Russia's security services against one another

Reference: Memo [190814-1] – Version: 1.0
Keywords: espionage, Russia, MVD, GRU, FSB, Kaspersky Lab
Sources: Publicly available information

Key Points

- Since 2014, Russia's security services are competition with each other.
- They act independently and take unnecessary risks in order to gain political influence over their counterparts.
- This has also resulted in an increase of treason allegations aimed at high-ranking Russian officials.

Summary

This year's Black Hat USA conference showcased several Russia-centric talks, including one related to the country's security services tense relationships with each other[1]. During her talk, Kimberly Zenz explained that, even though Russia's security services were often seen as one big entity, each one (MVD, GRU, FSB) having their own perimeter and working together if needed, services' "perimeters" overlapped at times. Law enforcement, intelligence and cybercrime are such areas of overlap[2]. In such cases, services tended to act independently, even if it meant attacking the same target multiple times[3]. According to the presenter, this started around 2014, following geopolitical pressures, economic uncertainty, conflicts within the country's elite and power shifts. Kaspersky Lab's name was cited along with Russian security services by Ms Zenz, for its links with the FSB, but more so because of its successful cybercrime fighting activities.

A side effect of the independence of the security services and their constant quest for operational success is boldness, sometimes even leading them to take unnecessary risks, according to Ms Zenz. In order to illustrate this, she took the example of NotPetya (officially attributed to Russia by the USA[4] and the UK[5]), saying that she did not "believe anyone in any Russian security services wanted to cause 10 billion in damages". The need to gain political advantage over competing services also results in a lack of coordination, with the example of the attack on the US Democratic National Committee, in 2016 by both the Turla (also known as Venomous Bear, ATT&CK G0010) and Fancy Bear (also known as APT28, ATT&CK G0007) threat actors.

Another effect of competition between services lies in the allegations of treason against high-ranking officials and the arrests following those. Until a few years ago, these manoeuvres would not have been possible and real accusations would have resulted in the resignation of the official. To support her claims, Ms Zenz detailed a case she was personally involved in, as an alleged US spy, which resulted in the arrest and imprisonment of several Russian citizens[6].

Comments

This disorganisation and lack of communication between Russia's services presents an advantage for their usual targets, which include the EU-I:

- The country is wasting resources attacking the same targets with several state-sponsored threat actors at a time.
- This type of behaviour increases the chances of detecting malicious activity in targets' information systems, due to the increase of non-nominal operations it might produce (compared to the activity of only one threat actor).

Additionally, the services' tendency for recklessness means that they might be less considerate towards the quality and security of operations (OPSEC). This could possibly assist detection at the victim site, but could also result in inadvertently causing major damages in the form of a new NotPetya-like incident.

As part of its Top Threat Actors program, CERT-EU maintains profiles (profiles, historical activities, TTPs) as well as a collection of actionable data for the most prominent Russian threat actors. If one of these were to become a direct and immediate threat to EU-I, a threat alert will be released by CERT-EU.

[1] https://www.blackhat.com/us-19/briefings/schedule/?hootPostID=db681a52c6a321681e1f9281b5124457#infighting-among-russian-security-services-in-the-cyber-sphere-14693
[2] https://www.pcmag.com/news/370107/russian-intel-agencies-are-a-toxic-stew-of-competition-and-s
[3] https://en.wikipedia.org/wiki/Democratic_National_Committee_cyber_attacks#Hacking_the_DNC
[4] https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/
[5] https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks
[6] https://www.thedailybeast.com/kremlin-accused-her-of-being-a-us-spy-she-offered-to-go-to-moscow