Behind the hack-and-leak scandal in Poland

vsquare.org/behind-the-hack-and-leak-scandal-in-poland/

Anna Gielewska 19.03.2022

There were over 60,000 emails in Michał Dworczyk's hacked mailbox. We have new evidence that UNC1151, a group related to the Belarusian government and serving a "Ghostwriter" operation in Russia's interest, is behind the attack.

FRONTSTORY.PL has reasons to believe that attackers may still have a vast amount of sensitive data from VIPs' emails up their sleeves.

This article was originally published in Polish on FRONTSTORY.PL

Since June 2021, all of Poland has been reading the contents of Michał Dworczyk's mailbox, right-hand man of Prime Minister Mateusz Morawiecki. The Polish government consistently plays down the importance of the breach, even though it exposed poor defense against cyber-attacks, and negligence on the part of politicians when it comes to sharing sensitive data. Dworczyk's emails uncover the backstage of Mateusz Morawiecki's administration – strategic decisions made with PR in mind, government media treated as useful tools, defamatory campaigns aimed against specific groups.

Key to Dworczyk's mailbox

We covered the multi-layered operation called "Ghostwriter", with trails leading to Belarus and Russia, almost a year ago on vsquare.org and tvn24.pl. Since then, we have been investigating its consecutive phases, trying to establish what goes on behind the scenes.

In one of the recent publications, we described how one of the phishing emails sent by attackers opened the door to Dworczyk's mailbox. Phishing is a form of fraud – a criminal pretends to be somebody else or an entity (i.e. email service provider), in order to trick the recipient and obtain credentials.

After publishing that story, we asked Marcin Siedlarz, an expert from Mandiant, an international company specializing in cyber-security, for additional analysis of data from a phishing email.

His conclusions? – The message was sent from an IP address used previously in other confirmed attacks by the UNC1151 group. This attribution is made with high confidence – assesses Siedlarz.

And what that means? We can assume with high probability, the attack on Dworczyk's mailbox was carried out by Belarusian hackers, who also serve a multi-layered cyber-espionage operation called "Ghostwriter". In cyber-security terminology "attribution" means accrediting a specific hacker group with a particular cyber attack.

Mandiant is one of the biggest companies assessing cyber-threats. In November 2021 report, its analysts revealed that members of hacker group UNC1151, who are responsible for attacks on people and institutions in Ukraine, Lithuania, Latvia, Poland, and Germany, and provide technical support for the "Ghostwriter" campaign, operate from Minsk, Belarus.

"UNC1151 provides technical support to the Ghostwriter information operations campaign, and is linked to the Belarusian government," stated the report. According to analysts, "Belarus is also likely at least partially responsible for the Ghostwriter campaign." The experts didn't rule out Russian contribution to the attacks, or its influence.

Now, we have also a confirmed link between the so-called Dworczyk Leaks and UNC1151 activities.

So what links "Ghostwriter" operation and disinformation attacks consistent with Kremlin agenda, with activities of a hacker group that is directly tied to Belarusian special services?

There are few possible answers. It is likely that UNC1151 is one of the groups providing technical support for a multi-layered Russian operation. Even more so, since UNC1151 seems to emulate the GRU patterns, as we reported in August 2021. They gather information that might benefit different autonomous operations: the "Ghostwriter" campaign, official Belarusian propaganda, but also reconnaissance and intelligence operations, and even blackmail. Given Russia's war in Ukraine, it is also likely that UNC1151 works closely with Russian hacker groups, and is responsible for getting access to designated targets.

The scale of the operation conducted simultaneously in different countries, its geopolitical goals, and content distribution in the Russian-speaking social media might go way beyond the capabilities of Belarusian services. Russian involvement was also investigated by German intelligence. Series of phishing attacks aimed at Bundestag members were linked to the "Ghostwriter" operation and were attributed to GRU. At the end of October 2021, the Council of the European Union condemned Russia for the "Ghostwriter" campaign.

Hack&Leak Operation

When on 24 February Russia invades Ukraine, the website Poufna Rozmowa ("Confidential Conversation"), which has been posting Michał Dworczyk's emails for the past nine months, doesn't notice it. It continues its work as usual, publishing new screens with emails that reveal how PiS (Law and Justice) politicians and people close to Prime Minister Morawiecki do their business.

