



By: TA Analysis

Thousands of open gateways to European power plants



The Dutch National Cyber Security Centre and the Hague-based company Modat, which scans the internet for vulnerable devices, published **research** on European wind farms and solar power plants.

In 35 of the 40 countries they examined, they found 8,547 power plant control systems accessible from the public internet.

Most are password-entry pages for controlling equipment, but among them is the page of a wind turbine with real-time production data, buttons to start and stop it, and its exact location on a map.

One of the authors, Soufian El Yadmani, stated that an **attacker** could take full control of a plant at around 181 locations.

The researchers stress that the real number is likely higher, as they counted only systems they could reliably link to a specific power plant, and they notified the owners through national cyber security services without releasing the names of the plants.

The findings come five months after the European Commission decided to phase out Chinese inverters – devices that adapt electricity from solar panels for the grid – from projects funded by the European Union.

With this decision, Brussels is protecting itself against the risk that a manufacturer from a country with which Europe has strained relations could retain the ability to manage power plants remotely.

Research from The Hague and the attack on the Polish energy sector in December last year show, however, that the main weakness of European power plants lies in factory-set passwords and control pages left on the public internet, regardless of who manufactured the equipment, while Europe is currently far more concerned with the origin of the devices than with how they are configured.

The countries that built the fastest left the most gateways

open

The largest number of systems accessible from the internet was found in countries that have built solar and wind farms most rapidly in recent years.

Of the 7,942 such systems in solar power plants, Spain has 2,766 and Greece 1,860, meaning Spain, Greece, Italy and Germany together account for three quarters of all the faults identified.

At wind farms, 605 systems were found in 23 countries, most of them in Germany, with 212, and Italy, with 192.

The researchers warn that this ranking partly depends on where they could reliably link systems to a specific power plant.

Renewable sources in the second quarter of 2026 provided 54.1 per cent of the electricity produced in the European Union

Today, these power plants generate a large share of Europe's electricity. According to **Eurostat data**, renewable sources in the second quarter of 2026 provided 54.1 per cent of the electricity produced in the European Union, and solar and wind together accounted for more than a third of total output.

Solar parks and wind farms are generally far from cities and operate without a permanent crew, so they are monitored, maintained and adjusted remotely, as sending service technicians to each turbine for every check would be too expensive.

The same connection through which the owner manages the power plant from another city or another country, however, is accessible to anyone who finds the management page and guesses or steals the password.

This is not difficult for an attacker today, because there are internet tools that recognise device types and their login pages.

Smaller solar parks use the same network devices, equipment management computers and monitoring software as dozens of others, so an attacker who finds a configuration error in one place can easily find it in hundreds of others.

The researchers also found pages where "root" was pre-entered as the username, a designation that on many devices grants full control over the system.

The attack on Poland went through the same door

What happens when someone actually passes through such an entrance was illustrated by a coordinated attack on Poland on 29 December 2025.

According to a report by **CERT Polska**, the Polish state cyber security service, more than 30 wind farms and solar power plants, one private manufacturing company and a large heating plant supplying heat to almost half a million users were attacked.

CERT Polska concluded that the sole objective of the attack was to destroy or disable equipment.

The attackers used a data-wiping programme but failed to run it in the heating plant, so users did not lose heating.

In the case of the wind farms and solar power plants, the attackers gained access to the substation control points linking the plants to the grid and severed the connection between the plants and the electricity distributor, even though the plants continued to generate power.

CERT Polska attributes the attack to a group known as Static Tundra, which it links to a unit of the Russian Federal Security Service

They accessed the equipment via remote-access devices reachable from the internet that were protected only by a password, without additional identity verification, and via equipment management computers that still used factory-set passwords.

These were exactly the weaknesses that researchers from The Hague identified at thousands of locations across Europe, and none of the devices cited by CERT Polska in the report was made in China.

CERT Polska attributes the attack to a group known as Static Tundra, which it links to a unit of the Russian Federal Security Service, while cybersecurity companies ESET and Dragos, with moderate confidence, attribute it to the Sandworm group, which is linked to Russian military intelligence.

The assessments therefore differ only over which Russian service was behind the attack. Moscow denies all accusations of sabotage and cyberattacks against European infrastructure.

From the wind farm to the city heating plant

The most serious finding was published in August, when CERT Polska presented details of another **heating plant attacked** on the same day, which supplies heat to around 50,000 residents.

The attacker first accessed a wind farm substation via a remote-access device protected only by a password and then, using a mobile connection, reached the closed network used by the electricity distributor to communicate with its facilities.

Owing to a configuration error, devices in that network could freely connect to one another, so the attacker located a computer used to control equipment in the heating plant, which still had the factory password, and used it to access the plant 11 days before the attack.

The perpetrator shut down the steam turbine and water treatment system and locked the control computers with new passwords

On the day of the attack, the perpetrator shut down the steam turbine and water treatment system and locked the control computers with new passwords, but workers managed to restore the plant before residents lost heat and power.

CERT Polska warns that the same configuration error is common in Poland and probably occurs in other countries as well, meaning that an inadequately protected wind farm can serve as an entry point to plants that supply heat and water to cities.

Disconnecting wind farms is not harmless, although it is often underestimated. The network operator must always know how much electricity is being produced and which power plants can be instructed to adjust their output.

When data from dozens of locations is lost, the operator must keep larger reserves and make decisions without a complete picture.

The **collapse of the grid in Spain** and Portugal on 28 April 2025 was not caused by a cyberattack, but by problems with voltage maintenance in the grid, as the final report of the European transmission network operators concluded in March.

However, it showed how quickly a system with a large share of solar energy can fail when the operator does not fully control power plant operations.

Spain currently has the largest number of solar systems accessible via the internet.

Brussels checks the origin of the device, attackers the

password

The European Union has significantly tightened the rules in recent years. The **NIS2 directive** requires medium-sized and large energy companies to assess and reduce the risk of cyber attacks, report serious incidents and follow rules for tenders for the construction of new solar and wind power plants which, from 2025, stipulate that protection must be built into the project and that operational control of the power plant must remain with a European company.

In January, the **Commission** proposed changes to cyber security laws that could exclude suppliers deemed risky by the EU from 18 key economic sectors, and in May it decided to phase out **Chinese inverters** from EU-funded projects, with full application to new contracts from April 2027.



Chinese manufacturers hold around 80 per cent of the global inverter market, and their chamber of commerce in Brussels has rejected claims that the equipment could be used against Europe

Chinese manufacturers hold around 80 per cent of the global inverter market, and their chamber of commerce in Brussels has rejected claims that the equipment could be used against Europe.

These rules mainly apply to new projects and larger companies, whereas much of Europe's solar and wind capacity was built before they became mandatory.

Solar and wind power plants in Europe have a

wide range of owners, from large energy companies and investment funds to local businesses and firms established solely to construct a single plant.

The NIS2 directive mainly covers medium-sized and large companies, so many smaller owners do not have the same obligations to protect against cyber attacks, unless the state explicitly includes them in its regulations.

Everyone involved in operating a power plant sees only their own part of the work.

The electricity distributor knows where the power plant is connected to the grid, the equipment manufacturer knows in which power plants its devices are installed, and the service company knows how to access those devices remotely.

None of them knows how many devices in total are reachable from the internet or where they are located. Such an overview for the whole of Europe has now been produced for the first time by researchers based in The Hague.

The real test will come in winter

Russian services have already demonstrated in Poland that they know how to identify such entry points and are prepared to use them to disable facilities.

The most challenging period for the European grid is winter, when electricity consumption is highest and any power plant outage affects supply.

How many of the 8,547 control systems have been removed from the public internet or protected with stronger passwords and additional identity verification

Until then, it remains to be seen what power plant owners have done following the warning from the Hague researchers: how many of the

8,547 control systems have been removed from the public internet or protected with stronger passwords and additional identity verification.

To a large extent, this will determine whether the attackers can repeat, this winter in another European country, what they accomplished in Poland last December, when they accessed a municipal heating plant via a wind farm and brought its turbine to a halt.

After 2022, Europe rapidly built solar and wind power plants to end its dependence on Russian gas, the flow of which Moscow could cut off whenever it wished.

But while the control systems of those power plants remain connected to the internet, Russian services can switch them off remotely and thus once again gain the opportunity to deny Europe part of its electricity supply.

Europe must treat an attack on a power plant in one member state as an attack on all and respond jointly, by publicly naming the Russian services and individuals responsible and using the sanctions that the EU already has available for cyber attacks, because the same service that attacked Polish power plants can attack Spanish, Greek or German ones tomorrow.