BANK POLICY INSTITUTE

Top 7 Things to Know About Ransomware and Why Criminals Prefer Crypto Payments

Angelena Bradfield and Stephanie Wake | May 12, 2021

The cyberattack on Colonial Pipeline is just the most recent example of ransomware – perpetrated by both criminal groups and nation-state actors – and the potentially massive impact such activity can have on its victims, including individuals, private entities, small businesses, publicly traded companies, non-profits, government agencies, legislative bodies and others. One of BPI's member banks has reported a 334 percent rise in attacks on its clients so far this year. The one constant in all these ransomware attacks appears to be the demand that the ransom be paid in cryptocurrency. Below are seven things to know about ransomware and why cryptocurrency is the preferred method for criminals to receive ransomware payments.

- **Ransomware attacks and the corresponding financial losses they cause are on the rise.** In 2020, the FBI's Internet Crime Complaint Center received 2,474 ransomware complaints resulting in adjusted losses of $29.1 million, a significant increase from the $8.9 million in reported losses in 2019. Most ransomware attacks, however, are not reported, and many go undetected. According to a Chainalysis report on crypto crime, the total amount paid by ransomware victims increased 311 percent in 2020 to reach nearly $350 million in cryptocurrency. It is not uncommon to hear reports of ransom demands measured in the tens of millions of dollars.

- **Ransomware attacks are borderless and many criminals operate from outside the U.S.** Ransomware attacks can be spread globally to computers and operating systems without regard to borders. The identity and location of a ransomware actor are often unknown. Similarly, ransom payments in the form of cryptocurrency can move rapidly across borders as they are not bound by geographic location. Cryptocurrency laundering methods can be used to obfuscate funds' origins, making it difficult for law enforcement to track the source of funds derived from a ransom upon their inevitable reentry to the global banking system. Recently, ransomware actors have been seen switching their demands for payments from Bitcoin to more anonymous and privacy-oriented digital currency, such as Monero, making it even more difficult to trace.

- **Ransomware actors are increasingly operating like businesses.** Many threat actors are now providing Ransomware-as-a-Service, allowing criminals to conduct ransomware attacks with much less technical sophistication. DarkSide, widely believed to be behind the Colonial Pipeline ransomware attack, publicly announced its ransomware campaign and released so-called "ethical principles" related to who it potentially targets. Ransomware has fast become a burgeoning criminal industry, with the goal of inflicting maximum damage on the target so as to encourage swift payment and intimidate future victims.

- **The transparency of payments on cryptocurrency exchanges – and lack of individual transparency – creates an ideal environment for ransomware payments.** Criminals demand ransom payments in cryptocurrency because it is quick, efficient, and they can easily verify if and when payments are made. The payment transparency of public blockchains provides a unique environment for ransomware actors to simply watch the public blockchain to see if the victim has paid. However, depending on the exchange, individuals sending transactions may not be required to identify themselves, and transactions may not be monitored for

suspicious activity reporting to national authorities, like in the traditional banking sector under anti-money laundering (AML) regulatory requirements.

- **While cryptocurrency firms operating in the U.S. are subject to AML requirements, many countries have not formally applied AML expectations to similar entities.** In the U.S., cryptocurrency firms are subject to AML requirements similar to banks, such as Know-Your-Customer expectations and monitoring and reporting for suspicious activity. However, other countries have yet to apply AML expectations to crypto firms, resulting in gaps around the globe relating to crypto regulation and enforcement. There may also be instances where individuals or entities use unhosted crypto wallets (wallets not hosted by a financial institution), which provide them a greater ability to remain anonymous and transact nefariously. A recent public-private sector study highlighted this asymmetry as a key area in need of global attention. In addition, in 2020, the G7 released a ransomware statement calling on other countries to apply international AML standards – particularly those established by the Financial Action Task Force, an intergovernmental body that sets AML-related international standards – to financial services, particularly virtual currencies. The body also committed to "enhanc[ing] its efforts at coordinated responses to ransomware, including where possible information sharing, economic measures, and support for effective implementation of the FATF standards."

- **Law enforcement discourages victims from paying ransomware demands, but does recognize that entities need to consider business continuity and other obligations when deciding whether to pay a ransom.** There is no federal law that prohibits or penalizes a victim for making a ransomware payment. However, the U.S. government does discourage payment by victims of ransomware. Intergovernmental guidance states that "after systems have been compromised, whether to pay a ransom is a serious decision, requiring the evaluation of all options to protect shareholders, employees, and customers." In addition, senior FBI personnel have acknowledged that, depending on the nature of the ransomware, ransomware payments may sometimes be the most practical response to a ransomware event. There is no record of U.S. law enforcement charging a victim of a ransomware attack.

- **Financial Institutions typically only become aware of a ransomware attack when a customer informs them.** Last year, both Treasury's Financial Crimes Enforcement Network and Office of Foreign Assets Control – the bureaus that set AML/CFT and sanctions compliance policy, respectively – released statements relating to ransomware trends and implications for all companies involved in assisting victims in remediating ransomware attacks and processing ransom-related payments, including financial institutions. However, because financial institutions are typically only aware that a payment is related to a ransomware event when informed by their customer, victims may choose not to alert a financial institution to a ransomware payment and "quietly pay off their attackers without notifying the authorities" or by using a third party, such as a crisis management firm, to assist with the payment or otherwise remediate the impacts of the ransomware attack. Ransomware events are also traditionally under reported to law enforcement.

The increase in ransomware attacks underscores the importance of coordination and information sharing between the private and public sectors. Current information sharing mechanisms and opportunities to provide early warnings of potential threats between critical infrastructure and government agencies are woefully inadequate. As a result, critical opportunities to share timely and usable information to prevent and respond to attacks are missed. DOJ recently created a new task force reportedly dedicated to targeting the entire criminal ecosystem around ransomware, including prosecutions, disruptions of ongoing attacks and curbs on services that support the attacks, highlighting the need to unify efforts across the government and devote more resources to intelligence sharing. CISA has launched a 60-day sprint on ransomware, and CISA and the FBI have issued a cybersecurity advisory. However, as gas prices continue to rise on the East Coast following the Colonial Pipeline attack and impacts are felt elsewhere, many people are questioning what can be done to put a stop to the proliferation, and pernicious impact on our country, of ransomware attacks. The government certainly has a role to play, but so does

every owner and operator of our nation's critical infrastructure. Financial institutions have made cybersecurity a priority for decades. It's time other sectors do so as well.

Disclaimer: The views expressed do not necessarily reflect those of the Bank Policy Institute's member banks, and are not intended to be, and should not be construed as, legal advice of any kind.