SUMMER 2018 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss cryptocurrency hacking events, as well as the regulatory and legal climate for blockchain and cryptocurrency technologies.

Cryptocurrency Hackers Exploit Bugs in Code and Steal Currency

There's a tradition among Navajo rug weavers that a mistake should be woven into every rug because perfection is only attainable by the creator, and by creator, the Navajo mean a divine entity. Positing that this Navajo belief has been adopted by blockchain code authors would be ludicrous, as the goal of creating immutable decentralized ledger technology is to create a flawless code, thus eliminating the need to correct errors. However, to cryptocurrency hackers, defeating flawless code is just the challenge they're looking for, and, in some very notable cases, challenges they've won. Like a rug connoisseur inspecting row by row a piece of woven art, hackers have meticulously combed lines of blockchain code looking for that one critical, albeit miniscule, error. Cryptocurrency hacks have been responsible for losses valued in the hundreds of millions, and for what are considered some fairly hardline responses to those who believe that blockchain code is the law where cryptocurrency is concerned. In this article, we'll look at some of significant cryptocurrency hacks since 2010.

Bringing Down a Mountain

At one point, cryptocurrency exchange Mt. Gox was handling 70% of all bitcoin exchanges. Not bad for a little site that started as a trading card exchange for a fantasy-based card game. Unfortunately, Mt. Gox became a cautionary tale for developers who don't believe in peer review, and the exchange experienced a series of hacks and mysterious losses. In February 2014, the mountain began to crumble.

On February 7, 2014, Mt. Gox halted bitcoin withdrawals in order "to obtain a clear technical view of the currency processes". (https://www.bloomberg.com/news/articles/2014-02-07/bitcoin-price-falls-as-mt-gox-exchange-halts-activity) By February 24, 2017, after more than 3 weeks of statements assuring customers that Mt. Gox was reviewing and addressing security concerns, the trading portal's webpage went dark, and a memo was leaked indicating that almost 750,000

bitcoins had been stolen through years of undetected theft. The landslide that followed would take down the largest bitcoin exchange at the time, lead to bankruptcy filings in two countries, culminate with the arrest of Mt. Gox CEO Mark Karpelès, and accumulate losses of almost $500 million worth of bitcoin, and eventually, assets worth over $2.4 trillion. On June 22, 2018, the attorney for the Japanese bankruptcy proceedings announced a schedule to begin receiving claims from Mt. Gox customers who lost money through the theft on the exchange with the goal of paying claims through recovered assets. Mt. Gox, however, has been leveled and is now defunct.

A Hack Leads to a Classic

The DAO, a Decentralized Autonomous Organization, was a blockchain-based organization operating on the Ethereum blockchain, and looked to sell DAO tokens to investors, which in turn would be used to fund projects that would generate profits for token holders. According to a Section 21(a) report by the Securities and Exchange Commission, "After DAO Tokens were sold, but before The DAO was able to commence funding projects, an attacker used a flaw in The DAO's code to steal approximately one-third of The DAO's assets." (https://www.sec.gov/litigation/investreport/34-81207.pdf) The loss was approximately 3.6 million Ether, worth approximately $60 million at the time of the attack. The hack took an interesting turn when "white hat" hackers moved the remaining assets to protect them from the "black hat" hackers.

The cure proposed to correct the vulnerability exposed by the hack was a "hard fork" which would restore the lost assets as if the hack had not occurred. A hard fork is a change in the processing of a blockchain which creates a new set of transaction links operating according to a revised code. To some, a hard fork contradicts the idea that blockchain is immutable technology, and there was a group of Ethereum members who did not embrace the idea of restoring DAO assets through a hard fork. In response, the original Ethereum blockchain was renamed "Ethereum Classic," and continued processing transactions accordingly, while the Ethereum blockchain is actually the hard-forked branch of the original.

The Mother of All Hacks – So Far

At 3:00 am local time on January 26, 2018, the Coincheck cryptocurrency exchange in Japan became the victim of the largest single hack in cryptocurrency to date, with losses of approximately $530 million. The method: hackers attacked Coincheck's "hot wallet" where the exchange stored coins, pickpocketing the exchange stealing the private key. Suspicions were raised, but never confirmed, that Coincheck insiders were involved, and to date, no official allegation of embezzlement has been issued by the Japanese investigators.

Criticism of Coincheck's decision not to use a "multisig wallet," led to analysts categorizing the hack as an error of corporate management, not a vulnerability of blockchain technology. A hot wallet requires one key to process a transaction. That key belongs to the wallet sending the coins. The recipient's key is not required in order to have coins deposited in their wallet. This is the original wallet design for blockchain cryptocurrency technology, the benefit of which is that there is no unrelated, third party holding a key, increasing privacy. A multiple signature, or multisig, wallet requires two of two, two of three, or even three of three keys to be verified before a transaction can occur. The third key is held by a third party, a departure from the original cryptocurrency wallet concept, but has the effect of increasing security. Multisig wallets came as a response to security concerns from entities who didn't want a single person in control of all cryptocurrency transactions for their organization, those who wanted a way to recover lost keys not available with hot wallets, and, those who worried that hot wallets were simply not secure

enough in the face of skilled hackers. Coincheck just may have proved them correct.

Unlike Mt. Gox, Coincheck survived its hack attack, and by March 2018 announced plans to reimburse losses, correct security concerns, and resume partial trading. In late April 2018, the sale of Coincheck to Japanese firm Monex was announced, which promised to lend stability to the exchange.

Cryptocurrency hacks are often used by pessimistic pundits to call attention to the vulnerability of the blockchain technology, and cryptocurrency in general, because of imperfect code. The flaw in that logic is that if we look at any aspect of the financial and banking industries, we can find hacks that exposed weaknesses in the nascent systems employed to modernize banking, investing, trading, and other associated transactions – and in fact, as recently as May 29, 2018, two Canadian banks were hacked, exposing 9,000 accounts to hackers. The idea that cryptocurrency is an invalid medium for exchange and investment because skilled hackers are determined to scrutinize code until they expose even the smallest weakness is akin to saying the minor flaws in Navajo rugs render them worthless trinkets. While the woven irregularities of Navajo rugs have an intentionality that bugs in code do not, the fact that there are ongoing efforts to create an increasingly perfect blockchain technology should reassure us. And as far as we know, there are no divine hackers.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

MASTERS CONFERENCE
New York, NY: July 24, 2018

BLACK HAT USA
Las Vegas, NV: August 04-09, 2018

ILTACON 2018
Washington, DC: August 19-23, 2018

HTCIA INTERNATIONAL 2018 CONFERENCE AND TRAINING EXPO
Washington, DC: August 19-22, 2018

TODAY'S GENERAL COUNSEL, "THE EXCHANGE" EDISCOVERY
Seattle, WA: September 1, 2018

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: