0-Day Vulnerabilities and Cybercrime

Paolo Foti, Jart Armin
CyberDefcon
Brighton, United Kingdom
paolo@hack-no-crack.it, jart@cyberdefcon.com

Marco Cremonini
DI - University of Milan
Crema, Italy
marco.cremonini@unimi.it

***Abstract*—This study analyzes 0-day vulnerabilities in the broader context of cybercrime and economic markets. The work is based on the interviews of several leading experts and on a field research of the authors. In particular, cybercrime is considered when involving traditional criminal activities or when military operations are involved. A description of different 0-day vulnerability markets - White, Black and Government markets - is provided, as well as the characteristics of malware factories and their major customers are discussed.**

***Keywords*-0-days vulnerability; cybercrime; security;**

I. Introduction

The aim of this paper is to study how 0-day vulnerabilities relates to the context of cybercrime and of the markets where they are traded. 0-day vulnerability are a sensitive and often murky topic, whose context continuously evolves, available documentation is scarce, and people involved in trading or development are reluctant to openly talk about the issue. Lacking a comprehensive overview of the phenomenon, it was decided that the best course of action to obtain up-to-date and relevant information was to interview some selected security experts with different backgrounds and from their different viewpoints try to produce a coherent description[1]. The selected experts are authoritative in their respective field of competence and are employed on a daily basis, albeit for different reasons, in the cybercrime area at national and international level. In addition to the interviews, several years of research have made it possible to analyse most of the documents available online about 0-day vulnerabilites and to discuss the issue with leading figures in the various disciplines of computer security and daily committed to contrast cybercrime.

This analysis serves as a basis for exploring the dynamics of 0-day vulnerability trading on the White, Black and Government Markets. A section is dedicated to an investigation about RBN (Russian Business Network) often considered as an example of an activity completely devoid of professional ethics and in particular, to its operating methods and services in recent years. Beside criminal networks like RBN, an essential role in the development of 0-day vulnerabilities and cyber weapons is played by Malware Factories.

[1]We have referenced with *[Int-n]* the quotes from the interviews given by security experts according with Table I.

Table I: Experts interviewed

#Int	Name	Description
Int-1	anonymous	Independent 0-day developer
Int-2	Cesar Cerrudo	CTO, IOActive Labs - Argentina
Int-3	Antonio Forzieri	Cyber Security Prac. Lead EMEA, Symantec - Italy
Int-4	Feliciano Intini	Technology Strategist, Microsoft - Italy
Int-5	Ioan Landry	Security Practitioner, S.B. - Canada
Int-6	Stefano Mele	Privacy, Intelligence & Security Legal expert - Italy
Int-7	Alessio Pennasilico	Security Evangelist, AlbaST - Italy
Int-8	anonymous	Postal and Communications Police - Italy
Int-9	Steve Santorelli	Director of Intel. and Outreach, Team Cymru - UK
Int-10	Boris Sharov	CEO, Doctor Web - Russia

II. What is cybercrime?

A. Cybercrime

Cybercrime is a form of crime that includes crimes committed through the use of the Internet or other computer networks. A computer (or another hardware device) or a computer network can perform two different roles: the instrument of a crime (if exploited to commit it) or the victim of a crime (if it is the target). Judge Fabio Licata[2] provided a comprehensive outline of cybercrime [1]. In his view, the unlawful actions carried out on the Internet and through the Internet can be classified into the following categories:

- Offences against the confidentiality, integrity and availability of computer data and systems (i.e., *CIA* offences). These offences include all illegal access to computer systems through hacking, unlawful interceptions, various forms of deception to the detriment of users (e.g., phishing), system spying (through spyware or Trojan horses), up to sabotage designed to compromise the system availability (for example through viruses, denial of service attacks, spamming or mail bombing);
- Traditional computer crimes, such as the classic frauds achieved by cloning credit cards, cashpoint cards or other means of payment, online business scams, various types of counterfeiting carried out through the computer etc.;
- Offences connected to the content of information or data transmitted over the Internet. Think of child pornography, racism and xenophobia or the incitement, instigation or transmission of instructions for

[2]Fabio Licata is judge of the first criminal chamber of the Court of Palermo, with jurisdiction also for the application of prevention measures.

978-1-4673-6590-1/15 $31.00 © 2015 IEEE
DOI 10.1109/ARES.2015.55

CPS Conference Publishing Services

the accomplishment of the most varied traditional crimes (e.g., terrorist propaganda). This category may also include various types of computer harassment (so-called cyberstalking and cyberbullying) and even fraudulent online gambling;
- The infringement of copyright and related property, such as the unlawful reproduction of computer programmes or all types of intellectual work on digital media (books, music, movies);
- The violation of privacy such as the unlawful access to personal data repositories or the unlawful collection and circulation of any such data.

According to Judge Licata, computer security performs an essential role "*to increase confidence in cyberspace as an element of economic, civil and cultural development.*" Judge Licata continues: "*In recent years, the awareness of this has led to a proliferation of documents and treaties by all the main supranational organizations: the United Nations and its collateral organizations, G8, the Commonwealth, the Organization of American States, the European Union, Asian Pacific Economic Cooperation (APEC), Organization for Cooperation and Economic Development (OCSE) and the Council of Europe.*"

In Italy, Law no. 48/2008, which ratifies the Budapest Convention of the Council of Europe (2001) on cybercrime [2], has been in effect since 2008. The Budapest Convention was the first international agreement on crimes committed through the use of the Internet or other computer networks, even if the proof of the crime is in electronic form; the Convention provides for extensive, coordinated collaboration between the signatory States.

While cybercrime increasingly scares citizens and small offices fearing to incur in economic losses or in damages to their data [3], the companies and business transactions are the main target of the cybercrime, as several recent studies have confirmed [4].

In Italy the authority responsible for investigating and prosecuting cybercrimes is the Postal and Communications Police, whose investigative activities conducted in 2013 on child pornography led to 55 arrests in respect of 344 charges. In an interview that took place in November, 2014 [Int-8], some officers of the Postal and Communications Police stated that the increase in the spread of computer crimes is due to a very high ROI (Return On Investment) deriving from this type of criminal activity.

Other experts interviewed [Int-6, Int-7, Int-10] claim that the increase in the spread of cybercrime is not only due to the ease of immediate income, but also for the international economic crisis and unemployment of recent years, which has pushed skilled professionals in the hands of criminals. By contrast our opinion is different: it is not the economic recession that triggered the increase in the sale of vulnerabilities on the black market, rather vulnerability sales have increased mostly due to a wider market created by core vulnerability developers and governmental cyberwar/cyber arms race perceptions.

The recruitment of cybercriminals is also often eased by the incorrect perception of the implications and consequences of cybercrime. People involved in cybercrimes often fail to fully understand the meaning and the consequences of illegal actions performed with the aid of IT equipment or on the Internet when, unlike traditional criminals, they feel they are in a safe environment with loose rules.

Personal and corporate information represents great value to criminals and fuels a highly prosperous market, but it is not easy to estimate the extent of the turnover from cybercrime.

As Alessio Pennasilico states [Int-7]: "*[] Russian Business Network, in 2009, had a turnover higher than Microsoft I don't know the turnover of other markets, but that of malware and cybercrime is generally high and rapidly increasing [].*"

According to Boris Sharov [Int-10], the cybercrime market is mostly invisible, underground and silent: "*[] While it is more or less known in the drugs field, it remains unexplored in the cyber field. I strongly doubt that it has exceeded the traditional major criminal industries [].*"

Stefano Mele, a lawyer working on technology, privacy, information security and intelligence issues, explains why it is particularly difficult to estimate the turnover from cybercrime [Int-6]: "*[] There is no public data in which we can find this information for various reasons, including reputation damage, market loss and the loss of trust. As there is no obligation to publish incident reports when there have been victims of computer attacks, leaving aside telecommunications companies, the companies attacked do not make any public announcements. The code of silence is not only a problem in Italy, in any case we cannot know if cybercrime has exceeded the more traditional markets in terms of turnover. It can be certainly be said though that it is a highly prosperous market in which the ROI is very high indeed, with little investment; if the right attack, the right phishing or the right ransomware comes along the earnings can be very high, hundreds of thousands of euros.*"

The Italian Postal and Communications Police shares the same view of Stefano Mele, but specifies that the difficulty in calculating the turnover does not only depend on the fact that it is produced in an underground market [Int-8]: "*[] it is very difficult to establish due to the variety of the crimes perpetrated via the Internet: from ransomware to phishing, spam, identity theft, and so on. All these crimes contribute to increase the turnover from cybercrime.*"

Steve Santorelli, underlines two significant aspects concerning the debate about the extent of the turnover of cybercrime [Int-9]: "*Theres massive debate on this number every year and its getting more complex as the traditional crimes are now employing cyber aspects all the time. You cant put a reliable number on it but I know that every organized criminal syndicate in the world is gravitating towards cybercrime as the risks are virtually zero and the rewards are at least as high as with their traditional work.*"

B. Military Cybercrime

Cybercrime in a military scenario (also called Cyberwar) should be considered differently: Investments are higher, attacks more targeted and focused on strategic objectives and their success is less certain, and consequently the ROI is considerably lower. Estimating the turnover of cybercrime in the military field is even more complicated, in this case geopolitical factors come into play that make pure gain a non-essential element. The aim of Stuxnet, a malware discovered in 2010 that infested various nuclear plants, for example, was not so much the earnings derived from an act of cybercrime as much as to slow Iran's nuclear development.

