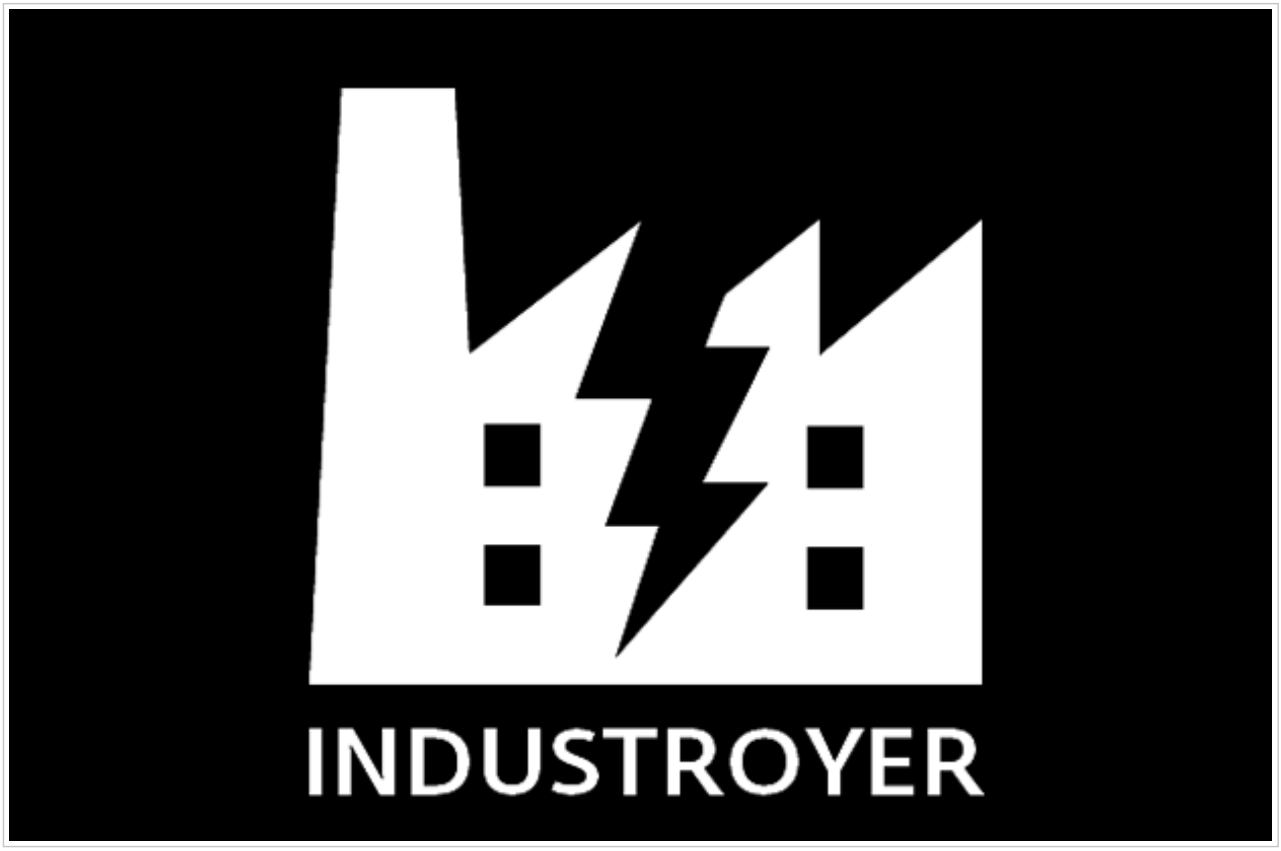
welivesecurity
News, views, and insight from the ESET security community

