Drexel Hamilton
A Service-Disabled Veteran Owned & Operated Business

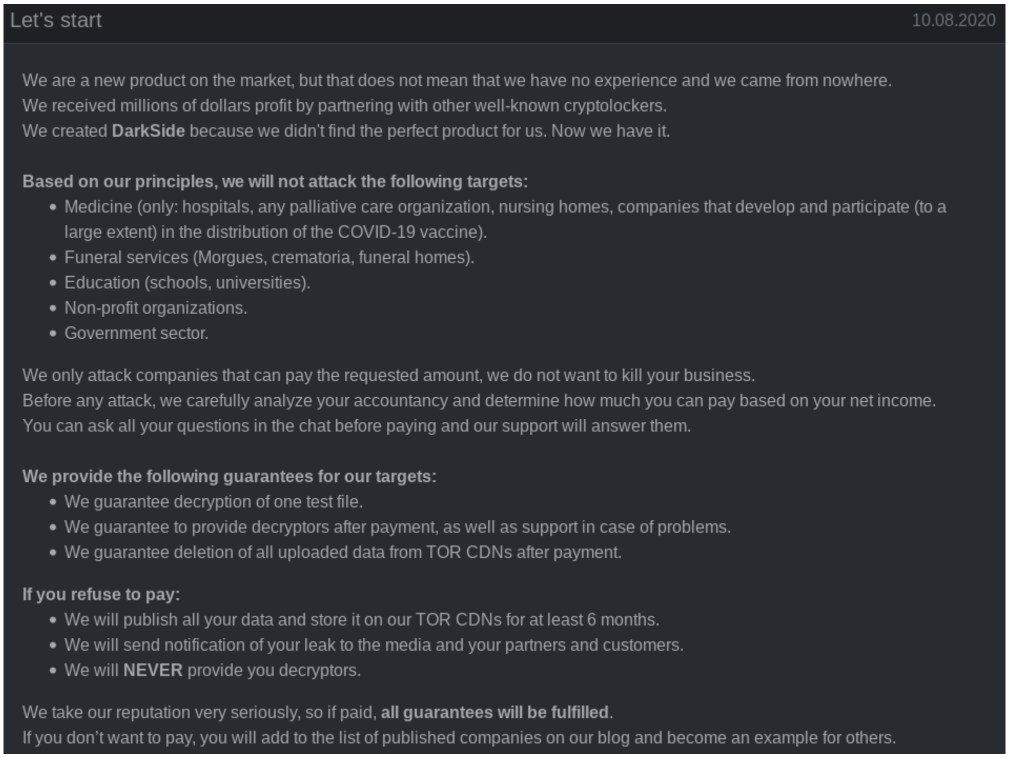
# Outside the Wire

# Update on the Colonial Pipeline and Clashes in Israel

## Situation 1: Cyberattack on the Colonial Pipeline

On May 7, a ransomware attack hit Colonial Pipeline. According to the FBI, the alleged attacker is a cybercriminal organization known as “Darkside.” Some intelligence sources believe Darkside may be operating out of Russia. They are a well-known group, and operate with standard protocols for cyber attacks. In many ways, these types of criminal organizations operate like a business and are concerned with their reputation namely their credibility in releasing the ransom once the payment is made.

In terms of operations, the group begins by breaching into a victim’s network and stealing their data. They then encrypt the entire network and demand a ransom payment from the victim to unlock the network. If the victim pays the ransom (usually with cryptocurrency), they are given a decryption key, informed of how the attack was completed, and then left alone. But if they refuse to pay the ransom, Darkside promises to release all of the data to public media, partners, and customers, and never provide the decryption key to get access to their networks back. Below is an advertisement for the Darkside Ransomware group that was found on the darknet:



Let's start 10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

**Based on our principles, we will not attack the following targets:**

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

**We provide the following guarantees for our targets:**

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

**If you refuse to pay:**

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

Disclaimer: The information and statistical data contained herein have been obtained from sources that Drexel Hamilton, LLC (“Drexel”) believes are reliable, but Drexel makes no representation or warranty as to the accuracy or completeness of any such information or data and expressly disclaims any and all liability relating to or resulting from your use of these materials. The information and data contained herein are current only as of the date(s) indicated, and Drexel has no intention, obligation, or duty to update these materials after such date(s). These materials do not constitute an offer to sell or the solicitation of an offer to buy any securities.

In response to the attack, Colonial Pipeline immediately shut down all of its networks to stop any further cyber activity. The pipeline system spans over 5,500 miles and transports approximately 45% of fuel on the East Coast. With echoes of the March 2020 run on toilet paper, consumers rushed to the pump to fill up in anticipation of supply running out.