Stefano Mele affirms that [Int-6]: "*[. . .] Governments invest huge sums in the military cybercrime field, particularly in the cyber espionage sector. Although espionage is an illegal practice there are no laws that explicitly condemn it. It is not only China or the US that illegally monitor other countries, but also European countries like France and the UK are involved in the same activity [. . .].*"

III. The ambiguous nature of vulnerabilities

A. 0-day vulnerabilities

The concept of *system violation* dates back to the '80s, the period in which the first 0-day vulnerabilities most likely occurred. In the '80s computer security was mainly studied and debated at academic level and there was no perception of the fundamental role that it would play in the immediate future.

Today the situation is radically different: systems are protected with increasingly state-of-the-art software and hardware. To attack a system it is essential to study it, understand its structure, identify the type of protection installed and the operating system in use and, lastly, identify its vulnerabilities. The purpose of violations is to plunder information that can provide a substantial gain or exploit IT assets.

As specified by Common Vulnerabilities and Exposures (CVE): "*An information security vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network. CVE considers a mistake a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system.*" For CVE, a vulnerability is a state in a computing system (or set of systems) that either allows an attacker to:

- Execute commands as another user;
- Access data that is contrary to the specified access restrictions for that data;
- Pose as another entity;
- Conduct a denial of service.

Examples of vulnerabilities include:

- *phf* (remote command execution as user nobody);
- *rpc.ttdbserver* (remote command execution as root);
- world-writeable password file (modification of system-critical data);
- default password (remote command execution or other access);
- denial of service problems that allow an attacker to cause a Blue Screen of Death;
- *smurf* (denial of service by flooding a network).

It should also be pointed out that vulnerabilities may result from the incorrect configuration of increasingly complex computer systems, or from the carelessness of system users, for example the use of weak passwords or the sharing of passwords with colleagues and friends.

To define the concept of 0-day vulnerabilities it is essential to clarify the role of the term *zero*. When does the zero actually start? From the time the vulnerability is discovered and made known, or the time it is used for the first time without anyone noticing? And how many times can a 0-day attack be used before it is no longer considered as such? Most of the people interviewed agreed with the following definition [5]: "*the term 0-day exploit describes an exploit that is not publicly known. It describes tools by elite hackers who have discovered a new bug and shared it only with close friends. It also describes some new exploit for compromising popular services (the usual suspects: BIND, FTP services, Linux distros, Microsoft IIS, etc.).*"

Many 0-day exploits are discovered by the victims when hackers use them, or by honeypots. The term 0-day describes the fact that the value of exploits quickly goes down as soon as they are announced. Broadly speaking, the next day a 0-day vulnerability has been publicly announced, its economic value halves. The 2nd day it is a quarter as valuable. Ten days later the value could be 1/1000 than on day 0. This is because script kiddies quickly use the exploit on computers throughout the Internet, compromising systems before anybody else can get to them. So a 0-day exploit is a computer security vulnerability that is being actively practiced before knowledge of the exploit becomes public information.

0-day vulnerabilities are increasingly a topic of discussion in the IT security community, and since 2000 the term has become a regular part of the scientific community's vocabulary. 0-day vulnerabilities, which today gain considerable interest among researchers and companies, also certainly existed before 2000, but they were not considered as distinct from common computer attacks so they did not have a specific name; they were simply known as 'attacks'.

The qualification of 0-day is used both when referring to a vulnerability (from the victim's point of view) and when referring to an attack (from the attacker's point of view).

In an interview, Cesar Cerrudo [Int-2], stated: "*0-day vulnerabilities have existed for a long time and they have been actively being used, you can see it in the latest Stuxnet incidents [6]. I guess in the future we will continue seeing more targeted attacks that use 0-day exploits.*"

As Cesar Cerrudo explains, attacks and 0-day vulnerabilities have always existed: it is likely, as already mentioned, that before 1986 they were not exploited for profit but rather to violate the intellectual property of software.

The definitions given above provide an understanding of how interesting and strategic 0-day vulnerabilities can be

for criminals, governments and the scientific community alike.

B. Threats Vs. Vulnerabilities

The difference between threat and vulnerability, often overlooked by many that refer to THEM as synonyms, is instead essential to identify the possible protection measures against 0-day vulnerabilities. As an example consider *Zeus* and *Heartbleed*, two of the best known attacks of recent years.

Zeus is a malware family especially created to exploit the vulnerabilities of Windows systems in order to steal bank credentials. It works as a man-in-the-browser keystroke logging and form grabbing. It is also capable of encrypting the information from infected systems to allow its users to demand a ransom. It has many aliases, including *PRG*, *Zbot* and *Infostealer*. In the US alone it has affected over 3.6 million personal computers. The malware has spread globally, infiltrating over 74,000 bank accounts and affecting companies such as Amazon, Oracle, Bank of America and NASA. Variations capable of infecting Blackberry and Android systems have also been discovered [7].

Heartbleed, on the other hand, exploits a security bug of the open-source cryptographic library OpenSSL, widely used to implement the TLS (Transport Layer Security) protocol [8]. The vulnerability was caused by a missed bounds check in managing the Heartbeat extension of the TLS protocol. It is estimated that around 17%, that is half a million of the secure web servers, certified by trusted authorities, were vulnerable to the attack. The Heartbleed exploit allowed the theft of server private keys as well as user passwords and cookies [9].

Both Zeus and Heartbleed exploit vulnerabilities, but while Zeus is comprised of a series of ad hoc programmes developed to take advantage of flaws in Windows systems, Heartbleed is a list of instructions written in command line that exploits a programming error in an essential library of a widely used service, without the help of software. It can therefore be concluded that Zeus is a *threat* while Heartbleed is an *exploit* that takes advantage of a *vulnerability*.

Threats and vulnerabilities share the characteristic of making a computer system open to attacks, but there may be fewer vulnerabilities if software development and maintenance were carried out with particular attention to security. If the software analysis of the Heartbeat libraries were carried out with greater care, the software error that caused the Heartbleed bug would most likely have been corrected before the software release.

A good practice for those who produce software could be to subject the modules developed to a new static analysis of the code at regular intervals in an attempt to minimize the number of bugs.

0-day vulnerabilities are able to expose computer systems to planned ad hoc attacks capable of causing damages with consequences that are difficult to predict: for this reason they are of great interest to those aiming to develop cyber weapons targeting among the others government organizations and critical infrastructures.

C. Malware Factories

Malware Factories are companies that create malwares on demand in exchange for a fee. In these companies, as in any software house, specific development groups are set up whose work could be defined as malware as a service. As it is essential for a malware to be made available in the shortest timeframe, to increase the effectiveness of its use, it is plausible to assume that work shifts are organized to allow development 24 hours a day. It is difficult to establish with certainty how many Malware Factories exist and where they are located.

Alessio Pennasilico states that "*this information is not known*" [Int-7], while Boris Sharov [Int-9] states: "*We have never tried to evaluate the number of such factories. From our point of view it is not that important - we have our statistics of incoming suspicious files (over 200,000 daily) and the number of new malware which we either add to our signature bases or treat them in different ways.*"

Steve Santorelli explains why it is not simple to obtain precise information on Malware Factories [Int-9]: "*[. . .] these people dont want to be found: they already have their network of contacts, nothing good would come to them by advertising in anything approaching a public forum. Whilst what they might be doing might not be technically illegal, they dont need the attention of governments, intelligence agencies, police and other researchers and media types [. . .].*"

In our opinion, and in particular according to coauthor Armin, in Russia and China there are two main Malware Factories, which are companies to all effects and purposes with a precise location and head quarter. It is a mistake however to think of Malware Factories as traditional white collar organizations set up with cubicles and fixed work hours. The country a Malware Factory belongs to depends on the location of the community that offers support and that can be considered origin of the malware. The most in-demand and developed malware in recent years mainly concern espionage software, Advanced Persistent Threat (APT), intrusion malware and cyber weapons. For these reasons, there are Malware Factories in the United States, Russia, China, United Kingdom, France, Turkey, Pakistan and India; these organizations must be contacted through intermediaries as they usually cannot be reached directly.

Equation Group should certainly be counted as one of the Malware Factories; the characteristics of this group were first discussed by Kaspersky Lab in a document published on 16 February 2015 [10] and so named with reference to the cryptography used in the development of malware. The malware developed by Equation Group are highly sophisticated and capable of infecting the firmware of hard disks produced by specific companies. It is important to point out that they can remain active even after the operating system has been reinstalled.

IV. 0-DAY VULNERABILITY MARKETS

A. White Market

Whoever discovers a 0-day vulnerability has various possibilities for the following course of action. First, the researcher can decide to publicly disclose the vulnerability only after the vendor has released a patch (*coordinated disclosure*). For instance, as described by Feliciano Intini [Int-4]. he/she could present the discovery at a security conference or the same vendor could give credits to the researcher when announces the software update. Otherwise, for whatever reason, the vulnerability discoverer can share it without the vendor being informed and then able to release a patch, or, eventually, he/she may want to monetize his/her work by deciding to sell the vulnerability on the market. This case is increasingly frequent, as well as the number of people that make a living out of researching for vulnerabilities. Furthermore, the market could be the *White Market*, the *Black Market* or the *Government Market*.

White Market is a legal market that is not hidden, in which information technology companies offer a payment to researchers willing to sell a 0-day vulnerability they have discovered. Whatever option the researcher chooses, he/she is well aware that the value (i.e. for technical recognition or the market price) of a 0-day vulnerability can rapidly drop from very high to almost zero.

The value is strictly linked to the vulnerabilitys notoriety: if it were disclosed and traded also by others or if a patch were to be suddenly released, the value of the vulnerability would drop until it was worth nothing and the researcher would risk suffering a significant financial loss because his/her work becomes worthless. For some critical vulnerabilities, the figures can reach hundreds of thousands of dollars and more, a potential gain that could disappear just by wasting a day too long arguing over the selling price. Time is a variable that makes it difficult even to find a trusted buyer [11].

Buyers, on their part, wish to protect their investment with respect to two aspects, at least: the vulnerability must be technically *effective*, meaning that it has to actually permit what it is supposed to permit, and the purchase must be *exclusive*, that is the vulnerability must not be resold in the future or being already sold to others. If a researcher were to resell a vulnerability to more than a single buyer, this would be perceived as a scam and would cause financial damage to the buyers. For this reason it is customary that vulnerability buyers perform due diligence on the seller and the agreement include the purchase of the intellectual property of the 0-day vulnerability and all the connected rights [12]. As easily foreseeable, the 0-day vulnerability market is largely based on reputations as the means to manage its intrinsic untrustworthiness.

The effect of the buyer actions is twofold: on the one hand they ensure the vulnerability researcher higher earnings by improving his/her reputation and on the other hand, they regulate the vulnerability market by reducing the number of scams.

As easily foreseeable, the 0-day vulnerability market is largely based on reputations as the means to manage its intrinsic untrustworthiness.

There are companies that buy 0-day vulnerabilities in order to then take responsibility for informing the vendor of a new bug and in the meantime shelter their customers by developing a temporary patch pending the definitive one. This is the case of the Zero Day Initiative (ZDI) laughed by Tipping Point, which started buying vulnerabilities using this method in 2003 [13]. ZDI is not the only programme that acquires 0-day vulnerabilities to make its customers secure: iDefense and Securiteam, for example, also offer payment to researchers who, in exchange, are willing to assign all the rights on the vulnerability.

Many large companies have officially launched Bounty Programs to recompense researchers who find vulnerabilities in their products. Facebook, for example, has introduced a dedicated page to its website where it explains how to buy the vulnerabilities and which vulnerabilities it considers suitable to report [14]. The minimum payment promised by the social network is $500 per vulnerability. In 2010 also Google launched a Bounty Program for the purchase of vulnerabilities of its products [15].

In general, the information given so far show that there is not a uniform tariff rate for 0-day vulnerabilities shared in the market. At various conferences dedicated to cybercrime it was possible to obtain some useful information on this particular feature. For the sake of simplicity, a short questionnaire is set out below which may serve as a guide in determining the value of the vulnerability:

- How widespread is the use of the application that is vulnerable?
- Does the application come by default with the operating system?
- Is the application turned on by default?
- Is authentication required to exploit the application?
- How well do typical firewall configurations block access to the application?
- What versions of operating systems/application are vulnerable?
- Is the vulnerability in a server or client application?
- Is user interaction required to exploit the vulnerability?
- How difficult it is to find the vulnerability (which is a proxy measurement of how long it will be before it is discovered by someone else)?
- How many people know about the vulnerability?
- How reliable is the exploit?
- Does a single exploit work against many versions?

