THREAT BULLETINS

Joint Cybersecurity Advisory – Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

TLP:WHITE

Apr 20, 2022

On April 20, 2022, the cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom released a joint Cybersecurity Advisory (CSA) (AA22-110A). The purpose of the release of this alert is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity is aligned with the potential for anticipated retaliation due to the unprecedented economic costs imposed on Russia as well as material support provided by the United States and US allies and partners.

Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks including distributed denial-of-service and deployment of destructive malware against critical infrastructure organizations.

All members are encouraged to review AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.

Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and operational technology (OT) networks; and disrupt critical industrial control systems (ICS)/OT functions by deploying destructive malware.

Historical operations have included deployment of destructive malware including BlackEnergy and NotPetya—against Ukrainian government and critical infrastructure organizations. Recent Russian state-sponsored cyber operations have included DDoS attacks against Ukrainian organizations.

Note: for more information on Russian state-sponsored cyber activity, including known TTPs, see joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.

Cyber threat actors from the following Russian government and military organizations have conducted malicious cyber operations against IT and/or OT networks:

- 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)

For additional details including previously observed malicious cyber operations of the aforementioned Russian state-sponsored groups, please see the full alert here.

Russian-Aligned Cyber Threat Groups

In addition to the APT groups identified in the Russian State-Sponsored Cyber Operations section, industry reporting identifies two intrusion sets—PRIMITIVE BEAR and VENOMOUS BEAR—as state-sponsored APT groups, but U.S., Australian, Canadian, New Zealand, and UK cyber authorities have not attributed these groups to the Russian government.

- **PRIMITIVE BEAR** has, according to industry reporting, targeted Ukrainian organizations since at least 2013. This activity includes targeting Ukrainian government, military, and law enforcement entities using high-volume spearphishing campaigns to deliver its custom malware. According to industry reporting, PRIMITIVE BEAR conducted multiple cyber operations targeting Ukrainian organizations in the lead up to Russia's invasion.

- **VENOMOUS BEAR** has, according to industry reporting, historically targeted governments aligned with the North Atlantic Treaty Organization (NATO), defense contractors, and other organizations of intelligence value. Venomous Bear is known for its unique use of hijacked satellite internet connections for command and control (C2). It is also known for the hijacking of other non-Russian state-sponsored APT actor infrastructure. VENOMOUS BEAR has also historically leveraged compromised infrastructure and maintained an arsenal of custom-developed sophisticated malware families, which is extremely complex and interoperable with variants developed over time. VENOMOUS BEAR has developed tools for multiple platforms, including Windows, Mac, and Linux.

Russian-Aligned Cybercrime Groups

Cybercrime groups are typically financially motivated cyber actors that seek to exploit human or security vulnerabilities to enable direct theft of money (e.g., by obtaining bank login information) or by extorting money from victims. These groups pose consistent threats to critical infrastructure organizations globally. Since Russia's invasion of Ukraine in February 2022, some cybercrime groups have independently publicly pledged support for the Russian government or the Russian people and/or threatened to conduct cyber operations to retaliate against perceived attacks against Russia or materiel support for Ukraine. These Russian-aligned cybercrime groups likely pose a threat to critical infrastructure organizations primarily through:

- Deploying ransomware through which cyber actors remove victim access to data (usually via encryption), potentially causing significant disruption to operations.
- Conducting DDoS attacks against websites.
    - In a DDoS attack, the cyber actor generates enough requests to flood and overload the target page and stop it from responding.
    - DDoS attacks are often accompanied by extortion.
    - According to industry reporting, some cybercrime groups have recently carried out DDoS attacks against Ukrainian defense organizations, and one group claimed credit for DDoS attack against a U.S. airport the actors perceived as supporting Ukraine (see the Killnet section).

Based on industry and open-source reporting, U.S., Australian, Canadian, New Zealand, and UK cyber authorities assess multiple Russian-aligned cybercrime groups pose a threat to critical infrastructure organizations. These groups include:

- The CoomingProject
- Killnet
- MUMMY SPIDER
- SALTY SPIDER
- SCULLY SPIDER
- SMOKEY SPIDER
- WIZARD SPIDER
- The Xaknet Team

Additional Details:

For additional information including mitigations, cyber incident preparedness, IAM best practices, and more, please review the full alert here.

Reference(s)	whitehouse, cisa, cisa, NCSC, cisa, Bleeping Computer, Global News, The Record, Reuters

Sources

BleepingComputer: US and Allies Warn of Russian Hacking Threat to Critical Infrastructure

CISA: AA21-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Global News: Canada, Allies Warn of Russian Cyberattacks on Critical Infrastructure Due to Ukraine War

Recorded Future: U.S., Allies Provide 'Comprehensive' Overview of Russia Cyber Threats

Reuters: West Warns of Russian Cyberattacks on Critical Infrastructure

Alert ID 5a805784

View Alert

Tags Russian State-Sponsored Cyber Threats, Joint Cybersecurity Advisory

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**