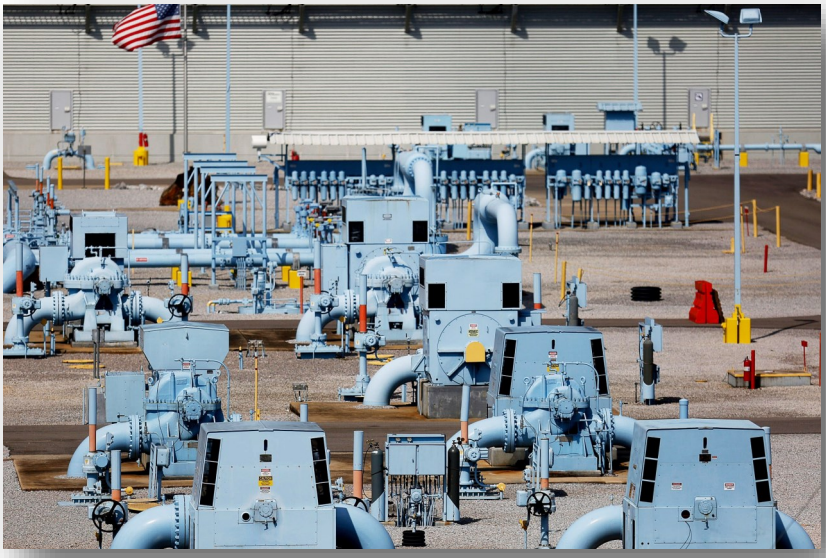
TechTips Newsletter

Insider Tips To Make Your Business Run Faster, Easier And More Profitably



The Colonial Pipeline Hack Is a New Extreme for Ransomware

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.

Continued on next page...

May 2021

This monthly publication provided courtesy of Richard Lynn, VP of Sales and Marketing Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

"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."

Continued on next page...

tech hero

Cloud Portal

Did you know about our new Cloud Portal? This new tool will allow you to open tickets directly with us here at Tech Hero at the click of a button!

To try it out, just go down to your system tray and look for the small blue IT icon. After you’ve double clicked on it you will need to sign in (You will only need to do this once!)

Once you are in you can click around explore the software.

If you have any questions, feel free to reach out to us at the number below!

(800) 900-TECH x2

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.—*Andy Greenberg for WIRED*

COSTCO WARNS ITS MEMBERS OF VARIOUS PHISHING SCAMS

Costco has updated its website to warn members of various scams that are specifically targeting past and present customers. Under a section called "Currently Known Scams," Costco has listed numerous threats, which include the following:

Fraudulent Satisfaction Survey
Fraudulent Facebook Post
Fraudulent Survey
Texts Regarding Loyalty Reward
Overcharge Reimbursement Texts
Survey with Exclusive Offers
Free Television
Coronavirus Stimulus
Exclusive Giveaway
Fake Interview Confirmation
Fraudulent Executive Rewards Redemption
Citi Rewards Direct Deposit Scam
Redeem your gift card!
Supermarket Customer Sweepstakes Raffle Draw

Continued on next page...

The common thread with these scams is that they are correspondences that convincingly appear to be from Costco. In almost all cases, there are links where the social engineers behind the scam try to collect sensitive data from you. This can include names, addresses, banking data, and much more. Some of these scams are merely photos with links, whereas others claim to be from executives at Costco Wholesale. In their notice, Costco states the following about the scams:

"Please see... examples of prominent fraudulent emails, texts, and posts that are currently circulating. These offers are not from Costco Wholesale. You should not visit any links provided in messages such as these, and you should not provide the sender any personal information."

Unfortunately, this notice is located in the Customer Service section of Costco's website. What this means is that unless a customer specifically visits this section, they may never get the warning. Many scammers hoodwink the less-aware by banking on their ignorance. It would be prudent of the Costco organization to send out frequent warnings when new scams appear.

Social engineering is so effective because it is becoming easier for cybercriminals to make convincing correspondences that catch even the most tech-savvy off-guard. A general rule is that, as with anything in life, if it sounds too good to be true, it probably is. Be very suspicious whenever you receive an email claiming you've won something (or some variant of this claim). Finally, never give away your personal data to any link asking for it. Especially if it is a company you shop with that should already have that data.

—*Derek Kortepeter for Techgenix*

Client Spotlight

ALLSTATE
PAVING & SITE DEVELOPMENT

We've been instrumental in helping Orlando grow for 17 years. We also perform work in Lake, Brevard, Seminole, Polk and Volusia counties. We specialize in customer satisfaction for all phases of site development and paving.

Allstate Paving specializes in Asphalt Paving, a preferred choice today for asphalt paving in place of concrete. Asphalt is a 100% recyclable product and extremely durable while offering enough flexibility to accommodate deficiencies in underlying surfaces.

TELEGRAM TARGETED BY NEW REMOTE ACCESS TROJAN TOXICEYE

Researchers at Checkpoint have been following malware trends on the messaging application Telegram. Due to a host of issues with competitor applications, Telegram has seen a surge in users. As Checkpoint notes in a new research post, this also applies to various threat actors. The post speaks of a new remote access Trojan (remote access Trojan) called ToxicEye deployed in Telegram. The remote access Trojan is through phishing emails that contain ToxicEye as an executable file. The executable is in an attachment that, once opened, begins quickly infecting the target device. Checkpoint states that ToxicEye can engage in "stealing data, deleting or transferring files, killing processes on the PC, hijacking the PC's microphone and camera to record audio and video (and) encrypting files for ransom purposes."

What makes Telegram a target for remote access trojans like ToxicEye, according to Checkpoint researchers, is that Telegram is an easy target. It has more than 500 million users, is not blocked by antivirus programs by default, only requires a phone number (allowing criminals to use spoofed accounts and remain anonymous), and is easily accessible globally.

Continued on next page...

Checkpoint states that the increase in remote access Trojan attacks on Telegram began in 2017. In their conclusion, they predict that this will only get worse for the following reasons:

"The developers who publish these tools disguise their true purpose by defining them as "Remote Administration Tool" or "for educational purpose only," although some of their characteristics are often found in malicious Trojans.

Given that Telegram can be used to distribute malicious files or as a C&C channel for remotely controlled malware, we fully expect that additional tools that exploit this platform will continue to be developed in the future."

The only tried and true defense against getting infected by remote access Trojans like ToxicEye is common sense. You can have the most advanced malware protection software, and as important as that may be, if you choose to open emails and download .EXE attachments… expect the worst.—*Derek Kortepeter for Techgenix*