# US DoJ indicts Russia’s Sandworm threat actor

Threat Memo - Date: 20/10/2020 - Version: 1.0

TLP:WHITE

| | Category | Type | Domain(s) | Sector(s) | Confidence |
|---|---|---|---|---|---|
| **FOR INFORMATION** | Cyberespionage, Cyberwar | Targeted intrusions, Disruptions | [EU], [World] | Energy, Political party, Government, Sport, Health, Media, Pharmaceutical, Chemical | A1 |

## Key Points

- US authorities charged 6 members of the Russian Military Intelligence unit 74455 (aka Sandworm) threat actor.
- Sandworm is accused of - mostly disruptive - cyberoperations in Ukraine (electric grid), France (political entities), UK and the Netherlands (chemical laboratories), Georgia (government, media), South Korea (2018 Winter Olympics) and globally (NotPetya).
- This indictment follows sanctions imposed on the same organisation by the EU in July 2020.

## Summary

In an indictment[1] dated October 15, the US court of the western district of Pennsylvania charged 6 members of the Russian Sandworm threat actor for computer fraud and conspiracy. The objective of the conspiracy was to deploy destructive malware and take other disruptive actions, for the “strategic benefit of Russia”. Sandworm (aka Telebots, Voodoo Bear, and

Hades), is the codename given by the cyber security community to the Unit 74455 of Russia's GRU military intelligence. The hackers are charged for cyber operations which include:

- Ukraine - Disruptive operations in December 2015 and December 2016 against the electric power grid (malware: Industroyer, BlackEnergy, KillDisk).
- France - Spearphishing campaign in April and May 2017 against political parties including the current French President Emmanuel Macron's La République en Marche.
- Global - Worldwide victims of the NotPetya malware attacks in June 2017, including 80 medical facilities in the US, a FedEx subsidiary, the Maersk shipping company, and a large US pharmaceutical manufacturer, totalling nearly $1 billion in losses.
- Global - International victims associated with the 2018 Winter Olympics, including Olympic partners and athletes, South Korean government agencies, and the International Olympic Committee (malware: Olympic Destroyer deployed against systems used by the Olympic Games information technology vendor, and the Organising Committee).
- Global - International and government organisations investigating the poisoning of a former GRU officer and his daughter in the UK in April 2018, including the Netherlands-based Organisation for the Prohibition of Chemical Weapons (OPCW) and UK's Defence Science and Technology Laboratory (DSTL).
- Georgia - Spearphishing campaign in January 2018 against NGOs, private companies, a media outlet. Defacement or disruption of approximately 15.000 websites in October 2019.

| Officer name | Role |
|---|---|
| Yuriy Sergeyevich Andrienko | Developed components of NotPetya and Olympic. Destroyer. |
| Sergey Vladimirovich Detistov | Developed components of NotPetya.<br>Prepared infrastructure for spearphishing 2018 Winter Olympics. |
| Pavel Valeryevich Frolov | Developed components of NotPetya and the malware used against Ukraine's Ministry of Finance and State Treasury Service. |
| Anatoliy Sergeyevic Kovalev | Sent spearphishing emails to a wide variety of entities and individuals (French local government entities, political parties, 2018 Winter Olympics, the DSTL and a Georgian media entity.<br>Engaged in spearphishing campaigns for apparent personal profit (Russian real estate and car dealers, cryptocurrency miners and cryptocurrency exchanges located outside of Russia). |
| Artem Valeryevich Ochichenko | Developed malicious email attachments and send spearphishing emails (officials and organisers of the 2018 Winter Olympics).<br>Targeted Georgian government and other Georgian entities in 2019. |

| Officer name | Role |
|---|---|
| Petr Nikolayevich Pliskin | Supervisory role - Development Team Lead / IT manager. Developed components of NotPetya and Olympic Destroyer. |

## Comments

The Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (aka GRU) has been accused of many malicious cyber operations. With at least 3 units involved, this organisation shows a large variety of skills including malware development, advanced supply chain compromises, large-scale data exfiltration, operational technology disruption, and information operations via hack-and-leak. More specifically:

- Unit 74455 (aka Sandworm threat actor) is specialised in targeted intrusions with a disruptive purpose,
- Unit 26165 (aka APT28 threat actor) has conducted a large number of intrusion attempts with espionage purposes,
- Unit 54777 administers the infrastructure and social media accounts used to run leak outlets, including DCLeaks. The specific role of this unit in Russian information operations was analysed in a recent report released by Facebook and the think tank DFRLab. See details TM-20-122.

In July 2020, the European Union imposed sanctions[2] against:

- four members of the GRU (Alexey Valeryevich Minin, Aleksei Sergeyvich Morenets, Evgenii Mikhaylovich Sebebriakov, Oleg Mikhaylovich Sotnikov) for their participation in the cyberattack against the Organisation for the Prohibition of Chemical Weapons (OPCW),
- the Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) for cyberattacks publicly known as NotPetya in June 2017 and the cyberattacks directed at the Ukrainian power grid in the winter of 2015 and 2016.

Before this most recent indictment, authorities in the US but also in Germany had already charged Russian intelligence officers for cyber operations. See examples in the table below.

| Date | Authorities | Details |
|---|---|---|
| Mar-17 | US | Indictments of four Russian nationals allegedly responsible for the 2014 breach into Yahoo! networks that compromised data of 500 million accounts. Two of the named individuals were reportedly employees of Russia’s Federal Security Service (FSB). |
| Nov-17 | US | Charges against six members of the GRU in the hacking of the Democratic National Committee computers before the 2016 US presidential election. |

| Date | Authorities | Details |
|---|---|---|
| May-20 | Germany | International arrest warrant for Dmitry Badin for his alleged role in the 2015 intrusion against the German Bundestag. Dmitry Badin reportedly acted on behalf of GRU and is a supervising officer in GRU Unit 26165. |

The list of cyberoperations for which US authorities are accusing Sandworm is extensive. The indictment provides a lot of details on techniques, tactics and procedures. Regarding Sandworm activities in Ukraine and South Korea in 2017-2018, a 2019 report[3] by Google's Threat Analysis Group detailed how Sandworm had been targeting Android users, using advanced supply chain compromise techniques in Android App development chain and the Play Store. See also TM-191206.

## References

1. https://beta.documentcloud.org/documents/20397870-gru-indictment
2. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/
3. https://blog.google/technology/safety-security/threat-analysis-group/protecting-users-government-backed-hacking-and-disinformation/