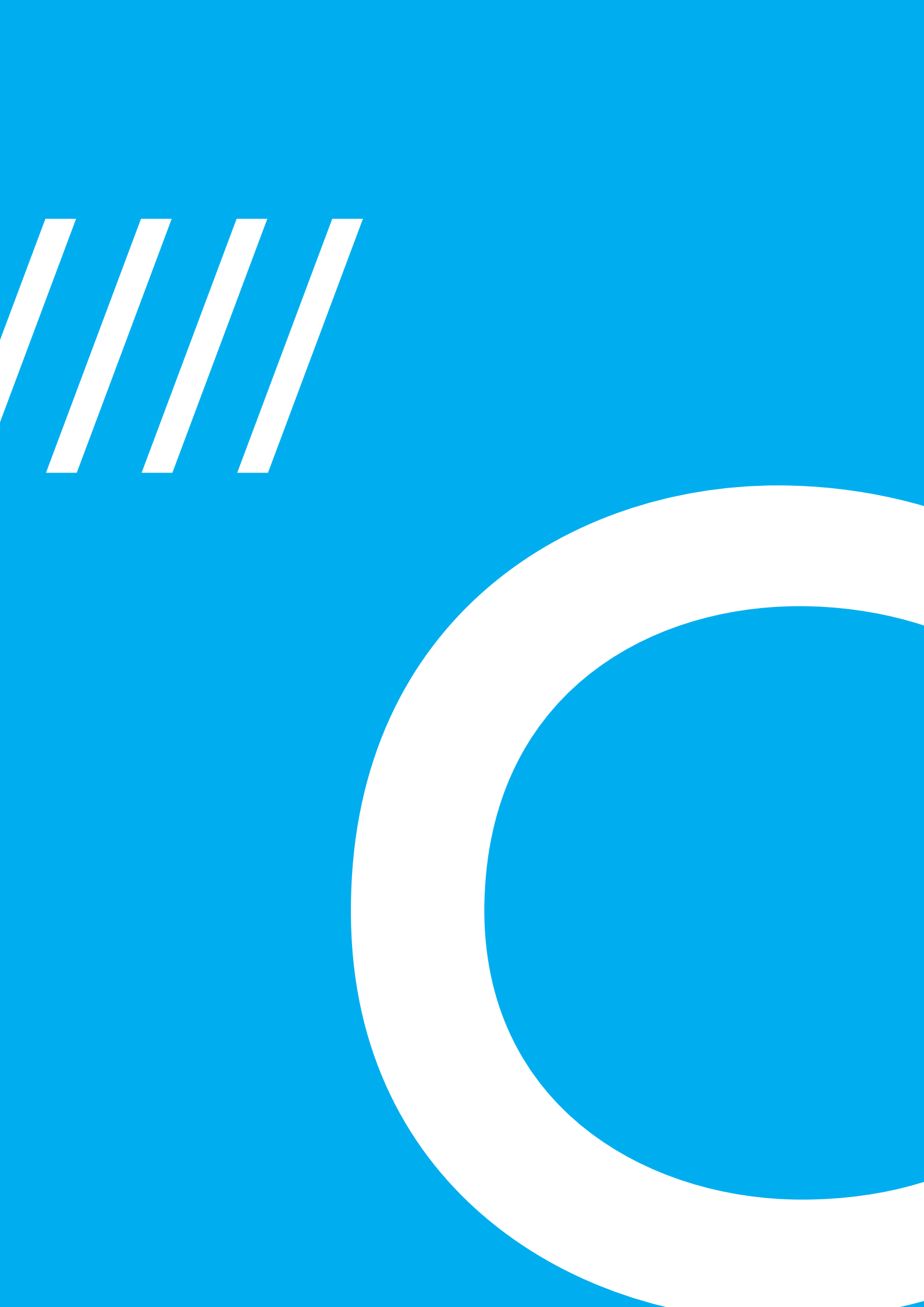
2018 Cryptocurrency Exchanges

User Accounts Leaks Analysis

www.group-ib.com



Contents

01

01—
Key Findings

IN COMPARISON WITH 2016, THE NUMBER OF COMPROMISED ACCOUNTS IN 2017 INCREASED BY 369%

BECAUSE OF THE FUSS ABOUT CRYPTOCURRENCIES THE NUMBER OF INCIDENTS IN JANUARY 2018 SKYROCKETED BY 689% AGAINST THE MONTHLY AVERAGE OF 2017

KEY FINDINGS

Group-IB, one of the global leaders in preventing and investigating high-tech crimes and online fraud, has analyzed 720 account leaks (logins and passwords) from 19 cryptocurrency exchanges based on data obtained from the Group-IB Threat Intelligence system.

***

The key findings of the study are as follows:

- We are witnessing a rising trend in the number of compromised login data. In comparison with 2016, the number of compromised accounts in 2017 increased by 369%.
- Because of the fuss about cryptocurrencies the number of incidents in January 2018 skyrocketed by 689% against the monthly average of 2017.
- At least 5 of 19 exchanges experienced targeted cyberattacks that led to financial losses (at least $80 million).
- The users of all the 19 analyzed exchanges have suffered from hackers.
- TOP-3 victims' countries are the USA, Russian Federation and China, with every third user from the USA.
- We identified at least 50 active botnets behind the mentioned leaks. The cybercriminals' infrastructure is distributed geographically mostly in the USA (56,1%), the Netherlands (21,5%), Ukraine (4,3%) and Russian Federation (3,2%).
- The number of malicious programs used by cybercriminals is constantly increasing, and the tools are regularly modified. Examples of malicious software used by cybercriminals to steal user accounts include AZORult stealer, Pony Formgrabber and Qbot.
- Criminals have adapted patterns of attack on banks and used the same tools to hack cryptocurrency exchanges and wallets and make attacks on users.

02

02–
Forewords

THE PRESENT STUDY AIMS TO ESTIMATE THE NUMBER OF ACCOUNT LEAKS FROM CRYPTOCURRENCY EXCHANGES AND TO ANALYZE THEIR NATURE

WE HAVE MADE AN ATTEMPT TO DEFINE THE REASONS OF THESE LEAKS AND PROVIDE FURTHER RECOMMENDATIONS FOR BOTH EXCHANGES AND VICTIMS

FOREWORDS

The hype around blockchain and cryptocurrencies is attracting more and more criminals to the segment. The first incidents of online wallets, cryptocurrency exchangers and exchanges hacks were recorded in 2011.

In 2017, along with the growth of broad interest in cryptocurrencies, we saw dozens of successful major attacks on cryptocurrency services, which showed that the criminals have adapted patterns of attack on banks and used the same tools to hack cryptocurrency exchanges and wallets and make attacks on users. Malwares are being actively modified and the new ones are being created — specifically aimed at mining activities.

***

As a result, in 2017, according to a joint study of EY and Group-IB analysts "EY research: initial coin offers (ICOs)" [12], cybercriminals managed to steal 10% of all funds invested in ICO through Ethereum, and the total damage amounted to almost $400 million. For example, as a result of the Coincheck hack in January 2018, a record amount of money ($533 million) was stolen.

Increased fraudulent activity and attention of hacker groups to cryptoindustry, additional functional of malicious software related to cryptocurrencies, as well as the significant amounts of already stolen funds signals that the industry is not ready to defend itself and protect its users. In 2018 we will see even more incidents.

The dark side of the cryptoindustry requires a response from the community, including researchers, scholars and the academia.

However, contrary to estimates in fiat currencies (e.g. thefts from banks), it is much more difficult to assess losses related to cryptocurrencies due to various reasons:

- high level of anonymity and reluctance to disclose the revelant data concerning the size of the stolen funds for fear of bankruptcy
- lack of regulation and obligations to disclose breaches and incidents;
- numerous existing blockchains and coins, attack vectors, cryptocurrency actors (e.g. ICO projects, wallets, exchanges, miners);
- significant amount of ICO projects which are scams by nature.

Because of the mentioned issues Group-IB experts decided to conduct the present study. The study aims to estimate the number of account leaks from cryptocurrency exchanges and to analyze their nature. We have made an attempt to define the reasons of these leaks and provide further recommendations for both exchanges and victims.

03

03—
Study Results

STUDY RESULTS

We have analyzed 720 incidents concerning the episodes when cybercriminals managed to get access to login data on the web-sites of cryptocurrency exchanges. The compromised accounts are related to the following exchanges: Binance, Bit-z, Bitfinex, Bithumb, Bitstamp, Bittrex, BTCC, CEX.io, Coinone, Gate.io, GDAX, Gemini, HitBTC, Huobi, Kraken, KuCoin, OKEx, Poloniex, Wex.nz. There was not any cryptocurrency exchange in our sample, users of which have not become the victims of cybercriminals.

3.1. LEAKS DISTRIBUTION BY EXCHANGES

Top compromised accounts in our sample distributed among: Poloniex — 174 accounts, Bittrex — 111, CEX.io — 95, HitBTC — 83, Kraken — 61 leaks (Figure 1). This distribution is the most luckely due to the popularity of these platforms among investors and on the Internet, which attracted the attention of cybercriminals.

3.2. MOMENTUM OF LEAKAGE GROWTH

Our systems detected the first 5 incidents in June 2014. By the end of 2016, there have already been 139 account leaks. According to Figure 2:

- in comparison with 2016, the number of compromised accounts in 2017 increased by 369%;
- the average monthly number of leaks in 2017 was 30,75;
- January 2018 only, exchanges faced with 212 leaks of login data;
- the number of incidents in January 2018 skyrocketed by 689% against the monthly average of 2017.

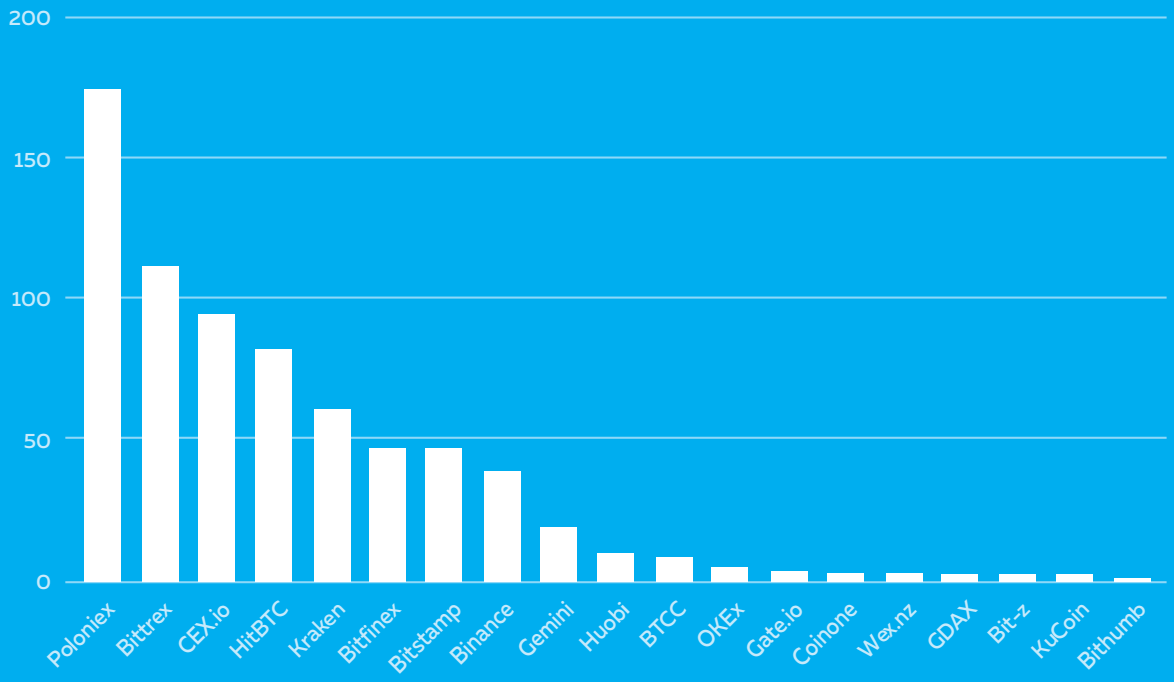


Figure 1: Number of account leaks distributed by exchanges
Source: Group-IB, 2018

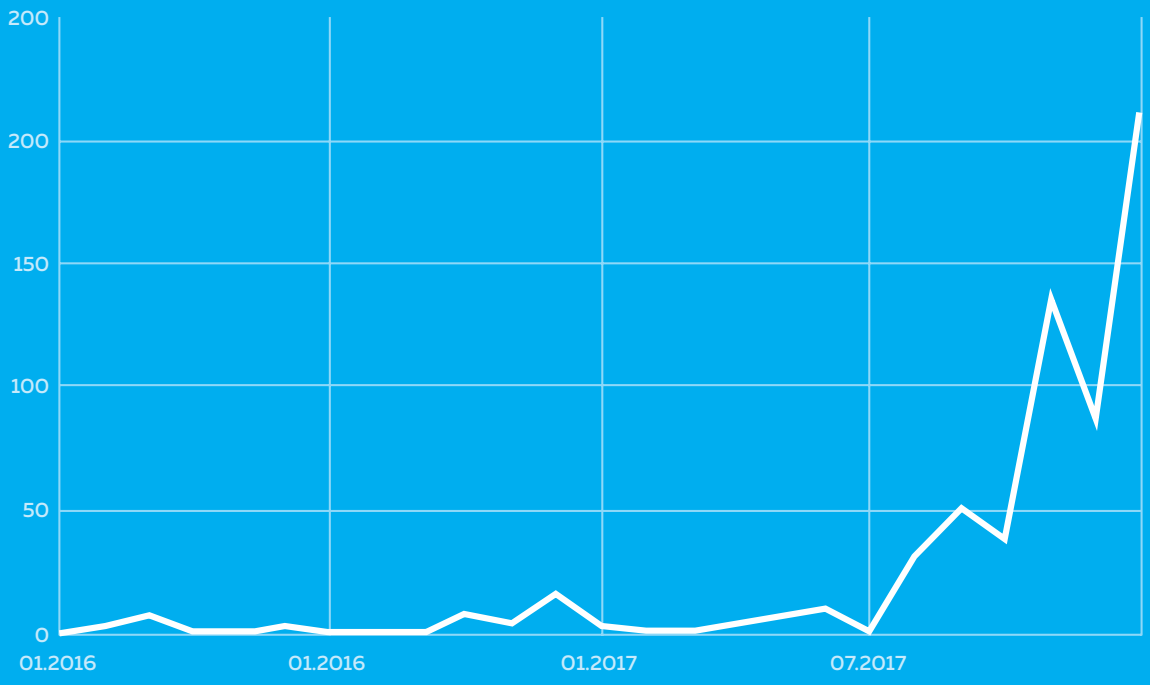


Figure 2: Monthly account leaks from January 2016 to January 2018
Source: Group-IB, 2018

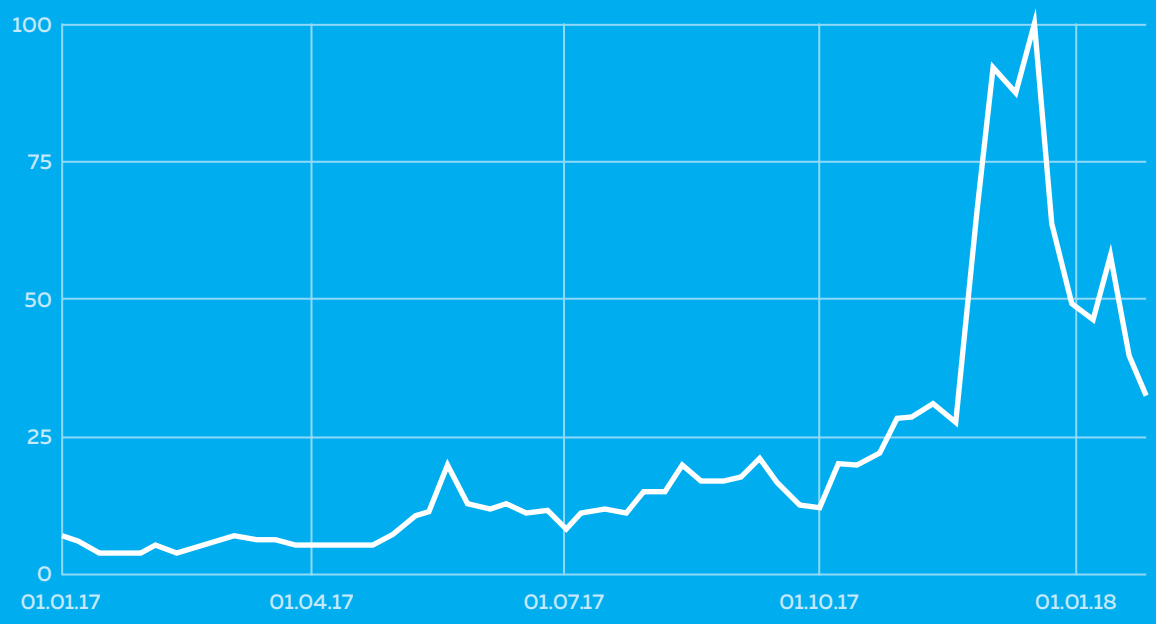


Figure 3: "Bitcoin" searches in Google dynamics
Source: Google Trends [1]

