US charges 4 Russian govt employees with critical infrastructure hacks

By Sergiu Gatlan

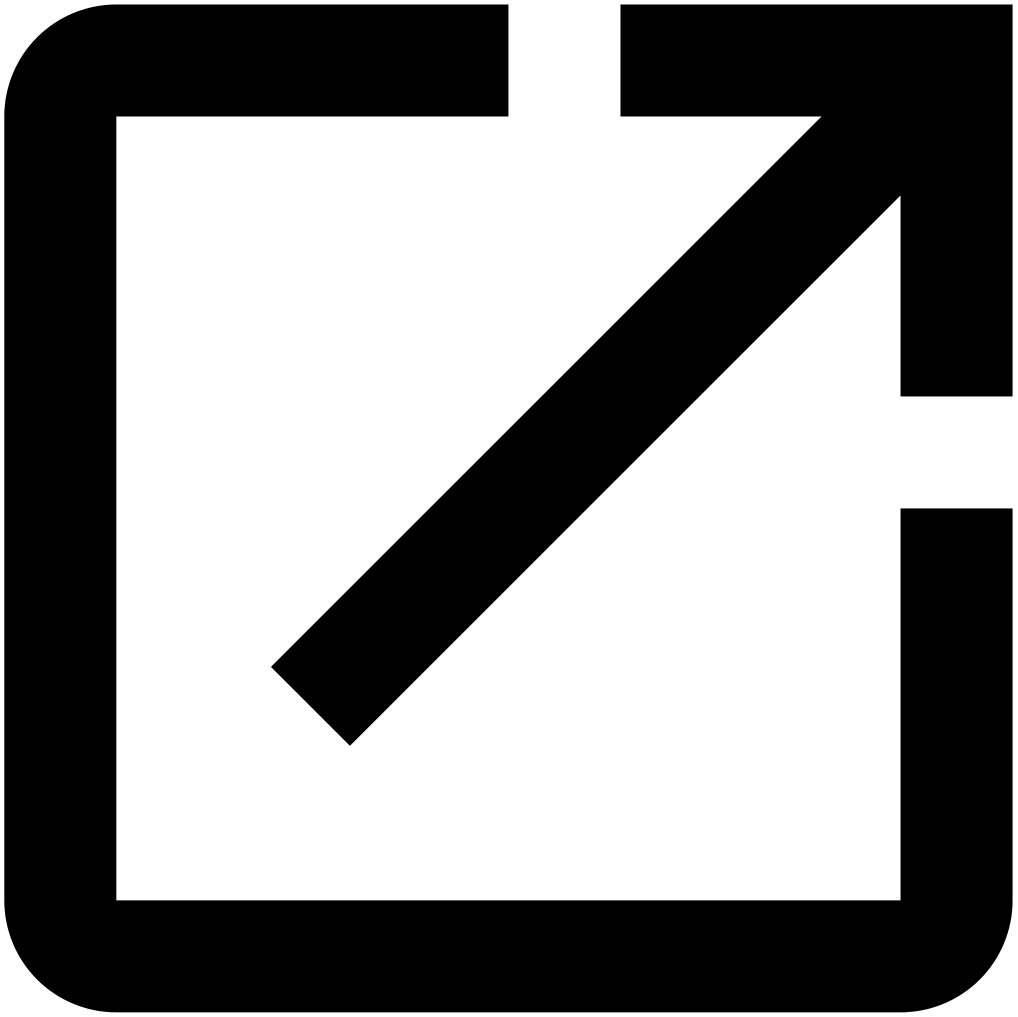
Published: 2022-03-24 · Archived: 2026-04-05 14:22:50 UTC

The U.S. has indicted four Russian government employees for their involvement in hacking campaigns targeting hundreds of companies and organizations from the global energy sector between 2012 and 2018.

"In total, these hacking campaigns targeted thousands of computers, at hundreds of companies and organizations, in approximately 135 countries," the Department of Justice said.

The Department of Justice unsealed two indictments on Thursday, one from June 2021 and one from August 2021, charging one employee of the Russian Federation Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) and three officers of Russia's Federal Security Service (FSB).


DIE LINKE.
0:00



Evgeny Viktorovich Gladkikh, a computer programmer at TsNIIKhM, and co-conspirators were behind attacks that caused two emergency shutdowns at a Middle East-based refinery facility between May and September 2017.

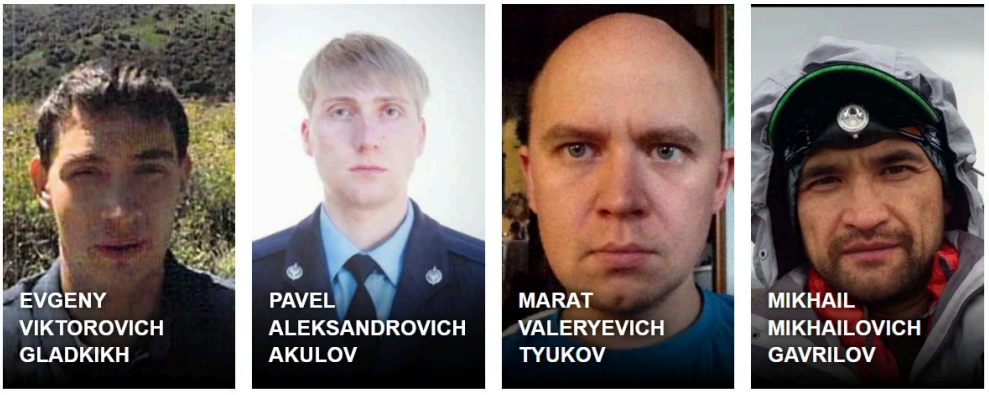
They did that by hacking the refinery's systems and installing malware known as Triton or Trisis on Schneider Electric Triconex Tricon PLCs used by safety systems.

The malware infects the Triconex Tricon PLCs by modifying in-memory firmware, which allowed the attackers to add additional programming and control the compromised systems remotely.

Subsequently, the group also tried to hack into the systems of a U.S. refinery between February and July 2018.

Pavel Aleksandrovich Akulov, Mikhail Mikhailovich Gavrilov, and Marat Valeryevich Tyukov, the ones charged in August 2021, were officers in Military Unit 71330 or 'Center 16' of the FSB.

They were also part of a hacking group tracked under multiple names, including Dragonfly, Berzerk Bear, Energetic Bear, and Crouching Yeti.



Wanted posters (FBI)

The FSB "Dragonfly" hacking campaigns

Between 2012 and 2017, the three FSB hackers and their team were behind multiple breaches and supply chain attacks targeting ICS or Supervisory Control and Data Acquisition (SCADA) systems used in the international energy sector, including oil and gas firms, nuclear power plants, as well as utility and power transmission companies.

In the first campaign, which took place between 2012 and 2014 and is known as Dragonfly or Havex, they infiltrated the networks of multiple ICS/SCADA system manufacturers and software providers and infected legitimate software updates with the Havex remote access Trojan (RAT).

Together with spearphishing and "watering hole" attacks, this supply chain attack enabled them to infect more than 17,000 unique devices in the United States and worldwide with malware.

Between 2014 and 2017, as part of the Dragonfly 2.0 campaign, they switched to spearphishing attacks and targeted over 3,300 users at more than 500 U.S. and international companies and entities, including U.S. government agencies such as the Nuclear Regulatory Commission.

"Russian state-sponsored hackers pose a serious and persistent threat to critical infrastructure both in the United States and around the world," said Deputy Attorney General Lisa O. Monaco.

"Although the criminal charges unsealed today reflect past activity, they make crystal clear the urgent ongoing need for American businesses to harden their defenses and remain vigilant."

CISA, the FBI, and the U.S. Department of Energy also published a joint cybersecurity advisory detailing the state-sponsored Russians' hacking campaigns targeting the U.S. and international Energy Sector, including oil refineries, nuclear facilities, and energy companies.

The U.S. Department of State is offering a reward of up to $10 million for any information leading to the identification or location of state-sponsored Russian hackers targeting U.S. critical infrastructure.

Source: https://www.bleepingcomputer.com/news/security/us-charges-4-russian-govt-employees-with-critical-infrastructure-hacks/