Cesar Cerrudo [Int-2] affirms: "*0-days value depends on what product is affected and how many people and/or servers run that product. 0-days for widely used software will be the most valuable.The highest value depending on the most valuable 0-days are those that will let you to remotely compromise servers without authentication and also vulnerabilities in client side software such as Internet Explorer, Adobe Reader, Microsoft Office, etc.*"

In conclusion, a researcher who has identified a vulnera-

bility and decides to sell it cannot know for sure how much he/she will earn from the discovery as, in the absence of a specific tariff, each case is assessed individually and independently by each potential purchaser; on the basis of an order of magnitude of which both parties are aware, a traditional commercial negotiation is established, the objective of which is mutual satisfaction.

B. Black Market

0-day vulnerabilities are also traded on the Black Market, a market of illegal goods and services where trading operations occur in two main ways: virtually, carried out through contacts and online sales, and physically, which takes place through personal meetings between the criminals that buy and/or sell digital vulnerabilities.

The Black Market therefore has different facets: there is a less hidden Black Market where most transactions involve the sale of illegal goods and services like stolen credit card numbers, fake documents, but not 0-day vulnerabilities. Within the Black Market there is an even more hidden market, where instead 0-day vulnerabilities are sold.

The sale of 0-day vulnerabilities in this more secluded underground market occurs in ways that are not clearly documented and also the opinions of the interviewed experts are mixed. Boris Sharov believes that in order to conduct transactions you first need to be introduced in specific darknet forums [Int-10].

According to our experience, to access the Black Market of 0-day vulnerabilities it is necessary to go through specific intermediary companies, therefore using the same method of approach described for Malware Factories.

One element that makes the Black Market particularly attracting for those wishing to sell a 0-day vulnerability is the profit that can be obtained. Pedram Amini, a security researcher, for instance, affirms that on the Black Market the prices for individual vulnerabilities range from 20,000 to 100,000 dollars, with an average price being around 50,000 dollars [16].

Intriguingly, there is also the possibility of the same 0-day vulnerability being sold on both the White Market and the Black Market by the same researcher. An interviewee who prefers to remain anonymous [Int-1] affirms that those who work in the sector can guess which researchers are involved in this kind of con game, both through personal acquaintances developed in such a tight-knit world and the standard of living that some researchers display. The anonymous interviewee continues, claiming to be directly acquainted with at least one researcher who sells 0-day vulnerabilities first to his/her government, which uses them to complete targeted attacks, then, once some time has passed, to the Black Market.

Ioan Landry [Int-5] does not rule out the existence of people who sell their vulnerabilities to more markets: Landry, however, warns these individuals of the dire consequences they may incur. If the double sales scheme were to become known the sellers would risk their reputation and could be expelled from the highly select circle of trusted researchers, as well as suffering criminal consequences.

A documented example of lack of attention is that involving Jeremy Jethro, an IT professional who sold an exploit for 60,000 dollars to the Gonzalez gang of Chicago which allowed unauthorized access to IT networks. The Gonzalez gang stole over 90 million credit and debit card numbers. Jeremy Jethro was sentenced to three years probation and a fine of 10,000 dollars. Jethro is not the only IT expert who has collaborated with the Gonzalez gang: Stephen Watt, former programmer at Morgan Stanley, provided a sniffer which enabled the Gonzalez gang to steal corporate data from the company TJX . Watt was sentenced to two years in prison and the payment of 171.5 million dollars as compensation for the damages suffered by the American company. Finally, Humza Zaman, former head of network security at Barclays Bank, was sentenced to 46 months in prison and a fine of 75 thousand dollars for having laundered between 600,000 and 800,000 dollars for the Gonzalez gang [17].

A striking example of Black Market is represented by RBN (Russian Business Network), a provider of illegal Internet services based in St. Petersburg. It is a completely anonymous provider, with no legal identity, in which the leading roles are held by anonymous people. The registered websites offer an anonymous contact email address and the services offered are not advertised, including the sale of computer attacks, services aimed at the theft of personal data and services connected to child pornography. Finally, payments can be made without leaving a trace. RBN has expanded its activity also through agreements between criminals outside the Russian borders, becoming the largest provider of illegal Internet services in the world. According to a Verisign estimate, the turnover of RBN derived from scams alone perpetrated through phishing amounts to 150 million dollars per year [18].

