Russian hackers sanctioned by European Council for attacks on EU and Ukraine

By Alexander Martin

Published: 2024-06-24 · Archived: 2026-04-05 18:32:05 UTC

Six hackers who have previously been connected to either Russian state-sponsored or financially motivated cyberattacks targeting the European Union and Ukraine were added to the EU's sanctions list on Monday.

The move marks the bloc's growing use of its so-called "Cyber Diplomacy Toolbox" which attempts to discourage cyberattacks against member states. Despite similar coordinated actions by Western states in recent years, these measures do not obviously appear to have impacted the volume and impact of Russian cyberattacks.

The EU's sanctions require all funds and economic resources within EU member states controlled by the listed individuals to be frozen. The sanctions also prevent any funds or economic resources being made to the sanctioned entities — although EU member states are allowed to make exceptions.

Four of the individuals added to the Council's list are Russian nationals currently covered by existing sanctions imposed by the United States and United Kingdom. Ruslan Peretyatko, Andrey Korinets, Mikhail Tsarev and Maksim Galochkin all currently face charges in the U.S. for alleged cybercrimes.

However two others, Oleksandr Sklianko and Mykola Chernykh, have not been publicly charged in the United States. The pair were first alleged to be officers in the counterintelligence branch of Russian Federal Security Service (FSB) operating from occupied Crimea back in 2021, by the Ukrainian Security Service (SSU).

According to the SSU, the pair are connected to a hacking group tracked as Armageddon or Gamaredon. The European Council's sanctions accuse them of conducting cyberattacks "with a significant impact on the governments of EU member states and Ukraine, including by using phishing emails and malware campaigns."

There are discrepancies between the European Council's sanctions against Peretyatko and Korinets and those of the United States and United Kingdom. When the Department of Justice charged the pair with targeting U.S. government and military officials as part of the Callisto Group hacking campaign — also aimed at the United Kingdom, Ukraine and NATO — it identified them as working for the FSB.

The European Council instead identified the Callisto Group as "a group of Russian military intelligence officers," which would typically be understood to mean a separate agency in Russia, the GRU. A spokesperson for the European Council did not respond to clarify whether the discrepancy was an error on the Council's part or due to a genuine difference in assessment.

The sanctions against Tsarev and Galochkin are the first the European Council has made against alleged criminal hackers. The pair were among 11 individuals sanctioned by the United States and United Kingdom last year for their roles in a criminal group behind the Trickbot malware and Conti ransomware schemes.

What's the point of sanctions?

The effectiveness of cyber sanctions in deterring malicious hacking, as deployed by the European Union, has been questioned. Law enforcement agencies in the United States and United Kingdom have told Recorded Future News that they view sanctions more as an operational tactic than as a direct mechanism for tackling attackers' finances.

As revealed by Recorded Future News earlier this year, the agency responsible for monitoring cyber sanctions in Britain has never detected an illicit payment to an entity embargoed under the country's counter-ransomware regime.

Multiple operational sources involved in the fight against ransomware said that the fact missed the true use that law enforcement is putting the sanctions to, which is not simply about frustrating the payments.

While officials in Britain "assessed that sanctions have hampered the ability of cyber threat actors to monetise their cyber criminal activities," more significantly law enforcement agencies deployed sanctions because they "contributed to sowing discord within certain groups."

In particular, naming previously anonymous cybercriminals undermines their operational security and adds stress to potential relationships between them and colleagues, as well as with corrupt officials in jurisdictions such as the Russian Federation where they may be expected to provide kickbacks or to receive tasking from the security services.

Choosing who to sanction also offers flexibility for a range of covert actions. Keeping a name off of the sanctions list can allow suspects a false sense of security to travel abroad if an arrest is planned, or it can provide leeway if a suspect is cooperating, officials have told Recorded Future News. A sense of injustice between those who have been sanctioned and any co-conspirators left off the list can also cause divisions within the organized crime groups.

Last June, the European Council agreed that new measures were needed to strengthen its Cyber Diplomacy Toolbox to "increase the EU's ability to prevent, discourage, deter and respond to malicious cyber activities."

No previous article

No new articles

Alexander Martin

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79
