On attribution: APT28, APT29…Turla: No, they are NOT the same

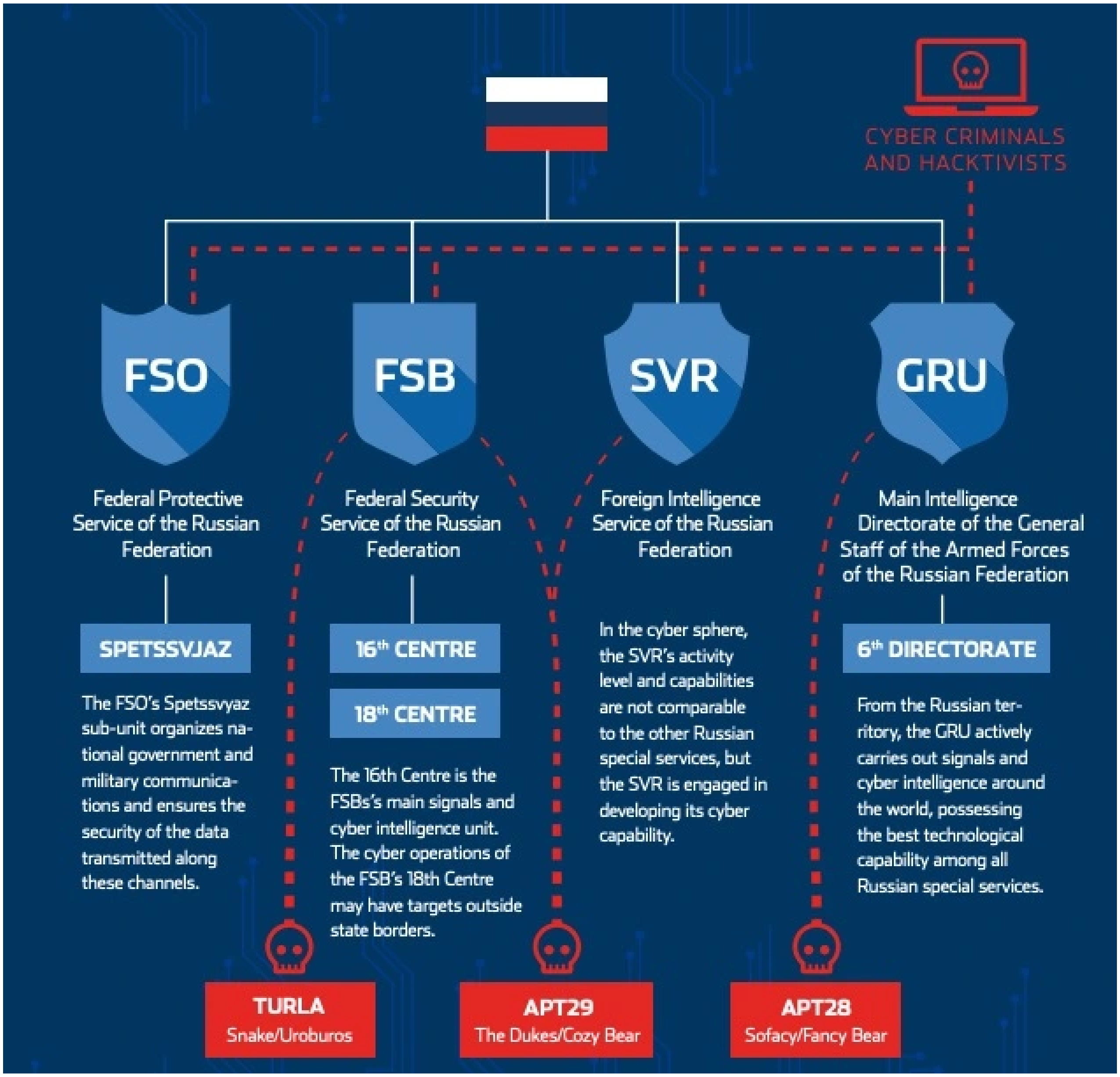
xorl.wordpress.com/2021/01/25/on-attribution-apt28-apt29-turla-no-they-are-not-the-same/

January 25, 2021

leave a comment »

Earlier today someone forwarded me (outside of work) a threat intelligence "report" – quotes because it was far from being a finished product – that was recommending that people impacted by one of those three nation-state actors should be communicated as "Russia targeting your organization". I found this assessment **dangerously wrong and inaccurate** so let me explain here why and maybe my post will help others avoid similar oversimplifications.

I cannot reference classified attribution intelligence products, but one of the most reputable public sources is Välisluureamet, Estonia's foreign intelligence service. In Välisluureamet's 2018 unclassified report they attributed those groups to specific organizations within the Russian Federation government. So let's assume that this is accurate for the sake of this blog post.


CYBER CRIMINALS
AND HACKTIVISTS
FSO
FSB
SVR
GRU
Federal Protective Service of the Russian Federation
Federal Security Service of the Russian Federation
Foreign Intelligence Service of the Russian Federation
Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation
SPETSSVJAZ
16th CENTRE
18th CENTRE
6th DIRECTORATE
TURLA
Snake/Uroburos
APT29
The Dukes/Cozy Bear
APT28
Sofacy/Fancy Bear

The FSO's Spetssvyaz sub-unit organizes national government and military communications and ensures the security of the data transmitted along these channels.

The 16th Centre is the FSBs's main signals and cyber intelligence unit. The cyber operations of the FSB's 18th Centre may have targets outside state borders.

In the cyber sphere, the SVR's activity level and capabilities are not comparable to the other Russian special services, but the SVR is engaged in developing its cyber capability.

From the Russian territory, the GRU actively carries out signals and cyber intelligence around the world, possessing the best technological capability among all Russian special services.

Why is it **dangerously wrong** to communicate that getting targeted by APT28, APT29 or Turla is "Russia targeting you" rather than the specific actors? Simply because they are significantly different organizations, with different modus operandi, different objectives, and different TTPs. This means that your threat model will be entirely different if you want to be protected against APT28 versus Turla or APT29. To be more precise…

APT28 (GRU's 6th Directorate/Military Intelligence)
A military intelligence agency is usually after intelligence of military value. Specifically this agency has shown that they are one of the most active actors in cyber with massive resources but not extremely sophisticated. Of course, when there are big geopolitical events, military research, investigations on Russian military activities or military exercises they will be around, and they will be after any connected systems that can get them military intelligence

that could benefit the Russian Federation and its allies. They have been seen using all intelligence disciplines without any noticeable preference on cyber over other means of collection.

APT29 (SVR/Foreign Intelligence)
This is the equivalent of the CIA for Russia and just like the CIA, their cyber operations are typically more on the targeted and less on the bulk collection. In numerous occasions they have been seen conducting close access operations, and their objectives typically are related to political and economical information. For example, finding dirt to recruit someone as an SVR agent or finding out the details of a commercial agreement or research that could benefit the Russian state or its allies. They are less in the SIGINT and more in the HUMINT space so they are more likely to recruit an insider to get them what they want than perform an extremely sophisticated cyber operation.

Turla (FSB's 16th Center/Signals Intelligence)
Turla is the equivalent of the NSA's Signals Intelligence Directorate (SID) and because of that, they are one of the most sophisticated cyber actors out there operating at a level similar to that of the NSA, including bulk collection. This means that they collect intelligence for a variety of agencies both for Russia but also Russia's allies under various agreements. So their target space is massive and they are the most advanced cyber operators of the Russian government. They have a massive organization and their sole purpose is SIGINT. So if you are targeted by Turla then expect some very advanced and complex cyber operations. Also, if you are targeted by Turla it doesn't mean that it's Russia targeting you, it could be that they execute an intelligence collection agreement for an ally of Russia that doesn't have such cyber intelligence collection capabilities, similarly to what the NSA's SID and other large SIGINT agencies do.

And this is why oversimplifying in a threat intelligence product that any of the above actors should be treated as simply "Russia is after you" is dangerous for cyber security departments/customers that have to develop defensive controls to protect their assets.

If you are unsure about the attribution it's better to **stay away from attributing it at all** until you have sufficient evidence, and focus on the lower level indicators and warnings that you can share to help defenders take some action. For example, what did you observe in terms of TTPs or even IOCs. It's better to share high confidence intelligence than "it's the Russians" that has zero practical application to develop protections without more context that can help in understanding the motivations and intentions.

The same applies if you are a briefer delivering those threat intelligence products, choose your words wisely. Finally, do not forget that some of those agencies collaborate on certain projects including sharing some software tools, libraries and TTPs (typically through lessons-learned sessions and internal policies).

Hopefully that clears it out…

Written by xorl

January 25, 2021 at 10:59

Posted in threat intelligence

Leave a Reply

Fill in your details below or click an icon to log in:

You are commenting using your WordPress.com account. (Log Out / Change)

You are commenting using your Twitter account. (Log Out / Change)

You are commenting using your Facebook account. (Log Out / Change)

Cancel
Connecting to %s