Sujet 1 - SSI Industrielle - CRASHOVERRIDE

- Supports de Cours - Licence Professionnel - Sujet SSI -

Publication date: samedi 17 mars 2018

The CRASHOVERRIDE malware impacted a single transmission level substation in Ukraine on December 17th, 2016. Many elements of the attack appear to have been more of a proof of concept than what was fully capable in the malware. The most important thing to understand though from the evolution of tradecraft is the codification and scalability in the malware towards what has been learned through past attacks. The malware took an approach to understand and codify the knowledge of the industrial process to disrupt operations as STUXNET did. It leveraged the OPC protocol to help it map the environment and select its targets similar to HAVEX. It targeted the libraries and configuration files of HMIs to understand the environment further and leveraged HMIs to connect to Internet-connected locations when possible as BLACKENERGY 2 had done. And it took the same type of approach to understanding grid operations and leveraging the systems against themselves displayed in Ukraine 2015's attack. It did all of these things with added sophistication in each category giving the adversaries a platform to conduct attacks against grid operations systems in various environments and not confined to work only on specific vendor platforms. It marks an advancement in capability by adversaries who intend to disrupt operations and poses a challenge for defenders who look to patching systems as a primary defense, using anti-malware tools to spot specific samples, and relying upon a strong perimeter or air-gapped network as a silver-bullet solution. Adversaries are getting smarter, they are growing in their ability to learn industrial processes and codify and scale that knowledge, and defenders must also adapt.