New Segment of the Shadow Digital Economy

Serghei Ohrimenco, Grigori Borta

ASEM, Chisinau, Moldova
osa@ase.md, grigori.borta@gmail.com

Abstract. The article presents the results of the analysis of the threat landscape in the shadow digital economy. The development of industrialization and digitalization of the economy is associated with the emergence of qualitatively new threats. It was concluded that, along with such traditional segments as the development and implementation of cyber weapons, targeted attacks and ATR groups, identity theft, etc., attacks on crypto-exchanges, crypto exchangers and money laundering using cryptocurrencies are emerging.

Keywords. Shadow digital economy, Segments of the shadow digital economy, Cryptoeconomics, Attacks on crypto-exchanges.

1. Introduction

Shadow activity attracts the attention of specialists in many countries. In this work, an attempt is made to outline the landscape of the shadow digital economy, highlight its main segments and describe a new field for counteraction, targeted at new emerging threats, such as criminal operations on cryptocurrency exchange and crypto exchanges.

This work is a logical continuation of the authors' publications on the topic of research related to the definition of the shadow digital economy (SDE) category, segmentation of the spheres of illegal activity, etc.

As a result of the research, the authors propose the following definitions of the shadow digital economy:

• shadow digital economy is a specific domain of economic activity with its inherent structure and system of economic relations. Specificity is determined by the illegality, informality, as well as the criminal nature of economic activity and concealment of income;

• from an economic point of view - the sector of economic relations, covering all types of production and economic activities, which in their direction, content, nature and form contradict the requirements of the existing legislation and are carried out in spite of state regulation of the economy and bypassing control over it;

• from a technological point of view, it is an individual and collective activity that is illegal, associated with the design, development, distribution, support and use of information and communication technology components, hidden from society.

Thus, SDE is all the illegal and hidden products and services that use and are based on information technology. The most important economic elements in this area are the following: illegal economic relations, illegal activities related to the production, distribution and use of prohibited products and services. Advances in information technology are creating new threats:

• Attacks are becoming more sophisticated through automation and the use of artificial intelligence and machine learning methods;

• Connection of a huge number of new unprotected devices (industrial Internet or Internet of things, as a data transfer network between physical objects, which are equipped

with built-in means and technologies of interaction with each other or with the external environment). Hackers use devices such as video cameras, coffee machines, etc to enter the network;

• As a result, the number of targets for attacks increases sharply.

It should be noted that blockchain technology instills trust in customers and proves the security of cryptocurrency transactions. However, the development of the cryptocurrency business has attracted attention of computer fraudsters. They paid attention and efforts to the activities of exchanges that specialized in buying and selling cryptocurrencies.

2. Main segments of the shadow digital economy

The authors examined the composition of the main criminal products and services related to SDE. However, their spectrum is constantly changing, new segments appear that require research and description. In previous articles, the following segments were considered: cyber weapons, as the concentration of all the achievements of information and communication technologies at the level of counteraction between states; targeted attacks and ATR groups; identity theft, etc.

It seems necessary to analyze the existing approaches to the classification of products and services, as well as to consider the segmentation of SDE. The generalized structure provides for the division into products and services, taking into account their constant variability. This property is decisive, since the achievements of scientific and technological progress and innovations in the field of information and communication technologies provide a rapid changeover of hardware and software platforms. In the information realm, tangible products are extremely few in number and usually refer to hardware, while most of this definition refers to software that is generally considered intangible. It should be noted that many classifications are used in information security practice.

The malware created is targeted at the following industries: hospitality and catering; educational services; finance and insurance; healthcare; information; production; public administration; retail, etc. The same Verizon report suggests a classification of incidents: Crimeware, Cyber-Espionage, Denial-of-Service, Insider and Privilege Misuse, Miscellaneous Errors, Payment Card Skimmers, Point of Sale Intrusions, Physical Theft and Loss, Web Application Attacks and others.

