

The New Gold Rush

Cryptocurrencies are the New Frontier of Fraud



Table of Contents

The New Gold Rush.....	2
Year of the Doge: Will 2018 Be the Year that AltCoins Challenge Bitcoin's Monopoly?	3
Living without AlphaBay: Declining Trust in the Criminal Ecosystem	4
Milking the Masses: Fraud Schemes Targeting Cryptocurrency Holders	5
1. Criminals targeting funds in user accounts	5
2. Criminals mining their own business.....	9
3. Criminals targeting Initial Coin Offerings	15
Forecasting Cryptocurrency Fraud	20
Protecting Yourself Against Cryptocurrency Fraud	22

In the mid-nineteenth century, the promise of gold inspired over 300,000 people to make the journey to California in the hope of striking it rich. Although gold mining itself was fruitless for most, some were able to amass large fortunes, including cunning opportunists who jumped at the chance to defraud desperate 49ers by selling synthetic gold deposits or fake mines of no real value.

Today, a similar situation has emerged. With over 1,442 cryptocurrencies in circulation, and new alternative coins – “altcoins” – emerging every week, cybercriminals have developed several schemes to defraud those looking to profit from the growth in cryptocurrencies. This paper highlights the most common methods used by these criminal actors, including account takeovers, mining fraud, and scams against initial coin offerings (ICOs). It also includes measures that organizations, consumers, and exchanges can adopt to stay protected.

With a deeper understanding of these issues, we can begin to address important questions about the outlook for digital currencies, including: If individuals lose trust in alternative coins and no longer see them as profitable, then what does this mean for the future of cryptocurrencies? How will the cryptocurrency landscape change in 2018? And will cryptocurrency fraud ultimately obstruct the rapid growth of digital currencies worldwide?

Cryptocurrency Fraud



Account Takeover

Phishing
Credential Stuffing



Mining Fraud

Botnets
Crypto Jacking



Initial Coin
Offering Fraud

Exit Scams
Pump and Dump

Year of the Doge: Will 2018 Be the Year that AltCoins Challenge Bitcoin's Monopoly?

It is routine for cybercriminals to pay for their goods and services with digital currencies, and has been for some time. Perfect Money, Yandex Coin, and Qiwi, for example, are some of the most popular digital currencies across Russian language criminal forums and marketplaces. Faced with the threat of law enforcement interference, criminals have sought to further obfuscate the links between their real-world personas and their earnings and new currencies have emerged.

The obvious leader in the cryptocurrency space is Bitcoin, a coin that rose in value from \$998 to \$13,860 between January 1 and December 31, 2017.¹ At its peak on December 16, the value of one bitcoin reached \$19,343. Despite these astronomical figures, it is alternative coins – or “altcoins” – that are behind the cryptocurrency market's greatest transformation. Challengers to Bitcoin, including Monero, Zcash, and Ethereum, emerged as real contenders in 2017. Many of these innovative altcoins offer new functionality that speak to the concerns of Bitcoin's governance model, difficulty of mining, and lack of anonymity of transactions. These difficulties are some of the reasons that Stripe has recently stopped supporting Bitcoin, claiming it is more of an asset to be traded than a payment method.²

Of course, not all these “altcoins” should be taken at face value. Nothing encapsulates the transformation of the altcoin market more than the rise of Dogecoin. Dogecoin was originally developed as a joke cryptocurrency in 2013,³ but it has emerged as a lucrative, tradeable commodity. Dogecoin reached \$2 billion in market capitalization in January, before losing half its value in a couple of weeks. This volatile price fluctuation is indicative of the extreme speculation that exists in the cryptocurrency market.

CURRENCY	PERCENTAGE OF MENTIONS SO FAR IN 2018
BITCOIN	63%
ETHEREUM	18%
LITECOIN	7%
ZCASH	6%
RIPPLE	3%
MONERO	2%
DASH	1%

Figure 1: Mentions of cryptocurrencies on criminal forums in 2018

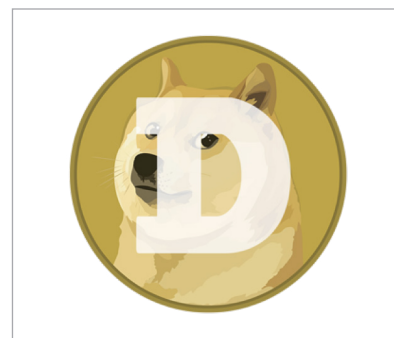


Figure 2: The Dogecoin logo

¹ <https://www.coindesk.com/price/>

² <http://www.bbc.com/news/business-42798935>

³ https://motherboard.vice.com/en_us/article/9kng57/dogecoin-my-joke-cryptocurrency-hit-2-billion-jackson-palmer-opinion

Living without AlphaBay: Declining Trust in the Criminal Ecosystem

The appeal of cryptocurrencies to cybercriminals is closely tied to the importance of trust – a precious and diminishing commodity within the criminal ecosystem.

The seizure of AlphaBay and Hansa marketplaces in July 2017 was a shock to the English-speaking cybercriminal community.⁴ Since their demise, cybercriminals have become more nervous and have sought new ways to conduct business with less risk.⁵ One such example is Tralfamadore, a marketplace based on Ethereum blockchain. All transactions are made using the Ether cryptocurrency and are recorded as smart contracts on the blockchain. This addresses problems with user trust — if all transactions are permanently and immutably recorded, vendors who attempt to scam other users can be more easily identified. Furthermore, platform operators have no control over listings and the platform is split among many nodes, making it highly resilient to law enforcement takedowns or attacks by other criminal actors.

Even during their peak, AlphaBay and Hansa appreciated the need for trust. This is why AlphaBay already offered Monero at the time it was seized and was even rumored to be incorporating Zcash as well.

With more cryptocurrencies in circulation, cybercriminals can hope to achieve even better anonymity, particularly with currencies like Monero, Dash and Zcash. As one Europol reported stated:⁶ “Cryptocurrencies continue to be exploited by cybercriminals, with Bitcoin being the currency of choice in criminal markets, and as payment for cyber-related extortion attempts, such as from ransomware or a DDoS attack. However, other cryptocurrencies such as Monero, Ethereum, and Zcash are gaining popularity within the digital underground.”

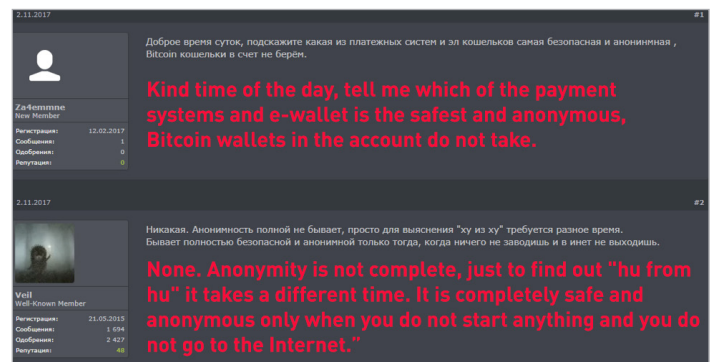


Figure 3: Russian language cybercriminals discussing anonymity and online currencies in November 2017.

Cybercriminals, however, are not naïve enough to believe that cryptocurrencies alone will keep them secure. In November 2017, when one Russian language forum user asked, “which of the payment systems and e-wallet is the safest and anonymous,” the first response he received was “it is completely safe and anonymous only when you do not start anything and you do not go to the Internet.” Although their response was facetious, the point is that while cryptocurrencies may offer increased anonymity, online users still need to take extra measures to maintain good operational security.

⁴ <https://www.digitalshadows.com/blog-and-research/alphabay-disappears-three-scenarios-to-look-for-next/>

⁵ <https://www.digitalshadows.com/blog-and-research/the-future-of-marketplaces-forecasting-the-decentralized-model/>

⁶ <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>

Milking the Masses: Fraud Schemes Targeting Cryptocurrency Holders

Although the crisis in confidence in the cybercriminal ecosystem has partly led to the rise of several new cryptocurrencies, this has also had the adverse effect of encouraging increasing amounts of fraud against cryptocurrency holders. Essentially, with more cryptocurrencies in circulation, and with more users adopting them, the opportunities for cybercriminal activity increases. The growing interest in cryptocurrencies means that account takeovers, mining fraud, and Initial Coin Offering (ICO) scams are all opportunities for cybercriminals to profit.

1. Criminals targeting funds in user accounts

A combination of Bitcoin's price hike and increased speculation of cryptocurrencies means that there are more online accounts available with a lot more money in them. This makes the accounts of exchanges and trading platforms particularly attractive targets for criminals.

Criminals frequently sell access to cryptocurrency exchange accounts online, including on criminal forums (Figure 4) and on paste sites (Figures 5 and 6).

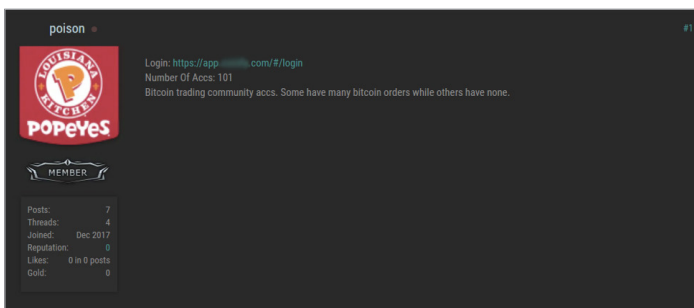


Figure 4: Over 100 user accounts offered on a criminal forum in January 2018

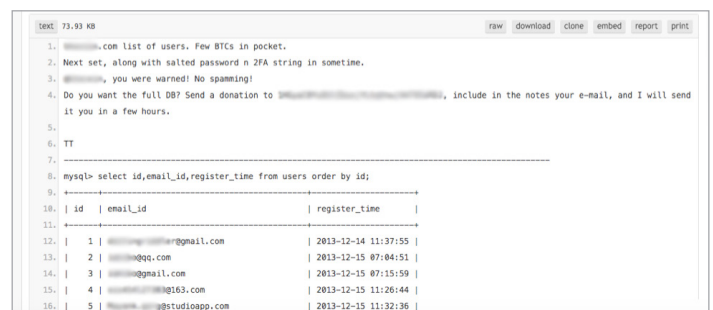


Figure 5: A claim of breach for another cryptocurrency exchange, alongside a sample of the data, from December 2017

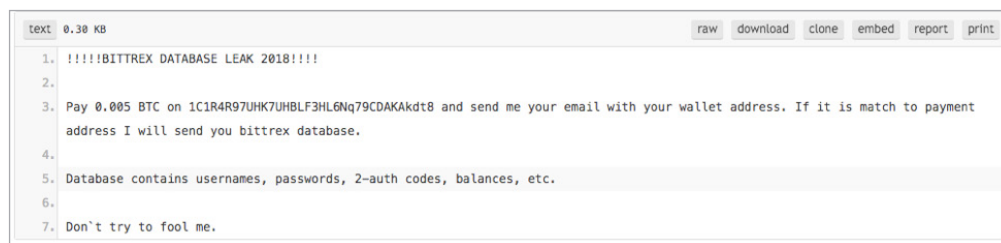


Figure 6: Another claim of a database leak, this time for the Bittrex exchange, from January 2018

Not all these claims will be legitimate, and many simply seek to capitalize on the interest in cryptocurrencies by tricking cybercriminals who are looking to gain access to user accounts. Yet for those whose claims are genuine, there are two common ways of targeting exchanges and trading platforms to obtain customer details: phishing and credential stuffing.

Phishing and credential harvesting

It is estimated that over \$225 million in cryptocurrencies were lost to phishing in 2017.⁷ Figure 7 shows a video demonstration of a Blockchain scam page provided by a cybercriminal. The scam page captured the victims' usernames and passwords and then directed them to the official Blockchain site to avoid arousing suspicion. The file shared by the YouTube video owner had been downloaded over 1,200 times.

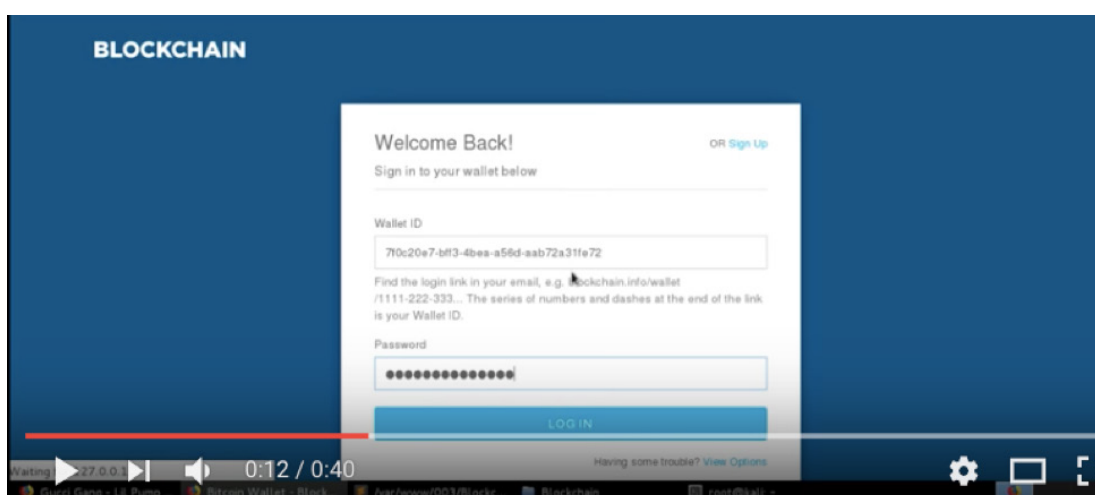


Figure 7: Blockchain[.]info phishing templates shared online

In another example, phishing emails were sent to users of the online Ethereum wallet site Myetherwallet.com. The email claimed that Myetherwallet.com had published a new update for its customers and encouraged email recipients to click on a link that took them to an impersonation of the legitimate Myetherwallet.com site. The phishing site, however, used a Unicode typosquatting technique to imitate the official domain. In Figure 8 below, you can see that the Latin character “T” was replaced with a T-comma (ț) — a letter from the Romanian alphabet. Unsuspecting victims then entered their wallet passwords into the site, which allowed the attackers to access their wallets and steal coins. Researchers investigating this phishing campaign found that over \$15,000 had been transferred into the attackers' wallets in under two hours.⁸

⁷ <http://fortune.com/2017/08/28/ethereum-cryptocurrency-stolen-bitcoin/>

⁸ <https://www.bleepingcomputer.com/news/security/ethereum-phishing-attack-nets-criminals-15k-in-two-hours/>

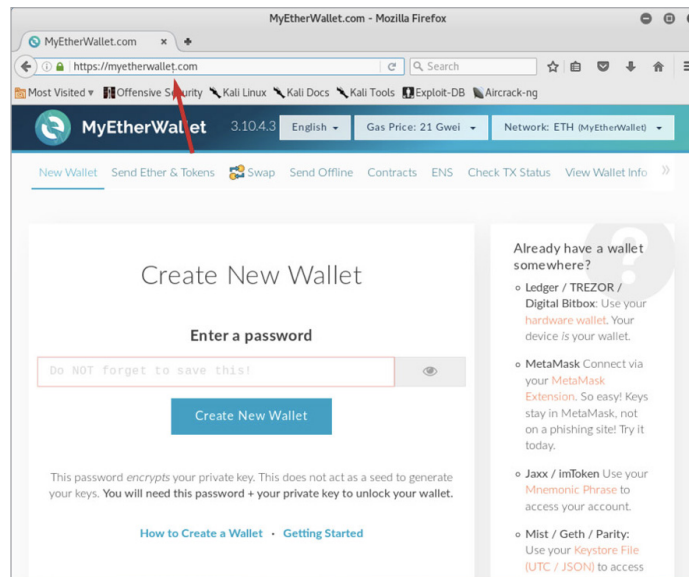


Figure 8: Myetherwallet.com phishing site. Source: dearbytes.com

However, there is more to phishing than typosquatted pages; social media is a breeding ground for scams. Spoof profiles are created to imitate exchanges, attempting to trick customers into disclosing their credentials.

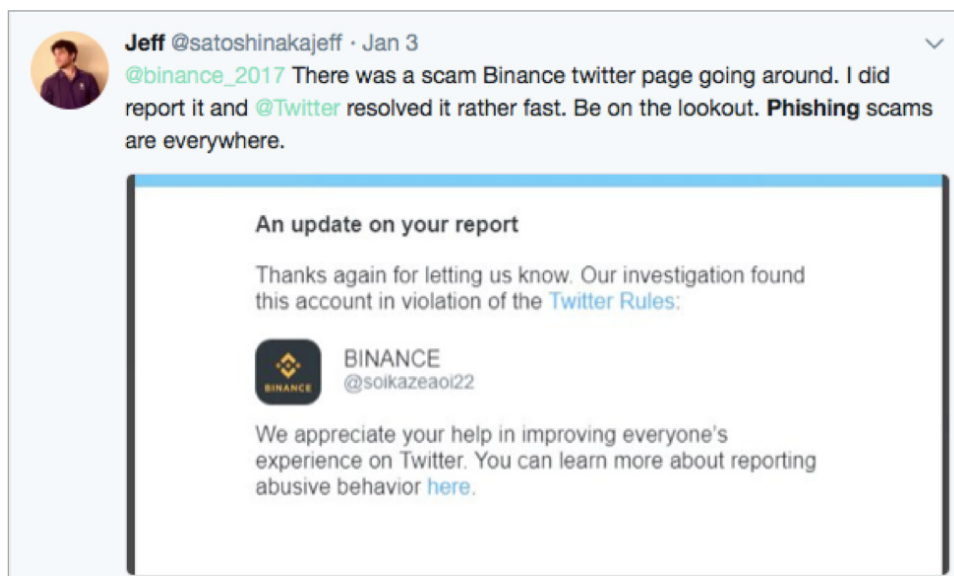


Figure 9: A spoof social media account of Binance, a popular cryptocurrency exchange.

Credential Stuffing

Another way to gain access is to target trading platforms and cryptocurrency exchanges directly. Instead of manually entering credentials into target sites, adversaries can automatically inject compromised username and password pairs into login portals to fraudulently gain access to user accounts. This technique, known as credential stuffing,⁹ is a type of brute force attack whereby large sets of credentials are automatically inserted into login pages until a match with an existing account is found. There are many credential stuffing tools in circulation, including SentryMBA, Vertex, and Account Hitman.

In order to make the software work, users require a configuration file. The configuration files map out the specific aspects of a target site, so the software knows where to attempt logins. This process is analogous to the macros dynamic web application scanners use to access and analyze websites. The configuration can be created by the more technical user, but for the less technical, the configurations are shared and sold on forums, marketplaces, and social media. This lowers the barrier to entry for those who do not understand web application design.

These configuration files are freely shared on a range of “cracking forums,” such as Neothingsgoez[.]com, cracking[.]org, and sentry[.]mba. Several configuration files have been shared on these forums, as shown in Figure 10.

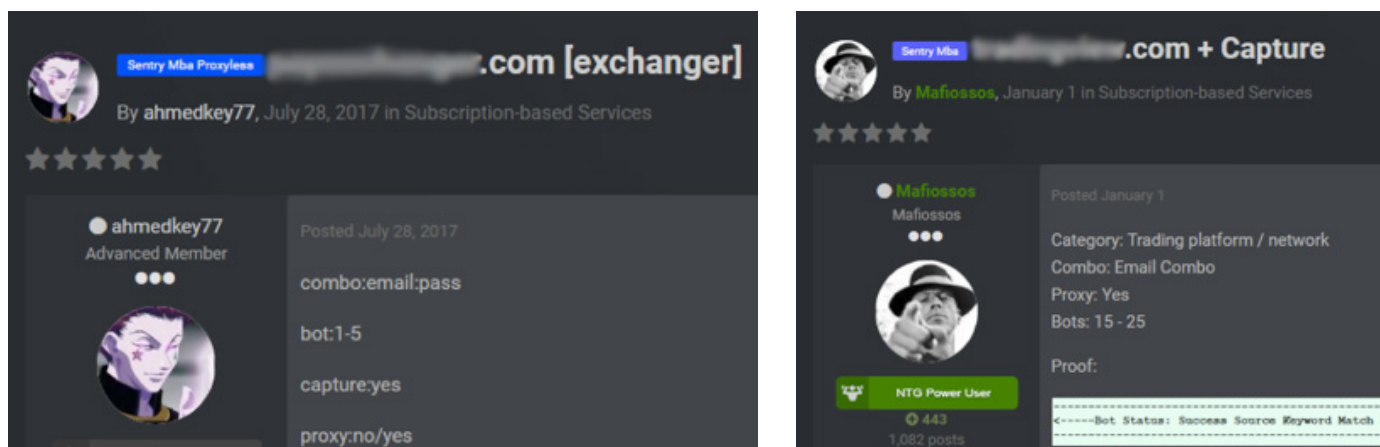


Figure 10: Configuration files for trading platforms and exchanges detected on a popular cracking forum.

⁹ Protect Customer and Employee Accounts, <https://resources.digitalshadows.com/whitepapers-and-reports/account-takeover-protect-your-customer-and-employee-accounts>

2. Criminals mining their own business

In the Gold Rush period, one of the most popular ways for individuals to make money was to mine for gold themselves, rather than pay more for gold procured by someone else. Similarly, those looking to profit from the cryptocurrency boom look to “mine” for the coins themselves.

Cryptocurrency transactions are recorded in a public ledger known as the blockchain, as it is made up of a series of transactions called blocks. Mining is the process by which computers validate these transactions. To do this, miners solve a computational problem – much like a mathematics puzzle – that contains the latest transaction data in it. Miners, or the operators of these mining machines, receive digital coins as a reward for solving these puzzles and contributing to the broader integrity of the blockchain. This process of mining began with Bitcoin in 2009 and has resulted in over 16.8 million mined Bitcoins. That’s 80% of the entire Bitcoin supply.¹⁰ As with gold, cryptocurrencies operate on a principal of limited supply, meaning that the more that is mined or taken out now has an impact on how easy it will be to mine in the future. In the case of bitcoin, there will only ever be 21 million Bitcoin.

Bitcoin has become so energy intensive to mine that malicious actors have turned to searching for organizations that expose their Amazon WorkSpace credentials on sharing sites like GitHub, and then using this access to steal computing power and mine Bitcoin.¹¹

Although bitcoin takes up significant amounts of computer processing power, Monero is easier to mine and is less energy intensive. This has led to a surge in individuals seeking to mine Monero. One such tool for doing so, SilentMiner, is shown in Figure 11. There are many miners that exist to assist this criminal pursuit of a range of cryptocurrencies. Figure 12 shows a piece of malware offered for sale on OpenBazaar - a decentralized market - which offers various mining options.

¹⁰ <https://cointelegraph.com/news/80-of-all-bitcoins-already-mined-only-42-million-coins-left-until-supply-cap>

¹¹ https://www.theregister.co.uk/2015/01/06/dev_blunder_shows_github_crawling_with_keyslurping_bots/

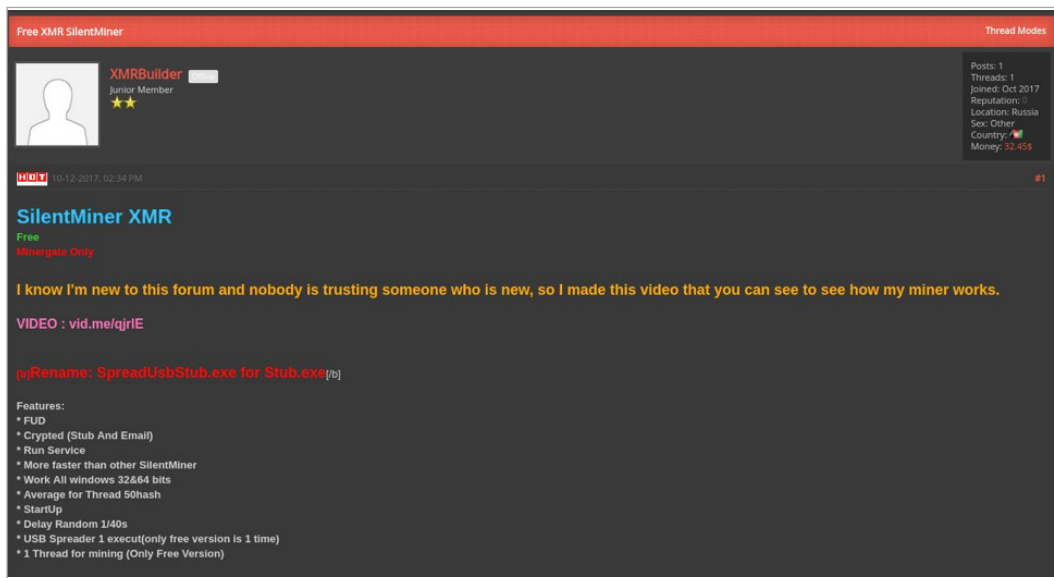


Figure 11: An advertisement for free Monero Mining malware from October 2017

Of course, where there is money to be made, cybercriminals soon follow. The actors behind WannaCry transferred the bitcoin they had received in ransom into Monero.¹² More recently, Monero miners were observed sending coins back to North Korea.¹³ The ransomware variant known as "VenusLocker" switched its business model to mine bitcoin rather than encrypt files on victims' computers. Similarly, the RIG exploit kit has incorporated Monero mining into its features.

Mining itself is far from an illegal act: it is an essential activity for cryptocurrencies. Nevertheless, there are two main ways that actors may fraudulently mine cryptocurrencies: botnets and crypto jacking.

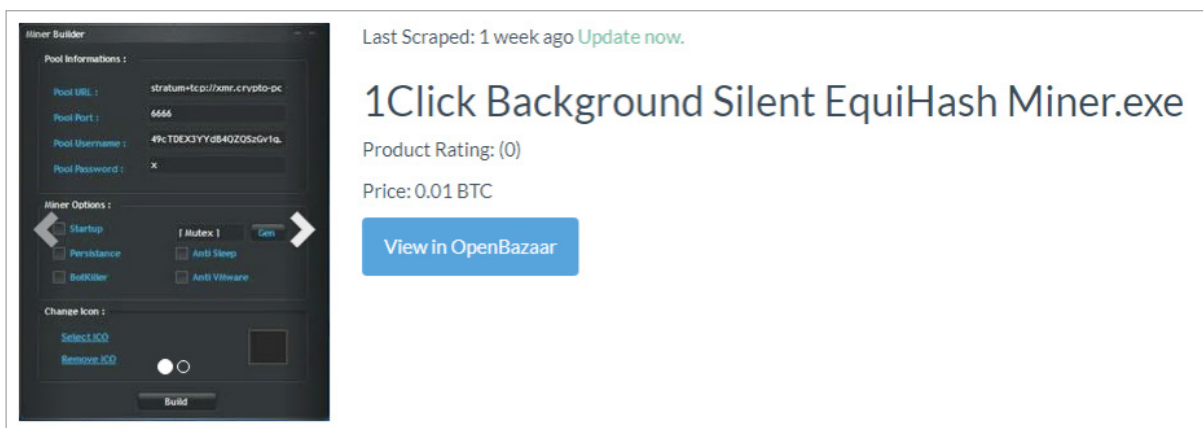


Figure 12: Miner advertised on Open Bazaar, for 0.01 BTC (110 USD at the time of writing)

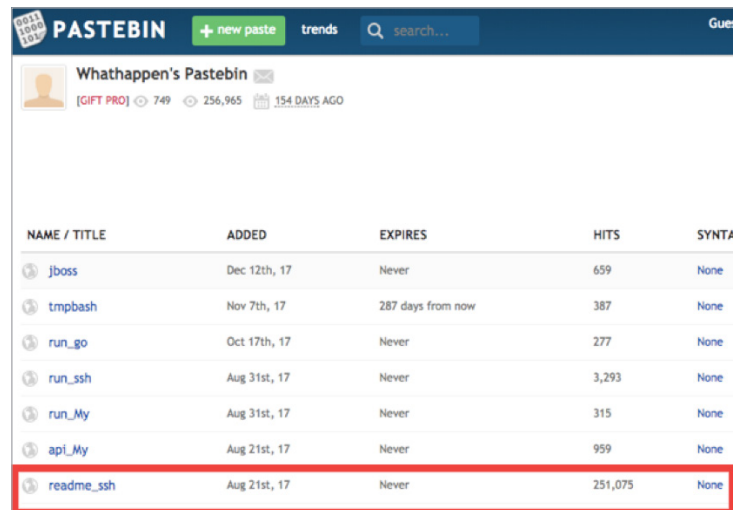
¹² <https://arstechnica.com/gadgets/2017/08/researchers-say-wannacry-operator-moved-bitcoins-to-untraceable-monero/>

¹³ <https://www.alienvault.com/blogs/labs-research/a-north-korean-monero-cryptocurrency-miner>

Botnets

In 2014, cybercriminals began to stop using their network of infected computers (or botnets) to mine Bitcoins as the increased difficulty of mining made it financially unviable.¹⁴ However, the ease of mining newer cryptocurrencies like Monero means this tactic is making a comeback.

The PyCryptoMiner uses Pastebin to publish its command and control (C2) domains rather than hardcoding them in to the malicious script itself; this hinders efforts to shut down or blacklist the domains and makes it easier for botnet operators to change C2 domains without affecting infection rates.¹⁵ To date, cybercriminals have successfully mined over \$46,000 worth of Monero using PyCryptoMiner.



NAME / TITLE	ADDED	EXPIRES	HITS	SYNTAX
jboss	Dec 12th, 17	Never	659	None
tmpbash	Nov 7th, 17	287 days from now	387	None
run_go	Oct 17th, 17	Never	277	None
run_ssh	Aug 31st, 17	Never	3,293	None
run_My	Aug 31st, 17	Never	315	None
api_My	Aug 21st, 17	Never	959	None
readme_ssh	Aug 21st, 17	Never	251,075	None

Figure 13: A Pastebin page used to host a PyCryptoMiner C2 server. Notice the disproportionate page views on the 'readme_ssh' page

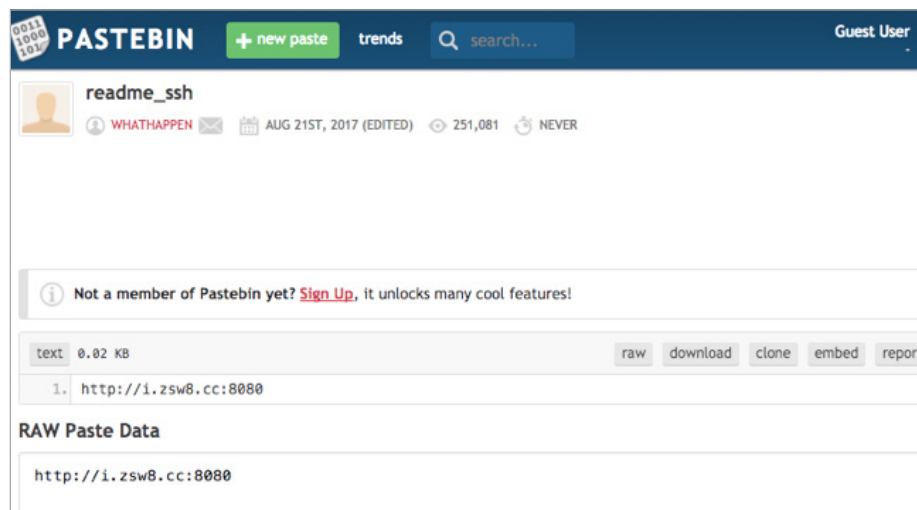


Figure 14: PyCryptoMiner C2 server address hosted on Pastebin.com

¹⁴ https://www.theregister.co.uk/2014/06/24/bad_news_malware_infections_are_mining_bitcoin_good_news_theyre_not_making_any_money/

¹⁵ <https://f5.com/labs/articles/threat-intelligence/malware/new-python-based-crypto-miner-botnet-flying-under-the-radar>

You do not have to look far to find other examples of inexpensive mining botnets. Figure 15 shows one available to rent for just \$125. These are popular items to buy on the dark web; Figure 16 shows another Monero mining botnet advertisement. This product costs the equivalent of \$30 and has flown off the shelves with almost 2,000 rentals so far.

jkoper
newbie

Бот:

- Поддержка CPU (определение: x32/x64)
- Поддержка GPU (определение: Radeon/Nvidia).
- Майнер не виден при детекте taskmanager, process explorer и подобных утилит.
- Возможность обновления бота (для смены майнеров, ввода нового функционала).
- Доступна торифицированная версия бота.
- Контроль майнеров (в любом случае майнер будет восстановлен, пока жив бот).
- Бесплатные ребилды.
- Вес: 50 КБ.
- NET 2.0.
- Все обновления и любая поддержка по боту бесплатны.

Стандартная сборка майнеров:
Monero (CPU) + Опционально: Decred (GPU)

ЯП: C#

Функционал Панели:

- Dashboard: [*] Онлайн, Живые, За все время, За сутки. [*] Последние машины.
- Machines: [*] Статистика по всем ботам. [*] Уникальный ID машины, Битность, Версия бота, Видеокарта, ЦПУ, Первый онлайн, Последний онлайн.
- Update: [*] Возможность обновить бота.

Цена Комплекта: 125\$.

Контакты: expfo@exploit.im

Figure 15: An advertisement for a botnet to mine Monero on a Russian language forum in October 2017, priced at \$125

MINE MONERO (XMR) USING INFECTED COMPUTERS

Vendor TopNotchMoneyMaker (5600) (4.73★) (@ 2819/115/98)

Price ₮0.000916 (\$10.4)

Ships to Worldwide

Ships from Digital

Escrow Yes

Figure 16: An advertisement for a Monero mining botnet on the Dream Marketplace, costing only \$30

Crypto Jacking

Another popular method for mining cryptocurrencies is via crypto jacking. Crypto jacking occurs when attackers secretly use your mobile device/computer resources to mine cryptocurrencies.

Since the middle of 2017, Internet browsers,¹⁶ browser extensions,¹⁷ and mobile apps¹⁸ have all been used to spread “Coinhive”, a Javascript miner for Monero. Coinhive originated as a tool designed to allow developers to mine Monero using their Web browsers, but it was quickly adopted by malicious threat actors, with reports it had become the sixth most common malware worldwide in November 2017.¹⁹

More recently, proof of concept (PoC) code for an application known as “CoffeeMiner”²⁰ was released, which allowed actors to access public Wi-Fi networks and mine cryptocurrencies using Coinhive. The name CoffeeMiner was inspired by attacks against Wi-Fi networks in coffee chains that allowed attackers to mine cryptocurrencies.

One of Coinhive’s biggest problems is that sites do not ask for user permission before running the mining software on their CPU, which has led security firms like Malwarebytes to block coinhive[.]com.²¹ While Coinhive does provide a separate product that requires explicit user opt-in – Authedmine – this is not the product chosen by many of its user base. It is also worth noting that Coinhive is not the only miner in town. “Crypto-Loot” is another example of a stealthy cryptocurrency miner that can be placed into websites.²²

We recently observed a new piece of mining software called “Crypto Jacker,” which combines Coinhive, Authedmine and Crypto-Loot into a WordPress plugin (cj-plugin), with added Search Engine Optimization (SEO) functionality. The domain cryptojacker[.]co was registered on November 30, 2017 and seeks to sell a one-time version of the Crypto Jacker software for \$29. Crypto Jacker customers can install the software on an unlimited number of their domains and begin mining.

¹⁶ https://www.reddit.com/r/blackberry/comments/7nqnnw/official_blackberry_mobile_site_uses_coinhive_to/

¹⁷ <https://www.bleepingcomputer.com/news/security/chrome-extension-with-100-000-users-caught-pushing-cryptocurrency-miner/>

¹⁸ <https://betanews.com/2018/01/08/fake-android-apps-coinhive/>

¹⁹ <https://www.bleepingcomputer.com/news/security/chrome-extension-with-100-000-users-caught-pushing-cryptocurrency-miner/>

²⁰ <http://arnaucode.com/blog/coffeeminer-hacking-wifi-cryptocurrency-miner.html>

²¹ <https://blog.malwarebytes.com/security-world/2017/10/why-is-malwarebytes-blocking-coinhive/>

²² https://www.theregister.co.uk/2017/10/23/cryptocurrency_miner_google_chrome_extension/

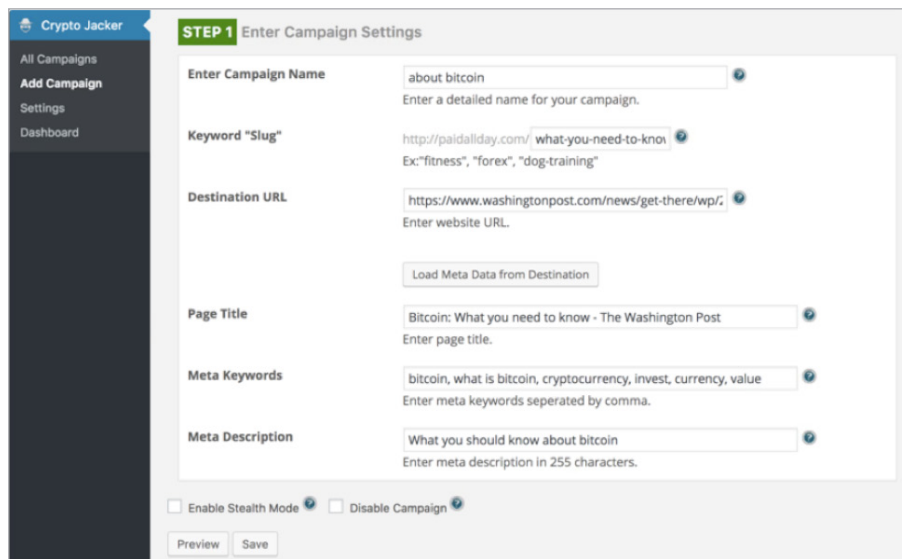


Figure 17: The user interface of the Crypto Jacker plug-in, as shown on cryptojacker[.]co

The software allows users to clone popular websites that can then be sent out in spam campaigns. According to the Crypto Jacker site, the software “provides a way to earn crypto currency from people who visit your links, even when you’re sharing other websites that you don’t own. We even cloak your website links for your (sic.) so they look like the original shares on social media.”

Our own tests of the demo domain shown on the Crypto Jacker website (paidallday[.]com/what-you-need-to-know-about-bitcoin) showed us that cryptocurrency mining was likely taking place. As shown in Figure 18, the website appeared to have the plugin “cj-plugin”, which launched the “cryptoloot[.]pro” script. When we visited the site, CPU usage increased significantly to 50% (as shown in Figure 19). While this does not confirm the Crypto Jacker product is legitimate, it does add credibility to its claim.

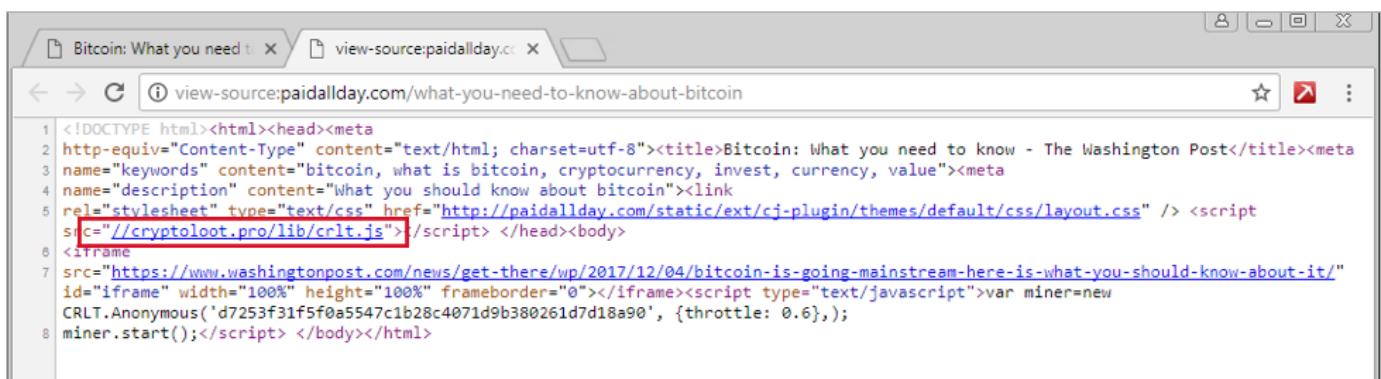


Figure 18: The source code of paidallday[.]com/what-you-need-to-know-about-bitcoin, a demo website shown in Crypto Jacker videos

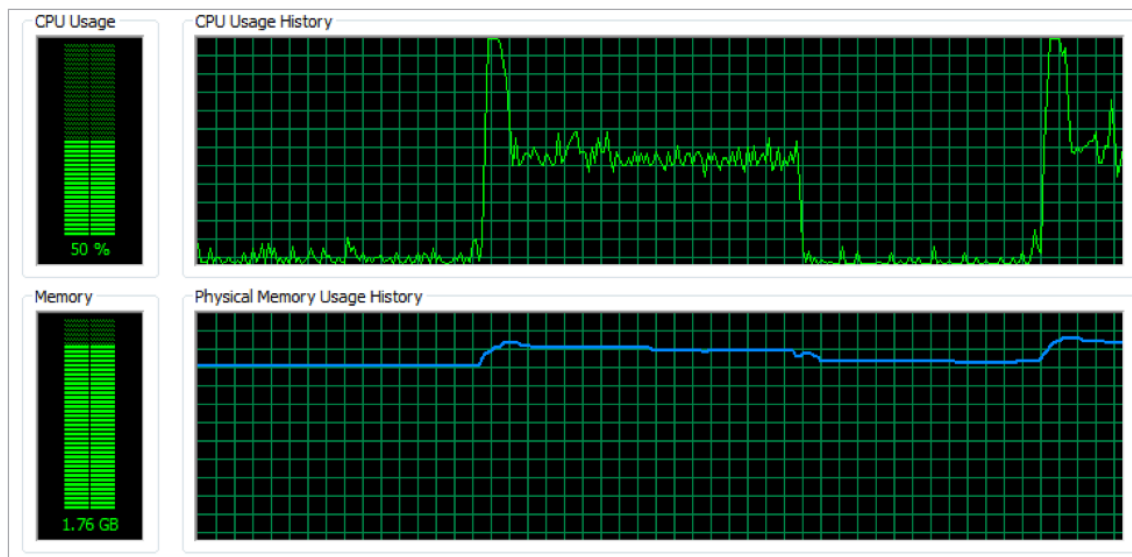


Figure 19: CPU usage peaking at the time of the visit to the website

Interest in cryptocurrencies shows no sign of slowing down and while Crypto Jacker does not appear to have developed a large user base, its emergence – if legitimate – is an attempt to lower the barriers to entry of stealthy cryptocurrency mining software.

3. Criminals targeting Initial Coin Offerings

During the excitement of the California Gold Rush, some individuals decided on more nefarious means to make their fortune. One such method was to create counterfeit or synthetic gold that could be passed off as the real thing. These man-made replicas were so realistic that they fooled many undiscerning 49ers to part with their cash. By the time they realized their mistake, the fraudsters had already packed their bags and disappeared with their newfound riches.

Like the 49er scammers, cybercriminals have looked to take advantage of the interest in new and emerging cryptocurrencies by creating their own fictitious coins and performing exit scams. As well as hawking scam currencies, criminals have also targeted legitimate currencies, either by stealing funds from Initial Coin Offerings (ICOs) or by manipulating prices through pump and dump schemes. The largest theft to date has been the targeting of Coincheck, resulting in the loss of over \$500 million.

ICO Compromise

ICOs are a way of crowdfunding cryptocurrencies. As consumers rush to be the first to invest in a promising new cryptocurrency, their investments can instead go into the account of criminals. In the case of CoinDash, criminals compromised the CoinDash website in July 2017 and swapped the Ethereum address to one controlled by the attacker. We tracked the attacker-controlled wallet at the time and noticed that during the CoinDash ICO, the attacker received at least 2,314 payments from prospective CoinDash investors totaling over 40,000 Ether, as shown in Figure 20. By the time Coindash noticed the switch and informed its customers to cease transactions, over \$7 million in Ethereum had been transferred to the fake address.²³ Even before the Coincheck hack, research estimated that up to \$400 million has been stolen by targeting ICOs.²⁴

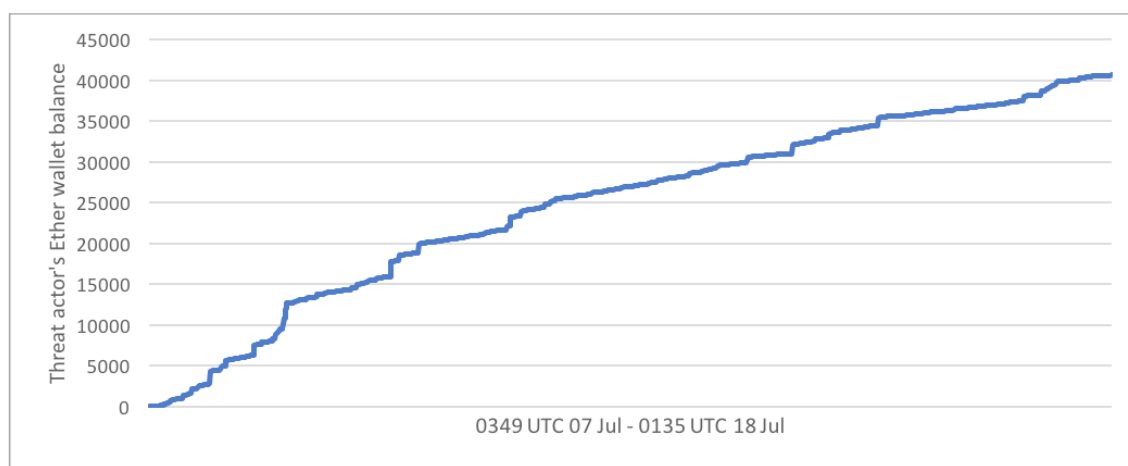


Figure 20: Attacker's Ether wallet during CoinDash ICO

Exit Scams

While CoinDash was a legitimate ICO that was compromised by a cybercriminal, there are many instances of individuals creating entirely fictitious cryptocurrencies and performing exit scams. This has occurred with a range of different exchanges and currencies, including the \$375,000 stolen as part of Confido's exit.²⁵

Threat actors commonly discuss this popular approach to fraud on criminal forums: "you can create a scam site...people will invest with the motivation for growth of this crypto currency."

²³ <https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer/>

²⁴ <http://www.zdnet.com/article/hackers-steal-almost-400-million-from-cryptocurrency-icos/>

²⁵ <https://www.cnn.com/2017/11/21/confido-ico-exit-scam-founders-run-away-with-375k.html>

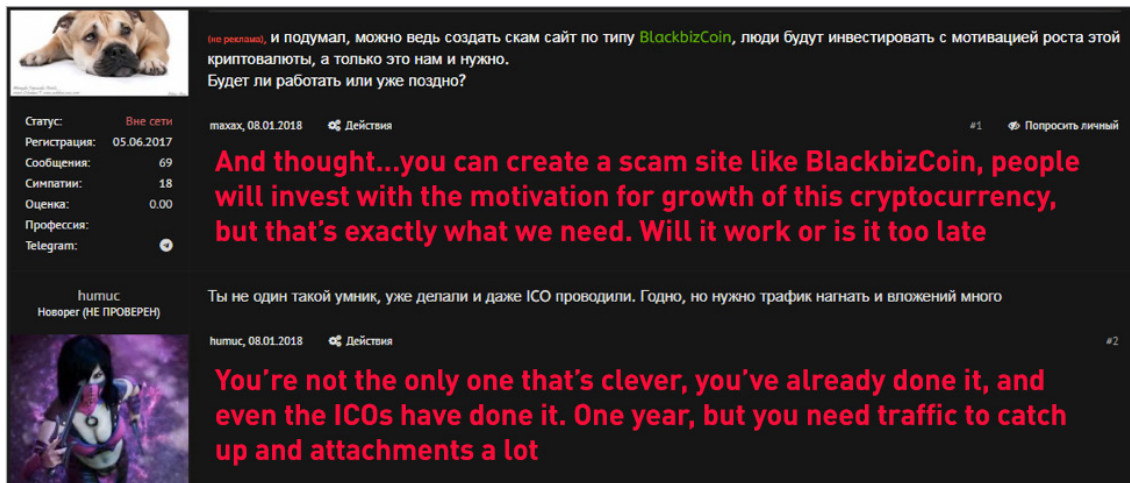


Figure 21: Russian language criminals discussing the creation of a fake cryptocurrency coin

You do not need to turn to the dark web and criminal forums to see this in action. A quick search of freelance job sites shows several individuals seeking assistance in cloning specific exchange sites (Figure 22) and creating new cryptocurrencies (Figure 23).

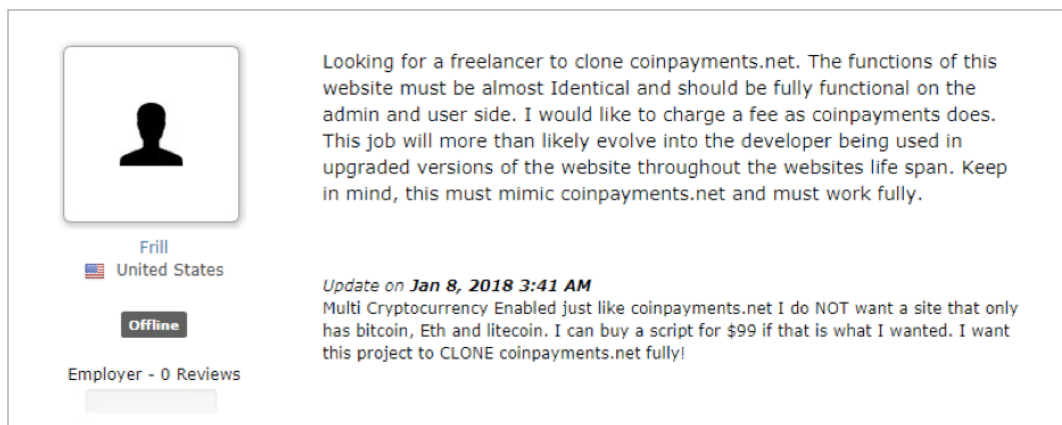



Figure 22: Individual looking for help to clone an online exchange

Project Description



Ginfo
New Zealand

Offline

Employer - 0 Reviews

We are looking to create a new cryptocurrency with wallet and need an experience cryptocurrency developer that can develop/build modules in php/mysql

This new cryptocurrency would need to have where X percentage of the "mined" coins go to help fund open source projects created by writers and software developers. We also want to make it so only X coins will be mined and then we can increase that number.

