CYMULATE

CRYPTOCURRENCY UNDER ATTACK
THE CUNNING WAYS CYBERCROOKS OPERATE

February 2018

"MONEY IS THE ROOT OF ALL EVIL"

CYMULATE

TABLE OF CONTENT

GLOSSARY

BAS platform	Breach & Attack Simulation platform
ICO	Initial Coin Offering

TABLE OF FIGURES

1 / INTRODUCTION

Since its inception in 2009, cryptocurrency (defined as any kind of peer-to-peer digital money powered by the blockchain technology) has made its mark in the financial market challenging conventional legal tenders that are controlled by central banks. (For a short history of cryptocurrency, see Appendix I). The most prominent cryptocurrency is Bitcoin (CTC). Others include XRP, Litecoin (LTC), Ether (ETH), Ripple, Dogecoin, and Onecoin. They are bought and sold via exchanges such as Bitstamp. Although they are under pressure from new rules banning anonymous trading and new digital currency regulations, they are still doing well. Bitcoin and Litecoin are listed on NASDAQ, hedge funds are investing in them, and Perth Mint announced in January 2018 that it is developing its own gold-backed cryptocurrency. Even banks such as Barclays, Citi Bank, Deutsche Bank and BNP Paribas are investigating ways they might be able to work with Bitcoin.

Although cryptocurrencies took a hit across the board during January 2018 and had a roller coaster ride during 2017, they still remain in demand for various reasons: (1) the secure transactions bypass traditional institutions, (2) there are no intermediaries to broker deals, (3) there are no credit bureaus involved that track activities to build financial trustworthiness profiles.

But everything of value is vulnerable, and it did not take cybercriminals and rogue nations long to hack, attack and hijack cybercurrencies.

CRYPTOCURRENCY CYBERATTACKS			
Date	Target	Attack	Result
Jan 2014	Mt.Gox, the world's largest Bitcoin exchange	Hackers gained access by compromising the computer belonging to an auditor of the company	850,000 Bitcoins were stolen (with a market value of ~ $64.5 million at January 2014 prices). Mt.Gox went bankrupt.
Aug 2016	Bitfinex was hacked	Hackers managed to get hold of the private keys held by Bitfinex	119,756 bitcoins were stolen (with a market value of ~$75 million at August 2016 prices). The U.S. Commodity Futures Trading Commission ordered Bitfinex to pay a $75,000 fine for offering illegal off-exchanged financed commodity transactions.
During 2017	Cryptocurrency exchange Bitthumb	North Korean hackers were behind attacks on cryptocurrency exchanges	Cryptocurrency with a value at that time of $6.99 million was stolen
Apr 2017	Cryptocurrency exchange YouBit	North Korean hackers used malware	4,000 Bitcoins were stolen, equal to 17% of the crypto assets. The exchange filed for bankruptcy.
Dec 2017	Slovenian mining marketplace NiceHash	Professional attackers used sophisticated social engineering	Approximately 4,700 bitcoin were stolen with a market value of close to $64M (at December 7, 2017 prices)
Jan 2018	Cryptocurrency exchange Coincheck was hacked	Hackers exploited Coincheck's security weaknesses	$500 million in NEM coins were stolen

Figure 1 - Cryptocurrency Cyberattacks

2 / THE THREE-PRONGED CRYPTOCURRENCY CRIME SPREE

As we have seen during the last few years, cybercriminals target three groups of victims:

1. CRYPTOCURRENCY OWNERS

Cryptocurrency owners are defrauded in three ways:

- **Ransom**- Hackers demand ransom to be paid in bitcoin for removing their ransomware from locked down PCs. To illustrate, a variant of CryptXXX will only decrypt computer files after paying the hackers a ransom of $500 in bitcoins. As we are seeing now, the volatility of bitcoin a combined with the lack of full anonymity, cybercrooks are turning to alternative cryptocurrency, such as Monero, Ethereum, and Zcash.
- **Breaking and entering** into the account of cryptocurrency holders - To illustrate, hackers gained control of a cryptocurrency owner's phone number. Which enabled them to change the password on one of the victim's cryptocurrency accounts and steal 1,000 OmiseGo (OMG) tokens and 19.6 BitConnect coins. The hackers then exchanged the coins for 2.875 Bitcoin and transferred it out of his account. The price of Bitcoin at the time was $7,118.80, which means that if the hackers cashed out the same day, they would have netted a profit of $20,466.55.
- **Scams** - In February 2018, hackers started scamming people on Twitter by closely mimic the verified accounts of well-known figures such as Elon Musk, John McAfee, or Ethereum cofounder Vitalik Buterin. In a tweet, they claim that they will send a significant quantity of cryptocurrency (e.g., 0.2 Ethereum which is ~ $1700) to anyone who sends a smaller amount of currency (e.g., 0.02 Ethereum which is ~ $ 170) to a particular wallet. The scam has already raked in thousands of dollars of Ethereum and bitcoin in less than a week.

Figure 2 - Scam Using Counterfeit Twitter Account

2. CRYPTOCURRENCY EXCHANGES / MINING MARKET PLACES

To keep cryptocurrencies safe, currency exchanges and market places need to keep the currencies safe. There are two main ways of doing this:

- **Multi-signature security**, a measure requiring multiple sign-offs before funds can be moved.
- **Cold wallet vs hot wallet.** It is best to use a cold wallet (a physical device, such as a USB flash drive, that is disconnect from the web and can be plugged in when needed) instead of a hot wallet which is an internet-connected account.

To illustrate how effective hacking cryptocurrency exchanges can be, let's have a look at the January 2018 Coincheck hack. Hackers (rumored to be state sponsored by North Korea) stole 523 million units of the cryptocurrency NEM, exceeding the US$480 million in virtually currency stolen in 2014 from another Japanese exchange, MtGox. Following the hack, Japanese authorities conducted search Coincheck's offices. The government will also strengthen its supervision of virtual currency exchanges.

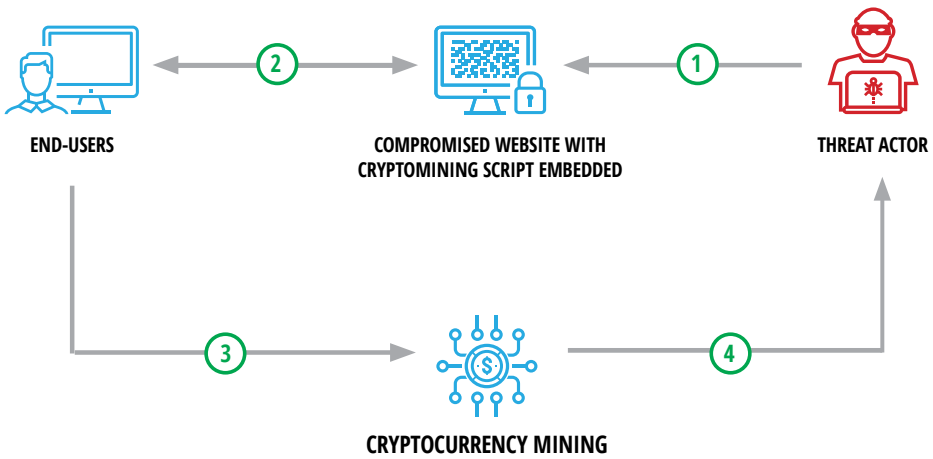
3. COMPUTER OWNERS FOR CRYPTOMINING RESOURCES

Hackers use "cryptojacking" to use their victims' computing devices to mine cryptocurrency without their victims even being aware of the attack. Although this attack vector in itself is not entirely new, it is still highly effective and has surged during the last months of 2017. Hackers abuse the cryptocurrency boom to mine Bitcoins, Litecoins, Ethereum, and Ripple, Iota as well as other cryptocurrencies. Cryptojackers use JavaScript on a legitimate webpage to mine digital cash. Since JavaScript is used on almost about every website, the JavaScript code responsible for in-browser mining doesn't need to be installed. This way, the cybercrooks are sure that their victims will not even notice that their computers are secretly abused to mine cryptocurrency.

As it looks now, 2018 is going to be the year of cryptojacking. The reason is clear, for cybercriminals, cryptojacking is more profitable than ransomware. The latter requires victims to pay ransom in amounts that many cannot afford. Of all the malware attacks used, cryptojacking is by far the easiest and most efficient one. It doesn't require a download, starts instantly, and works like a charm. Furthermore, it's easy to install the mining malware on legitimate websites such as Politifact and Showtime. (figure 3) To illustrate how easy it is, we only have to look the hacker who manipulated the Wi-Fi system of Starbucks in Buenos Aires delaying the connection in order to mine the cryptocurrency Monero with shoppers' devices. Once cybercrooks hijack a website or a public Wi-Fi network to mine cryptocurrency in the background, entire networks of devices across the internet can be hacked. Even if no currency is stolen, the cryptojacking will still damage individual computers or mobile devices since the malware uses so much power that it can overwork the processors.

To complicate things even further, harnessing other peoples' processing power without their permission is not illegal for two reasons. Firstly, no malware enters their systems. Secondly, the script itself doesn't create a permanent vulnerability for exploitation by other cybercrooks.

In its October 2017 report "A look into the global 'drive-by cryptocurrency mining' phenomenon", Malwarebytes identified the US and Spain as the countries that are most impacted by drive-by mining.



Steps

1. The threat actor compromises a website
2. Users connect to the compromised website and the cryptomining script executes
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

Figure 3 - How Cryptojacking Works

3 / THE CYMULATE ASSESSMENT

To protect users and organizations, it is important to check regularly if the organization's infrastructure has been compromised. Since social engineering remains popular, organizations need to be vigilant and make sure that their employees will not fall victim to emails containing malware or phishing attacks that will trick them in downloading the malicious cryptomining script or other scams using social engineering. By using the Cymulate platform, enterprises can run simulations anytime and from anywhere to check how resilient their infrastructure is against such attacks.

As *Figure 4 - The Cymulate Testing Procedure* shows, the testing consists of three steps resulting in a comprehensive multi-vector threat validation report outlining the vulnerabilities that need to be mitigated.

Figure 4 - The Cymulate Testing Procedure

ABOUT CYMULATE

Cymulate helps companies to stay one step ahead of cyber attackers with a unique breach and attack simulation platform that empowers organizations with complex security solutions to safeguard their business-critical assets. By mimicking the myriad strategies hackers deploy, the system allows businesses to assess their true preparedness to handle cyber security threats effectively. An on-demand SaaS-based platform lets users run simulations 24/7 from anywhere, shortening the usual testing cycle, and speeding up time to remediation. Cymulate was established in 2016 by former IDF intelligence officers and leading cyber researchers with extensive experience in offensive cyber solutions. The company serves a broad range of industries, including finance, health care, and telecommunication.

www.cymulate.com

APPENDIX I
THE HISTORY OF CYBERCURRENCY

2008

Satoshi Nakamoto published a paper called "Bitcoin – A Peer to Peer Electronic Cash System" discussing cryptography.

2009

Bitcoin is launched, allowing the general public to mine Bitcoins. Transactions are recorded and verified on the blockchain.

2010

Bitcoin is valued for the first time by people paying for two pizzas with 10,000 Bitcoins. (Fun fact: those 10,000 Bitcoins were worth more than $100 million at the end of 2017).

2011

Rival cryptocurrencies emerged, starting to take market share away from Bitcoin as shown in the graph from the Global Cryptocurrency Benchmarking Study 2017 of the University of Cambridge below.

2014

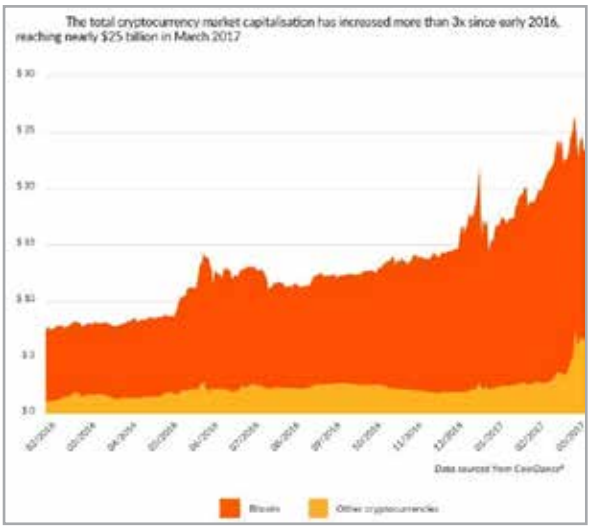
The number of scams and hacks increased since cryptocurrencies became an attractive and lucrative target for criminals. In January 2014, the world's largest Bitcoin exchange Mt.Gox went offline, and the owners of 850,000 Bitcoins lost all.

2016

Ethereum, which uses cryptocurrency to facilitate blockchain-based smart contracts and apps, entered the market. The first ICOs were issued. These are fundraising platforms offer investors the chance to trade what are often essentially stocks or shares in startup ventures, in the same manner that they can invest and trade cryptocurrencies.

2017

Bitcoin reached its all-time high of around $19,500 in December 2017.



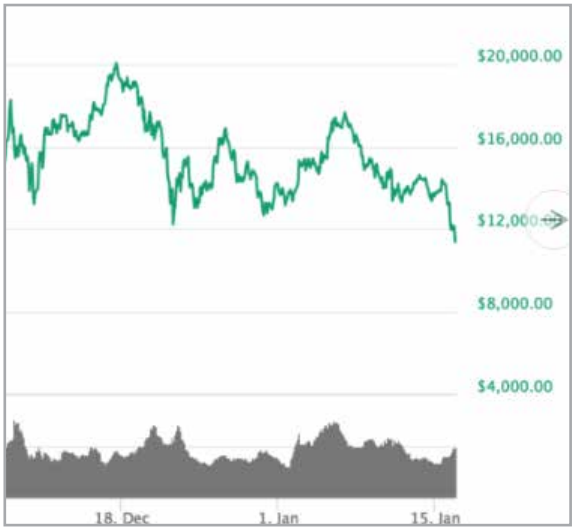


Figure 5 - Bitcoin Performance