CRYPTO SECURITY REPORT

JANUARY 2019

BitIRA

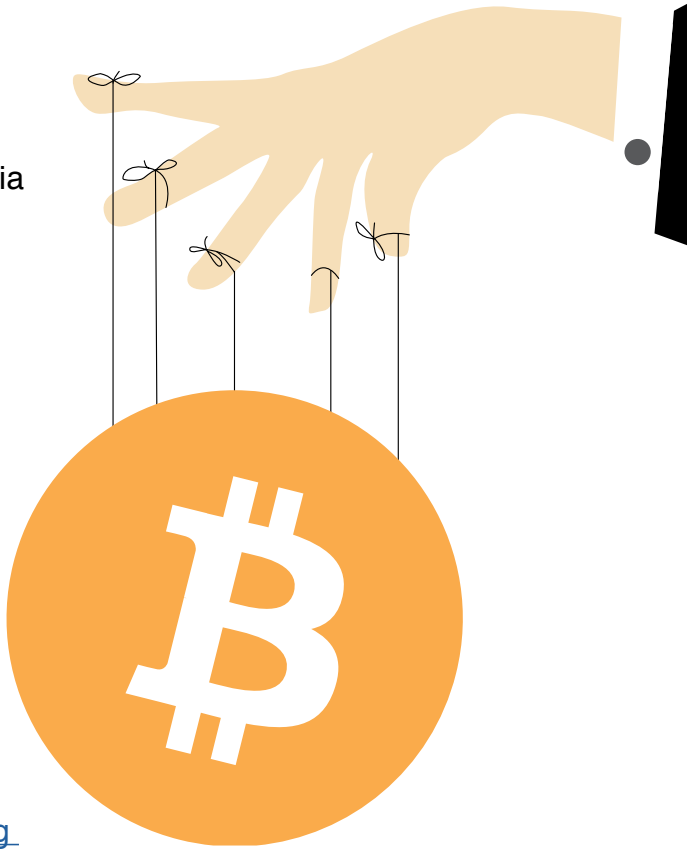
Hackers Target High-Profile Companies

There has been a spate of attacks in the past couple of months against well-known organizations by crypto scammers. In November, the official Twitter account of Target was hacked, and a Bitcoin scam message was tweeted out. A day or so later, an official Twitter account of Google was also seized by scammers, who sent out a similar sham tweet. These are some of the biggest companies that have been successfully breached by crypto scammers to date.

Also in November, a ubiquitous web analytics website, StatCounter, was hacked to exploit a vulnerability and gain access to the cryptocurrency exchange, Gate.io. The injected malicious script replaced users' bitcoin address with one used by the hackers. An unknown amount of BTC was stolen in this way.

Perhaps stooping to a new low, hackers in December targeted the Make-A-Wish Foundation website. Taking advantage of increased traffic to the charity during the holiday season, the hackers installed cryptojacking malware that illegally mined Monero using visitors' computers.

“ICOs Are Dead”. What’s the Next Move for Regulators?



According to TokenData, total capital raised by ICOs each month has plummeted by over 90% since early 2018. Undoubtedly, the crypto bear market for most of 2018 had a large part to play in pushing out scam ICOs preying on naïve investors drawn in by the media buzz about Bitcoin. But some analysts also argue that increased regulations have had a large role in disincentivizing the creation of productive ICOs.

It’s hard to fault regulators for wanting to curb the harmful, speculative aspects of ICOs. Indeed, a Wall Street Journal research study in December showed that 15% of crypto ICOs are still highly questionable. But there’s very likely even more regulation of initial coin offerings by government agencies to come. The courts are also moving forward with prosecution of scammers, with an important federal case in November of Maksim Zaslavskiy setting a precedent that ICOs are subject to securities laws.

In November, the Securities and Exchange Commission (SEC) announced that they’re expanding their crackdown on crypto fraud. Analysts suggest that this next phase for the agency will see it employ a “guidance by enforcement” strategy. Rather than creating a clear set of rules for cryptocurrency (which may be challenged extensively in court), the agency is prosecuting crypto fraud on a case-by-case basis. In the short term, this approach may be frustrating for industry.

In early December, an Under Secretary at the U.S. Treasury called on crypto industry leaders and regulators worldwide to help the United States curb money laundering and financing of terrorism in the cryptocurrency space. In some cases, the private sector is responsive to such efforts. In November, for instance, Nasdaq announced that it had developed tools to help combat fraud on crypto exchanges.

But when does regulation of virtual currencies begin to defeat the fundamental ideal of freedom behind Bitcoin? For instance, the U.S. Department of Homeland Security (DHS) announced in late November that it intends to track privacy-focused coins, such as Zcash. Time will tell whether a balance will be struck between the blockchain ideals of a decade ago and the realities of regulation today.

Evolving Malware and Brazen Scammers

Cybersecurity researchers had observed in late November that a new type of crypto mining malware was using a kind of AI to "evolve" its code so that it can remain undetected. In December, it was also reported that Vertcoin, a well-respected altcoin, experienced a dreaded "51% attack". In such an attack, hackers concentrate a large amount of computing resources to overwhelm the blockchain network and force malicious changes to the ledger. Not all coins are equally vulnerable to such attacks, but Vertcoin's ordeal in late 2018 serves as a cautionary tale for the crypto industry.

Crypto scammers' strategies are shifting in other ways, as well. North Korea, one of the main sources of crypto hacking, has begun to target individuals who hold large amounts of virtual currencies, rather than crypto exchanges and financial institutions. In the U.S., some Bitcoin scammers emailed bomb threats in December to various businesses, schools, and other places, prompting evacuations from those locations across the country. Such brazen attacks may increase government scrutiny of the cryptocurrency industry even further.

Nevertheless, as we enter a new year and Bitcoin begins its second decade of existence, many crypto bulls remain optimistic that the "rude awakening" of 2018 was actually a good thing for the industry, which may yet show its true potential.