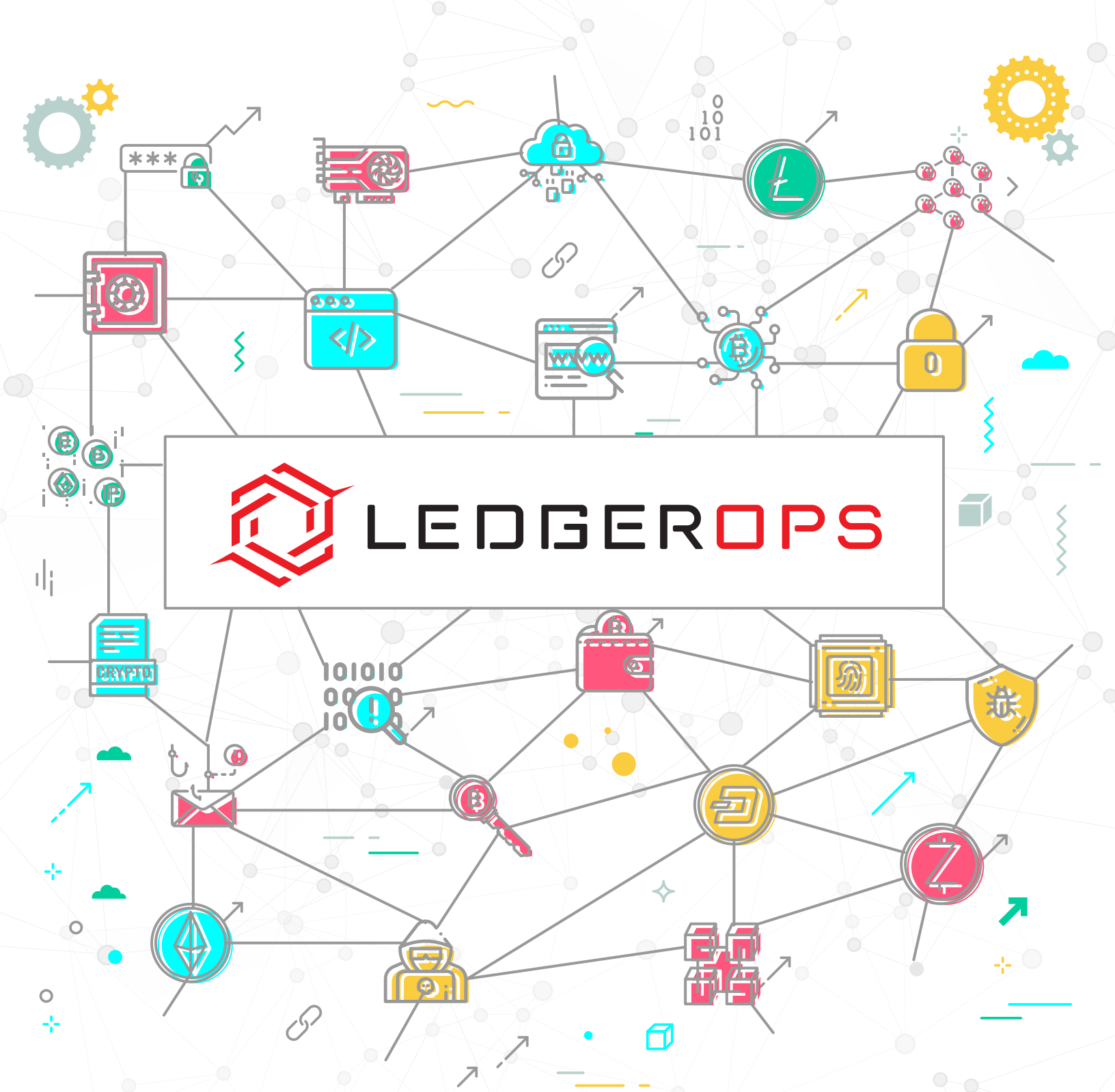


BLOCKCHAIN SECURITY THREAT REPORT

2018 REVIEW

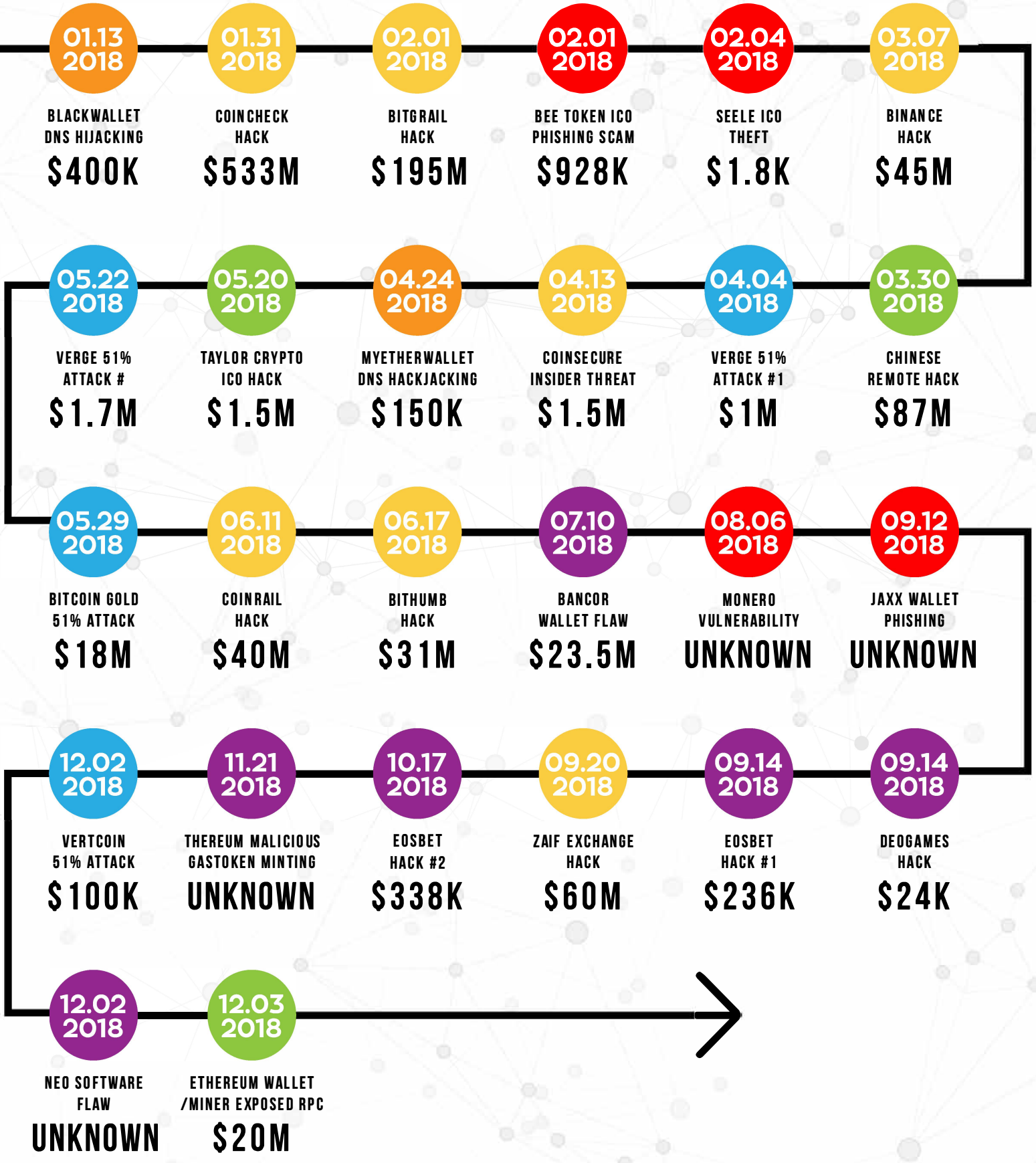
In 2018, the word blockchain started to appear in many conversations within the technology industry. Organizations and individuals questioned what a blockchain truly is and how beneficial it may be to growing businesses. Soon after that, you saw a whole host of companies begin to implement a blockchain into their operations.

There's a lot to gain from blockchain technology, there's no denying it. However, the introduction of increasingly sophisticated attacks surrounding the nature of cryptocurrency makes widespread adoption increasingly difficult, and with no fund insurance for end-users, casual use becomes daunting. As organizations continue to utilize blockchain technology further, it's important to understand the security risks that may come with it.

In this report, we cover the types of threats that blockchains and blockchain users face, some classic examples of each category, and how you can avoid becoming a victim yourself. We break down:

Types of attack:

- PHISHING & SOCIAL ENGINEERING
- DNS HIJACKING
- EXCHANGE HACK
- OTHER HACKING
- 51% ATTACK
- SOFTWARE FLAW



What Is Blockchain Technology?

A blockchain is the core technology for cryptocurrencies like Bitcoin and Ethereum. It's effectively a shared, trusted, and immutable public ledger of transactions.

The technology provides a decentralized, cryptographically secure, tamper-resistant database that puts power in the hands of the people. Instead of placing your trust in a centralized authority, like a bank, you instead trust computing code - code that's available for the public to review and has been vetted by some of the world's top computer scientists.

Blockchain Benefits

Without going into too much detail, blockchain-specific features provide significant value in certain situations:

Robust: A redundant number of computers around the world store copies of a blockchain's ledger. If one (or a few) computers go offline, a record of the blockchain still exists on numerous other computers.

Censorship-resistant: Because no single entity controls a blockchain, there isn't someone who can freeze or control your funds.

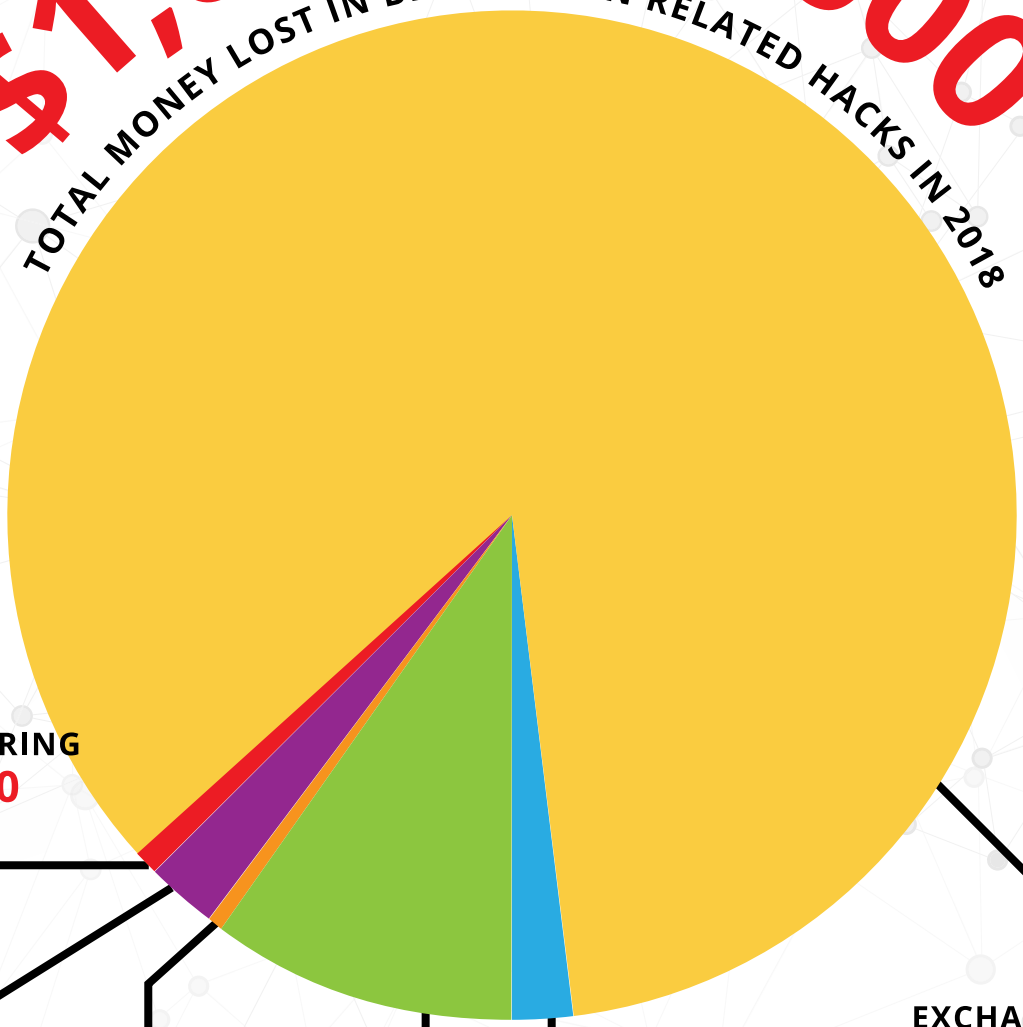
Trustless: At first glance, trustlessness may seem like a con, it's not though. A block chain enables direct, peer-to-peer transactions that utilize mathematics to ensure their validity. Therefore, you can comfortably send money (or data) across the globe without sacrificing the time and fees that usually come with intermediaries.

However, blockchain technology isn't all sunshine and rainbows, as you'll soon see, the young industry is chock-full of potential security threats.

Hacks by Category

$1,064,176,000

TOTAL MONEY LOST IN BLOCKCHAIN RELATED HACKS IN 2018



PHISHING & SOCIAL ENGINEERING
$2,728,000

DNS HIJACK
$550,000

SOFTWARE FLAWS
$24,098,000

OTHER HACKING
$108,500,000

51% ATTACKS
$20,800,000

EXCHANGE HACKS
$907,500,000

Types of Blockchain Attacks

Exchange Hacks

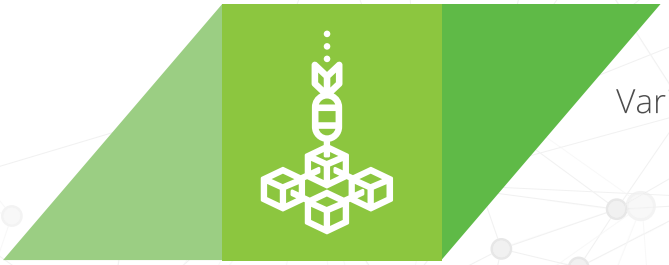
Variety of techniques used to steal crypto from exchanges.

Total Lost: $907,500,00

Other Threats

Variety of traditional attacks that affect systems connected to a blockchain.

Total Lost: $88,500,000



Software Flaws (Wallets and DApps)

Bugs in code allowing abuse of functionality.

Total Lost: $24,098,000

51% Attacks

Rewriting the blockchain with majority control of the network.

Total Lost: $20,800,000

Phishing & Social Engineering

Impersonating official communications to steal credentials.

Total Lost: $2,728,000

Malware/ Cryptojacking

Using a device's resources to mine cryptocurrency without the owner's permission.

Total Lost: N/A

Top Blockchain Security Threats of 2018

In 2018, coin thefts dominated the cryptocurrency market, affecting users, wallets providers, and exchanges alike. Hackers **stole $1 billion** from cryptocurrency exchanges and other platforms just last year alone. Let's take a look at the deceptive tactics that attackers adopted to target their victims to learn how to avoid becoming a hacking statistic.

Phishing and Social Engineering

Phishing and social engineering scams are one of the most widespread attacks in cryptocurrency today. In these attacks, malicious parties use a variety of tricks to dupe unsuspecting victims into sending over their private keys or login information.

What is phishing? Phishing scams attempt to duplicate authentic organization online identities (either through email or social media accounts) to trick you into thinking you're receiving information from an official entity. Scammers usually deceive users by developing replica identities that mimic cryptocurrency-related companies.
They'll copy a company's entire identity including:

EMAIL SIGNATURE

SOCIAL MEDIA HANDLE

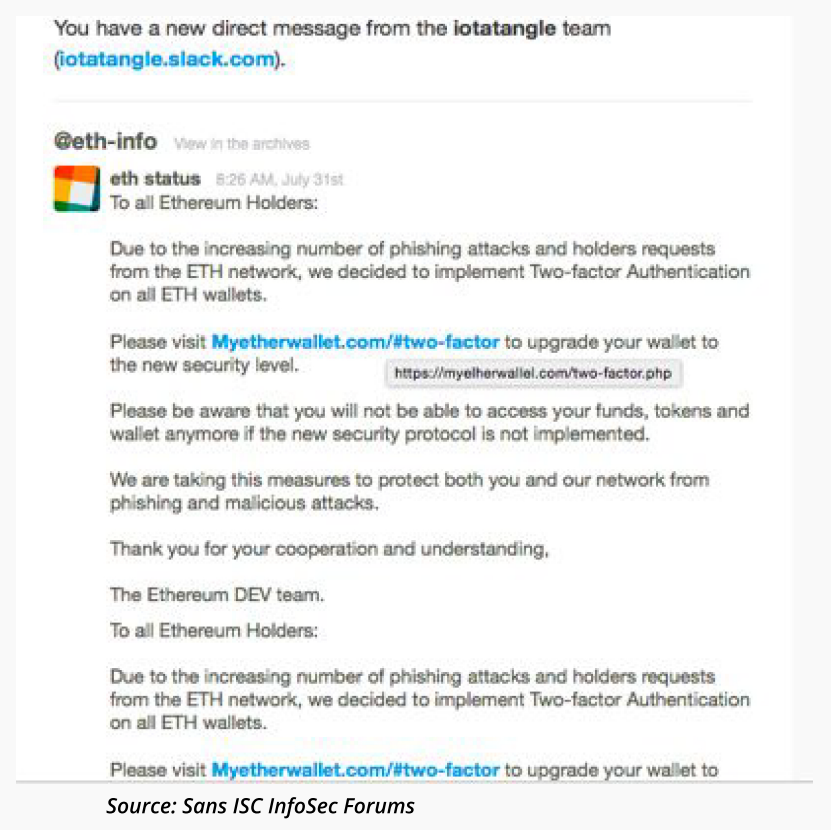
URL DESIGN

WEBSITE DESIGN

Often, phishing emails include an official-looking message describing a fictitious issue or chance to receive free tokens. These emails usually contain a call-to-action with a sense of urgency as well.

My Ether Wallet - A Prime Phishing Example

My Ether Wallet (MEW) is a common platform to store Ethereum and ERC-20 tokens. As such, it's a favorite target for phishers. The message below was sent across several chat groups as well as in an email to MEW users. **Can you spot the issue?**



You have a new direct message from the **iotatangle** team (iotatangle.slack.com).

@eth-info View in the archives

eth status 8:26 AM, July 31st

To all Ethereum Holders:

Due to the increasing number of phishing attacks and holders requests from the ETH network, we decided to implement Two-factor Authentication on all ETH wallets.

Please visit **Myetherwallet.com/#two-factor** to upgrade your wallet to the new security level. https://myetherwallet.com/two-factor.php

Please be aware that you will not be able to access your funds, tokens and wallet anymore if the new security protocol is not implemented.

We are taking this measures to protect both you and our network from phishing and malicious attacks.

Thank you for your cooperation and understanding,

The Ethereum DEV team.

To all Ethereum Holders:

Due to the increasing number of phishing attacks and holders requests from the ETH network, we decided to implement Two-factor Authentication on all ETH wallets.

Please visit **Myetherwallet.com/#two-factor** to upgrade your wallet to

Source: Sans ISC InfoSec Forums

Notice the difference between the two URL addresses. As you can see, this looks like a legitimate message. However, if you hover over the Myetherwallet.com/#two-factor hyperlink, you'll notice it's instead redirecting you to myetherwallel.com/two-factor.php - clearly a malicious link. Those two URLs are reasonably different so you may have easily caught the attempt. Many phishers are much brighter, though.

For example, the official URL for MEW is www.myetherwallet.com. Attackers have attempted phishing MEW users by sending them an almost identical URL, www.myėtherwallet.com.

Can you spot the difference here? The only change between the two is that the second URL has a small dot above the first "e." It's a minor change that could go unnoticed to the multitasking eye. Once you click any of these phishing links, you arrive at a malicious website that asks for your information. As these websites typically look identical to their official counterparts, many sucumb to their deceiving tricks. With your credentials in their possession, the thieves then clear out your cryptocurrency wallets.

By massively spamming messages like the one above across multiple channels, the criminals have easy access to unsuspecting victims. It only takes a few dubious individuals to turn a quick profit. A gift and a curse of blockchain, these transactions are irreversible, and the funds are unlikely to be recovered.

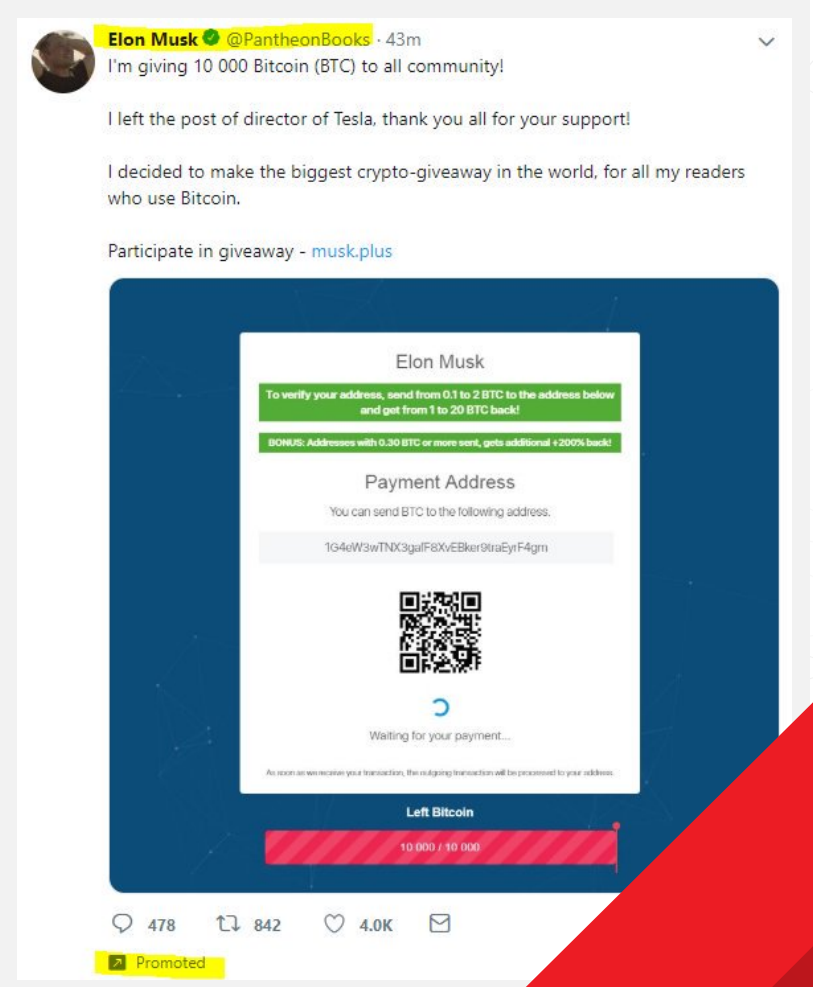
Fake Social Media Accounts

With promises of free tokens or bonus returns, scam artists have used nifty tricks to deceive thousands of social media users as well. They primarily do so by impersonating high-profile individuals on platforms like Twitter and Facebook and directing followers to send them crypto-currency.

Twitter. (Fake) Elon Musk

Fraudsters have hijacked several Twitter posts pretending to be Elon Musk hosting a cryp-to-giveaway. They promise to send all participants a certain amount of cryptocurrency...as long as you send crypto to them first.

The Twitter scam artists go so far as to copy the exact profile picture and Twitter name that Elon Musk uses, some will even try to replicate his Twitter handle using the same strategy as the URL spoofers we explained above. Even scarier, many of these copy-cats are verified on Twitter even though they're not who they say they are.



Source: twitter.com

Same profile picture, name, and verification. Different Twitter handle.

Instagram (Fake Instagram)

Last year, a phony Instagram account for Ethereum co-founder Vitalik Buterin amassed 24,000 followers. The profile held a “giveaway” similar to the Elon Musk Twitter scam, collecting 37 ETH from foolish followers.

To some, scams like these seem laughable. However, thousands of individuals were deceived into sending cryptocurrency with the hopes of making free money. Unfortunately, phishing and social engineering scams racked up almost $2,728,000 worth of cryptocurrency in 2018.

No One Is Safe

When it comes to phishing and social engineering, there’s no end to who thieves will target. Some investors in EOS, a blockchain project with a $4 billion ICO, fell victim to a phishing campaign that amassed millions of dollars. Also, Jaxx, a notable online wallet, faced a copy-cat domain that would replace the wallet address of a user’s recipient with the thief’s personal wallet, stealing the coins from transactions.

Protecting Yourself Against Phishing and Social Engineering

When dealing with social media or company communications, it’s okay to have a healthy dose of paranoia.

Before taking any action, check to make sure every aspect of what you’re reading makes sense. Do the names, pictures, branding, handles, and URLs match exactly what they should be? Is the communication free of any spelling or grammar mistakes? If your answer is “no” to either of these questions, don’t hesitate to reach out to the other party directly or contact customer support to ask for more information.

For additional protection:

NEVER TELL ANYONE YOUR PRIVATE KEY OR LOGIN CREDENTIALS.

DON’T CLICK ON SUSPICIOUS LINKS.

ALWAYS TYPE URLS DIRECTLY INTO YOUR ADDRESS BAR.

IF A DEAL SEEMS TOO GOOD TO BE TRUE, IT USUALLY IS.

Malware/Cryptojacking

Malware activity such as cryptojacking rose a staggering 629 percent in the first quarter of 2018, according to a report published by cybersecurity firm McAfee Labs.

What is cryptojacking?: Cryptojacking is the use of a device's resources to mine cryptocurrency without the device owner's permission. Most of the time, the device owner doesn't even know it's happening.

In the first quarter of 2018 alone, there were over 2.9 million known samples of coin mining malware that infected millions of systems. By using crypto mining malware (which remember, doesn't require an intermediary), criminals can covertly monetize their attacks. Over a billion visitors on hundreds of websites have unknowingly ran crypto mining scripts, and as cryptojacking has a lower likelihood of being discovered than other types of malware, the numbers may continue to rise.

A Harmless Attack?

Because cryptojackers aren't directly stealing funds from their victims, some people see it as a harmless crime. This opinion couldn't be further from the truth.

Many attackers target large corporations with substantial resources (i.e., large servers), and the performance impact on potentially critical business infrastructure can be devastatingly high. Negative effects include:

AN OVERALL SLOWDOWN IN DEVICE PERFORMANCE

DETERIORATION OF DEVICES

INCREASED COSTS DUE TO INCREASED ELECTRICITY USAGE

AN OPEN DOOR FOR OTHER MALWARE

BRAND DAMAGE

Even as an individual, cryptojacking can affect you. Using phishing attacks, or other deceptive tactics, cybercriminals can trick you into downloading and booting malicious software. This software then runs in the background as you operate your laptop. With your computer now constantly mining cryptocurrency, you experience severe performance issues and may not be able to use specific programs.

Another infection method occurs when visiting a website or ad in which a hacker has injected malicious code. As you browse the site, the code harnesses your computer's resources to mine cryptocurrency; it's bad for you, it's terrible for the site, it's a miserable experience for everyone involved, except for the cryptojacker of course. Thankfully, this type of crypto-mining only occurs while your computer displays the website or ad.

Monero - A Popular Choice for Cryptojackers

Due to its anonymous nature, Monero is a common choice for cryptojacking. One example, the Smominru Monero mining botnet, made millions for its operators when in operation. Using a Microsoft Windows software vulnerability, dubbed EternalBlue, the miner spread through devices, earning a total of $3.6 million at the time.

Nearly Undetectable Cryptojacking

Some cryptojacking malware, like PowerGhost, attempt to be completely unnoticeable. To start, PowerGhost silently attaches malware to your workstation. From there, the malware then tries to log in to network user accounts through the legitimate remote administration tool, Windows Management Instrumentation (WMI). After that, it obtains logins and passwords using Mimikatz, a data extraction tool.

PowerGhost is more difficult to detect than typical cryptojacking malware because it doesn't download malicious files to the device. If you don't notice the increased use of your resources, you may never detect it. Malware like this brings additional risk to organizations as it opens up the pathway for rootkits or other malware types to be installed, causing further damage to a business.

How to Avoid Cryptojacking

A lot of cryptojacking malware works tirelessly to be undetectable, so you need to stay vigilant to avoid becoming a victim. If you start to experience performance issues on your computer, take a look at your Task Manager (Windows) or Activity Monitor (Mac).

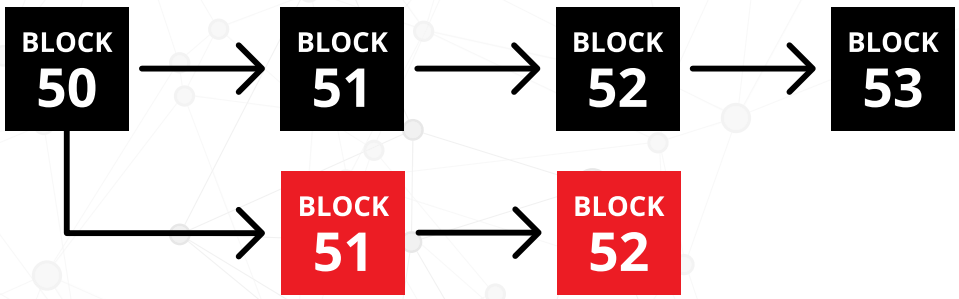
Cryptojackers target CPUs, so check to see if you have any unfamiliar programs with high CPU usage. Most of the time, uninstalling those programs will solve your issue.

There are some tools as well that protect your computer from installing cryptojacking malware in the first place. No Coin and minerBlock are two options you can try out.

51% Attacks

Another blockchain threat is the 51% attack. While previous vulnerabilities have focused on the user, this one is an attack on a blockchain itself. They've drastically affected many different blockchains/coins in 2018 and continue to pose an existential threat to many cryptocurrencies, specifically ones using a Proof-of-Work consensus.

What is a 51% attack? A 51% attack is when a single entity controls the majority of a blockchain's hashrate, "potentially causing a network disruption." Such an attack allows that malicious entity to effectively reverse transactions, leading to the potential of coins to be spent twice (a double-spend). To explain further, a double-spend enables the attacker to obtain coins they just spent and return them to their wallet. Ultimately, the attacker spends coins without actually losing possession, allowing them to pad their wallet with free crypto.



ZenCash, Verge, Monacoin, Bitcoin Gold, and even Ethereum Classic have all suffered 51% attacks in the past year. These, plus several other attacks have led to losses of about $20.8 million.

Verge's Vulnerabilities

The privacy-focused cryptocurrency Verge fell victim to 51% attacks multiple times in 2018. Let's break down the most impactful one:

In April 2018, an attacker successfully forked the Verge blockchain through a 51% attack and exploited a bug that allowed miners to set false timestamps on blocks. With an incorrect time-stamp, they were able to rapidly mine new blocks in quick succession before other miners had a chance to.

Typically, Verge rotates between five mining algorithms to prevent any one type of miner from dominating the hash rate. With this bug, the attacker was able to trick the network into continu-ously accepting proof-of-work from the Scrypt mining algorithm. By abusing the Scrypt algo-rithm, attackers mined coins unbothered while honest miners switched to a different algorithm.

Without miner competition, the bad actor overtook the hash power, mining blocks every second. Within a few hours, the attacker stole approximately 35 million XVG - worth almost $1.75 million at current prices.

The total damage from all of Verge's 51% attacks - $2.85 million.

Protection Against 51% Attacks

As an individual, there's not much you can do to protect yourself against 51% attacks. If you're working with a blockchain, it should be one with a significant hash rate, like Bitcoin, or one that uses a consensus method other than Proof-of-Work.

To get an idea of how costly it is to perform a 51% attack on different blockchains, check out Crypto51. You'll be shocked at some of the costs.

On the blockchain side, there are a few solutions that projects have incorporated, although no solution is perfect. Some projects, like Dogecoin and Elastos, incorporate merged mining into their network. Using merged mining, these two projects effectively piggyback off the hash power of Litecoin and Bitcoin, respectively.

Other projects have ditched Proof-of-Work altogether, capitalizing on a different consensus mechanism. The number of varying consensus methods is seemingly endless, but some of the favorites include Proof-of-Stake, Delegated Proof-of-Stake, and Delayed Proof-of-Work.

Exchange Hacks

Exchanges were one of the most popular targets for cybercriminals in 2018, and that doesn't appear to be changing in 2019. One of the largest cybersecurity heists of all time was due to a cryptocurrency exchange breach.

The Half-Billion Coincheck Hack

In January 2018, Coincheck, one of the most used cryptocurrency exchanges in Japan, was hacked for a record $530 million. Further analysis in Coincheck's history revealed that not only did the exchange conduct notoriously poor security practices, it also wasn't registered with Japan's Financial Service Agency (FSA).

To explain further, Coincheck had two significant security vulnerabilities. First, the platform didn't use a Multi-signature contract smart signing app. Using this protocol provides additional layers of security as it requires multiple exchange managers to sign off on large transactions, without approval from the managers, the transaction fails. If the company implemented this Multisig protocol as the developers requested, this massive theft might have been stopped in its tracks.

Secondly, Coincheck stored all of the exchange's NEM (the stolen coin) in a single hot wallet. A hot, or online, wallet is connected to external networks and susceptible to breaches. Because of this security risk, it is standard practice for cryptocurrency exchanges to store the majority of their funds in cold (offline) wallets.
In Coincheck's case, having a private key stolen from their hot wallet was like the cherry on top of an incredibly unsecure sundae.

Binance - Doing the Right Thing

Binance, arguably the world's most popular cryptocurrency exchange, also experienced a unique type of attack in 2018. In a carefully planned phishing and API attack campaign, someone (or some people) attempted to steal over 96 bitcoins from Binance users.

Through the use of Binance look-a-like phishing websites, hackers accumulated the account credentials of numerous users. The attackers then created an API key for each account and stood by until the ideal time to strike.

In just two minutes on March 7th, the attackers used those API keys to place a large number of market buys on the VIA/BTC market which rapidly pushed the price higher. On the other side, they had 31 pre-deposited accounts waiting there to sell VIA at the top. They then attempted to quickly withdraw their newly obtained BTC from those 31 accounts to a wallet outside the platform.

Thankfully, Binance's risk management system automatically disabled the withdrawals, stopping them from successfully going out. This scenario exhibits the increasing complex attacks malicious individuals develop to steal cryptocurrency. The hackers were well organized, patient, and waited for the most opportune moment act. Fortunately for users, Binance had the right tools in place to prevent a successful attack.

Safeguarding Against Exchange Hacks

Most cryptocurrency exchanges don't have the security rigor that Binance does. When trading on an exchange, you should keep the minimum amount of funds you need to actively trade on the platform. The rest of your money should be kept in a hardware wallet like Ledger or Trezor.

There's an adage in cryptocurrency: Not your keys, not your crypto. Because an exchange controls the private keys to your funds, you may have no recourse in the case of a hack. When deciding which crypto exchange to trade on, you should know their security policies. They should keep the majority of their funds in offline wallets and have redundant forms of protection against large withdrawals. Some exchanges, like Gemini, even provide FDIC insurance for up to $250,000.

Software Flaws (Wallets and DApps)

Even if an underlying protocol (e.g., Bitcoin or Ethereum) is tamper-proof, the products built on top of it may have flaws. Software is bound to have bugs, and blockchain products are no exception.

Software Flaws Can Go Undiscovered for Years

In early 2018, a community member indentified a critical security vulnerability in the popular Electrum wallet that had lain undiscovered for almost two years. Electrum is a free software wallet that numerous cryptocurrency sites, including merchants and exchanges, used to store bitcoin.

The vulnerability allowed the thieves to steal bitcoins from Electrum users who visited certain malicious websites. While the Electrum software was running without an encrypted password, the thieves could continue to steal funds.

The vulnerability was discovered in 2016 but went unpatched until January 2018. It existed in Electrum's JSON-RPC interface, allowing malicious users to execute wallet commands, modify user settings, change the list of contacts in a wallet, and most importantly, edit the payto and amount fields of the Electrum user interface.

Because of the extended period that developers knew about the bug, it's difficult to determine precisely how much was stolen due to it.

Many DApps Lack Security

Due to common security flaws, hackers heavily target decentralized applications (dApps) as well. Simply put, dApps are applications and programs that run on a blockchain instead of a central database.

Gambling dApps were among the hottest targets in 2018, losing over $598,000 to malicious activity.

A Lesson in What Not to Do

EOSBet is a classic example of a dApp with serious security vulnerabilities. Due to bugs in the software's code, hackers targeted the dApp multiple times, making off with around one million dollars.

The first attack against EOSBet drained $236,000 from user accounts. The bug was narrowed down to a faulty assertion statement in the code that allowed the hacker to bypass paying when they lost bets. Using the flaw in the system to their advantage, the attacker ultimately developed a perfect casino scenario in which they never lost money, only won.

Having fixed the bug, and with a promise of increased security auditing of their platform, EOSBet fell victim to another breach. Attackers found another loophole in the code and struck for the second time in October 2018. As seen below, the attackers were able to siphon 65,000 EOS (approximately $338,000 at the time) from the operational wallet of the gambling dApp.

Hackers stole hundreds of thousands of dollars from EOSBet in a matter of minutes.

Source: AMBCrypto

They were able to fool EOSBet's smart contracts into wrongly crediting their accounts with large amounts of cryptocurrency by injecting malicious code into standard EOS accounts. The malicious code injections instantly activated the funds' transfer function, tricking the wallets into matching every transaction with an equivalent amount of cryptocurrency from EOSBet's operational wallet. In a continuous, rapid cycle, the hackers sent transactions among themselves to evoke the wallet's generation of cryptocurrency, effectively draining the EOSBet holdings **in less than a minute.**

Staying Safe With Wallets and DApps

Unfortunately, there's only so much vetting you can do on a wallet and dApp. When researching your choices, it's paramount to read numerous user reviews, checking for any negative reports of bugs or lost funds. Additionally, any wallet or dApp that you decide on should have gone through at least one third-party security audit (if not more). Additionally, if the developers open-source their code then the entire community can audit it. Even with third-party audits and community review some bugs are bound to slip through the cracks. And because blockchain is such a nascent industry, you should always use extreme caution no matter the dApp you operate.

