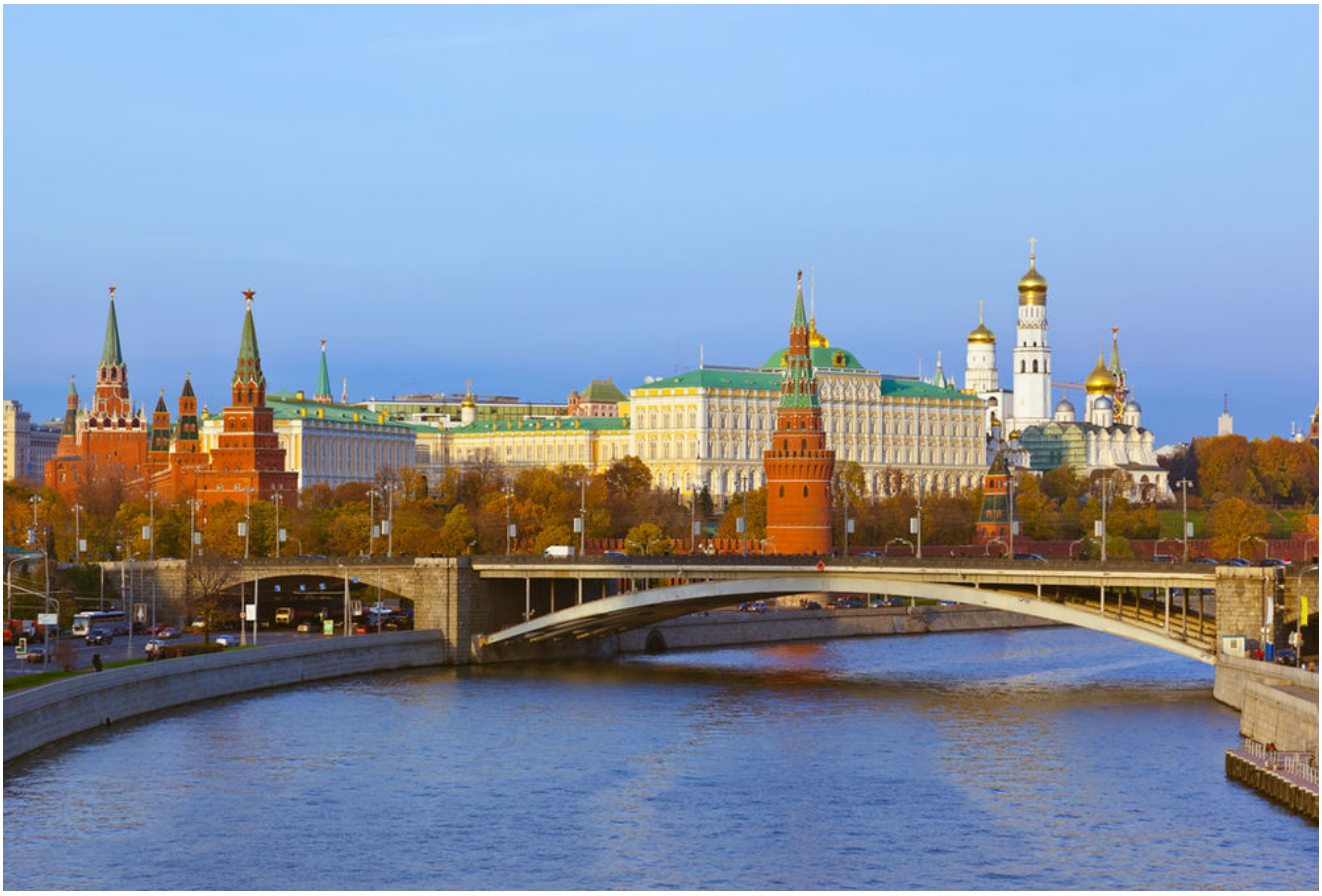
Revisited: Fancy Bear's New Faces...and Sandworms' too

riskint.blog/post/revisited-fancy-bear-s-new-faces-and-sandworms-too

October 19, 2020



- Curtis
-
-
    - Oct 19, 2020
    -
    - 5 min read

Summary

Since last posting on Unit 26165 and Unit 74455, new details have been released publicly and further analysis conducted on Anatoliy Sergeyevich Kovalev and Artem Andreyevich Malyshev. Periodic review of past collection can often identify new details. Recent findings indicate Anatoliy Sergeyevich Kovalev is associated with the cyber threat actor commonly referred to as Sandworm (a.k.a. Voodoo Bear, Telebots, Iron Viking), and he could have links

to Russia's Federal Protective Service (FSO). An account using the name and picture of Artem Andreyevich Malyshev, an officer in Unit 26165 (a.k.a. Fancy Bear, APT28), appears on a Russian freelancing website advertising computer services, such as system administrator and programming.

