FORTRESS
Information Security

Threat Intelligence Report

Major U.S. Pipeline Systems Shutdown After Alleged Ransomware Attack

May 10, 2021

Date: May 10, 2021
https://www.fortressinfosec.com

Fortress Information Security, LLC
Phone: 855.FORTRESS
189 S. Orange Ave., Orlando, FL 32801

Table of Contents

**The usage and distribution of this document is strictly governed by the terms of our agreement with our client, and this document may not be relied upon anyone other than our client. Only individuals with a specific contractual right to view this document may do so, and if you believe you may have received this document in error, please do not read further and contact us via email at Compliance@FortressInfoSec.com as soon as possible.

To the extent this document is provided to or obtained by a governmental entity, please note that confidential treatment of this document is requested under both the Freedom of Information Act, as well as any similar applicable state or local laws governing the public disclosure of documentation, and written notice of any request for this document is requested to be sent to us via email at Compliance@FortressInfoSec.com as soon as possible.

The analysis set forth herein is made as of the date listed in this document, and we are under no obligation to correct or modify this document on an ongoing basis, unless we have specifically contracted with our client to do so in a mutually executed agreement. The usage of critical, high, medium, moderate, nominal, low, or other scaled indicators or parlance associated with the rating of risk is based on our subjective determinations, and our subjective determination may deviate from regulatory determination, and determinations by others. Our determinations are based on facts and data we receive, and to the extent any facts or data are incorrect, our determinations may then be correspondingly incorrect. Any included recommendations provided are non-inclusive and are only intended to serve as exemplar actions to address security risks, rather than as the sum-total of all actions recommended to address security risks.

Information security threats change on a daily basis, and no amount of security testing or verification can ensure that any systems or hardware are fully secure from unauthorized access. We make no guarantees or representations of accuracy beyond those contained in any mutually executed agreement with our client that address the contents of this document. This document only provides our findings under the terms of our agreement with our client and does not constitute a representation or warranty that any systems or hardware are advisable to use or free of defects or malicious code.

Executive Summary

On May 6th, 2021, attackers took nearly 100 gigabytes of data out of Colonial Pipeline's network. Colonial halted their operations on Friday, May 7th, after learning they had been hit by a cyber-attack. The investigation is still in the early stages; however, it is believed this attack could be the work of "DarkSide", a group known for deploying ransomware and extorting victims.

While it is not expected to have an immediate impact on fuel supply or prices, the attack on Colonial Pipeline, which carries almost half of the gasoline, diesel, jet fuel and home heating oil used on the East Coast, underscores the potential vulnerability of critical infrastructure to the expanding threat of ransomware attacks. A prolonged shutdown of the line would likely cause prices to spike at gasoline pumps ahead of peak summer driving season, a potential blow to U.S. consumers and the economy. Larger impacts could extend to other industries, as the pipeline supplies jet fuel to major airports and military bases across the United States. Lengthy shutdowns of the Colonial Pipeline have in the past caused gas prices to surge across the southeastern U.S. For example, in 2016, Georgia drivers saw gas prices increase by more than 30 cents per gallon after a leak forced the pipeline to shut down for over 10 days.

Colonial Pipeline is currently taking steps to understand and resolve this issue by bringing in cybersecurity firm FireEye to investigate the situation while the Department of Energy is leading the federal government response; the FBI and Department of Homeland Security have also been engaged. As of May 9th at 7pm EST, there has been no update to when the pipeline will be brought back online, with Colonial only stating they will bring it back online when they believe it is safe to do so.

Fortress Information Security (FIS) will continue to monitor this threat and will update this report as new information is observed.

Threat Identification[1][2]

Attackers took nearly 100 gigabytes of data, in just under 2 hours, out of Colonial Pipeline's network on Thursday, May 6th. Colonial halted their operations on Friday, May 7th, after learning they had been hit by a cyber-attack. The investigation is still in the early stages; however, they believe this attack could be the work of "DarkSide", a group known for deploying ransomware and extorting victims while avoiding targets in post-Soviet states.

