BIZCOMMUNITY

# The growing menace of cryptocurrency exchange hacks

By Simon McCollough

29 Mar 2019

There are many reasons cryptocurrencies are inherently attractive to hackers. One of the biggest reasons is a lack of heavy regulation compared with the traditional financial industry. There simply aren't as many stringent, mandatory technical and administrative protection measures in place.

Simon McCollough is major channel account manager, F5 Networks

Security can be lax, and there are more fly-by-night operators. Worst of all, it is very difficult to reverse cryptocurrency transactions. Some cryptocurrency exchanges cover customer losses but the door is often closed when figures stretch into the millions.

F5 Labs looked at the last seven years of major cryptocurrency thefts. Seventy-three major incidents were identified. In 2011, Bitcoin had parity with the US dollar. Today, and despite significant fluctuations, it is worth around $3,5k. At the same time, we have witnessed an almost twelve-thousand-fold increase in crypto thefts. Over the past seven years of cryptocurrency data thefts, F5 Labs found that the average take on an incident was around $31m.

## Who is being hacked?

There are many technological services in the cryptocurrency industry, all of which are targets for cybercriminals. The most commonly hit technical services, according to F5 Labs research, are cryptocurrency exchanges (63% of incidents). These exchanges are the digital equivalent of currency exchanges. These sites enable customers to buy or sell various cryptocurrencies, making them a nexus for high value transactions.

Cryptocurrency uses storage mechanisms called wallets, and there are two kinds. A “hot wallet” is internet-connected and used to store cryptocurrencies used for day-to-day transactions. It is basically the equivalent of your real-life wallet. Hot wallets can run on cryptocurrency exchanges for easy trading, but they can also run as client software on a computer or mobile device. As a result, hot wallets are more likely stolen by cyber-criminals.

How safe is cryptocurrency investment?

5 Mar 2019

To reduce the risk, cryptocurrency technology also leverages “cold wallets” that are not connected online. The best cold wallets are air-gapped systems, such as a USB stick with a strong password. Within cryptocurrency exchanges, cold wallets exist as separate, strongly-encrypted databases requiring a wallet owner to unlock it with a private key. Of the known attacked technologies, hot wallets within exchanges are ripped off three times as much as cold wallets. Wallet software for clients that is outside of an exchange can also be attacked. These incidents currently represent around one-seventh of all cryptocurrency thefts.

Mining services are another potentially hackable cryptocurrency technology, although this is a relatively rare occurrence.

## Where to next?

Applications are complex conglomerations of interacting services in a variety of environments, glued together with APIs, authentication credentials, and networks. This means they have an extensive attack surface and therefore need extensive security testing and protection.

Governments around the world are finally starting to regulate the cryptocurrency industry, and some have already begun defining cybersecurity measures. Korea Regulation 5.5.7 (Regulation on Supervision of Electronic Finance) is being looked at as one of the leaders in this respect, as it treats cryptocurrency exchange cybersecurity measures the way a financial institution would. Hopefully, we’ll start to see other governments follow suit soon.

## ABOUT THE AUTHOR

Simon McCollough is major channel account manager, F5 Networks