The Use of Bitcoin and Cryptocurrencies in Ransomware Attacks: Why Employers Should Care

Insights
7.06.21

As ransomware attacks continue to become more of a concern for employers of all sizes, an increasing number of hackers are demanding cryptocurrency such as Bitcoin in exchange for ending their attack. The recent ransomware attacks of Colonial Pipeline Co. and other corporations have shown us that Bitcoin and a familiarity with how to readily access the digital currency may be increasingly important for the modern employer. What do you need to know about this recent trend and why should you care about Bitcoin's role in ransomware cases?

Why the Recent Rise in Attacks?

Employers' reliance on technology increased substantially throughout the pandemic. Indeed, COVID-19 mitigation measures forced companies to utilize remote workforces for an extended time and in ways many never envisioned previously – and the remote work revolution doesn't appear to be ending anytime soon. With the increase of remote work comes an increased exposure for cyberattacks and data breaches, most of which are caused by well-meaning employees who inadvertently put companies at risk. Robust cybersecurity measures should be on the minds of businesses everywhere to prevent phishing, hacking, or ransomware attacks.

What is Ransomware?

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. The FBI has recently reported that the number of ransomware incidents in the U.S. continues to rise, with 2,474 incidents reported in 2020. But the recent high-profile attacks involving Colonial Pipeline and others have brought ransomware to the forefront, highlighting the importance Bitcoin plays in these attacks.

What is Bitcoin?

Bitcoin is the world's first widely adopted cryptocurrency. It allows for secure peer-to-peer transactions on independent computers spread across the globe. Importantly, every Bitcoin transaction is tracked on Bitcoin's blockchain, which is a digital ledger that keeps a record of every transaction ever made using the digital currency. Bitcoin's blockchain is decentralized, which means that there is no single controlling entity and anyone can participate and transact on the ledger.

What Happened?

In the Colonial Pipeline ransomware incident, attackers hijacked the company's network, preventing anyone from using it. The attackers then requested sums of money in exchange for an encryption key to gain access to the networks. Within hours after the attacks, Colonial Pipeline ($4.4 million) paid attackers in Bitcoin.

On June 7, the United States Department of Justice announced that it had recovered 63.7 of the Bitcoins from the Colonial Pipeline ransom paid to the hackers known as DarkSide. And according to the Justice Department, this was the first time a task force devoted to ransomware was able to recover some of the money. The FBI remains tight-lipped on how, exactly, this was done. However, court records show that FBI investigators tracked the publicly visible Bitcoin ledger as hackers transferred the currency to other digital addresses and traced the transactions to a digital wallet, which they seized under court order. Apparently, the FBI was then able to access the wallet using the private key (i.e., a password for the wallet), although it still remains unclear how the FBI retrieved the key.

Even though the Bitcoin blockchain is a digital public ledger that records transactions – meaning that anyone can observe the transaction online – there is a misconception that parties to the transaction can remain fully anonymous. This attack serves as a reminder that Bitcoin is a pseudonymous cryptocurrency, which means that while it provides a basic degree of anonymity, each user is identified by the address of their wallet. Careful analysis of the blockchain can reveal information about both the sender and recipient, which can be used to track transactions.

In short, although tracing a Bitcoin transaction to a specific person is difficult, it is not impossible.

Why Should Employers Care?

When discussing the recovery of the ransomed Bitcoin, the U.S. Deputy Attorney General stressed to businesses that the threat of a severe ransomware attack presents a "clear and present danger to your organization, to your company, your customers, your shareholders and your long-term success."

In a recent FBI Internet Crime Complaint Center (IC3) report, the FBI reported that the IC3 received a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1 billion. According to the report, this represented a 69% increase in total complaints from 2019. And although business e-mail compromise (BEC) schemes continued to be the costliest (19,369 complaints with an adjusted loss of approximately $1.8 billion) with phishing scams the most prominent (241,342 complaints), the number of ransomware incidents in the U.S. continues to rise, with 2,474 incidents reported in 2020 alone.

According to the report, the most common means used in ransomware attacks are:

- email phishing campaigns where the cybercriminal sends an email containing a malicious file or link which deploys malware when clicked by a recipient;
- remote desktop protocol (RDP) vulnerabilities which is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet; and
- software vulnerabilities where attackers take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware.

What Should Employers Do?

As part of any emergency plan to deal with such an attack, you should ensure you have access to individuals or entities (i.e., either specifically trained employees within your organization or third-party service providers) that comprehensively understand blockchain technology and how to access, hold, and transfer cryptocurrency such as Bitcoin. In times of an emergency or crisis resulting from a ransomware or other cyber attack, immediate efforts may prove crucial to your ability to quickly respond to the attack in a way that minimizes the damage – or in the case of Colonial Pipeline, allow you to recover a substantial amount of the ransom.

In addition, other steps you can take to protect your business from falling victim to ransomware and other cyberattacks include:

- Provide robust cyber security training to employees on an annual basis.
- Review security protocols and update them regularly.
- Encrypt data at rest and in transit whenever possible.
- Avoid utilizing local hard drive space.
- Require Two-Factor Authorization to access your internal company network.
- Require employees to set up passwords with multiple characters (including numbers, letters, and symbols) and require that the passwords be routinely changed.
- Create an incident response plan in the event of a cyber attack or compromised system.
- Consider Cyber Insurance.

Conclusion

Regardless of where you stand on the pros and cons of Bitcoin, one thing is clear: there has been widespread adoption of Bitcoin and other cryptocurrencies by retail investors, financial institutions, and companies such as Tesla, Paypal and JP Morgan over the past 18 months. It is unlikely Bitcoin disappears anytime soon, and in fact many contend that widespread acceptance and utilization of cryptocurrencies such as Bitcoin is inevitable. As a result, you need to develop a plan and be prepared for the variety of new issues that can result as Bitcoin and other cryptocurrencies continue to become more prevalent.

We'll continue to monitor developments in this area, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have any questions about how this decision may impact your business, please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Cryptocurrency and Blockchain Taskforce.

Related People

Patrick W. Dennison
Partner
412.822.6627
Email

Phillip C. Bauknight
Partner
908.516.1059
Email

Service Focus

Privacy and Cyber

Industry Focus

Healthcare