Jart Armin, one of this paper coauthors, in a still unpublished independent research shows that the turnover of RBN is around 200 million pounds per year. He also specified that most of the scams were perpetrated online and that a gambling website was especially created in order to launder the money stolen illegally. Behind RBN there are criminals and former KGB agents, where the founder 's identity is unknown. He is only known by his pseudonym *Flyman*. During their investigations, Armin and some of his collaborators had the opportunity to inspect some RBN servers, where they identified 200 to 300 folders containing identities, bank accounts and credentials for compromised computers, for an estimated value of 5 million pounds per folder. Before Armin's work, the only known investigation on RBN was up to 2007, when RBN apparently dismantled its operations [19]. Now, thanks to the new investigation, it is possible to reconstruct the history of this criminal gang tracing its activity from its foundation, in 2000, up to March 2015:

(a) *Origins (2000-2003) and Structure*: Russian Business Network (RBN) was originally a cellular structured cybercrime operation. It was established as a collabo-

rative activity based in St. Petersburg and financed and sheltered by the organized crime enterprise the Tambov Gang. The initial operations centred around Too-Coin Software and the earlier ValueDot/SBT Telecom Network.

(b) *Main Open Operational Activities (2003-2007)*: RBN was best described during this period as a bulletproof host. The server was owned/controlled and operated by RBN: It served phishing, malicious code/tools, botnet command-and-control (C&C), and distributed denial of service (DDoS) attacks and child pornography. It was so significant that the ISP seemingly hosted virtually every major Trojan horse that targeted banking information at some point. RBN was not a stand-alone entity, and its illegal activities did not end within its IP range. Instead, RBN was at the centre of a network of St. Petersburg-based organizations engaged in activities that could be classified as RBNs. The criminal organization was not only located in Russia, but it also had branches in Panama, the Seychelles, Hong Kong and Turkey.

(c) *Cloaked and Related Spin-off Operations (2008-2015)*: It was seen at the time (November 2007) the RBN went offline. However, RBN may even now be breaking up into smaller pieces farmed out to multiple countries' Internet infrastructures. Although little information has been publicly disclosed, one of the key areas of RBN distributed activities was child pornography. As later discovered in 2010, this activity, although it created increased and negative public awareness of RBN in 2007, was an important and ongoing action. It was primarily for the purposes of extortion and protection from law enforcement & investigation, as a database of 18,000 users is now known of, with key members of the Russian Duma, government officials, legal officers, and people from 25 other countries named in the DB.

C. Government Market

Besides White and Black markets, there is a market that can be defined as Government Market or Grey Market.

A confidential interviewee affirms that the American government buys 0-day vulnerabilities not to protect itself, but rather to attack [Int-1].

The emails stolen by Anonymous from the private company HBGary, a company specialized in IT security, seem to witness such government activities. The emails contain communications between members of the computer security company and members of US government. Among the contents of the emails it is worth mentioning a plan to discredit WikiLeaks by introducing fake documents into its website, the supposed identification of some members of Anonymous, but above all some 0-day vulnerabilities and their operation; in this last case some emails have attachments containing the actual vulnerabilities discussed in the emails. Some emails even give the impression that a private company such as HBGary has conducted cyberwar operations in place of the regular army. It seems that the emails were stolen due to an email server configuration error which was hacked through an SQL injection operation *greenberg2011*. The stolen emails are unencrypted and written in plain language, and in fact they are very clear and explicit. The recipients range from known private companies to public institutions and the emails were sent to people who perform key roles within the organization. Some contain attachments that may be private documents and examples of fake documents, or even viruses, sent as compressed files without passwords, and are therefore easy to unzip and analyse.

The governments of some countries are organized to implement technical training programmes for future hackers, the best of which will have the opportunity to work in intelligence agencies. The following information and data were provided anonymously, so there are no documented sources.

In China, at Shanghai Shao Cond University, students who are particularly gifted in computer science and mathematics are taught industrial espionage against foreign governments and how to create malware to use both for attacks on third parties and to improve their own protection systems.

India has a government organization called NTRO (National Technical Research Organization), which a law authorizes, in the event of an attack, to retaliate using hacking techniques; the government also encourages its young talents to enter a programme to protect the country.

There is also a group, called ICA (Indian Cyber Army) [21], which, on a daily basis, confronts a group of Pakistani hackers, the PCA (Pakistan Cyber Army) [16]. The purpose of both groups is to safeguard the national security of the State they represent and attempt to conquer the opponent.

Stefano Mele [Int-6] affirms that: "*[. . .] an attack is made on a hostile country and, pretending that the information has leaked, the author of the attack is made known. This way all governments can ascertain that that particular country has the economic power to create effective cyber weapons. In practice it is a warning because at this point the other countries will be afraid of revenge if an attack is attempted. Keeping the attack secret would not produce the same warning effect [. . .].*"

The purchase of 0-day vulnerabilities is an important cyber strategy for a government both in order to make its critical infrastructure secure, as affirmed by the interviewees [Int-6, Int-7, Int-8, Int-9], and to attack. A growing number of countries are willing to spend considerable sums of money to acquire 0-days vulnerabilities.