Please ONLY BID if you can create this quickly and have A LOT of Experience and Skills in Crypto Currencies and Bitcoin (alt-coins).

This would be a New Business Partnership with Huge Potential long term for ALL parties involved so please don't look at this as just a "Project" or "Job." If you like solid long term business with great upside then make sure to message me or bid for this Business Project!

After the currency is created we will need other help on other projects including but not limited to a Mining Pool, Apps, Marketing Campaigns and a lot more.

Figure 23: Individual looking for help to create a new cryptocurrency

Pump and Dump

Just as traders illegally inflate prices of stock in the real world, so too do groups of cybercriminals. Pump and dump groups exist to inflate the price of smaller, less well-known currencies in order to cash in on the increase in value.

BITCOIN INSIDER

PACKAGES CONTACT US

PACKAGE 1



PUMP COINS

- DAILY emails of ALL the coins that will be pumped that day.
- You will have at least 1 hr before the first pump to start buying all the coins for that day.
- Price: 0.02 BTC
- 3 Months Subscription
- You subscription fee will be made back over the first 2 pumps or your MONEY BACK

PACKAGE 2



PALMBEACHCONFIDENTIAL

- Palm Beach Confidential reports emailed to you.
- Price: 0.02 BTC
- 3 Months Subscription

PACKAGE 3



TELEGRAMPAID GROUPS

Choose one of the following PAID channels to be added to:

- King VIP Signals
- Korean VIP Signals
- Dude PAID Channel
- Palm Beach PAID
- Trading Crypto Coach PAID
- Whale Leaks PAID
- ... others on request.
- Price: 0.02 BTC (3 Months)

Figure 24: Insider and "Pump" packages for sale, each one for 0.02 BTC (220 USD at the time of writing)

In our previous report on The Business of Disinformation, we focused on "the insider," a dark web site that claims to "manipulate the price of an altcoin to make profit."²⁶ This technique appears to be far more widespread. In one pump and dump group on the Discord messaging app that we monitor, the administrator claimed:

"We spread great news on twitter and Reddit. After sending the coin name and link, we will send the Twitter and Reddit post. We have around 5000 people online...Everyone will need to have a twitter and reddit account. We will mass retweet, like and react on the tweet that I send, spam it with #hashtags etc. We will massively upvote and react on the reddit post to get it to the first page." (Figure 25)

²⁶ <https://resources.digitalshadows.com/whitepapers-and-reports/the-business-of-disinformation-fake-news>

@here
Good morning guys,
The next pump is tomorrow, Sunday 31 December. Unlike last pump, we are going to try and let this one last longer than 2 minutes. We will try to let this be a HODL and dump it on outsiders. How will we achieve this? And can we achieve this? To start of with the first question, we have a thought out strategy for this one. We spread great news on twitter and Reddit. After sending the coin name and link, we will send the Twitter and Reddit post. We have around 5000 people online (probably more, but we will focus on 5000). Everyone will need to have a twitter and reddit account. We will mass retweet, like and react on the tweet that I send, spam it with #hashtags etc. We will massively upvote and react on the reddit post to get it to the first page. The only problem is, it will take 10 minutes for the news to reach the masses. My second question, can we achieve this? It is really hard for me to give a proper and honest answer. A lot of traders are driven by greed, definitely not everyone, but most are. Once they see a profit of 10-15% they will sell. And once this selling begins, we cannot stop it which will result in the dump. So, will this work 100%? Definitely not 100%, however if enough people believe in it and follow the plan we will succeed. Are we going to try it? Yes we definitely are! We can fight whales, we are a strong group. What if it fails? If this fails, we will have to continue looking for new plans and ideas, we are always open to discuss them with you in DM. Dm any of the admins or the helpers!
Have a great day,

Figure 25: A description of how “pump and dump” works, as described in one Pump and Dump Discord group

It is important to note that these “pump and dump” campaigns are not a new phenomenon. In May 2014, we observed IRC conversations in which users warned their peers of becoming involved: “yes the alternative coins are major pumps, stay out if you do not know what you’re doing.” What has changed is how many groups are now involved in this type of activity; we have observed over 20 active channels that are being used on Discord alone.²⁷

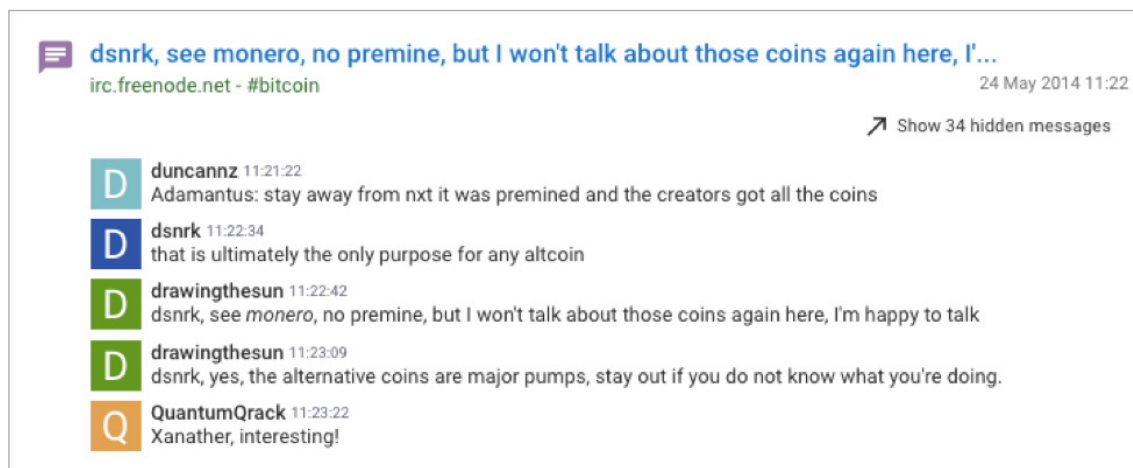


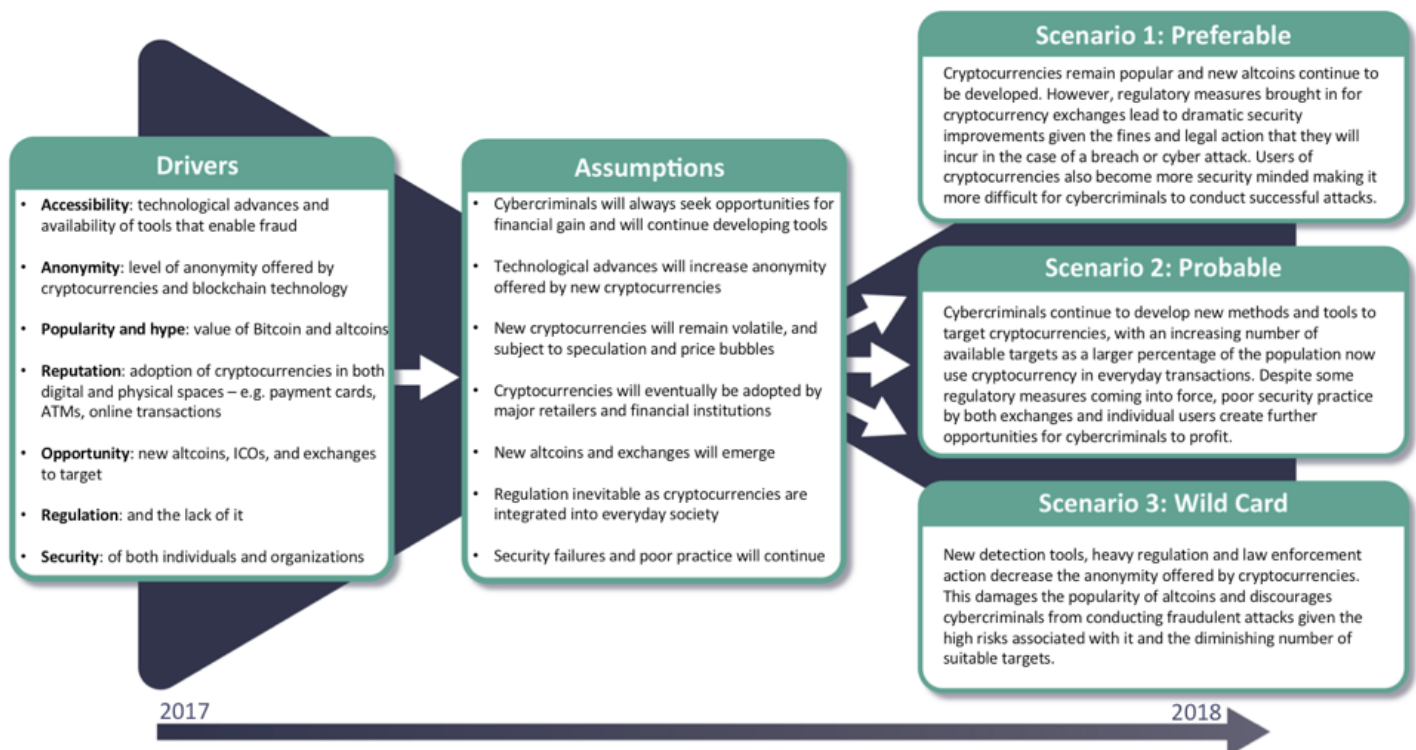
Figure 26: An IRC conversation discussing the “pumping” of alternative coins

