US & Russia mutually targeting their power grids

Reference: Memo [190620-1] Date: 20/06/2019 - Version: 1.0
Keywords: energy, power grids, United States, Russia, critical infrastructure, Triton, ICS, disruption
Sources: publicly available information

Key Points

- A New York Times report alleges that the US has infiltrated the Russian electrical grid with offensive malware.
- The infiltration is not known to have been linked with any disruption.
- If the report is true, this activity poses risks of escalation and retaliation.
- A separate report by a security company indicates that a Russian threat group is probing US and Asian electrical grids.

Summary

On June 15, the New York Times (NYT) reported on the alleged deployment of US malware in Russian electrical grid systems as a strategic warning as well as a demonstration of capabilities. The action reportedly took place due to the newly granted (since August 2018) authority to the US cyber command to deploy and conduct cyber operations aggressively. The details of the mandate have not been disclosed.

The reported covert activity is viewed as a "companion" measure to other, more public actions aimed at dissuading Russian activities against the US. As such, the activity plays the role of a deterrence measure and even its way of publication is likely part of an effort to increase its effectiveness.

According to NYT, the US has probably been utilising reconnaissance probes against the control systems of the Russian electrical grid since at least 2012. However, the reported activity is clearly of offensive nature, also demonstrating a high degree of aggressiveness. In the same time, it is a demonstration, a warning, a deterrence measure, and has the potential for activation and use in case of a conflict.

Taking the offensive capabilities of Russian threat groups as a certainty, US officials are considering, according to the report, the possible scenario of Russian actions incurring blackouts ahead of the 2020 US presidential elections. The pre-installation of aggressive malware in the Russian electrical grid can act as a preventive measure.

It has not been clarified if the alleged intrusions have been with the order or approval of the President of the US, or they proceeded on the initiative of the US cyber command only. In Twitter remarks, right after the publication of the report, the US President has condemned the newspaper and characterised the story as untrue. In this respect it is also plausible that the story may be misguided or that the US President had not been briefed on the operation.

In a parallel development, analysis by the security company Dragos indicates that the threat group Temp.Veles (also known as Xenotime) has been probing US (as well as Asian-Pacific area) power grids for weaknesses. In 2017, Temp.Veles became known as the perpetrator of an attack against Schneider Electric's Triconex safety instrumented system (SIS). The custom malware used for this purpose has been identified with the name Triton. Importantly, Triton is one few cases of custom made specialised malware designed to attack Industrial Control Systems and the only one operating against security instrumented systems.

Comments

If confirmed, the US activity poses a significant escalation risk. It is highly likely that threat actors will attempt to increase their capacity to attack electrical grids and intensify their infiltration efforts, even outside the context of a specific conflict. In general, the situation poses the important question on whether the electrical grids constitute a valid target in time of war.

It is interesting that the deterrence intention between countries somehow mimics relevant cases in the area of nuclear weapons. It should be noted however, that, contrary to nuclear weapons, non-affiliated threat actors could perform cyber-attacks against electrical grids and such attacks could be difficult to be attributed, thus complicating retaliation actions.

Concerning the Triton malware, CERT-EU has reported on previous activity in Memo [190411-1], in April 2019. This sophisticated cyber-weapon was designed to prevent safety instrumented system (SIS) in industrial control systems from executing their intended function. During an attack, some SIS controllers entered a failed safe state, which automatically shut down the industrial process. Two options are available to the attackers: (1) manipulate safety mechanism to cause industrial process shutdown, (2) manipulate the safety mechanism to allow an unsafe state causing physical consequences (e.g. impact to equipment, product, environment and human safety) due to a loss of SIS functionality.

According to the security firm FireEye, the deployment of Triton in previous events was supported by the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM; a.k.a. ЦНИИХМ), a Russian government-owned technical research institution located in Moscow.