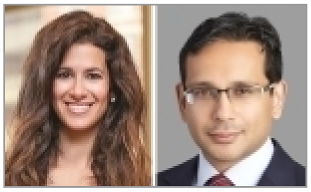
THE LAWYER'S DAILY

The Lawyer's Daily | 111 Gordon Baker Road, Suite 900 | Toronto, ON M2H 3R1 | www.thelawyersdaily.ca
Phone: (800) 668-6481 | Fax: (905) 479-3758 | John.Carson@lexisnexis.ca

In-House Counsel

Cryptocurrency and cybersecurity: The implications

By **Sharon Bauer and Imran Ahmad**



Sharon Bauer and Imran Ahmad

(November 30, 2017, 8:32 AM EST) -- This is part two of a two-part series.

Similar to the way money is stored in a bank, cryptocurrency can be stored in forms of "cryptocurrency wallets" where sensitive information is encrypted and securely stored. If an owner of a bitcoin uses an online wallet, also known as an "exchange," the exchange provider stores the encrypted information on behalf of the owner. This is arguably the most popular way to store cryptocurrency.

Exchanges

Despite this popular method of storing cryptocurrency, exchanges are considered the weakest link in the cryptocurrency ecosystem. Exchanges are managed by third parties and are counterintuitive to the decentralized nature of cryptocurrency. There are several examples of exchanges being hacked by cyber criminals, a modern day bank robbery.

The most infamous exchange hack targeted the high-profile Mt. Gox exchange. At the time, Mt. Gox was the largest bitcoin exchange. In 2014, Mt. Gox was reportedly hacked, and almost 25,000 customers lost approximately 650,000 bitcoins which, at the time, equalled to approximately $400 million. Users whose bitcoins were stolen have no means of recovering their stolen property. Exchanges are largely uninsured and unregulated. Due to cryptocurrency's anonymity and encryption, it is nearly impossible to trace the thieves or recover the currency.

Owners of cryptocurrencies that store them on exchange should carefully read the terms of service, which may expressly state that the exchange is not liable should a hack or viral attack occur. In such cases, no recourse could be sought nor could the exchange company be held accountable.

There are alternatives to storing cryptocurrency on exchanges. Cryptocurrency can also be stored in hardware wallets that are not connected to a network and therefore cannot be hacked. If cryptocurrency is saved locally in a hardware wallet, it is imperative that the hardware itself is not lost or compromised as it contains the key to the cryptocurrency. Put simply, if the hardware is lost, so is the cryptocurrency.

Social engineering attacks

When cryptocurrency is connected to a network, a hacker can gain access using a social engineering attack. Having a plethora of information at their fingertips through social media, a malicious party can obtain a target's e-mail address and mobile number. The hacker then contacts the victim's mobile service provider and ports the victim's number to the hacker's device. Since most e-mail servers provide a phone number as a backup access option, the hacker can have the password sent to their mobile device and easily gain access into the victim's e-mail account. The hacker can then gain access into an exchange using a two-factor authentication and move the victim's cryptocurrency to the hacker's own digital wallet. The cryptocurrency can then be converted to various other types of cryptocurrencies and eventually converted into money, making it nearly impossible to trace the hacker or recover the lost currency.

In order to prevent this from happening, cryptocurrency users are encouraged to assign their mobile devices to "do not port" with their mobile service providers. Users should not use text message two-factor authentication.

Ransomware

Cryptocurrency’s anonymity has driven the recent increase in ransomware attacks. WannaCry and Petya are two recent ransomware attacks that have garnered much attention on a global scale.

With ransomware, an organization may find that malicious software has taken over its computer system and encrypted its data, which has caused the organization’s activities to come to a halt. In order to decode the data and regain control over its system, the organization must pay a ransom.

Previously, there were ways to potentially track the ransom money, for example if it was wired or if dollar bills were stamped. However, ransoms paid in cryptocurrency can quickly and easily be converted into other forms of cryptocurrencies and, eventually, into cash. All of this can be done without leaving an identifiable trail.

As ransomware continues to rise, organizations need to be proactive and develop a response plan in advance of such an event. All data should be regularly encrypted and backed up. Organizations would be well-advised to investigate whether their cyber insurance policy covers incidents of ransomware and the scope of that coverage, which may or may not include coverage of the cryptocurrency ransom, business interruptions and legal costs.

Hacking for the purpose of mining

A relatively new type of cryptocurrency hacking involves a hacker hijacking an electronic device for the purpose of using its processing power to mine a cryptocurrency. This is referred to as “cryptojacking.”

To highjack a device, hackers compromise a website by installing malware on it. Users of that site unknowingly download cryptocurrency mining software. Once the software is installed on that user’s electronic device, the hacker then uses that device’s processing power to mine cryptocurrency. Some websites are unaware of the malware distributed through their website. Other sites purposely allow this malware to be installed so they can share in the profit of the mined cryptocurrency, instead of relying solely on revenue generating ads.

Conclusion

Cryptocurrency provides a depth of security that traditional currency cannot. However, the anonymity and encryption that makes cryptocurrency so appealing can be used against the user and to the benefit of a new age robber.

While the security of cryptocurrencies has been heavily promoted, the real security threats lay in the broader ecosystem which can be compromised by cybercriminals.

Accordingly, organizations owning or engaging in the trade of cryptocurrencies should have a clear understanding of the ecosystem and understand their vulnerabilities so that they can implement appropriate risk mitigation strategies.

Sharon Bauer is a partner at Wolfe Lawyers *and can be reached at* sbauer@wolfelawyers.com. *Imran Ahmad is a partner and national leader of the cybersecurity law practice at* Miller Thomson LLP *and can be reached at* iahmad@millerthomson.com.

Photo credit / derrrek ISTOCKPHOTO.COM