Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware

October 23, 2020

Washington – Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated, pursuant to Section 224 of the Countering America's Adversaries Through Sanctions Act (CAATSA), a Russian government research institution that is connected to the destructive Triton malware. The Triton malware — known also as TRISIS and HatMan in open source reporting — was designed specifically to target and manipulate industrial safety systems. Such systems provide for the safe emergency shutdown of industrial processes at critical infrastructure facilities in order to protect human life. The cyber actors behind the Triton malware have been referred to by the private cybersecurity industry as "the most dangerous threat activity publicly known."

"The Russian Government continues to engage in dangerous cyber activities aimed at the United States and our allies," said Secretary Steven T. Mnuchin. "This Administration will continue to aggressively defend the critical infrastructure of the United States from anyone attempting to disrupt it."

In recent years, the Triton malware has been deployed against U.S. partners in the Middle East, and the hackers behind the malware have been reportedly scanning and probing U.S. facilities. The development and deployment of the Triton malware against our partners is particularly troubling given the Russian government's involvement in malicious and dangerous cyber-enabled activities. Previous examples of Russia's reckless activities in cyberspace include, but are not limited to: the NotPetya cyber-attack, the most destructive and costly cyber-attack in history; cyber intrusions against the U.S. energy grid to potentially enable future offensive operations; the targeting of international organizations such as the Organization for the Prohibition of Chemical Weapons and the World Anti-Doping Agency; and the 2019 disruptive cyber-attack against the country of Georgia.

Triton Malware

In August 2017, a petrochemical facility in the Middle East was the target of a cyber-attack involving the Triton malware. This cyber-attack was supported by the **State Research Center**

of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), a Russian government-controlled research institution that is responsible for building customized tools that enabled the attack.

The Triton malware was designed to target a specific industrial control system (ICS) controller used in some critical infrastructure facilities to initiate immediate shutdown procedures in the event of an emergency. The malware was initially deployed through phishing that targeted the petrochemical facility. Once the malware gained a foothold, its operators attempted to manipulate the facility's ICS controllers. During the attack, the facility automatically shut down after several of the ICS controllers entered into a failed safe state, preventing the malware's full functionality from being deployed, and prompting an investigation that ultimately led to the discovery of the malware. Researchers who investigated the cyber-attack and the malware reported that Triton was designed to give the attackers complete control of infected systems and had the capability to cause significant physical damage and loss of life. In 2019, the attackers behind the Triton malware were also reported to be scanning and probing at least 20 electric utilities in the United States for vulnerabilities.

TsNIIKhM is being designated pursuant to Section 224 of CAATSA for knowingly engaging in significant activities undermining cybersecurity against any person, including a democratic institution, or government on behalf of the Government of the Russian Federation.

As a result of today's designation, all property and interests in property of TsNIIKhM that are in or come within the possession of U.S. persons are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. Additionally, any entities 50 percent or more owned by one or more designated persons are also blocked. Moreover, non-U.S. persons who engage in certain transactions with TsNIIKhM may themselves be exposed to sanctions.

View identifying information on the entity designated today.