Colonial Pipeline is hopeful to get their system back online by the end of the week. They are currently working with the Department of Energy to prioritize the manual delivery of fuels to areas that need it the most. Their latest response made last night contained the following:

*"Colonial Pipeline continues to make forward progress in our around-the-clock efforts to return our system to service, with additional laterals operating manually to deliver existing inventories to markets along the pipeline. Markets experiencing supply constraints and/or not serviced by other fuel delivery systems are being prioritized. We are collaborating with the Department of Energy (DOE) to evaluate market conditions to support this prioritization."*

Additionally, users may have noticed that the Colonial Pipeline website went down for a few hours yesterday morning. The site is back up at this time and it appears that the company has put a preventative reCAPTCHA filter on to prevent another attack.

## Moving Forward:

This issue can be worked on by the public and private sectors. In the public sector the U.S. government can start holding foreign state actors accountable for these types of attacks. As we have noted in the past, the U.S. government lacks a comprehensive cyber deterrence strategy. There is the possibility of retributions on nation-states that launch or sponsor cyber-attacks against the U.S. specifically in the form of sanctions or through diplomatic actions. Actions must be implemented that would effectively raise the cost of performing an attack, so that the perpetrators would be forced to ask themselves beforehand, "is this really worth it?". Things like sanctions, embargos, penalties, and U.S. responses "in-kind" could be enacted to hit the enemy in their wallets. Stricter punishments should be put in place and publicly known for those who wish to tamper with cybersecurity. Finally, the United States could enable or institute a national supply-chain hardening system so that there are more controls over vendors and suppliers of cybersecurity products. Legislation could require vendors of security software for private companies and the DOD to prove that their networks are heavily secured.

U.S. infrastructure needs greater defense funding for physical improvements to resources that are reliant on computer networks so there is redundancy when the systems go offline. This could be supported by a dedication to cybersecurity-related physical improvements in the currently proposed infrastructure bill. Due to a reliance on technology networks for defense, much of the military has been training for a potential environment in which power and computer networks are lost. As seen in this situation, that threat is becoming more realistic by the day.

Disclaimer: The information and statistical data contained herein have been obtained from sources that Drexel Hamilton, LLC ("Drexel") believes are reliable, but Drexel makes no representation or warranty as to the accuracy or completeness of any such information or data and expressly disclaims any and all liability relating to or resulting from your use of these materials. The information and data contained herein are current only as of the date(s) indicated, and Drexel has no intention, obligation, or duty to update these materials after such date(s). These materials do not constitute an offer to sell or the solicitation of an offer to buy any securities.

In the private sector, there are many things that individuals and companies can do to strengthen their security. First, there should be increased due diligence on an organization's internal network security. Too often people lose passwords, do not use strong passwords, and are victims of phishing scams. Social engineering remains the biggest threat. This is a problem that requires training and education of the workforce. There is no easy technical solution. Second, every company that has valuable data on a computer network should be invested in some sort of cybersecurity effort. Whether that includes hiring a third-party cybersecurity firm, or IT personnel who specialize in penetration testing so that vulnerabilities are patched before breachers can hack them.

## Situation 2: Clashes and Violence in Israel

While the situation in Israel is being highly covered in the media, there have always been high tensions between the Israeli government and Palestinians (Hamas) living in Israel.

The Israeli government is currently dealing with what they have termed as domestic terrorism. In the past few days, we have seen reports of airstrikes, rocket attacks, and riots throughout their country. As of this morning, there have been around two dozen people killed, and hundreds hospitalized as a result of these clashes.

The current situation began with Israel and Palestine on edge all week over a dispute for land near Gaza. Six Palestinian families were evicted by Israeli Police from their homes in Sheikh Jarrah a week ago because of a court order, which came to be from a few Israeli settlers filing a claim for the land. Israelis and Palestinians have always had tensions due to a difference in religious beliefs and a lack of homeland for which they have to share.

In response to this, Palestinians gathered and had been performing somewhat peaceful protests for a few days. Violence began escalating when Israeli police attempted to disperse the gatherings. On May 9, a few hundred Palestinians crowded the Al-Aqsa Mosque and refused to leave despite commands from the police. Israeli police then performed a raid on the compound and remained there to get a foothold.

The Palestinians decided to evacuate the area and changed course by shooting rockets at police forces in the mosque and in greater Jerusalem. Finally, the Israeli government has been responding by pulling their forces out and launching airstrikes into various areas of Jerusalem.

Israeli Prime Minister Benjamin Netanyahu has spoken publicly about these events, stating that order needs to be restored.

---

We will continue to monitor these situations and provide feedback on them as they go on.

Disclaimer: The information and statistical data contained herein have been obtained from sources that Drexel Hamilton, LLC ("Drexel") believes are reliable, but Drexel makes no representation or warranty as to the accuracy or completeness of any such information or data and expressly disclaims any and all liability relating to or resulting from your use of these materials. The information and data contained herein are current only as of the date(s) indicated, and Drexel has no intention, obligation, or duty to update these materials after such date(s). These materials do not constitute an offer to sell or the solicitation of an offer to buy any securities.