Cyber Security – EnC developments

Blueprint Energy Solutions GmbH
Elena Boskov-Kovacs

Vienna, 02.07.2019.

Agenda

1. Introduction
2. Overview of project objectives and progress
3. Methodology and Next steps

Year 2018 in EU Cyber Security

ENISA Threat Report

„2018 was a year that has brought significant changes in the cyberthreat landscape. Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors."

Source: ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends, FINAL VERSION 1.0 ETL 2018, JANUARY 2019

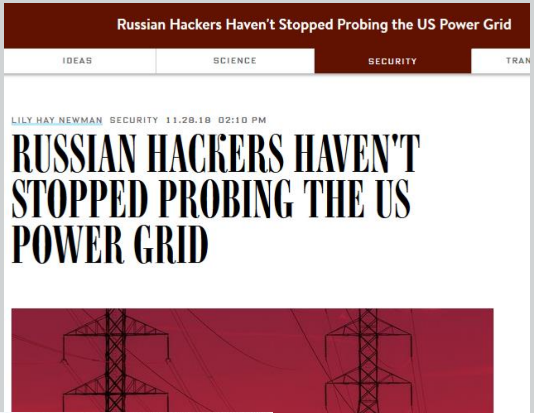
Cyber threats in energy systems

Security challenges in the energy sector

- Moving towards interconnected, digitalized and decentralized systems
- Proliferation of highly interactive but poorly secured ("user friendly") information and communication technologies
- Outsourcing and renting of infrastructures and services
- Increased interdependency and exchange of data among market players
- Protection concepts and design rules of energy facilities not adequate to modern threats
- Dependence on foreign technologies (integrity and compatibility of components)
- Cross-border interconnected energy network – the "weakest link" and "cascade" effects
- Constraints imposed by security measures – in contrast to real-time-availability requirements
- Availability of human resources and their competences
- Evolving cybercrime business models, growing powers / interests of cybercrime communities
- Diverse ownership structures and related rights and decisions

Threat Landscape of EnC Member States

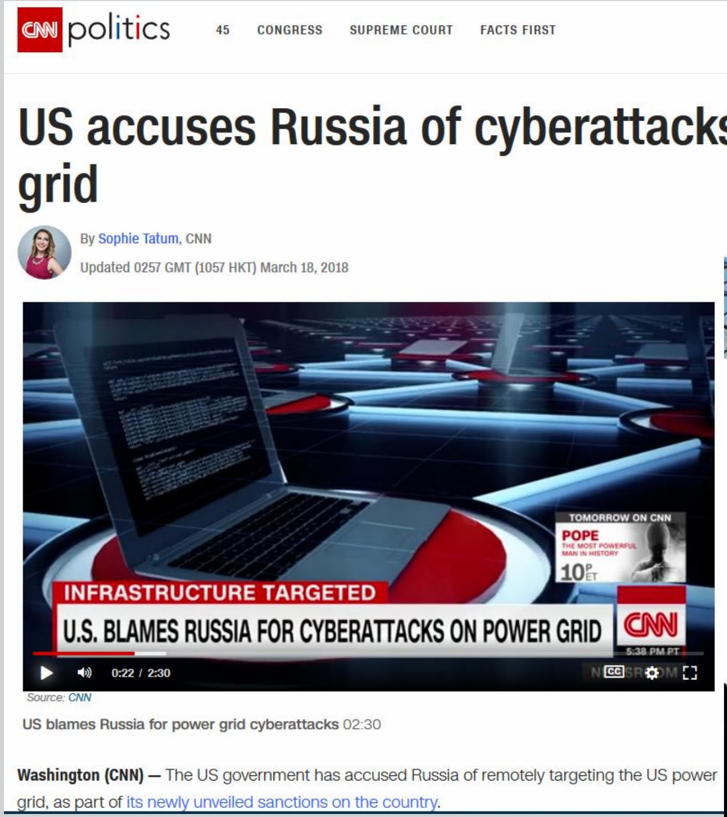
Worldwide:



