US Treasury sanctions Russian research institute behind Triton malware

By Catalin Cimpanu

Published: 2020-10-23 · Archived: 2026-04-05 21:06:52 UTC

CNIIHM, Moscow

Image: Google Maps

The US Treasury Department announced sanctions today against a Russian research institute for its role in developing Triton, a malware strain designed to attack industrial equipment.

Sanctions were levied today against the **State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics** (also known as CNIIHM or TsNIIKhM).

A FireEye report published in October 2018 identified CNIIHM as the possible author of the Triton malware.

The Triton malware, also known as Trisis or HatMan, is a piece of malware that was designed to specifically target a certain type of industrial control system (ICS) equipment — namely, Schneider Electric Triconex Safety Instrumented System (SIS) controllers.

According to technical reports from FireEye, Dragos, and Symantec, the malware was distributed via phishing campaigns. Once it infected a workstation, it would search for SIS controllers on a victim's network, and then attempt to modify the controller's settings.

Researchers said Triton contained instructions that could either shut down a production process or allow SIS-controlled machinery to work in an unsafe state, creating a risk of explosions and risk to human operators and their lives.

Triton almost caused an explosion at a Saudi petrochemical plant

The malware was first spotted after it was used successfully in 2017 during an intrusion at a Saudi petrochemical plant owned by Tasnee, a privately owned Saudi company, where it almost cause an explosion.

Since then, the malware has been deployed against other companies. Furthermore, the group behind the malware (known as TEMP.Veles or Xenotime) has also been seen "scanning and probing at least 20 electric utilities in the United States for vulnerabilities," the US Treasury said today in a press release.

Today's sanctions prohibit US entities from engaging with CNIIHM and also seize any of the research institute's US-based assets.

"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."

> This style of sanctioning is significant and honestly entirely appropriate against those involved in the first ever cyber attack to intentionally try to kill people in civilian infrastructure. #TRISIS #TRITON https://t.co/dVzAn0kusq
>
> — Robert M. Lee (@RobertMLee) October 23, 2020

Today's Treasury sanctions end a week from hell for Russian state-sponsored hacking groups. On Monday, the US Department of Justice filed charges against six hackers part of the Sandworm group, believed to have created the NotPetya, KillDisk, BlackEnergy, and OlympicDestroyer malware.

On Thursday, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) exposed a recent hacking campaign of a Russian hacking group known as Energetic Bear.

On the same day, the EU also imposed sanctions on two Russian intelligence officers for their role in the 2015 German Parliament hack.

But as several security researchers pointed out today on Twitter, shortly after the Treasury announcement, the US may not have the moral high-ground, mainly because the US pioneered attacks against industrial systems through its work and deployment of the Stuxnet malware against Iran's nuclear program in 2010.

> They… uh… the Treasury realizes that we don't really have the high ground to stand on here… right?
> *cough* Stuxnet *cough*
>
> — MikeTalonNYC (@MikeTalonNYC) October 23, 2020

Source: https://www.zdnet.com/article/us-treasury-sanctions-russian-research-institute-behind-triton-malware/