

Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide

Published: 2022-03-24 · Archived: 2026-04-06 15:39:39 UTC

The Department of Justice unsealed two indictments today charging four defendants, all Russian nationals who worked for the Russian government, with attempting, supporting and conducting computer intrusions that together, in two separate conspiracies, targeted 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.

A June 2021 indictment returned in the District of Columbia, *United States v. Evgeny Viktorovich Gladkikh*, concerns the alleged efforts of an employee of a Russian Ministry of Defense research institute and his co-conspirators to damage critical infrastructure outside the United States, thereby causing two separate emergency shutdowns at a foreign targeted facility. The conspiracy subsequently attempted to hack the computers of a U.S. company that managed similar critical infrastructure entities in the United States.

An August 2021 indictment returned in the District of Kansas, *United States v. Pavel Aleksandrovich Akulov, et al.*, details allegations about a separate, two-phased campaign undertaken by three officers of Russia's Federal Security Service (FSB) and their co-conspirators to target and compromise the computers of hundreds of entities related to the energy sector worldwide. Access to such systems would have provided the Russian government the ability to, among other things, disrupt and damage such computer systems at a future time of its choosing.

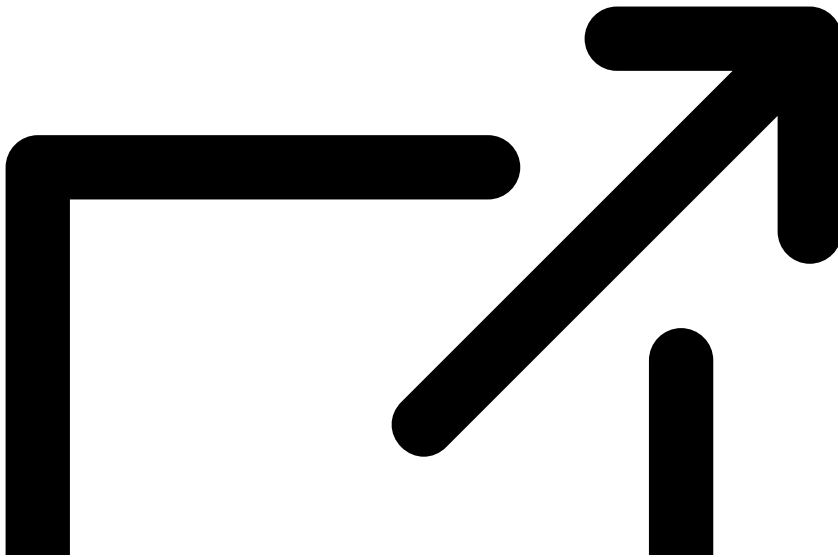
"Russian state-sponsored hackers pose a serious and persistent threat to critical infrastructure both in the United States and around the world," said Deputy Attorney General Lisa O. Monaco. "Although the criminal charges unsealed today reflect past activity, they make crystal clear the urgent ongoing need for American businesses to harden their defenses and remain vigilant. Alongside our partners here at home and abroad, the Department of Justice is committed to exposing and holding accountable state-sponsored hackers who threaten our critical infrastructure with cyber-attacks."

"The FBI, along with our federal and international partners, is laser-focused on countering the significant cyber threat Russia poses to our critical infrastructure," said FBI Deputy Director Paul Abbate. "We will continue to identify and quickly direct response assets to victims of Russian cyber activity; to arm our partners with the information that they need to deploy their own tools against the adversary; and to attribute the misconduct and impose consequences both seen and unseen."

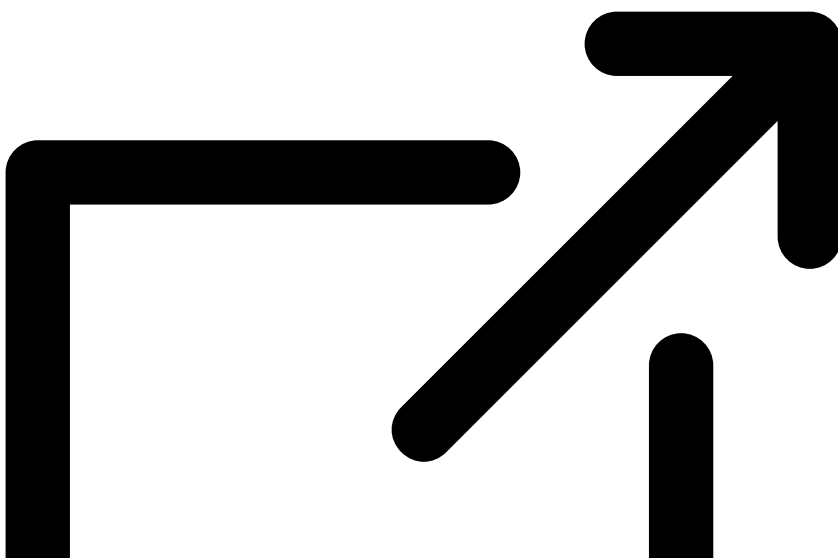
"We face no greater cyber threat than actors seeking to compromise critical infrastructure, offenses which could harm those working at affected plants as well as the citizens who depend on them," said U.S. Attorney Matthew M. Graves for the District of Columbia. "The department and my office will ensure that those attacking operational technology will be identified and prosecuted."

“The potential of cyberattacks to disrupt, if not paralyze, the delivery of critical energy services to hospitals, homes, businesses and other locations essential to sustaining our communities is a reality in today’s world,” said U.S. Attorney Duston Slinkard for the District of Kansas. “We must acknowledge there are individuals actively seeking to wreak havoc on our nation’s vital infrastructure system, and we must remain vigilant in our effort to thwart such attacks. The Department of Justice is committed to the pursuit and prosecution of accused hackers as part of its mission to protect the safety and security of our nation.”

In addition to unsealing these charges, the U.S. government is taking action to [enhance private sector network defense efforts](#)



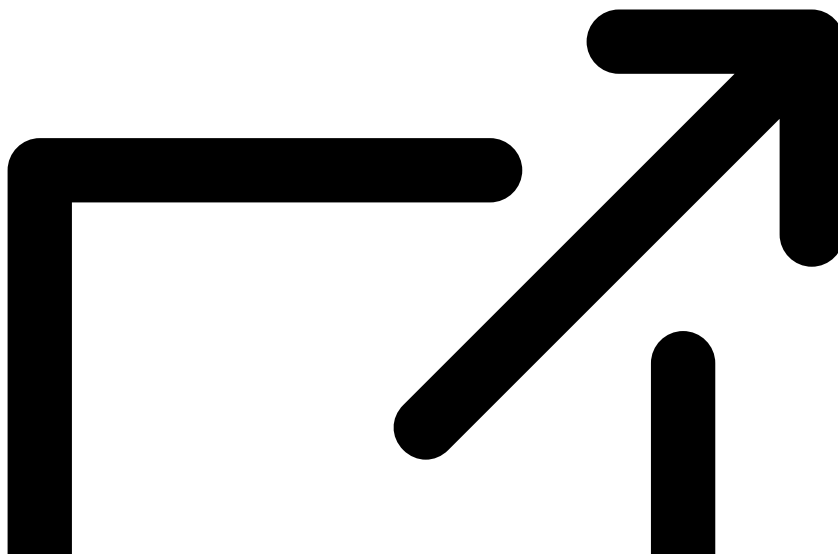
and [disrupt similar malicious activity](#).



The Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) has already released numerous Technical Alerts, ICS Alerts and Malware Analysis Reports regarding Russia’s malign cyber

activities, including the campaigns discussed in the indictments. These are located at:

<https://www.cisa.gov/shields-up>



1. *United States v. Evgeny Viktorovich Gladkikh – defendant installed backdoors and launched malware designed to compromise the safety of energy facilities*

In June 2021, a federal grand jury in the District of Columbia returned an indictment charging Evgeny Viktorovich Gladkikh (Евгений Викторович Гладких), 36, a computer programmer employed by an institute affiliated with the Russian Ministry of Defense, for his role in a campaign to hack industrial control systems (ICS) and operational technology (OT) of global energy facilities using techniques designed to enable future physical damage with potentially catastrophic effects.

According to the indictment, between May and September 2017, the defendant and co-conspirators hacked the systems of a foreign refinery and installed malware, which cyber security researchers have referred to as “Triton” or “Trisis,” on a safety system produced by Schneider Electric, a multinational corporation. The conspirators designed the Triton malware to prevent the refinery’s safety systems from functioning (*i.e.*, by causing the ICS to operate in an unsafe manner while appearing to be operating normally), granting the defendant and his co-conspirators the ability to cause damage to the refinery, injury to anyone nearby, and economic harm. However, when the defendant deployed the Triton malware, it caused a fault that led the refinery’s Schneider Electric safety systems to initiate two automatic emergency shutdowns of the refinery’s operations. Between February and July 2018, the conspirators researched similar refineries in the United States, which were owned by a U.S. company, and unsuccessfully attempted to hack the U.S. company’s computer systems.

