

Who Is Dmitry Badin, The GRU Hacker Indicted By Germany Over The Bundestag Hacks?

 [bellingcat.com/news/2020/05/05/who-is-dmitry-badin-the-gru-hacker-indicted-by-germany-over-the-bundestag-hacks/](https://www.bellingcat.com/news/2020/05/05/who-is-dmitry-badin-the-gru-hacker-indicted-by-germany-over-the-bundestag-hacks/)

May 5, 2020



May 5, 2020

- [Germany](#)
- [GRU](#)

On 5 May 2020, German media reported that Germany's Federal Prosecutor has issued an arrest warrant against Russian citizen Dmitry Badin, the main suspect in the 2015 hacking of the German Bundestag.

What Was The 2015 Bundestag Hack?

In April 2015, members of the German parliament as well as members of Merkel's Bundestag office, received an email that ostensibly originated from the United Nations, based on its visible domain name "@un.org". The mail was titled "*Ukraine conflict with Russia leaves economy in ruins*". The email carried malicious executable code that installed itself on the victim's computer.

Over the next several weeks, the malicious software — which appeared to steal passwords and spread via the local networks — had taken over the whole Bundestag IT infrastructure, rendering its online services and external website inaccessible. In the background, logs later

showed, over 16 gigabytes of data had been sucked up by a foreign-based hacker. These included complete mailboxes of German parliamentarians. According to media reports, Angela Merkel’s parliamentary office was also breached.

Who Is Dmitry Badin?

German media report that the German Federal Police has been able to link the 2015 phishing campaign and subsequent data theft to Dmitry Badin, an assumed member of GRU’s elite hacking unit 26165, better known among cyber security analysts as APT28. The operations’ linkage to him has reportedly been made based on log analysis and “information from partner services”; however, no specific evidence of how the attribution was made has yet been made public.

Dmitry Badin was already on the FBI’s wanted list over his alleged involvement in several hacking operations attributed to GRU’s APT28 unit. Among these operations was the hack of the anti-doping organization WADA while it was investigating a doping administration program, as well the DNC hack on the eve of the U.S. presidential elections.

DETAILS

On October 3, 2018, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against 7 Russian individuals for their alleged roles in hacking and related influence and disinformation operations targeting, among others, international anti-doping agencies, sporting federations, and anti-doping officials. The indictment charges Dmitry Sergeevich Badin, Artem Andreyevich Malyshev, Alexey Valerevich Minin, Aleksei Sergeevich Morenets, Evgenii Mikhaylovich Serebriakov, Oleg Mikhaylovich Sotnikov, and Ivan Sergeevich Yermakov, with computer hacking activity spanning from 2014 through May of 2018, including the computer intrusions of the United States Anti-Doping Agency (USADA), the World Anti-Doping Agency (WADA), and other victim entities during the 2016 Summer Olympics and Paralympics and afterwards. The indictment charges these defendants with conspiracy to commit computer fraud, conspiracy to commit wire fraud, wire fraud, aggravated identity theft, and conspiracy to commit money laundering. The United States District Court for the Western District of Pennsylvania in Pittsburgh, Pennsylvania, issued a federal arrest warrant for each of these defendants upon the grand jury’s return of the indictment.

THESE INDIVIDUALS SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK
If you have any information concerning this case, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

Validating Dmitry Badin’s Linkage To The GRU

FBI documents describe Dmitry Badin briefly as “alleged to have been a Russian military intelligence officer, assigned to Unit 26165”, born in Kursk on 15 November 1990. His passport photograph was published as part of his *Wanted* package.

Based on analysis of data from primarily open sources, we can confirm that Dmitry Badin, born 15 November 1990, indeed works for GRU's unit 26165.

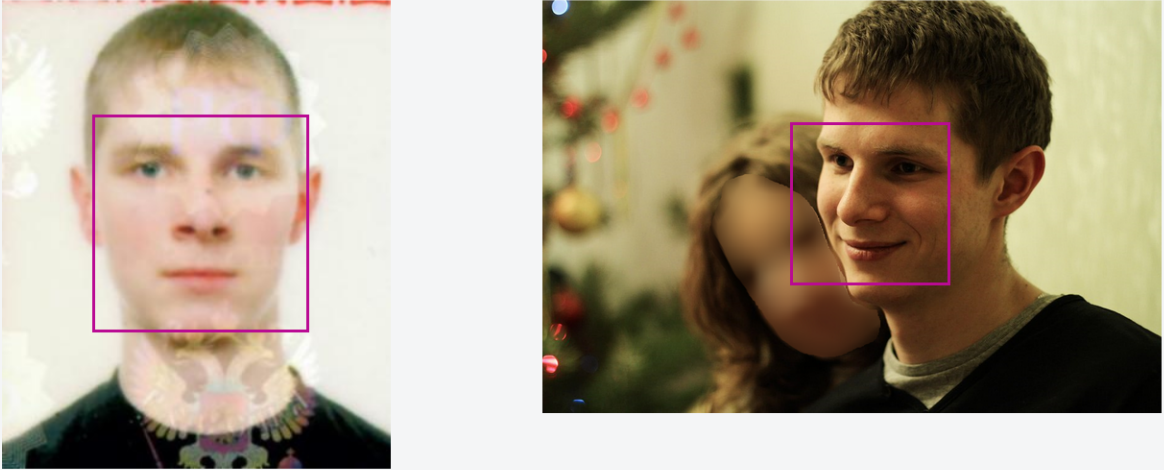


Image URL

Image URL

Verification result: The two faces belong to the same person. **Confidence is 0.86537.**

Using Russian social-media reverse-image search application FindClone, we found Dmitry Badin's photographs in his wife's VK account. We then re-validated that this is the same person by comparing the two photos in Microsoft Azure's Face Verification tool

A search for Badin's full name and birth date in previously leaked Moscow car registration databases provided a match: Dmitry Sergeevich Badin, born on 15 November 1990, purchased a KIA PS car in June 2018. The car registration included the owner's passport number and place of issue (St. Petersburg), as well as his registered address. Badin's registered address, as of 1 June 2018, was *Komsomolsky Prospekt 20*.

ИНФОРМАЦИЯ ПО ТРАНСПОРТНОМУ СРЕДСТВУ

Дата операции: 01.06.2018
Государственный номер: B57 [REDACTED]
Марка: KIA
Модель: PS (SOUL)
Год выпуска: 2018
Модель двигателя: G4FG
VIN: [REDACTED]
Номер двигателя: JH850977
Серия регистрационного документа: 5058
Номер регистрационного документа: 990218
Серия ПТС: ОУ
Номер ПТС: [REDACTED]
Дата выдачи ПТС: 08.05.2018
Стоимость: 1109900

ИНФОРМАЦИЯ ПО ВЛАДЕЛЬЦУ

ФИО: БАДИН ДМИТРИЙ СЕРГЕЕВИЧ
Дата рождения: 15-11-1990
Удостоверяющий личность документ: 4010 [REDACTED]
Место выдачи удостоверяющего личность документа: ОУФМС ПО САНКТ-ПЕТЕРБУРГУ И ЛЕНИНГРАД...
Дата выдачи удостоверяющего личность документа: 08-12-2011
Адрес: КОМСОМОЛЬСКИЙ ПРОСП. Д.20

This is the address of GRU's military unit 26165, as can be seen from [publicly available](#) Russian corporate registries. Unit 26165 is also known as the GRU's 85th Main Center, specializing in cryptography. The center first gained public notoriety in 2017, when our Russian investigative partner The Insider [discovered](#) that an officer from this unit had inadvertently left his personal metadata in a document leaked as part of the so-called Macron Leaks.

| Название компании | Статус | ИНН | Руководитель | Дата регистрации | Адрес |
|---|-------------|------------|--------------------------------|------------------|--|
| ФКУ "ВОЙСКОВАЯ ЧАСТЬ 26165" <small>ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ "ВОЙСКОВАЯ ЧАСТЬ 26165"</small> | Действующее | 7704739810 | Михайлов Дмитрий Александрович | 30.11.2009 | 119021, г Москва, проспект Комсомольский, 20 |

Address registration for Unit 26165

We have previously [identified](#) a breach in the operational security of Russia's military intelligence that allowed the identification of at least 305 officers who had their cars registered at this same address. Dmitry Badin was not among the list of 305 officers we identified then due to the fact that he purchased his car after the car-registration database we consulted in October 2018 had been publicly leaked.

Scaramouche, Scaramoush!



Currently, we have no knowledge of how German investigators were able to link Dmitry Badin to the Bundestag hack. However, open-source evidence we discovered may point to his role in many more than the three hacking operations that his name has been linked to.

Using the license plate number of Badin's car, we searched a leaked Moscow parking [database](#) and found that he frequently parked his car near the dormitory of Russia's Military Academy, at Bolshaya Pirogovskaya 51. The parking logs also contained two phone







numbers that he had used for mobile payments for his parking sessions. We then looked up both of these numbers in various phone messengers and reverse-search phone databases.

One of the numbers appeared in the Viber messenger app under the obviously assumed name of Gregor Eisenhorn, a character from the fantasy Warhammer 40,000 game.

The other number appeared in two different phone-number look-up apps, both under his real name and under what would later appear to be his favorite alias: “Nicola Tesla.”

| | | | |
|---|---|---|--|
|  | Getcontact Result for +7999829 [redacted]: Никола Тесла |  | SmartSearchBot Запрос принят, ожидайте ответа! ООО "Скартел" (г. Москва и Московская область) Тел.: 7999829 [redacted] ФИО: Бадин Дмитрий |
|---|---|---|--|

We then checked if this number was linked to a social media account in Russia, and discovered that it had been connected to a now-deleted account on VKontakte (VK). Searching through archived copies of this account, we discovered that as of 2016 it had been used under the name Dmitry Makarov. Even earlier, however, it had borne the name Nicola Tesla, and also had the user name “*Scaramouche*”.

-  Тел.: **7911825** [redacted]
-  "VK": <https://vk.com/id14503478>
-  адрес: **Курск**
-  Тел.: **7471258** [redacted]
-  ФИО: **Tesla Nicola**
-  **Scaramouche**

Data from archived copy of the now-defunct VK account, showing two linked numbers, including a Kursk land-line number

During this period — which we could not date precisely from the archived copy — the user of the VK account had been based in Kursk, which is where Dmitry Badin was born, and where he grew up before moving to St. Petersburg. His Petersburg period — which can be established both from the place of issuance of his passport and from photos on his wife’s VK account prior to 2014 — is likely linked to his university studies. Our prior investigations into members of GRU’s hacking team have established that a large number of the hackers graduate from St. Petersburg computer science universities.

We also found out that Badin’s mobile number is linked to a Skype account, which, like his now defunct VK account, is in the name of “Nicola Tesla”, but uses the username **Scaramoush777**.

SKYPE DIRECTORY



Nicola Tesla

S scaramoush777

📍 Russian Federation

Scaramouche, from the Italian word **scaramuccia**, literally “little skirmisher”, is the standard evil-ish clown character from 16th-century commedia dell’arte. The word is probably better known from the well-known *recitative* from Queen’s Bohemian Rhapsody. However, to cyber security researchers investigating state-actor hacking operations, this word carries an additional payload.

In March 2017, the cyber threats unit of the cyber security firm SecureWorks(c) published its own attribution white paper, reasoning its conclusions that the hacking exploits by APT28 (which SecureWorks refers to with its own code name “Iron Twilight”) are a government-sponsored operation, which is most likely linked to Russia’s military intelligence. In its report, SecureWorks lists both the targets that it has identified APT28 as having attacked, as well as the tool set used by this shadowy hacker group.

The endpoint kit used by APT28 to perform screen captures and steal targets’ credentials, is called Scaramouche. This particular set of malware got its name from the SecureWorks Cyber Threats Unit who named it, in their own words, “after the Scaramouche username found in the PDB path of both tools”.

Given that Dmitry Badin used the Scaramouche username —judging by all evidence — before he joined the GRU, it is unlikely that he usurped a pre-existing user name for his VK and Skype accounts. This is clear when based on being part of a team of GRU coders called “scaramouche”. Much more plausibly, the user name “*scaramouche*” discovered by CTU was namely Badin’s own user name. This, in turn, would mean that the endpoint kit written by Dmitry Badin was a crucial piece of the malware used in all hacks attributable to APT28. from attacks on Russian opposition figures and journalists to Western media organizations (including Bellingcat), the MH17 investigation team, the German Bundestag, and the DNC.

It would be prudent to ask: is it plausible that such a prolific and savvy hacker would leave such traces that would readily implicate him in serial cyber crime? It is not so hard to believe, given GRU hackers’ own nonchalance towards covering their own tracks. Badin’s colleagues

who were caught trying to hack the OPCW's lab in the Hague, for example, were carrying on taxi receipts explicitly showing a route from GRU's headquarters to the airport. We could easily identify 305 of them simply by the address they had registered their cars at, not to mention Badin himself registered his vehicle to the official address of his GRU unit.

The most surreal absence of *"practice-what-you-breach"* among GRU hackers might be visible in their lackadaisical attitude to their own cyber protection. In 2018, a large collection of hacked Russian mail accounts, including user name and passwords, was dumped online. Dmitry Badin's email — which we figured out from his Skype account, which we in turn obtained from his phone number, which we of course got from his car registration — had been hacked. He had apparently been using the password *Badin1990*. After this, his email credentials were leaked again as part of a larger hack, where we see that he had changed his password from *Badin1990* to the much more secure *Badin990*.