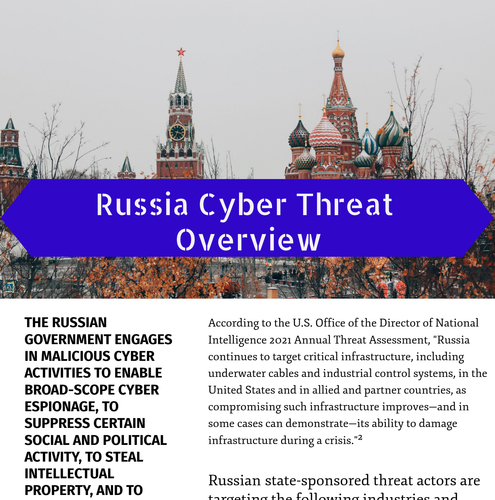

Russia Cyber Threat Overview

THE RUSSIAN GOVERNMENT ENGAGES IN MALICIOUS CYBER ACTIVITIES TO ENABLE BROAD-SCOPE CYBER ESPIONAGE, TO SUPPRESS CERTAIN SOCIAL AND POLITICAL ACTIVITY, TO STEAL INTELLECTUAL PROPERTY, AND TO HARM REGIONAL AND INTERNATIONAL ADVERSARIES.[1]

According to the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis."[2]

The FBI and DHS assess Russian Foreign Intelligence Service (SVR) cyber actors—also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and Yttrium—will continue to seek intelligence from US and foreign entities through cyber exploitation, using a range of initial exploitation techniques that vary in sophistication, coupled with stealthy intrusion tradecraft within compromised networks[3]

Russian state-sponsored threat actors are targeting the following industries and organizations in the United States and other Western nations[1]:

- COVID-19 Research
- Governments
- Election Organizations
- Healthcare & Pharmaceutical
- Defense
- Energy
- Video Gaming
- Nuclear
- Water
- Aviation
- Critical Manufacturing
- Commercial Facilities

Russia has fewer financial resources to invest in intelligence capabilities than the US or China. One means of compensating for this, it seems, is to blur the dividing line between state and non-state actors.[4]

The use of so-called 'patriotic hackers' and organized cyber-crime expertise is believed to substantially enhance Russia's cyber capabilities.[4]

It is unclear precisely how much direction patriotic hackers and cyber criminals are given by the Kremlin, but often their activities have no discernible motive apart from furthering the aims of the Russian state.[4]

SVR-leveraged TTPs

- Password spraying
- Leveraging Zero-Day Vulnerability
- WELLMESS Malware
- Tradecraft Similarities of SolarWinds-enabled Intrusions

SVR cyber operators are capable adversaries. In addition to the techniques described above, FBI investigations have revealed infrastructure used in the intrusions is frequently obtained using false identities and cryptocurrencies.[3]

Dutch Case Highlights

The Dutch Intelligence and Security Service - AIVD - highlighted a case of Russian cyber activities in their 2020 yearly report.

The Netherlands is one of the most developed countries in the world in terms of economy, science and technology. That makes it a target for states that want to steal technology and knowledge.

Russia spied on technology companies in the Netherlands in 2020. In December, the AIVD disrupted the work of a Russian intelligence officer. He had a significant, clandestine network of more than ten people who worked or had worked in the Dutch high-tech sector.

He used that network to obtain sensitive information about nanotechnology, semiconductors, artificial intelligence and dual-use technology, among other things. He paid some individuals for that information.

The intelligence officer was operating under a diplomatic cover. In reality, he worked for the civil intelligence service SVR. He has been declared *persona non grata*, along with a second Russian intelligence officer who did support work, and have left the country.[5]

The AIVD has made the disruption operation public in order to signal to Russia that such intelligence activities will not be tolerated. And to make companies and citizens more aware of the existence of economic espionage. The government is currently investigating how espionage can be criminalized.

Source: AIVD Jaarverslag 2020

SOURCES:

[1]CISA Russia Cyber Threat Overview and Advisories https://us-cert.cisa.gov/russia

[2]Annual Threat Assessment of the US Intelligence Community, ODNI, April 9, 2021 https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2204-2021-annual-threat-assessment-of-the-u-s-intelligence-community

[3]Joint Cybersecurity Advisory; Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders, April 26, 2021 https://us-cert.cisa.gov/ncas/alerts/aa21-116a

[4] Cyber Capabilities and National Power: A Net Assessment, The International Institute for Strategic Studies, June 2021 https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

[5] Internationale dreigingen en politieke veiligheidsbelangen, Jaarverslag AIVD 2020, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2020/internationale-dreigingen-en-politieke-veiligheidsbelangen