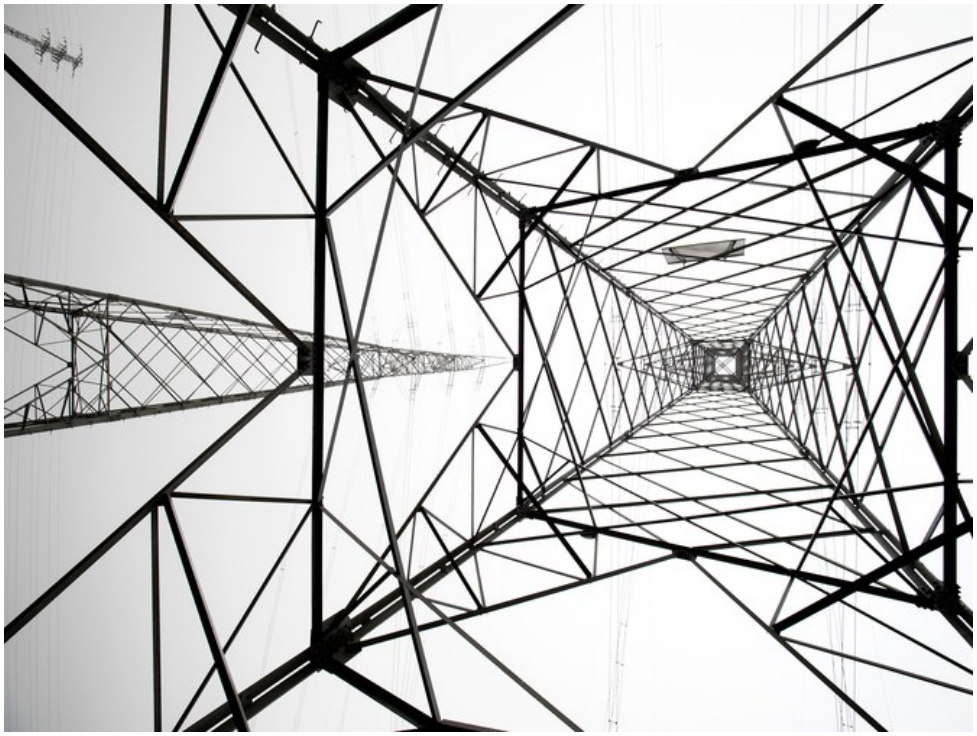
KIM ZETTER SECURITY 03.03.16 07:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattyaoblenergo control center, which distributes power to the region's residents, operators too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord.

He watched as it navigated purposefully toward buttons controlling the circuit breakers at a substation in the region and then clicked on a box to open the breakers and take the substation offline. A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the

thousands of residents had just lost their lights and heaters.

The operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive. Then as the cursor moved in the direction of another breaker, the machine suddenly logged him out of the control panel. Although he tried frantically to log back in, the attackers had changed his password preventing him from gaining re-entry. All he could do was stare helplessly at his screen while the ghosts in the machine clicked open one breaker after another, eventually taking about 30 substations offline. The attackers didn't stop there, however. They also struck two other power distribution centers at the same time, nearly doubling the number of substations taken offline and leaving more than 230,000 residents in the dark. And as if that weren't enough, they also disabled backup power supplies to two of the three distribution centers, leaving operators themselves stumbling in the dark.

A Brilliant Plan

The hackers who struck the power centers in Ukraine—the first confirmed hack to take down a power grid—weren't opportunists who just happened upon the networks and launched an attack to test their abilities; according to new details from an extensive investigation into the hack, they were skilled and stealthy strategists who carefully planned their assault over many months, first doing reconnaissance to study the networks and siphon operator credentials, then launching a synchronized assault in a well-choreographed dance.

"It was brilliant," says Robert M. Lee, who assisted in the investigation. Lee is a former cyber warfare operations officer for the US Air Force and is co-founder of Dragos Security, a critical infrastructure security company. "In terms of sophistication, most people always [focus on the] malware [that's used in an attack]," he says. "To me what makes sophistication is logistics and planning and operations and … what's going on during the length of it. And this was highly sophisticated."

Ukraine was quick to point the finger at Russia for the assault. Lee shies away from attributing it to any actor but says there are clear delineations between the various phases of the operation that suggest different levels of actors worked on different parts of the assault. This raises the possibility that the attack might have involved

nation-state actors.

"This had to be a well-funded, well-trained team. … [B]ut it didn't have to be a nation-state," he says. It could have started out with cybercriminals getting initial access to the network, then handing it off to nation-state attackers who did the rest.

Regardless, the successful assault holds many lessons for power generation plants and distribution centers here in the US, experts say; the control systems in Ukraine were surprisingly more secure than some in the US, since they were well-segmented from the control center business networks with robust firewalls. But in the end they still weren't secure enough—workers logging remotely into the SCADA network, the Supervisory Control and Data Acquisition network that controlled the grid, weren't required to use two-factor authentication, which allowed the attackers to hijack their credentials and gain crucial access to systems that controlled the breakers.

The power wasn't out long in Ukraine: just one to six hours for all the areas hit. But more than two months after the attack, the control centers are still not fully operational, according to a recent US report. Ukrainian and US computer security experts involved in the investigation say the attackers overwrote firmware on critical devices at 16 of the substations, leaving them unresponsive to any remote commands from operators. The power is on, but workers still have to control the breakers manually.

That's actually a better outcome than what might occur in the US, experts say, since many power grid control systems here don't have manual backup functionality, which means that if attackers were to sabotage automated systems here, it could be much harder for workers to restore power.

Timeline of the Attack

Multiple agencies in the US helped the Ukrainians in their investigation of the attack, including the FBI and DHS. Among computer security experts who consulted on the wider investigation were Lee and Michael J. Assante, both of whom teach computer security at the SANS Institute in Washington DC and plan to release a report about their analysis today. They say investigators were pleasantly surprised to discover that the Ukrainian power distribution companies had a vast collection of firewall and system logs that helped them reconstruct events—an uncommon bonanza for any

which seldom have robust logging capabilities.

According to Lee and a Ukrainian security expert who assisted in the investigation, the attacks began last spring with a spear-phishing campaign that targeted IT staff and system administrators working for multiple companies responsible for distributing electricity throughout Ukraine. Ukraine has 24 regions, each divided into between 11 and 27 provinces, with a different power distribution company serving each region. The phishing campaign delivered email to workers at three of the companies with a malicious Word document attached. When workers clicked on the attachment, a popup displayed asking them to enable macros for the document. If they complied, a program called BlackEnergy3—variants of which have infected other systems in Europe and the US—infected their machines and opened a backdoor to the hackers. The method is notable because most intrusions these days exploit a coding mistake or vulnerability in a software program; but in this case the attackers exploited an intentional feature in the Microsoft Word program. Exploiting the macros feature is an old-school method from the 90's that attackers have recently revived in multiple attacks.

The initial intrusion got the attackers only as far as the corporate networks. But they still had to get to the SCADA networks that controlled the grid. The companies had wisely segregated those networks with a firewall, so the attackers were left with two options: either find vulnerabilities that would let them punch through the firewalls or find another way to get in. They chose the latter.

Over many months they conducted extensive reconnaissance, exploring and mapping the networks and getting access to the Windows Domain Controllers, where user accounts for networks are managed. Here they harvested worker credentials, some of them for VPNs the grid workers used to remotely log in to the SCADA network. Once they got into the SCADA networks, they slowly set the stage for their attack.

First they reconfigured the uninterruptible power supply[1], or UPS, responsible for providing backup power to two of the control centers. It wasn't enough to plunge customers into the dark—when power went out for the wider region they wanted operators to be blind, too. It was an egregious and aggressive move, the sort that could be interpreted as a "giant fuck you" to the power companies, says Lee.

Each company used a different distribution management system for its grid, and during the reconnaissance phase, the attackers studied each of them carefully. Then

Ethernet converters at more than a dozen substations (the converters are used to process commands sent from the SCADA network to the substation control systems). Taking out the converters would prevent operators from sending remote commands to re-close breakers once a blackout occurred. "Operation-specific malicious firmware updates [in an industrial control setting] has *never* been done before," Lee says. "From an attack perspective, it was just so awesome. I mean really well done by them."

The same model of serial-to-Ethernet converters used in Ukraine are used in the US power-distribution grid.

Armed with the malicious firmware, the attackers were ready for their assault.

Sometime around 3:30 p.m. on December 23 they entered the SCADA networks through the hijacked VPNs and sent commands to disable the UPS systems they had already reconfigured. Then they began to open breakers. But before they did, they launched a telephone denial-of-service attack against customer call centers to prevent customers from calling in to report the outage. TDoS attacks are similar to DDoS attacks that send a flood of data to web servers. In this case, the center's phone systems were flooded with thousands of bogus calls that appeared to come from Moscow, in order to prevent legitimate callers from getting through. Lee notes that the move illustrates a high level of sophistication and planning on the part of the attackers. Cybercriminals and even some nation-state actors often fail to anticipate all contingencies. "What sophisticated actors do is they put concerted effort into even unlikely scenarios to make sure they're covering all aspects of what could go wrong," he says.

The move certainly bought the attackers more time to complete their mission because by the time the operator whose machine was hijacked noticed what was happening, a number of substations had already been taken down. But if this *was* a political hack launched by Russia against Ukraine, the TDoS likely also had another goal Lee and Assante say: to stoke the ire of Ukrainian customers and weaken their trust in the Ukrainian power companies and government.

As the attackers opened up breakers and took a string of substations off the grid, they also overwrote the firmware on some of the substation serial-to-Ethernet converters, replacing legitimate firmware with their malicious firmware and rendering the converters thereafter inoperable and unrecoverable, unable to receive

recovery]. You have to be at that site and manually switch operations," Lee says. "Blowing [these] gateways with firmware modifications means they can't recover until they get new devices and integrate them."

After they had completed all of this, they then used a piece of malware called KillDisk to wipe files from operator stations to render them inoperable as well. KillDisk wipes or overwrites data in essential system files, causing computers to crash. Because it also overwrites the master boot record, the infected computers could not reboot.

Some of the KillDisk components had to be set off manually, but Lee says that in two cases the attackers used a logic bomb that launched KillDisk automatically about 90 minutes into the attack. This would have been around 5 p.m., the same time that Prykarpattyaoblenergo posted a note to its web site acknowledging for the first time what customers already knew—that power was out in certain regions—and reassuring them that it was working feverishly to figure out the source of the problem. Half an hour later, after KillDisk would have completed its dirty deed and left power operators with little doubt about what caused the widespread blackout, the company then posted a second note to customers saying the cause of the outage was hackers.

Was Russia the Cause?

Ukraine's intelligence community has said with utter certainty that Russia is behind the attack, though it has offered no proof to support the claim. But given political tensions between the two nations it's not a far-fetched scenario. Relations have been strained between Russia and Ukraine ever since Russia annexed Crimea in 2014 and Crimean authorities began nationalizing Ukrainian-owned energy companies there, angering Ukrainian owners. Then, right before the December blackout in Ukraine occurred, pro-Ukrainian activists physically attacked substations feeding power to Crimea, leaving two million Crimean residents without power in the region that Russia had annexed, as well as a Russian naval base. Speculation has been rampant that the subsequent blackouts in Ukraine were retaliation for the attack on the Crimean substations.

But the attackers who targeted the Ukrainian power companies had begun their operation at least six months before the Crimean substations were attacked. So, although the attack in Crimea may have been a catalyst for the subsequent attack on

says. Lee says the forensic evidence suggests in fact that the attackers may not have planned to take out the power in Ukraine when they did, but rushed their plans after the attack in Crimea.

"Looking at the data, it looks like they would have benefited and been able to do more had they been planning and gathering intelligence longer," he says. "So it looks like they may have rushed the campaign."

He speculates that if Russia is responsible for the attack, the impetus may have been something completely different. Recently, for example, the Ukrainian parliament has been considering a bill to nationalize privately owned power companies in Ukraine. Some of those companies are owned by a powerful Russian oligarch who has close ties to Putin. Lee says it's possible the attack on the Ukrainian power companies was a message to Ukrainian authorities not to pursue nationalization.

That analysis is supported by another facet of the attack: The fact that the hackers could have done much more damage than they did do if only they had decided to physically destroy substation equipment as well, making it much harder to restore power after the blackout. The US government demonstrated an attack in 2007 that showed how hackers could physically destroy a power generator simply by remotely sending 21 lines of malicious code.

Lee says everything about the Ukraine power grid attack suggests it was primarily designed to send a message. "'We want to be seen, and we want to send you a message,'" is how he interprets it. "This is very mafioso in terms of like, oh, you think you can take away the power [in Crimea]? Well I can take away the power from you."

Whatever the intent of the blackout, it was a first-of-its-kind attack that set an ominous precedent for the safety and security of power grids everywhere. The operator at Prykarpattyaoblenergo could not have known what that little flicker of his mouse cursor portended that day. But now the people in charge of the world's power supplies have been warned. This attack was relatively short-lived and benign. The next one might not be.

[1]*Correction 3/03/16 8:17 a.m. ET: UPS here stands for uninterruptible power supply, not universal power supply.*

VIEW COMMENTS

SPONSORED STORIES

POWERED BY OUTBRAIN

ANDY GREENBERG
'Crash Override': The Malware That Took Down a Power Grid

BRIAN BARRETT
Security News This Week: A Devious Twitter Attack Wreaks Real Havoc

ANDY GREENBERG
Everything We Know About Russia's Election-Hacking Playbook

ASHLEY FEINBERG
James Comey Said Exactly What You Wanted Him to Say

GARRETT M. GRAFF
James Comey Goes Back to Washington

ELIZABETH STINSON
Ai Weiwei Gets Artsy-Fartsy About Surveillance

MORE SECURITY

DATABASES

The Scarily Common Screw-Up That Exposed 198 Million Voter Records

LILY HAY NEWMAN

SECURITY

Security News This Week: Microsoft's Patching *Old* Versions of Windows Because Things Are That Bad

LILY HAY NEWMAN

FACEBOOK

Facebook's Counterterrorism Playbook Comes Into Focus

EMILY DREYFUSS

NATIONAL AFFAIRS

The Texting Suicide Case Is About Crime, Not Tech

ISSIE LAPOWSKY

WIKILEAKS

WikiLeaks Reveals How the CIA Could Hack Your Router

ANDY GREENBERG

NORTH KOREA

North Korea's Sloppy, Chaotic Cyberattacks Also Make Perfect Sense

ANDY GREENBERG

GET OUR

WIRED's biggest stories, delivered to your inbox.

Enter your email

SUBMIT

WE'RE ON PINTEREST

See what's inspiring us.

FOLLOW

CUSTOMER CARE	CONTACT US
SECUREDROP	T-SHIRT COLLECTION
NEWSLETTER	WIRED STAFF
JOBS	RSS

CNMN Collection

Use of this site constitutes acceptance of our user agreement (effective 3/21/12) and privacy policy (effective 3/21/12). Affiliate link policy. Your California privacy rights. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.