IF YOU USE A COMPUTER, YOU HAVE TO THINK ABOUT RANSOMWARE

Christopher Gannatti — Head of Research, Europe
06/17/2021

I've started to notice an unfortunate rhythm to the news flow over the course of any given week in 2021: there is usually some sort of report that an entity was hit by a ransomware attack.

If we go back in our minds a few years, ransomware seemed far more "exotic." It existed, but many people and many companies had logical reasons to believe it was far removed from their operations.

In 2021, it's become clear that ransomware can impact any business at any time.

Colonial Pipeline: Ransomware Crosses the Rubicon

We may look back on 2021 and view the Colonial Pipeline attack as the moment that galvanized a coherent U.S. policy and enforcement response to ransomware.

As of this writing, this was the largest single impact on the U.S. energy system that we've seen from a cyberattack, with officials noting that the consequences have a similar feel to a severe hurricane or weather event that causes physical damage[1].

To recap: The Colonial Pipeline is roughly 5,500 miles long and is the largest refined products pipeline in the U.S., supporting about 45% of East Coast fuel consumption. It runs from the Houston, Texas, area on the Gulf Coast up to the New York metro area.

The actual ransomware attack hit Colonial's information technology systems, but as a precautionary measure the firm shut down its operational technology systems because it was uncertain in the early hours how deeply the attack could spread[2].

It is the case today that most ransomware attacks, even if they hit industrial targets, impact information technology systems as opposed to operational technology systems. Ransomware experts are seeing an uptick in the targeting of industrial control systems, but a critical point is that many such targets do not have high connectivity between information technology and operational control. It is not always a simple matter for malware to jump from the IT side to the operational side.

DarkSide: Victim of the Publicity Paradox

Within the ransomware world, anonymity is one of the most-prized assets.

DarkSide, widely viewed as producing the specific malware used in the Colonial Pipeline attack, views ransomware as a business. Cybereason estimates that its malware has been used to compromise more than 40 victims, demanding figures between $200,000 and $2 million in each case. However, the group is not unconcerned with its reputation, declaring publicly that it would not target health care systems, schools or businesses that it believes cannot pay ransoms[3].

During the COVID-19 pandemic, cloud computing and the concept of "Software-as-a-Service" (SaaS) have proliferated. DarkSide is seeking to be a player in "Ransomware-as-a-Service." The organization is offering its software on loan to criminal organizations, and it is actually those organizations that turn around and use the software.[4]

The most profitable, long-run strategy for DarkSide would be to remain in the shadows. A consequence of the Colonial Pipeline attack was the awakening of the fully unified force of the U.S. Justice Department and Biden administration, making "DarkSide" almost a household name. It was even reported that the group would be disbanding as a result of events surrounding this attack.

To Pay or Not to Pay—That Is the Question

To hear the FBI advice, the view is apparently "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 organizations are going to make the effort, they want to ensure the maximum chance that they will receive a payday.

The CEO of the Colonial Pipeline did opt to pay the ransom, which was roughly 75 Bitcoin, valued at the time as roughly $4.4 million.[5] While companies paying ransoms does encourage further ransomware, it is very difficult to make this decision when you are in the position of power or influence at an affected firm. Depending on the circumstances, it is possible that not paying could lead to months of service outages and the utter impossibility of ever recovering certain data.

To be fair, paying doesn't always guarantee a favorable result, but each company has to approach this decision in its own way.

It is recommended that, in all cases, victims of ransomware work with an expert firm of some sort, 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 white paper 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 follow.[6]

In the case of the Colonial Pipeline attack, roughly 64 of the 75 Bitcoin 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 obtain the appropriate public and private keys to make the seizure.

While the details behind every step of this process have not all been publicized, it's notable that this all happened within about a month of the initial attack and payment.[7]

When criminals use cash and international bank accounts, authorities need to go through many layers of lawyers and bureaucracy to make seizures. This can take months or even years depending on the situation. Authorities, duly motivated, do not face such lawyers or such bureaucracies on the blockchain, so seizures may occur faster in certain cases.

