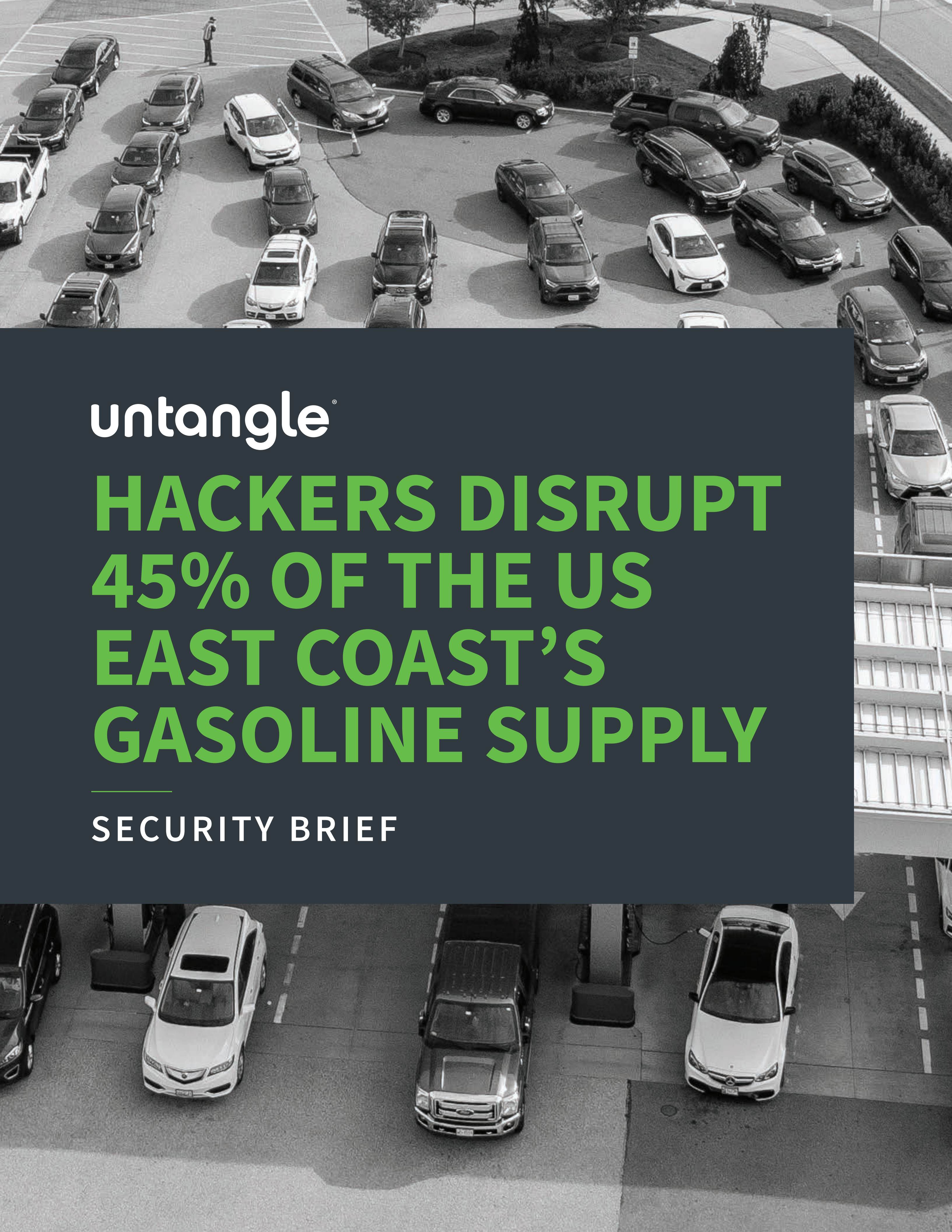


untangle

HACKERS DISRUPT 45% OF THE US EAST COAST’S GASOLINE SUPPLY

SECURITY BRIEF

On Friday, May 7, the news broke that Colonial Pipeline had been hacked and shut down its operations until the problem was resolved.

As the impact of the Colonial Pipeline attack continues to unravel, it's a sobering site to see the human impact that takes us back to a similar response last year of supermarket lines with shoppers buying up paper products. News sites have recently been filled with images of cars and trucks waiting in line to fill up with gas before either the prices go up significantly, or there is no more gas available. Gas stations in Virginia, North Carolina, and Georgia have already been completely running out of fuel amidst the dwindling supply.

The Colonial Pipeline attack is one of the most impactful IoT attacks, which stopped the function of a 5,500 mile long gasoline delivery mechanism spanning from New Jersey to Texas. The pipeline can carry 3 million barrels of fuel along its length every day, and is relied on by 45% of the USA's East Coast's fuel needs. Fuel includes not only gasoline for cars, but also includes home heating, fuel for jet airplanes and military needs.

While the attack caused massive disruption to the East Coast's gasoline supply, it was also unique in the fact that there were conflicting reports as to whether Colonial paid the ransom. DarkSide, the group that has claimed responsibility for the attack, demanded over $5 million in payment to release Colonial's data. First reports indicated that Colonial had no intention of paying for ransom and had sought help from Government officials to assess the extent of the damage. In addition they isolated the attack and took the servers that could have further proliferated the damage off line.

However, subsequent reporting of the attack indicates that Colonial did indeed pay the $5M in ransom. Widely discouraged by security professionals, paying ransom acts as encouragement to hackers, by showing how successful and lucrative the criminal activity can be, and not a deterrent.

HOW DID THE ATTACK HAPPEN?

The impact from the attack is being felt by individuals and businesses. From what is known so far, the attack stemmed from a ransomware attack that held hostage data from systems that Colonial Pipeline relied on for the running of its business.

Ransomware is a type of malware that once it has access to a device, or system can lock up all the data so that it can no longer be accessed. This is done by encrypting everything with the hacker holding the key to decrypt it. Ransomware can get onto a system from a malicious piece of code running on a web page, or can be transmitted through an email where the recipient doesn't realise that an action they take can allow the ransomware to infiltrate their device or network.

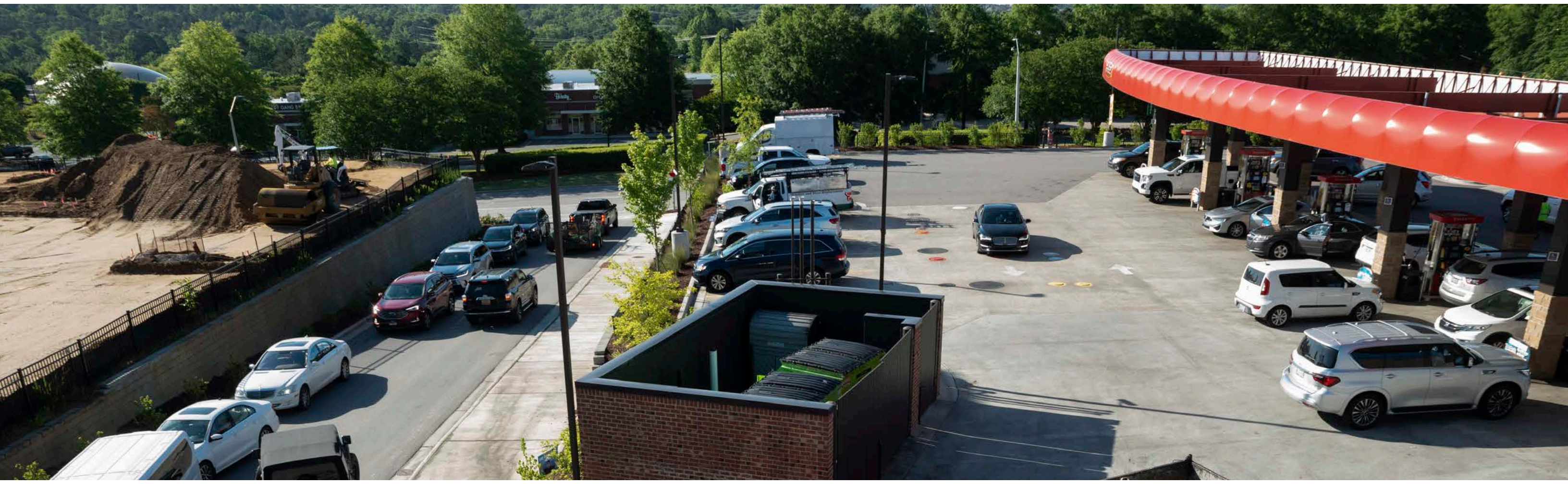
WHAT CAN BE DONE TO MITIGATE THIS TYPE OF ATTACK?

One way to stop these types of attacks is to keep infrastructure for critical systems completely offline, or isolated on a completely separate system to those that can be accessed from the outside. If it can't be accessed from the outside, it cannot be hacked. However, that's becoming less feasible with more advantages to building automated systems with components that have their own IP address that once inside a network can be discovered. Furthermore, there are generally such great advantages in efficiency and automated control and running when part of a larger system of checks.

Colonial Pipeline responded well by quickly taking certain systems offline to contain the threat and contacting law enforcement and other federal agencies. In addition, they immediately engaged a third-party cybersecurity firm to investigate the nature and scope of the attack so that they could stop it from widening further across their systems. Unfortunately it takes time to assess the impact, and to ensure that it is safe to put systems back online in order to get business operations back to normal.

WHY DID THE ATTACKERS FEEL THEY WOULD BE SUCCESSFUL?

Attackers, such as the cyber criminal group DarkSide, that have admitted responsibility for this attack, have become more emboldened because there have been some incredible amounts of ransom paid for ransomware attacks recently. 2020 was a particularly bad year with businesses, universities, healthcare facilities, and cities being targeted. Attacks on the city of Florence, FL and Yazoo County School District, MS, cost each $300,000, while the University of San Francisco (UCSF) paid $1.14M in ransom. Once a capable hacker sees the potential to gain millions of dollars, many are willing to take the risk to try and infiltrate multiple businesses in the hopes that one or more will pay up.

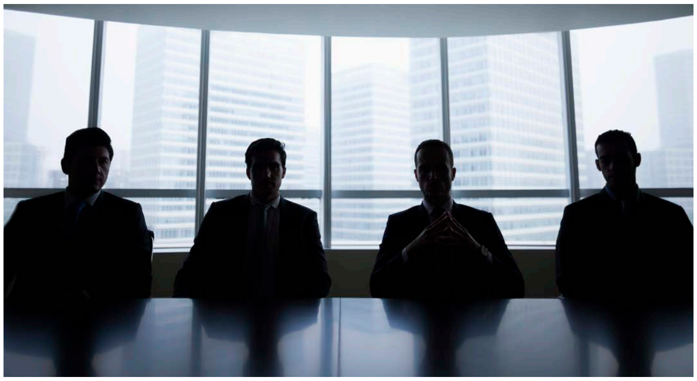


WHO WAS RESPONSIBLE FOR THE ATTACK?

There are many reasons why hackers choose to spend their time trying to take down systems. Common reasons have included monetary gains or a sense of power by being able to control something impactful. For some, the reason is because it is fun due to the challenge of breaking into something that they are not allowed access to, or that is meant to be well protected.

In the case of the Colonial Pipeline attack, however, there was a new motivation, besides monetary, which was fueled by a group who felt morally justified in what they were doing. DarkSide, who has now shut down operations after they found that their own servers were seized, had publicly declared that they give a percentage of their gains to charities, even including a list of charities on their website. However, many, if not all, recipients declined the gift.

The group shared their moral justification, which in their eyes was the fact that they only targeted large, for-profit companies who could afford to pay and they would never target organizations such as schools, hospitals, and non-profit organizations. After the Colonial Pipeline hack, they even issued a statement trying to distance themselves from the attack stating, in essence, that they didn't condone partners using their software in attacks that disrupt society in the way that this attack has.



The fact that the DarkSide group openly declared their principals gave them plenty of press coverage. Each business that paid the ransom encouraged them to plot more attacks. Their coverage in the news gave them notoriety, potentially highlighting them as an attacker that, if you are the victim, your best option is to pay up. However, the notariety may have proved too much in the Colonial Pipeline attack as it was so high profile that they are now retreating and have said that they will release decrypted data for all their outstanding victims who have not yet paid the ransoms demanded.

WHAT MITIGATION TECHNIQUES ARE THERE TO PREVENT THIS FROM HAPPENING TO OTHER ORGANIZATIONS?

- **Backup all systems**, and consider where the backups are stored. Ensure the backups themselves are not accessible by hackers. When an attack happens, being able to go back by six hours, or one day to the time before the attack happened will help restore systems to working order quickly.

- **Segregate Network access** and ensure that employees are only given access to the systems that they need. Putting different systems on different networks, that are only accessible by the groups of employees that need them, is important to ensure that if a breach does happen, fewer systems can be compromised.

- **Update software and install patches** immediately to protect your network. Attacks often take advantage of vulnerabilities that may have been reported and have fixes, yet companies procrastinate on updating.

- **Provide Continuous Employee Training.** Employee behavior is a top cause for breaches, so training is a critical step to protecting your network. Teach employees about how to recognize suspicious emails, not to open attachments from unknown senders, and to report anything out of the ordinary to the IT team.

HOW UNTANGLE CAN HELP

Untangle enables organizations to address network concerns and remain vigilant against unauthorized network access. The Untangle Network Security Framework provides IT teams with the ability to ensure protection, monitoring and control for all devices, applications, and events, enforcing a consistent security posture across the entire digital attack surface.

Untangle's cloud based centralized management tool, Command Center, does not rely on customer update schedules. Every update can be pushed within minutes to improve the security posture of the whole network management system.

UNTANGLE NETWORK SECURITY FRAMEWORK

ADVANCED SECURITY

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

INTELLIGENT SD-WAN

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Untangle AI-based Precitive Routing technology for first packet, dynamic path selection
- Manage one or many appliances from Command Center

CLOUD MANAGEMENT AT SCALE

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints

untangle

Untangle, Inc.
25 Metro Drive, Ste. 210
San Jose, CA 95110
www.untangle.com

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.