This report today will cover:

The Colonial Pipeline Ransomware attack, the threat actors, Malware, response efforts, and additional developments and effects of the cyber-attack that have had an impact on society and the industry.

**The Threat Actors:**

In this breach of Colonial Pipeline, wherein the hackers stole nearly 100 gigabytes of data in just 2 hours, the threat actors are a Russian outfit called DarkSide, which surfaced in August 2020, sells Ransomware as a Service and are known to have ties to Russian President Vladimir Putin. DarkSide has already created a leak website used in double-extortion campaigns, in which victim companies are not only locked out of their systems, but also have their information stolen. Darkside largely target for-profit companies from English-speaking countries. They have openly acknowledged that their malware was used by associates in the Colonial Pipeline attack. The group actually fashions itself as a modern-day cyber-Robin Hood—making money off of the rich and even donating some to charity. The organization is part of a constellation of criminal actors—that are long-known in the cybersecurity world—that emanates from Russia and its former Soviet states, as well as North Korea, China, Syria, and Iran. Darkside claimed to disband on May 14th, but many Cybersecurity experts suspect DarkSide was just laying low for a while to allow the attention to abate from the Colonial Pipeline Ransomware attack, and that the group would re-emerge under a new banner in the coming months. According to an analysis published May 18 by cryptocurrency security firm Elliptic, DarkSide was able to extort a total of $90 million in Bitcoin from 47 cybercrime victims.

**Ransomware:**

The Ransomware used in the attack by DarkSide is ransomware they sold to affiliates using the Ransomware-as-a-Service (RaaS) distribution model, so attacks are carried out by affiliates. There are currently two known versions of DarkSide: DarkSide v1.0 and DarkSide v2.1. The latter is less weighty in terms of file size (53 KB versus 59.5 KB). v2.1 has a shorter decryption time and a new “call on us” feature, which allows ransomware affiliates to conduct a Voice Over IP (VoIP) session with victim organizations, their partners, and even journalists. It is believed that they added this feature to exert extra pressure against their victims. DarkSide also has a Linux version that is capable of targeting VMWare ESXi vulnerabilities, making virtual machines (VMs) susceptible to hijacking and encryption of virtual drives.

DarkSide is human-operated, which means that the ransomware is executed by an actual person behind the screen after they have successfully infiltrated a target network. This makes it possible for threat actors to move laterally, scouring the entire network to persistently backdoor several systems until they gain administrative access. They use these administrator credentials to deploy the DarkSide. They also use their time in the network to harvest data and upload to their servers, before they encrypt the victim’s copy.

Once deployed, DarkSide begins to: Encrypt all files using a combination of Salsa20 and RSA-1024; empty the Recycle Bins; uninstall services; delete shadow copies; terminate processes; encrypt local disks; and encrypt network shares.

After all the data has been exfiltrated, they post it on their leak site, DarkSide Leaks, along with other pertinent information about the attack, such as the name of the company, the date it was breached, how much data was stolen, sample screenshots of the stolen data, and the types of stolen data. DarkSide ensures that victims feel their personalized touch by customizing the ransom note and file extension for their victims.

**The techniques used:**

DarkSide demonstrate many modern ransomware techniques. The malware first collects basic information about its victim’s computer systems to learn the details of the technical environment. Darkside skips victims from certain geographical regions by checking the language used by their systems. (Notably, DarkSide does not attack systems that use Russian or other Eastern European languages).  Then, DarkSide determines what files to encrypt.  They’re particularly selective about what files they encrypt, and select them mainly by examining their file directories, file names, and file extensions. In order to remain anonymous and prevent prompt shutdown, websites for contacting ransomware threat actors are hosted in the Tor network.

**Darkside’s Anti-detection techniques:**

To stay under the radar until the victim’s systems are impacted, DarkSide incorporates the commonly used techniques below:

**Self-encryption:**

Most of Darkside’s critical strings are encrypted to avoid triggering detection. For the same reason, the malware’s main configuration is also encrypted. It is compressed with aPLib, with individual configuration values encoded with a Base64 algorithm.

**Darskide use Dynamic API resolution:**

They don’t immediately have all the APIs used available in the import table, as legitimate executables do. Instead, they resolve them dynamically before using them, some by hashed names and some by encrypted names.

**DarkSide incorporates multiple techniques to ensure ransom is paid:**

Ransomware makes sure that standard backup solutions are unusable on the targeted machines. Windows particularly has a feature called Shadow Copy aimed at dealing with such situations. It allows the creation of backup copies of computer files so they can be restored when needed, but the main limitation of this approach is that the backup files are stored on the same system as the original files. DarkSide disables various backup solutions, searching for them by name and when the malware compromises the system, the backup files are readily deleted.

**Darkside also use asymmetric and symmetric encryption correctly:**

Darkside only embeds the public key in the malware and keeps the private key confidential. The main disadvantage of asymmetric encryption over symmetric is the encryption speed, and to get the best of both worlds, the authors of DarkSide encrypt victims’ files using a symmetric encryption algorithm (Salsa20 with a custom matrix), and then they encrypt the corresponding symmetric keys with their asymmetric public key (the RSA-1024).

