U.S. not prepared for power grid cyberattack

By Garance Burke and Jonathan Fahey, AP

Security researcher Brian Wallace was on the trail of hackers who had snatched a California university's housing files when he stumbled into a larger nightmare: Cyberattackers had opened a pathway into the networks running the United States power grid.

Digital clues pointed to Iranian hackers. And Wallace found that they had already taken passwords, as well as engineering drawings of dozens of power plants, at least one with the title "Mission Critical." The drawings were so detailed that experts say skilled attackers could have used them, along with other tools and malicious code, to knock out electricity flowing to millions of homes.

Wallace was astonished. But this breach, the Associated Press has found, was not unique.

About a dozen times in the last decade, sophisticated foreign hackers have gained enough remote access to control the operations networks that keep the lights on, according to top experts who spoke only on condition of anonymity due to the sensitive nature of the subject matter.

The public almost never learns the details about these types of attacks — they're rarer but also more intricate and potentially dangerous than data theft. Information about the government's response to these hacks is often protected and sometimes classified; many are never even reported to the government.

These intrusions have not caused the kind of cascading blackouts that are feared by the intelligence community. But

so many attackers have stowed away in the systems that run the U.S. electric grid that experts say they likely have the capability to strike at will.

And that’s what worries Wallace and other cybersecurity experts most.

“If the geopolitical situation changes and Iran wants to target these facilities, if they have this kind of information it will make it a lot easier,” said Robert M. Lee, a former U.S. Air Force cyberwarfare operations officer. “It will also help them stay quiet and stealthy inside.”

In 2012 and 2013, in well-publicized attacks, Russian hackers successfully sent and received encrypted commands to U.S. public utilities and power generators; some private firms concluded this was an effort to position interlopers to act in the event of a political crisis. And the Department of Homeland Security announced about a year ago that a separate hacking campaign, believed by some private firms to have Russian origins, had injected software with malware that allowed the attackers to spy on U.S. energy companies.

“You want to be stealth,” said Lillian Ablon, a cybersecurity expert at the RAND Corporation. “That’s the ultimate power, because when you need to do something you are already in place.”

The hackers have gained access to an aging, outdated power system. Many of the substations and equipment that move power across the U.S. are decrepit and were never built with network security in mind; hooking the plants up to the Internet over the last decade has given hackers new backdoors in. Distant wind farms, home solar panels, smart meters and other networked devices must be remotely monitored and controlled, which opens up the broader system to fresh points of attack.

Hundreds of contractors sell software and equipment to energy companies, and attackers have successfully used those outside

companies as a way to get inside networks tied to the grid.

Attributing attacks is notoriously tricky. Neither U.S. officials nor cybersecurity experts would or could say if the Islamic Republic of Iran was involved in the attack Wallace discovered involving Calpine Corp., a power producer with 82 plants operating in 18 states and Canada.

Private firms have alleged other recent hacks of networks and machinery tied to the U.S. power grid were carried out by teams from within Russia and China, some with governmental support.

Even the Islamic State group is trying to hack American power companies, a top Homeland Security official told industry executives in October.

Homeland Security spokesman SY Lee said that his agency is coordinating efforts to strengthen grid cybersecurity nationwide and to raise awareness about evolving threats to the electric sector through industry trainings and risk assessments. As Deputy Secretary Alejandro Mayorkas acknowledged in an interview, however, “we are not where we need to be” on cybersecurity.

That’s partly because the grid is largely privately owned and has entire sections that fall outside federal regulation, which experts argue leaves the industry poorly defended against a growing universe of hackers seeking to access its networks.

As Deputy Energy Secretary Elizabeth Sherwood Randall said in a speech earlier this year, “If we don’t protect the energy sector, we are putting every other sector of the economy in peril.”

The attack involving Calpine is particularly disturbing because the cyberspies grabbed so much, according to interviews and previously unreported documents.

Cybersecurity experts say the breach began at least as far back as August 2013, and could still be going on today.

Calpine spokesman Brett Kerr said the company's information was stolen from a contractor that does business with Calpine. He said the stolen diagrams and passwords were old – some diagrams dated to 2002 – and presented no threat, though some outside experts disagree.

Kerr would not say whether the configuration of the power plants' operations networks – also valuable information – remained the same as when the intrusion occurred, or whether it was possible the attackers still had a foothold.

According to the AP investigation, the hackers got:

- User names and passwords that could be used to connect remotely to Calpine's networks, which were being maintained by a data security company. Even if some of the information was outdated, experts say skilled hackers could have found a way to update the passwords and slip past firewalls to get into the operations network. Eventually, they say, the intruders could shut down generating stations, foul communications networks and possibly cause a blackout near the plants.
- Detailed engineering drawings of networks and power stations from New York to California – 71 in all – showing the precise location of devices that communicate with gas turbines, boilers and other crucial equipment attackers would need to hack specific plants.
- Additional diagrams showing how those local plants transmit information back to the company's virtual cloud, knowledge attackers could use to mask their activity. For example, one map shows how information flows from the Agnews power plant in San Jose near the San Francisco 49ers football stadium, to the company headquarters in Houston.

Wallace first came across the breach while tracking a new strain of noxious software that had been used to steal student housing files at the UC Santa Barbara.

“I saw a mention in our logs that the attackers stored their malware in some FTP servers online,” said Wallace, who had recently joined the Irvine-based cybersecurity firm Cylance Inc., fresh out of college. “It wasn’t even my job to look into it, but I just thought there had to be something more there.”

Wallace started digging. Soon, he found the FTP servers, typically used to transfer large numbers of files back and forth across the Internet, and the hackers’ ill-gotten data — a tranche of more than 19,000 stolen files from thousands of computers across the world, including key documents from Calpine.

Before Wallace could dive into the files, his first priority was to track where the hackers would strike next — and try to stop them.

He started staying up nights, often jittery on Red Bull, to reverse-engineer malware. He waited to get pinged that the intruders were at it again.

Months later, Wallace got the alert: From Internet Protocol addresses in Tehran, the hackers had deployed TinyZbot, a Trojan horse-style of software that the attackers used to gain backdoor access to their targets, log their keystrokes and take screen shots of their information. The hacking group, he would find, included members in the Netherlands, Canada, and the United Kingdom.

The more he followed their trail, the more nervous Wallace got. According to Cylance, the intruders had launched digital offensives that netted information about Pakistan International Airlines, the Mexican oil giant Pemex, the Israel Institute of Technology and Navy Marine Corps Intranet,

a legacy network of the U.S. military. None of the four responded to AP's request for comment.

Then he discovered evidence of the attackers' most terrifying heist – a folder containing dozens of engineers' diagrams of the Calpine power plants.

According to multiple sources, the drawings contained user names and passwords that an intruder would need to break through a firewall separating Calpine's communications and operations networks, then move around in the network where the turbines are controlled. The schematics also displayed the locations of devices inside the plants' process control networks that receive information from power-generating equipment. With those details, experts say skilled hackers could have penetrated the operations network and eventually shut down generating stations, possibly causing a blackout.

Cylance researchers said the intruders stored their stolen goods on seven unencrypted FTP servers requiring no authentication to access details about Calpine's plants. Jumbled in the folders was code that could be used to spread malware to other companies without being traced back to the attackers' computers, as well as handcrafted software designed to mask that the Internet Protocol addresses they were using were in Iran.

Circumstantial evidence such as snippets of Persian comments in the code helped investigators conclude that Iran was the source of the attacks.

Calpine didn't know its information had been compromised until it was informed by Cylance, Kerr said.

Iranian U.N. Mission spokesman Hamid Babaei did not return calls or address questions emailed by AP.

Cylance notified the FBI, which warned the U.S. energy sector in an unclassified bulletin last December that a group using

Iran-based IP addresses had targeted the industry.

Whether there was any connection between the Iranian government and the individual hackers who Wallace traced — with the usernames parviz, Alireza, Kaj, Salman Ghazikhani and Bahman Mohebbi — is unclear.

Cyberattacks designed to steal information are steadily growing in scope and frequency; there have been high-profile hacks of Target, eBay and federal targets such as the U.S. Office of Personnel Management. But assaults on the power grid and other critical infrastructure aim to go a step further.

Trained, well-funded adversaries can gain control of physical assets — power plants, substations and transmission equipment. With extensive control, they could knock out the electricity vital to daily life and the economy, and endanger the flow of power to mass transportation, military installations and home refrigerators.

In summer 2014, a hacker of unknown origin, using masking software called Tor, took over the controls of a large utility's wind farm, according to a former industry compliance official who reviewed a report that was scrubbed of the utility's name. The hacker then changed an important setting, called the automatic voltage regulator, from "automatic" to "manual," he said.

That seemingly simple change to any power plant can damage the generator and destabilize parts of the nearby grid if the plant's output is high enough.

Last year, Homeland Security released several maps that showed a virtual hit list of critical infrastructure, including two substations in the San Francisco Bay area, water and gas pipelines and a refinery. And according to a previously reported study by the Federal Energy Regulatory Commission, a

coordinated attack on just nine critical power stations could cause a coast-to-coast blackout that could last months, far longer than the one that plunged the Northeast into darkness in 2003.

“The grid is a tough target, but a lucrative target,” said Keith Alexander, the former director of the National Security Agency who now runs a cybersecurity firm. The number of sophisticated attacks is growing, he said. “There is a constant, steady upbeat. I see a rising tide.”

No one claims that it would be easy to bring down the grid. To circumvent companies’ security, adversaries must understand the networks well enough to write code that can communicate with tiny computers that control generators and other major equipment. Even then, it’s difficult to cause a widespread blackout because the grid is designed to keep electricity flowing when equipment or lines go down, an almost daily occurrence that customers never see.

Because it would take such expertise to plunge a city or region into darkness, some say threats to the grid are overstated — in particular, by those who get paid to help companies protect their networks. Still, even those who said the risks of cyber threats can be exaggerated agree it is possible for cyberattackers to cause a large-scale blackout.

Traditional central power stations and transmission systems include equipment that is decades old and physically unable to handle electronic threats. Some run on machines that use software that is so old that malware protections don’t exist, such as Windows ’95 and FORTRAN, a programming language developed in the 1950s.

At the Tennessee Valley Authority, a corporation owned by the federal government that powers 9 million households in the southeastern U.S., a former operations security expert said in recent years he saw passwords for some key operating systems

stored on sticky notes.

“Some of the control systems boot off of floppy disks,” said Patrick Miller, who has evaluated hydroelectric dam cybersecurity for the U.S. Bureau of Reclamation and Army Corps of Engineers. “Some dams have modeling systems that run on something that looks like a washing machine hooked up to tape spools. It looks like the early NASA stuff that went to the moon.”

The rush to tie smart meters, home programmable thermostats and other smart appliances to the grid also is causing fresh vulnerabilities.

About 45 percent of homes in the U.S. are hooked up to a smart meter, which measures electricity usage and shares information with the grid. The grid uses that information to adjust output or limit power deliveries to customers during peak hours.

Those meters are relatively simple by design, mostly to keep their cost low, but their security is flimsy. Some can be hacked by plugging in an adapter that costs $30 on eBay, researchers say.

FERC recently raised concerns about another area that is not covered by federal cybersecurity rules: contractors that sell energy companies software and equipment. As is evident from the Calpine incident, attackers have used outside companies to pull off hacks against energy companies.

“We’ve got these vulnerable systems out there that are old and never had security built into them, and now we’re exposing them to a wider audience,” said Justin Lowe, a utility cybersecurity expert at PA Consulting Group.

“That wider audience is getting much more hostile.”

The full extent of the attacks on the grid is not public knowledge. A Freedom of Information Act request by the AP for

information regarding any FBI investigations of such hacks was not fulfilled. The Department of Justice said that agency kept no record of how often any such cases had been prosecuted.

The North American Electric Reliability Corporation, which oversees the reliability of the electrical sector, collects information about cyber incidents involving utilities and other users, owners, and operators of the bulk power system – but it is scrubbed of identifying information and details are confidential and exempt from disclosure under FOIA.

Authorities say they take the threat seriously. In response to a FOIA request, Homeland Security said it had helped more than 100 energy and chemical companies improve their cyber defenses, and held both classified and unclassified briefings in June 2013 and late 2014 on threats to companies associated with power grid operations.

A small DHS team compiles statistics about hacks and vulnerabilities on control systems powering the grid and other public infrastructure, and responds to some attacks. But former federal employees who spoke on the condition of anonymity because the information was sensitive said government red tape kept the team from thoroughly responding to the smaller municipal and rural utilities that most needed their help, and that the statistics overstated the agency's grasp of the problem.

The companies themselves say they are vigilant – though they caution no fortifications are foolproof.

Early this year, an operations supervisor in Virginia for a subsidiary of American Electric Power – the nation's largest power grid operator, with operations in 38 states – opened a personal email on a company laptop and unwittingly downloaded a piece of malware called CryptoLocker.

Known as "ransomware," CryptoLocker is a relatively common type of malware that reaches to outside servers, usually

overseas, and downloads encryption instructions that scramble a computer's contents, making them inaccessible to anyone without a specific "key." The malware then moves through a computer – and computer network – and encrypts all the files it can, keeping users from accessing anything.

In exchange for a fee, the hackers provide the victim a key that allows the files to be unlocked.

Members of AEP's cyber-security team – housed in the company's Columbus, Ohio, headquarters behind an unmarked door that unlocks with a fingerprint scanner – saw the strange network behavior as soon as it started.

"When you see this (code) attempting to hit thousands of systems outside of the AEP network, that's a 'holy crap' moment," said Sean Parcel, AEP's lead cyberinvestigator.

Had CryptoLocker wormed its way into AEP's system, the business and operations networks could have locked up, experts say.

But Parcel said AEP's cyberteam already had blocked the foreign addresses that the malware needed to reach to start encrypting files, part of a policy of systematically blocking hundreds of Internet Protocol addresses each week to keep employees from inadvertently downloading malicious code.

AEP said the team remotely isolated and erased the supervisor's computer before its systems were affected.

Like most big utilities, AEP's power plants, substations and other vital equipment are managed by a network that is separated from the company's business software with layers of authentication, and is not accessible via the Internet. Creating that separation, and making sure that separation is maintained, is among the most important things utilities can do to protect the grid's physical assets.

But cybersecurity experts say the protective gaps between computer systems that manage utilities' business operations and machines that manage their grids are not always as wide or as unbridgeable as utilities say they are. And even the utilities' own experts, who maintain it would be extraordinarily difficult for a hacker to knock out power to customers, admit there is always a way in.

"If the motivation is high enough on the attacker side, and they have funding to accomplish their mission," Parcel said, "they will find a way."