CyberThreats_
Telefónica

Cyberextortion, a Growing Industry

22/02/2016

Telefónica

securely powered by
ElevenPaths

Major findings

There is an increasing tendency towards aggression in numerous cyber-attacks, notably those using some method of extortion in particular. In this sense, the conclusions on the methods carried out which are having the greatest impact are as follows:

- Extortion via **DDoS attacks** is being firmly established. The *modus operandi* of the DD4BC group could give rise to more attackers impersonating them without the need for a great infrastructure and extensive technical knowledge. On the other hand, possible money outflows with the aim of laundering returned to the source of the extortion are the online gaming and trading platforms.
- **Security breaches** are assuming a way of extortion based on the sensitivity of filtered information. Currently, two ways are being opted to monetise the attacks, either to sell the database or to extort it directly to users. The payment method required is usually Bitcoin.
- A growing trend is **sexual extortion**, also known as sextortion. The sharing of files using peer-to-peer networks remains the main platform for access to child abuse material and for its distribution in a non-commercial manner. In the same way, other anonymous networks and platforms such as Tor are considered as a threat in this area. However, what worries Security Authorities and Bodies the most is the live streaming of child abuse due to the difficulty to detect and investigate it since criminals tend not to store a copy of the material.
- Since 2015, the threat of **ransomware** has increased by 165%. The most reported infection vector is e-mail with malicious attachments. However, a growth is expected, driven by an increased use of the cloud, POS and the Internet of Things.

The use of the **cryptocurrencies**, as well as Tor and P2P networks are elements common to the different types of extortion and will continue to remain the main threats while there are no powerful enough solutions for their monitoring.

Table of contents

Introduction

Computer-related crime is becoming increasingly hostile. There is an increasing tendency towards aggression in many cyber-attacks, notably those using some sort of extortion method in particular. These attacks have some psychological impact with the aim of inducing fear and uncertainty in their victims. This aggressive environment is closer to organised crime than it is to a computer-related offence.

In this regard, Security Authorities and Bodies face certain challenges in the investigation stage when it comes to law enforcement. Many operations often end up thwarted because criminals resort to tools used for the anonymity and encryption of communications. The knowledge of security in operations is high and the easy access cyber-criminals have to products and services easily accessible online, both to anonymise their activity as well as their identity, tends to complicate forensic analyses.

In this sense, the report aims to identify the main techniques used with a greater impact in attacks from DDoS, theft of confidential information, sexual extortion and ransomware, in order to to inform about what technical limitations the investigator is confronted with before performing possible attribution exercises in the network.

Methods of extortion

Extortion can be defined as the act of obtaining property or money from another individual by threatening to use any kind of force. In addition, threats on the network that use the technique of extortion are as follows:

Distributed Denial-of-Service attacks. (DDoS)

Reports made by the security industry considered the DDoS attacks as threats with major implications. This threat is a type of attack on an equipment network causing a service or resource to be inaccessible to legitimate users. In 2015, even though several attacks exceeded 100 Gigabits per second, others of lesser magnitude also caused significant availability problems. In fact, three-quarters of attacks generally tend to last less than four hours, which suggests it is more than enough time for an attacker to achieve his goal (1).

Extortion through this vector of attack is being firmly established. One of the groups that have achieved greater repercussions has been DD4BC (DDoS for Bitcoin). Their first attacks were recorded in late 2014 and their ransoms ranged from 1 to 100 bitcoins depending on the perceived financial situation of the victim and their willingness to follow the instructions. In order to enhance the credibility of their threat, the group tends to launch a small attack on the victim's infrastructure and tries to communicate regularly with them demanding a higher ransom. Table I shows the most common procedures on how the group makes contact with their victims

DD4BC is primarily aimed at the online gaming industry but it has recently expanded its activity and it is now directing their attacks at financial companies as well (Annex A). On the other hand, it is not clear that all attacks can be attributed to a single criminal group or to what extent other criminals are trying to replicate their business model by using their name.

Table I. Location of DD4BC profiles.

Profile name	Platform	URL	Registration address
dd4bc	Klout	http://www.klout.com/dd4bc	
	Twitter	http://twitter.com/dd4bc	bo********@t*****.***
	Bitcointalk	https://bitcointalk.org/index.php?action=profile;user=dd4bc	
	Instagram	http://www.instagram.com/dd4bc	d****9@hotmail.com
	Disqus	https://disqus.com/dd4bc	
	Bitcointa	http://bitcointa.lk/members/?username=dd4bc	
	eBay	http://www.ebay.com/usr/dd4bc	
	Slideshare	http://www.slideshare.net/dd4bc	
	Fanbitcoin	http://fanbitcoin.com/index.php?action=profile;user=dd4bc	
dd4bcddos	Skype		
ddd4bc	Skype		dd4bc@outlook.com
dd4bc1	Skype		
	Bitmessage[1]	BM-NC1jRewNdHxX3jHrufjxDsRWXGdNisY5	

At the moment, it has not been possible to establish whether it is a single group or more that have been replicating their modus operandi. In any case, as the reputation of DD4BC and their different modus operandi becomes known, it could turn into a phenomenon in which attackers could impersonate this group without the need for a large infrastructure and extensive technical knowledge.

Key Threat: cryptocurrencies as a means of payment

Bitcoin is the cryptocurrency par excellence used by DD4BC to receive ransoms. While the logical use tends to be employing one Bitcoin address per ransom in order to hinder the monitoring of transactions, this group has a tendency for using the same addresses for different extortions. Addresses of alleged attackers were even shown to appear among the ones which should be addresses belonging to an alleged victim. In addition, the amounts received by the addresses registered as the attacking ones are too low. These signs introduce the possibility that fictional scenarios are being generated in order to make their victims believe payments into their addresses truly exist. If this hypothesis were correct, the attackers would simply be forced to launch

[1] Bitmessage is a P2P communications protocol used to send encrypted messages to another person or to many subscribers.

the attack while having available a series of emails or profiles open with the purpose of contacting the victim and having conducted a series of Bitcoin basic operations in order to create a credible scenario. Both actions involve a cost and require a minimum planning time.

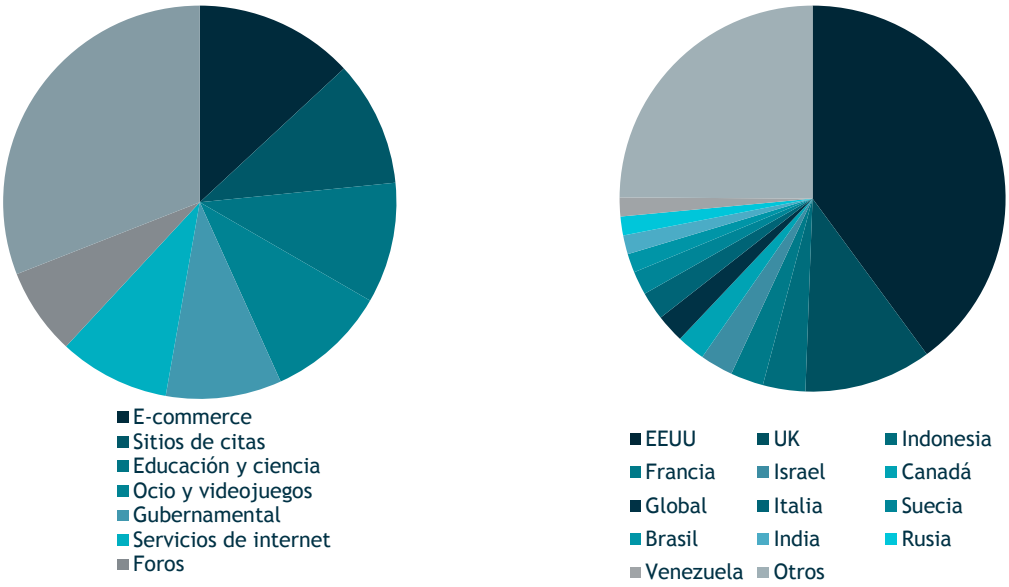
In the same way, the addresses associated with DD4BC have issued bitcoins towards two types of platforms: online gaming and trading. The first, in exchange for a reasonable cost to make the bet could multiply profits. On the other hand, trading platforms would be directed at making money deposits during a given time with overly high revenues. Besides allowing gains form extortion to duplicate, both methods would also enable to blur the trail, as only this type of online platforms would contain information on the addresses used by each user.

Theft of confidential information

December 2013 produced one of major security breaches with the leakage of personal information of more than 70 million customers of the American company Target (2). This incident prompted an immediate mobilization of resources in cyber-security which amounted to five million dollars (3). Despite de fact businesses are increasingly aware of the need to secure their technology assets, 2015 has been plagued by a large number of security breaches that resulted as a threat to both for users and companies, regardless of the country and the sector to which they belong (4).

Although the motivations underlying a filtration may have different objectives, the main one is to yield a profit on stolen information, largely by putting it for sale in the black market or through extortion campaigns directed at affected users. In May and July 2015, Adult Friend Finder and Ashley Madison saw the leakage of their personal and sensitive data of millions of their customers, exposing their users to possible extortion (5) given the nature of the leaked information.

Table II. Number of attacks by sector (left) and country (right).



Key Threat: nature of the leaked information

This type of information leaks are particularly relevant in the event one has clear access to passwords, in case the user used the same one or one deduced from it, there would be a risk of unauthorised access. Normally, this is not the case because the standard practice is to store a summary or a hash of it. However, if the password is weak, cracking techniques could be employed and the original password could be retrieved. Even in the most harmless scenario, the attacker would have a valid e-mail account that could be used to carry out spam or social engineering attacks, in addition to being aware of a user's consumption of a particular service.

Key Threat: anonymous networks and anonymous payment mechanisms

Once one has access to users' information, the attacker usually opts for two ways depending on the sensitivity of the information, either to sell the entire database using Tor forums as it was the case with Adult Friend Finder (6) or to extort users directly, as it happened with Ashley Madison (7). In both cases, the method of payment requested was Bitcoin.

Sexual extortion or *sextortion*

A growing trend happens to be **sexual extortion**, also known as *sextortion*. We perceive this kind of extortion as the situation occurring when a person is coerced with an image or video of him or herself naked or during sexual intercourse which has been shared previously.

The modus operandi normally starts with an initial contact through social platforms. Given the large number of minors who use this type of platforms, attackers are trying to find those most likely to respond in a favourable manner (8). On the other hand, other more sophisticated techniques have also been observed, where some victims were instigated to download Malicious software (9) to take pictures of those minors and subject them to continuous physical abuse taking place offline.

Many other cases of extortion are a consequence of sexting. Sexting is defined as the exchange of text messages and sexually explicit pictures, usually self-generated, sent via mobile phone or the Internet (10). Existing technology can facilitate unwanted diffusion of pictures to third parties, affecting the well-being of their author, and which can lead to harassment or intimidation, both online or offline, with dramatic consequences which have led to the suicide of those affected in some cases.

Key Threat: peer-to-peer platforms and anonymous networks

The sharing of files using peer-to-peer networks remains the main platform for access to child abuse material and for its distribution in non-commercial form. This technology is perceived by the attackers as easy to use given that content can be identified through search tools. already in 2015, Europol identified a transfer made by attackers from anonymous networks into peer-to-peer networks (11).

Despite this, platforms such as Tor and other anonymous networks are also considered as a threat in this field, as they are being used by attackers to facilitate the exchange of pictures or videos in a way which is difficult to trace. According to Europol, these networks would also be used to share guidelines on how to remove any traces that could identify the perpetrators or how to include details in the background of pictures to introduce noise for investigators (12). Similarly, recent developments in Tor include both the possibility of downloading mobile applications on Android devices as well as hardware intended to anonymise traffic, what could motivate an increase in its use.

There have also been exchanges of child abuse material in exchange for bitcoins through Tor Mail. Even though many of the attackers exchanged this type of content

with economic goals, Tor and Bitcoin create the ideal scenario to add an economic variable to traditional exchange.

In any case, there is an increased use not only of Tor, but also the use of encryption systems, such as TrueCrypt, or the use of VPN, disposable emails, proxies, or Internet connections through open WiFi networks.

Key Threat: live streaming

The popularisation of webcams and chat platforms enabling video transmission are giving rise to their exploitation by child molesters. In exchange for a fee, some of the applications would allow emissions protected by passwords, providing an extra layer of anonymity. Live broadcast of child abuse is likely to be increased due to the difficulties involved in the detection and subsequent investigation since criminals do not typically store a copy of the material.

Key Threat: commercial distribution

According to Security Bodies and Authorities there is a need to understand the current scope of the types of distribution of child abuse material through the network. In addition to the traditional distribution method in devoted websites, new methods such as "disguised websites", cyberlockers[2], live streaming-on-demand as well as commercial bodies across anonymous networks(13). In addition, it has been observed that traditional payment mechanisms have migrated into different ones offering a greater degree of anonymity as Bitcoin.

Ransomware

This method of extortion is a type of malware that prevents or limits users from accessing their information once it has been encrypted using techniques that do not allow the retrieval of the information unless the cybercriminal provides passwords to users so they can decrypt the files. In this way, he forces their victims to pay a ransom through certain online payment methods for the purpose of being able to recover their systems or data once again (14). In early 2015, companies like McAfee observed their detections to increase by 165% with regards to this threat (15). In addition, its characteristics have evolved in complexity. It is becoming increasingly frequent to come across more secure communications, concealed launch techniques and a greater awareness of sandbox environments (16).

[2] Cyberlockers are services specifically designed to host static content, mostly large files.

Key Threat: most frequent infection vectors

The most widely used infection practice by criminals is the distribution of malware via emails with malicious attachments. At the same time, the use of exploit kits hosted on websites that exploit vulnerabilities in Flash, Internet Explorer, Silverlight and Java is becoming increasingly common. Also, the methods used by attackers to lure victims are based on the results obtained through search engines from potentially illegal or embarrassing terms.

Key Threat: most used payment mechanisms

After initially asking for payoffs to be paid by means of a credit card, the fast payment system was adopted, although it varies according to the regional infection of the ransomware. This system was implemented until it was replaced by the use of the cryptocurrencies combined with the use of Tor for the total anonymisation of trace. This trend is mainly due to increased knowledge about the uses that can be granted to digital currencies.

Key Threat: new forms of ransomware

There are different types of ransomware that are being detected, and that can become a trend. Depending on the affected asset they can be classified as follows:

- *RansomWeb*

The first discovered cases of ransomware exploiting the vulnerabilities in web servers could be an indication of a future trend. The RansomWeb technique was unveiled in early 2015 when a financial services company carried out the ransom for 50 000 dollars of one of its databases, a figure which would rise by 10% with every week that passed (17). However, it has been proven that the most effective attacks are being carried out on SMEs with ransoms revolving around 1,000 dollars.

- *Ransomware-as-a-Service*

Even though the industrialisation of the Crimeware-as-a-Service is not new, the distribution of ransomware has revealed to be particularly innovative with its criminal business strategy. In May 2015, McAfee discovered a kit called 'Tox' available for free at Tor for the purpose of acquiring a stake of 30% of Bitcoins on ransoms carried out (18). The Tox base code lacked the complexity of the other crypto-ransomware variants. Nevertheless, this business model is likely to be developed by offering a more advanced malware to less tech-savvy criminals.

- *Mobile ransomware*

Ransomware attacks on mobile devices are becoming more frequent. In this regard, the Trojan-Ransom malware recorded the highest growth rate of all mobile threats. According to Kaspersky Lab, the number of new samples detected in the first quarter of 2015 amounted to 1,113, which translated into a 65% increase in the number of mobile ransomware samples (19).

- *Cloud, Point of Sale and Internet of Things*

Possibly the widespread use of smart devices and the growing use of cloud promote the use of simple methods for obtaining economic benefits through malware infections. Furthermore, the evolution in refinement of the methods of data exfiltration from credit cards from point of sale (POS) terminals is also possible, especially during periods in which there are sales peaks.

Common traits among different types of extortion

Due to the characteristics of virtual coins, these are becoming a payment mechanism commonly used among cybercriminals. In order to minimise this trend, cryptocurrencies are slowly gaining acceptance among European governments whether it means proposing a regulation to the European Union (20) or recognising them under the legislation of the Member States (21). The truth is that any regulation of cryptocurrencies as they are designed today, is probably only applicable to identifiable users who make use of exchange gateways, since these are the ones holding information about activities and accounts associated with each of its users. The inability to perform attribution exercises by investigators on transactions carried out makes it difficult to imagine how any regulation could be applied in practice to users who use this type of currency on a daily basis.

Communication options used by criminals differ considerably. Email, chat rooms or IRCs remain the most common communication methods, located both on the surface as well as in the deep web. For real-time communication, Jabber and ICQ are used fairly regularly.

Also, according to the Security Bodies and Authorities of the countries of the European Union claim that more than three quarters of investigations came across the use of some form of encryption to protect the information and/or to foil forensic analysis of seized media. In the same way, an increase in the use of encrypted email was also observed.

Lastly, any cybercriminal who intends to preserve a minimum of operational security has affordable anonymisation solutions within his grasp, such as the use of proxies and VPNs as well as the growth of the adoption of Tor and I2P as alternative solutions.

Recommendations

Given the threat of different kinds of extortion on the web, a series of recommendations are proposed for different security providers in order to reduce technical constraints in allocation exercises when confronted with extortion on the web:

- There is room for improvement in the creation of solutions for investigation and monitoring of cryptocurrency payments and finding users in anonymous networks. Currently, the solutions available are limited to attribution exercises.
- On many occasions, the solution for the detection of offences on the Internet involves the creation of human sources units motivated by technical constraints and the need to create certain links with the attacker in order to obtain additional information and reaching beyond automatic collection processes.
- With regards to cryptocurrencies, there is a need for common legislation allowing Security Bodies and Authorities to request the necessary information to the existing currency exchange platforms on the Internet in a swift manner.
- It is necessary to create in communities aimed at sharing existing knowledge in Big Data and in methods used for the efficient conducting of attribution exercises on the web, as well as its relation with other previous cases.

Annexes

List of identified DD4BC attacks

Date	Email	Victim	Bitcoin address	Price
23/09/2014		Nitrogen Sports	17WQov8BTXJAemWmqn5XJ8ibiq13SNoaqs	
oct-14		Cex.io		2 BTC
oct-14	dd4bc@outlook.com	Coinsweeper	16JEzTkXGeCFPrCoPo9hnSVZWLHMau31fg	2 BTC
23/10/2014	dd4bc@outlook.com	bitsquare.io		2 BTC
28/10/2014	dd4bc@outlook.com	Mmpool.org	17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp	
29/10/2014		SocialCex.com		
nov-14		blisterpool.com	17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp	2 BTC
02/11/2014	anonymousemail@anonymousemail.us	nicehash.com	16JEzTkXGeCFPrCoPo9hnSVZWLHMau31fg	1 BTC
03/11/2014	dd4bc@outlook.com	bitalo.com	17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp	1 BTC
07/11/2014	dd4bc@outlook.com	bitbillions.com	17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp	1 BTC
15/11/2014	dd4bc@outlook.com	mpex.co	132EdUarcghK2barhkxgaKQ2XqnchPbWSB	1 BTC
17/11/2014	dd4bc@unseen.is	ruggedinbox.com	1MRFFgSexGzyWgbLEhX1Bi3YXR6FaaebV8	1 BTC
ene-15		Betbtc.com		
22/01/2015		Hivewallet.com		
03/02/2015		Exco.in		
15/02/2015	dd4bc@safe-mail.net	Bitquick.com	1HpFnMfz6iDBbckWFMVvKR8mfTteXKHWZc	1.5 BTC
15/02/2015	dd4bc@Safe-mail.net	Holytransaction.com	1E8R3cgnr2UcusyZ9k5KUvkj3fXYd9oWW6	1.5 BTC
mar-15		Antpool		
mar-15		Bitmain		
mar-15		Bw.com		
mar-15		Ckpool		3 BTC
may-15		Ghash.io		
mar-15		HashNest		
01/04/2015		Neteller		
05/04/2015		betatcasino.com	1NbhLM43duL2J2tBX2qQWBojEm5fNSoMEp	10 BTC
05/04/2015		betatcasino.com		
05/04/2015		slottyvegas.com	1NbhLM43duL2J2tBX2qQWBojEm5fNSoMEp	10 BTC
05/04/2015		Slottyvegas.com		
09/04/2015		Redbet.com		
09/04/2015	dd4bct@gmail.com		18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z	20 BTC
10/04/2015		Pokerstars.com		
19/04/2015			15QMfpfymmkgj1AtEy9uvqvpgsTfDuGzJF	15 BTC
may-15		Expresscoin.com		
21/06/2015	dd4bcteam@keemail.me		1KU3TFMNxmE5UTMsjBmep34K6QJtJNJ6wD	25 BTC
		Nitrogen Sports	1H2bstU3yCpqJyrNzHSrnperZnTMSwLa5K	
			198QaeuJ6oMeuan2p5gyDx75odweMWzNXH	

Bibliography

1. **Securelist.** Kaspersky DDoS Intelligence Report Q2 2015. [Online] 4 agosto 2015. [Cited: 15 febrero 2016.] https://securelist.com/analysis/quarterly-malware-reports/71663/kaspersky-ddos-intelligence-report-q2-2015/.

2. **Target.** Target Provides Update on Data Breach and Financial Performance. [Online] 10 enero 2014. [Cited: 21 diciembre 2015.] https://corporate.target.com/press/releases/2014/01/target-provides-update-on-data-breach-and-financia.

3. —. Target Invests $5 Million in Cybersecurity Coalition. [Online] 18 febrero 2014. [Cited: 21 diciembre 2015.] https://corporate.target.com/article/2014/02/target-to-invest-5-million-in-cybersecurity-coalit.

4. **Telefónica.** *2015: The Year of Information Leaks.* 2015.

5. **SC Magazine UK.** Possible Ashley Madison extortion campaign identified. [Online] 23 octubre 2015. [Cited: 9 febrero 2016.] http://www.scmagazineuk.com/possible-ashley-madison-extortion-campaign-identified/article/448993/.

6. **The Hacker News.** Hackers Selling Database of 4 Million Adult Friend Finder Users at $16,800. [Online] 25 mayo 2015. [Cited: 9 febrero 2016.] http://thehackernews.com/2015/05/AdultFriendFinder-database.html.

7. **ZDNet.** In Ashley Madison's wake, here's one man's story of sex, sorrow and extortion. [Online] 24 septiembre 2015. [Cited: 9 febrero 2016.] http://www.zdnet.com/article/in-ashley-madisons-wake-heres-one-mans-story-of-sex-sorrow-and-extortion/.

8. *Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children.* **Oficina de las Naciones Unidas contra la Droga y el Delito.**

9. **FBI.** Cyber Alerts for Parents & Kids. [Online] https://www.fbi.gov/news/stories/2012/february/sextortion_021012.

10. *A qualitative study of children, young people and sexting.* **Science, The London School of Economics and Political.**

11. *The Internet Organised Crime Threat Assessment (IOCTA).* **Europol.** 2015.

12. *The Internet Organised Crime Threat Assessment (iOCTA).* **Europol.** 2014.

13. *Internet Watch Fundation Annual and Charity Report 2013.* **IWF.** 2013.

14. **Trend Micro USA.** Ransomware. [Online] [Cited: 9 febrero 2016.] http://www.trendmicro.com/vinfo/us/security/definition/Ransomware.

15. *Threats Report May 2015.* **McAfee.** 2015.

16. **Telefónica.** Ransomware. [Online] 6 julio 2015. [Cited: 9 febrero 2016.]

17. **Forbes.** RansomWeb: Crooks Start Encrypting Websites And Demanding Thousands Of Dollars From Businesses. [Online] 28 enero 2015. [Cited: 11 febrero 2016.] http://www.forbes.com/sites/thomasbrewster/2015/01/28/ransomweb-50000-dollar-extortion/#3f1541bd7d47.

18. **Security Affairs.** Tox, how to create your ransomware in 3 steps. [Online] 26 mayo 2015. [Cited: 12 febrero 2016.] http://securityaffairs.co/wordpress/37180/cyber-crime/tox-ransomware-builder.html.

19. **Securelist.** IT threat evolution in Q1 2015. [Online] 6 mayo 2015. [Cited: 12 febrero 2016.] https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/.

20. **hipertextual.com.** Europa quiere terminar con el anonimato del Bitcoin. [Online] 3 febrero 2016. [Cited: 15 febrero 2016.] http://hipertextual.com/2016/02/anonimato-del-bitcoin.

21. **RT News.** Germany recognizes Bitcoin as 'private money'. [Online] 18 agosto 2013. [Cited: 15 febrero 2016.] https://www.rt.com/news/bitcoin-germany-recognize-currency-641/.