Confluence INVESTMENT MANAGEMENT

Weekly Geopolitical Report

By Bill O'Grady

June 14, 2021

The Geopolitics of the Colonial Pipeline Ransomware Attack: Part I

On Thursday, May 6, 2021, hackers attacked the Colonial Pipeline, capturing data by infiltrating the company's business software. In response, the company closed its 5,500-mile pipeline to assess the damage and protect critical infrastructure. Eventually, the company paid the ransom and service was restored.

Although a criminal event usually doesn't have geopolitical ramifications, this one did, in our opinion. The attack brought down a pipeline that connects refineries in Texas and Louisiana that provide petroleum products as far north as New Jersey. The situation highlighted the vulnerabilities of critical infrastructure, the nature of criminal ransomware enterprises, the role of cryptocurrencies in criminal transactions, and the problems of scale in criminal activity.

In Part I of this report, we will begin with an overview of the attack followed by reflections on organized crime. We will also deal with the attractiveness and growth of ransomware. Comments about the firm involved in the attack, Darkside, will follow. Part II will discuss why this cyberattack was a serious mistake. The subsequent discussion will focus on the parties that were adversely affected by this event and we will close with market ramifications.

The Colonial Pipeline Cyberattack

As noted above, the company became aware of the attack on May 6, when it discovered company data had been encrypted. The Colonial Pipeline is an important part of America's energy infrastructure.

(Source: Colonial Pipeline via Axios)

This long pipeline supplies 45% of fuel consumed by the Eastern Seaboard. It has been called the "jugular" of the U.S. fuel pipeline system.

What happened? Hackers deployed ransomware onto the Colonial Pipeline business software. It's important to note that the attackers didn't go after the command and control software, which are the parts of the system that control and monitor the flows of product on the pipeline. Instead, they attacked the business software which controls billing and sales. In general, critical infrastructure entities tend to separate business software from command and control software. Because they are so sensitive, the latter software are often "air gapped" from the rest of the system and the internet. In other words, they aren't connected to the internet and therefore usually can't be indirectly accessed. But, in the case of the Colonial Pipeline, the command and control software weren't completely separate. This condition likely occurred because the company wanted to use the flow information from the command and control software to communicate with

the business software for billing and other business purposes. Because the company wasn't sure of the extent of the attack, it decided to shut down the entire system.

At first glance, closing down the pipeline over a disruption of billing seems aggressive. After all, it would seem that the company could figure out, over time, what it was owed. However, in this case, the billing software was tied to the flow of product, and so without it, the pipeline couldn't be sure where it had shipped product. So, even if the command and control systems were not affected, the potential for mayhem remained elevated.

In addition, the hackers took control of critical business information and threatened to "dump" it on the open market. This action would have made sensitive account data available to the criminal elements, causing further damage.

Shortly after the pipeline was closed, shortages began to develop. The inability of refiners to move product onto the Colonial Pipeline system led to shutdowns of parts of several refineries. The lack of supply, coupled with panic buying, led to higher gasoline prices. Gas lines began to appear.

(Source: KTLA)

There were reports of gasoline stations running out of fuel. Gas lines and signs saying "no gas" are a danger for any U.S. political party in power. The Biden administration moved to relax rules on shipping fuel by truck and rail. But, ultimately, the administration needed the pipeline to reopen.

Eventually, Colonial Pipeline management were contacted by the hackers. The company decided to pay the hackers and operations were restarted on May 12. The company paid around $4.4 million to receive its data back. As a result, the company sent the hackers 75 bitcoins and received back software that only partially reversed the encryption. In general, the FBI warns against paying ransomware hackers. In some cases, the hackers deceive its victims and fail to decrypt the data. In other cases, multiple criminal entities may be involved, and it is hard to tell which criminal group controls the encrypted data. Some reports suggest that victims have found that one criminal group may control part of the encrypted data while another group may control other parts. But the biggest worry is a macro one. Although it might make sense for an individual firm to pay the ransom, if all hacked entities pay, it becomes more appealing for criminals to continue to encrypt data and demand money.

Reflections on Organized Crime

Before we address the specifics of the alleged hackers, a reflection on organized crime might assist in framing their behavior and goals. Organized crime tends to engage in two types of activities. The first is to satisfy demand for products or services that society deems detrimental. The classic example of this first type is Prohibition. The U.S. government outlawed the sale of alcoholic beverages to protect society from the ills of alcohol consumption. Americans still wanted to consume alcohol and organized crime moved to fill the supply to meet that demand. There are numerous

examples of this sort of behavior, including illicit drugs, prostitution, gambling, etc., that society deems should not be provided by the licit private sector, but sufficient demand still exists for such products and services. Or, there are some cases where these products and services are provided but are heavily regulated and taxed. Organized crime will offer an unregulated and untaxed product to consumers.

The second major activity of organized crime is to engage in threatening behaviors to extract money from the economy. Protection rackets, extortion, kidnapping, robbery, etc. are examples. Unlike the previous example, there is no obvious demand for such activities. In general, society tends to tolerate these behaviors to a certain point. In other words, when the cost of eradicating the activity is seen as greater than the cost of its existence, it is allowed. But, for society, the perceived cost of these activities is not fixed. What may have been allowed before can become intolerable in the right circumstances.

Ransomware in the Tolerated Category

Ransomware falls into the second category. Initially, ransomware struck individuals. Often, households neglect to purchase malware protection and upgrade operating systems. Weak passwords are common and home users can be susceptible to "phishing" campaigns where malware is inadvertently introduced to a computer by opening a link in an email. Payment for such activities was small.

However, over time, much more sophisticated operations have developed that target corporate users. These gangs often have ties to intelligence services in some nations; it is not uncommon for such criminals to have been in the military or intelligence agencies. Russia and Eastern Europe tend to harbor these activities. Although these governments don't necessarily direct these operations, they are given protection from Western law enforcement.[1]

As organized crime has moved into ransomware, the activity has become more lucrative and sophisticated. In 2019, the FBI's Internet Crime Report showed that ransomware losses were over $8.9 million. Last year, losses were $29.1 million. Most analysts believe that the FBI's reports fail to capture much of the losses to ransomware, which may run as high as $2.4 billion in the U.S. alone.

There are two factors that have made ransomware quite attractive. First, the losses to ransomware are often insured, so the decision to pay the ransom is easier if the losses are not directly borne by the company. We note that AXA (SA, USD, 27.55) recently announced it will no longer reimburse ransomware losses in France.[2] The wider the losses from this activity, the more it becomes an uninsurable risk; an insurable risk requires non-correlation in order to properly assess the likelihood of an event. Once it becomes common, it is also concentrated enough to become impossible to insure. Complicating matters further is that the existence of insurance leads to moral hazard. In other words, the cost of insurance has to rise to a point where paying for better security is economic.

---

[1] North Korea and China also engage in hacking, but more often it is state directed. Although North Korea uses criminal activity to raise revenue for the state, its targets are often state directed. There is also some evidence to suggest organized crime in the PRC is starting to engage in similar behaviors as seen by those operating in Russia and Eastern Europe, but they are not to that scale as of yet.

[2] In what may be the ultimate example of irony, the company's operations in Asia were hit with ransomware attacks.

The second factor is that cryptocurrencies are the payment of choice for these actors. These currencies offer a degree of pseudo-anonymity and can be easily transferred across borders. The recent rally in cryptocurrencies means that the ill-gotten gains from criminal activity are rising in value, allowing these gangs to build more talented staff and become even more effective.

As ransomware has become more lucrative, it is growing rapidly and is becoming increasingly sophisticated. One development, which was seen in the Colonial Pipeline attack, is the so-called "double attack." Not only is the data encrypted, but the hackers threaten to release the data to the public and the media if the target doesn't pay. This double attack means that simply maintaining air-gapped backups doesn't protect the victim because even if they can restore the data without the encryption key, the hacker can still disclose it and embarrass the firm (by making internal comments public) and reveal sensitive customer information.

The gold standard of ransomware is to attack a victim successfully, with the knowledge that they will likely pay and not make a public spectacle of the event. After all, the aim isn't to cripple the firm but to extract ransom.

Darkside

Soon after the attack on Colonial Pipeline, speculation rose that the hacker Darkside was involved. This crime group, which is said to circulate in Russia and Eastern Europe, is thought to be very sophisticated. The gang operates a "ransomware as a service" model, which means it not only conducts its own ransomware operations but allows other criminal enterprises to use its software to conduct ransomware attacks. According to reports, it interviews potential users carefully and restricts application of its software. Darkside even has a customer service department and offers testimonials to its victims about its trustworthiness in holding up its end of the bargain if the ransom is paid.[3] The gang also restricts targets for the groups that use its software; it won't allow its software to be used against hospitals, non-profits, educational institutions, or providers of funeral services. And, it strictly prohibits attacking any victim in the Commonwealth of Independent States, which is most of the former Soviet Union. This has given credence to the idea that it has ties to Russia.

When Darkside is looking for victims, it studies them closely to see not only where their software vulnerabilities lie but also their financial shape and if they carry insurance. It takes this information into account when it hacks a target and sets a ransom that is more likely to get paid without incident. The enterprise has framed ransomware as a professional activity.

Part II

Next week, we will discuss why this attack was a mistake and who suffers from it, and close with market ramifications.

Bill O'Grady
June 14, 2021

[3] Listen from the 6:20 mark on the linked podcast.

Confluence Investment Management LLC

Confluence Investment Management LLC is an independent Registered Investment Advisor located in St. Louis, Missouri. The firm provides professional portfolio management and advisory services to institutional and individual clients. Confluence's investment philosophy is based upon independent, fundamental research that integrates the firm's evaluation of market cycles, macroeconomics and geopolitical analysis with a value-driven, company-specific approach. The firm's portfolio management philosophy begins by assessing risk and follows through by positioning client portfolios to achieve stated income and growth objectives. The Confluence team is comprised of experienced investment professionals who are dedicated to an exceptional level of client service and communication.