MALWARE THAT CAN KNOCK OUT POWER GRIDS DISCOVERED

Researchers from Slovakian Anti Virus company ESET have publicized information on malware especially targeted for automation in power grids. The malware is tied to an attack in Ukraine 2016. ESET have worked alongside researchers from another company, Dragos, to analyze the code. Investigators from ESET and Dragos will come to Cyber Security Summit CS3STHLM in Stockholm in October to present and discuss their findings.

Robert Lipovski, one of the researchers at ESET, states in Washington Post: “The potential impact of malware like this is huge. It’s not restricted to Ukraine. The industrial hardware that the malware communicates with is used in critical infrastructure worldwide.”

This malware is called the most dangerous code since Stuxnet, malware discovered in 2010 aimed specifically towards Iran’s nuclear program.

Robert Malmgren, owner and co-founder of CS3STHLM: -” The fact that this malware can be used and re-used in critical infrastructure everywhere makes it an enormous threat to non protected Industrial Control Systems.”

CS3STHLM takes place at Nalen in Stockholm October 24-26.

For more information regarding the malware, please contact
Robert Malmgren
Phone: +46 708 33 03 78

For information regarding CS3STHLM, please contact
Maria Engstrom Ostby
Phone: +46 705 12 42 93

FACTS CS3STHLM
CS3STHLM is hosted by Omnisiens, owned by Swedish Cyber Security Experts Robert Malmgren; voted number one IT security specialist in Sweden in trade magazine Computer Sweden and Erik Johansson, PhD; Security Researcher, Advisor, and Contractor working at the intersection of Information Technology (IT) and Operational Technology (OT)