EU officially blames Russia for 'Ghostwriter' hacking activities

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** September 24, 2021 12:11 PM **0**

Image: Christian Lue (https://unsplash.com/@christianlue)

The European Union has officially linked Russia to a hacking operation known as Ghostwriter that targets high-profile EU officials, journalists, and the general public.

"These malicious cyber activities are targeting numerous members of Parliaments, government officials, politicians, and members of the press and civil society in the EU by accessing computer systems and personal accounts and stealing data," European Council officials said in a press release (https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/) today.

"Such activities are unacceptable as they seek to threaten our integrity and security, democratic values and principles and the core functioning of our democracies."

The EU officials added that these hacking activities are in stark contrast to normal state behavior endorsed by all UN member states.

The attacks are also seen as clear attempts to undermine EU's democratic institutions and processes, including but not limited to enabling disinformation and information manipulation.

Linked to Russia's GRU military intelligence service

The Ghostwriter "malicious cyber activities" were also connected by Germany to the GRU military intelligence service earlier this month (https://www.dw.com/en/germany-warns-russia-over-cyberattacks-ahead-of-election/a-59101191), with German Foreign Ministry spokeswoman Andrea Sasse saying that the German parliament was targeted at least three times this year.

Sasse's statement came after German security authorities detected multiple attempts to steal personal login details of German lawmakers before the September 26 federal election, likely as part of a preparation effort for disinformation campaigns

"The German government has reliable information on the basis of which Ghostwriter activities can be attributed to cyber actors of the Russian state and, specifically, Russia's GRU military intelligence service," Sasse said.

In March, Germany also said that the Ghostwriter Russian military intelligence hacking group is the main suspect behind a spearphishing attack that targeted multiple Parliament members (https://www.bleepingcomputer.com/news/security/german-parliament-targeted-again-by-russian-state-hackers/).

They are believed to have breached the email accounts of seven members of the German federal parliament (Bundestag) and 31 members of German regional parliaments.

"The European Union and its Member States strongly denounce these malicious cyber activities, which all involved must put to an end immediately. We urge the Russian Federation to adhere to the norms of responsible state behaviour in cyberspace," the European Council added today.

"The European Union will revert to this issue in upcoming meetings and consider taking further steps."

Who is Ghostwriter?

Ghostwriter (https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html) has been coordinating "information operations," pushing various narratives aligned with Russian security interests beginning with March 2017, according to a 2020 report from cybersecurity firm FireEye.

These attacks continued through 2021, with FireEye identifying over twenty additional incidents (https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/unc1151-ghostwriter-update-report.pdf) believed to be part of Ghostwriter activity.

"The Ghostwriter campaign leverages traditional cyber threat activity and information operations tactics to promote narratives intended to chip away at NATO's cohesion and undermine local support for the organization in Lithuania, Latvia, and Poland," FireEye said.

This hacking group used fabricated personas posing as analysts and journalists to target Lithuanian, Latvian, and Polish audiences with anti-North Atlantic Treaty Organization (NATO) narratives disseminated via spoofed email accounts and compromised websites.

APT28 members sanctioned for a similar attack

The Council of the European Union also sanctioned multiple members of the Russian state-backed APT28 hacking group (https://www.bleepingcomputer.com/news/security/eu-sanctions-russian-

hackers-over-2015-german-parliament-attack/) in October 2020 for compromising several Bundestag members' email accounts in 2015.

The same month, the US Cyber Command also shared info on malware implants (https://www.bleepingcomputer.com/news/security/us-shares-info-on-russian-malware-used-to-target-parliaments-embassies/) used by Russian state hackers in attacks targeting national parliaments, ministries of foreign affairs, and embassies.

In August 2020, Norway disclosed a strikingly similar attack that led to the breach of email accounts belonging to Norwegian Parliament (https://www.bleepingcomputer.com/news/security/hackers-breached-norwegian-parliament-emails-to-steal-data/) representatives and employees.

Norway's Minister of Foreign Affairs Ine Eriksen Søreide revealed that the August attack (https://www.bleepingcomputer.com/news/security/norway-says-russian-hackers-were-behind-august-parliament-attack/) was coordinated by Russian state hackers who stole data from each of the hacked accounts and the Norwegian Police Security Service said APT28 was likely behind the operation (https://www.bleepingcomputer.com/news/security/norway-russian-apt28-state-hackers-likely-behind-parliament-attack/).

In February 2021, the National Security and Defense Council of Ukraine (NSDC) also linked Russian-backed state hackers to an attack against the Ukrainian government (https://www.bleepingcomputer.com/news/security/russian-hackers-linked-to-attack-targeting-ukrainian-government/) attempting to breach state agencies after compromising the government's document management system.

Related Articles:

German Parliament targeted again by Russian state hackers (https://www.bleepingcomputer.com/news/security/german-parliament-targeted-again-by-russian-state-hackers/)

WhatsApp to appeal $266 million fine for violating EU privacy laws (https://www.bleepingcomputer.com/news/security/whatsapp-to-appeal-266-million-fine-for-violating-eu-privacy-laws/)

US sanctions cryptocurrency exchange used by ransomware gangs (https://www.bleepingcomputer.com/news/security/us-sanctions-cryptocurrency-exchange-used-by-ransomware-gangs/)

Russian state hackers use new TinyTurla malware as secondary backdoor (https://www.bleepingcomputer.com/news/security/russian-state-hackers-use-new-tinyturla-malware-as-secondary-backdoor/)

Autodesk reveals it was targeted by Russian SolarWinds hackers (https://www.bleepingcomputer.com/news/security/autodesk-reveals-it-was-targeted-by-russian-solarwinds-hackers/)