vb 2024 DUBLIN

2 - 4 October, 2024 / Dublin, Ireland

CODE BLUE: ENERGY

Righard Zwienenberg

ESET, The Netherlands

Josep Albors

Ontinet, Spain

righard.zwienenberg@eset.com
josep@ontinet.com

ABSTRACT

No, this paper is not about an energy drink: it's all about the experience of encountering a life-threatening emergency. Energy: its availability is something we all take for granted and are all highly dependent on; hence its generation and distribution is part of a nation's critical infrastructure (CI).

It's understandable that, in modern warfare, nation-states or APT groups (try to) attack their opponent's CI, including the energy sector. Remember BlackEnergy or Industroyer, where energy systems fell victim to cyber attacks?

An energy system does not have to fall victim to a cyber attack to stop producing energy. We have the sad examples of the nuclear reactors at Fukushima after a natural disaster, as well as the Zaporizhzhia Nuclear Power Plant in Ukraine, where we still are in fear because of the ongoing war.

With the ever-increasing price of energy, many homes are now equipped with solar panels. Besides cost savings, solar panels also make the building's occupants less dependent on the power grid. These solar panels are also able to return any unused generated electricity to the power grid. Since almost all houses that have solar panels are smart homes, the panels are connected, and it can be fun to see one's daily savings in an app.

However, worldwide, power grids are mostly old and cannot handle too much generated power being put back into the net – the result could be an overload, causing cables to melt. To stop this from happening, power companies can usually either not take your generated electricity or shut down one or more of your solar panels – and that, without you knowing it, is costing you money. Of course, this is understandable, as melted electricity supply cables are not something we want. But if the power company can shut down your solar panels remotely, so can other people when they figure out how to do it.

To cut emissions, last year, the European Union adopted a law to make all new cars and vans sold in Europe zero-emission from 2035, and many people are already switching to electric vehicles. The future traffic jams will be at the charging stations. But the charging stations are the next problem. For mobility, we will be dependent on electricity. Not only can a country be paralysed by shutting down a power system, but it will be paralysed further when most cars are electric, and more so if *all* vehicles are electric, including emergency service vehicles.

Critical infrastructure always needs to be protected against attacks. But what happens if an attack is successful? In our presentation we will investigate potential attacks against the energy sector, the problems around solar panels, attacks against hybrid cars, and the hacking of and physical damage to electric car chargers as a result of a cyber attack. We will present real-life scenarios where these attacks can affect our daily lives and threaten not just our cars and houses, but also all the smart buildings under construction around the world.

INTRODUCTION

Since the industrial revolution we have been consuming more and more energy. Until the mid-19th century, traditional biomass was the dominant source of energy used across the world, but with the industrial revolution came the rise of coal to power steam engines and machinery, and throughout the 20th century the world adopted a broader range of sources [1] as fossil-fuel-driven engines became the norm and electricity became an integral part of our everyday lives. In 1882 Thomas Edison's Pearl Street Station became the first purpose-built power station [2], but electricity plants became commonplace through the 20th century, ranging from coal and gas burning to hydropower and nuclear power plants. Nowadays, these are complemented with solar panel parks, wind turbine parks and geothermal plants. These are all needed, since in this era of computers, IoT devices, smart homes, smart cities, electric cars, and mining of crypto coins, we consume extremely large amounts of power. It is no surprise that electricity is considered a basic necessity of life and thus a part of the critical infrastructure.

And of course, with modern warfare, attacks on the critical infrastructure are an unfortunate reality for civilians.

CYBER ATTACKS TARGETING CRITICAL ELECTRICAL INFRASTRUCTURE

In recent years we have seen several examples of cyber attacks targeting energy-related critical infrastructure. The most recent ones are operations involved in the war between Russia and Ukraine – incidents that intensified after Russia's invasion of Ukraine on 24 February 2022. But the Russian cyber attacks didn't begin on that date; APT groups with direct links to the Kremlin, such as Sandworm (APT44), have been deploying threats in the Ukrainian energy infrastructure for over a decade, some of which have been very advanced.

Consider, for example, BlackEnergy – an attack that took place on 23 December 2015, in which around half of the homes in the Ivano-Frankivsk region of Ukraine were left without electricity for a few hours. *ESET* researchers discovered that this case was not an isolated incident and that other energy companies in Ukraine were targeted by the attackers at the same time [3].

Until that date, BlackEnergy was known as malware used for various purposes, such as a series of cyberespionage attacks against high-value, government-related targets in Ukraine, as discussed at the *Virus Bulletin* security conference in 2014 [4]. But in those attacks, a destructive KillDisk trojan was downloaded and executed on systems previously infested with

the BlackEnergy trojan. Interestingly, this KillDisk trojan would look for any process related to industrial control systems (ICS), terminating it and overwriting its corresponding executable file on the hard drive with random data in order to make restoration of the system more time-consuming and difficult.

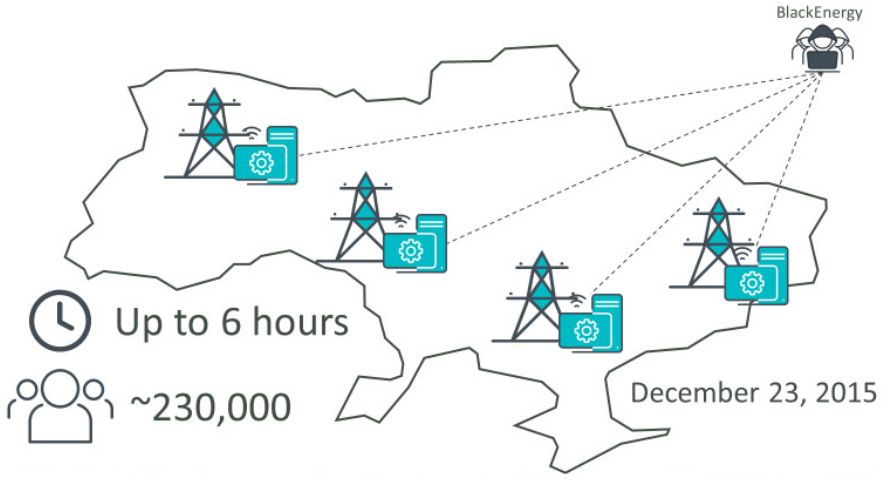

Figure 1: BlackEnergy: the first blackout.

But the BlackEnergy cyber attack in 2015 was just the preparation for what was going to come a year later. On 17 December 2016 the malware later known as Industroyer was deployed in a local electrical substation in Ukraine, using advanced techniques to look for specific industrial control devices whose communication protocols it could speak. Then, like a time bomb going off, it apparently opened every circuit breaker at once, while defying any attempts by the substation operators to regain easy control: if an operator tried to close a breaker, the malware opened it back up [5].

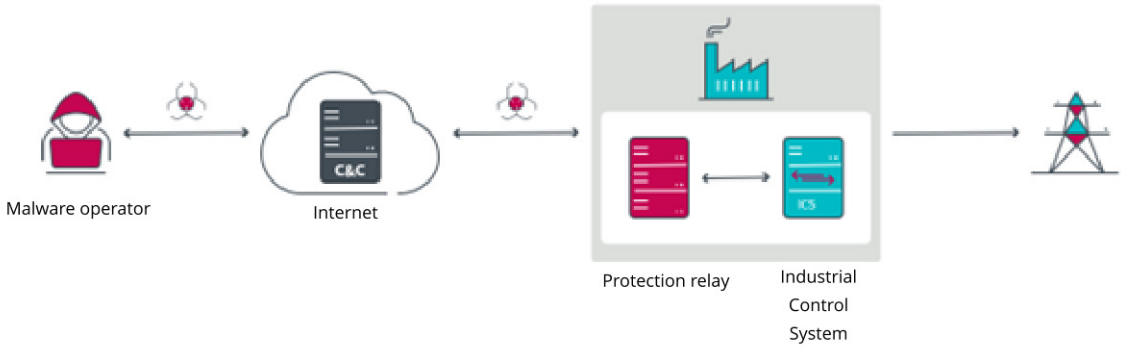

Figure 2: Industroyer (December 2016).

When the Russian invasion of Ukraine started, we saw an evolution of Industroyer as Sandworm made an attempt to deploy the Industroyer2 malware against high-voltage electrical substations in Ukraine [6, 7]. Luckily, this attempt was discovered by CERT-UA, who, along with *ESET* researchers, worked to remediate and protect this critical infrastructure network. Unlike Industroyer, Industroyer 2 only implements the IEC-104 (a.k.a. IEC 60870-5-104) protocol to communicate with industrial equipment. This includes protection relays, used in electrical substations. This is a slight change from the 2016 Industroyer variant, which is a fully modular platform with payloads for multiple ICS protocols.

In coordination with the deployment of Industroyer2 in the ICS network, the attackers attempted to wreak havoc with a new version of the CaddyWiper destructive malware [7]. It is believed that this was intended to slow down the recovery process and prevent operators of the energy company from regaining control of the ICS consoles. It was also deployed on the machine where Industroyer2 was executed, likely to cover the attackers' tracks. Figure 3 shows an overview of the malware deployed in the attack.

The first version of CaddyWiper was discovered by *ESET* researchers in Ukraine on 14 March 2022 [8], when it was deployed in the network of a bank. It was deployed via Group Policy Object (GPO), indicating that the attackers had gained control of the target's Active Directory Domain Services on the network beforehand. The wiper erases user data and partition information from attached drives, making the affected systems inoperable and unrecoverable.

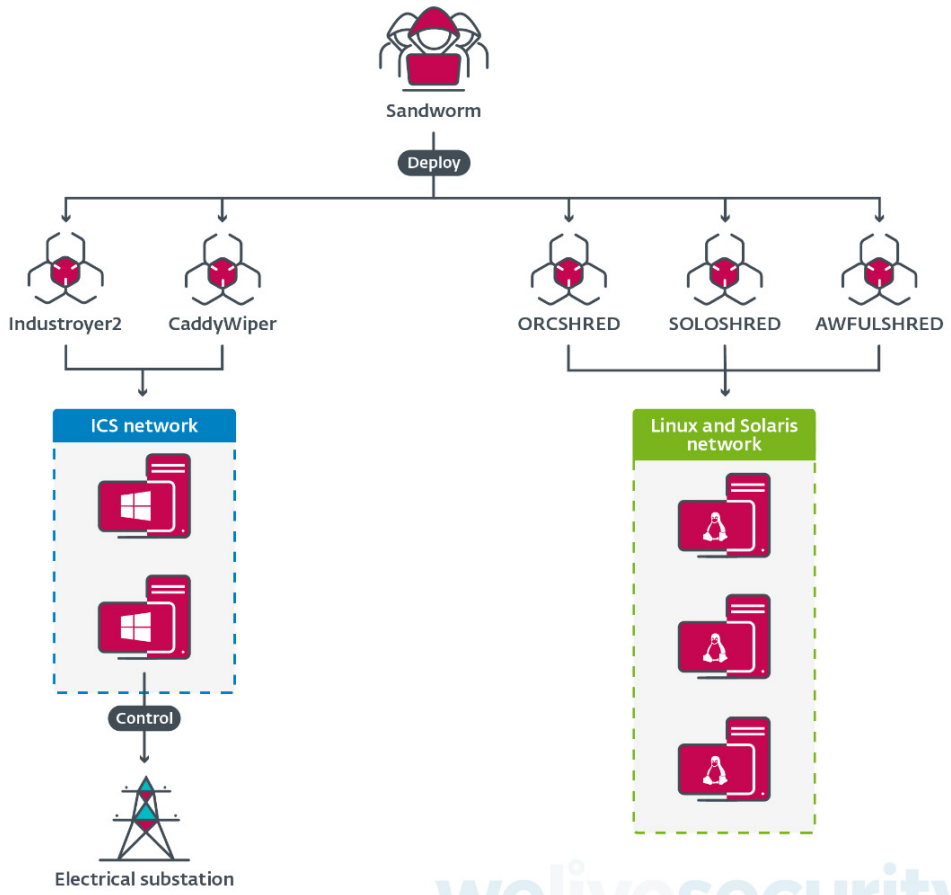

Figure 3: Overview of the malware deployed in the attack.

OTHER POTENTIAL DANGERS TO CRITICAL ELECTRICAL INFRASTRUCTURE

There are other potential risks to electrical infrastructure besides cyber attacks. We have to take into consideration the forces of nature and how they can affect the infrastructures of all kinds of electrical power generators. It's not only that we can't generate enough power on a cloudy day if we use solar panels and that we can't generate enough power from wind farms if there's no wind. Even other ways of generating power are affected by nature. We have the tragic example of the Fukushima Daiichi nuclear accident on 11 March 2011 [9], which occurred as a direct consequence of the M 9.1 undersea earthquake in the Pacific Ocean, 72 km east of the Oshika Peninsula of the Tōhoku region of north-east Japan, and its consequent tsunami. The power plant's security procedure resisted the earthquake, with all operating reactors shutting down, but the tsunami waves (some of them reaching 13-14m) damaged nearly all of the power plant's backup energy sources, and the subsequent inability to cool the nuclear reactors after shutdown compromised containment and resulted in the release of radioactive contaminants into the surrounding environment.

If we continue to focus on the war in Ukraine, we see that conventional warfare has done a lot of damage to power plants around the country. From bombing power plants using missiles to destroying hydroelectric infrastructure, the Russian army has already caused a lot of physical damage that has put Ukraine's power supply at risk. Not only that, but Russian forces have on several occasions threatened to destroy the Zaporizhzhia nuclear power plant – the largest nuclear power plant in Europe – and any such incident could affect not only Ukraine but also nearby European countries, as we know all too well from the 1986 Chernobyl disaster.

One might think that there is no way that Russian forces would provoke such a disaster, considering that it would also affect their troops and Russian territory, but we have experience from the destruction of the Kakhovka Dam in June 2023 [10], which caused extensive flooding along the lower Dnieper river, submerging several villages in Ukrainian- and Russian-controlled areas and destroying an important hydroelectric power plant.

SOLAR INSTALLATIONS

One way for people to ensure resilience in situations in which the electrical infrastructure is at risk is the use of (private) solar panels. That way, a household can still have electricity during daylight hours, and even during the night if the solar panels are complemented with a battery for storage.

Many people nowadays deploy solar panels on their roofs or install small solar panel farms. On average, a solar panel pays for itself within seven years in terms of cost savings, and thereafter it will provide you with free energy, but in some cases a solar panel can pay for itself even before that: energy that is generated but unused can be fed into the electricity grid, where you get paid for it. A story too good to be true? Yes and no. At the moment, in many countries a practice known as 'net metering' [11] records the excess energy generated by a solar installation and applies it to the customer's bill as credit toward energy drawn from the grid. A good incentive for consumers to invest in the installation of solar panels.

However, the energy grid, designed decades ago, is increasingly showing its age as it struggles to accommodate the rising influx of power from both residential and commercial solar installations. Originally constructed to support a one-way flow of electricity from centralized power plants to consumers, the grid was not engineered to handle the bidirectional flow of energy now prevalent with distributed renewable energy sources like solar panels. This fundamental design limitation poses significant challenges, such as voltage fluctuations, grid instability, and potential overloads. As more households and businesses install solar panels, the excess energy fed back into the grid can lead to situations where the supply exceeds the demand, complicating the management of a stable and reliable power system [12].

The outdated infrastructure further exacerbates these challenges by lacking the necessary technological upgrades to integrate and optimize renewable energy sources effectively. Traditional grids often do not have the advanced monitoring and control systems needed to manage the variable and intermittent nature of solar power. Without these smart grid technologies, such as real-time data analytics, automated control systems, and enhanced grid storage solutions, utilities face difficulties in balancing the grid and maintaining energy quality. Upgrading the grid to a modern, flexible system that can seamlessly integrate distributed energy resources is crucial. This involves substantial investment in infrastructure enhancements, including smart inverters, advanced metering infrastructure (AMI), and robust energy storage systems. Only through these upgrades can the grid support the growing usage of solar panels and other renewable energy sources, ensuring a resilient and sustainable energy future.

Where the energy grid currently remains outdated, the energy companies have implemented measures to manage the surplus energy generated by solar panels, particularly during peak sunlight hours when production may exceed demand. One common measure is to exercise remote shutdown capabilities, enabled by smart inverters and grid management systems [13]. These smart inverters, required by regulation in many regions, can receive commands from the utility company to reduce or completely halt the energy production of individual solar installations. This is typically done to maintain grid stability, prevent overloads, and ensure a balanced supply-demand equation. When the grid is at risk of being overwhelmed by excess energy, the utility can remotely signal the inverters to curtail or cease production, effectively reducing the influx of solar-generated electricity into the grid.

Another approach involves dynamic pricing and incentive-based programmes where energy companies encourage consumers to use more electricity during times of high solar production. However, in situations where these measures are insufficient, utilities may also employ hardware-level interventions. For instance, grid operators might activate distributed energy resource management systems (DERMS) to selectively throttle or disconnect solar arrays from the grid. This integration of advanced grid management technology ensures that energy production aligns with real-time consumption patterns, preventing grid instability. By managing solar output in this manner, energy companies can maintain a stable and reliable power supply, accommodating the variable nature of renewable energy sources while safeguarding the integrity of the electrical grid.

Climate change-induced heat waves present both opportunities and challenges for consumers generating energy with solar panels. On the one hand, solar panels are particularly efficient during periods of intense sunlight, which often coincide with heat waves. This can result in increased energy production and potentially significant savings on electricity bills for consumers. Additionally, generating solar energy reduces reliance on fossil fuels, contributing to efforts to mitigate climate change by lowering carbon emissions. Many consumers view solar panels as a sustainable and environmentally friendly investment, aligning with broader societal goals of transitioning towards renewable energy sources.

However, the surge in solar energy production during heat waves also poses a high risk of overloading the grid. As temperatures rise, so does the demand for electricity, driven by the increased use of air conditioning and cooling systems. Simultaneously, solar panels ramp up their energy output, potentially flooding the grid with surplus electricity. If not managed properly, this excess energy can strain the grid, leading to instability and even blackouts. To address this challenge, effective grid management strategies, such as smart grid technologies and energy storage systems, are essential. These solutions can help balance supply and demand, optimize energy distribution, and enhance the grid's resilience to fluctuations caused by heat waves.

ELECTRIC VEHICLES

EU law requires that, from 2030, all new cars must have 55% lower CO_2 emissions versus 2021 levels, and that, starting in 2035, all cars sold in the European Union must be zero-emission vehicles. This ambitious mandate reflects a major push towards reducing the automotive sector's impact on the climate, aiming to significantly reduce greenhouse gas emissions and combat climate change, aligning with the EU's broader environmental and sustainability goals.

To meet these targets manufacturers will need to innovate aggressively, incorporating advanced technologies such as lightweight materials, hybrid systems, and more efficient powertrains. Automotive manufacturers will need to accelerate

their development of affordable, high-performance zero-emission models, while governments and private sectors must invest heavily in expanding the infrastructure for electric vehicle charging and investing in renewable energy sources to power these vehicles. Achieving these goals will not only contribute to lowering greenhouse gas emissions, but also drive economic and technological advancements in the automotive industry.

Having more and more electric vehicles comes with problems, e.g. at EU holiday parks where people are using the electric sockets in their bungalows to charge their electric vehicles. Holiday parks are increasingly reassessing their policies on providing free electric vehicle charging for tourists, driven by the growing number of electric vehicles on the road and the rising costs associated with offering this amenity. Initially, many holiday parks offered free electric vehicle charging as an incentive to attract eco-conscious tourists and promote sustainable travel. However, as electric vehicle adoption has surged, the demand for charging facilities has grown rapidly, leading to significant increases in electricity consumption and associated costs. This has prompted many holiday park operators to reconsider their approach, moving towards paid charging models to cover the expenses of electricity and maintenance of the charging infrastructure.

To manage this transition, holiday parks are implementing various strategies to ensure a smooth shift from free to paid electric vehicle charging. Some parks are introducing tiered pricing structures, where guests can choose from different charging speeds at varying costs, thereby providing flexibility based on their needs and budgets. Others are partnering with specialized electric vehicle charging service providers to install advanced charging stations that can handle increased usage efficiently while integrating seamless payment systems. Additionally, holiday parks are investing in renewable energy sources, such as solar panels, to power their charging stations sustainably and reduce overall operational costs. By moving to paid electric vehicle charging, holiday parks aim to create a sustainable model that supports the growing number of electric vehicle users while ensuring fair distribution of costs and resources.

SERVICE VEHICLES

A more serious consideration relating to electric vehicles is that an energy outage can quickly escalate into a logistical nightmare when all service vehicles rely on electricity. In today's world, where many service fleets have transitioned to electric vehicles for environmental and economic reasons, a sudden loss of power can render these vehicles immobile, crippling essential services. Imagine a scenario where emergency responders, utility repair teams, and delivery services are all unable to operate due to a lack of energy. Without access to fuel stations, which also require electricity to function, these vehicles become stranded, exacerbating the impact of the outage.

Moreover, the interconnectedness of modern infrastructure magnifies the consequences of such a scenario. With electric vehicles unable to move, essential services like medical assistance and food distribution are severely disrupted. Hospitals may struggle to receive critical supplies, and communities could face shortages of basic necessities. This vulnerability underscores the importance of diversifying energy sources and investing in robust backup systems to ensure that essential services can continue even in the face of energy disruptions.

Electric vehicles increasingly mean smart vehicles, and as we have seen with IoT devices, this inevitably means that attempts will be made to hack them for various criminal activities. While that is a topic for another paper, researchers are already investigating the implications of smart vehicle-mediated crime [14].

CONCLUSION

Having reviewed several of the potential risks that the power generating infrastructure and mobility solutions based on electricity are facing, or will face in the near future, it is time for us to think about what we can do to avoid as many of those risks as possible. It is good to evolve to a carbon-free society based on renewable energies (and new generation nuclear reactors working as backup), but we can't look away from those risks. We have to face them and consider all the possibilities of suffering an incident – no matter whether it's caused by nature, a war, or a cyber attack – to minimize negative consequences as much as possible.

REFERENCES

[1] Ritchie, H. How have the world's energy sources changed over the last two centuries? OurWorldInData.org. 2021. https://ourworldindata.org/global-energy-200-years.

[2] Patel, S.; Larson, A.; Harvey, A. History of Power: The Evolution of the Electric Generation Industry. POWER. October 2017. https://www.powermag.com/history-of-power-the-evolution-of-the-electric-generation-industry/.

[3] Lipovsky, R. BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry. We Live Security. 4 January 2016. https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.

[4] Lipovsky, R.; Cherepanov, A. Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland. Virus Bulletin. 2014. https://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland.

[5] Cherepanov, A.; Lipovsky, R. Industroyer: Biggest threat to industrial control systems since Stuxnet. We Live Security. 12 June 2017. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

[6] Lameiras, A. Industroyer: A cyber-weapon that brought down a power grid. We Live Security. 13 June 2022. https://www.welivesecurity.com/2022/06/13/industroyer-cyber-weapon-brought-down-power-grid/.

[7] ESET Research. Industroyer2: Industroyer reloaded. We Live Security. 12 April 2022. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

[8] https://x.com/ESETresearch/status/1503436420886712321.

[9] Wikipedia. Fukushima nuclear accident. https://en.wikipedia.org/wiki/Fukushima_nuclear_accident.

[10] Wikipedia. Destruction of the Kakhovka Dam. https://en.wikipedia.org/wiki/Destruction_of_the_Kakhovka_Dam.

[11] Solar Energy Industries Association. Net Metering. https://www.seia.org/initiatives/net-metering.

[12] Hier. Crowded power grid and solar panels failing: this is what you need to know. https://www.hier.nu/zonnepanelen/drukte-op-het-stroomnet-waarom-vallen-zonnepanelen-soms-uit.

[13] Liander. Inverter switches off. https://www.liander.nl/storingen-en-onderhoud/spanningsproblemen/omvormer-schakelt-uit.

[14] Goretsky, A.; Camp, C. Fuel for thought: Can a driverless car get arrested? We Live Security. 21 November 2023. https://www.welivesecurity.com/en/cybersecurity/fuel-thought-can-driverless-car-get-arrested/.