Cybersecurity: The Megatrend Everyone Must Consider

Megatrends are being "created" all the time. Some will persist and survive, while others will not.

Consider a scenario, however. One business is saying that it prefers not to focus on artificial intelligence. We may have our own 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 it prefers not to focus on cybersecurity. Does it 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, and 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 2020.
- Mandiant has reported that the average demand has been anywhere from $250,000 to $50 million.[8]
- Mandiant's figures indicate that one in ten businesses is forced to close once it is a victim of a ransomware attack.
- Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) are 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 reach $2.0 billion by 2023. "**Don't forget cloud security**" is a phrase the comes to mind from this statistic.[9]

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

[1]Source: Andy Greenberg, "The Colonial Pipeline Hack is a New Extreme for Ransomware," WIRED, 5/8/21.

[2]Source: Colin Eaton and Dustin Volz, "U.S. Pipeline Cyberattack Forces Closure," Wall Street Journal, 5/8/21.

[3]Source: Lily Hay Newman, "DarkSide Ransomware Hit Colonial Pipeline—and Created an Unholy Mess," WIRED, 5/10/21.

[4]Source: Lily Hay Newman, "DarkSide Ransomware Hit Colonial Pipeline—and Created an Unholy Mess," WIRED, 5/10/21.

[5]Source: Collin Eaton, "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." Wall Street Journal, 5/19/21.

[6]Source: Nicole Perlroth, Erin Griffith and Katie Benner, "Pipeline Investigation Upends Idea That Bitcoin Is Untraceable," The New York Times, 6/9/21.

[7]Source: Nicole Perlroth, Erin Griffith and Katie Benner, "Pipeline Investigation Upends Idea That Bitcoin Is Untraceable," The New York Times, 6/9/21.

[8]FireEye 2021 Corporate Presentation.

[9]Source: CrowdStrike Corporate Overview, March 2021.

Important Risks Related to this Article

There are risks associated with investing, including the possible loss of principal. Crypto assets, such as bitcoin and ether, are complex, generally exhibit extreme price volatility and unpredictability, and should be viewed as highly speculative assets. Crypto assets are frequently referred to as crypto "currencies," but they typically operate without central authority or banks, are not backed by any government or issuing entity (i.e., no right of recourse), have no government or insurance protections, are not legal tender and have limited or no usability as compared to fiat currencies. Federal, state or foreign governments may restrict the use, transfer, exchange and value of crypto assets, and regulation in the U.S. and worldwide is still developing. Crypto asset exchanges and/or settlement facilities may stop operating, permanently shut down or experience issues due to security breaches, fraud, insolvency, market manipulation, market surveillance, KYC/AML (know your customer/anti-money laundering) procedures, noncompliance with applicable rules and regulations, technical glitches, hackers, malware or other reasons, which could negatively impact the price of any cryptocurrency traded on such exchanges or reliant on a settlement facility or otherwise may prevent access or use of the crypto asset. Crypto assets can experience unique events, such as forks or airdrops, which can impact the value and functionality of the crypto asset. Crypto asset transactions are generally irreversible, which means that a crypto asset may be unrecoverable in instances where: (i) it is sent to an incorrect address, (ii) the incorrect amount is sent or (iii) transactions are made fraudulently from an account. A crypto asset may decline in popularity, acceptance or use, thereby impairing its price, and the price of a crypto asset may also be impacted by the transactions of a small number of holders of such crypto asset. Crypto assets may be difficult to value, and valuations, even for the same crypto asset, may differ significantly by pricing source or otherwise be suspect due to market fragmentation, illiquidity, volatility and the potential for manipulation. Crypto assets generally rely on blockchain technology, and blockchain technology is a relatively new and untested technology that operates as a distributed ledger. Blockchain systems could be subject to Internet connectivity disruptions, consensus failures or cybersecurity attacks, and the date or time that you initiate a transaction may be different than when it is recorded on the blockchain. Access to a given blockchain requires an individualized key, which, if compromised, could result in loss due to theft, destruction or inaccessibility. In addition, different crypto assets exhibit different characteristics, use cases and risk profiles. Information provided by WisdomTree regarding digital assets, crypto assets or blockchain networks should not be considered or relied upon as investment or other advice, as a recommendation from WisdomTree, including regarding the use or suitability of any particular digital asset, crypto asset, blockchain network or any particular strategy. WisdomTree is not acting and has not agreed to act in an investment advisory, fiduciary or quasi-fiduciary capacity to any advisor, end client or investor, and has no responsibility in connection therewith, with respect to any digital assets, crypto assets or blockchain networks.

For more investing insights, check out our Economic & Market Outlook

View the online version of this article here.

IMPORTANT INFORMATION

U.S. investors only: Click here to obtain a WisdomTree ETF prospectus which contains investment objectives, risks, charges, expenses, and other information; read and consider carefully before investing.

There are risks involved with investing, including possible loss of principal. Foreign investing involves currency, political and economic risk. Funds focusing on a single country, sector and/or funds that emphasize investments in smaller companies may experience greater price volatility. Investments in emerging markets, currency, fixed income and alternative investments include additional risks. Please see prospectus for discussion of risks.

Past performance is not indicative of future results. This material contains the opinions of the author, which are subject to change, and should not to be considered or interpreted as a recommendation to participate in any particular trading strategy, or deemed to be an offer or sale of any investment product and it should not be relied on as such. There is no guarantee that any strategies discussed will work under all market conditions. This material represents an assessment of the market environment at a specific time and is not intended to be a forecast of future events or a guarantee of future results. This material should not be relied upon as research or investment advice regarding any security in particular. The user of this information assumes the entire risk of any use made of the information provided herein. Neither WisdomTree nor its affiliates, nor Foreside Fund Services, LLC, or its affiliates provide tax or legal advice. Investors seeking tax or legal advice should consult their tax or legal advisor. Unless expressly stated otherwise the opinions, interpretations or findings expressed herein do not necessarily represent the views of WisdomTree or any of its affiliates.

The MSCI information may only be used for your internal use, may not be reproduced or re-disseminated in any form and may not be used as a basis for or component of any financial instruments or products or indexes. None of the MSCI information is intended to constitute investment advice or a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such. Historical data and analysis should not be taken as an indication or guarantee of any future performance analysis, forecast or prediction. The MSCI information is provided on an "as is" basis and the user of this information assumes the entire risk of any use made of this information. MSCI, each of its affiliates and each entity involved in compiling, computing or creating any MSCI information (collectively, the "MSCI Parties") expressly disclaims all warranties. With respect to this information, in no event shall any MSCI Party have any liability for any direct, indirect, special, incidental, punitive, consequential (including loss profits) or any other damages (www.msci.com)

Jonathan Steinberg, Jeremy Schwartz, Rick Harper, Christopher Gannatti, Bradley Krom, Tripp Zimmerman, Michael Barrer, Anita Rausch, Kevin Flanagan, Brendan Loftus, Joseph Tenaglia, Jeff Weniger, Matt Wagner, Alejandro Saltiel, Ryan Krystopowicz, Kara Marciscano, Jianing Wu and Brian Manby are registered representatives of Foreside Fund Services, LLC.

WisdomTree Funds are distributed by Foreside Fund Services, LLC, in the U.S. only.

You cannot invest directly in an index.

DEFINITIONS

Cloud computing : computing capabilities deployed via internet connection in form of applications, platform services, or infrastructure.

Software-as-a-Service (SaaS) : Software applications provided over a network connectio.

Bitcoin (the currency) : A digital currency (also called a cryptocurrency) created in 2009, which is operated by a decentralized authority as opposed to a traditional central bank or monetary authority.

Artificial intelligence : machine analysis and decision-making.

Infrastructure-as-a-service (IaaS) : A type of cloud computing service that offers essential compute, storage, and networking resources on demand, on a pay-as-you-go basis. IaaS is one of the four types of cloud services, along with software as a service (SaaS), platform as a service (PaaS), and serverless.

Platform-as-a-Service (PaaS) : A complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications.