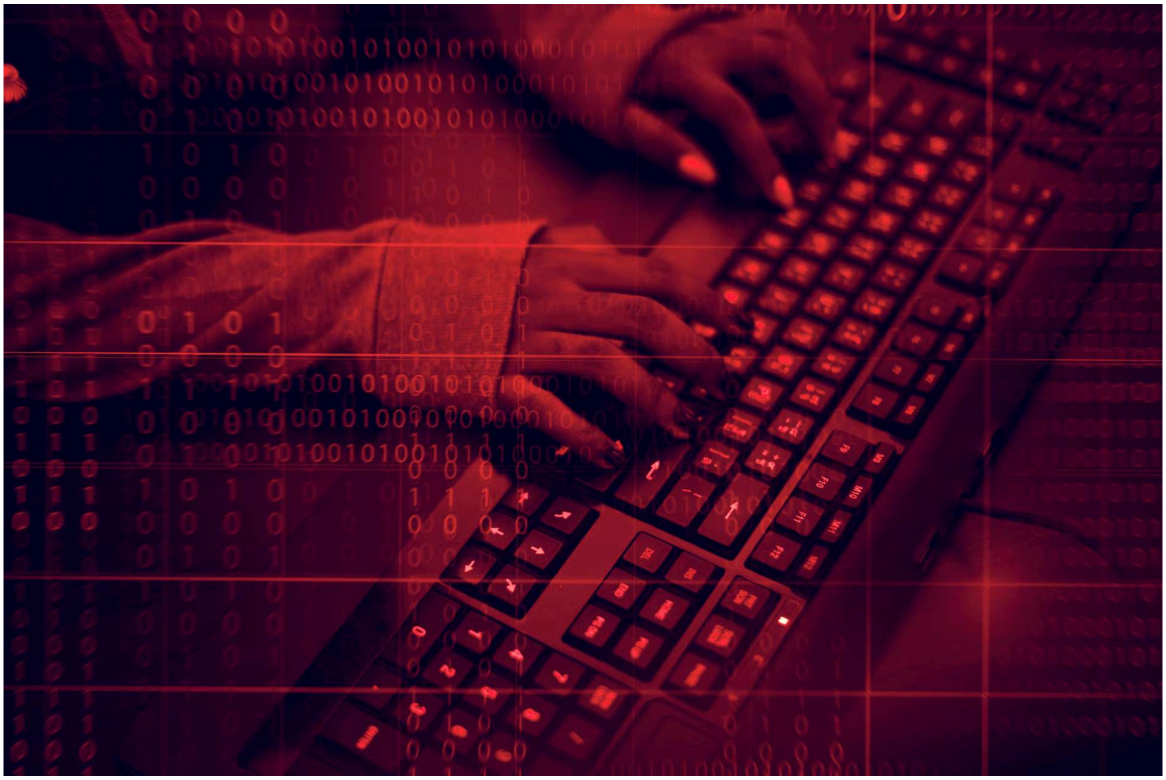
Russia’s ‘Ghostwriter’ hacker group takes aim at German election

www.politico.eu/article/russia-brash-hackers-turn-to-german-election/

21 September 2021

1. News
2. Technology

A group with ties to Moscow’s intelligence is provoking European countries to respond to cyberattacks.



The EU’s cybersecurity agency released a warning saying they had "reported a substantial increase of cybersecurity threats for both private and public organisations across the EU | Image via iStock

September 21, 2021 9:48 am CET

By Laurens Cerulus and Liv Klingert

If Russian hackers have their way, the German election could serve up a "September surprise."

Having disrupted democratic processes in Lithuania, Latvia and Poland, a young, brazen hacking group linked to the Kremlin has now zoned in on Europe's biggest country, which goes to the polls this week, in a hugely consequential test of the bloc's ability to stop Russian aggressors blatantly targeting its political process.

Germany's foreign ministry called out the Russian state this month for being behind a hacking campaign targeting members of its federal parliament and regional parliaments with fake emails — in apparent attempts to hack into confidential information that can be used to destabilize or tilt the election.

"A number of [member of parliament] accounts have been targeted," a foreign office spokesperson said, linking the campaign "to cyber actors of the Russian State, more specifically to the military intelligence agency GRU." The German government "will also work with our partners towards a joint European response," the spokesperson said.

It's unclear what information if any the Russian hackers were able to obtain from German officials. German officials declined to comment on whether the hack was successful. Other operations led by the Ghostwriter group have led to highly damaging leaking campaigns, including one that riled Poland's political class for months.

The attackers, known for running disinformation campaigns by the name of "Ghostwriter," are not new to cybersecurity authorities on the Continent. They've managed to sow distrust and confusion several times across countries by hacking politicians and news organizations, and spreading false information on websites, social media and email.

The hackers' pivot to target Europe's biggest election shows the group is growing more powerful and more bullish in their efforts to disrupt European politics — with experts saying it could soon pop up in the U.S. and is already targeting French officials too.

Bigger targets

The group started its attacks on German politicians as early as March, sending fake emails posing as email providers GMX and Deutsche Telekom's T-Online to take over email accounts for "further use," according to a letter seen by German magazine Der Spiegel.

Just before the summer it also hacked Polish politicians, triggering a national political scandal over leaked private emails of top officials including Prime Minister Mateusz Morawiecki.
The group in recent years also targeted the Baltics, attacking politicians and media companies in Lithuania, Latvia and the military alliance NATO with "phishing" emails to steal sensitive data like usernames and passwords, posting false stories on news sites they hacked and spreading disinformation over email.

The Ghostwriter attacks are "a really elegant combination of cyberattacks using methodologies to socially-engineer users through phishing attempts and emails that are well-constructed to get people to click," said Karim Hijazi, chief executive of Prevailion, a U.S. cybersecurity firm that mapped the hackers' infrastructure in a recent report.

GERMANY NATIONAL PARLIAMENT ELECTION POLL OF

POLLS

All 3 Years 2 Years 1 Year 6 Months Smooth Kalman

For more polling data from across Europe visit POLITICO *Poll of Polls.*
The group doesn't exploit software glitches and vulnerabilities like other hackers. Instead, it specializes in deceiving officials to obtain access to compromising information and then leaking it to the press, as well as spreading disinformation.

"It's highly personal. The level of research we found somewhat unique, in that they were extremely clear on who their targets were, the political people they were after," Hijazi said, adding the group's recent attacks "looked really well-funded."

Last year, hackers circulated a forged letter that looked like it was from NATO Secretary-General Jens Stoltenberg claiming that the defense alliance was withdrawing its forces from Lithuania due to the coronavirus. "Fake news like this piece are aimed at sowing distrust in our alliance partners and NATO unity," the Lithuania's then-Minister of Defense Raimundas Karoblis said at the time.

Cybersecurity firm FireEye in April linked parts of the Ghostwriter attacks to a group called UNC1151, affiliated with the Russian military intelligence service. The attacks in Lithuania showed the group was openly pushing disinformation in Russia's favor. In the recent attacks in Poland and Germany, the group has grown into a serious threat that likely to move on to target the U.S. and other countries too. It already targeted French ministry of defense officials, Prevailion found.

Sanctions track record

Germany can call on other EU countries to jointly sanction Russian individuals and services thought to be responsible for cyberattacks with asset freezes and travel bans.

The EU placed the first of such sanctions on high-profile Russian, Chinese and North Korean groups in July 2020. At the request of the German government, it also sanctioned Russia's GRU officials in October 2020 for hacking its national parliament in 2015.

The spurt of increasingly sophisticated attacks on Europe have prompted Germany to call for a "joint European response" to Russia's cyber aggressions.

Countries already plagued with attacks by the Russian hacker group support the idea. Lithuania's Vice-minister of National Defence Margiris Abukevičius said the bloc "must make use of measures [available to the EU] and send a strong signal to the threat actor that such behavior in cyberspace is unacceptable and will bear consequences, including possible application of cyber sanctions."

The attacks have also emboldened European officials to speak up. Margaritis Schinas, who oversees EU security policy, told POLITICO earlier this month: "It's: You come after us, we come after you." "On these kinds of incidents, Europe is much better prepared now than it used to be," he said, stressing it's up to member countries to ask for EU support first.

An EU Commission spokesperson said "we are in contact with Germany and Poland and express our solidarity to the victims of this malicious cyber activity," The spokesperson would not speculate about possible sanctions targeting the Ghostwriter campaign, saying "it will be for the Council to decide by unanimity."