

Poland blames Russia for breach, theft of Polish officials' emails

bleepingcomputer.com/news/security/poland-blames-russia-for-breach-theft-of-polish-officials-emails/

Sergiu Gatlan

By

[Sergiu Gatlan](#)

- June 18, 2021
- 01:40 PM
- 0



Poland's deputy prime minister Jarosław Kaczyński says last week's breach of multiple Polish officials' private email accounts was carried out from servers within the Russian Federation.

"After reading the information provided to me by the Internal Security Agency and the Military Counterintelligence Service, I inform you that the most important Polish officials, ministers, and deputies of various political options were subject to a cyber attack," Kaczyński said in a statement published today.

"The analysis of our services and the secret services of our allies allows us to clearly state that the cyber attack was carried out from the territory of the Russian Federation. Its scale and range are wide."

Polish security services' investigation is still ongoing, with evidence of the email hacking incident being collected.

"On Friday, Poland handed over to the EU Member States, the European Commission and the Council a document on the details of cyber attacks carried out in recent days," an EU diplomat with knowledge of the incident told [Politico](#).

In all, over 30 Polish MPs, government officials, and journalists were impacted by the attacks that began last year, in September.

The "operational and technical analysis carried out by Polish national cybersecurity incident response teams confirmed that the infrastructure and modus operandi used during cyberattacks were the same as those used by Russian-sponsored entities," the EU diplomat added.

Polish officials' emails stolen and leaked on Telegram

Today's statement comes after Michał Dworczyk, the Head of the Polish Prime Minister's Office, said on June 9th that unknown attackers breached his email account.

At the time, Polish media reported that emails from government officials' private mailboxes were stolen and leaked on a Telegram channel, according to [Reuters](#).

"In connection with the reports of hacking into my email and my wife's mailbox, as well as our social media accounts, the relevant state services were informed," Dworczyk [said](#) in a statement.

"Currently, I cannot say when exactly my email account was successfully hacked, but I would like to emphasize once again that I did not use it to send any information that could pose a threat to state security," he [added](#) two days later.

Ongoing Russian cyber-espionage activity

The Microsoft Threat Intelligence Center (MSTIC) said one month ago that the Russian-backed hackers behind the SolarWinds supply-chain attack are now coordinating a large-scale [phishing campaign targeting government agencies worldwide](#).

"This wave of attacks targeted approximately 3,000 email accounts at more than 150 different organizations," MSTIC researchers revealed.

"While organizations in the United States received the largest share of attacks, targeted victims span at least 24 countries."

The US govt also [warned of continued cyber-espionage attacks](#) in April, attacks coordinated by the Russian Foreign Intelligence Service (SVR) (aka APT29).

SVR operators target both US and foreign organizations, focusing on government networks, think tanks and policy analysis orgs, and information technology companies.

Related Articles:

[Russian hackers perform reconnaissance against Austria, Estonia](#)

[Russian govt impersonators target telcos in phishing attacks](#)

[T-Mobile confirms Lapsus\\$ hackers breached internal systems](#)

[GitHub: Attackers stole login details of 100K npm user accounts](#)

[Google shut down caching servers at two Russian ISPs](#)