[1] https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

[2] https://www.nytimes.com/2021/05/08/us/cyberattack-colonial-pipeline.html

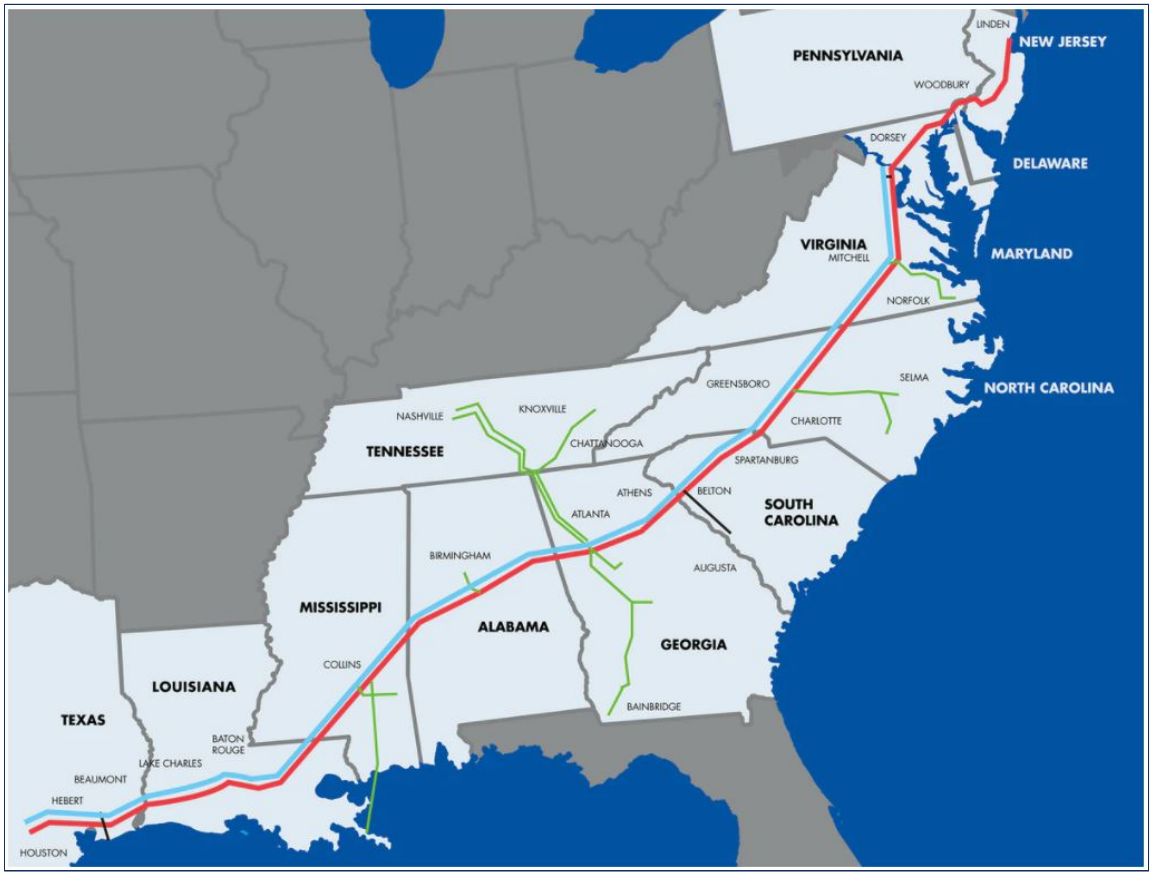


Figure 1 Colonial Pipeline System Map

While it is not expected to have an immediate impact on fuel supply or prices, the attack on Colonial Pipeline, which carries almost half of the gasoline, diesel and other fuels used on the East Coast, underscores the potential vulnerability of critical infrastructure to the expanding threat of ransomware attacks. A prolonged shutdown of the line would cause prices to spike at gasoline pumps ahead of peak summer driving season, a potential blow to U.S. consumers and the economy.

Colonial is taking steps to understand and resolve this issue. Cybersecurity firm FireEye and the FBI have also been brought in to investigate the situation. While the DarkSide ransomware operators are suspected, the exact identity of the attacker is currently unknown. As of Sunday, May 9th, Colonial Pipeline has stated that although the four major pipelines remain offline, some smaller lines between terminals and delivery points are now operational. However, the four shall remain offline until it has been deemed safe to bring them back online.

Colonial Pipeline is the largest supplier of hydrocarbons to the region, transporting more than 2.5 million combined barrels a day. The second largest supplier, Kinder Morgan's Plantation Pipeline, transports approximately 700 thousand barrels a day to the same region and appears to be unaffected by the incident.

Colonial Pipeline subsidiaries, affiliates, and joint venture partners include the following:

- Bengal Pipeline Company, LLC
- Colonial Terminal Logistics, LLC
- Colonial Premier Terminals
- Energy Logistics Solutions, LLC

- Powder Springs Logistics, LLC
- Transport 4, LLC

In-Depth Threat Analysis

Ransomware

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Threat actors then demand a ransom payment in exchange for a decryption key. Threat actors often threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.

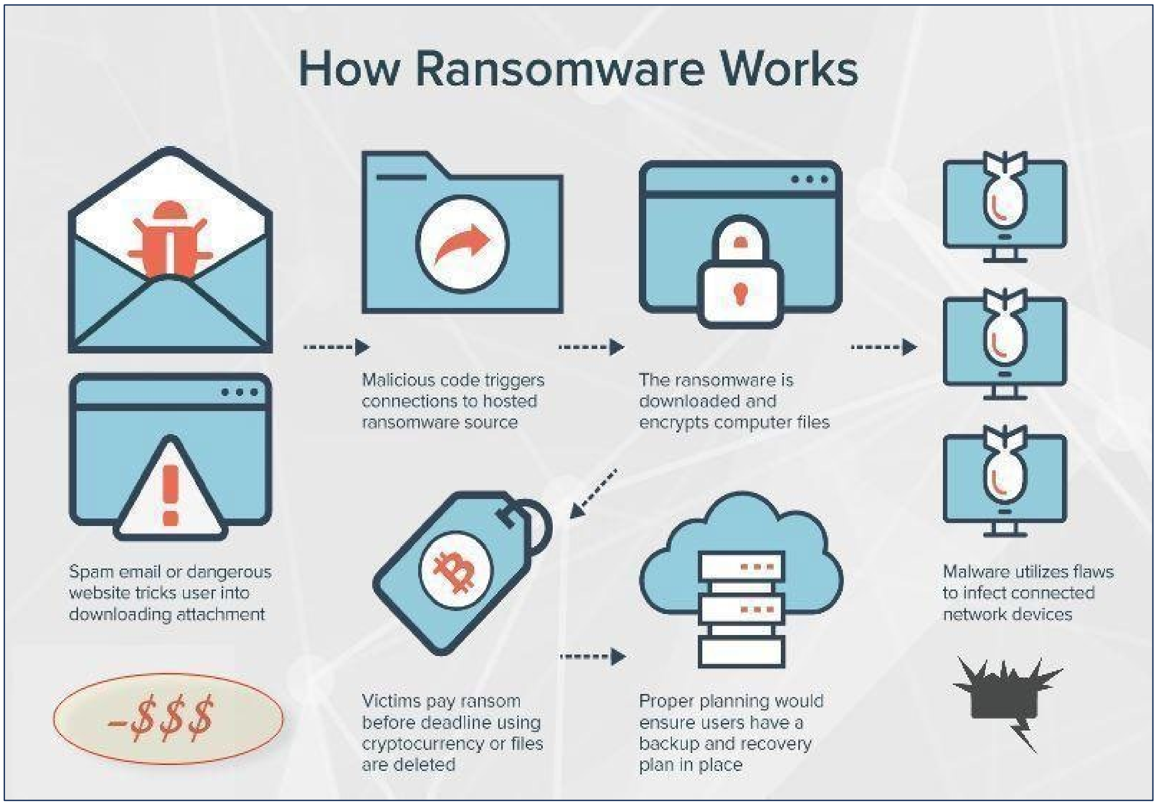

How Ransomware Works
Spam email or dangerous website tricks user into downloading attachment
Malicious code triggers connections to hosted ransomware source
The ransomware is downloaded and encrypts computer files
Malware utilizes flaws to infect connected network devices
Victims pay ransom before deadline using cryptocurrency or files are deleted
Proper planning would ensure users have a backup and recovery plan in place
-$$$

Figure 2 Example of how Ransomware works

Adversaries may encrypt data on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or to render data permanently inaccessible in cases where the key is not saved or transmitted. Common user files like Office documents, PDFs, images, videos, audio, text, and source code files are typically encrypted. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR. To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques. In cloud environments, storage objects within compromised accounts may also be encrypted.

No matter what the scenario, even if the ransom is paid, there is no guarantee that affected users will be able to fully access their systems again. When a ransom demand is paid, a decryption key is supposed to be delivered to the victim; however, there are no guarantees this will happen. Additionally, if a company is known to have paid a ransom in the past, they may see an increase in ransomware attacks from threat actors as the attackers now know the company is likely to give in to ransom demands.

DarkSide Ransomware Group[3]

The DarkSide ransomware group introduced their RaaS (Ransomware-as-a-Service) in August of 2020. Since then, they have become known for their professional operations and large ransom demands. They provide web chat support to victims, build intricate data leak storage systems with redundancy, and perform financial analysis of victims prior to attacking. The group leverages both Windows and Linux toolsets. Much like other ransomware groups NetWalker and REvil, DarkSide has an affiliate program that offers anyone who helps spread their malware 10-25% of the payout.

Historically, ransomware attacks by DarkSide have lasted an average of 5 business days. It is currently believed that DarkSide has only infiltrated the corporate systems; however, it is possible the Colonial tank batteries could have been infected as well.

Anatomy of an Attack

The DarkSide ransomware focuses on the use of stealthy techniques, especially in the early stages. The group performs reconnaissance and takes steps to ensure that their attack tools and techniques evade detection on monitored devices and endpoints. While their initial entry vectors vary, their techniques are more standardized once inside a victim’s network.

Stealth tactics include:

- Command and control over TOR
- Avoiding nodes where EDR is running
- Waiting periods & saving noisier actions for later stages
- Customized code and connection hosts for each victim
- Obfuscation techniques like encoding and dynamic library loading
- Anti-forensics techniques like deleting log files

During the later stages of their attack sequence, they:

- Harvest credentials stored in files, in memory, and on domain controllers
- Utilize file shares to distribute attack tools and store file archives
- Relax permissions on file shares for easy harvesting
- Delete backups, including shadow copies
- Deploy customized ransomware

The following sites offer lists of **Indicators of Compromise (IoC)** associated with DarkSide:

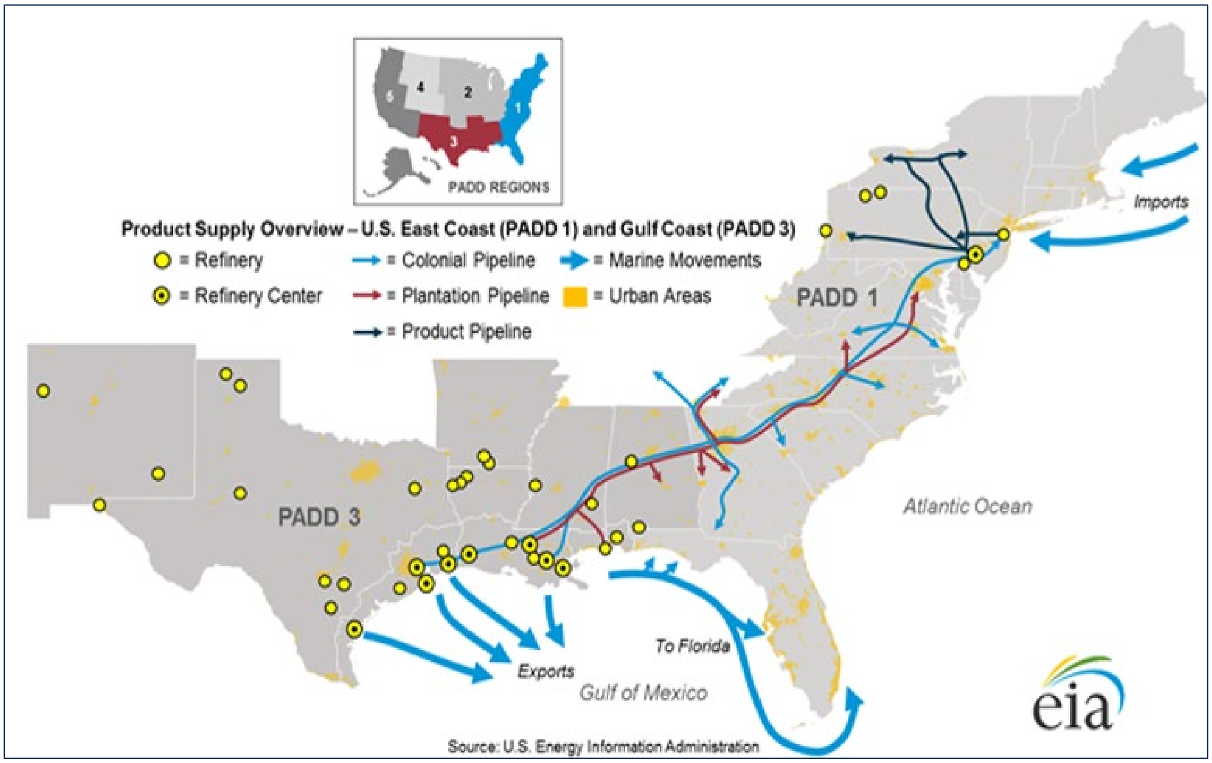
- https://www.areteir.com/darkside-ransomware-caviar-taste-on-your-big-game-budget

[3] https://www.varonis.com/blog/darkside-ransomware/

- https://www.acronis.com/en-us/articles/darkside-ransomware/
- https://www.digitalshadows.com/blog-and-research/darkside-the-new-ransomware-group-behind-highly-targeted-attacks/

Business Impact[4][5]

Current inventory for the Petroleum Administration for Defense Districts (PADD) 1 is approximately 65,029 thousand barrels of total gasoline, 10,811 thousand barrels of jet fuel, and 40,067 thousand barrels of distillate fuel oil (diesel). Using historical data, the gasoline surplus stock will likely be depleted within a month without any refinery input. This can be attributed to the increase in demand stemming from reduced COVID-19 restrictions on travel and normal seasonal travel. Previous outages, such as in 2016, showed that imports can be scaled up to provide relief. Shipping, rail, trucking, and air transport are all options with PADD 2 (Midwest) to PADD 1 sea transit times taking roughly eight days. Imports from Europe can arrive to Europe in as few as ten days, which will reduce the shortage. Due to this, it is estimated that US gas prices should only be increased for a week or two.



Source: U.S. Energy Information Administration

Figure 3 U.S. East Coast (PADD 1) and Gulf Coast (PADD 3) transportation fuels product flows.

[4] https://www.cisa.gov/ransomware

[5] https://www.usnews.com/news/business/articles/2021-05-09/major-us-pipeline-halts-operations-after-ransomware-attack

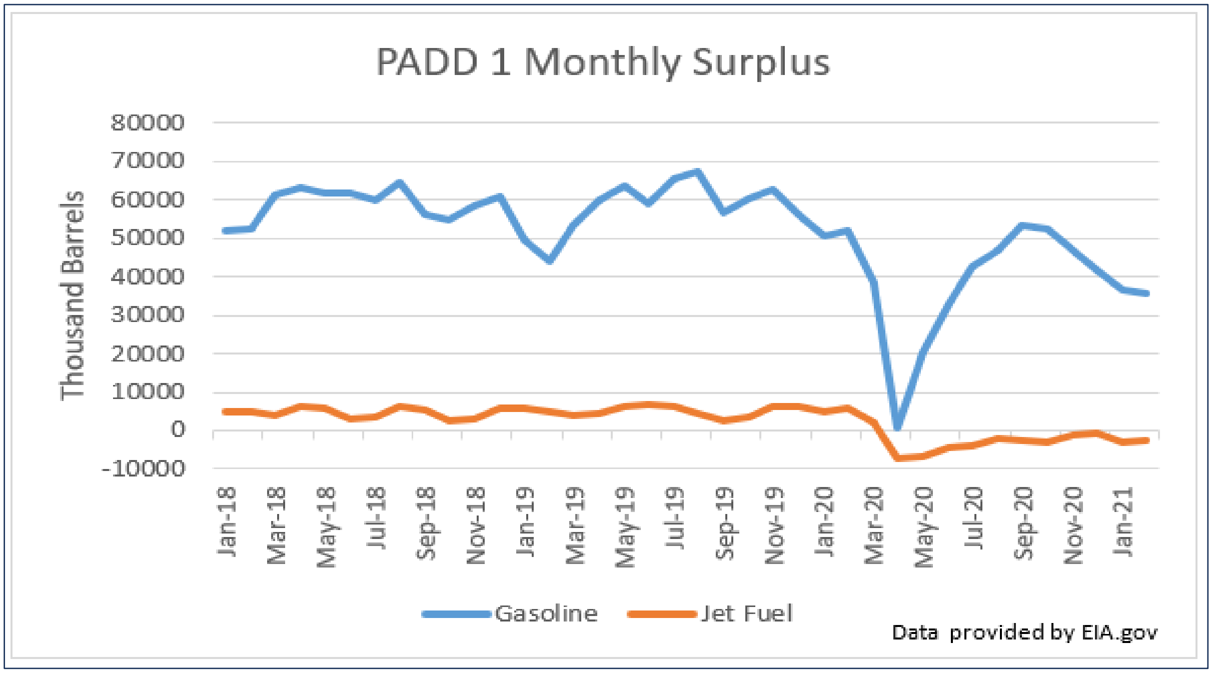


Figure 4 PADD 1 Monthly Surplus

Impacts caused by the outage could extend to multiple industries, as the pipeline supplies jet fuel to major airports and military bases across the United States. Lengthy shutdowns of the Colonial Pipeline have in the past caused gas prices to surge across the southeastern U.S. For example, in 2016, Georgia drivers saw gas prices increase by more than 30 cents per gallon after a leak forced the pipeline to shut down for over 10 days. An outage lasting five or six days could cause gas shortages and price hikes, especially in areas stretching from Alabama to Washington, D.C. Extended delays could also lead to major impacts on jet fuel supplies, affecting major airports operating in Atlanta and Charlotte.

