MARSH

Ransomware: Paying Cyber Extortion Demands in Cryptocurrency

One of the most common and serious cyber-attacks involves ransomware, in which a threat actor locks an organization's data with encryption until a ransom demand is met. These attacks are increasing not only in number, but also in severity. In the first half of 2020, average ransomware payments increased by **60%**, with bitcoin used for most payments.

Bitcoin accounts for approximately **98%** of ransomware payments. Whether an organization pays the ransom or attempts to recover the data independently, a clear understanding of bitcoin is essential for cyber incident response planning.

Why Bitcoin?

Anonymity. Speed. Access.

Bitcoin, like other cryptocurrencies, allows cybercriminals to receive funds with a high degree of anonymity, making transactions difficult to track. Bitcoin gained notoriety as the common currency of the Dark Web, where it remains popular. It is seen as the essential cryptocurrency — easy to acquire and use, making threat actors believe victims will be more likely to pay.

Occasionally, cyber threat actors demand other cryptocurrencies, such as Monero and Zcash. These have additional privacy features that make tracking payees more difficult, but are the exceptions to the rule.

How Payment Works

Organizations should be aware that arranging a cryptocurrency payment may take more time than expected. It is advisable to have payment arrangements pre-established in your **cyber incident response plan**. Prior arrangements can speed up and expedite recovery. If a ransomware payment is permissible, your external counsel or cyber forensic provider should manage the cryptocurrency transaction, including ensuring compliance with **OFAC** or other regulatory guidance related to ransomware payments.

In terms of the process itself, a cryptocurrency transaction consists of a payer sending funds to a payee, with both parties identified only by an account number or address. To purchase and send bitcoin, payers use either a bitcoin wallet or bitcoin ATM.

While bitcoin operates on a public blockchain that allows anyone to see all bitcoin transactions, there is no direct way to determine the account owner.

Can Cyber Criminals be Traced?

Law enforcement, private sector companies, and service providers have teamed up to develop approaches to trace bitcoin transactions. These approaches combine multiple data sources (including social media activity) and analytics to identify transaction patterns that sometimes make it possible to determine individual identities.

Cyber criminals, however, use obfuscation techniques to increase anonymity and avoid detection. One common approach is "mixing," in which a service provider mixes the funds of different users to break the traceable trail of transactions, making it unlikely they will be caught.

What You Can Do?

With ransomware attacks increasing, organizations need to be prepared well in advance. Effective data backups are critical. And it's important to update your incident response plans to account specifically for ransomware.

To learn more about what organizations can do before, during, and after a ransomware attack, see **Ransomware: Remove Response Paralysis with a Comprehensive Incident Response Plan**.

For more information and other solutions from Marsh, visit marsh.com, or contact your local Marsh representative.

JIM HOLTZCLAW
Senior Vice President, Cyber Risk Consulting, Marsh Advisory
+1 202 297 9351
james.holtzclaw@marsh.com

REID SAWYER
Practice Leader, US Cyber Risk Consulting, Marsh Advisory
+1 630 442 3506
reid.sawyer@marsh.com