

Unearthed: CosmicEnergy, malware for causing Kremlin-style power disruptions

Getty Images

reader comments

9 with

Researchers have uncovered malware designed to disrupt electric power transmission and may have been used by the Russian government in training exercises for creating or responding to cyberattacks on electric grids.

Known as CosmicEnergy, the malware has capabilities that are comparable to those found in malware known as Industroyer and Industroyer2, both of which have been widely attributed by researchers to Sandworm, the name of one of the Kremlin's most skilled and cutthroat hacking groups. Sandworm deployed Industroyer in December 2016 to trigger a power outage in Kyiv, Ukraine, that left an estimated large swath of the city without power for an hour. The attack occurred almost a year after an earlier one disrupted power for 225,000 Ukrainians for six hours. Industroyer2 came to light last year and is believed to have been used in a third attack on Ukraine's power grids, but it was detected and stopped before it could succeed.

The attacks illustrated the vulnerability of electric power infrastructure and Russia's growing skill at exploiting it. The attack in 2015 used repurposed malware known as BlackEnergy. While the resulting BlackEnergy3 allowed Sandworm

to successfully break into the corporate networks of Ukrainian power companies and further encroach on their supervisory control and data acquisition systems, the malware had no means to interface with operational technology, or OT, gear directly.

The 2016 attack was more sophisticated. It used Industroyer, a piece of malware written from scratch designed to hack electric grid systems. Industroyer was notable for its mastery of the arcane industrial processes used by Ukraine's grid operators. Industroyer natively communicated with those systems to instruct them to de-energize and then re-energize substation lines. As WIRED reporter Andy Greenberg reported:

Industroyer was capable of sending commands to circuit breakers using any of four industrial control system protocols, and it allowed the modular components of code for those protocols to be swapped out so that the malware could be redeployed to target different utilities. The malware also included a component to disable safety devices known as protective relays—which automatically cut the flow of power if they detect dangerous electrical conditions—a feature that appeared designed to cause potentially catastrophic physical damage to the targeted transmission station's equipment when the Ukrenergo operators turned the power back on.

Industroyer2 contained updates to Industroyer. While ultimately failing, its use in a third attempted attack signaled that the Kremlin's ambitions for hacking Ukrainian electric power infrastructure remained a top priority.

Advertisement

Given the history, the detection of new malware designed to cause widespread power disruptions is of concern and interest to people charged with defending the grids. The concern is ratcheted up further when the malware has potential ties to the Kremlin.

Researchers from Mandiant, the security firm that found CosmicEnergy, wrote:

COSMICENERGY is the latest example of specialized OT malware capable of causing cyber physical impacts, which are rarely discovered or disclosed. What makes COSMICENERGY unique is that based on our analysis, a contractor may have developed it as a red teaming tool for simulated power disruption exercises hosted by Rostelecom-Solar, a Russian cyber security company. Analysis into the malware and its functionality reveals that its capabilities are comparable to those employed in previous incidents and malware, such as INDUSTROYER and INDUSTROYER.V2, which were both malware variants deployed in the past to impact electricity transmission and distribution via IEC-104.

The discovery of COSMICENERGY illustrates that the barriers to entry for developing offensive OT capabilities are lowering as actors leverage knowledge from prior attacks to develop new malware. Given that threat actors use red team tools and public exploitation frameworks for targeted threat activity in the wild, we believe COSMICENERGY poses a plausible threat to affected electric grid assets. OT asset owners leveraging IEC-104 compliant devices should take action to preempt potential in the wild deployment of COSMICENERGY.

Right now, the link is circumstantial and mainly limited to a comment found in the code suggesting it works with software designed for training exercises sponsored by the Kremlin. Consistent with the theory that CosmicEnergy is used in so-called Red Team exercises that simulate hostile hacks, the malware lacks the ability to burrow into a network to obtain environment information that would be necessary to execute an attack. The malware includes hardcoded information object addresses typically associated with power line switches or circuit breakers, but those mappings would have to be

customized for a specific attack since they differ from manufacturer to manufacturer.

“For this reason, the particular actions intended by the actor are unclear without further knowledge about the targeted assets,” Mandiant researchers wrote.

<https://arstechnica.com/?p=1942377>