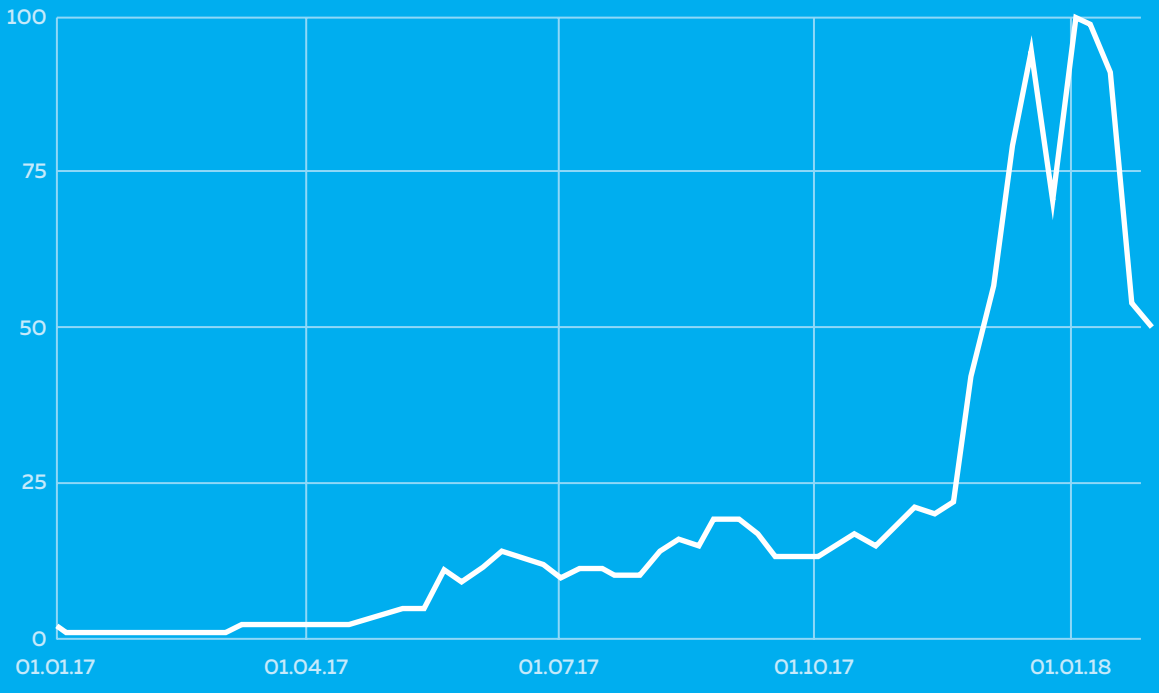


Figure 4: "Cryptocurrency" searches in Google dynamics
Source: Google Trends [2]

3.3. FACTORS BEHIND AN EXPLOSIVE GROWTH OF LEAKS

The significant growth in the number of compromised accounts coincides with the growing people's interest in cryptocurrencies.
According to Google Trends, the highest interest to the topic of cryptocurrencies peaked at the end of 2017.

"Bitcoin" was named second most popular topic in Global news by Google. It became more popular than significant geopolitical and environmental issues of 2017.

The search query "How to buy bitcoin" also made it TOP-3 in 2017 [6].

***

The end of 2017 set records in global cryptocurrency market capitalization. On January 3, 2018 the overall value of the global cryptocurrency market surpassed $700 billion, and exceeded $800 billion for the first time on January 7, 2018. This figure is only slightly less than the capitalization of Apple on January 8, 2018, which amounted to $885 billion. During the first week of January, market capitalization increased by approximately $250 billion (by 44%).

Bitcoin hit a new record reaching $20,000 in December 2017. Its value doubled the $10,000 figure it reached in late November.

TOP SEARCH QUERIES IN 2017
1. Hurricane Irma
2. Bitcoin
3. Las Vegas Shooting
4. North Korea
5. Solar Eclipse

Figure 5: Top search queries in 2017
Source: Google Trends Global, 2017 [3]

Such interest from the general public led to mass registration on cryptocurrency trading platforms. At some point cryptocurrency exchanges were adding 100,000+ users per day [7]. In a blog post released mid-December last year, US-based exchange Kraken said it was receiving 50,000 new user registrations per day, plus 10,000 new support tickets, a sizable increase on previous quarter sign-ups [8].

It provoked reaction from exchanges in a form of restrictive measures. They were under pressure to keep up with the soaring growth of the booming digital coin market. In late December 2017 at least three cryptocurrency exchanges — Bittrex, Bitfinex, and CEX.io — stopped onboarding new users altogether [9].

Binance exchange had to temporary disable new registrations in January 2017 in order to allow for an infrastructure upgrade after adding 240,000 users in just one hour [10]. Mr. Changpeng Zhao, its founder and CEO, revealed in his twitter it was "just too much demand" [11].

Some exchanges introduce daily/weekly/monthly buy and sell limits, e.g. Bittrex (100 BTC withdrawal limit), HitBTC ($10,000 limit for daily deposit & withdrawal), CEX.io ($10,000 daily deposit & withdrawal limit), Poloniex ($25,000 limit), GDAX ($10,000 daily deposit & withdrawal limit).

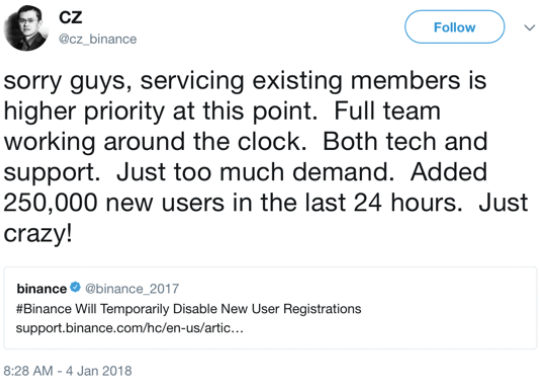


Figure 8: Twitter post by Mr. Changpeng Zhao, the Binance founder

Figure 6: Total cryptocurrency market capitalization
Source: coinmarketcap.com [4]

Figure 7. Bitcoin (USD) Price
Source: coindesk.com [5]