The three-count indictment alleges that Gladkikh was an employee of the State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics’ (Государственный научный центр Российской Федерации федеральное государственное унитарное предприятие Центральный научно-исследовательский институт химии и механики, hereinafter “TsNIIKhM”) Applied Developments Center (“Центр прикладных разработок,” hereinafter “ADC”). On its website, which was modified after the Triton attack became public, TsNIIKhM described itself as the Russian Ministry of Defense’s leading research

organization. The ADC, in turn, publicly asserted that it engaged in research concerning information technology-related threats to critical infrastructure (*i.e.*, that its research was defensive in nature).

The defendant is charged with one count of conspiracy to cause damage to an energy facility, which carries a maximum sentence of 20 years in prison, one count of attempt to cause damage to an energy facility, which carries a maximum sentence of 20 years in prison, and one count of conspiracy to commit computer fraud, which carries a maximum sentence of five years in prison.

Assistant U.S. Attorneys Christopher B. Brown and Luke Jones for the District of Columbia, in partnership with the National Security Division's Counterintelligence and Export Control Section, are prosecuting this case. The FBI's Washington Field Office conducted the investigation.

The U.S.-based targets of the conspiracy cooperated and provided valuable assistance in the investigation. The Department of Justice and the FBI also expressed appreciation to Schneider Electric for its assistance in the investigation, particularly noting the company's public outreach and education efforts following the overseas Triton attack.

2. United States v. Pavel Aleksandrovich Akulov, Mikhail Mikhailovich Gavrilov, and Marat Valeryevich Tyukov – defendants undertook years-long effort to target and compromise computer systems of energy sector companies

On Aug. 26, 2021, a federal grand jury in Kansas City, Kansas, returned an indictment charging three computer hackers, all of whom were residents and nationals of the Russian Federation (Russia) and officers in Military Unit 71330 or "Center 16" of the FSB, with violating U.S. laws related to computer fraud and abuse, wire fraud, aggravated identity theft and causing damage to the property of an energy facility.

The FSB hackers, Pavel Aleksandrovich Akulov (Павел Александрович Акулов), 36, Mikhail Mikhailovich Gavrilov (Михаил Михайлович Гаврилов), 42, and Marat Valeryevich Tyukov (Марат Валерьевич Тюков), 39, were members of a Center 16 operational unit known among cybersecurity researchers as "Dragonfly," "Berzerk Bear," "Energetic Bear," and "Crouching Yeti." The indictment alleges that, between 2012 and 2017, Akulov, Gavrilov, Tyukov and their co-conspirators, engaged in computer intrusions, including supply chain attacks, in furtherance of the Russian government's efforts to maintain surreptitious, unauthorized and persistent access to the computer networks of companies and organizations in the international energy sector, including oil and gas firms, nuclear power plants, and utility and power transmission companies. Specifically, the conspirators targeted the software and hardware that controls equipment in power generation facilities, known as ICS or Supervisory Control and Data Acquisition (SCADA) systems. Access to such systems would have provided the Russian government the ability to, among other things, disrupt and damage such computer systems at a future time of its choosing.

According to the indictment, the energy sector campaign involved two phases. In the first phase, which took place between 2012 and 2014 and is commonly referred to by cyber security researchers as "Dragonfly" or "Havex," the conspirators engaged in a supply chain attack, compromising the computer networks of ICS/SCADA system manufacturers and software providers and then hiding malware – known publicly as "Havex" – inside legitimate software updates for such systems. After unsuspecting customers downloaded Havex-infected updates, the conspirators would use the malware to, among other things, create backdoors into infected systems and scan

victims' networks for additional ICS/SCADA devices. Through these and other efforts, including spearphishing and "watering hole" attacks, the conspirators installed malware on more than 17,000 unique devices in the United States and abroad, including ICS/SCADA controllers used by power and energy companies.

In the second phase, which took place between 2014 and 2017 and is commonly referred to as "Dragonfly 2.0," the conspirators transitioned to more targeted compromises that focused on specific energy sector entities and individuals and engineers who worked with ICS/SCADA systems. As alleged in the indictment, the conspirators' tactics included spearphishing attacks targeting more than 3,300 users at more than 500 U.S. and international companies and entities, in addition to U.S. government agencies such as the Nuclear Regulatory Commission. In some cases, the spearphishing attacks were successful, including in the compromise of the business network (*i.e.*, involving computers not directly connected to ICS/SCADA equipment) of the Wolf Creek Nuclear Operating Corporation (Wolf Creek) in Burlington, Kansas, which operates a nuclear power plant. Moreover, after establishing an illegal foothold in a particular network, the conspirators typically used that foothold to penetrate further into the network by obtaining access to other computers and networks at the victim entity.

During the Dragonfly 2.0 phase, the conspirators also undertook a watering hole attack by compromising servers that hosted websites commonly visited by ICS/SCADA system and other energy sector engineers through publicly known vulnerabilities in content management software. When the engineers browsed to a compromised website, the conspirators' hidden scripts deployed malware designed to capture login credentials onto their computers.

The conspiracy's hacking campaign targeted victims in the United States and in more than 135 other countries.

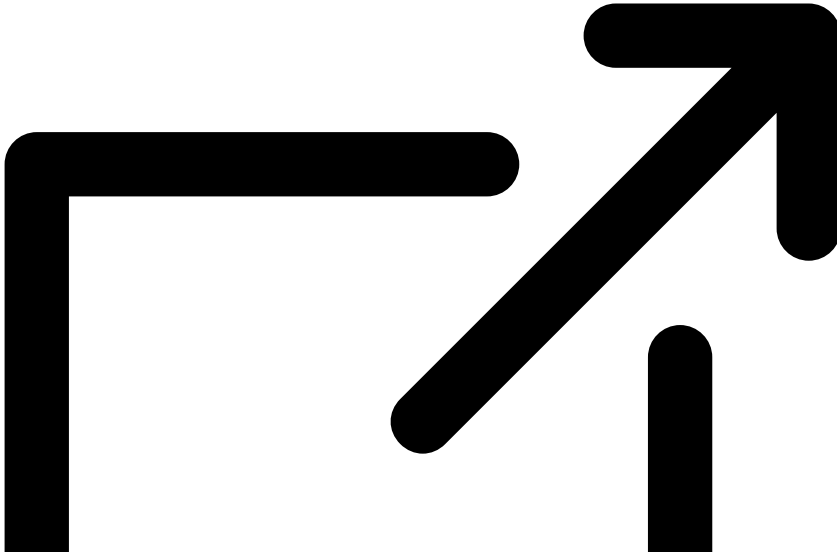
Akulov, Gavrilov and Tyukov are charged with conspiracy to cause damage to the property of an energy facility and commit computer fraud and abuse, which carries a maximum sentence of five years in prison, and conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison. Akulov and Gavrilov are also charged with substantive counts of wire fraud and computer fraud related to unlawfully obtaining information from computers and causing damage to computers. These offenses carry maximum sentences ranging from five to 20 years in prison. Finally, Akulov and Gavrilov are also charged with three counts of aggravated identity theft, each of which carry a minimum sentence of two years consecutive to any other sentence imposed.

Assistant U.S. Attorneys Scott Rask, Christopher Oakley and Ryan Huschka for the District of Kansas, and Counsel for Cyber Investigations Ali Ahmad and Trial Attorney Christine Bonomo of the National Security Division's Counterintelligence and Export Control Section are prosecuting this case. The FBI's Portland and Richmond field offices conducted the investigation, with the assistance of the FBI's Cyber Division.

Numerous victims, including Wolf Creek and its owners Evergy and the Kansas Electric Power Cooperative, cooperated and provided invaluable assistance in the investigation.

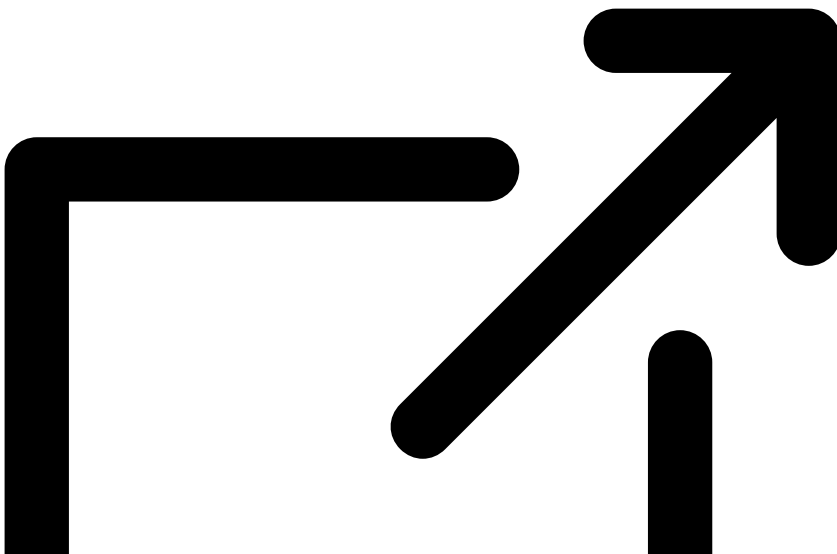
An indictment is merely an allegation and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

Note: View the concurrent announcement by the Department of State of [a \\$10 million reward](#)



for information leading to the arrest of a defendant or identification of other conspirators as part of its Rewards for Justice program.

View the concurrent announcement by the FBI, Department of Energy and Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) of a [Joint Cybersecurity Advisory](#).



containing technical details, indicators of compromise and mitigation measures.

Source: <https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical>