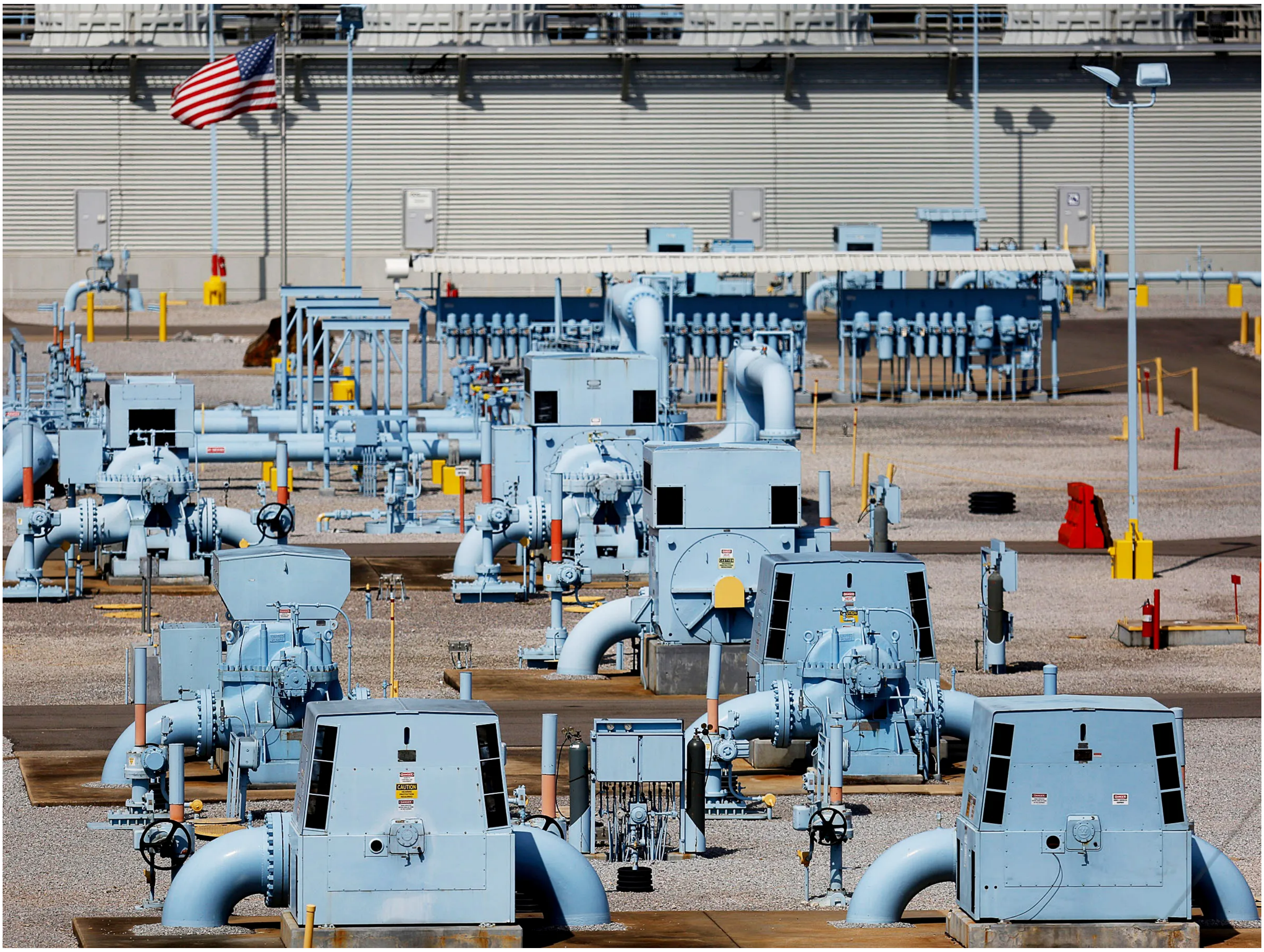
ANDY GREENBERG SECURITY 05.08.2021 05:33 PM

The Colonial Pipeline Hack Is a New Extreme for Ransomware

An attack has crippled the company's operations—and cut off a large portion of the East Coast's fuel supply—in an ominous development for critical infrastructure.



Colonial Pipeline supplies nearly half of the East Coast's fuel—until a ransomware attack took it offline. PHOTOGRAPH: LUKE SHARRETT/BLOOMBERG/GETTY IMAGES

FOR YEARS, THE cybersecurity industry has warned that state-sponsored hackers could shut down large swathes of US energy infrastructure in a geopolitically motivated act of cyberwar. But now apparently profit-focused cybercriminal hackers have inflicted a disruption that military and intelligence agency hackers have never dared to, shutting down a pipeline that carries nearly half the fuel consumed on the East Coast of the United States.

On Saturday, the Colonial Pipeline company, which operates a pipeline that carries gasoline, diesel fuel, and natural gas along a 5,500 mile path from Texas to New Jersey, released a statement confirming reports that ransomware hackers had hit its network. In response, Colonial Pipeline says it shut down parts of the pipeline's operation in an attempt to contain the threat. The incident represents one of the largest disruptions of American critical infrastructure by hackers in history. It also provides yet another demonstration of how severe the global epidemic of ransomware has become.

"This is the largest impact on the energy system in the United States we've seen from a cyberattack, full stop," says Rob Lee, CEO of the critical-infrastructure-focused security firm Dragos. Aside from the financial impact on Colonial Pipeline or the many providers and customers of the fuel it transports, Lee points out that around 40 percent of US electricity in 2020 was produced by burning natural gas, more than any other source. That means, he argues, that the threat of cyberattacks on a pipeline presents a significant threat to the civilian power grid. "You have a real ability to impact the electric system in a broad way by cutting the supply of natural gas. This is a big deal," he adds. "I think Congress is going to have questions. A provider got hit with ransomware from a criminal act, this wasn't even a state-sponsored attack, and it impacted the system in this way?"

> **“In the last seven or eight months we’ve been seeing a spike in cases.”**
>
> — ROB LEE, DRAGOS

Colonial Pipeline's short public statement says that it has "launched an investigation into the nature and scope of this incident, which is ongoing." Reuters reports that incident responders from security firm FireEye are assisting the company, and that investigators suspect that a ransomware group known as Darkside may be responsible. According to a report by the security firm Cybereason, Darkside has compromised more than 40 victim organizations and demanded between $200,000 and $2 million in ransom from them.

The Colonial Pipeline shutdown comes in the midst of an escalating ransomware epidemic: Hackers have digitally crippled and extorted hospitals, hacked law enforcement databases and threatened to publicly out police informants, and paralyzed municipal systems in Baltimore and Atlanta.

The majority of ransomware victims never publicize their attacks. But Lee says his firm has seen a significant uptick in ransomware operations targeting industrial control systems and critical infrastructure, as profit-focused hackers seek the most sensitive and high-value targets to hold at risk. "The criminals are starting to think about targeting industrial, and in the last seven or eight months we've been seeing a spike in cases," says Lee. "I think we will see a lot more."

In fact, ransomware operators have increasingly had industrial victims in their sights in recent years. Hydro Norsk, Hexion, and Momentive were all hit with ransomware in 2019, and security researchers last year discovered Ekans, the first ransomware apparently custom-designed to cripple industrial control systems. Even targeting a gas pipeline operator isn't entirely unprecedented: In late 2019, hackers planted ransomware on the networks of an unnamed US natural gas pipeline company, the Cybersecurity and Infrastructure Security Agency warned in early 2020—though not one of the size of Colonial Pipeline's.

In that earlier pipeline ransomware attack, CISA warned that the hackers had gained access to both the IT systems and the "operational technology" systems of the targeted pipeline firm—the computer network responsible for controlling physical equipment. In the Colonial Pipeline case, it's not yet clear if the hackers bridged that gap to systems that could have actually allowed them to meddle with the physical state of the pipeline or create potentially dangerous physical conditions. Merely gaining broad access to the IT network could be cause enough for the company to shut down the pipeline's operation as a safety precaution, says Joe Slowik, a threat intelligence researcher for security firm Gigamon who formerly led the Computer Security and Incident Response Team at the US Department of Energy. "The operator did the right thing in this case as a response to events," Slowik says. "Once you can no longer assure positive control over the environment and clear visibility into operations, then you need to shut it down."

Ransomware intrusions that can reach those operational technology systems are far more rare than those that merely target IT networks. But Lee says Dragos has seen a growing number of ransomware groups working to infect the OT systems that control industrial and manufacturing equipment, with the aim of totally disrupting their victims' operations. Organizations increasingly connect those more sensitive networks to the internet for efficiency and remote automation, and a spate of vulnerabilities in the VPNs companies use to remotely connect to those networks has left them more exposed.

"These gangs figure out, here's a bunch of internet-facing devices, here are vulnerabilities that give us access to them, and here are the IP ranges of a bunch of big industrial companies," says Lee. "Cool, let's go big game hunting."

The response to the rising ransomware threat, meanwhile, has not stemmed the tide. A public-private partnership released recommendations last month, but any proposed solution would require buy-in from multiple government agencies and must contend with the fact that many of the most aggressive hacking groups appear to be located in countries like Russia, whose governments rarely prosecute—and often collaborate with—the hackers in their midst.

That leaves critical infrastructure providers in the US with little choice but to bolster their defenses against an onslaught of loosely organized criminal hackers—whose disruptive ambitions are only growing.

More Great WIRED Stories

- 📩 The latest on tech, science, and more: Get our newsletters!
- The cold war over McDonald's hacked ice cream machines
- It began as an AI-fueled dungeon game. It got much darker
- Don't underestimate the challenge of building a PC
- Plastic is falling from the sky. But where's it coming from?
- NFTs and AI are unsettling the very concept of history
- 👁️ Explore AI like never before with our new database

- 🎮 WIRED Games: Get the latest tips, reviews, and more
- 💻 Upgrade your work game with our Gear team's favorite laptops, keyboards, typing alternatives, and noise-canceling headphones

Andy Greenberg is a senior writer for WIRED, covering security, privacy, and information freedom. He's the author of the book *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. The book and excerpts from it published in WIRED won a Gerald Loeb Award for... Read more

SENIOR WRITER

Featured Video

WATCH

What is Ransomware and How Do You Deal With It?

What is Ransomware and How Do You Deal With It?

Ransomware. It's malware but worse. It takes the contents of your device hostage and demands Bitcoin as a, you guessed it, ransom. Here's how to avoid it and what to do if your laptop gets locked.

TOPICS RANSOMWARE HACKING CRIME CRITICAL INFRASTRUCTURE