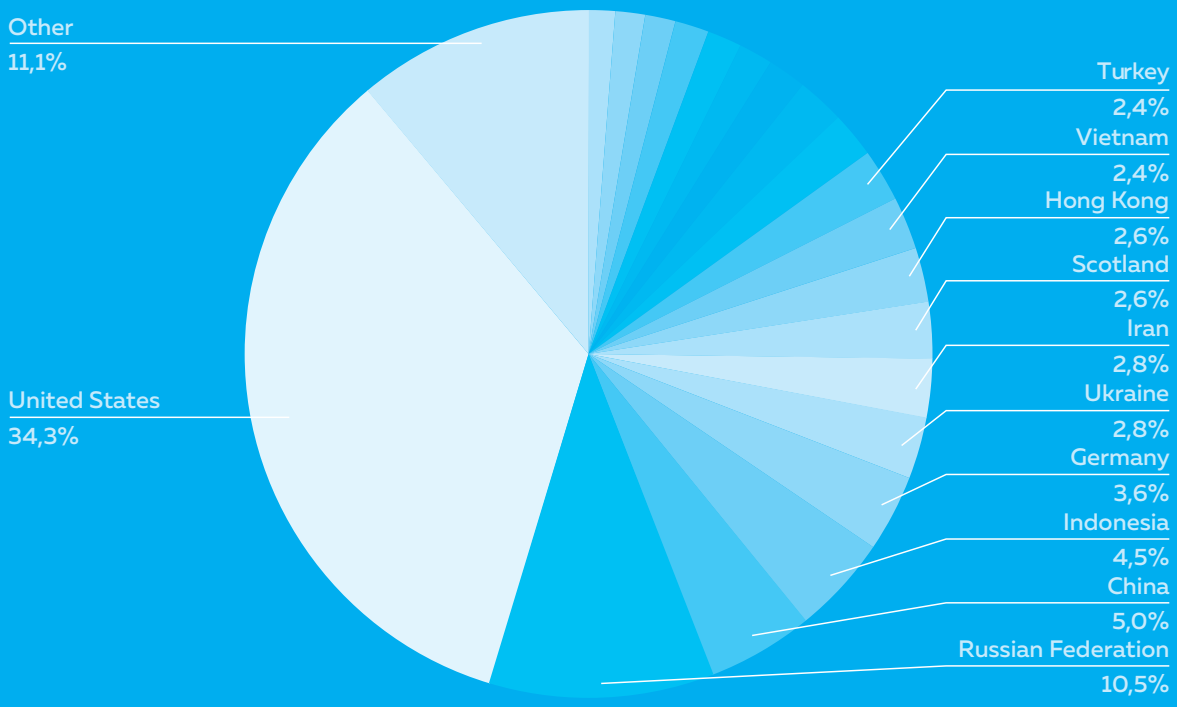


Figure 9: Victims distribution by countries
Source: Group-IB, 2018

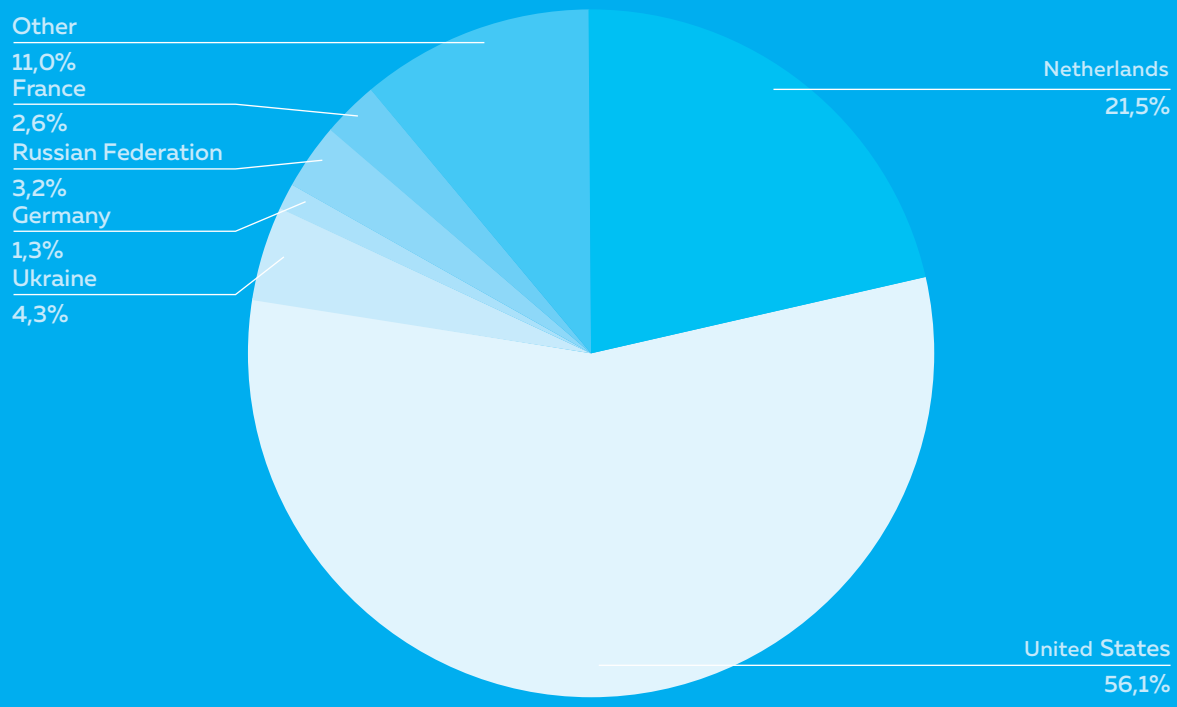


Figure 10: Cybercriminals host countries
Source: Group-IB, 2018

3.4. VICTIMS DISTRIBUTION BY COUNTRIES

Compromised accounts in our sample belong to users from all over the globe. However, TOP-3 countries are the USA, Russian Federation, China, with every third user from the USA.

These results represent the most active countries in the cryptocurrency industry: most ICO projects in 2017 originated in the USA and Russian Federation [12].

***

When we analyzed such distribution, our first assumption was that cybercriminals had used "bulletproof" hosts - a service provided by some web hosting providers that allows their customers significant tolerance in the kinds of material they may upload and distribute. We found only 1 such host in our sample. However, it is a common practice when a criminal buys a legitimate hosting on a black market via a reseller, who helps the criminal to manage the host: this person changes IP-addresses, replies to abuses, etc.

We assume the USA and the Netherlands are used in 3/4 of cases due to the following reasons: the infrastructure is relatively cheap (both on the legal and the black market), these locations are major infrastructure hubs guaranteeing low latencies.

3.5. CYBERCRIMINALS' INFRASTRUCTURE

We have identified at least 50 active botnets behind the mentioned leaks. These botnets are managed from different IP-addresses (C&C) around the globe.

The cybercriminals' infrastructure is distributed geographically as follows:

- most of the hosts are concentrated in the USA (56,1%);
- the Netherlands ranked the second (21,5%) most popular location, followed by Ukraine (4,3%) and Russian Federation (3,2%).

Several IP-addresses in our sample are related to proxy services intended to hide true location of the C&C (e.g. Cloudflare, Blazingfast, etc).

3.6. MALICIOUS SOFTWARE

Below are several examples of malicious software used by cybercriminals to steal user accounts examined in this study

3.6.1. AZORult

AZORult stealer is known since 2016 when it appeared on underground market. This malware is able to steal passwords from popular browsers and dat files of popular crypto wallets.

First advertisements about AZORult selling were detected on underground forums in Spring 2016. New version "AZORult2" was released in 2017. Also, AZORult obtained updates during 2017. Now it has the following functions.

- Stealing passwords from browsers, email clients, FTP-clients, IM-clients: Chrome, Mozilla Firefox, Opera, Yandex Browser, Comodo Dragon, Internet Explorer, Microsoft Edge, Outlook, Thunderbird, Amigo, Pidgin, PSI, PSI + and others.
- Stealing cookies files, data from autocomplete forms in browsers Chrome, Mozilla Firefox, Opera, Yandex Browser, Comodo Dragon, Amigo, etc.
- Stealing banking cards' data from Chrome-like browsers.
- Collecting dat files from popular crypto wallets.
- Collecting files from Skype and files from victim's desktop.
- Collecting information about victim's system (ip/comp/user, list of processes, list of applications).

3.6.2. Pony Formgrabber

Pony Formgrabber has been used by cybercriminals since 2012. This malware is aimed at obtaining users' authentication data. This information is being gathered from config files, databases, secret storages of more than 70 programmes on the victim's computer.

After the malware is launched, it gathers information about OS and its main language, steals user's credentials and transfers this data to the corresponding C&C server. Sources of information may include: FTP-clients, Web-browsers, E-mail passwords (POP3, IMAP, SMTP), Certificates for digital signatures, RDP passwords collection (Remote Desktop Connection), dat collection (bitcoin key).

3.6.3. Qbot aka Quakbot

Qbot, also known as Quakbot, is a network-aware worm with backdoor capabilities, primarily designed as a credential harvester. It can download and execute files, delete itself, replicate itself across network, terminate processes in an OS. After infecting system Qbot injects into explorer.exe and browser processes. All stollen data will be collected and sent to FTP servers.

It is an old threat and was well-described by Symantec back in 2009. In December 2015, several researchers reported that websites hosting the Rig Exploit Kit were serving an updated version of Qbot. Then in January 2016, over 500 devices at a large public organisation were infected with Qbot.