One week after the attack, a disinformation campaign focused on refugees starts. Suspicious local Facebook groups circulate false content against people of colour and non-Ukrainian refugees who cross the Polish-Ukrainian border. When Poufna Rozmowa posts a text that says: "If those savages cross into Poland, days of PiS are numbered," its connotations are obvious. In fact, it is a screen of an email from 2016, extracted from, most likely, hacked mailbox belonging to Joachim Brudziński, a politician and PiS member. Someone forwarded him at that time a group email titled: "Voices of Poles/protecting border with Ukraine."

Three days later Poufna posts the Ukrainian flag with words: "Solidarity with Ukraine."

Breach into Dworczyk's mailbox is a special case of Hack&Leak operation (we wrote about the most famous Hack&Leak operations – an attack on John Podesta, former chairman of Hilary Clinton's campaign, and attack on Emmanuel Macron – in August). It is special, because screens with emails belonging to the Chief of Chancellery, with attached photos and titles, are being dosed and spoon-fed to general public almost daily for the last nine months.

From June 2021, the contents of Dworczyk's mailbox were distributed through a Telegram channel. But it was blocked for Polish viewers in July. Few days later, on 27 July, after experimenting with other platforms (i.e. Yandex.com chat and profile on Russian social network vk.com), website Poufna Rozmowa was registered and immediately launched (the next day another website publishing military materials and documents in Russian was also launched).

We don't know who registered both websites – trail stops with a service anonymizing owners' names, in Iceland.

New Telegram channel promoting Poufna Rozmowa website has been online since August 2021. Original chat created by channel authors has 1500 members – mostly anti-vaxxer accounts.

Website posts during work hours

Our analysis shows that Poufna Rozmowa usually posts new materials from Monday to Friday during working time (6 AM to 4 PM CET). Usually, it is two screens per day. Between July 2021 and February 2022, website posted a total number of 366 entries. Monthly, it is viewed by 240,000 users (this number has been dropping in last weeks). Most traffic is made through browsers or search engines – the heaviest traffic is generated by people typing the address directly or searching words “poufna rozmowa” (“confidential conversation”), and “maile Dworczyka” “Dworczyk’s emails”).

We have found out that attackers, who hacked Dworczyk’s mailbox, might have gained access to a vast amount of materials. Dworczyk was using it for over 20 years, including periods when he served as Deputy Minister of National Defence (2017), and Chief of Chancellery. At the time of the breach, his mailbox included over 60,000 emails.

We can’t rule out the possibility that Dworczyk’s mailbox has been used by attackers as a “mother box” – a database containing private addresses of people with whom Dworczyk exchanged emails. And as such, it could serve as a reference for future phishing attacks.

We still don’t know at what phase the whole operation is right now. According to our unofficial findings, screens of emails leaked from the Chief of Chancellery’s mailbox published so far are genuine. But the content of a few attached files that were published initially on the Telegram channel has been modified. We have reported such manipulations in our previous articles.

Leaking some genuine material doesn’t mean that all screens will stay genuine in the future. The strategy called “tainted leaks” has been described by John Railton from CitizenLab (who also investigates the Pegasus scandal). Once the attackers gain public trust, they can use such credibility to publish complete false content. This threat seems even bigger now, amid Russia’s war in Ukraine.

One hundred accounts of people in power

In August 2021, shortly after the scandal broke, we reported some evidence points to “Dworczyk Leaks” being a part of bigger operation:

- Dworczyk’s email address and address of his wife (both created in wp.pl domain) were targets of phishing attacks carried out between 2020-21. Attackers hacked Facebook account belonging to Dworczyk’s wife and posted a fabricated message with a link to the Telegram channel informing about the leak. This post started “the hack-and-leak scandal.”

- content distribution in social media – creators of the Russian-speaking Telegram channel might have access to Dworczyk’s mailbox a few months before the launch of Poufna Rozmowa website and the Polish-speaking Telegram channel. Telegram channel (in Russian) was used extensively as a fuel for Belarussian propaganda, which accused Poland of organizing and funding protests in Belarus. The same content was distributed through other Russian-speaking channels.

Apart from the content of Dworczyk’s mailbox, Poufna Rozmowa posted screens from private mailboxes of Joachin Brudziński (PiS politician) and Piotr Bączek, former chief of Military Counterintelligence Service (SKW). And this means the authors of Poufna Rozmowa have, or receive from somebody else, a selected excerpt of emails from hacking attacks.

SKW is conducting a separate investigation regarding Bączek’s case but refuses to comment.

In June 2021, two weeks after the breach into Dworczyk’s mailbox was made public, Polish Internal Security Agency (ABW) informed that “at least 4350 email addresses” were attacked, and “at least 500 users responded to phishing emails (…). Among attacked addresses, over 100 belong to public figures – former and current ministers, members of parliament, senators, local government officials.”

Our investigation suggests that private addresses of Bączek and Brudziński were on the list of compromised emails mentioned in the ABW’s statement.

PiS office warns against phishing

We have followed a trail left by ABW, and asked new questions. What other mailboxes were targets and which might have been compromised? Who was informed by the police about the attacks on their mailboxes?

We have also researched the content distribution from previously known hacked accounts and cyber-attacks patterns (i.e. spoofing domains’ lists included in cyber threat reports).

Finally, we have reconstructed a partial list of attacked mailboxes. FRONTSTORY.PL has reasons to believe that apart from Dworczyk’s mailbox, attackers may have compromised private mailboxes belonging to Paweł Szrot, Chief of Cabinet of President; Mariusz Kamiński, Minister-Special Services Coordinator, and Daniel Obajtek, head of PKN Orlen, as well as few high-ranking military officials, both in active service and retired, and family members of people who died in Smolensk plane crash.

When we asked about the possible breaches (we sent emails before publication), we didn’t get any comment neither from Orlen’s press office nor from Stanisław Żaryn, spokesman of Minister-Special Services Coordinator. Paweł Szrot declined any comments on the phone.

Day after publication in the Polish media, Żaryn sent us a statement: “There is no reason to claim that anyone gained unauthorised access to the mailbox used by Mariusz Kaminski. Minister Kaminski did not open the content of any information which could have been used to compromise his mailbox. He also did not provide access passwords on sites that were used to phish for such passwords. After verification, security of the email box used by Minister Kaminski was confirmed by authorised cyber security institutions.”

Żaryn didn’t reply to our question whether Kamiński’s private email was listed among the hundred accounts belonging to the public figures mentioned in the ABW’s statement in 2021.

Why hackers choose such targets in particular? And to what purpose? How many mailboxes were they able to hack? Police and prosecutor’s office are very reluctant to answer these questions.

More forthcoming are people whose social media accounts have been used in previous one-time disinformation attacks.

Iwona Michałek, former deputy minister in the Ministry of Development, was informed about the attack by her co-workers on 12 January 2021. “I saw a post on my account, and I wasn’t the author,” told us the member of Agreement (Porozumienie) party. Hackers also gained access to her mailbox and Twitter account. “I used this address both for private and official businesses, but very seldom for the latter. I don’t think I discussed politics there. It was not linked with ministerial mailbox,” said Michałek. When she received a notification about the breach, she reported it to the police. “Soon after, me and my co-workers were questioned,” she recalled.

Three weeks later, a phishing email is sent to Bogdan Rzońca, member of EP and PiS party. “I was on a plane, flying from Brussels. I was going through my mail, and accidentally opened one of the messages with pornographic content,” said Rzońca. When he landed in Warsaw, he received a call from PiS offices. “Someone called and said that I was a target of a phishing attack, and asked if I logged to my mailbox this morning. I said yes, but I didn’t read the message,” explained Rzońca. Then, he was told a similar email was sent earlier to Marek Suski, a member of the Polish Parliament. “I was instructed to change the password,” said Rzońca. His assistant managed to block a Twitter account before attackers made use of it. Rzońca didn’t report the incident to the police or prosecutor’s office.

Prosecutor writes to Panama

Phishing attacks, if successful, allowed hackers to gain access to emails. If hacked mailboxes were linked with social media accounts, attackers could use them to post false content on Facebook and Twitter. Most often, such posts were aligned with Russian and Belarussian propaganda goals (i.e. attacks on NATO or Polish-Lithuanian relations).

Sometimes, they included links to fabricated stories posted on hacked websites belonging to local media or public institutions. We have covered these tactics and methods in our previous articles, analysing particular attacks in detail.

Similar attack was carried out on private mailbox of general Bogusław Pacek in November 2021. Attackers also hacked his Facebook and Twitter accounts, and used them to post anti-Ukrainian content. Hacked website belonging to a local media outlet was also used to spread a fabricated message supposedly written by Pacek. The title read: "Shame on our authorities! Modern-day Banderians will come to Poland."

General's private address was probably not on the ABW list, because he didn't receive any warning from the police prior to the attack. Pacek immediately informed the media about the attack. What happened after? "People from NCBC (National Center for Cyberspace Security) offered me help in retrieving my accounts. I was surprised, but they delivered on a promise. It was my old, private mailbox. I used it very seldom, so I don't think the attackers gained anything from it, apart from one-time action with an anti-Ukrainian post," said Pacek.

The attackers have used at least 25 public accounts in similar attacks thus far. They belonged to members of Parliament Marcin Duszek, Marek Suski, Arkadiusz Czartoryski, Iwona Arent, and Joanna Borowiak, Minister Marlena Maląg, Marshal of the Sejm Elżbieta Witek (all from the ruling coalition), Andrzej Melak, as well as right-wing publicists and local government officials. Some of the faked posts published in those attacks can still be found online.

Prosecutor's Office in Toruń handed the investigation of hacker attacks to the Cybercrime Department of Bydgoszcz Provincial Police Headquarters. We have asked if any real progress has been made on the case, but received an enigmatic answer suggesting only that 14 people are victims of the attacks investigated by the prosecutor's office. Prosecutors also asked German, Austrian, French, Swedish, Dutch, Spanish, Panamanian, and Indian authorities for help.

Meanwhile, separate investigation regarding Dworczyk's mailbox is being carried out by Prosecutor's Office in Warsaw. Did prosecutors manage to find out who hacked Prime Minister's aide so many months ago? "The proceedings pertinent to the case are still being carried out, which means that no charges have been filed thus far. Currently, the Prosecutor's Office is in the process of gathering evidence. Bearing the interest of the proceedings in mind, Prosecutor's Office in Warsaw will not disclose any detailed information pertaining to the findings, and any actions, performed or planned," informed us the Warsaw office.

Both offices extended their investigations for additional months.

Questions still to answer

For months, Polish security services weren’t answering key questions about the biggest cyber-espionage operation in the history of Polish politics. An operation that should have, given the dangers of information warfare, put all intelligence on high alert. Meanwhile, Polish security services compiled its report in October 2021, and closed the so-called “critical incident”, although emails leaked from Dworczyk’s mailbox are being published almost every day.

Few of the questions we have asked while researching the “Ghostwriter” operation remain unanswered: how many groups might be involved in the entire operation? In what way their actions might be coordinated? Do they cooperate or are they acting independently, “providing services” for the multi-layered cyber-operation? And finally, whether any human resources of Russian intelligence in Poland might be involved?

As we stressed in previous publications, the immediate goal of such attacks is to cause confusion, chaos, and incite negative emotions through sensitive topics. Attacks may also have another aspect – they are used for testing reactions, coverage, infrastructure, and even for profiling or blackmailing specific targets.

UNC1151 attacks Ukraine

On 27 February, Facebook published a report, informing about the increased “Ghostwriter” activity in Ukrainian internet, and the attacks carried out mostly against military officials and public figures. “Ghostwriter typically targets people through email compromise and then uses that to gain access to their social media accounts and post disinformation,” wrote the authors of the report. “We detected attempts to target people on Facebook to post YouTube videos portraying Ukrainian troops as weak and surrendering to Russia, including one video claiming to show Ukrainian soldiers coming out of a forest while flying a white flag of surrender.”

Ukrainian CERT warned about mass phishing attacks and increased activity of UNC1151 group in Ukrainian internet even before the invasion. “The Minsk-based group ‘UNC1151’ is behind these activities. Its members are officers of the Ministry of Defence of the Republic of Belarus,” informed CERT-UE. “Besides Ukrainian and Polish targets, the group is attacking Belarusians.”

On 25 February, CERT-UA posted an additional message on Facebook with a list of domains used in attacks.

Analysts from Proofpoint informed that cyber-attackers used hacked mailboxes belonging to Ukrainian military officials to send fabricated messages to “target European government personnel involved in managing the logistics of refugees fleeing Ukraine” in order to trick them into downloading malicious software. According to Proofpoint, this time the goal was “to gain intelligence regarding the logistics surrounding the movement of funds, supplies, and people within NATO member countries.”

Another company, Secureworks, analysed domains used in recent phishing attacks (the list was published by Ukrainian CERT, and the attacks were attributed to UNC1151 group), and found an additional domain cluster (accounts registered by “Apolen Zork” and “Radek Dominik”).