Russian Hackers Haven't Stopped Probing the US Power Grid

LILY HAY NEWMAN SECURITY 11.28.18 02:10 PM

RUSSIAN HACKERS HAVEN'T STOPPED PROBING THE US POWER GRID



US accuses Russia of cyberattacks on power grid

By Sophie Tatum, CNN

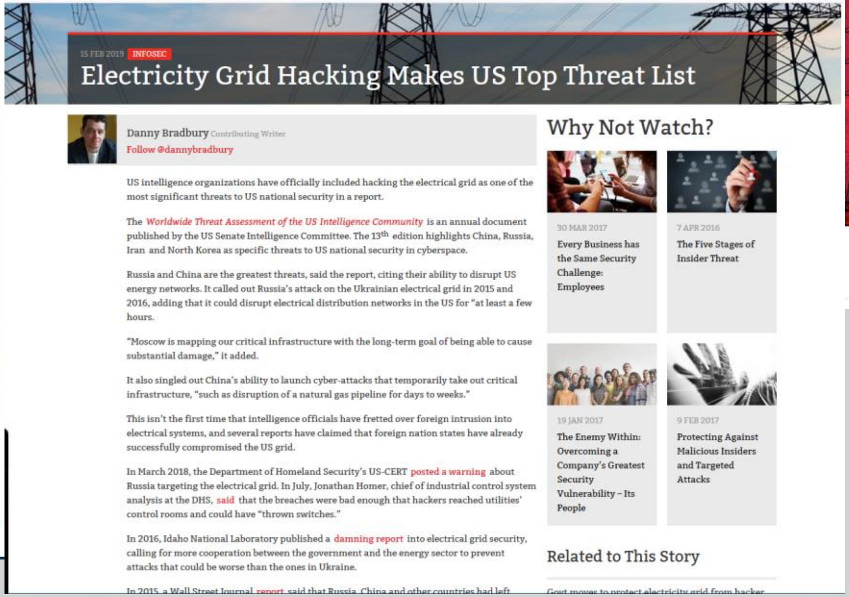
Updated 0257 GMT (1057 HKT) March 18, 2018

TOMORROW ON CNN
POPE
THE MOST POWERFUL MAN IN HISTORY
10P ET
INFRASTRUCTURE TARGETED
U.S. BLAMES RUSSIA FOR CYBERATTACKS ON POWER GRID
CNN
5:38 PM PT
0:22 / 2:30

Source: CNN

US blames Russia for power grid cyberattacks 02:30

Washington (CNN) — The US government has accused Russia of remotely targeting the US power grid, as part of its newly unveiled sanctions on the country.



15 FEB 2019 INFOSEC

Electricity Grid Hacking Makes US Top Threat List

Danny Bradbury Contributing Writer
Follow @dannybradbury

US intelligence organizations have officially included hacking the electrical grid as one of the most significant threats to US national security in a report.

The *Worldwide Threat Assessment of the US Intelligence Community* is an annual document published by the US Senate Intelligence Committee. The 13th edition highlights China, Russia, Iran and North Korea as specific threats to US national security in cyberspace.

Russia and China are the greatest threats, said the report, citing their ability to disrupt US energy networks. It called out Russia's attack on the Ukrainian electrical grid in 2015 and 2016, adding that it could disrupt electrical distribution networks in the US for "at least a few hours.

"Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage," it added.

It also singled out China's ability to launch cyber-attacks that temporarily take out critical infrastructure, "such as disruption of a natural gas pipeline for days to weeks."

This isn't the first time that intelligence officials have fretted over foreign intrusion into electrical systems, and several reports have claimed that foreign nation states have already successfully compromised the US grid.

In March 2018, the Department of Homeland Security's US-CERT posted a warning about Russia targeting the electrical grid. In July, Jonathan Homer, chief of industrial control system analysis at the DHS, said that the breaches were bad enough that hackers reached utilities' control rooms and could have "thrown switches."

In 2016, Idaho National Laboratory published a damning report into electrical grid security, calling for more cooperation between the government and the energy sector to prevent attacks that could be worse than the ones in Ukraine.

In 2015, a Wall Street Journal report said that Russia, China and other countries had left

Why Not Watch?

