Russian Hacking

https://www.cnn.com/2022/04/27/europe/russia-cyberattacks-ukraine-war-microsoft/index.html

Defendants' Separate Campaigns both target software and hardware for operational technology systems. These attacks targeted thousands of computers, in approximately 135 countries, including many in the energy sector. A June 2021 indictment charged a Russian national working for a Russian defense agency, and his co-conspiring hackers, with damaging critical infrastructure outside the United State, by targeting computers within a U.S. firm managing similar facilities abroad.FSB agents hacked into the computers of hundreds of companies involved in the energy industry. Their goal was to steal secrets about how to make nuclear weapons. In order to do this, they had to get access to the company's computers. But instead of stealing information, they were actually making nuclear bombs."Russian state-sponsored hackers posed a serious and persistent threat. Hackers were targeting critical infrastructure both in the US and around the world. Although the criminal charges unsealed on Friday reflect past activity, they made crystal clear the urgent ongoing needs for American businesses to hardening their defenses and remaining vigilant. Alongside our domestic and foreign partners, the Department of Justice was focused on identifying and quickly directing response assets to victims of malicious cyber activity. We will continue to identify and rapidly direct response assets to victims. We will also arm our partners with the knowledge they need to deploy their tools against the adversary and attribute the misconduct and impose consequence both seen and unseen. We face no greater cyber threat then actors seeking to compromise critical infrastructures, offenses which could harm people working at affected plants as much as the citizens who rely on them. The Department of Justice will ensure that those attacking operation technologies will be identified and prosecuted."

Evgeniy Victorovich Gladkikh - defendant installed backdoors and used malware designed to compromise the security of energy facilities. He was charged with hacking into ICS and OT of global energy facilities. A federal grand jury in Washington D.C. returned an indictment against him.A hacker tried to attack a foreign plant and make it stop working. He didn't succeed, but he did get away with some money.A Russian government agency called the Russian Federal Agency for State Security (or FSB), or Russia's secret police, was involved in the development of the Triton malware. The Russian government also used this malware to spy on people.The defendant is charged with one charge of conspiracy to cause damage or destruction of property owned by an entity receiving federal financial assistance, which carries a maximum penalty of 10 years in prison and a $250,000 fine. He is also charged with two counts of attempted causing damage or destruction of property belonging to an entity receiving federal financial aid, which carries a maximum punishment of 20 years in prison and a fine of up to $500,000 per count. Finally, he is charged with one count conspiracy to commit wire fraud, which carries a possible 5-year term of imprisonment and a fine of up $250,000.A group of Russians hacked into computers of energy companies including Schneider Electric.