISA") released a summary of Russian cyber threats. Both at the outset of Russia's "special military operation" in Ukraine and as the war has continued, many observers worried about a retaliatory wave of Russian cyberattacks against U.S. critical infrastructure in response to U.S. sanctions against Russia, prominent Russians, and U.S. direct aid to Ukraine.

Despite these fears, the widespread disruption to the U.S. economy from Russian attackers has not yet materialized. Russian capabilities to execute widespread cyberattacks may have been overestimated, much like the overestimation of Russian military power, which was revealed by its underperformance on the ground in Ukraine. Even so, the recent summary released by CISA, supported by surrounding events and impending regulations, paints a broad picture of the risks to critical infrastructure in the current environment. This is the time to recommit to your organization's security hygiene.

Regulations for Critical Infrastructure

Even though the reported threats of widespread and coordinated cyberattacks have not yet materialized, critical infrastructure faces serious risk. Recognizing the long list of potential threats, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (as Division Y of the Consolidated Appropriations Act of 2022), which President Biden signed on March 15, 2022. This new law will impose 72-hour reporting requirements following certain cybersecurity incidents for organizations defined as "critical infrastructure" under Presidential Policy Directive 21. Critical infrastructure is defined as the following sectors, with the following sector-specific agencies:

- Chemical:
  Sector-Specific Agency: Department of Homeland Security
- Commercial Facilities:
  Sector-Specific Agency: Department of Homeland Security
- Communications:
  Sector-Specific Agency: Department of Homeland Security
- Critical Manufacturing: Sector-Specific Agency: Department of Homeland Security
- Dams:
  Sector-Specific Agency: Department of Homeland Security

- Defense Industrial Base:
  Sector-Specific Agency: Department of Defense
- Emergency Services:
  Sector-Specific Agency: Department of Homeland Security
- Energy:
  Sector-Specific Agency: Department of Energy
- Financial Services:
  Sector-Specific Agency: Department of the Treasury
- Food and Agriculture:
  Co-Sector-Specific Agencies: U.S. Department of Agriculture and Department of Health and Human Services
- Government Facilities:
  Co-Sector-Specific Agencies: Department of Homeland Security and General Services Administration
- Healthcare and Public Health:
  Sector-Specific Agency: Department of Health and Human Services
- Information Technology:
  Sector-Specific Agency: Department of Homeland Security
- Nuclear Reactors, Materials, and Waste:
  Sector-Specific Agency: Department of Homeland Security
- Transportation Systems:
  Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation; and
- Water and Wastewater Systems:
  Sector-Specific Agency: Environmental Protection Agency.

The details of these reporting requirements and the specific effective date of any requirements will not materialize for some time. CISA has 24 months to propose regulations (in consultation with the sector-specific agencies identified above), and then another 18 months to adopt final regulations before any requirements become effective. The key take away is that all categories of critical infrastructure will soon be responsible for reporting certain cyber incidents, specifically including ransomware attacks, within 72 hours and to provide detailed information to assist CISA in tracking and combatting these threats.

The Threats

Critical infrastructure faces two categories of threats: state actors and private groups. CISA identified the key threats coming from the following Russian state actors:

- The Russian Federal Security Service (FSB), including FSB’s Center 16 and Center 18
- Russian Foreign Intelligence Service (SVR)
- Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS)
- GRU’s Main Center for Special Technologies (GTsST)
- Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)

On the private side, Russia reportedly permits and tacitly supports an army of private hacking groups. These private Russian groups typically focus on extortion through the deployment of ransomware, which now almost always includes data theft and a threat to publicize. For example, Conti (reportedly the top ransomware group of

2021) faced a widely publicized leak of internal communications earlier this year. These leaks paint a picture of a relatively “professional” organization, operating like a business.

Securing Your Organization

In the face of the escalating threats by sophisticated and well-funded threat actors, those responsible for security at critical infrastructure organizations can feel overwhelmed. With limited security resources, organizations are well-advised to assess likely risks and threats, and prioritize vulnerabilities, and re-focus on the basics. The CISA provides helpful tools for risk assessments. Given the current environment, private organizations are typically focused on preventing and responding to ransomware. In view of government warnings, and the expectation of attacks on critical infrastructure organizations, security teams should use the results of an updated risk assessment to review their information security program. Focus first on securing access: enhance awareness training, implement or enhance multi-factor authentication, and consider restricting access from other than whitelisted devices if feasible. Patch management should also be revisited, and reported vulnerabilities should be patched. Vendor management has never been more important, as many recent compromises have originated with vendor access.

Attacks from motivated and well-resourced state-actors are difficult to defend, but the concepts and approaches for cybersecurity are the same. Updating risk assessments, establishing priorities, and methodically approaching needed cybersecurity enhancements, is the best approach to maintaining security in an unprecedented threat environment.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber