If you use a Computer, You've Gotta think about Ransomware…

Published 28 June 2021

Christopher Gannatti, CFA
Global Head of Research

We will look back on 2021 and view the Colonial Pipeline attack as the moment that galvanised a coherent US policy and an enforcement response to ransomware. This was one of the largest hacks a US energy system has ever endured1.

To recap: The Colonial Pipeline is roughly 5,500 miles and is the largest refined products pipeline in the US, supporting about 45% of East Coast fuel consumption2. It goes from Houston, Texas on the gulf coast up to the New York (NY) metro area. The actual ransomware attack hit Colonial's information technology (IT) systems, but, as a precautionary measure, the firm shut down their operational technology systems as a result of uncertainty in the early hours of the attack3.

It is the case today that most ransomware attacks impact IT systems as opposed to operational technology systems. Ransomware experts are seeing an uptick in the targeting of industrial control systems, but a critical point to note is that many systems do not have high connectivity between IT and operational control.

Darkside: Victim of the Publicity Paradox

Within the ransomware world, anonymity is one of the most prized assets. Darkside, a cybercriminal hacking group and widely viewed as possibly producing the specific malware used in the Colonial Pipeline attack, views ransomware as a business. Cybereason, a cybersecurity defence platform, estimates that their malware has been used to compromise more than 40 victims, demanding figures between $200,000 and $2 million in each case4. However, they are conscious of their reputation, declaring publicly that they would not target health care systems, schools, or businesses that they believe cannot pay ransoms5.

During the Covid-19 Pandemic, cloud computing and the concept of 'Software-as-a-Service' (SaaS) has proliferated. Darkside is seeking to be a player in 'Ransomware-as-a-Service.' The organisation is offering their software on loan to criminal organisations6.

The most profitable, long-run strategy for Darkside would be to remain in the shadows. As a consequence, the Colonial Pipeline attack has awakened the full unified force of the US justice department and Biden Administration, making 'Darkside' almost a household name.

To Pay or Not to Pay—this is the Crucial Ransomware Question

To hear the Federal Bureau of Investigation's (FBI) advice is apparently to 'never pay.' If every victim perfectly adhered to this advice, then it would be impossible for a ransomware attacker to make money.

Ransomware attackers have an oddly rational stance in the sense that while many victims might feel ‘unlucky’, it is much more likely that targets are researched in detail. Why? If the criminal organisations are going to take the effort, they may want to ensure the likelihood of payment.

The CEO of the Colonial Pipeline did opt to pay the ransom, which was roughly 75 bitcoin, valued at roughly $4.4 million at the time7. Depending on the circumstances, it is possible that not paying could lead to months of service outages and a hindered chance at recovering certain data. Paying doesn’t always guarantee that the result is favourable, but each company has to approach this decision in their own way.

It is recommended that in all cases, victims of ransomware work with an expert firm, like FireEye, and that they also notify the FBI of their situation.

Is Bitcoin or Cash more Anonymous for Criminal Purposes?

When Satoshi Nakamoto’s whitepaper came out, introducing Bitcoin to the world, one of the virtues of the new cryptocurrency widely touted was anonymity. It’s possible that this was truer in Bitcoin’s earlier times than at present—market participants now understand that if being anonymous is the critical desire, other cryptocurrencies may exceed Bitcoin’s capabilities. Experts have indicated that transactions on the blockchain create ‘digital breadcrumbs’ that authorities can then follow8.

In the case of the Colonial Pipeline attack, roughly 64 of the 75 bitcoins were seized by authorities. That means that they were able to trace the specific on-chain activities related to the attack, to find the digital wallet associated with Darkside, and then to obtain the appropriate public and private keys to make the seizure. While the details behind every step of this process have not been publicised, it’s notable that this all happened within about a month of the initial attack and payment9.

Cybersecurity: The Megatrend Everyone Must Consider

Megatrends are being ‘created’ all the time. Some will persist and survive, others will not. Consider a scenario, however, one business is saying that they prefer not to focus on artificial intelligence (AI). We may have our opinions on this statement—but in the end, it may be the case that AI would have only limited value depending on the details. However, now picture a firm saying that they prefer not to focus on cybersecurity, do they have computers? Email? A network? Not focusing on AI could be an interesting debate, whereas not focusing on cybersecurity is a serious business risk. We may not know which services companies will use, but we do know that a lack of focus is irresponsible, possibly even reckless.

It’s important to keep the current landscape in mind:

- Mandiant, a cybersecurity response firm, has reported ransomware response frequency increasing 10 times from 2018 to 202010.
- Mandiant has reported the average demand has been anywhere from $250,000 up to $50 million11.
- Mandiant’s figures indicate that one in ten businesses are forced to close once they are victims of a ransomware attack12.

- Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) is estimated to see global revenues around $217.7 billion by 2023 as cloud computing massively proliferates. However, Worldwide Hybrid Cloud Security Spending is estimated to be at $2.0 billion by 2023. **Don't forget cloud security** is a phrase that comes to mind from this statistic13.

Aligning an investment thesis with the growth of cybersecurity could be a very interesting proposition in 2021.

1 Source: Greenberg, Andy. "The Colonial Pipeline Hack is a New Extreme for Ransomware." WIRED. 8 May 2021.

2 CNBC, as of 8th May 2021

3 Source: Eaton, Collin & Dustin Volz. "U.S. Pipeline Cyberattack Forces Closure." Wall Street Journal. 8 May 2021.

4 Nasdaq, as of 20th June 2021

5 Hay Newman, Lily. "DarkSide Ransomware Hit Colonial Pipeline—and Created an Unholy Mess." WIRED. 10 May 2021.

6 WIRED, 10 May 2021.

7 Source: Eaton, Collin. "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." Wall Street Journal. 19 May 2021.

8 Source: Peroth et al. "Pipeline Investigation Upends Idea that Bitcoin is Untraceable." New York Times. 9 June 2021.

9 New York Times, 9 June 2021.

10 Source: FireEye 2021 Corporate Presentation.

11 Source: FireEye 2021 Corporate Presentation.

12 Source: FireEye 2021 Corporate Presentation

13 Source: Crowdstrike Corporate Overview, March 2021.

Related blogs

+ A rational take on cybersecurity amidst so many threats and attacks

+ Energy prices rise in the wake of Colonial cyberattack

Related products

+ WisdomTree Cybersecurity UCITS ETF – USD Acc (WCBR/CYSE)

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an oer for sale nor a solicitation of an oer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can oen lead to a number of dierent interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public oering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any ailiate, nor any of their respective oicers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.