²⁷ <https://pastebin.com/xVjxtn2p>

Forecasting Cryptocurrency Fraud

While the future of cryptocurrencies remains somewhat uncertain, what we can be sure of is that cybercriminals will continue to find new ways of making money as long as there are enough suitable targets and the profits to be made justify their time and effort. One way of envisaging the future of cryptocurrencies is to employ what is known as the “Cone of Plausibility,” a Structured Analytic Technique used by Digital Shadows’ intelligence analysts to generate plausible scenarios and help organizations plan for multiple eventualities.²⁸

One of the greatest benefits of this forecasting approach is that it allows us to outline the drivers behind the rise in cryptocurrency fraud, which can give us key insights into the factors that will determine its future. In this case we have focused on the accessibility of fraud-enabling tools, the anonymity of cryptocurrencies, the popularity and media attention they have recently received, the ample opportunities and targets provided by new altcoins and exchanges, the lack of regulation and oversight, and the relative lack of security maturity by both cryptocurrency users and organizations. By changing the assumptions behind these drivers, alternative plausible scenarios can be imagined.



By outlining these drivers and assumptions, it’s possible to look at ways of avoiding the less favorable scenarios. Specifically, this can be done by limiting the opportunity available to threat actors and the accessibility of tools that enable fraud, as well as strengthening security practices and regulation.

²⁸ <https://www.digitalshadows.com/blog-and-research/you-should-consider-forecasts-not-predictions/>

Opportunity

As we have seen, the sheer number of new altcoins, exchanges and coin offerings means that fraudsters have a wealth of potential targets. Greater education about cryptocurrencies and the risks associated with them for consumers can help fight this trend. In particular, consumers should look out for phishing sites or unsolicited messages offering great returns on new altcoins and ICOs. For exchanges and ICO projects, securing public-facing applications and websites can help prevent website compromises like the one suffered by CoinDash.

Accessibility

Cybercriminals will always find new ways to conduct fraud or incorporate mining tools into their attacks. Recently, a new Mirai Internet of Things (IoT) botnet known as Satori was repurposed and used to deliver an Ethereum crypto miner. To help limit the number of available resources to fraudsters, consider:

- Replacing factory-default credentials with unique and strong passwords to prevent IoT devices from being incorporated into botnets.
- Authenticating your cloud services like AWS, as fraudsters can steal your processing power to mine for cryptocurrency.

Security

As long as organizations and individuals fail to improve their security measures, opportunities for fraud will continue to exist. Though simple measures, both organizations and consumers can combat this by:

- Enforcing strong password security rules across the organization, which includes enabling multi-factor authentication (MFA) on online accounts used to handle cryptocurrencies if possible.
- Patching known vulnerabilities being used in the delivery of crypto miners.

Regulation

The success of pump and dump schemes and scam ICOs is aided by a lack of regulation and oversight. In a regulated market, this type of fraud would be illegal and therefore precipitate necessary law enforcement action. Exchanges and ICO projects would be under more pressure to improve their security practices, as they would face tough consequences if they were found to have facilitated a breach or fraud. United States authorities recently filed charges against PlexCorps, which was accused of defrauding investors through a scam ICO.²⁹

Regulatory measures will likely be uneven though, with some countries such as China and South Korea choosing to ban ICOs completely.³⁰ While stricter regulation could have a beneficial effect in reducing fraud, it may also deter would-be investors and drive down the value of cryptocurrencies.

Protecting Yourself Against Cryptocurrency Fraud

Despite their volatility, high valuations, and the projected adoption of cryptocurrency in both online and physical transactions, cryptocurrency fraud will not go away any time soon. Even with long-established regulatory and law enforcement measures, traditional currencies are still targeted by fraudsters, so there is no reason to expect cryptocurrencies will be any different. One contributing factor to cryptocurrency fraud is the opportunity provided to fraudsters through poor security practices both on an individual and organizational level. Although it is too much to expect fraud to be completely eradicated, there are several measures that organizations, consumers and exchanges can take to mitigate cryptocurrency fraud risks.

Organizations	Action	Resources
	Authenticate cloud services like Amazon WorkSpace (AWS) as criminals can steal your resources and mine for cryptocurrency.	Amazon provides guidance on configuring AWS Command Line Interface and authenticating access to AWS .
	Monitor GitHub and other paste sites for Amazon WorkSpace credentials.	Sites like HavelBeenPwned monitor common dump sites and can be used to alert you if any company credentials are leaked online.
	Blacklist C2 domains used by cryptocurrency botnets and mining tools.	A good place to start is the CoinBlockersList project on GitHub, where new crypto mining domains are added daily.
	Apply patches and mitigation to known vulnerabilities as these can be used to deliver crypto miners. In December 2017 PyCryptoMiner, for example, began exploiting a vulnerability affecting JBoss servers that was first discovered in October. More recently, a Struts server exploit has been used for Monero mining. ³¹	Sites such as the US CERT , the National Vulnerability Database and MITRE can provide the latest information on newly disclosed vulnerabilities. Red Hat Software provided mitigation advice for the JBoss vulnerability exploited by PyCryptoMiner. Patches for the Struts vulnerabilities are also available.
	Have a reputable ad blocker in place.	Consider ad blockers such as AdBlock , AdBlock Plus , 1Blocker , and UBlock . The NoCoin browser extension was also developed to block coin miners such as Coinhive.

²⁹ <https://www.sec.gov/news/press-release/2017-219>

³⁰ <https://www.forbes.com/sites/forbestechcouncil/2017/12/11/how-will-the-china-and-south-korea-ico-bans-impact-cryptocurrencies/>

³¹ <https://blog.trendmicro.com/trendlabs-security-intelligence/struts-dotnetnuke-server-exploits-used-cryptocurrency-mining/>

	Action	Resources
Consumers	Do your research and be cautious before investing in new cryptocurrencies.	Does the coin you are looking to invest in have an active online community with engaged developers? Have other online users reported the coin as a scam? Look out for red flags such as sites or seller with unsolicited offers, or coins that guarantee high returns and hide behind marketing jargon that makes no effort to explain the technical aspects.
	Monitor for personal credentials that might have been leaked or stolen.	Sites like HaveIBeenPwned monitor common dump sites and can be used to alert you if your credentials are leaked online.
	Enable multi-factor authentication (MFA), where possible, on any online accounts used to handle cryptocurrencies. This includes exchanges and wallets.	Many sites now offer MFA (aka 2FA), so a secondary, one-time proof of identity is needed alongside the password to log in. This can be a device (e.g. SecureID token), software (e.g. Google Authenticator) or an SMS message. You can check whether a site offers MFA by visiting twofactorauth.org .
	Look for phishing sites.	Check phishing databases and more specialist cryptocurrency fraud sites such as the Ethereum Scam Database before using any sites that you are unfamiliar with.
Exchanges	Guard against credential stuffing software like Sentry MBA, Vertex, and Account Hitman.	Web Application Firewalls can also be used to prevent account takeover from credential stuffing tools.
	Monitor for username and password breaches for your site's administrators and users.	Sites like HaveIBeenPwned monitor common dump sites and can be used to alert you if your credentials are leaked online.
	Look for phishing sites.	DNS Twist is a python script that can find phishing sites and typosquats based on your domains. Detect these before your customers lose out.

About Digital Shadows

Digital Shadows provides insight into an organization's external digital risks and the threat actors targeting them. Digital Shadows SearchLight™ service combines scalable data analytics with human analysts to monitor for cyber threats, data leakage, and reputation risks. Digital Shadows continually monitors the Internet across the visible, deep and dark web, as well as other online sources to create an up-to-the minute view of an organization and provide it with tailored threat intelligence. The company is jointly headquartered in London and San Francisco. For more information, visit www.digitalshadows.com.

London

Level 39, One Canada Square,
London, E14 5AB

+44 (0) 203 393 7001

info@digitalshadows.com

San Francisco

332 Pine St. Suite 600,
San Francisco, CA 94104

+1 (888) 889 4143