The study by Brandon Levine uses a different classification. There are four groups of malware:

- Banker. This is a kind of malware specially designed to manipulate online banking. Programs in this category use WebInjects (a set of HTML and JavaScript code that displays forms for entering credentials of remote banking systems (RBS) and WebFakes (using fake web pages to trick users into entering confidential information as a method of social engineering);

- Ransomware. This is software used to lock a computer or personal files of a user with the subsequent demand for a ransom for restoring access;

- Stealer. Malicious programs designed to steal passwords stored in the system. May include keylogging malware;

- Miner. Malicious software that uses the resources of an infected information system to generate cryptocurrencies without the knowledge and permission of the system owner.

In addition, the report analyzes a wide range of malware and criminal programs, including GameOver Zeus, Cryptolocker, Dridex, Dyre, Trickbot, Ramnit. The main findings of this study are as follows:

First, it notes that the risk of using malware is clearly underestimated, making it difficult to protect against. This leads to the fact that the losses from the impact of criminal software grow, the countermeasures taken reduce the effectiveness of the confrontation. The impact of criminal software is enormous, and if countering efforts are not significantly increased, the consequences can be more serious and widespread in scope and cost.

Second, the growth of criminal software is steady; the frequency of distribution of new variants is growing from year to year. As a result, criminal software is a more serious threat to business impact than targeted attacks on information systems.

Third, the implementation of criminal software is not expensive and does not require a lot of effort on the part of motivated participants, which ensures that attacks are optimized to achieve profitable goals. The ability to increase agility and change strategies has led to increasingly sophisticated and targeted business assault programs.

Fourth, it is noted that the effectiveness of the efforts of law enforcement agencies to counter criminal software decreases over time. The ability of developers and attackers traditionally outstrips the capabilities of law enforcement agencies in searching, finding and prosecuting by adapting to changing conditions. The attacker models the risk of prosecution based on the practice of law enforcement agencies and is entirely based on the possibility of making a profit. As a result, taking into account such factors as time, geographic location and others, the activities of law enforcement agencies are seriously limited and efforts are reduced to scanty results. At the same time, these factors allow developers and analyzers of criminal software to have spare time to adapt new versions and make their software more "effective" and harmful in relation to users of information systems.

Fifth, it is recognized that crimeware is serious business. Developers model their activities in accordance with corporate standards to maximize profits. An example is the emergence of "crimeware-as-a-service" as a demonstration of its capabilities. Cybercriminals are dramatically changing their toolkits over a three-month period to achieve new results. An additional example is also Cryptomining as an operation. The cryptocurrency market initially peaked at the end of 2017 and began to decline by February 2018. The downward trend in the Bitcoin index was directly reflected in the activity of "Cryptomining as an operation", which fell by more than 50% during the year. The statistical correlation between bitcoin index jumps and the popularity of "Cryptomining as an operation" can be seen as a highly profitable tool for influencing business.

Finally, the goals of cyber fraudsters have changed. Whereas previously the target was the user of a personal computer, now the corporations and corporate victims are the targets. As the danger of real threats grows, organized crime groups have turned to corporations.

Another confirmation of the thesis that crimeware is a serious business is the publication in July 2020 of information that Cerberus is the world's first malware with the function of stealing two-factor authentication codes. The developers of the Android banking Trojan Cerberus intend to sell their entire project.

Bidding will be held in the form of an auction, and the starting price is $ 50 thousand. For $ 100 thousand, the developers are ready to part with their brainchild without haggling. For their money, the buyer will receive the source code of the Trojan, APK, modules, an administration panel, servers, and lists of current and potential customers, an installation guide and scripts necessary for the smooth operation of all components.

For at least one year, Cerberus developers have been actively promoting their services and renting out malware for $ 12,000 a year. Clients also had access to rent for a shorter period ($ 4 thousand for 3 months and $ 7 thousand for 6 months). According to the seller's

publication on one of the Russian-language cybercriminal forums, the business currently generates income of $ 10 thousand per month. According to them, the Cerberus team has disintegrated, and the remaining developers do not have enough time to support the Trojan 24/7.

3. A new segment of the shadow digital economy

A relatively new trend is the attack on crypto exchanges, theft of cryptocurrencies and money laundering. The high market capitalization of certain cryptocurrencies attracts hackers. Consider the main trends in cryptocurrency capitalization as of 01/09/21. As an example, we use the data shown in Table 1.

Table 1. Top 10 cryptocurrencies by market capitalization as of January 9, 2021

Cryptocurrency	Price per coin	Market capitalization
Bitcoin	40 542,52 $	754 321 316 827 $
Ethereum	1 218,19 $	138 640 801 067 $
Tether	0,992037 $	23 477 377 980 $
XPR	0,324559 $	14 590 916 168 $
Litecoin	169,84 $	11 200 359 477 $
Cardano	0,322639 $	9 958 280 954 $
Polkadot	9,37 $	8 909 423 935 $
Bitcoin Cash	454,28 $	8 416 703 785 $
Stellar	0,305411 $	6 672 633 057 $
Chainlink	16,10 $	6 418 005 819 $

Source: Top 100 currencies by market capitalization (https://www.coingecko.com/ru) and CoinMarketCap website (https://coinmarketcap.com/)

For comparison, you can give the data of cryptocurrency quotes as of December 23, 2020. The leaders were the following cryptocurrencies.

Table 2. Current data on the cost of major cryptocurrencies (as of 23.12.2020).

Name	Ticker	Price per coin	Market capitalization
Bitcoin	BTC	23.570	439,57B$
Ethereum	ETH	609,25	69,76B$
Tether	USDT	0,9997	20,47B$
Ripple	XRP	0,31428	14,57B$
Litecoin	LTC	105,212	7,07B$
Bitcoin Cash	BCH	291,12	5,46B$
Chainlink	LINK	11,82	4,74B$

Source: Leading Cryptocurrencies. https://ru.investing.com/crypto/

Increased criminal interest is caused, first, by the increased capitalization of bitcoin. The rise in price to $ 40,000 and above significantly increased the capitalization of the first cryptocurrency, bringing the indicator a little closer to the market value of gold. For example, on January 9, 2021, the cost of bitcoin was $ 40,951. The approximate market value of all mined gold is $ 10.6 trillion. The market capitalization of bitcoin at the end of 2020 is $ 736.3 billion, which is 6.94% of the total value of the precious metal. Bitcoin has surpassed Tencent and Alibaba in market capitalization and is now competing with Facebook. For example, Facebook's market capitalization at the beginning of 2021 is $ 763.644.814.249 versus $ 747.716.811.296 for Bitcoin. The capitalization of the entire cryptocurrency market at the end of 2020 is $ 1.06 trillion. Analysts are wondering about Bitcoin's ability to climb to $ 100,000 per coin before it depreciates. Leading experts do not give an accurate prediction, but agree that the enthusiasm for bitcoin and cryptocurrencies will fade over time, but that it may take another two, three or even four decades before that. Bitcoin is predicted to rise to $ 500,000 and become a new store of value that can surpass gold, but for this, the price of bitcoin must increase 25 times.

One of the relatively new types of attacks or a new direction of the criminal business is the organization of attacks on crypto exchanges and crypto exchangers. The latter appeared about 10 years ago and were used to exchange virtual coins for dollars, euros or another currency at the request of the owner. After a while, a peak in the activity of cryptocurrencies was registered and bitcoin became more popular than the leading currencies.

Group-IB experts analyzed attacks on cryptocurrency exchanges over the past two years and revealed total losses of $882 million. The report indicates that crypto exchanges will become a new target for aggressive hacker groups in 2019, and their efforts will shift from attacks to commercial banks. However, not only crypto exchanges, but also cryptocurrency companies that organize the launch of the ICO, raise funds and provide for the sale of tokens to private investors are put forward as goals.

Table 3.The top 10 cryptocurrencies by capitalization as of October 2020.

Name	**Ticker**	**Price per coin**	**Market capitalization (billion)**
Bitcoin	BTC	$10 610	$196,4
Ethereum	ETH	$340	$38,3
Tether	USDT	$1,00	$15,6
Ripple	XRP	$0,24	$11,1
Bitcoin Cash	BCH	$219,01	$4,05
Binance Coin	BNB	$27,45	$3,9
Polkadot	DOT	$3,81	$3,2
Chainlink	LINK	$8,80	$3,08
Crypto.com Coin	CRO	$0,14	$3,02
Litecoin	LTC	$45,89	$3,01

Source: Cryptocurrency Capitalization: Features and How It Affects Trading.

Cryptocurrency market capitalization exceeded $ 400 billion. The most attention of investors and traders is focused on those cryptocurrencies that have the highest capitalization.

Despite the fact that the comparison of cryptocurrencies in this indicator is considered by some to be not completely objective, it is capitalization that is the main factor determining the interest in a separate coin from not only buyers, but also cyber fraudsters. For comparison, we present data on 10 cryptocurrencies by capitalization at the beginning of October 2020, which are represented in the following table.

During the analysis of the data obtained, Group-IB specialists discovered that more than 10% of the funds raised during the ICO were stolen. This is the period from 2017 to September 2018. More than half of the funds stolen from ICOs were associated with phishing attacks. The goal of the hacker groups was not only the virtual currency itself, but also lists of investors interested in ICOs for the implementation in the future of such actions as blackmail or targeted phishing attacks.

Hacker attacks on exchanges and crypto exchanges can be roughly divided into two stages. The first covers the interval from 2010 to 2016, and is characterized by relatively simple mechanisms of action and, accordingly, the results obtained. For example, in the summer of 2010, Bitcion was hacked and the hacker managed to create a transaction of 184 million bitcoins, with a limited volume of 21 million, which was detected and fixed. In the spring of 2014, Mt.Gox, the third largest exchange in the cryptocurrency market, was hacked. Almost $ 480 million was stolen from the attack, leading to bankruptcy. In early 2015, the BitStamp exchange was hacked and the hackers received only $ 5 million. In the summer of 2016, The DAO, an organization specializing in another cryptocurrency, Ethereum, was hacked. The cybercriminals managed to find a bug in the software, which ensured the theft of $ 50 million in this cryptocurrency. July 2016. Steemit.com is hacked. Hackers who hacked over 250 accounts and stole $ 85,000 in cryptocurrency attacked the social network Steem. August 2016. More than $ 72 million in cryptocurrency was stolen from Bitfinex. The hackers took advantage of the vulnerabilities in the wallets of this exchange.

The second stage is characterized by the use of advanced attack mechanisms and the work of specialized teams. Examples of successful attacks on crypto exchanges and the corresponding losses are shown in the following table.

Table 4. Examples of successful attacks on crypto exchanges in 2017-2018.

Date	**Project**	**Country**	**Group**	**Damage in crypto**	**Damage in billion $**
Feb. 2017	Bithumb	South Korea	-	-	7
Apr. 2017	YouBit	South Korea	-	-	5,6
Apr. 2017	Yapizon	South Korea	Lazarus	3,816 BTC	5,3
Apr. 2017	Ether Delta	-	Unknown	-	0,225
Aug. 2017	OKEx	Hong-Kong	Unknown	-	3
Sep. 2017	Coinis	South Korea	Lazarus	-	-
Dec. 2017	YouBit	South Korea	Lazarus	17% of assets	-
Jan. 2018	Bitstamp	Luxemburg	Unknown	18.000 BTC	5
Jan. 2018	Coincheck	Japan	Lazarus	532.000.000 NEM	534
Feb. 2018	Bitgrail	Italy	Unknown	17.000.000 NANO	170
June 2018	Bithumb	South Korea	Lazarus	-	32
June 2018	Coinrail	South Korea	Unknown	-	37
June 2018	Bancor	-	Unknown	-	23
Sep. 2018	Zaif	Japan	Unknown	-	60
				Total	882

Source: Report: Cryptocurrency Exchanges Lost $882 Million to Hackers.

The growing interest in cryptocurrencies has given rise to the development of massive attacks on these services. Thus, from 2016 to 2017, the number of compromised user accounts of cryptocurrency exchanges increased by 369%. In January 2018, the number of incidents increased by 689% compared to the 2017 monthly average. Group-IB experts analyzed the thefts of 720 user accounts of the 19 largest cryptocurrency exchanges and found that the USA, Russia and China became the leaders in terms of the number of victims of cyber-attacks (see Table 6).

Table 5. Distribution of victims of crypto-exchanges by country

№	Country	% of stolen assets
1	USA	34,3
2	Russia	10,5
3	China	5,0
4	Indonesia	4,5
5	Germany	3,6
6	Ukraine	2,8
7	Iran	2,8
8	Slovakia	2,6
9	Hong-Kong	2,6
10	Vietnam	2,4
11	Turkey	2,4
12	Other	11,1

Source: Number of hacked accounts on bitcoin exchanges in early 2018 increased by 689%.

It is impossible to ignore the functioning of specialized groups in this SDE segment.

Additional information on the activities of such groups can be obtained from the contents of the following table.

Table 6. Hacker group activities.

Country	Group	Codename	Activity
China (9 groups)	APT1	Unit 61398, Comment Crew	Information technology, aerospace industry, government, satellites and telecommunications, scientific research and consultations, energy, transport, construction and production, etc.
	APT3	UPS Team	Aerospace and defense industry, construction and engineering, high technology, telecommunications, transport.
	APT10	Menupass Team	Construction and engineering, aerospace and telecommunications companies, as well as the governments of the USA, Europe, and Japan.
	APT12	Calc Team	Journalists, government, defense industry base.

	APT15	Ke3chang, Mirage, Metushy, Vixen Panda	Government ministries throughout Europe.
	APT16		Japanese and Taiwanese organizations in the field of high technology, public services, media and financial services.
	APT17	Tailgator Team, Deputy Dog	US government, international law firms and IT companies.
	APT18	Wekby	Aerospace and defense industry, construction and engineering, education, healthcare and biotechnology, high technology, telecommunications, transport.
	APT30	-	Members of the Association of Southeast Asian Nations.
Russia (3 groups)	APT28	Fancy Bear, Sofacy, Pawn Storm, Tsar Team	The Caucasus, in particular Georgia, countries and military of Eastern Europe, NATO and other European security organizations and defense firms.
	APT29	Cozy Bear, the Dukes	Targeted invasions of the US National Democratic Committee, Governments of Western Europe, foreign policy groups and other similar organizations.
		Turla, Snake, Uroburos, Venomous Bear	A likely campaign against federal institutions in Germany, including the Foreign Ministry.
North Korea (3 groups)	APT37	Reaper, Group123, ScarCruft	First of all, South Korea, as well as Japan, Vietnam and the Middle East - in the chemical, electronic, industrial, aerospace, automotive and medical fields.
	-	Lazarus, BlueNoroff, Hidden Cobra	Suspected on hacking of Sony.
Iran (2 groups)	APT33		Several industries are headquartered in the United States, Saudi Arabia, and South Korea.

	APT34		A variety of industries, including financial, government, energy, chemical, and telecommunications in the Middle East.
	-	Charming Kitten, Flying Kitten	Persons of interest to Iran in the fields of research, human rights and the media.

Source: Pennino A, Bromiley M (2019) Threat Research. GAME OVER: Detecting and Stopping an APT41 Operation.

4. Technologies

One of the most popular schemes for stealing cryptocurrency assets is the following. First, a DDoS attack is organized and the site is blocked. This is followed by sending out phishing emails with fake addresses. Fake addresses are used to redirect to a phishing site, which is used to steal passwords and logins. Based on the stolen logins and passwords, electronic wallets are opened and the withdrawal and cashing of assets is performed.

In addition, with the help of hacker attacks, cryptocurrency exchange rates are changed to gigantic values. Therefore, in December 2020, hackers took control of the infrastructure of Livecoin and the Bitcoin exchange rate increased from $23,000 per unit to $450,000, Ethereum increased in price from $600 to $15,000 in the exchange, and the price of Ripple's XRP token increased from $0.27 up to more than $17.

The technologies used in this segment require in-depth research. The main reason for the lag is the use of elements of artificial intelligence and machine learning.

5. Conclusion

Over the past few years, cybercrime has stepped over many technical and software barriers and moved from a highly specialized niche into one of the most significant strategic risks facing the world today. The development of digital forms of fraud (cryptocurrencies and ICOs, ransomware infection, installation of an application on a smartphone, phishing, etc.) largely contributes to the development of technical progress.

According to the forecasts of the results of the study of global risks, cybersecurity and other factors related to IT will remain and will have a significant impact. Thus, short-term risks in the 0-2 year interval are assessed and are associated with failures in cyber security systems (39% of respondents noted) and digital inequality (38%). In turn, medium-term risks (3-5 years) are associated with a breach of the IT infrastructure (53.3%), failures in cybersecurity systems (49.0%), failures in technology management (48.1). Existential threats, taking into account long-term risks (5-10 years), are associated with unfavorable technical achievements (50.2% of respondents).

References

1. Ohrimenco S., Borta G. Chapter 8. Challenges for Digital Transformation in the Manufacturing Industry. Socio-Economic Development. Interdisciplinary Ecosystems Perspective. The Jubilee Book Dedicated to Professor Kazimierz Zielinski. Cracow University of Economics, 2020, Poland, Cracow. 330 p. ISBN 978-83-8175-233-6.
2. Ohrimenco S., Borta G. The challenges of shadow information economics. Proceedings of the Conference on Mathematical Foundations of Informatics.MFOI'2018, July 2-6, 2018, Chisinau, Republic of Moldova. pp.190-199.

3. Ohrimeenco S., Borta G. Rental Relations in SIE. 5th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE-2015). November 13 – 14th, 2015. University of National and World Economy Sofia, Bulgaria. P. 27-33. ISSN 2367-7635.
4. 2017 Data Breach Investigation Report. 10th Edition. https://vz.to/3qh4bIE
5. Levene B. Crimeware in the Modern Era: A Cost We Cannot Ignore. https://bit.ly/3jK9nCk
6. Kondratiuk A. The capitalization of bitcoin was 7% of the total market value of gold. https://bit.ly/3phrPn9
7. Krupenchenkova K., The capitalization of the cryptocurrency market has exceeded $ 400 billion, but this is still not enough. https://bit.ly/34IEw2I
8. cbt.center, Cryptocurrency capitalization: Features and how it affects trading. https://bit.ly/3rtjkaQ
9. artforlife.ru, The biggest hacker attacks on bitcoin, cryptocurrency and cryptocurrencies https://bit.ly/2OBrOOj
10. Report: Cryptocurrency Exchanges Lost $882 Million to Hackers. https://bit.ly/37QWoKV
11. Crypto Crime Report. Decoding increasingly sophisticated hacks, darknet markets, and scams. January 2019. https://bit.ly/34LqPQL
12. Pennino A, Bromiley M (2019) Threat Research. GAME OVER: Detecting and Stopping an APT41 Operation. https://bit.ly/2KZbTnG.
13. Global Risks Perception Survey 2020 Results. https://bit.ly/3rPQ8ua