Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout

Malware which speaks the language of industrial machines is a danger to all of our critical services.

By Charlie Osborne for Zero Day | April 30, 2018 -- 11:08 GMT (04:08 PDT)

File Photo

BRATISLAVA, SLOVAKIA: When Ukraine's power grid unexpectedly dropped in 2016, the city of Kiev lost all power for an hour.

While 60 minutes does not seem like a long time, for operators at the substations responsible for keeping power flowing in the city, it must have felt like a lifetime.

As they panicked while trying to resume electrical services -- and were scuppered at every turn by system failures caused by malware -- it was also an hour which now highlights the damage cyberattackers are able to do to critical systems.

The sudden collapse of systems responsible for serving Kiev with electricity was investigated, eventually leading to the discovery of a cyberattack caused by malware known as Industroyer.

During a presentation at ESET headquarters in Bratislava, Slovakia, security researcher Robert Lipovsky called Industroyer "the most sophisticated, the biggest threat to industrial control systems since Stuxnet," an almost legendary worm in the cybersecurity field which was used to attack an Iranian nuclear facility's centrifuges in 2010.

While Stuxnet is widely believed to have been created by the US government to disrupt Iranian nuclear plans -- albeit, a theory never acknowledged by those allegedly responsible -- Industroyer has only been detected so far in Ukraine.

Lipovsky says that Industroyer is, perhaps, the only malware in existence which has been "specifically designed to attack the power grid."

According to ESET, Industroyer was able to automatically impact and disrupt industrial processes within the Ukrainian substation responsible for power flows by covertly disrupting a select group of industrial systems and protections.

The first stage of the Industroyer campaign was to infiltrate the substation. This was made possible by exploiting CVE-2015-5374 (https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01), a vulnerability in Siemens SIPROTEC 4 and SIPROTEC Compact devices.

The security flaw, first reported back in 2015, can result in denial-of-service (DoS) disruption.

DoS attacks can be a nuisance when levied against website domains, but when launched at systems responsible for critical services, their effects can be disastrous.

Once this vulnerability was exploited, the malware had a hook into industrial systems and created a backdoor.

The malware was also able to maintain persistency by making a copy of the main backdoor, as well as a backup backdoor which would spring into action should the first version be uncovered. The backup masqueraded as a Trojanized version of Windows Notepad.

According to the security researcher, Industroyer then went straight for the industrial hardware on-site. In particular, Industroyer focused on the substation's circuit breakers and protection relays.

However, an attack against these systems was far from immediate. Hidden within the malware's code in hex characters was a pre-defined timer containing the date and time for the blackout to take place.

When the minute struck, Industroyer activated its payload. Commands were then sent to the circuit breakers and protection relays which only opened circuit breaker switches but also activated a malicious launcher component.

Four elements of the payload targeted particular communication protocols specified in the standards IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OLE for Process Control Data Access (OPC DA).

Industroyer is modular, and this allowed the four communications protocols to be targeted, no matter the device type, vendor, or configuration files. As long as one of the above communication protocols were in use, the attack could continue.

"They all do, on a high level, more or less the same thing," the researcher noted. "They all send commands to devices, [no matter] whether the circuit breakers are those that continuously open or those that flip between on and off states."

When the malware has wrestled control of the circuit breakers through these modules, two other components came into play to amplify the attack.

The first was a denial-of-service tool which targeted protection relays, rendering them unresponsive.

The second was a wiper tool which honed in on Microsoft Windows workstations used to administer, control and configure protection relays though ABB MicroScada software.

The data wiper scanned workstation hard drives for specific file extensions belonging to the software. If these files were detected, the wiper removed them all, preventing recovery unless a backup was available.

The malware then crashed the system.

"From the perspective of an operator at that substation, the industry wasn't flowing as the circuit breakers kept being reopened due to the first payload group, their protection relays were not responding due to the service attack, and then when they sat down and tried to fix the problem they found their SCADA software wasn't responding," Lipovsky said. "So, not the ideal scenario for them."

Attribution is difficult, but there are indications that the Ukrainian attack was potentially a testbed for further assaults.

> A log file analyzed by the firm was renamed from iec104.log to iec104sev.log. The "sev" addition may link to "north" -- as the substation was located in northern Ukraine -- and there seems to be little purpose to renaming the file unless more attacks were planned, at least at one point in time.

Unlike regular crimeware, Industroyer is able to "speak the language of these devices," according to ESET, due to its use of different communication protocols and vendor-specific as well as vendor-agnostic exploits.

These kinds of capabilities are dangerous and made worse as patching industrial systems is far from easy -- especially with so many substations, grid controllers, and more using legacy systems and components which do not have over-the-air (OTA) update capabilities.

The use of a known 2015 exploit to take out the power of an entire city -- no matter for how long for -- may be a dangerous precedent for the future.

Should Industroyer end up on the open market, Lipovsky suggests it would take no more than a "day of coding" to customize the modular malware to the attacker's requirements and target industrial control systems in Europe, the US, and beyond.

However, there have been no indications that Industroyer has been used in any attacks since.

ESET expected another to take place given the malware's sophisticated functionality and the log file clues, and this is still a possibility.

The Ukrainian power grid attack may not be the last time we hear of Industroyer.