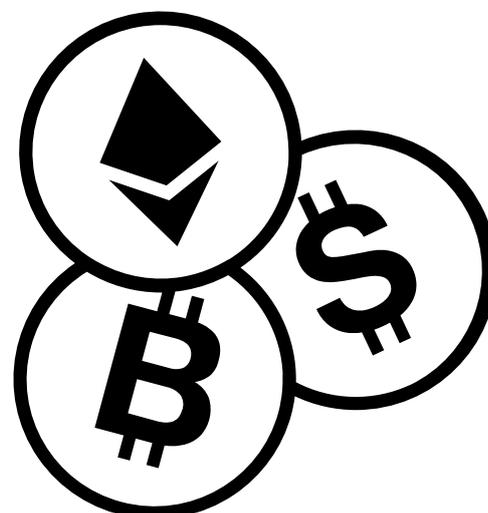


Cybercriminal interest in cryptocurrencies

Date: May 18 (update)

Version: 2.0

Authors: OSINT Unit –
Part of the Orange Cyberdefense
Epidemiology Lab



Abstract

According to Hacked, in an information taken over by Malwarebytes, an estimated **10 to 20 percent of all Bitcoin (BTC) in existence is held by criminals**¹. Illegal activities in the cyberspace usually go more unnoticed than criminal activity in the real world. Collecting evidence of an illegal activity is complicated, since cyber spooks can hide behind numerous anonymous accounts and cryptocurrency allows relative untraceable transactions. **Cryptocurrencies can be used to get rid of existing banking regulations.**

Cryptocurrencies are born with the creation of Bitcoin in 2009, a “peer-to-peer electronic cash system”. Bitcoin was a response to the “too big to fail” banks because it operated outside of a central authority, with no server and no one entity running the show.

Unlike "ordinary" currency, cryptocurrency is entirely virtual and not managed by a bank or a central authority but by a technology called “**Blockchain**”, a register that records all the transactions made and publicly available.

Cryptocurrencies, and notably Bitcoin, have often been qualified of “**safe haven**”, considered by some investors as stable assets that are less correlated/not very sensitive to the current market conditions. However, in the context of the **COVID-19 pandemic**, Bitcoin has been facing its **first major economic crisis** and has fallen by 60%.



Source : <https://tradingview.com>

¹ <https://hacked.com/biggest-bitcoin-hacks-thefts-time/>

<https://blog.malwarebytes.com/101/2017/11/cryptocurrency-works-cybercriminals-love/>

Transactions observed on illicit markets have also declined. Bitcoin then seemed to return to its pre-crisis value and even passed the symbolic \$10,000 (€9236) threshold as of May 8, 2020. The **halving that happened on May 11, 2020** (an operation that halves the block reward per block created) **has allowed the prices to go up again**, similarly to what happened during the two previous halving events of 2012 and 2016. The price went down to €8070 on May 10, 2020 (just before the halving) and has started to increase again on May 12, 2020. It is now reaching €9034 (May 18, 2020). **The final evolution of the price after the halving will have to be followed throughout the year 2020, or even 2021.**

Anyway, the significant drop observed in March 2020 is over and this **has not totally called into question Bitcoin's capacity to be a safe haven, since it is a medium and long-term investment.**

Bitcoin is **the most used currency on illicit markets and by cybercriminals** for various reasons. It seems to be the preferred currency for criminals among the 2500 cryptocurrencies existing (as of May 18, 2020), even though it can be **interesting to have a diversified portfolio** with different "classes" of cryptocurrencies because of the market capitalization².

Some **ransomware operators have also started to accept other cryptocurrencies** than Bitcoin to make it harder for law enforcement to track ransom payments, such as REvil/Sodinokibi that switched to the well-known untraceable cryptocurrency "Monero". We have also observed **"partnerships" between ransomware operators** in order to maximize the stolen money.

Looking at the fluctuation of the market capitalization of BTC, our OSINT Unit may suggest **a two-way correlation between the major ransomware campaigns and the BTC price**. It is yet difficult to prove it with certainty, partly because the number of transactions in BTC and the amount of money involved are so huge that it can be hard to see the influence of ransomware campaigns on the BTC price. However, it is possible that the sums involved and/or the good timing and trading skills of the attackers could impact the crypto market, with the aim of making a profit and building up a reserve of money for their activities.

Before reading

Based on NATO's codification of information scoring (see the appendice in section 10), the OSINT Unit of Orange Cyberdefense aims to be as exhaustive as possible and seeks to develop hypothesis that are considered to be the most likely.

The sources of this report mainly come from Open Source Intelligence and are considered from reliable to fairly reliable by the OSINT Unit.

Information have always been cross-checked, unless specifically mentioned in the text.

² A useful metric to know the total value of cryptocurrency: it is the product of the coin's circulating supply and the price of each coin.

Table of content

Abstract – Pharmaceutical Sector	1
1 Introduction	5
2 Cryptocurrencies: a revolution with the Blockchain technology	6
2.1 What is cryptocurrency?	6
2.2 The Blockchain technology	6
3 How can people get Bitcoin?	7
3.1. Exchanging "common" currency for Bitcoin	7
3.2. Being paid in Bitcoin rather than in currency	8
3.3. Bitcoin can be "mined"	8
4 Bitcoin, a safe haven?	9
4.1 Gold vs. Bitcoin	9
4.2 The special case of the COVID-19 pandemic.....	11
5 Why is Bitcoin so popular among criminals?	14
6 Bitcoin or Altcoins?	16
6.1. The Bitcoin dominance	16
6.2. A diversified portfolio reduces risks and potentially allows more benefits	18
6.3. The use of other cryptocurrencies to hide money trail	19
7 “Partnerships” for ransoming: Emotet, TrickBot & Ryuk	21
8 Does BTC market capitalization fluctuate because of ransomware?	22
8.1. CryptoLocker	22
8.2. Locky	23
8.3. Ryuk	24
8.4. WannaCry	26
8.5. REvil	27
8.6. GandCrab	28
8.7. Maze	29
8.8. DoppelPaymer	30
8.9. Conclusion and Hypothesis	32
9. Conclusion of our OSINT Unit	33
10 Appendices	34
10.1. Selected Repository for the Classification of Sources and Information	34
10.2. Disclaimer.....	35

1 Introduction

While ransomware such as WannaCry, NotPetya, Locky or Ryuk have received strong media coverage, ransomware have not always required a payment in Bitcoin or in another cryptocurrency. In 1989, the trojan called “AIDS” encrypted the names of files and folders and imposed its victims to pay a ransom of \$189 in hard cash addressed to a post office box in Panama³:

```
Dear Customer :

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue
```

Source : [https://en.wikipedia.org/wiki/AIDS_\(Trojan_horse\)](https://en.wikipedia.org/wiki/AIDS_(Trojan_horse))

It is only in 2013 that CryptoLocker was probably the first successful broadcast to demand a Bitcoin ransom against a key to decrypt the victims' files and partitions.

Many ransomware have used traditional methods, such as bank transfers or transfers via Western Union to collect the ransom, but anonymous means of payment have greater advantages. Prepaid cards are good candidates but cryptocurrencies are even better.

Cryptocurrency is mainly used to get rid of existing banking regulations. Traditional paper money poses a lot of problems for cybercriminals, since some banking regulations such as “KYC” (Know Your Customer⁴) and “AML” (Anti Money Laundering)⁵ can induce banks to block or freeze funds in case of suspicious transactions, with the knowledge of the account owner.

That is why we want to understand why cryptocurrencies are so popular among cybercriminals and if criminal activities have an influence on the BTC price (“market capitalization”).

³ <https://www.zdnet.fr/actualites/ransomware-et-cryptomonnaies-jamais-l-un-sans-l-autre-39893607.htm>

⁴ Know Your Customer: The know your customer or know your client (KYC) guidelines in financial services requires that professionals make an effort to verify the identity, suitability, and risks involved with maintaining a business relationship.

⁵Anti Money Laundering: Anti-money laundering refers to a set of laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income.

2 Cryptocurrencies: a revolution with the Blockchain technology

2.1 What is cryptocurrency?

In the wake of Occupy Wall Street and the economic crash of 2008, Satoshi Nakamoto (an anonymous person using a pseudonym) created Bitcoin, a “peer-to-peer electronic cash system.” Bitcoin was a response to the “too big to fail” banks because it operated outside of a central authority, with no server and no one entity running the show⁶. The goal was to eliminate the “middle-man” in order to cancel interest fees, make transactions transparent and fight corruption.

Unlike "ordinary" currency, such as the euro or the dollar, cryptocurrency is not issued in the form of material coins or notes. It is entirely virtual. The money we use every day is linked to governments and central banks that are responsible for its creation and regulation. Cryptocurrency is not managed by a state or a central bank but is still regulated by using a technology called "Blockchain".

2.2 The Blockchain technology

On the one hand, transactions in “real money” are monitored by an intermediary. It verifies that the buyer has the money to pay for what he buys, and thus guarantees the sustainability of the system.

On the other hand, Blockchain technology could be defined as a register that records all the transactions made and publicly available. It is composed of "blocks", which are used to record new exchanges and new data, and "chains", which link the "blocks" together. With this technology, it is impossible to carry out a fake cryptocurrency transaction.

For instance, it is impossible to pay someone in Bitcoin (the most famous cryptocurrency) if you don't have it in your "wallet". The entire history of transactions since the beginning of Bitcoin is written down and the Blockchain certifies whether or not you have Bitcoin in your wallet.

⁶ <https://blog.malwarebytes.com/101/2017/11/cryptocurrency-works-cybercriminals-love/>

3 How can people get Bitcoin?

3.1. Exchanging "common" currency for Bitcoin

Similar to an exchange office, it is possible to carry out an exchange of "common currency" into Bitcoin. For your information, the value of Bitcoin in January 2013 was 1 Bitcoin for 13 euros. In 2018, this value ranged between 3,000 and 4,000 euros. Today, it is estimated that one Bitcoin amounts to more or less 9000 euros (May 18, 2020).



Here is the variation of Bitcoin (in USD) from 2012 to today.

Source : <https://www.abcbourse.com/graphes/eod.aspx?s=BTCUSDu>

All cryptocurrency investors use an "exchange", a marketplace dedicated to crypto-currencies, in order to exchange crypto-assets for fiat currencies or other crypto-currencies. Some of the best known "exchanges" include Coinbase, Binance, Kraken, bitFlyer, LocalBitcoins, Coinhouse, Bittrex, Cex.io, BitStamp and BitFinex⁷. This list is of course not exhaustive.

⁷ <https://cryptoast.fr/qui-controle-possede-exchange-crypto/>

3.2. Being paid in Bitcoin rather than in currency

Bitcoin can be a means of payment for goods and services in some sectors.

3.3. Bitcoin can be "mined"

As we discussed it, the verification of transactions is not carried out by a large institution but by the "community" securing the blockchain. Computers (not people) "constantly" check transactions. These computers were first owned by individuals ("volunteers") but most of them now belong to business and crypto investors.

New Bitcoins are created every 10 minutes and distributed to these "miners" who make their computers available for "mining". Special hardware specification and software have to be set up on the computer, but there are also dedicated systems (called "ASIC") only made/used for mining activities. In exchange, these "volunteers" are paid in fractions of Bitcoins – but only for the miner who "validates" the block.

Note that the difficulty to mine depends on the miners' activities. That is why some "miners" come together to create "pools" of mines to gather their forces and share benefits (if a miner from a pool validates a block, the amount of BTC earned is distributed to all the pool contributors depending on the amount of work done by each one).

4 Bitcoin, a safe haven?

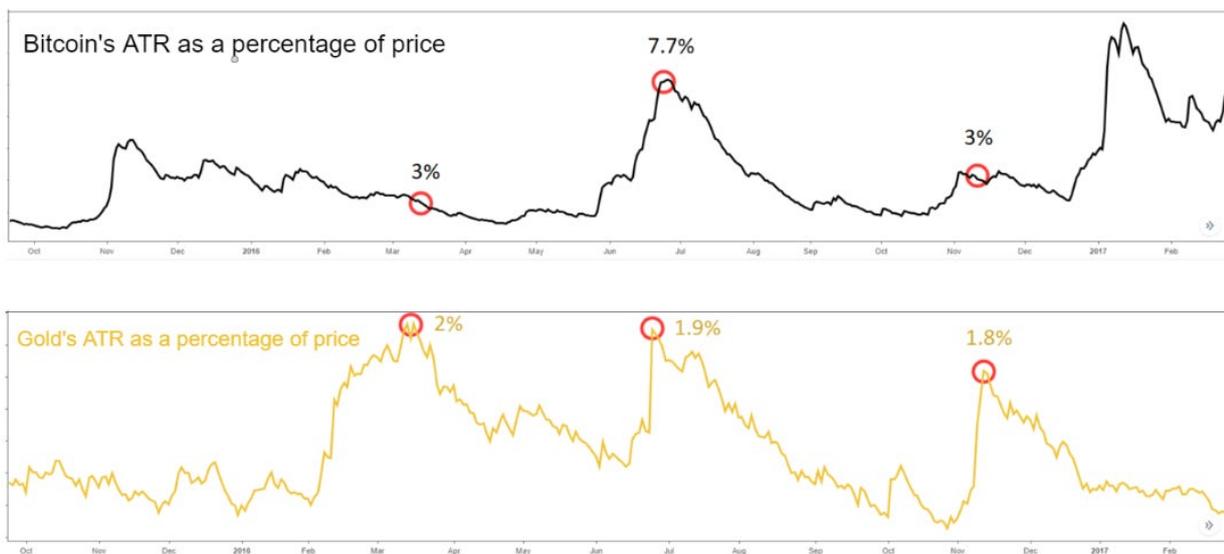
4.1 Gold vs. Bitcoin

Since the creation of cryptocurrencies and notably Bitcoin in 2009, they have often been qualified of "safe haven".

Safe havens are considered by some investors **as stable assets that are less correlated/ not very sensitive to current market conditions**. Gold is considered as a safe haven. Actually, "unlike the ordinary currencies we use on a daily basis, most crypto-currencies are designed so that the creation of new currency units is gradual. Of course, this currency has a ceiling on the money supply that will eventually be in circulation. The aim is to imitate the scarcity of precious metals, in order to increase value and avoid hyperinflation".⁸

Gold and Bitcoin are not infinite values and both **have secure storage** (vaults for gold and wallets for Bitcoin).

One of the major differences comes from the **much higher volatility of Bitcoin**, as shown in the following study in 2016.⁹



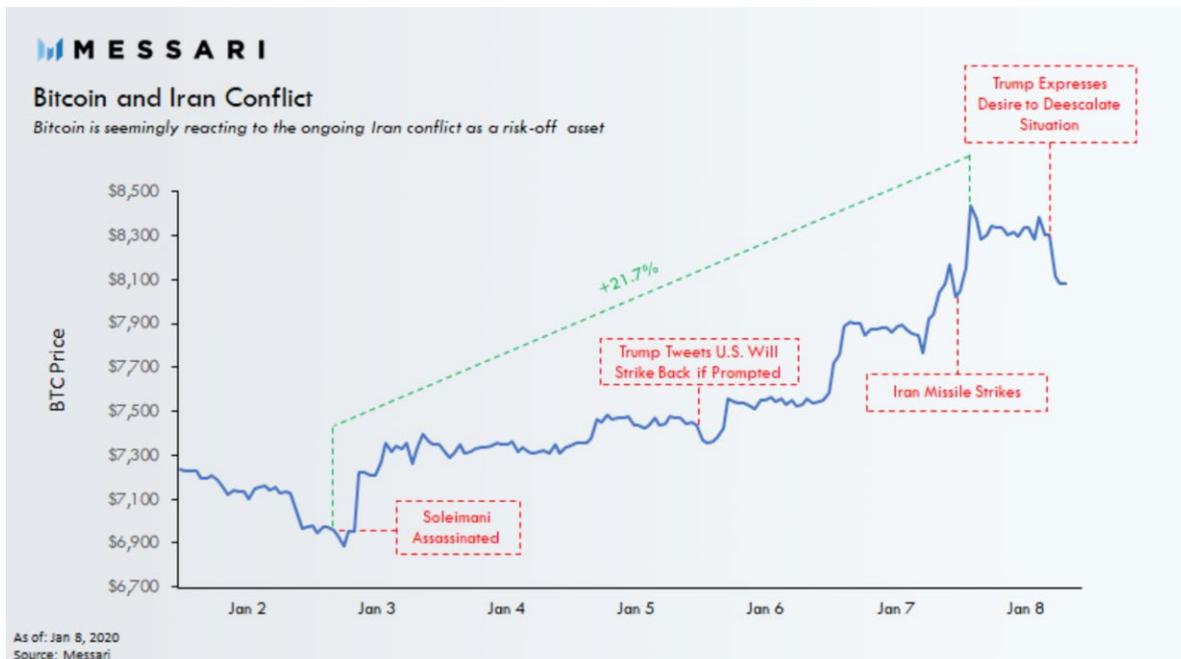
Source : <https://www.dailyfx.com/francais/bitcoin/comparaison-bitcoin-once-or.html>

The circled areas on the chart show the average range of price movements over the last 14 days. This proves that in most cases the fluctuations of Bitcoin are larger than those of gold. Hence, these fluctuations provide more opportunities but also more risks to an investor.

⁸ <https://www.supinfo.com/articles/single/5139-crypto-monnaie>

⁹ <https://www.dailyfx.com/francais/bitcoin/comparaison-bitcoin-once-or.html>

However, the trading price of **Bitcoin showed similarities to gold prices in times of international crisis**, i.e. an upward trend – such as during the U.S. vs. Iran crisis in January 2020¹⁰.



Source : <https://www.capital.fr/entreprises-marches/bitcoin-une-nouvelle-valeur-refuge-dans-les-pas-de-lor-1359345>

All along the escalation of the crisis the price of Bitcoin continued to rise, before dropping sharply at the moment of de-escalation. This type of price behaviour looks close to a safe haven.

However, looking at the drop during the Bitcoin “Corona-krach” makes it difficult to really categorize it as a safe haven or a speculative asset.



Source : <https://tradingview.com>

¹⁰ <https://www.capital.fr/entreprises-marches/bitcoin-une-nouvelle-valeur-refuge-dans-les-pas-de-lor-1359345>

4.2 The special case of the COVID-19 pandemic

A downward trend...

Since February 2020, Bitcoin has been facing its first major economic crisis.

Between February 14, 2020 and March 12, 2020, the value of Bitcoin went down from 9000 to 4500 euros¹¹, following the curve of large stock market values. A few days later it rebounded slightly without returning to its previous level. This instability has not been observed in other markets¹².

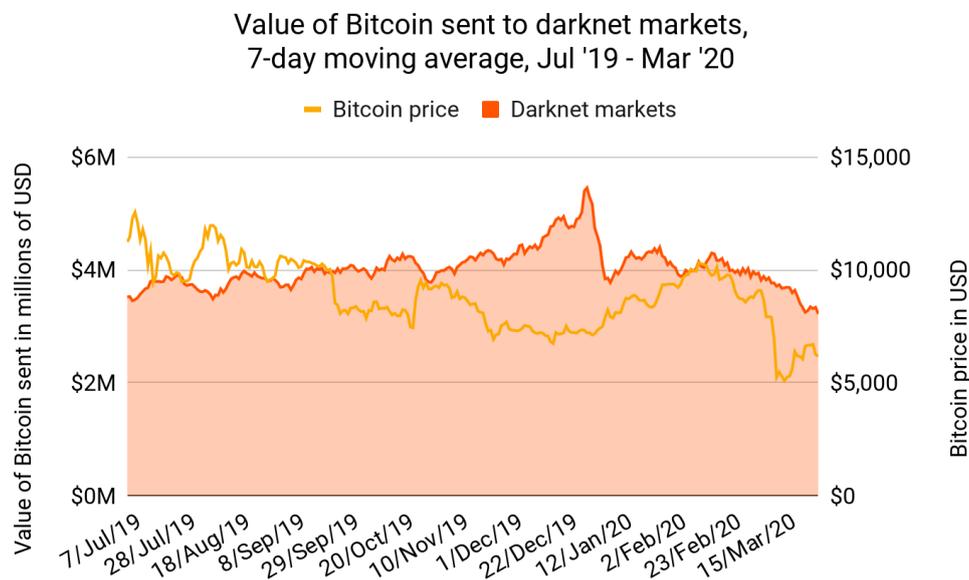
The downward trend kept going over several weeks: **“Those who had hoped that cryptocurrency - decorrelated [from the traditional stock market] - would be a good haven during the crisis were disappointed”**, according to the Italian business newspaper *Il Sole-24 Ore*¹³. Two explanation can be put forward for this drop, according to several experts¹⁴:

The need for liquidity at the beginning of this crisis led to the use of Bitcoin as a reservoir

“The fall can be explained by the sales made by institutional investors looking for liquidity (as in the commodity and gold markets). This market practice was for example observed at *iExec* and *ChainLink*, with a liquidation of the entire USDT order book, truly to recover dollars.”

The arrival of institutional funds in crypto-currency since 2018.

Furthermore, it is worth noting **the decline in transactions observed on illicit markets** as well as on legal markets. They usually tend to follow opposite curves, as shown in the following study¹⁵:



This illustrates the quite exceptional nature of this crisis, which sees half of the planet being confined and calls into question legal and illegal markets.

¹¹ <https://fr.tradingview.com/symbols/BTCEUR/>

¹² <https://24plus.ilssole24ore.com/art/il-crollo-mercati-non-risparmia-bitcoin-e-criptovalute-ADGwDVJ>

¹³ Ibid.

¹⁴ <https://cryptonaute.fr/bitcoin-crypto-pas-valeurs-refuge-tot-pour-dire/>

¹⁵ <https://cryptoast.fr/transactions-illicites-le-dark-net-souffre-lui-aussi-de-la-crise-du-covid-19/>

... followed by an unexpected Bitcoin price after the halving

Bitcoin then has seemed to return to its pre-crisis value over the weeks. On May 8, 2020, the price of Bitcoin even passed the symbolic \$10,000 threshold.¹⁶

On May 11th 2020, a halving has taken place, an operation that takes place every ~four years or so. As we discussed in section 3.3., miners are rewarded a certain amount of bitcoins whenever a block is produced. When Bitcoin first started, 50 Bitcoins per block were given as a reward to miners. After every 210,000 blocks are mined (approximately every 4 years), the block reward halves and will keep on halving until the block reward per block becomes 0 (approximately by year 2140). The block reward was **12.5** coins per block until May 11th 2020 and has now decreased to **6.25** coins per block¹⁷.

Bitcoin was indeed designed as a deflationary currency: the premise is that over time, the issuance of bitcoins will decrease and thus become scarcer. Halving then **generally allows the prices to go up again** because of the scarcity of available bitcoins and the difficulty to mine new ones. This means Bitcoin can be used as a hedge against inflation, as the price, guided by price equilibrium, is supposed to increase.

There is a debate on what will happen to Bitcoin pricing for a halving event : some believe that the halving is already priced in by the market (anticipation) and therefore there's no expectation for the price to do anything, while others believe that due to price equilibrium, a halving of supply should cause an increase in price if demand for Bitcoins is equal or greater than what it was before the halving event¹⁸. Below is a chart showing past price performance of the two halving events:



Source : <https://www.bitcoinblockhalf.com>

¹⁶ <https://www.journaldunet.com/patrimoine/guide-des-finances-personnelles/1210185-bitcoin-le-cours-baisse-dans-la-foulee-du-halving/>

¹⁷ <https://www.bitcoinblockhalf.com>

¹⁸ Ibid.

During the previous two halving events, which took place on November 28, 2012 and July 9, 2016, the price of bitcoin had risen significantly.

The **halving that happened on May 11, 2020** (an operation that halves the block reward per block created) **has finally allowed the prices to go up again**, similarly to what happened in 2012 and 2016. The price went down to €8070 on May 10, 2020 (just before the halving) and has started to increase again on May 12, 2020. It is now reaching €9034 (May 18, 2020)¹⁹. **The final evolution of the price will have to be followed throughout the year 2020 and even 2021 in order to see the final influence of the halving on it.**

The significant **drop observed in March is over**, which shows that **the crisis did not totally call into question Bitcoin's capacity to be a safe haven since it is a medium and long-term investment.**

¹⁹ <https://coinmarketcap.com/fr/currencies/bitcoin/>

5 Why is Bitcoin so popular among criminals?

According to Hacked, an estimated 10 to 20 percent of all Bitcoin (BTC) in existence is held by criminals²⁰. Why is it so popular among them?

A free and decentralised currency

Only users can control it: there is no central authority.

The value of Bitcoin resides solely in the trust users place in it. It is therefore the market law that sets the price via supply and demand: if users do not trust the currency, then they will want to sell and the price of the BTC will fall. On the opposite, if users trust it, then the price will rise in proportion to demand²¹.

Dispense with a trusted third party: financial freedom

Blockchain technology makes it possible: only an internet connexion is needed to carry out a transaction. This is called “peer-to-peer” transactions. Opening a “wallet” is also very easy, fast, anonymous and does not require a bank account. The crypto coins deposited in a wallet of cryptocurrency accounts are actually owned by their owner, not by a bank (usually the beneficiary of the funds deposited by customers). Users of cryptocurrencies are free to use this money as they want and the crypto market is unregulated. Similar to anonymous/unregulated technologies, crypto currencies are a haven for criminal activity around the globe.

Rapidity, unlimited volume and low fees

Bitcoin allows quick payment transfers (in seconds or minutes depending on the coin blockchain technology), compared with classic bank transfers that can take up to several days. Cryptocurrency transfers can be carried out with no maximum or minimum amount limit, from anywhere in the world, at any time of the day or night and at extremely low fees compared to those offered by traditional banks. With the rise in globalization, cryptocurrencies also became attractive thanks to their ability to easily carry millions of pounds across borders without detection.

Bitcoin is extremely safe

It is nearly impossible to hack a wallet because of a high cryptography technology. This security is one of the main successes of Bitcoin. Only the owner of the private key (a kind of password) of a wallet is able to use the funds in the wallet. Once validated, transactions are recorded forever and cannot be erased. This is a guarantee of security for users since a money transfer cannot be cancelled²².

²⁰ <https://hacked.com/biggest-bitcoin-hacks-thefts-time/>

²¹ <https://karadocteur.fr/blog/bitcoin-cryptomonnaies-avantages-inconvenients>

²² Ibid.

Bitcoin is a transparent and relatively anonymous currency

Anyone can see every transaction that is made: it is possible to trace back to the very first Bitcoin transactions since its creation to analyse where the money came from. However, we do not know who made what transaction or who holds what portfolio. Crypto transactions do not require real names, so it is easy for a criminal to remain unidentified as he moves and uses crypto. The European Banking Authority (EBA) explained that crypto assets often fall outside the scope of the EU financial regulations, so it is hard to build context around individual transactions²³. Bitcoin is then interesting for criminals since it is a safe and anonymous means of payment. For instance, Bitcoin has been used over the recent years as a payment method on Silkroad, a Darknet black market that used the Tor network to ensure anonymity for both buyers and sellers in the sale of illegal goods, including drugs and weapons. Silkroad was closed in 2014.