DNS Hijacking

Cryptocurrency wallets have become large targets for thieves with a goal of stealing private keys, login information, and other sensitive data. A favorite tactic of these thieves is DNS hijacking. In this type of attack, an individual forcibly redirects queries to a fraudulent site using the wallet's domain name server (DNS). Once the individual has control of the DNS, they can direct you to a web page that looks identical to the original one but is set up to then steal information or deploy malware.

On January 13th, attackers highjacked the DNS for BlackWallet.co, a web-based wallet application for the Stellar Lumen (XLM) cryptocurrency. The attackers were able to access the host provider account, change the DNS settings to redirect to their malicious website, and steal almost 670,000 Stellar Lumens (around $400,000) from users' accounts. Then, they moved the ill-gotten funds to a cryptocurrency exchange and converted them to another digital currency to evade detection.

DNS Hijacking Avoidance Tips

Unfortunately, if a company's DNS gets hijacked, it's difficult for you to discover and avoid as a regular user. Try to keep an eye out for any differences in a website that you normally visit and be wary of any pop-ups asking for your information.

Additionally, follow the platforms you commonly use on social media and check their messaging platforms periodically. More often than not, community users or an official company representative will post security alerts to one of these channels before publishing an official statement.

FINAL THOUGHTS

As organizations begin to integrate blockchain technology into their fundamental operations, they must not take security threats lightly. In 2018, we saw the creative tactics criminals employ to deceive and steal from users to the tune of **$1,064,176,000.**

Using traditional attacks such as phishing, malware, or DNS-hijacking, hackers keep a steady rhythm of malicious activity in the blockchain world. Not only do they target users, but large exchanges have fallen victim to massive breaches as well. Risk assessments of different applications and software surrounding blockchain technology need to be adequately conducted to assist in the development of a more secure industry.

Evaluating the errors made in many of the breaches throughout 2018 allows us as an industry to develop a stronger and more secure environment for all parties involved. Without this higher level of security and accountability, blockchain will continue to face trouble getting the adoption that it truly deserves.

Works Cited

Andrew, Paul. "Verge Suffers 51% Attack, Hard Forks in Response." CoinCentral, CoinCentral, 5 Apr. 2018, coincentral.com/verge-suffers-51-attack-hard-forks-in-response/.

Avan-Nomayo, Osato. "51 Percent Attack: Hackers Steals $18 Million in Bitcoin Gold (BTG) Tokens." Bitcoinist.com, 26 May 2018, bitcoinist.com/51-percent-attack-hackers-steals-18-milion-bitcoin-gold-btg-tokens/.

Barth, Bradley. "Malicious Websites Steal from Vulnerable Electrum Cryptocurrency Wallets." SC Media UK, 9 Jan. 2018, www.scmagazineuk.com/malicious-websites-steal-vulnerable-electrum-cryptocurrency-wallets/article/1473512.

Binance. "Summary of the Phishing and Attempted Stealing Incident on Binance." Binance, Feb. 2018, support. binance.com/hc/en-us/articles/360001547431.

Binance. "What Is a 51% Attack?" What Is a 51% Attack?, www.binance.vision/security/what-is-a-51-percent-attack.

Bitcoin Exchange Guide News Team. "6 Crypto Coin Tokens Got Attacked Via The 51% Blockchain Hack In 2018." BitcoinExchangeGuide, 19 Sept. 2018, bitcoinexchangeguide.com/6-crypto-coin-tokens-got-attacked-via-the-51-blockchain-hack-in-2018/.

Bitcoin Exchange Guide News Team. "EOS Phishing Scam: Users Beware of Fraudulent EOS Token Emails Asking For Private Keys." bitcoinexchangeguide.com/eos-phishing-scam-users-beware-of-fraudulent-eos-token-emails-asking-for-private-keys/.

BlockchainHub. "Blockchain Glossary." BlockchainHub, BlockchainHub, blockchainhub.net/blockchain-glossary/.

Bloomberg, Jason. "Cryptojacking Displaces Ransomware As Most Popular Cyberthreat." Forbes, Forbes Magazine, 3 Aug. 2018, www.forbes.com/sites/jasonbloomberg/2018/07/29/cryptojacking-displaces-ransomware-as-most-popular-cyberthreat/#652b9f6f86e9.

Bloomberg. "How Hackers Stole $500 Million in Digital Currency." Fortune, Fortune, 31 Jan. 2018, fortune.com/2018/01/31/coincheck-hack-how/.

Bluetower, Danielys. "EOS Bet Hacked Again: Attackers Siphon $338,000 in Funds from the DApp." ELEVENEWS, 18 Oct. 2018, elevenews.com/2018/10/18/eos-bet-hacked-again-attackers-siphon-338000-in-funds-from-the-dapp/.

Burgess, Matt. "Everything You Need to Know about EternalBlue – the NSA Exploit Linked to Petya." WIRED, WIRED UK, 29 June 2017, www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch.

Burgess, Matt. "Everything You Need to Know about EternalBlue – the NSA Exploit Linked to Petya." WIRED, WIRED UK, 29 June 2017, www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch.

Cimpanu, Catalin. "Hackers Hijack DNS Server of BlackWallet to Steal $400,000." BleepingComputer, BleepingComputer.com, 15 Jan. 2018, www.bleepingcomputer.com/news/security/hackers-hijack-dns-server-of-blackwallet-to-steal-400-000/.

Coign, Biht. "Come on @Twitter @TwitterSupport ??This Is a Blatant Scam Which Is Being Promoted by Twitter and by Other Potencially Hacked or Impersonating VERIFIED Accounts.tweet: Https://T.co/ZHZxWAxtbrcc: @Elonmusk @Cointelegraph @Coindesk @ADCuthbertson @Verified @BillyBambrough Pic.twitter.com/DOC4uVlH5w." Twitter, Twitter, 5 Nov. 2018, twitter.com/abztrdr/status/1059446327355105280.

Comben, Christina. "$1 Billion Dollar's Worth of Cryptocurrency Stolen in 2018." CCN, CCN, 12 Dec. 2018, www.ccn.com/1-billion-dollars-worth-of-cryptocurrency-stolen-in-2018/.

Curran, Brian. "The History of The Coincheck Hack: One of The Largest Heists Ever." Blockonomi, 21 Dec. 2018, blockonomi.com/coincheck-hack/.

Cuthbertson, Anthony. "Elon Musk Bitcoin Scam on Twitter Sees Hundreds of People Lose Thousands of Dollars." The Independent, Independent Digital News and Media, 6 Nov. 2018,
www.independent.co.uk/life-style/gadgets-and-tech/news/elon-musk-bitcoin-scam-twitter-hackers-cryptocurrency-a8620436.html.

FMF. "A 51% Attack Happened- How Did It Happen to Bitcoin Gold?" Medium.com, Medium, 1 June 2018,
medium.com/formosa-financial/a-51-attack-happened-how-did-it-happen-to-bitcoin-gold-da131a8080a6.

Franceschi-Bicchierai, Lorenzo. "Electrum Bitcoin Wallets Were Vulnerable to Hackers for Two Years." Motherboard, VICE, 8 Jan. 2018,
motherboard.vice.com/en_us/article/ev55na/electrum-bitcoin-wallets-were-vulnerable-to-hackers-for-two-years-json-rpc.

Hope, Computer. "What Is DNS Hijacking?" DNS Hijacking, 30 Oct. 2017, www.computerhope.com/jargon/d/dnshijac.htm.

Huillet, Marie. "'Infect and Collect': Cryptojacking Up 629% in Q1 2018, Says McAfee Report." Cointelegraph, Cointelegraph, 21 Jan. 2019,
cointelegraph.com/news/infect-and-collect-cryptojacking-up-629-in-q1-2018-says-mcafee-report.

Jose, Febin. "EOS-Based Gambling DApp EOSBet Hacked Again; $338,000 Stolen from Operational Wallets." AMBCrypto, AMBCrypto, 16 Oct. 2018,
ambcrypto.com/eos-based-gambling-dapp-eosbet-hacked-again-338000-stolen-from-operational-wallets/.

KAFEINE. "Smominru Monero Mining Botnet Making Millions for Operators." Proofpoint, 14 Dec. 2018,
www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators.

Khatri, Yogita. "Nearly $1 Billion Stolen In Crypto Hacks So Far This Year: Research." CoinDesk, CoinDesk, 18 Oct. 2018,
www.coindesk.com/nearly-1-billion-stolen-in-crypto-hacks-so-far-this-year-research.

Lab, Kaspersky. "PowerGhost: Beware of Ghost Mining." PowerGhost: Beware of Ghost Mining, 30 Jan. 2018,
www.kaspersky.com/blog/powerghost-fileless-miner/23310/.

Lanz, Jose Antonio. "Fake Phishing Website Mimicking Jaxx Wallet Shut Down." Ethereum World News, 14 Sept. 2018,
ethereumworldnews.com/fake-jaxx-phishing-website-shut-down/.

Maloney, Conor. "Cryptojacking Is up 459% in 2018, and It's the NSA's Fault." CCN, CCN, 20 Sept. 2018,
www.ccn.com/cryptojacing-is-up-459-in-2018-and-its-the-nsas-fault/.

Malwa, Shaurya. "Binance Suffers Massive API Attack Causing Hackers to Sell One Syscoin for Over 96 Bitcoins." BTCMANAGER, 28 Aug. 2018,
btcmanager.com/binance-api-attacked-as-hackers-sell-one-syscoin-for-96-bitcoins/.

Munkachy, Alex. "30+ Cryptocurrency Exchange Hacks - A Comprehensive List." CoinIQ, 29 Sept. 2018,
coiniq.com/cryptocurrency-exchange-hacks/#2018.

Nadeau, Michael. "What Is Cryptojacking? How to Prevent, Detect, and Recover from It." CSO Online, CSO, 13 Dec. 2018,
www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html.

O'Neill, Patrick Howell. "Monero Mining Botnet 'Smominru' Earns Hackers $3.6 Million." Cyberscoop, CyberScoop, 31 Jan. 2018,
www.cyberscoop.com/monero-botnet-smominru-proofpoint/.

Osborne, Charlie. "2018's Most High-Profile Cryptocurrency Catastrophes and Cyberattacks." ZDNet, ZDNet, 21 Jan. 2019,
www.zdnet.com/article/2018s-most-high-profile-cryptocurrency-catastrophes-ico-failures-and-cyberattacks/.

Osborne, Charlie. "Jaxx Wallet Phishing Campaign Aimed to Steal User Cryptocurrency." ZDNet, ZDNet, 13 Sept. 2018,
www.zdnet.com/article/jaxx-cryptocurrency-wallet-phishing-campaign-empties-user-wallets/.

Pollock, Darryn. "Story of Coincheck: How to Rebound After the 'Biggest Theft in the History of the World'." Cointelegraph, Cointelegraph, 3 Apr. 2018,
cointelegraph.com/news/story-of-coincheck-how-to-rebound-after-the-biggest-theft-in-the-history-of-the-world.

Schuster, Brian. "Know Your Cryptocurrency Scams: Phishing Scams – Hivergent." Hivergent, 19 Sept. 2017,
hivergent.com/know-cryptocurrency-scams-phishing-scams/.

Suberg, William. "Cryptocurrency Mining Malware Detections Up Almost 500 Percent in 2018: Report." Cointelegraph, Cointelegraph, 21 Jan. 2019, cointelegraph.com/news/cryptocurrency-mining-malware-detections-up-almost-500-percent-in-2018-report.

Team, Changelly. "Phishing in Cryptocurrency: How to Avoid Scams and Save Your Money." Medium.com, Medium, 23 Mar. 2018, medium.com/@Changelly/phishing-in-cryptocurrency-how-to-avoid-scams-and-save-your-money-d3d1b442a16a.

Team, Changelly. "Phishing in Cryptocurrency: How to Avoid Scams and Save Your Money." Medium.com, Medium, 23 Mar. 2018, medium.com/@Changelly/phishing-in-cryptocurrency-how-to-avoid-scams-and-save-your-money-d3d1b442a16a.

Terlato, Peter. "$673 Million Stolen in Crypto Hacks in 2018." Finder US, Finder US, 18 Oct. 2018, www.finder.com/673-million-stolen-in-crypto-hacks-in-2018.

Wieczner, Jen. "Hackers Are Stealing From This $4 Billion Cryptocurrency ICO Using This Sneaky Scam." Fortune, Fortune, 31 May 2018, fortune.com/2018/05/31/cryptocurrency-eos-ico-scam/.

Wilmoth, Josiah. "Privacy Coin Verge Succumbs to 51% Attack [Again]." CCN, CCN, 22 May 2018, www.ccn.com/privacy-coin-verge-succumbs-to-51-attack-again/.

LEDGEROPS

LEDGEROPS.COM

CONTACT@LEDGEROPS.COM