Security Recommendations and Remediation Strategies

Mitigation

Securing Networks and Systems

- **Have an incident response plan** that includes what to do during a ransomware event.
- **Backups are critical.** Use a backup system that allows multiple iterations of the backups to be saved in case a copy of the backups includes encrypted or infected files. Routinely test backups for data integrity and to ensure it is operational.
- **Use antivirus and anti-spam solutions.** Enable regular system and network scans with antivirus programs enabled to automatically update signatures. Implement an anti-spam solution to stop phishing emails from reaching the network. Consider adding a warning banner to all emails from external sources that reminds users of the dangers of clicking on links and opening attachments.
- **Disable macros scripts.** Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
- **Keep all systems patched**, including all hardware, including mobile devices, operating systems, software, and applications, including cloud locations and content management systems (CMS), patched and up to date. Use a centralized patch management system if

possible. Implement application whitelisting and software restriction policies (SRP) to prevent the execution of programs in common ransomware locations, such as temporary folders.
- **Restrict Internet access.** Use a proxy server for Internet access and consider ad-blocking software. Restrict access to common ransomware entry points, such as personal email accounts and social networking websites.
- **Apply the principles of least privilege and network segmentation.** Categorize and separate data based on organizational value and where possible, implement virtual environments and the physical and logical separation of networks and data. Apply the principle of least privilege.
- **Vet and monitor third parties** that have remote access to the organization's network and/or your connections to third parties, to ensure they are diligent with cybersecurity best practices.
- **Participate in cybersecurity information sharing** programs and organizations, such as MS-ISAC and InfraGard.

Securing the End User
- **Provide social engineering and phishing training to employees.** Urge them not to open suspicious emails, not to click on links or open attachments contained in such emails, and to be cautious before visiting unknown websites.
- **Remind users to close their browser** when not in use.
- **Have a reporting plan** that ensures staff knows where and how to report suspicious activity.

Fortress Information Security Recommendations

Fortress Information Security (FIS) recommends companies take defensive measures to minimize the risk of exploitation of vulnerabilities. Specifically, companies should:

Implement Controls to Prevent and Detect Malware Deployment:
- Ensure that antivirus/endpoint protection software is deployed on all endpoints. Antivirus signatures should be kept updated to ensure it is protecting against the latest threats.
- Monitor outbound network traffic for any suspicious activity – this could serve as an indicator of malware attempting to communicate with a Command and Control (C2) server.
- Ensure your security tools are monitoring for known indicators of compromise.
- Malware is frequently delivered by phishing emails, so ensure that users are trained not to open attachments or click on links from suspicious sources.

Protect your Network from External Attackers:
- Ensure all network and system resources are properly protected by firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS).
- Configure firewalls to block known malicious IP addresses.
- If remote access to corporate resources is needed, be sure employees use a Virtual Private Network (VPN).
- Ensure that your company maintains an up-to-date inventory of all externally facing assets. Maintaining an accurate asset inventory is critical in ensuring defensive measures are properly deployed across the entire perimeter.

Develop a Data Loss Prevention Program:
- Ensure system monitoring is in place to be able to track who is accessing specific files. This will help pinpoint exactly when files were extracted and who was involved.

- Scan all outgoing emails to detect any potential confidential data leaving the company's network.
- Consider limiting access to cloud storage websites that can be accessed from outside of the corporate network. If there is not a legitimate business need to use these types of websites, they may present undue risk of data exfiltration.
- Limit users' ability to store data on external storage devices, unless there is a business need to do so.

Have a Vendor Risk Management Program:

- Security breaches at vendors that have access to your company's data or systems can pose just as much of a threat as a data breach at your company. Ensure you have a program in place to manage these risks and respond to vendor breaches when they occur.
- Ensure that network traffic and email communications between your company and its vendors is monitored for any anomalies that could indicate malicious activity.
- Evaluate all vendors' security controls regularly to ensure they align with your company's risk posture.

FIS reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.