Industroyer: Biggest threat to industrial control systems since Stuxnet

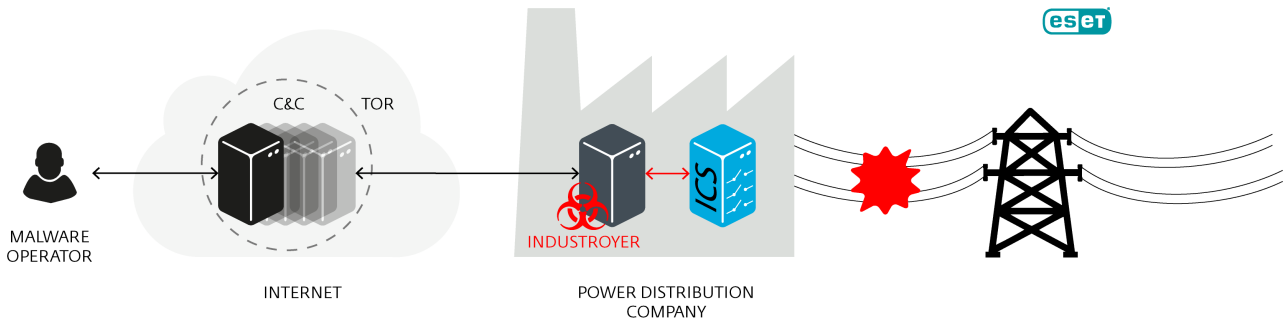
BY ANTON CHEREPANOV AND ROBERT LIPOVSKY POSTED 12 JUN 2017 - 02:00PM



Update (July 17th): The authors of the Industroyer research, Anton Cherepanov and Robert Lipovsky, will present their findings at *Black Hat USA in Las Vegas on July 26th, 2017. More information can be found **here**.*

The 2016 attack on Ukraine's power grid that deprived part of its capital, Kiev, of power for an hour was **caused by a cyberattack**. ESET researchers have since analyzed samples of malware, detected by ESET as Win32/Industroyer, capable of performing exactly that type of attack.

Whether the same malware was really involved in what cybersecurity experts consider to have been a **large-scale test** is yet to be confirmed. Regardless, the malware is capable of doing significant harm to electric power systems and could also be refitted to target other types of critical infrastructure.



Industroyer is a particularly dangerous threat, since it is capable of controlling electricity substation switches and circuit breakers directly. To do so, it uses industrial communication protocols used worldwide in power supply infrastructure, transportation control systems, and other critical infrastructure systems (such as water and gas).

These switches and circuit breakers are digital equivalents of analogue switches; technically they can be engineered to perform various functions. Thus, the potential impact may range from simply turning off power distribution, cascading failures and more serious damage to equipment. The severity may also vary from one substation to another, as well. Needless to say, disruption of such systems can directly or indirectly affect the functioning of vital services.

Industroyer's dangerousness lies in the fact that it uses protocols in the way they were designed to be used. The problem is that these protocols were designed decades ago, and back then industrial systems were meant to be isolated from the outside world. Thus, their communication protocols were not designed with security in mind. That means that the attackers didn't need to be looking for protocol vulnerabilities; all they needed was to teach the malware "to speak" those protocols.

The recent power outage occurred on December 17th, 2016, almost exactly one year after the **well-documented cyberattack** that caused a blackout that affected around 250,000 households in several regions in Ukraine on December 23rd, 2015.

In 2015, the perpetrators infiltrated the electricity distribution networks with the **BlackEnergy malware, along with KillDisk** and other malicious components, and then abused legitimate remote access software to control operators' workstations and to cut off power. Aside from targeting the Ukrainian power grid, there are no apparent similarities in code between BlackEnergy and Industroyer.

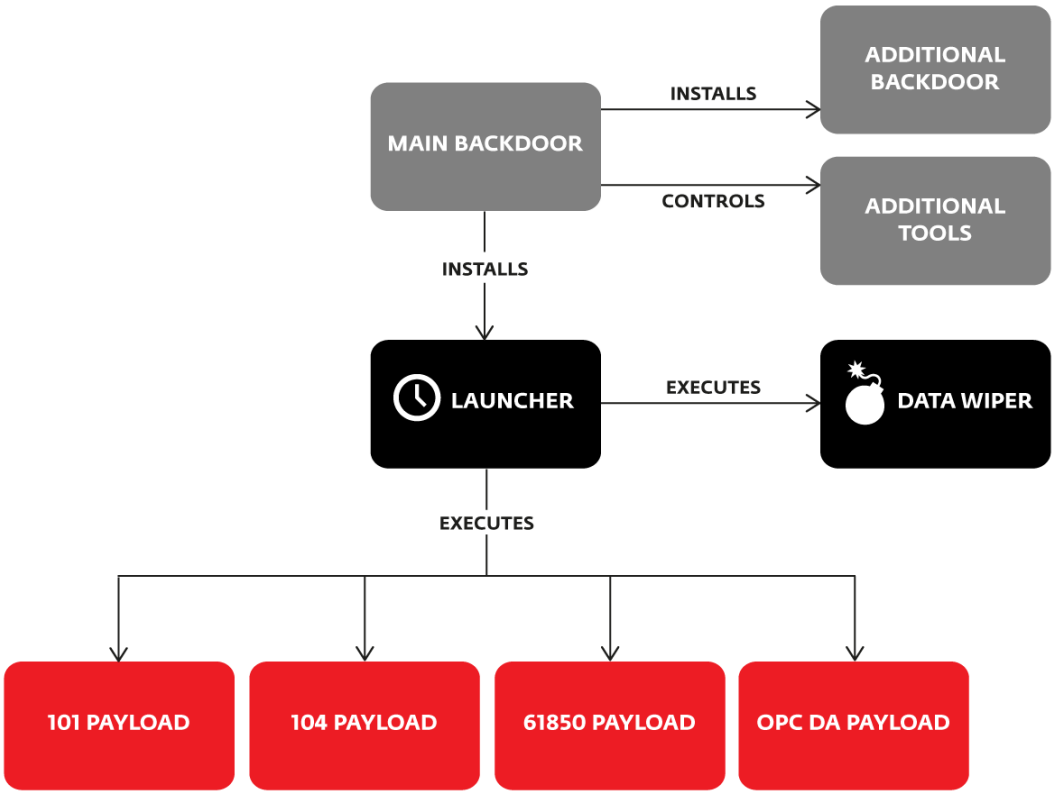
Structure and key functionalities

Industroyer is modular malware. Its core component is a backdoor used by attackers to manage the attack: it installs and controls the other components and connects to a remote server to receive commands and to report to the attackers.

What sets Industroyer apart from other malware targeting infrastructure is its use of four payload components, which are designed to gain direct control of switches and circuit breakers at an electricity distribution substation.

Each of these components targets particular communication protocols specified in the following standards: **IEC 60870-5-101**, **IEC 60870-5-104**, **IEC 61850**, and **OLE for Process Control Data Access (OPC DA)**.

Generally, the payloads work in stages whose goals are mapping the network, and then figuring out and issuing commands that will work with the specific industrial control devices. Industroyer's payloads show the authors' deep knowledge and understanding of industrial control systems.



The malware contains a few more features that are designed to enable it to remain under the radar, to ensure the malware's persistence, and to wipe all traces of itself after it has done its job.

For example, the communication with the C&C servers hidden in Tor can be limited to non-working hours. Also, it employs an additional backdoor – masquerading as the Notepad application – designed to regain access to the targeted network in case the main backdoor is detected and/or disabled.

And its wiper module is designed to erase system-crucial Registry keys and overwrite files to make the system unbootable and the recovery harder. Of interest is the port scanner that maps the network, trying to find relevant computers: the attackers made their own custom tool instead of using existing software. Finally, yet another module is a Denial-of-Service tool that exploits the **CVE-2015-5374** vulnerability in Siemens SIPROTEC

devices and can render targeted devices unresponsive.

Conclusion

Industroyer is highly customizable malware. While being universal, in that it can be used to attack any industrial control system using some of the targeted communication protocols, some of the components in analyzed samples were designed to target particular hardware. For example, the wiper component and one of the payload components are tailored for use against systems incorporating certain industrial power control products by ABB, and the DoS component works specifically against Siemens SIPROTECT devices used in electrical substations and other related fields of application.

While in principle it's difficult to attribute attacks to malware without performing an onsite incident response, it's highly probable that Industroyer was used in the December 2016 attack on the Ukrainian power grid. On top of the fact that the malware clearly possesses the unique capabilities to perform the attack, it contains an activation timestamp for December 17th, 2016, the day of the power outage.

The 2016 attack on the Ukrainian power grid attracted much less attention than the attack that occurred a year earlier. However, the tool most likely used, Win32/Industroyer, is an advanced piece of malware in the hands of a sophisticated and determined attacker.

Thanks to its ability to persist in the system and provide valuable information for tuning-up the highly configurable payloads, attackers could adapt the malware to any environment, which makes it extremely dangerous. 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.

*Additional technical details on the malware and Indicators of Compromise can be found in our comprehensive **white paper**, and on **github**. For any inquiries, or to make sample submissions related to the subject, contact us at: **threatintel@eset.com**.*