EINPRESSWIRE

Industroyer: A cyber-weapon that brought down a power grid

DUBAI, UNITED ARAB EMIRATES, June 16, 2022 /EINPresswire.com/ -- Five years ago, ESET researchers released their analysis of the first ever malware that was designed specifically to attack power grids
Authored by André Lameiras, security writer at ESET

On June 12th 2017, ESET researchers published their findings about unique malware that was capable of causing a widespread blackout. Industroyer, as they named it, was the first known piece of malware that was developed specifically to target a power grid.

Indeed, Industroyer had been deployed to considerable effect a few months earlier – it caused thousands of homes in parts of Kyiv, Ukraine to lose power supplies for about an hour on December 17th, 2016, after the malware struck a local electrical substation. A few days later, ESET malware researcher Anton Cherepanov would start dissecting Industroyer.

A ticking bomb
Once planted, Industroyer spread throughout the substation’s network looking for specific industrial control devices whose communication protocols it could speak. Then, like a time bomb going off, it apparently opened every circuit breaker at once, while defying any attempts of the substation operators to regain easy control: if an operator tried to close a breaker, the malware opened it back up.

To clean up its footprint, the malware unleashed a data wiper that was designed to leave the substation’s computers inoperable and delayed the return to normal operations. Indeed, the wiper often failed, but had it been more successful, the consequences could have been much worse – especially in wintertime when a power outage can allow pipes filled with water to crack when they freeze.

A final malicious act was made by the malware to disable some of the protective relays at the substation, but that failed too. Without functioning protective relays in place, the substation equipment could have been at high risk of damage when the operators eventually reestablished electric transmission.

As Cherepanov and fellow ESET researcher Robert Lipovsky said at the time, the sophistication of Industroyer makes it possible to adapt the malware to any similar environment. In fact, the industrial communication protocols that Industroyer speaks are used not only in Kyiv, but also "worldwide in power supply infrastructure, transportation control systems, and other critical infrastructure systems (such as water and gas)".

On the other hand, considering how sophisticated Industroyer was, its impact was ultimately rather underwhelming, as ESET researchers noted themselves back in 2017. Perhaps it was only a test for future attacks, or perhaps it was a sign of what the group behind it could do.

The work of Sandworm

The shenanigans of the malware, ESET researchers noted, mirror the malicious intentions of the people who created it. At a Virus Bulletin conference in 2017, Lipovsky highlighted that the "attackers had to understand the architecture of a power grid, what commands to send, and how that will be achieved". Its creators went a long way to create this malware, and their objective was not just a power outage. "Some clues in the Industroyer configuration suggest they wanted to cause equipment damage and malfunction".

At Black Hat 2017, Cherepanov also pointed out that it "seems very unlikely anyone could write and test such malware without access to the specialized equipment used in the specific, targeted industrial environment".

In October 2020, the United States attributed the attack to six officers belonging to Unit 74455, aka Sandworm, a unit within Russia's military intelligence agency GRU.

A comeback for Industroyer

Fast forward to 2022 and it's no surprise that in the weeks just before and after Russia's invasion on February 24th, ESET telemetry showed an increase in cyberattacks targeting Ukraine.

On April 12th, together with CERT-UA, ESET researchers announced they had identified a new variant of Industroyer that targeted an energy supplier in Ukraine. Industroyer2 had been scheduled to cut power for a region in Ukraine on April 8th; fortunately, the attack was thwarted before it could wreak further havoc on the war-torn country. ESET researchers assessed with high confidence that Sandworm was again responsible for this new attack.

A harbinger of things to come

In recent years, it's become more than clear that the world's critical infrastructure services are at major risk for disruptions. The string of incidents that have impacted critical infrastructure in

Ukraine (and, indeed, other parts of the world) have awakened much of the public to the risks of cyberattack-induced power outages, water supply interruptions, fuel distribution disruptions, loss of medical data and many other consequences that can do far more than just disrupt our daily routines – they can be truly life-threatening.

Back in 2017, both Cherepanov and Lipovsky concluded their research blog with a warning that, five years later, still holds true: “Regardless of whether or not the recent attack on the Ukrainian power grid was a test, it should serve as a wake-up call for those responsible for security of critical systems around the world”.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here