Analysis

Unit 74455

On October 15, 2020, the US Department of Justice indicted six Russian General Staff Main Intelligence Directorate (GRU/GR) officers from Unit 74455 (a.k.a. Sandworm, Voodoo Bear, Telebots, Iron Viking) for their alleged roles in computer network operations. The alleged intrusions included the following targets:

- Critical infrastructure in Ukraine (a.k.a. Black Energy, KillDisk, Industroyer);
- A political campaign in France;
- The country of Georgia;
- International victims of the “NotPetya” malware attacks;
- 2018 Winter Olympic Games (a.k.a. Olympic Destroyer); and
- Investigations of nerve agent attacks that have been publicly attributed to the Russian government.

In February 2020, the US State Department reported that GRU's Main Center for Special Technologies (GTsST), in particular Unit 74455 and 'Sandworm' carried out a disruptive cyber attack against the country of Georgia. Approximately five months later, the European Union (EU) sanctioned several cyber threat actors, including Unit 74455. The EU further elaborated on their designation of Unit 74455 by saying it aligns with the threat actor Sandworm. Prior to these details it was not publicly reported that Unit 74455 corresponded to the Sandworm threat actor, and all the intrusions described in the October 2020 indictment were perpetrated by Unit 74455.

The Report on the Investigation into Russian Interference in the 2016 Presidential Election, commonly referred to as the Mueller Report, provide new details on the role Unit 74455 played in interference of the 2016 US Presidential Elections. According to the report, Unit 74455 assisted with the release of documents stolen by Unit 26165, the promotion of those release documents, and the publication of anti-Clinton content on social media. Furthermore, officers from Unit 74455 separately targeted state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the

administration of U.S. elections. One of the individuals previously reported on, Anatoliy Sergeyevich Kovalev is an officer in Unit 74455. **Anatoliy Sergeyevich Kovalev** (Ковалев Анатолий Сергеевич)

Since last identifying information related to Anatoliy Sergeyevich Kovalev, hereinafter Mr. Kovlev, one of the VK accounts linked to Mr. Kovalev has been deleted. It is unclear why only one of the two previously linked accounts is deleted, but the account used the alias Nikita Abramov. The deletion of the account inspired further analysis on the other active account.

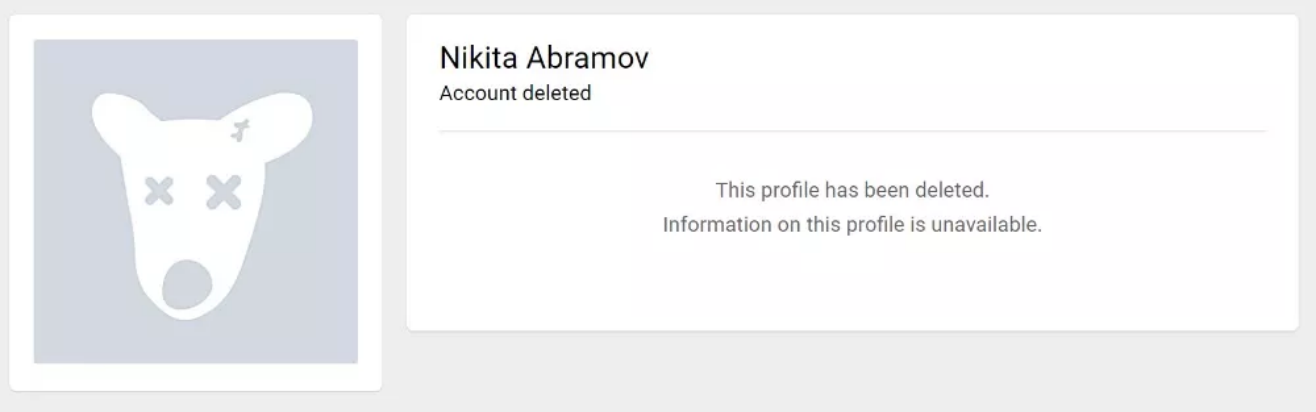


Figure 1 - Deleted VK account linked to Mr. Kovalev

One of the pictures on the active account is the same picture that was observed on the now deleted Nikita Abramov account, as seen in figure 2. The picture shows Mr. Kovalev in a race bib sporting number 155. At the time, the number on the bib was used to cross refence both accounts and confirm their relation to Mr. Kovalev. A newly discovered facial recognition tool identifies if two faces are the same person with some level of certainty. That race bib picture compared to the FBI picture of Mr. Kovalev produced a match with 88% certainty. An overlooked emblem on the race bib also provides new insights into Mr. Kovalev's career.

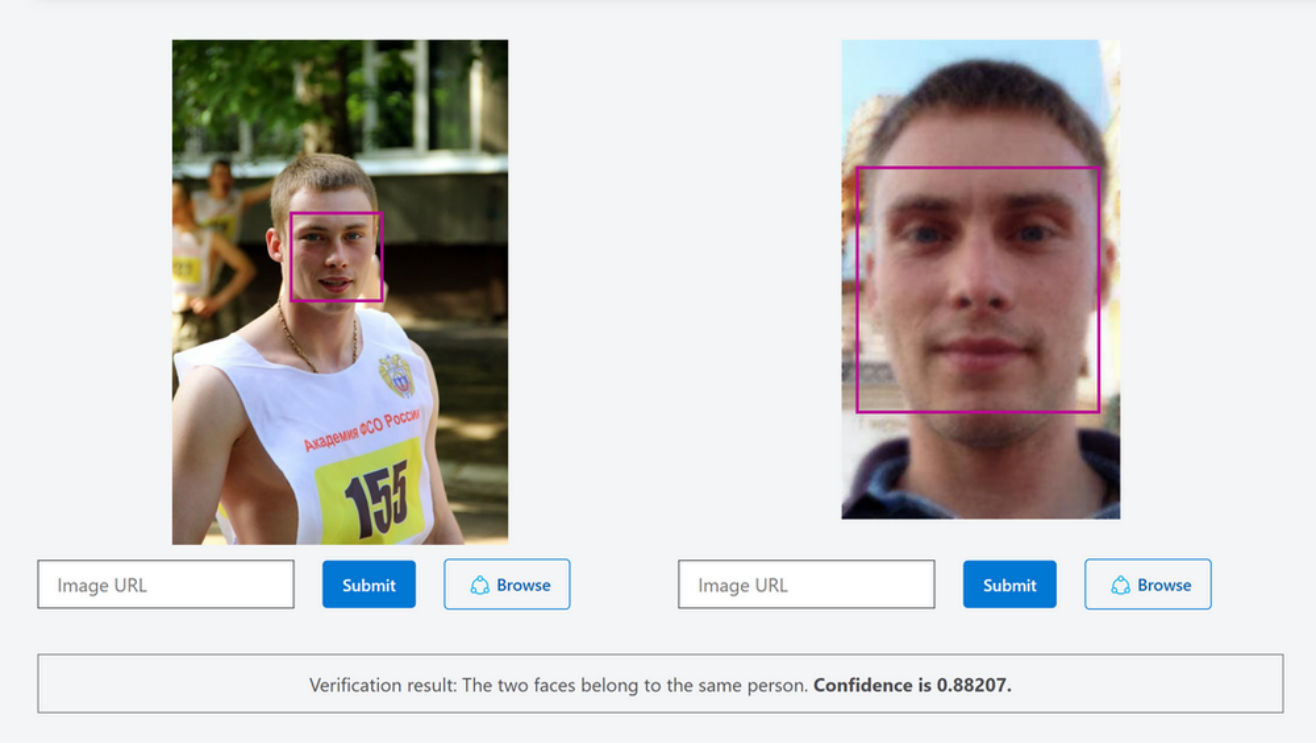


Figure 2 - Face match of Mr. Kovalev

The emblem on the top right of the race bib is actually the insignia for Russia's Federal Protective Service (FSO). The FSO is a Russian government agency focused on protecting high-ranking state officials, including the Russian President. The picture was posted on the VK account sometime in or around 2013, which would put Mr. Kovalev at 21 or 22 years old in the picture (using the date of birth provided by the FBI). There is even chance that in or around 2013 Mr. Kovalev either joined or attempted to join the FSO, but by at least 2016 had became a part of Sandworm. Mr. Kovalev appears to have a full career working for the Russian government. However, Mr. Kovalev's colleague, Artem Andreyevich Malyshev appears to be venturing into the private sector.

Figure 3 - FSO logo on Mr. Kovalev's clothing

Artem Andreyevich Malyshev (Артём Андреевич Малышев)

Artem Andreyevich Malyshev, hereinafter Mr. Malyshev, has risen through the ranks from a likely military cook to an officer in Unit 26165. One of the pictures of Mr. Malyshev that was previously identified on multiple online accounts, possesses a 84% certainty match with the FBI picture of Mr. Malyshev. This same picture has been recently identified on a Russian freelancing website.

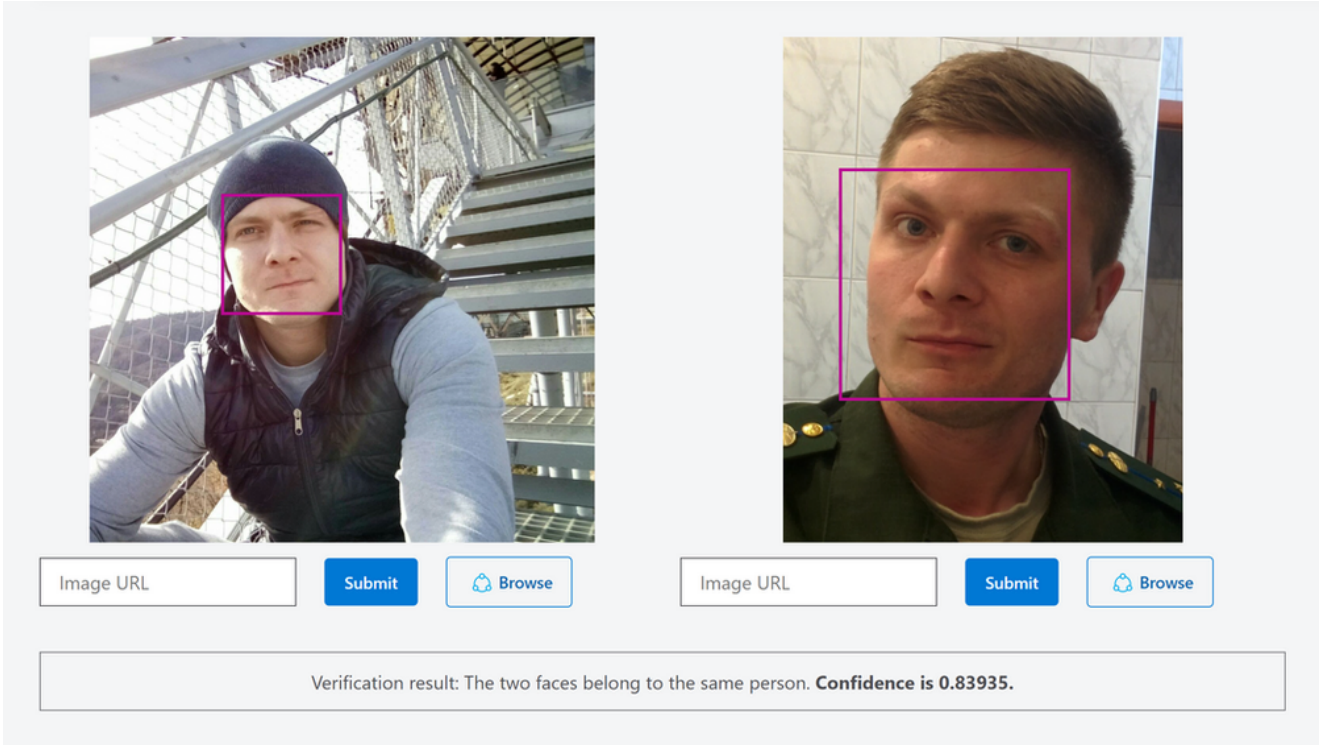


Figure 4 - Face match of Mr. Malyshev

A reverse image search of the picture seen in Figure 4 produced an account on a Russian freelancing website. The account is linked to a "Malyshev Artem Andreyevich", which is the same name as Mr. Malyshev, but with his surname before his given name. The account shows services offered include System Administrator, Programming, IT outsourcing, Web Design, Typing and Printing. The prices for these services are unavailable and need to be requested. Each freelancer account has a rating that uses a scale from one to five, with one being poor and five being great. The account with Mr. Malyshev's photo is only rated a 4.1 out 5. There are many other freelancers who have a higher rating, including many with a 5 out of 5.

Figure 5 - Freelancer account with Mr. Malyshev

There is not date on the account to assess if it is owned and controlled by Mr. Malyshev. The picture is publicly available and could be used by anyone to create the account. However, I like to think Mr. Malyshev went from hacking the Democratic National Convention, United States Anti-Doping Agency (USADA) and the World Anti-Doping Agency (WADA) to becoming a run-of-the-mill system admin for you average mom and pop shop. If Mr. Malyshev was driving Uber he would be suspended with that weak 4.1 rating.

Conclusion

Revisiting previous analysis can be quite useful for anyone in an analytical profession. In this case, newly released details on Sandworm allow for better attribution of Mr. Kovalev and Unit 74455. Overlooked details in a picture of Mr. Kovalev help understand his career path and possible affiliations with other Russian government organizations. It remains unconfirmed if Mr. Malyshev has or is currently moonlighting as a freelancer, but periodic checks on past collection could be beneficial for identifying new and critical details.