ACER
Agency for the Cooperation of Energy Regulators

Implications of COVID-19 on the security of energy system operation

Prepared by: Stefano Bracco (Stefano.BRACCO@acer.europa.eu)
(Knowledge Manager and Security Officer at the Agency for the Cooperation of Energy Regulators)

Webinar on The Regulatory Role in Supporting Cybersecurity Investments
17 June 2020

ACER
Agency for the Cooperation of Energy Regulators

Before....

Severe acute respiratory syndrome coronavirus 2 isolate Wuhan-Hu-1, complete genome

Implications of COVID-19 on the security of energy system operation

ACER
Agency for the Cooperation of Energy Regulators

During....

Entso-E targeted in recent cyberattack

The European Network of Transmission System Operators for Electricity said on Monday that unidentified hackers recently targeted its computer networks.

MARCH 10, 2020 BRIAN PUBLICOVER

GRIDS & INTEGRATION | INSURANCE | MARKETS | MARKETS & POLICY | POLICY | TECHNOLOGY | TECHNOLOGY AND R&D | FINLAND | SWEDEN | WESTERN EUROPE

Image: Sfedor/Pixabay

Cyber Attack On U.K. Electricity Market Confirmed: National Grid Investigates

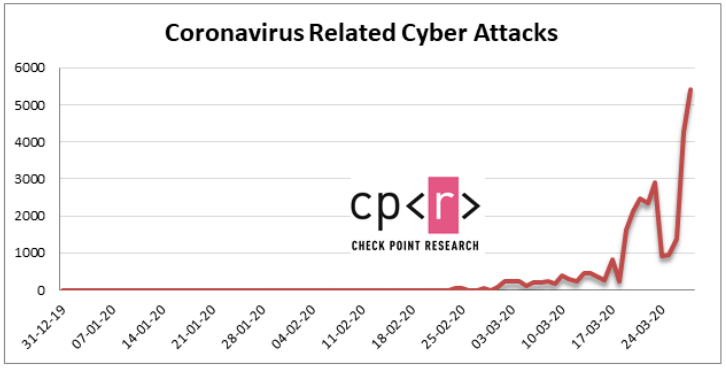
The company that facilitates payments on the U.K. electricity market, tracking the trade between those who produce electricity and those who supply it and resolving the differences, has fallen victim to a cyber-attack. Elexon is at the center of the balancing and settlement system, working with Great Britain's National Grid Electricity System Operator (ESO) to keep the lights on. The lights didn't go off across the U.K. as a result of this cyber-attack, but internal IT systems and laptops at Elexon went dark.

WORLD ECONOMIC FORUM Agenda Platforms Reports Events About English TopLink

Global Agenda | COVID-19 | Cybersecurity | Cybercrime

Why COVID-19 is making utilities more vulnerable to cyberattack - and what to do about it

Photo credit: Getty Images



RANSOMWARE | THREAT ANALYSIS

Honda and Enel impacted by cyber attack suspected to be ransomware

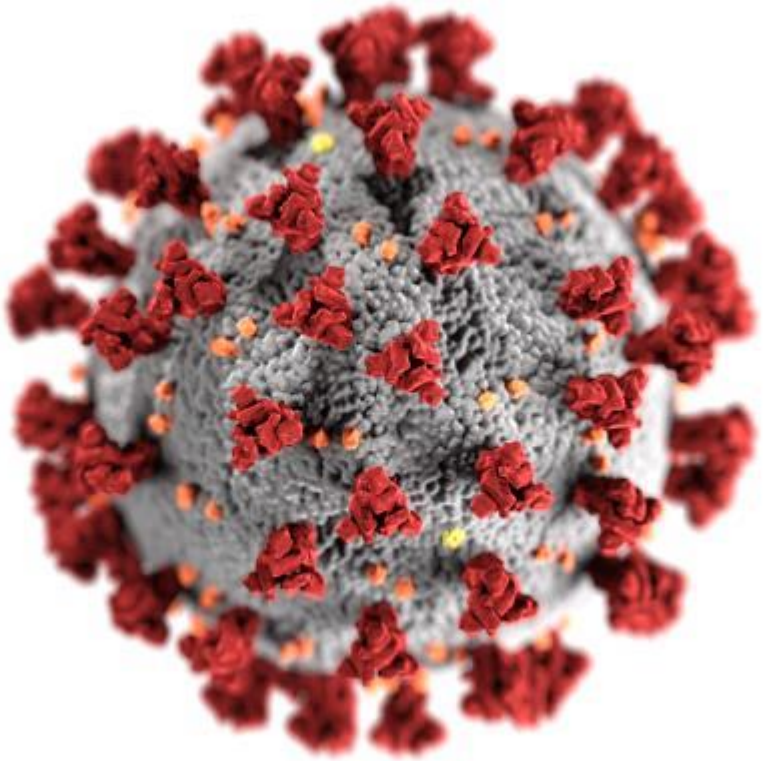
Posted: June 9, 2020 by Threat Intelligence Team

Car manufacturer Honda has been hit by a cyber attack, according to a report published by the BBC, and later confirmed by the company in a tweet. Another similar attack, also disclosed on Twitter, hit Edesur S.A., one of the companies belonging to Enel Argentina which operates in the business of energy distribution in the City of Buenos Aires.

Based on samples posted online, these incidents may be tied to the EKANS/SNAKE ransomware family. In this blog post, we review what is known about this ransomware strain and what we have been able to analyze so far.

ACER
Agency for the Cooperation of Energy Regulators

And After?



ACER
Agency for the Cooperation of Energy Regulators

My lessons learned.....

- **Trends linked to cybersecurity in the energy sector are unpredictable**: it is not easy (or almost impossible) to be prudent when all elements fluctuate around an unreasonable level of risk.
- From today, let's focus on **investments for a "secure digitalisation"**: let's stop talking of "digitalisation" and "cyber security" on two parallel rails: they must converge to achieve a really prudent approach.
- **Regulators** shall stop now: try to assess status of plans, assess and understand status of cybersecurity in the respective markets, assess cybersecurity trends and cybersecurity priorities (in terms of "measures"), review objectives, talk to consumers and operators.
- **Operators** shall stop now: assess their own risks and the risks they may create for others, re-assess costs of projects in a high demand time, make a consistent evaluation of absolutely necessary priorities, focus on those priorities (e.g. Cyber hygiene).
- **Consumers shall sustain the markets**, and thanks to the reduction of the energy prices (at least in the case of Europe), will be more open to understand (if they will be explained in the appropriate manner that cybersecurity) that cybersecurity expense if not yet another "tax" but a well-justified need.

At the end of the pandemic I expect we will .....

- ...be more **mature** and more **prudent** in **respect to the Cybersecurity** approach and the way it shall be tackled;
- ..... be more aware of the **need to act as a «system»** without the need of having prescriptive regulation, jut in the common interest;
- ..... be more **cooperative and open to listen** when the topic starts with the world «cyber».
- …. be fully aware that there is **no perfect and prudent plan in emergency**, but **«prudence» can and shall still be the «core» of good regulatory efforts**.
- ….. understand that **frameworks** can give us a **substantial help** in setting-up regulatory efforts, but during an **emergency**, **prudence of investments is also delegated to the individual responsibility of all actors taking part to the life of the global energy community and of the grid** (We cannot rely on the Regulator only, but we rely on all of «Us»).
- ….be aware that the **grid is an essential** (and not only a «critical») **infrastructure**, and we need all together be very **prudent in investing money in order to safeguard and defend** (but not only) **its underlying cyber space**.

Thank you for your attention!

Please, share with me (us) your feedback, reflections and comments:

Stefano.BRACCO@acer.europa.eu

www.acer.europa.eu