Cryptocurrencies are fickle: an advantage for risk-managing people

Due to their low capitalization, some cryptocurrency projects are extremely fickle. The price of financial assets is set according to supply and demand: the more money and individuals are invested in these crypto-assets, the more stable the prices will be. This volatility can be a brake on mass adoption by the general public since they may be afraid of losing all their savings if they see it as an investment for the purpose of storing value, but traders or more generally people managing risks (and so the criminals) will see it as an advantage²⁴.

It can be interesting for criminals to earn Bitcoin since the exchanges in local fiat currency or foreign currency fluctuate widely and can be very profitable: it can worth a lot more months after they got it with a ransom payment.

Finally, the real risk for cybercriminals lies at the moment of the exchange of Bitcoin into local fiat currency, because the risk of being identified is then at his peak (the advantages such as “no trusted third party”, “free and decentralised currency”, etc. disappear)

²³ <https://www.forbes.com/sites/vishalmarria/2019/02/04/how-cryptocurrencies-are-empowering-cybercriminals/#4c9312f837c5>

²⁴ <https://karadocteur.fr/blog/bitcoin-cryptomonnaies-avantages-inconvenients>

6 Bitcoin or Altcoins?

6.1. The Bitcoin dominance

The numerous crypto-assets existing are usually ranked by their Market Capitalization.

As a reminder, “stock market capitalization”, commonly called “market cap”, is “the market value of a publicly traded company's outstanding shares”. It is equal to the share price multiplied by the number of shares outstanding²⁵.

“Cryptocurrency market capitalization” or “cryptocurrency market cap” is a useful metric to know the total value of cryptocurrency. The website “Coinmarketcap” ranks the coins in the descending order of their market cap (as of May 18, 2020)²⁶:

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Vol. Change (24h)	Price Graph (7d)
1	 Bitcoin	\$176582752247	\$9607,30	\$44996647312	18380068 BTC	0,99%	
2	 Ethereum	\$23498653671	\$211,75	\$18037286321	110976024 ETH	4,82%	
3	 XRP	\$8970089467	\$0,203344	\$1904795836	44112853111 XRP *	0,57%	
4	 Tether	\$8810449302	\$1,00	\$53753923587	8798069379 USDT *	-0,09%	
5	 Bitcoin Cash	\$4540405549	\$246,62	\$3440118333	18410244 BCH	3,34%	
6	 Bitcoin SV	\$3667662067	\$199,23	\$1932119166	18409065 BSV	4,73%	
7	 Litecoin	\$2906574437	\$44,88	\$4573990744	64756206 LTC	1,85%	
8	 Binance Coin	\$2561250882	\$16,47	\$339072481	155536713 BNB *	1,25%	
9	 EOS	\$2456347261	\$2,66	\$3537527459	922724272 EOS *	1,35%	
10	 Tezos	\$1934053414	\$2,72	\$130880018	710858597 XTZ *	2,01%	

Source : <https://coinmarketcap.com>

²⁵ https://en.wikipedia.org/wiki/Market_capitalization

²⁶ <https://coinmarketcap.com>

In the case of “cryptocurrency market cap”, **Market Cap = Circulating supply * Price of each coin**

Note that the circulating supply (i.e. at the moment) should not be confused with total supply, which represents the number of tokens that will be available over the long term.

In other words, the crypto market cap is a product of the coin’s circulating supply and the price of each coin. This means that even if the individual price of an A coin is more than of a B coin, the overall value of the B coin will be much more than the A coin if there are much more B coins in circulation than A coins. This is why market cap is a better indicator of a company’s worth than the price of its individual tokens.

According to Coinmarketcap, there are **almost 2500 different cryptocurrencies** existing at the time. This very high number adds vagueness to an environment that is already very opaque to the general public, what slows down their adoption by people who do not know which project to invest in. Moreover, this staggering number of projects divides the total capitalization of the cryptos market, which in turn increases volatility.

Bitcoin remains the sole “stable” cryptocurrency over time. It was the first one to use the Blockchain technology in 2009. Bitcoin was then a real innovation by setting up a network and public blockchain technology. Other cryptocurrencies have since been created, claiming their functionalities, protocols, decentralisation (or not), etc. were more efficient than the Bitcoin network features. However, these changes in features are mainly based on the Blockchain technology... that started with the Bitcoin revolution.

Then, Bitcoin benefits from an important network effect, due to the largest number of users. People using Bitcoin attract more and more new people to the network. As a pioneer, Bitcoin has also received **more media coverage than all Altcoins**²⁷.

Here is an illustration of the Bitcoin (BTC) dominance, which shows the share of Bitcoin in the overall market:



Source: <https://coin360.com> (May 18, 2020)

²⁷ “Altcoins” is the name given to other cryptocurrency projects.

As of May 3rd 2020, it's a little over **63%**²⁸. The Bitcoin dominance makes it possible to observe the evolution of the altcoins. Some had believed to see in 2017 a potential reversal of the hierarchy with the explosion of Ethereum. However, the **flipping**, consecration of a reversal of dominance has so far remained purely theoretical.

Finally, the security of the Bitcoin network has been proven over time. It has never been successfully hacked to date. If it does not have all the functionalities other Altcoins claim, the simple structure of Bitcoin allows it to be the more robust. This is also why Bitcoin technology can still be considered as the most reliable technology on the cryptocurrency market today²⁹.

6.2. A diversified portfolio reduces risks and potentially allows more benefits

The importance of “market-cap” to understand the utility of a diversified portfolio

Analysing the range by market capitalization is useful since it shows the level of risk associated with an investment in a cryptocurrency. As explained by “Blockgeeks”³⁰, cryptocurrencies can be broadly classified into “large-cap”, “mid-cap” and “small-cap”.

- **Large-cap cryptocurrencies** (more than \$10 billion) have a big market cap and as such are **safe investments** to make. However, this investment will mostly not experience any major growth. Still, it will have some slight conservative growth because cryptocurrencies remain a lot more volatile than traditional stocks.
- **Mid-cap cryptocurrencies** (between \$1 billion and \$10 billion) have a smaller market cap but more risks than large-cap cryptos. Their growth potential is higher than large-cap **cryptos**, because they may still be in the stage of increasing their market or utility.
- **Small-cap cryptocurrencies** (below \$1 billion) have low market cap and the highest risk because the chances of failure are much higher. However, they have the potential to truly explode in value and give big returns on investment.

Hence, it **makes sense for some investors to have a diversified portfolio mixing selected coins of all the three classes.** It may reduce the risk and allow to benefit from all potential advantages of owning assets in all classes.

The **total market-cap** is used to calculate the market capitalisation of all the cryptosystems on the market (currently 190 billion)³¹. It is a **measure of the health and evolution of the crypto-currency ecosystem**, although it is not the only indicator. However, a rising total market cap tends to show a good shape of the sector.

²⁸ <https://cryptoast.fr/quest-ce-que-le-market-cap-definition-interets-et-limites/>

²⁹ <https://www.thecointribune.com/actualites/pourquoi-bitcoin-btc-est-si-different-des-autres-cryptomonnaies/>

³⁰ <https://blockgeeks.com/guides/cryptocurrency-market-cap/>

³¹ <https://cryptoast.fr/quest-ce-que-le-market-cap-definition-interets-et-limites/>

Yet, market-cap takes into account currency in circulation, so the exact figures of this indicator cannot be known precisely: only the owner of the private key gets access to its account, so the coins are “lost” when the owner dies without transmitting it or simply “loses” the key. Even so, the coins are still considered to be in circulation³²...

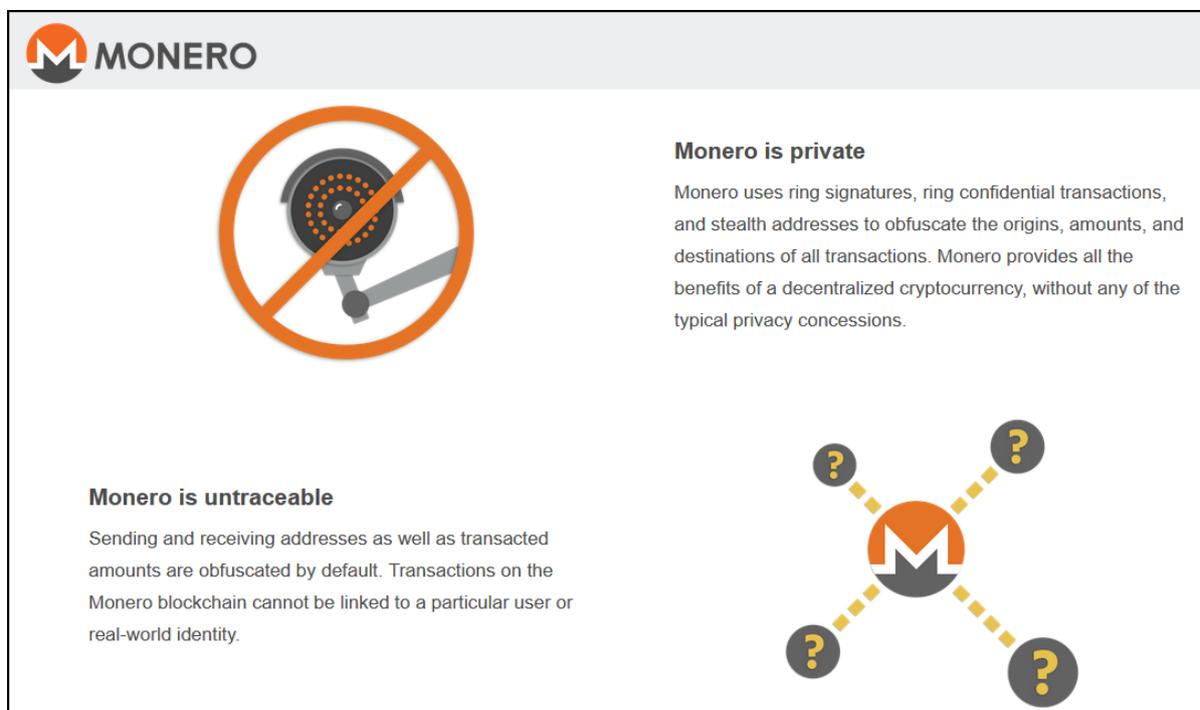
That is why market-cap is a good tool, but not enough to get an idea of the value of a cryptocurrency. The analysis of liquidity and volumes, thorough research and an understanding of the currency are also fundamental.

The potential effect of the COVID-19 crisis

Because of the downward trend of BTC in the wake of the crisis, there could have been a **shift of interest** in the world of cryptocurrencies **from BTC to other digital currencies backed by cash values** such as the dollar. This is the case for the Tether or the USD Coin, which seem to be protected from the volatility experienced by Bitcoin in March. However, the recent return of Bitcoin to its pre-value crisis should reassure investors.

6.3. The use of other cryptocurrencies to hide money trail

According to Bleeping Computer³³, the **REvil/Sodinokibi** ransomware has started to accept the **Monero cryptocurrency to make it harder for law enforcement to track ransom payments**. It also plans to stop allowing Bitcoin payments.



The infographic features the Monero logo (an orange 'M' in a circle) at the top left. On the left side, there is a large orange circle with a diagonal slash over a grey camera icon, representing untraceability. On the right side, there is a central orange 'M' in a circle connected by dashed yellow lines to four smaller grey circles, each containing a yellow question mark, representing privacy. The text is arranged around these visual elements.

MONERO

Monero is private
Monero uses ring signatures, ring confidential transactions, and stealth addresses to obfuscate the origins, amounts, and destinations of all transactions. Monero provides all the benefits of a decentralized cryptocurrency, without any of the typical privacy concessions.

Monero is untraceable
Sending and receiving addresses as well as transacted amounts are obfuscated by default. Transactions on the Monero blockchain cannot be linked to a particular user or real-world identity.

Source : <https://www.getmonero.org>

³² Ibid.

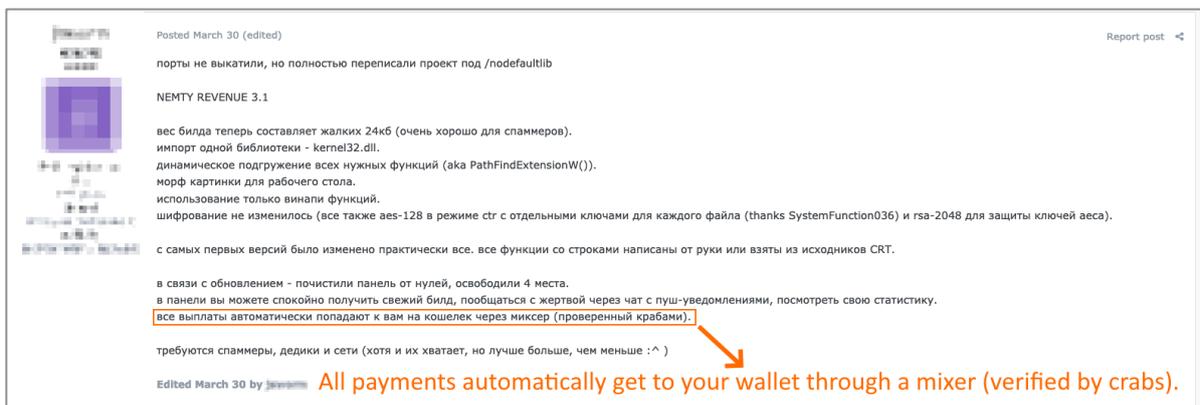
³³ <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-to-stop-taking-bitcoin-to-hide-money-trail/>

The Monero cryptocurrency is impossible to track: REvil/Sodinokibi ransomware operators stated on a hacker and malware forum that “due to CryptoNote and the obfuscation added to the protocol, passive mixing is provided: all transactions in the system are anonymous, and all participants in the system can use plausible denial in case of capture.”

Actually, the combination of the anonymous browser Tor and Monero makes it impossible to trace the funds or the actors who received them, according to a 2019 webinar from Europol³⁴.

REvil/Sodinokibi operators **want to stop BTC payments in the future**: Monero has already become the default payment currency on their site and the amount of the ransom is increased by 10% if a victim wants to use BTC to make a ransom payment.

This switch could also be explained by the **necessity for some hackers to use/pay an additional service to transfer Bitcoin** (called “mixer”, that is like a money launder):



Source: Nemty (Ransomware As A Service) developers' post on an underground forum

That is why cybercriminals sometimes try to diversify their portfolio of cryptocurrencies and make exchanges, or even switch from Bitcoin to an even more anonymous cryptocurrency.

³⁴ <https://www.bitchute.com/video/PWXU7D4VV0IB/>

7 “Partnerships” for ransoming: Emotet, TrickBot & Ryuk

If we look to major malware operators, we can observe “partnerships” to carry out ransoming. For instance, the famous Emotet, TrickBot and Ryuk malware associated to gain footholds in target companies before delivering ransomware and demanding large Bitcoin payments.

This typically begins with an infection by the Emotet malware, for instance through phishing email. Then the operator will at some point push the TrickBot malware as a payload to the Emotet-infected machine. TrickBot is often used to steal credentials and launch actions inside a network. The final stage in the infection operation is the delivery of an APT payload for a manual hacker’s interaction, leading once performed to the Ryuk ransomware. Ryuk will then encrypt selected files on the infected systems and drop notes demanding a Bitcoin payment. The ransom demand can vary, from one or two Bitcoin, to as high as 99³⁵.

This partnership is interesting because methods and objectives are usually different: **Ryuk asks for ransom in cryptocurrency, while TrickBot is a banking trojan capturing banking credentials** (that give access to “real” money) **& POS payment data**³⁶ to pass them to criminals.

We can wonder why they associate. One **hypothesis of our OSINT Unit is that they want to gather their strengths and diversify their incomes to become stronger**: they can both steal confidential data and banking information (to carry out fraudulent transfers or sell this information on the Darknet) and encrypt data to ask for a ransom in Bitcoin. We can then guess that they share the income of their different malicious actions.

However, how is this share operated? We are talking about criminals: the notions of “fairness” and “loyalty” are not really applicable.

Looking at who operates them can give us a good clue. According to CrowdStrike, **GRIM SPIDER would have operated Ryuk** since August 2018 using the “big game hunting” methodology (i.e. targeting large organizations for a high-ransom return). This would signal a shift in operations for **WIZARD SPIDER, a criminal enterprise of which GRIM SPIDER appears to be a cell**. Here is an interesting fact: **the WIZARD SPIDER threat group is known as the Russia-based operator of TrickBot**³⁷.

Our **OSINT hypothesis is then that the link of Russian “paternity” between Ryuk and TrickBot may explain why they have teamed up and how they can manage the distribution of stolen money**.

³⁵ <https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware>

³⁶ The point of sale (POS) or point of purchase (POP) is the time and place where a retail transaction is completed.

³⁷ <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf>

8 Does BTC market capitalization fluctuate because of ransomware?

In order to understand if ransomware have had influence on the BTC price (“market cap”), we compared the dates of ransomware campaigns with the price of BTC at that time.

On the one hand, we used Google Trends to determine the first time that a research was done on a ransomware campaign, which roughly corresponds to the time of its launch. On the other hand, we used the website Coinmarketcap to visualize the Bitcoin price at that time, taking a range from -7 days before the date to +1 month after the date.

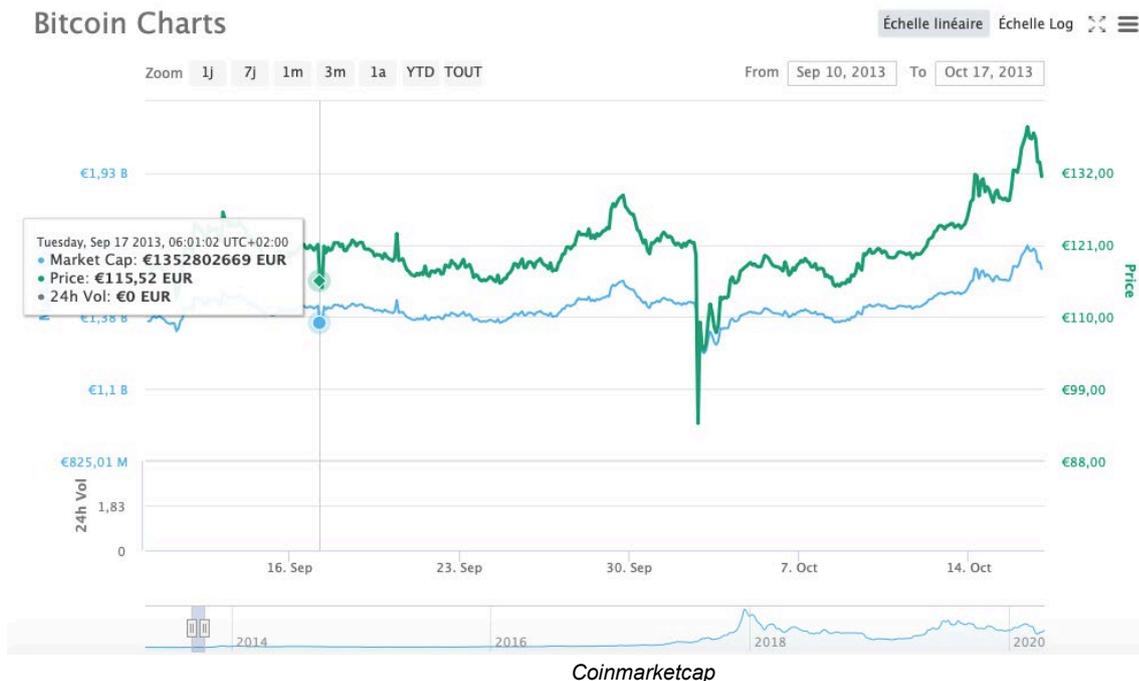
We studied the following ransomware, among the most famous ones: Crypto Locker, Locky, Ryuk, WannaCry, REvil/Sodinokibi, GandCrab, Maze and DoppelPaymer. They all asked a ransom in BTC in order to decrypt data they encrypted.

8.1. CryptoLocker



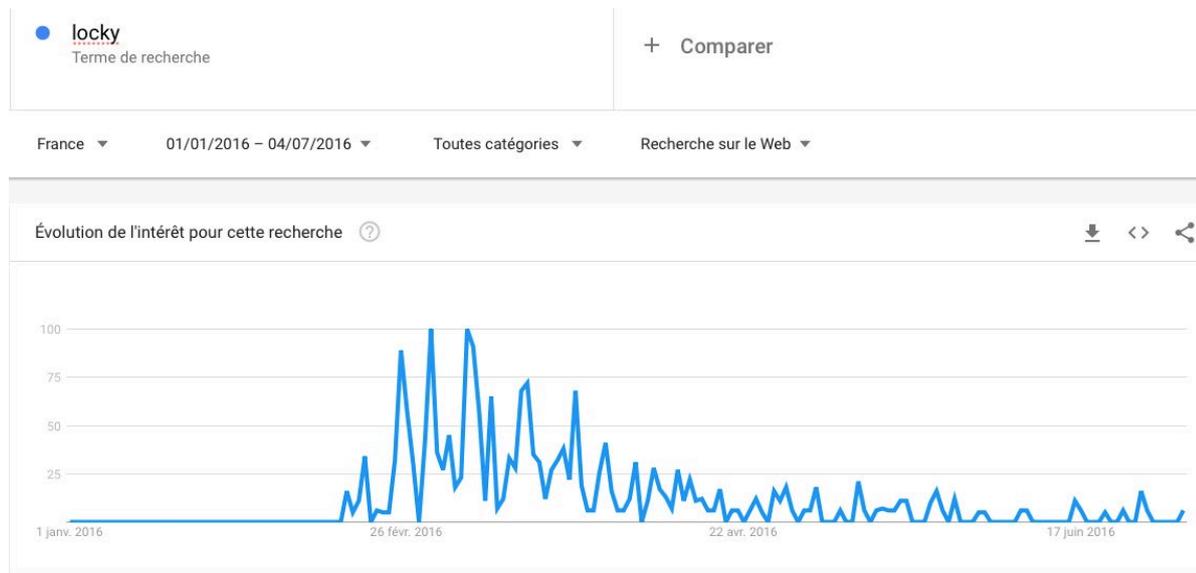
Source: Google Trends

The first appearance dates back to September 17, 2013.



There is a really slight decrease of BTC price at that date, so there might be a small correlation. Later, there is a significant drop on October 2, 2013, but it is too far from September 17, 2013 to link them with certainty.

8.2. Locky



Source: Google Trends.

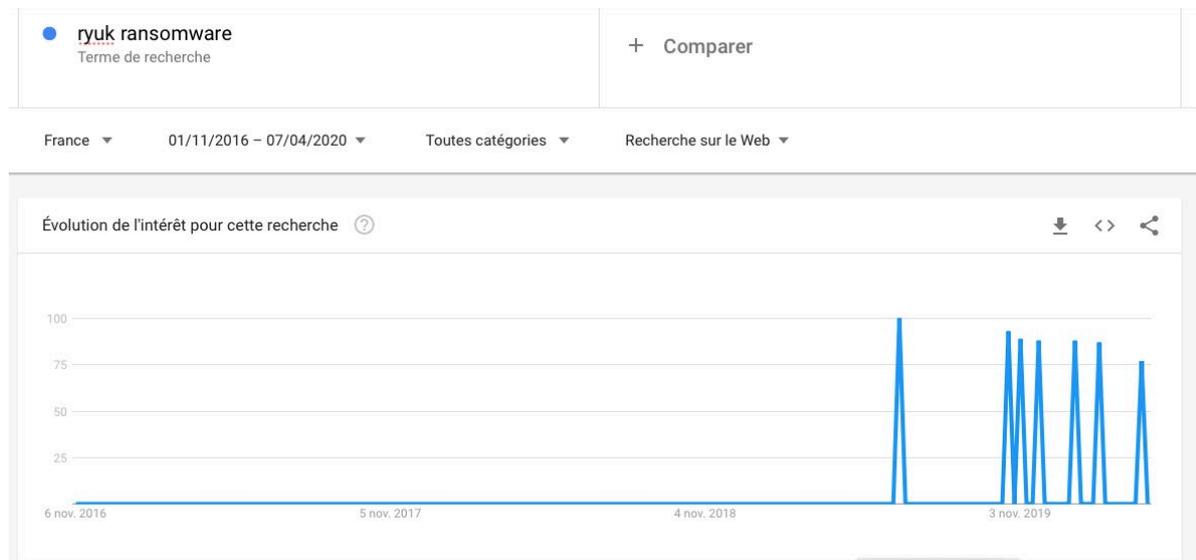
The first appearance dates back to February 17, 2016.



Source : Coinmarketcap

We can observe a slight increase as of February 17, 2016, but this increase takes place in a global larger increase that has already started before the ransomware campaign. We can therefore not assess that there is a correlation, but this was anyway in the interest of the hackers who benefited of this price evolution.

8.3. Ryuk



Source: Google Trends

Research is focused on “Ryuk ransomware”, because “Ryuk” only can refer to other researchs (such as the Death Note manga character). The first appearance dates back to June 4, 2019.

Bitcoin Charts



Source: Coinmarketcap

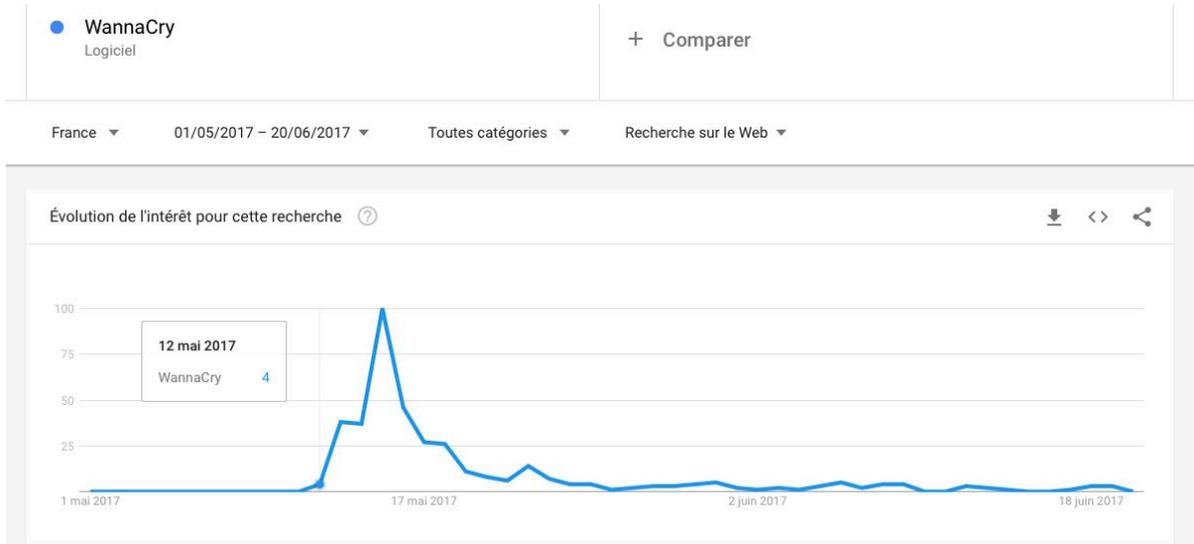
As of June 4, 2019, there is no relevant change in BTC price. However, as illustrated by the graph below, there is a significant increase from the second part of June 2019, that reaches a peak on June 26, 2019.

Bitcoin Charts



Source : Coinmarketcap

8.4. WannaCry



Source: Google Trends

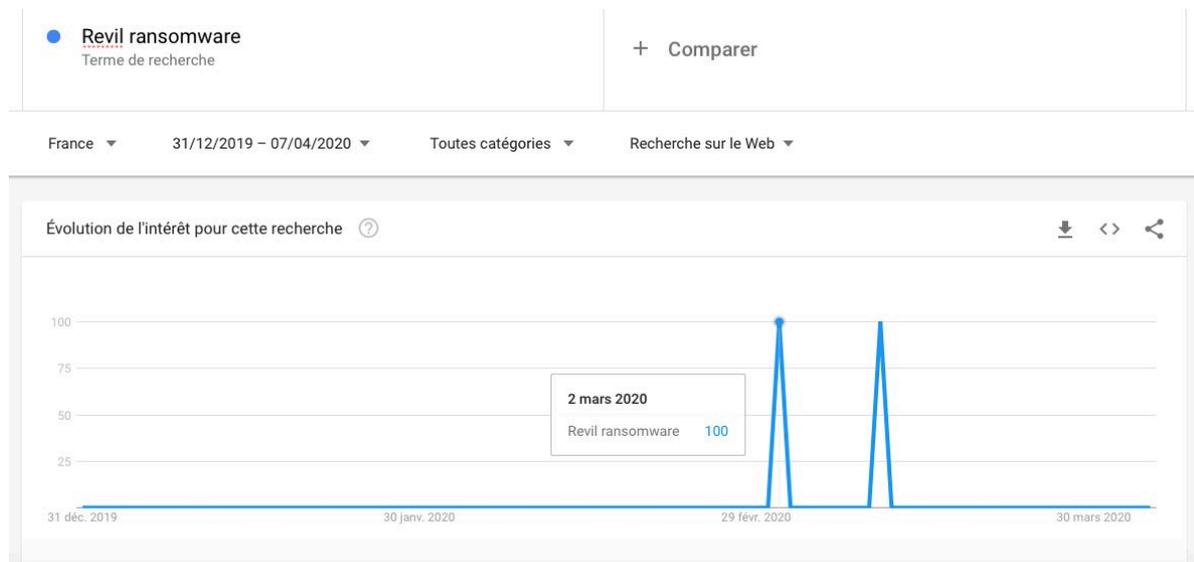
The first appearance dates back to May 12, 2017.



Source : Coinmarketcap

As of May 12, 2017, nothing in particular happened on the BTC price. There is a slight decrease in the following days, but this is not significant enough to make a correlation.

8.5. REvil



Source: Google Trends

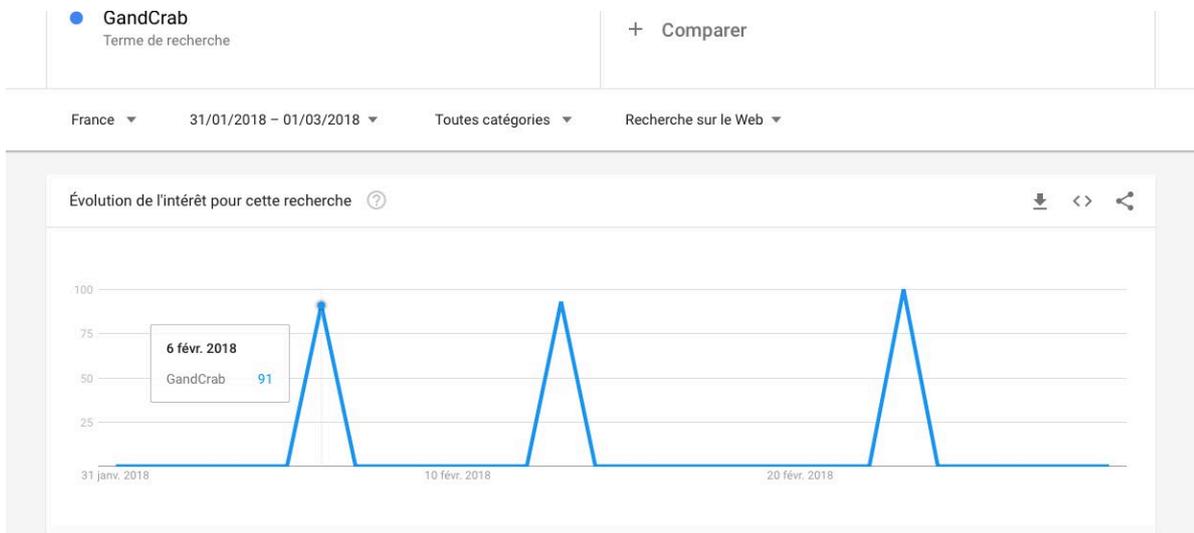
The first appearance dates back to March 2, 2020.



Source: Coinmarketcap.

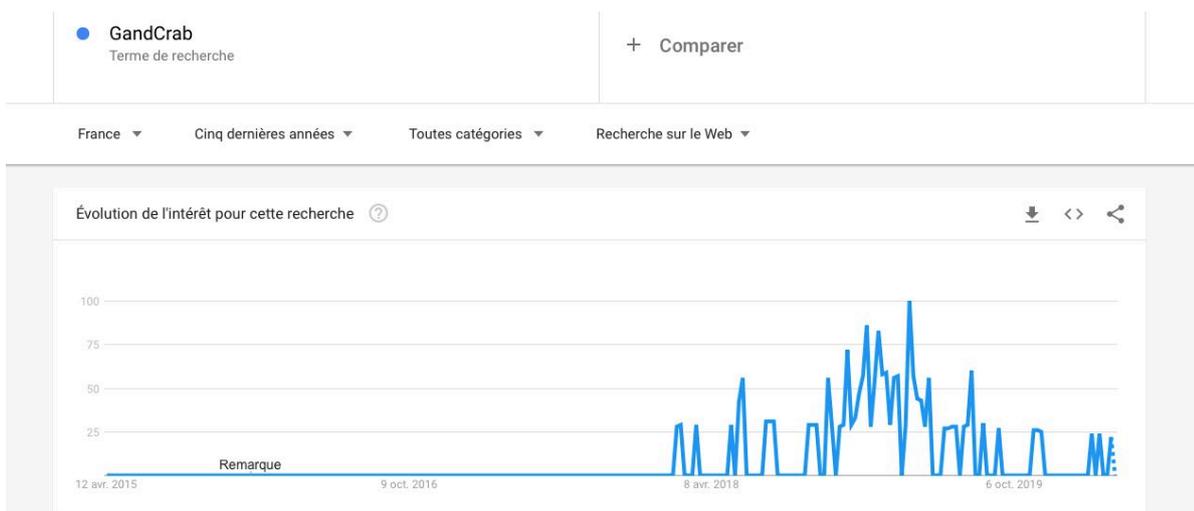
There is no change as of March 2, 2020, but we can observe a significant drop 10 days later, as of March 12, 2020. It is however a bit too late to make a correlation.

8.6. GandCrab



Source: Google Trends

The first appearance dates back to February 6, 2018. The graph below shows that there was no research before.



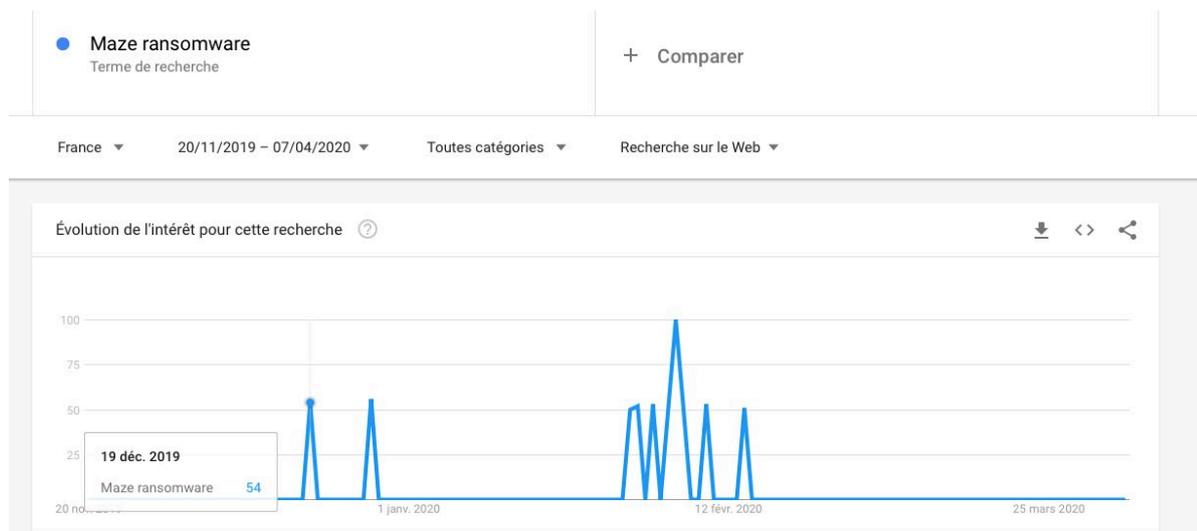
Source: Google Trends.



Source: Coinmarketcap

There is a significant drop as of February 6, 2018. This could then be related to the launch of GandCrab ransomware.

8.7. Maze



Source: Google Trends

Research is focused on “Maze ransomware” because “maze” only can refer to other research, since it is a common name in English. The first appearance dates back to December 19, 2019.

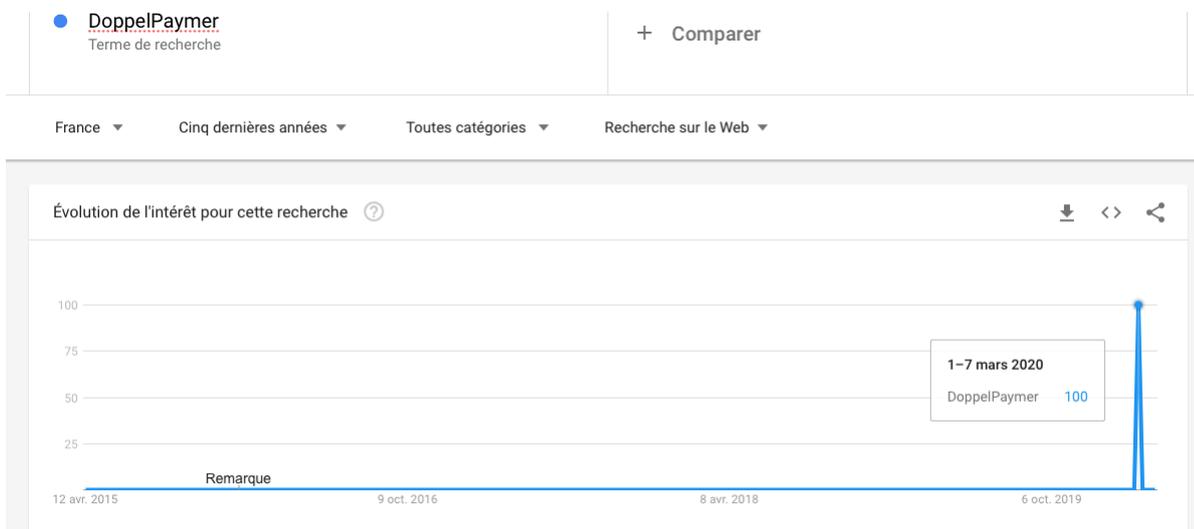
Bitcoin Charts



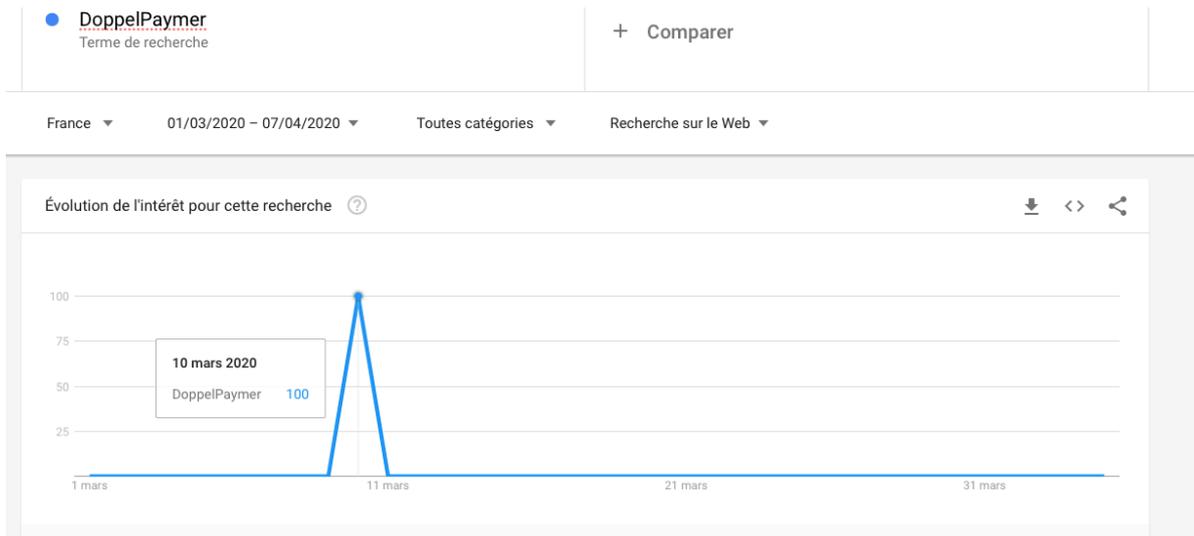
Source: Coinmarketcap

There seems to be no link between the launch of the ransomware and the BTC price.

8.8. DoppelPaymer



Source: Google Trends.



Source: Google Trends.

The first appearance dates back to March 10, 2020.



Source: Coinmarketcap.

We can observe a significant drop in BTC price a few days later, around March 12, 2020. However, nothing happened between March 10, 2020 and March 11, 2020. If we can potentially make a correlation, this is uncertain.

8.9. Conclusion and Hypothesis

If ransomware are undoubtedly a source of money inflow, it is **difficult to prove with certainty** the link between ransom campaigns and the price (“market cap”) of Bitcoin.

Actually, the **number of transactions in BTC and the sum of money needed are so huge** that it can be hard to see the influence of ransomware campaigns on the BTC price.

However, as we demonstrated it with the graphs above, **some campaigns coincide with certain rises in BTC price**. It is then possible that the sums involved and/or the good timing of the attackers in relation to the price behaviour allowed a higher potential gain.

Moreover, our OSINT Unit thinks that **ransomware campaigns can have an influence on Altcoins**, since less money is needed to make their price move. Nonetheless, this is hard to prove as well because it is even more untraceable.

If a **victim** has to pay a ransom, it is also likely that she/he will **first use Google to search for information** about ransomware. Below is an overlay of Google's searches (*worldwide*) about ransomware, correlated with the market capitalization of all crypto currencies:



Source: Laboratory of Epidemiology – Orange Cyberdefense

How can we explain the similarities?

- Since ransomware are a major vector of money inflow, we could consider that people searching “ransomware” on Google are potential victims who will pay. Once the payment is made, this would then increase the market capitalization.
- Broadcasters could follow market fluctuations and be more active at some periods. Some “crypto addicts” have investment knowledge but it seems to be too correlated here.
- These similarities could also be only coincidences.

That is why we will be careful not to make any conclusions. However, we wanted to share these similarities observed on this time-lap.

9. Conclusion of our OSINT Unit

Cryptocurrencies are, by their functionalities and protocols, **a good way to earn/manage income for cybercriminals**. Their anonymity and rapidity, among other features, allow to hide money trail and to get rid of existing banking regulations.

Among all cryptocurrencies, **Bitcoin remains since its creation the most popular one**. Criminals are no exception: most ransomware ask for a ransom in BTC.

However, we observed in recent times some changes in the world of cryptocurrencies. If Bitcoin still reigns on it, the popular cryptocurrency faced its **first major economic crisis since the COVID-19 pandemic** has started. Some ransomware operators have also started to ask for ransom in Monero (another cryptocurrency) to make it harder for law enforcement to track ransom payment.

Bitcoin yet remains the safest cryptocurrency and is a middle to long-term investment.

We also highlighted that **Bitcoin inflow and other cryptocurrencies have links to cybercriminal activity**. This link will be further developed in another report from our OSINT Unit, but looking at the fluctuation of the market capitalization may suggest a correlation between the major ransomware campaigns and the BTC price.

It is a two way correlation:

- If the BTC price grows up significantly (even though it has not happened yet after the recent halving), ransomware activities are likely to expand because criminal will follow the potential of this price increase.
- If massive ransomware activities grow up and so do big ransom payments, these transactions and massive transfers done by criminals could impact the crypto market.

It is yet difficult to prove it with certainty, partly because the number of transactions in BTC and the amount of money involved are so huge that it can be hard to see the influence of ransomware campaigns on the BTC price. However, it is **possible that the sums involved and/or the good timing & trading skills of the attackers could impact the crypto market, with the aim of making a profit and building up a reserve of money for their activities.**

10 Appendices

10.1. Selected Repository for the Classification of Sources and Information

Source ratings³⁸

Code	Source rating	Explanation
A	Reliable	No doubt of authenticity, trustworthiness or competency; has a history of complete reliability
B	Usually reliable	Minor doubt about authenticity, trustworthiness or competency; has a history of valid information most of the time
C	Fairly reliable	Doubt of authenticity, trustworthiness or competency, but has provided valid information in the past
D	Not usually reliable	Significant doubt about authenticity, trustworthiness or competency but has provided valid information in the past
E	Unreliable	Lacking in authenticity, trustworthiness and competency; history of invalid information
F	Cannot be judged	No basis exists

³⁸ US Department of the Army (September 2006). "FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations" (PDF). FM 2-22.3. Retrieved 2007-10-31.

Information content ratings³⁹

Code	Rating	Explanation
1	Confirmed	Confirmed by other independent sources; logical in itself; consistent with other information on the subject
2	Probably true	Not confirmed; logical in itself; consistent with other information on the subject
3	Possibly true	Not confirmed; reasonably logical in itself; agrees with some other information on the subject
4	Doubtfully true	Not confirmed; possible but not logical; no other information on the subject
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
6	Cannot be judged	No basis exists

10.2. Disclaimer

Orange Cyberdefense strives to ensure the accuracy of the information gathered in this document, but no warranty, express or implied, can be given.

Orange Cyberdefense disclaims any liability for errors or omissions resulting from/related to the use of the information and material in this document.

³⁹ Ibid.

Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.