Last-minute paper: Industroyer: biggest threat to industrial control systems since Stuxnet

virusbulletin.com/conference/vb2017/abstracts/last-minute-paper-industroyer-biggest-threat-industrial-control-systems-stuxnet/

Thursday 5 October 14:30 - 15:00, Green room

Anton Cherepanov (ESET)
Robert Lipovsky (ESET)

Industroyer is the first ever malware specifically designed to attack power grids. This unique and extremely dangerous malware framework was involved in the December 2016 blackout in Ukraine. What sets Industroyer apart from other malware targeting infrastructure, such as BlackEnergy (a.k.a. SandWorm), is its ability to control switches and circuit breakers directly via four different industrial communication protocols.

Our talk will cover a detailed analysis of Industroyer's malicious payloads that directly interfere with the targeted industrial control systems, as well as supporting modules responsible for command & control communication, persistence, and so on.

In addition to explaining why Industroyer can be considered the biggest threat to industrial control systems since the infamous Stuxnet worm, we will take a look at the 2016 power outage in the context of the other numerous cyber attacks against Ukrainian critical infrastructure in the recent years, some of which were covered in our previous *Virus Bulletin* talks.

We will also assess the attackers' motivations and what this threat means to utilities around the world. As the protocols and hardware targeted by Industroyer are employed in power supply infrastructure, transportation control systems, and other critical infrastructure systems, like water and gas, worldwide, the malware can be re-purposed to target vital services in other countries. This discovery should serve as a wake-up call for those responsible for the security of these critical systems.

Watch Video At:

https://youtu.be/oGE6xHEQyog

- **Anton Cherepanov**

  Anton Cherepanov graduated from the South Ural State University in 2009. Currently working at *ESET* as a malware researcher, his responsibilities include the analysis of complex threats. His research has been presented at numerous conferences, including Virus Bulletin, CARO Workshop, PHDays, and ZeroNights. His interests focus on IT security, reverse engineering and malware analysis automation.

- **Robert Lipovsky**

  Robert Lipovsky is Senior Malware Researcher in *ESET*'s Security Research Laboratory, having worked for *ESET* since 2007. He is responsible for malware intelligence and research and leads the Malware Research team in Bratislava. He is a regular speaker at security conferences, including Virus Bulletin, EICAR, and CARO. He runs a reverse engineering course at the Slovak University of Technology, his alma mater, and the Comenius University. When not bound to a keyboard, he enjoys sports, playing guitar and flying an airplane.