DOJ unseals indictments of four Russian gov't officials for cyberattacks on energy companies

By Jonathan Greig

Published: 2023-01-17 · Archived: 2026-04-05 14:19:00 UTC

The indictments of four Russian nationals were unsealed by the Justice Department on Thursday, revealing a widespread hacking campaign against energy companies around the world.

Evgeny Viktorovich Gladkikh – indicted in June – was charged with one count of conspiracy to cause damage to an energy facility, one count of attempt to cause damage to an energy facility and one count of conspiracy to commit computer fraud.

The DOJ accused the 36-year-old Gladkikh and other accomplices of using the Triton malware during attacks on a refinery's Schneider Electric safety systems between May and September 2017.

He is also accused of launching other attacks on the industrial control systems (ICS) and operational technology (OT) of global energy facilities, with the intention of physically damaging the facilities.

Gladkikh and others designed Triton – also known as Trisis – to prevent the refinery's safety systems from functioning. When he launched the attack, the DOJ says it "caused a fault that led the refinery's Schneider Electric safety systems to initiate two automatic emergency shutdowns of the refinery's operations."

They added that Gladkikh and others did research into US-based refineries and tried to hack into other systems between February and July 2018.

Gladkikh worked for the State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics' Applied Developments Center, which said it "engaged in research concerning information technology-related threats to critical infrastructure."

Gladkikh is facing a maximum of 20 years in prison for two of the charges respectively and five years for the third charge.

“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 Graves.

Three military officers indicted

The other indictment – returned in August – involved 36-year-old Pavel Aleksandrovich Akulov, 42-year-old Mikhail Mikhailovich Gavrilov, and 39-year-old Marat Valeryevich Tyukov, who are accused of launching attacks against oil and gas firms, nuclear power plants, and utility and power transmission companies.

The DOJ said the three – who are identified as officers in Military Unit 71330 or “Center 16” of the FSB – specifically targeted ICS and SCADA systems. Center 16 was known by cybersecurity researchers as “Dragonfly,” “Berzerk Bear,” “Energetic Bear,” and “Crouching Yeti.”

Akulov, Gavrilov and Tyukov are facing charges related to computer fraud and abuse, wire fraud, aggravated identity theft and causing damage to the property of an energy facility.

Between 2012 and 2017, the three are accused of launching supply chain attacks that gave the Russian government “surreptitious, unauthorized and persistent access” to the networks of several energy companies.

From 2012 to 2014, they compromised several ICS/SCADA system manufacturers and software providers before hiding the “Havex” malware inside networks. They used a range of spearphishing and “watering hole” attacks to install malware on more than 17,000 devices in the US and other countries.

Between 2014 and 2017, the DOJ said the group went after “specific energy sector entities and individuals and engineers who worked with ICS/SCADA systems.” These attacks targeted more than 3,300 users at more than 500 U.S. and international companies and entities, in addition to US government agencies such as the Nuclear Regulatory Commission.

“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,” the DOJ explained.

The group was successful in compromising the business systems of the Wolf Creek Nuclear Operating Corporation (Wolf Creek) in Burlington, Kansas through spearphishing. They also found success with watering hole attacks, which captured the login credentials of energy sector engineers through compromised websites.

These attacks targeted people in more than 136 countries. The three are facing a maximum of five years in prison for the conspiracy to cause damage to the property of an energy facility and commit computer fraud and abuse charge and 20 years in prison for the conspiracy to commit wire fraud charge.

Akulov and Gavrilov were separately charged with wire fraud and computer fraud, which carry sentences ranging from five to 20 years in prison. The two are also facing three counts of aggravated identity theft, each of which carry a minimum sentence of two years consecutive to any other sentence imposed.

“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.”

Joint government advisory

Alongside the unsealed indictments, The Cybersecurity and Infrastructure Security Agency (CISA), FBI and Department of Energy released a joint advisory that highlights historical tactics, techniques, and procedures as well as mitigations that energy companies can take to protect their networks.

CISA Director Jen Easterly said that while the intrusions highlighted in the advisory span an earlier period of time, the associated tactics, techniques, procedures, and mitigation steps "are still highly relevant in the current threat environment."

"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.

"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."

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
