https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors

By Rebecca Smith and Rob Barry
Jan. 10, 2019 11:18 a.m. ET

One morning in March 2017, Mike Vitello's work phone lighted up. Customers wanted to know about an odd email they had just received. What was the agreement he wanted signed? Where was the attachment?

Mr. Vitello had no idea what they were talking about. The Oregon construction company where he works, All-Ways Excavating USA, checked it out. The email was bogus, they told Mr. Vitello's contacts. Ignore it.

Then, a few months later, the U.S. Department of Homeland Security dispatched a team to examine the company's computers. You've been attacked, a government agent told Mr. Vitello's colleague, Dawn Cox. Maybe by Russians. They were trying to hack into the power grid.

"They were intercepting my every email," Mr. Vitello says. "What the hell? I'm nobody."

"It's not you. It's who you know," says Ms. Cox.

The cyberattack on the 15-person company near Salem, Ore., which works with utilities and government agencies, was an early thrust in the worst known hack by a foreign government into the nation's electric grid. It set off so many alarms that U.S. officials took the unusual step in early 2018 of publicly blaming the Russian government.

A reconstruction of the hack reveals a glaring vulnerability at the heart of the country's electric system. Rather than strike the utilities head on, the hackers went after the system's unprotected underbelly—hundreds of contractors and subcontractors like All-Ways who had no reason to be on high alert against foreign agents. From these tiny footholds, the hackers worked their way up the supply chain. Some experts believe two dozen or more utilities ultimately were breached.

The scheme's success came less from its technical prowess—though the attackers did use some clever tactics—than in how it exploited trusted business relationships using impersonation and trickery.

The hackers planted malware on sites of online publications frequently read by utility engineers. They sent out fake résumés with tainted attachments, pretending to be job seekers. Once they had computer-network credentials, they slipped through hidden portals used by utility technicians, in some cases getting into computer systems that monitor and control electricity flows.

The Wall Street Journal pieced together this account of how the attack unfolded through documents, computer records and interviews with people at the affected companies, current and former government officials and security-industry investigators.

The U.S. government hasn't named the utilities or other companies that were targeted. The Journal identified small businesses such as Commercial Contractors Inc., in Ridgefield, Wash., and Carlson Testing Inc., in Tigard, Ore., along with big utilities such as the federally owned Bonneville Power Administration and Berkshire Hathaway 's PacifiCorp. Two of the energy companies targeted build systems that supply emergency power to Army bases.

The Russian campaign triggered an effort by the Federal Bureau of Investigation and Homeland Security to retrace the steps of the attackers and notify possible victims. Some companies were unaware they had been compromised until government investigators came calling, and others didn't know they had been targeted until contacted by the Journal.

"What Russia has done is prepare the battlefield without pulling the trigger," says Robert P. Silvers, former assistant secretary for cyber policy at Homeland Security and now a law partner at Paul Hastings LLP.

The press office at the Russian Embassy in Washington didn't respond to multiple requests for comment. Russia has previously denied targeting critical infrastructure.

Early victims

In the summer of 2016, U.S. intelligence officials saw signs of a campaign to hack American utilities, says Jeanette Manfra, assistant secretary of Homeland Security's cybersecurity and communications program. The tools and tactics suggested the perpetrators were Russian. Intelligence agencies notified Homeland Security, Ms. Manfra says.

In December 2016, an FBI agent showed up at a low-rise office in Downers Grove, Ill., less than an hour west of Chicago. It was home to CFE Media LLC, a small, privately held company that publishes trade journals with titles such as "Control Engineering" and "Consulting-Specifying Engineer."

According to a CFE email, the agent told employees that "highly sophisticated individuals" had uploaded a malicious file onto the website for Control Engineering. The agent warned it could be used to launch hostile actions against others.

Steve Rourke, CFE Media's co-founder, says his company took steps to fix the infected site. Before long, though, attackers laced other CFE Media trade publications with malicious content, according to security researchers at Accenture 's iDefense unit and RiskIQ, a San Francisco cybersecurity company, who later analyzed details of the attack.

Like lions pursuing prey at a watering hole, the hackers stalked visitors to these and other trade websites, hoping to catch engineers and others and penetrate the companies where they worked. The Russians could potentially take down "anybody in the industry," says RiskIQ researcher Yonathan Klijnsma.

By planting a few lines of code on the websites, the attackers invisibly plucked computer usernames and passwords from unsuspecting visitors, according to government briefings on the attack and security experts who have reviewed the malicious code. That tactic enabled the Russians to gain access to ever more sensitive systems, said Homeland Security officials in industry briefings last year.

Mr. Vitello of All-Ways Excavating has no idea how the hackers got into his email account. He doesn't recall reading CFE's websites or clicking on tainted email attachments. Nonetheless, the intrusion was part of the Russian campaign, according to the security companies that studied the hack.

On March 2, 2017, the attackers used Mr. Vitello's account to send the mass email to customers, which was intended to herd recipients to a website secretly taken over by the hackers.

The email promised recipients that a document would download immediately, but nothing happened. Viewers were invited to click a link that said they could "download the file directly." That sprang the trap and took them to a website called imageliners.com.

The site, registered at the time to Matt Hudson, a web developer in Columbia, S.C., was originally intended to allow people to find contract work doing broadcast voice-overs but was dormant at the time. Mr. Hudson says he had no idea Russians had commandeered his site.

The day the email went out—the same day Mr. Vitello's office phone lighted up in Oregon—activity on the voice-over site surged, with computers from more than 300 IP addresses reaching out to it, up from only a handful a day during the prior month. Many were potential victims for the hackers. About 90 of the IP addresses—the codes that help computers find each other on the internet—were registered in Oregon, a Journal analysis found.

Web developer Matt Hudson says he had no idea Russians had hacked into his site. PHOTO: SEAN RAYFORD FOR THE WALL STREET JOURNAL

It isn't clear what the victims saw when they landed on the hacked voice-over site. Files on the server reviewed by the Journal indicate they could have been shown a forged login page for Dropbox, a cloud-based service that allows people to share documents and photos, designed to trick them into turning over usernames and passwords. It also is possible the hackers used the site to open a back door into visitors' systems, giving them control over their victims' computers.

Once Mr. Vitello realized his email had been hijacked, he tried to warn his contacts not to open any email attachments from him. The hackers blocked the message.

All-Ways Excavating is a government contractor and bids for jobs with agencies including the U.S. Army Corps of Engineers, which operates dozens of federally owned hydroelectric facilities.

Some two weeks later, the attackers again used Mr. Vitello's account to send a barrage of emails.

One went to Dan Kauffman Excavating Inc., in Lincoln City, Ore., with the subject line: "Please DocuSign Signed Agreement—Funding Project."

Office manager Corinna Sawyer thought the wording was strange and emailed Mr. Vitello: "Just received this from your email, I assume you have been hacked."

Back came a response from the intruders who controlled Mr. Vitello's account: "I did send it."

Ms. Sawyer, still suspicious, called Mr. Vitello, who told her the email, like the earlier one, was fake.

The attack spreads

One company that got one of the bogus emails was a small professional-services firm in Corvallis, Ore. That July, FBI agents showed up there, telling employees their system had been compromised in a "widespread campaign" targeting energy companies, according to the company owner.

After receiving Mr. Vitello's first bogus email on March 2, a subsequent Homeland Security investigative report says, an employee at the Corvallis firm clicked on the link leading to the hacked voice-over site. She was prompted to enter a username and password. By day's end, the cyberoperatives were in her company's network, according to the report, which hasn't been made public but was reviewed by the Journal.

They then cracked open a portal in the company's firewall, which separates sensitive internal networks from the internet, and created a new account with broad, administrative access, which they hid from view.

"We didn't know about it or catch it," says the company's owner.

In June 2017, the hackers used the Corvallis company's systems to go hunting. Over the next month, they accessed the Oregon company's network dozens of times from computers with IP addresses registered in countries including Turkey, France and the Netherlands, targeting at least six energy firms.

In some cases, the attackers simply studied the new targets' websites, possibly as reconnaissance for future strikes. In other instances, the investigative report indicates, they may have gained footholds inside their victims' systems.

Two of the targeted companies had helped the Army create independent supplies of electricity for domestic bases.

On June 15, hackers visited the website of ReEnergy Holdings LLC. The renewable-energy company had built a small power plant that allows Fort Drum in western New York to operate even if the civilian power grid collapses. Fort Drum is the home of one of the Army's most frequently deployed divisions and is under consideration to be the site of a $3.6 billion interceptor system to defend the East Coast from intercontinental ballistic missiles.

ReEnergy, owned by private-equity investor Riverstone Holdings LLC, suffered an intrusion but its generating facilities weren't affected, says one person familiar with the matter. The Army was aware of the incident, said a spokesman, who declined to provide additional details.

That same day, the hackers began hitting the website of Atlantic Power Corp. , an independent power producer that sells electricity to more than a dozen utilities in eight states and two Canadian provinces. In addition to downloading files from the site, the attackers visited the

company's virtual private network login page, or VPN, a gateway to the firm's computer systems for people working remotely, the report says.

Atlantic Power said in a written statement it regularly encounters malicious acts but doesn't comment on specifics. "To our knowledge, there has never been a successful breach of any of the company's systems," it said.

Around midnight that June 28, the hackers used the Corvallis company's network to exchange emails with a 20-person carpentry company in Michigan called DeVange Construction Inc. The emails appeared to come from an employee called Rick Harris—a persona fabricated by the attackers.

DeVange Construction's systems already may have been compromised. Applications to energy companies from nonexistent people seeking industrial-control systems jobs came from DeVange email addresses, according to security experts and emails reviewed by the Journal. Bogus résumés were attached—tweaked to trick recipients' computers into sending login information to hacked servers.

The Journal identified at least three utilities that received the emails: Washington-based Franklin PUD, Wisconsin-based Dairyland Power Cooperative and New York State Electric & Gas Corp. All three say they were aware of the hacking campaign but don't believe they fell victim to it.

A DeVange employee says federal agents visited the company. The company's owner, Jim Bell, declined to discuss the incident.

That June 30, the hackers sought remote access to an Indiana company that, like ReEnergy, installs equipment to allow government facilities to operate if the civilian grid loses power. That company, Energy Systems Group Ltd. of Newburgh, Ind., a unit of Vectren Corp. , declines to say whether it was hacked but says it has a robust focus on cybersecurity.

The company's website says one of its customers is Fort Detrick, an Army base in Maryland with a complex of laboratories that defend the nation against biological weapons. Fort Detrick referred questions to Army officials, who said they take cybersecurity seriously but declined to comment further.

As the summer of 2017 wore on, the attackers took aim at companies that help utilities manage their computer control systems. On July 1, the attackers used the Corvallis company to attack two English companies, Severn Controls Ltd. and Oakmount Control Systems Ltd. Next, they attacked Simkiss Control Systems Ltd. also in England, and accessed "account and control system information," according to the government report.

Simkiss's website says it markets tools that allow technicians to have remote access to industrial control networks. Among its customers are big electrical equipment makers and utilities including National Grid , which runs electric transmission lines in Britain and parts of the U.S., where it owns utilities in New York, Rhode Island and Massachusetts.

Oakmount, Severn and Simkiss declined to comment, and National Grid says its cybersecurity processes are "aligned with industry best practice."

After breaching the network of Dan Kauffman Excavating in Oregon, hackers blasted out emails to roughly 2,300 of the company's contacts. PHOTO: LEAH NASH FOR THE WALL STREET JOURNAL

By that fall, the hackers returned to Dan Kauffman Excavating in Oregon, breaching its network on Sept. 18, according to the firm. They appeared to lurk quietly for a month. Then, on the night of Oct. 18, emails blasted out to roughly 2,300 of the company's contacts. The message said, "Hi, Dan used Dropbox to share a folder with you!" and contained a link that said, "View folder."

Among the recipients: employees of PacifiCorp, a multistate utility; the Portland, Ore.-based Bonneville Power Administration, which runs 75% of the Pacific Northwest's high-voltage transmission lines, and the Army Corps of Engineers.

Federal officials say the attackers looked for ways to bridge the divide between the utilities' corporate networks, which are connected to the internet, and their critical-control networks, which are walled off from the web for security purposes.

The bridges sometimes come in the form of "jump boxes," computers that give technicians a way to move between the two systems. If not well defended, these junctions could allow operatives to tunnel under the moat and pop up inside the castle walls.

In briefings to utilities last summer, Jonathan Homer, industrial-control systems cybersecurity chief for Homeland Security, said the Russians had penetrated the control-system area of utilities through poorly protected jump boxes. The attackers had "legitimate access, the same

as a technician," he said in one briefing, and were positioned to take actions that could have temporarily knocked out power.

The federally owned Bonneville Power Administration says it doesn't believe the utility was breached, though it appears to have received suspicious emails. PHOTO: NATALIE BEHRING/GETTY IMAGES

PacifiCorp says it takes a multilayered approach to risk management and that it wasn't compromised by any attack campaigns.

Gary Dodd, Bonneville's chief information security officer, says he doesn't believe his utility was breached, though it appears to have received suspicious emails from both All-Ways Excavating and Dan Kauffman Excavating. "It's possible something got in, but I really don't think so," he says.

The Army Corps says it doesn't comment on cybersecurity matters.

Going public

The U.S. government warned the public about the hacking campaign in an October 2017 advisory. It attributed it to a shadowy group, sometimes called Dragonfly or Energetic Bear, that security researchers have tied to the Russian government.

In March 2018, the U.S. went further, releasing a report that pinned responsibility for the hostile activities on "cyber actors" working for the Russian government, saying they had been active since at least March 2016. Governments generally have shied away from naming countries involved in cyberattacks, not wanting divulge what they know.

> In April 2018, the FBI notified at least two companies by letter that they appeared to have received malicious emails from All-Ways Excavating's Mr. Vitello.

One was Commercial Contractors of Ridgefield, Wash., which helped renovate an office for the Bonneville Power Administration. Eric Money, the company's president, says employees

thought they had resisted the tainted emails. But the Journal found that a computer with an IP address linked to the company visited Mr. Hudson's hacked voice-over site the day of the attack.

The other company notified by the FBI, Carlson Testing of Tigard, Ore., has done work for utilities including Portland General Electric, PacifiCorp, Northwest Natural Gas and the Bonneville Power Administration.

Vikram Thakur, technical director of security response for Symantec Corp. , a California-based cybersecurity firm, says his company knows from its utility clients and from other security firms it works with that at least 60 utilities were targeted, including some outside the U.S. About two dozen were breached, he says, adding that hackers penetrated far enough to reach the industrial-control systems at eight or more utilities. He declined to name them.

The government isn't sure how many utilities and vendors in all were compromised in the Russian assault.

Vello Koiv, president of VAK Construction Engineering Services in Beaverton, Ore., which does subcontracting for the Army Corps, PacifiCorp, Bonneville and Avista Corp. , a utility in Spokane, Wash., says someone at his company took the bait from one of the tainted emails, but his computer technicians caught the problem, so "it was never a full-blown event." Avista says it doesn't comment on cyberattacks.

Mr. Koiv says he continued to get tainted emails in 2018. "Whether they're Russian or not, I don't know. But someone is still trying to infiltrate our server."

Last fall, All-Ways Excavating was again hacked.

Industry experts say Russian government hackers likely remain inside some systems, undetected and awaiting further orders.

—Lisa Schwartz contributed to this article.

—Graphics by Joel Eastwood and Angela Calderon

Write to Rebecca Smith at rebecca.smith@wsj.com and Rob Barry at rob.barry@wsj.com

Appeared in the January 11, 2019, print edition as 'Russian Hack Exposes Weakness in U.S. Power Grid.'