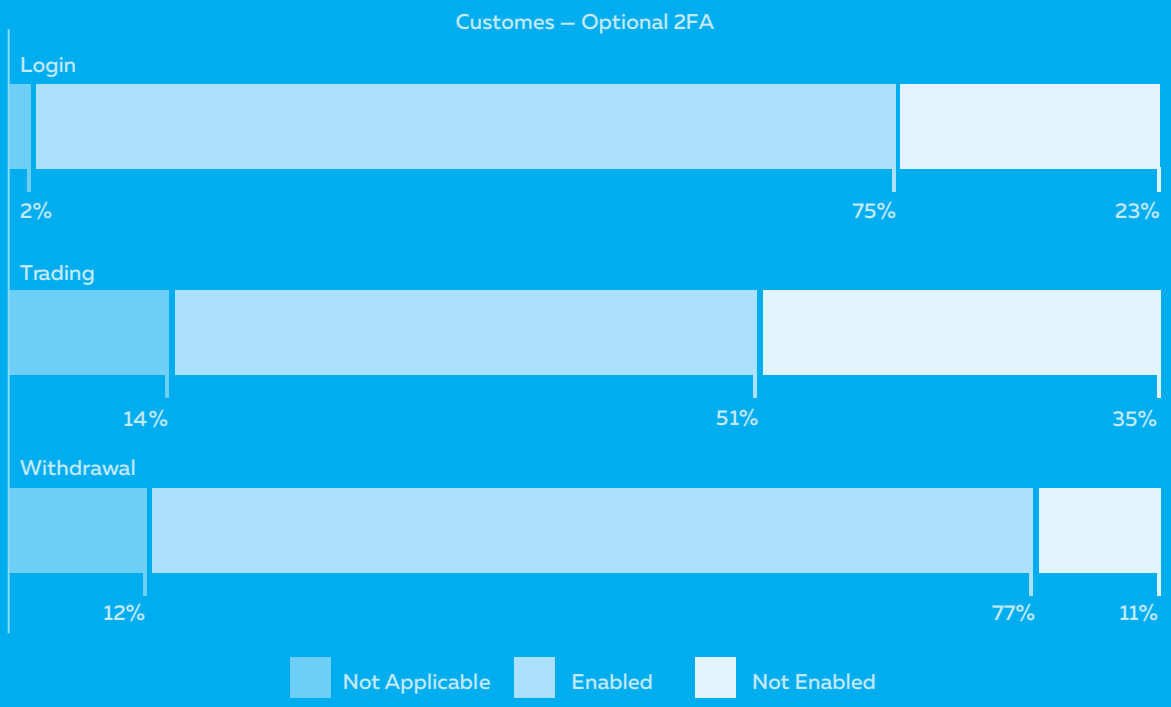


Figure 11: Exchanges and their policy regarding optional 2FA
Source: Cambridge Centre for Alternative Finance, 2017 [13]

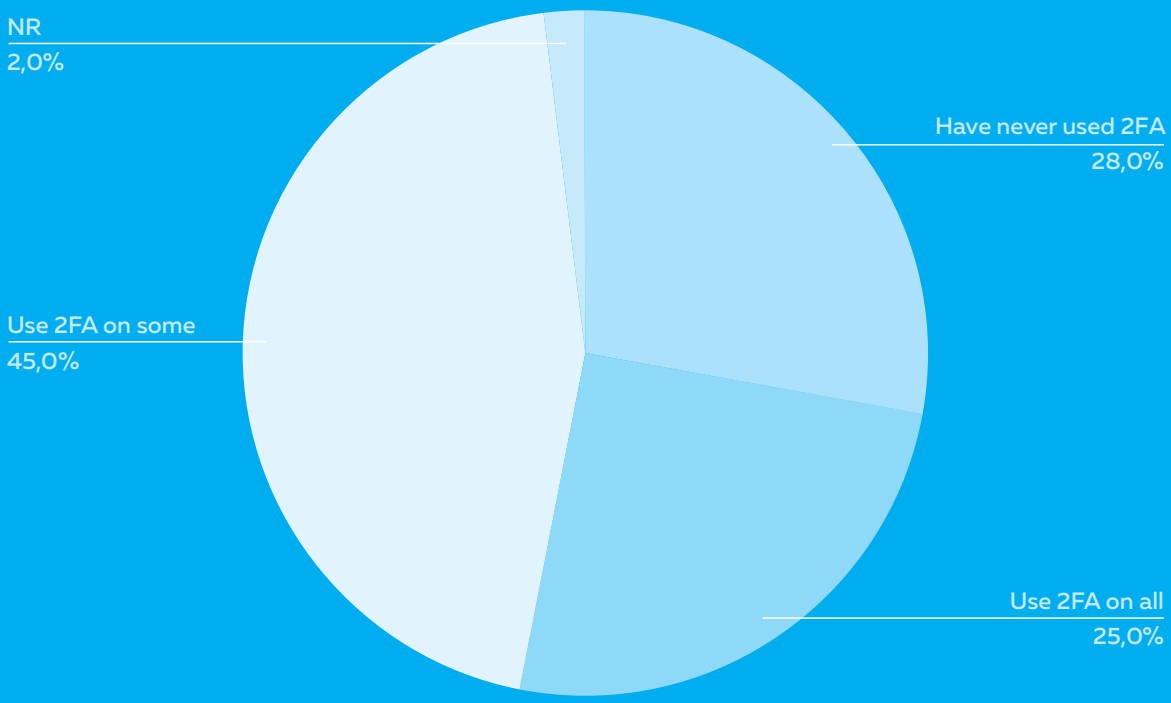


Figure 12: Usage of 2FA
Source: University of Maryland and John Hopkins University, 2016 [14]

3.7. REASONS OF SUCCESSFUL CYBERATTACKS

3.7.1. Two-factor authentication functional is not available in many cases

Leaked account authentication data can lead to the cryptocurrency stolen by a criminal. One of the measures that helps to avoid illegal disposition of funds is usage of a second "factor" that is required to confirm the transaction. Two-factor authentication (2FA) is the most widely used form of a multi-factor authentication, which requires the user to provide two "factors" in order to identify himself (e.g. a unique generated token or sms in addition to the password).

According to the study by Cambridge Centre for Alternative Finance, 75% of exchanges provide optional 2FA for users to log into their accounts and only 23% consider it obligatory. Only 35% of services make 2FA obligatory for trading transactions and 11% oblige their users to enable it for withdrawal. Thus, less than a half of the cryptocurrency exchanges consider 2FA activation to be a crucial measure to prevent any unauthorized access to accounts, and most of them provide it only in an optional format. There are also notable differences between small and large exchanges: 80% of large exchanges have 2FA enabled for all listed actions compared to 32% of small exchanges [13].

It is important to note that 2FA is an optional security feature that most exchanges offer to their customers and encourage use, but that users are not required to activate 2FA.

3.7.2. When 2FA is available, users generally do not use it

According to the joint University of Maryland and Johns Hopkins University study [14], approximately 28% of people have never used 2FA. 64% of them had never seen information about it nor had been prompted to use this security strategy. Only 25% of respondents used it on all of the devices or services that offered it, while 45% enabled 2FA on some, but not all services (Figure 12).

Their findings correspond with Duo Labs Report [15], according to which only 28% of people are using 2FA and over half of the respondents (56%) had not even heard of 2FA in the first place.

In a presentation at Usenix's Enigma 2018 security conference in California, Google software engineer Mr. Grzegorz Milka revealed that today less than 10% of active Google accounts use two-step authentication to lock down their services [16].

3.7.3. Users fail to choose strong and long passwords

According to Verizon Data Breach Investigations Report, 81% of hacking related breaches leveraged either stolen passwords and/or weak or guessable passwords [17].

According to the study by Dashlane [31] that was conducted on the basis of password protocols of 35 leading cryptocurrency exchanges, it was found that more than 70% of platforms allow users to protect their accounts with weak passwords. The researchers found that about 43% of sites allow the users to create accounts using passwords with seven or fewer characters, and 34% do not require alphanumeric passwords. The study also indicated that the testers were able to create trading accounts with such passwords as "12345", "password" or just a repeating letter. As a result, Dashlane evaluated the password security requirements on the exchanges at the beginning of 2018 on a scale of one to five.

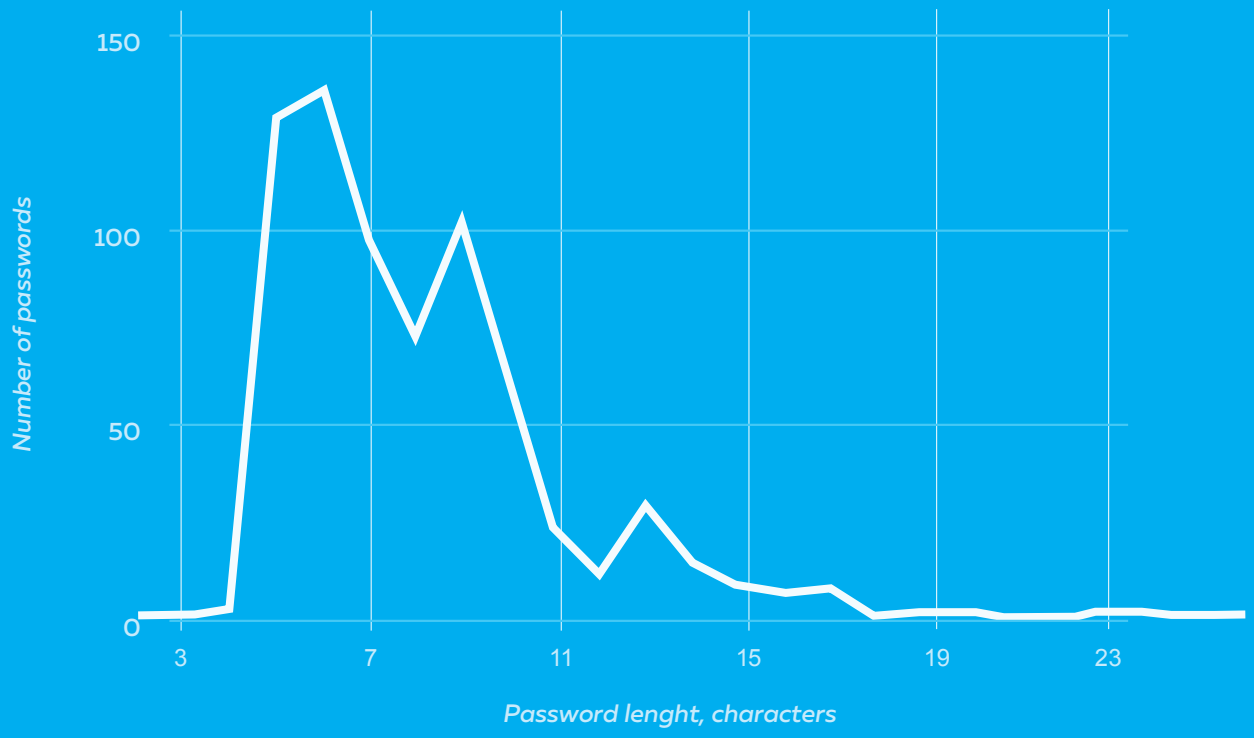


Figure 13: Leaked password length
Source: Group-IB, 2018

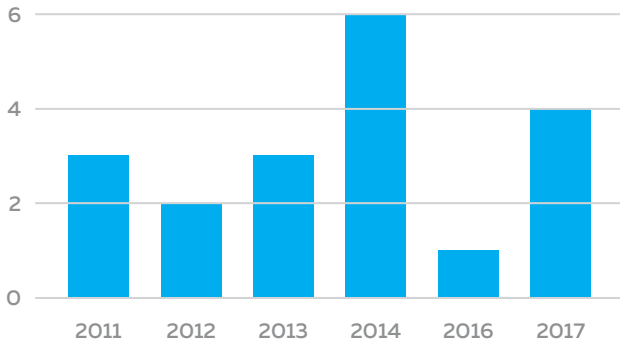


Figure 14: Exchanges annual distribution according to the foundation year
Source: Group-IB, 2018

3.8. Exchanges and Related Data Breaches

At the moment there is no cryptocurrency exchange that would provide its users with absolute security – whether it is a large exchange with a large team of highly paid engineers and programmers or a newcomer to the market. The initial sample consisted of 19 largest cryptocurrency exchanges by capitalization, most of which were created before 2017.

BITSTAMP
Date of breach: January 4, 2015
Amount stolen/lost: 19,000 BTC ($5,1 million)
Founded in 2011 as an alternative to Mt.Gox this exchange also was not much of a safe alternative [20]. In January 2015 some of the operational wallets of Bitstamp were hacked, which led to the loss of about 19,000 BTC. A few weeks before the incident, many employees of Bitstamp have suffered from phishing attacks. Files with malware were sent via personal emails and messages in Skype.

POLONIEX
Date of breach: March 4, 2014
Amount stolen/lost: 12,3% of all BTCs (97 BTC)
Poloniex is one of the busiest exchanges of Bitcoin and altcoins. Basically, the hackers exploited a faulty withdrawal code of Poloniex. Soon after the hack, Poloniex suspended operations for some time and declared in the forum that funds of all Poloniex holders would be reduced by 12.3%. Thus, Poloniex distributed losses among all the users, avoiding panic withdrawal of funds, as a result of which some traders could completely lose their coins [22].

HITBTC
Date of breach: early 2015
HitBTC was hacked at around the same time as BTER and Excoin. However, it did not disclose how many coins were stolen and commented that no user funds were affected [21].

HUOBI
Date of breach: late 2015
Rumours are it was probably hacked: SpeedflyChris (on Reddit) found a big transfer 12,000 BTC with Chinese exchange Huobi in 2015, and put forward the theory that the Chinese exchange was also hacked. However, Huobi denies hacking and claims that it was a normal transaction. Probably Huobi hid "small" in the framework of the burglary, in order not to create panic among the customers [23] [24].

BITFINEX
Date of breach: August 2, 2016
Amount stolen/lost: 120,000 BTC (worth about $72 million at the time) [18]
Attackers exploited a vulnerability in the multi-sig wallet architecture of Bitfinex and BitGo. Multi-Sig was considered to be more secure by Creating several private keys distributed between different parties, since all the participants needed confirmation to access the wallet. In this case, Bitfinex had two keys and BitGo kepto one. However, BitGo servers were not hacked, which means that voluntarily signed the criminals' transations, and multi-sig was not undermined.

BITHUMB
Date of breach: June 29, 2017
Amount stolen/lost: more than $1 million
Bithumb said that the thieves stole a database of users' information off the personal computer of an employee, rather than off the company's internal network. The attackers allegedly got access to the names, email addresses, and mobile phone numbers (no passwords, apparently), of more than 31,800 customers [19].


04

04— Recommen-dations

RECOMMENDATIONS

Security is responsibility of both users and cryptocurrency exchanges

4.1. For users

- Choose strong and complex passwords.
- Use different emails and passwords on different exchanges.
- Turn on two-factor authentication wherever possible.
- Avoid using an exchange that does not provide 2FA.
- Change your attitude - the threat is real.
- Be very careful and check everything twice.
- Avoid using public Wi-Fi.
- Keep your devices and home infrastructure clean and updated.
- Control your online presence.
- Avoid advertising possession of cryptocurrencies.

4.2. For exchanges

- Enable 2FA and make it obligatory, not optional.
- Perform regular audits of IT infrastructure and related processes.
- Allocate resources for training and awareness-raising as regards personnel security - from managers to ordinary employees.
- Develop a plan for rapid response to information security incidents.
- Use Threat Intelligence.
- Implement anti-phishing system.
- Install Anti-APT solutions like Group-IB Threat Detection System.

4.3. FRAUD PROTECTION FOR CRYPTO-EXCHANGES

Advanced user authentication and fraud prevention for cryptoindustry (Group-IB Secure Portal)

PRECISELY IDENTIFIES LEGITIMATE USERS

Cutting-edge technologies for authentication with precision close to that of the iris recognition.

> Device fingerprinting — identification of a user device based on it's unique configurations.
>
> User behaviour analysis (UBA) — identification of a man behind the device based on his unique behaviour profile.

DISCOVERS NEW FRAUD INDICATORS AND SCHEMES

We use machine learning algorithms to detect anomalies in users' behavior. We label those related with fraud, and enrich the predictive model with new parameters. This allows us to constantly discover new fraudulent schemes across different sessions and multiple accounts and notfy our clients about malicious actors.

DETECTS SIGNS OF FRAUD PREPARATION

Secure Portal leverages unique data from GIB Forensic Lab and the world-class Threat Intelligence to detect fraud at the earliest stages and raise a red flag before the damage is done.

Malware infected devices

Malware indicators of compromise (IOCs) and IMEI of infected mobile devices instantly reveal signs of remote access and malicious activity on user's device.

Compromised credentials

Thousands of compromised e-mails, logins, wallets, private keys extracted from botnets and phishing kits provide opportunity to stop criminals at the sign-in page.

Obfuscation

TOR node, Socks-proxy and other suspicious IP.

- A light JavaScript module runs seamlessly and doesn't affect page loading speed
- All data transferred for the analysis is anonymised, SP has no access to your clients' personal information
- Cloud interface with detailed information on suspicious sessions, statistics and search
- Realtime API for instant response

For more details:
www.group-ib.com/secure_portal

05

05—
Research Team

WE WOULD LIKE TO THANK GROUP-IB THREAT INTELLIGENCE TEAM FOR THEIR GUIDANCE AND SUPPORT

RESEARCH TEAM

Ruslan Yusufov
Director, Special Projects

Elizaveta Chalenko
Analyst, Private Client Services

06

06—
Methodology

THE SAMPLE CONSISTS OF 720 ACCOUNT LEAKS OCCURRED FROM 2014 TILL 2018 RELATED TO 19 CRYPTOCURRENCY EXCHANGES AND THE CORRESPONDING DATA

THE EXCHANGES IN QUESTION INCLUDE SOME OF THE LARGEST EXCHANGES IN TERMS OF THEIR TRADING VOLUME IN JANUARY 2018

METHODOLOGY

The present study aims to estimate the number of account leaks from cryptocurrency exchanges and to analyze their nature. We have made an attempt to define the reasons of these leaks and provide further recommendations for both exchanges and victims.

The object of this study is compromised accounts of cryptocurrency exchanges' users.

The sample consists of 720 account leaks occurred from 2014 till 2018 related to 19 cryptocurrency exchanges and the corresponding data. The exchanges in question include some of the largest exchanges in terms of their trading volume in January 2018.

The research team collected data on the compromised user accounts obtained from Group-IB Threat Intelligence (see Annex 2 for more details).

We contacted all exchanges from our sample informing them about the ongoing study. Prior to this release every exchange had a chance to obtain all the information in our possession related to the leaks of their users and to take the appropriate measures.

07

07—
Glossary

GLOSSARY

Cryptocurrency
A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank [25].

Command-and-control (C&C) server
A server used to remotely send malicious commands and receive outputs of machines part of a botnet or a compromised network of computers.

Cryptocurrency exchange or digital currency exchanges (DCE)
A market maker who exchanges legal tender for electronic currency, or who exchanges one electronic currency for another. A digital currency exchanger charges a commission for this type of transaction, with transactions often occurring through websites rather than physical locations. This commission can be in the form of a fee or taking the bid/ask spread [26].

Threat Intelligence or cyber threat intelligence (CTI)
Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard [29].

Botnet
A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam [27].

Malicious software (malware)
A variety of forms of harmful or intrusive software which are specifically designed to disrupt, damage, or gain authorized access to a computer system [28], including computer viruses, worms, trojans, ransomware, spyware, and other malicious programs.

08—
Annexes

ANNEX 1: CRYPTOCURRENCY EXCHANGES OVERVIEW

Name	Year	Volume 24H 31.01.18	Trading Pairs	Number of Leaks	Incidents
Binance	2017	$2 222 672 484	252	39	No
Bit-Z	2016	$236 374 114	69	2	No
Bitfinex	2012	$1 881 119 042	103	48	Yes
Bithumb	2013	$1 783 489 020	12	1	Yes
Bitstamp	2011	$514 697 740	14	48	Yes
Bittrex	2014	$743 909 464	261	112	No
BTCC	2011	$103 530 000	4	9	No
CEX.io	2013	$53 713 354	23	95	No
Coinone	2014	$222 211 947	9	3	No
Gate.io	2017	$103 092 086	226	4	No
GDAX	2012	$926 158 460	12	2	No
Gemini	2014	$277 474 980	3	19	No
HitBTC	2014	$494 363 548	421	83	Yes
Huobi	2013	$1 256 939 172	171	10	Probably
Kraken	2011	$884 409 505	45	61	No
KuCoin	2017	$157 142 723	212	2	No
OKEx	2014	$2 701 097 580	422	5	No
Poloniex	2014	$383 900 716	99	174	Yes
Wex.nz	2017	$69 440 237	35	3	No

Trading data source: coinmarketcap.com, trading volume on January 30, 2018 [30]

Dashboard
Compromised data
Threats
Attacks
Hacktivism
Suspicious IP
Targeted malware
Brand abuse
Administration

Dashboard

Potential damage

Adjust estimates by altering the parameters used in the calculation by altering the numbers in the account settings section (gear icon)

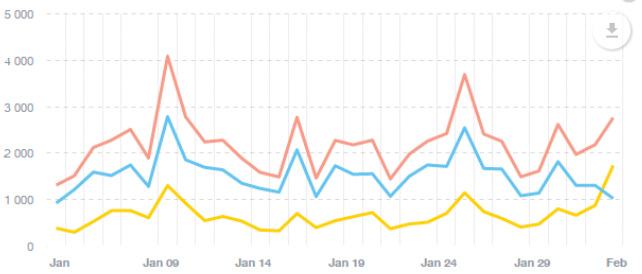
Range: 2017-01-04 - 2017-02-03

Total	Compromised Account Credentials	Phishing	Compromised Credit Cards
$40 023 625	7 891 $4 931 875	68 085 $33 560 250	12 252 $1 531 500
$108 000 ↑	1 908 ↑	-7 398 ↓	4 824 ↑

Phishing

Range: 2017-01-04 - 2017-02-03

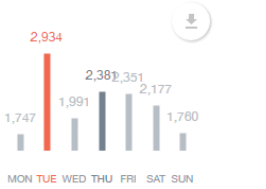
Malicious events · Events Blocked · Active events



68085 Phishing Identified

23 Average Take-Down time

29 Average Global Take-Down Time



Days of Highest Probability for Phishing Attacks

Malware

Malware targeting your business and your clients

for Windows · for Android

- Honli
- PONY FORMGRABBER
- Phishing
- Ramnit
- Gootkit

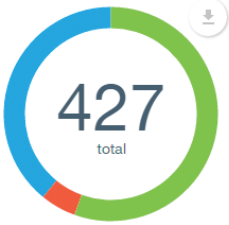
Details

Malicious e-mails

Range: 2017-01-04 - 2017-02-03

Distribution of drop email accounts capturing compromised credentials

gmail.com · yahoo.com



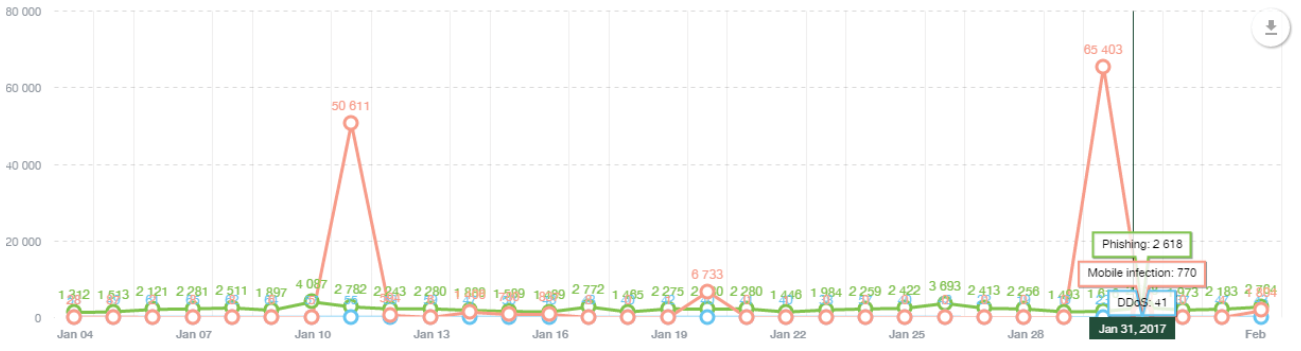
- admin@website.com
- supertool@mxtoolbox.com
- wirez@googledocs.org
- team_pbggggg@yahoo.com
- hahaha@ahaha.com

Details

Attacks

Range: 2017-01-04 - 2017-02-03

Phishing · DDoS · Mobile infection



Attacking Infrastructure

Range: 2017-01-04 - 2017-02-03

Phishing server · Phishing Kit email · Client location

ANNEX 2:
GROUP-IB THREAT INTELLIGENCE

Group-IB has been pioneering incident response and cybercrime investigation practices in Russia since 2003. This experience and understanding of threat actors' behaviours have evolved from our own investigation tool to intelligence gathering network which now feeds Group-IB Threat Intelligence.

Threat Intelligence collects and analyzes large amounts of unique and proprietary information to deliver tailored, trusted and actionable intelligence in order to predict risks, while preventing and mitigating any targeted attacks. Group-IB private technology based on patented algorithms and machine learning enables to get information which includes data not only on malware control panel or criminal infrastructure - accounts, bank cards, money mules, International Mobile Equipment Identity (IMEIs) but also on when, where and how it has been exposed. We use real-time monitoring and cloud-based services that allows to work with statistics, see and track trends as well as make efficient decisions based on statistical analysis.

For more details:
www.group-ib.com/intelligence

09—
About Group-IB

ABOUT GROUP-IB

GROUP-IB is one of the global leaders in preventing and investigating high-tech crimes and online fraud.

Since 2003, the company has been active in the field of computer forensics and information security, protecting the largest international companies against financial losses and reputational risks. Group-IB has a wealth of experience solving cybercrimes around the world, with a profound and unparalleled expertise regarding Russian-speaking criminal groups.

Group-IB's experience and threat intelligence has been fused into an eco-system of highly sophisticated software and hardware solutions to monitor, identify and prevent cyber threats.

1000+ successful investigations worldwide, 150 of which were of special complexity

80% of high-profile cybercrimes in Russia and CIS are investigated by Group-IB

$300 million returned to our clients due to Group-IB's efforts

For more details:
www.group-ib.com

- The largest computer forensics laboratory in Eastern Europe, with an experienced investigation team capable of identifying suspects, collecting and analyzing evidence
- CERT-GIB — Group IB's official computer emergency response team monitor online activity 24/7 in order to identify and respond to any incidents or security breaches
- A wide range of services to test the readiness of your staff and partners in the event of a real-world attack. With security assessment, proactive DDoS, and penetration testing, you can be certain you are protected from any vulnerability.

Our mission is to protect clients in cyberspace with innovative products and services.

GROUP-IB CRYPTO

Group-IB started to defend crypto industry companies in September 2017. Our team was able to protect ICOs in a total amount of about $300 million in 4 months last year. At present, Group-IB is successfully defending ICO-projects in Russia and on the international market. We have already protected Blackmoon, Tokenbox, BANKEX, WAVES and other clients.

For more details:
www.group-ib.com/crypto

Official Interpol and Europol partner

The first Russian provider of threat intelligence solutions included in the Gartner and Forrester reports

Recommended by the Organization for Security and Co-operation in Europe (OSCE)

Russia Threat Intelligence Security Services Market Leader according to IDC

One of the 7 most influential companies in the cyber security sphere according to Business Insider

Permanent member of the World Economic Forum


10

10— References

REFERENCES

[1] Google Trends. Available at: https://trends.google.com/trends/explore?date=2017-01-01%202018-01-31&q=bitcoin (Accessed: February 2, 2018)

[2] Google Trends. Available at: https://trends.google.com/trends/explore?date=2017-01-01%202018-01-31&q=bitcoin (Accessed: February 2, 2018)

[3] Google Trends. Available at: https://trends.google.com/trends/yis/2017/GLOBAL/ (Accessed: February 2, 2018)

[4] CoinMarketCap. Cryptocurrency Market Capitalizations. Available at: https://coinmarketcap.com/charts/ (Accessed: February 2, 2018)

[5] Coindesk. Available at: https://www.coindesk.com/price/ (Accessed: February 2, 2018)

[6] Google Trends. Available at: https://trends.google.com/trends/yis/2017/GLOBAL/ (Accessed: February 2, 2018)

[7] Cointelegraph, Jan. 2018. "Exponential Growth: Cryptocurrency Exchanges Are Adding 100,000+ Users Per Day". Available at: https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day (Accessed: February 2, 2018)

[8] Kraken Blog, Dec. 2017. "Degraded Service, Upgrade Next Week". Available at: https://blog.kraken.com/post/1399/degraded-service-upgrade-next-week/ (Accessed: February 2, 2018)

[9] UK Business Insider, Dec. 2017. "Some of the biggest crypto exchanges are shutting out new users because they can't keep up with demand". Available at: http://uk.businessinsider.com/crypto-exchanges-are-shutting-out-new-users-because-they-cant-keep-up-with-demand-2017-12 (Accessed: February 2, 2018)

[10] UK Independent, Jan. 2018. "Binance: World's top cryptocurrency exchange adds 240,000 users in just one hour". Available at: http://www.independent.co.uk/news/business/news/binance-bitcoin-latest-cryptocurrency-exchange-trading-users-increase-numbers-hong-kong-a8153496.html (Accessed: February 2, 2018)

[11] Changpeng Zhao Twitter. Available at: https://twitter.com/cz_binance/status/948954415662219264?lang=en (Accessed: February 2, 2018)

[12] EY & Group-IB, 2017. "EY Research: Initial Coin Offerings (ICOs)". Available at: http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf (Accessed: February 2, 2018)

[13] Cambridge Centre for Alternative Finance, 2017. "Global Cryptocurrency Benchmarking Study". Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf (Accessed: February 2, 2018)

[14] University of Maryland and Johns Hopkins University, 2016. "How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior". Available at: https://dl.acm.org/citation.cfm?doid=2976749.2978307 and https://www.umiacs.umd.edu/~mmazurek/papers/ccs2016-learned-secure.pdf (Accessed: February 8, 2018)

[15] Duo Labs, 2017. "State of the Auth. Experiences and Perceptions of Multi-Factor Authentication". Available at: https://duo.com/assets/ebooks/state-of-the-auth.pdf (Accessed: February 8, 2018)

[16] The Register, Jan. 2018. "Who's using 2FA?". Available at: http://www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/ (Accessed: February 2, 2018)

[17] Verizon, 2017. "Data Breach Investigations Report". Available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ (Accessed: February 2, 2018)

[18] Fortune, Aug. 2016. "Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong". Available at: http://fortune.com/2016/08/03/bitcoin-stolen-bitfinex-hack-hong-kong/ (Accessed: February 2, 2018)

[19] Fortune, July 2017. "One of the Biggest Ethereum and Bitcoin Exchanges Got Hacked". Available at: http://fortune.com/2017/07/05/bitcoin-ethereum-bithumb-hack/ (Accessed: February 2, 2018)

[20] Coindesk, July 2015. "Details of $5 Million Bitstamp Hack Revealed". Available at: https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/ (Accessed: February 2, 2018)

[21] CoinTelegraph, Feb. 2015. "3-Way Bitcoin Exchange Hack Dwarfed by 15-month $300 million Bank Heist". Available at: https://cointelegraph.com/news/3-way-bitcoin-exchange-hack-dwarfed-by-15-month-us300-million-bank-heist (Accessed: February 2, 2018)

[22] Coindesk, Mar. 2014. "Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack". Available at: https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/ (Accessed: February 2, 2018)

[23] Steemit, Dec. 2017. "Attacked the Tether may be involved in other major hacks". Available at: https://steemit.com/bitcoin/@rollsman/attacked-the-tether-may-be-involved-in-other-major-hacks (Accessed: February 2, 2018)

[24] David Gerard Blog. Available at: https://davidgerard.co.uk/blockchain/2017/11/22/correction-huobi-wasnt-hacked-in-2015-but-the-2015-bitstamp-hacker-did-withdraw-12000-btc-from-huobi/ (Accessed: February 2, 2018)

[25] CoinMarketCap. Available at: https://coinmarketcap.com/exchanges/volume/24-hour/ (Accessed: January 31, 2018)

[26] Oxford Dictionaries. "Cryptocurrency". Available at: https://en.oxforddictionaries.com/definition/cryptocurrency (Accessed: February 2, 2018)

[27] Investopedia . "Digital Currency Exchanger - DCE". Available at: https://www.investopedia.com/terms/d/digital-currency-exchanger-dce.asp (Accessed: February 2, 2018)

[28] Oxford Dictionaries. "Botnet". Available at: https://en.oxforddictionaries.com/definition/botnet (Accessed: February 2, 2018)

[29] Oxford Dictionaries. "Malware". Available at: https://en.oxforddictionaries.com/definition/malware (Accessed: February 2, 2018)

[30] Gartner. "Threat Intelligence". Available at: https://www.gartner.com/doc/2487216/definition-threat-intelligence (Accessed: February 2, 2018)

[31] Dashlane, March 2018. "Cryptocurrency Exchange Password Power Rankings 2018". Available at: https://blog.dashlane.com/cryptocurrency-exchange-password-power-rankings-2018/ (Accessed: March 22, 2018)

11—
Contacts

GROUP-IB
Global cyber security company

Progress Plaza Business Center
Sharikopodshipnikovskaya, bld. 1, Fl. 9,
Moscow, Russia

Skolkovo Innovation Center
Bolshoy, bld. 42, Core 4, Fl. 4,
Moscow, Russia

+7 495 984-33-64
crypto@group-ib.com
group-ib.com/crypto

GROUP IB


GLOBAL CYBER SECURITY COMPANY
GIB
GLOBAL CYBER SECURITY COMPANY