**The response efforts by Colonial Pipeline and Mandiant (The organization colonial brought in to investigate):**

A little more than one week after the hack occurred, on May 7, an employee in colonial’s control room saw a ransom note demanding cryptocurrency, that appeared on a computer just before 5 a.m. The employee notified an operations supervisor who immediately began to start the process of shutting down the pipeline. By 6:10 a.m., the entire pipeline had been shut down. So, they responded rather quickly to the news of the hack.

Colonial brought Mandiant in to investigate. Mandiant swept the network so that they could understand how far hackers had probed and they also installed new detection tools that would alert Colonial of any follow-on attacks. They found a VPN account, which has since been deactivated, didn’t use multifactor authentication, allowing the hackers to breach the network using just a compromised username and password. They did an exhaustive search of the environment to try and determine how Darkside actually got those credentials, and they found nothing. Their investigators haven’t found any evidence the same group of hackers tried to regain access either.

Mandiant also traced the hackers’ movements within the network to determine how close they got to compromising the pipeline’s operating systems. Colonial Pipeline said the attackers only hit its business IT networks — not its pipeline security and safety systems. Now, while the hackers did move around within the company’s information technology network, there wasn’t any indication they were able to breach the more critical pipeline operational technology systems. After Mandiant and Colonial were able to conclusively determine that the attack had been contained, that’s when they considered re-opening their pipeline.

**The final portion of this report will cover the lasting effects that the attack had on society and on the company:**

**The Additional Developments after the attack were that:**

President Biden signed an executive order to improve federal cybersecurity. The order includes a shift to multi-factor authentication, data encryption both at rest and in transit, a zero-trust security model, and improvements in endpoint protection and incident response.

A Cybersecurity Safety Review Board was established. Also, a Security Directive was implemented by The Department of Homeland Security, which requires three critical actions. First, it requires TSA-specified Owner/Operators to report cybersecurity incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Second, it requires Owner/Operators to designate a Cybersecurity Coordinator who is required to be available to TSA and CISA 24/7 to coordinate cybersecurity practices and address any incidents that arise. Third, it requires Owner/Operators to review their current activities against TSA's recommendations for pipeline cybersecurity to assess cyber risks, identify any gaps, develop remediation measures, and report the results to TSA and CISA.

Also, the FBI and CISA issued a joint cybersecurity advisory (CSA) against DarkSide ransomware. It contains detailed mitigation steps that businesses should follow to reduce the risk of successful ransomware attacks overall. These include simple steps, such as: Enabling stronger spam filters, updating software to their latest versions, regularly scanning systems using a good antivirus product, and limiting access to resources over networks.

**The lasting effects on the company:**

**Business Consequences:**

**Business disruption:**

Colonial Pipeline impacts a large swath of the United States, as they transport 45% of the United States' gas, diesel, military supplies, etc., along the East Coast.  The breach forced Colonial to shut down its Houston to New England fuel pipeline for a week and prompted long lines, price hikes, and gas shortages at gas stations across the nation. Some of those companies are still being pursued legally for price gouging.

**Revenue loss:**

In this case, even after the decryption key was passed along from Darkside to Colonial, the systems couldn’t be adequately brought back online quickly, and the Colonial CEO stated they were still unable to properly bill customers. The long-term impact, according to the CEO, will likely cost the company tens of millions of dollars.

**Reputational damage:**

Of course, business wise reputation is everything. Anytime a breach of this magnitude occurs, and it's part of the news cycle for weeks, it’s bad for business. For this reason, customers can defect to the competition because they lose confidence in the business' ability to keep their information safe.

**Monetary Damage:**

Colonial Pipeline acknowledged that they paid a 75 bitcoin, or the equivalent of $4.4 million ransom to DarkSide. The U.S. Department of Justice did recover $2.3 million worth of Bitcoin that Colonial Pipeline paid to Darkside, but that still means Colonial Pipeline took a $2.1 million hit. That’s not pocket change, so they will definitely feel the effects from that loss.

The business can also be hit with fines and penalties for non-compliance with governmental and industry guidelines, rules and regulations. Depending upon what they were found to be non-compliant with, GDPR fines can cost an organization up to 4% of its revenue.

The company can also incur regulatory scrutiny as even after paying fines and penalties for non-compliance, businesses can be subjected to costly regulatory audits for years to come.

Sources: [cnn.com](https://www.cnn.com/2021/05/16/tech/colonial-ransomware-darkside-what-to-know/index.html), [bloomberg.com](https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password), [The Daily Signal](https://www.dailysignal.com/2021/05/20/what-we-know-about-darkside-the-russian-hacker-group-that-just-wrecked-havoc-on-the-east-coast/), [The Washington Post](https://www.washingtonpost.com/business/2021/05/25/colonial-hack-pipeline-dhs-cybersecurity/), [krebsonsecurity.com](https://krebsonsecurity.com/2021/06/justice-dept-claws-back-2-3m-paid-by-colonial-pipeline-to-ransomware-gang/), [zdnet.com](https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/), [Malwarebytes Blog,](https://blog.malwarebytes.com/ransomware/2021/05/threat-spotlight-darkside-the-ransomware-used-in-the-colonial-pipeline-attack/) and [automation.com](https://www.automation.com/en-us/articles/may-2021/colonial-pipeline-ransomware-attack-darkside-works)