30 MAR 2017
Every Business has the Same Security Challenge: Employees

7 APR 2016
The Five Stages of Insider Threat

19 JAN 2017
The Enemy Within: Overcoming a Company's Greatest Security Vulnerability – Its People

9 FEB 2017
Protecting Against Malicious Insiders and Targeted Attacks

Related to This Story

Govt moves to protect electricity grid from hacker

Study project of Energy Community

Study on Cybersecurity in energy

- Objectives:
  - Identify and assess key weaknesses, risks and exposure to cyber threats in the energy systems
  - Identify the existing regulatory framework and regulatory gaps for cybersecurity governance
  - Identify the relevant provisions of the NIS Directive and the Directive on European critical infrastructure and provide an impact assessment of their implementation in the Energy Community
  - Propose the necessary measures to improve cybersecurity in Contracting Parties (national level)
  - Propose a model for regional cooperation in managing cybersecurity risks and reporting incidents as well as a common cooperation platform, common certification framework and common framework for research, education and training programmes
  - Explore the possibility for the participation of Contracting Parties in the work of the European Union Agency for Network and Information Security (ENISA).

Study project of Energy Community

On the basis of Procedural Act 2018/2/MC-EnC: on the Establishment of an Energy Community **Coordination Group for Cyber-Security and Critical Infrastructure**, created among other to promote a high level of security of network and information systems and of critical infrastructures within the Energy Community, a coordination group for cyber-security and critical infrastructure was set up.

1st Cybersecurity Day in the Energy Community - gathering representatives from Ministries, regulatory bodies and system operators from Albania, BiH, North Macedonia, Georgia, Kosovo*, Moldova, Montenegro, Serbia and Ukraine

Engagement and ongoing activities

		Month	1	2	3	4	5	6	7	8	9	10
Task	Activity	Activity Date	January	February	March	April	May	June	July	August	September	October
		Bi monthly reports			⬛		⬛		⬛		⬛	
T0		Inception report	⬛									
T1	1.1	Overview of legal, regulatory and institutional cybersecurity frameworks		🟦								
T1	1.2	Questionnaire development		🟦	🟦							
T1	1.3	Workshop1: Identification of relevant stakeholders and questionnaire presentation			🟨							
T1	1.4	Questionnaire delivery and collection			🟦	🟦						
T1	1.5	Questionnaire					🟦	🟦 ★				
T1	1.6	Field activity (Contracting Parties)					🟩	🟩				
T1	1.7	Threat identification and risk assessment						🟦	🟦			
T1	1.8	Workshop2 – Cyber-risks workshop						🟦				
T1	1.9	First interim report						🟦	⬛			
T2	2.1	GAP assessment								🟦		
T2	2.2	Second interim report								🟦	⬛	
T3	3.1	Propose recommendations									🟦	
T3	3.2	Workshop3 - Make an impact assessment of implementation of proposed measures and acts in the Energy Community Contracting Parties and in the Energy Community									🟨	
T3	3.3	Relevant information for impact assesment collection (for W3 survey)									🟦	
T3	3.4	Information for impact assesment analysis (for W3 survey)									🟦	
T3	3.5	Final report									🟦	⬛
T3	3.6	Workshop4 - Final meeting										🟨

We are here

July 2019:
different speed of development
and data collection
in individual countries

⬛	Reports (Inception, Interim, Finl, Bi Mothly)
🟦	Project activity
🟨	Field activity

Methodology – key tasks

- Information gathering
  - Awareness raising
  - Segmented by stakeholders
  - Interactive
- GAP assessment (-> obstacles)
  - EU rules and best practices
  - Current state of Cybersecurity in EnC Contracting Parties
- Propose minimum common framework
  - Measures
  - Institutions (necessary to implement measures)
  - Assess impact of proposed measures
  - Implementation roadmap

- Budapest convention implementation
- ECI and NIS implementation related information
  - Cybersecurity strategy
  - Critical infrastructure identification/criteria
  - Essential services
  - Incident reporting (contact points)
- Standards
- Cyber security cooperation, projects and assistance
- Awareness, education and training programmes and cooperation
- Cyber risk assessment
- Impact assessment of proposed measures

Standards and Good Practice

EU Commission Recommendation Features

- Real-time requirements (segregation, authentication, encryption, physical security…)
- Cascading effects (from grid to grid – from country to country)
- Legacy technology combined with network of IoT devices

- Description of some recommended standards (ISO/IEC 27001/27019, IEC62443, IEC62351, ISO/IEC31000)

Questions?