New domains, exposed during the attacks, were registered in November 2021 and afterwards. Some of them pose as Polish service providers which means that the attacks are ongoing, and aimed against military facilities in Poland.

“Let’s not talk about the scandal”

In days following the breaking of the hack-and-leak scandal, some PiS members attentively monitored the list of names and contacts leaked from Dworczyk’s mailbox. In unofficial talks, few politicians even voiced their regret for not making the “email group.” Why? The group was viewed as a circle of people closest to Prime Minister Mateusz Morawiecki. This perspective changed only after subsequent publications of Poufna Rozmowa website. Today, members of the ruling party are afraid of whose emails could be published next. Dworczyk and his aides were allegedly thinking about resigning, but preparations were put on hold due to Russia’s war in Ukraine. To this day, no one took responsibility for the scandal, or any other incident stemming from emails leaked from Dworczyk’s mailbox.

Special services and politicians of the ruling party don’t want to answer questions regarding the scandal and keep repeating statements that make chaos surrounding the so-called Dworczyk Leaks only worse.

When Krzysztof Izdebski from the Stefan Batory Foundation filed a motion to the Chancellery of the Prime Minister in February 2021, asking for disclosure of detailed information regarding the scandal, he was pointed to statements published previously by ABW. FRONTSTORY.PL team has been treated exactly the same for many months.

What motives drive the “ghost” behind this operation? The hack-and-leak scandal seems to have a broader dimension than influencing the current state of political affairs in Poland. It is rather a part of a multi-layered cyber operation aimed at destabilisation of the whole region.

We are starting a series of reports on Russian connections and influences in Poland. We have been covering major figures of pro-Kremlin propaganda, and their operations, for years on our vsquare.org and FRONTSTORY.PL websites and other media, publishing texts written by Paweł Reszka, Anna Gielewska, Pavla Holcova, Szabolsc Panyi, Konrad Szczygieł, Wojciech Cieśla, and many more. In 2016-21, we have uncovered behind-the-scenes actions of Alexander Usovski, Bela Kovacs and Mateusz Piskorski. We have exposed the gears of pro-Kremlin propaganda machine, its disinformation operations, and assets accumulated in Poland and Central Europe. We have watched closely, how radical groups and organizations act, including the arson attack on cultural center in Uzhorod. In 2019, we have uncovered the assets and modus operandi of Russian bank operating in Visegrád countries.

Below, you'll find a list of selected articles on Russian connections and influences (in English).

Putin's Orchestra: The Supporter, 10.03.2022

Travel Agency "Eye of Sauron", 4.08.2021

The Ghostwriter Scenario, 13.08.2021

Privet, You Have Just Been Hacked, 30.03.2021

The Nuclear Influence. How Russia Acts on the Central European Energy Market, 20.03.2020

Russia-Related Accounts and Cyberattack in Poland, 9.05.2020

Inland, Though Offshore. How Russia Planned to Secure Its Money, 3.08.2019

Elections under the Polish and Russian Watchful Eyes,30.08.3019

Budapest. A Welcoming Gateway to Europe for a Russian Bank, 18.07.2019

Make Spain Great Again, 26.04.2019

German Politician and Polish Nationalists in the Kremlin's Service, 22.04.2019

Poland's New Minister: Nationalist, Supporter of Russia, 7.01.2019

Nuclear Lobbyists, Judo Championship and Putin's Tricks, 15.02.2018

Target or Ally? Hungary Faces the Elections Battle, 3.04.2018

Usovsky's Network Active in Poland, 18.05.2018

Western Ukraine Burning. How Russia Sets Fire to the EU's External Border, 27.06.2018

From Internet Brigades to Troll Factories, 28.12.2017

The Dogs of War, The Dogs of Disinformation, 24.11.2017

Satan's Hand: Russian Meddling Behind Budapest's Metro Chaos, 27.10.2017

The Hunter of Russian Propaganda, 21.10 2017

Information Warfare. Journalists Are the Target, Manipulation is a Tool, 4.10.2017

The Man Who Wanted More, 14.10.2017

A Story of the Snake That Ate Its Own Tail, 4.10.2017

A Pocket Revolution Bought With Russian Money, 4.10.2017

The Great Escape of ‘KGBéla’, Hungarian MEP Accused of Spying for Russia, 4.10.2017