On this issue members of the Italian Postal and Communications Police affirm that [Int-8]: "*[. . .] Italy does not buy any kind of vulnerability, at least according to our information nothing like that occurs. Other governments buy these vulnerabilities [. . .].*"

Police forces are also employed in controlling the vulnerabilities bought and sold and for this purpose, as well as consulting websites such as Shodan, a search engine capable of indexing the devices connected to the Internet,

they visit Dark Web forums.

V. Conclusions

The present study has shown that market forces and cybercrime activities involving 0-day vulnerabilities drive the research on 0-day vulnerability. We have seen that the goal could be the highest economic profit or the opportunistic exploitation of the vulnerability in non-military cybercrime, or in government settings, to obtain a strategic advantage over adversaries.

Non-military cybercrime often hits as many targets as possible through one or more attacks that exploit the same type of vulnerability, with the sole objective of maximizing profit. On the contrary, military cybercrime invests substantial sums of money in developing highly sophisticated and stealthy attacks especially designed to hit specific targets.

The information collected in the study have made it possible to outline a relatively precise and detailed picture of the three markets known as the White, Black and Government Markets in which the sale of this type of vulnerability occurs, as well as the mechanisms that govern the relationships between the diverse participating entities.

Considering the information collected and the direct testimonies of the interviewees, one issue is still open and could be the subject of further speculation: To which extent 0-day vulnerabilities are part of complex geopolitical relationships that mark the international military, political and economic conflicts in which cyberweapons are used?

To conclude, we wish to attempt a prediction on the future course of actions in this area. The market of 0-days vulnerabilities is likely to expand and become even more governmental-oriented, emerging from the muddy waters of today darknets or underground forums. This would perhaps lead to new regulations similar to the laws controlling the trade of arms. This way companies specialised in vulnerability research will become more transparent, a trend that we are already noticing with some companies openly advertising their activity, sometimes specifying that their customers are governs for national security and law enforcement agencies for contrasting organised crime. However if this trend continues, it is possible that the difference between cybercrime, cyberwar, legal o illegal cyberarms will become even more confused than today.

Acknowledgment

The authors are deeply indebted to all experts who kindly accepted to be interviewed.

References

[1] Licata, F., *La Convenzione del Consiglio dEuropa sul cybercrime e le forme della cooperazione giudiziaria: una risposta globale alle nuove sfide della criminalit transnazionale*. Rome, Italy, 19 September 2005.

[2] Council of Europe, *Convention on Cybercrime*, Budapest, Hungary, 2001. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[3] Team Cymru, *SOHO Pharming - Growing Exploitation of Small Office Routers Creating Serious Risks*, February 2014.

[4] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., Moore, T., and Savage, S., *Measuring the cost of cybercrime*, The economics of information security and privacy, pp. 265-300, Springer, 2013.

[5] Haas, J., *0-day (zero-day)*, About Tech, About.com, 2015. http://linux.about.com/cs/linux101/a/0-day__zero-day.htm

[6] Matrosov, A., et al., *Stuxnet under the microscope*, ESET LLC, September 2010. http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

[7] Wiki-Security, Security Encyclopedia, *Zeus Trojan*. http://www.wiki-security.com/wiki/Parasite/ZeusTrojan/

[8] Codenomicon, *The Heartbleed Bug*, April 2014. http://heartbleed.com/

[9] Mutton, P., *Half a million widely trusted websites vulnerable to Heartbleed bug*, Netcraft, April 2014. http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

[10] Kaspersky Labs' Global Research & Analysis Team, *Equation Group: Questions and Answers*, Kaspersky Lab, Moscow, Russia, February 2015. https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

[11] Bilge, L. and Tudor D., *Before we knew it: an empirical study of zero-day attacks in the real world*, Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.

[12] Miller, C., *The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales*. In Sixth Workshop on the Economics of Information Security, 2007. http://weis2007.econinfosec.org/papers/29.pdf

[13] Tipping Point, *Zero Day Initiative*. http://www.zerodayinitiative.com/

[14] Facebook Inc., *Bug Bounty*, 2015. https://www.facebook.com/whitehat/

[15] Google Inc., *Google Vulnerability Reward Program (VRP) Rules*, 2015. http://www.google.it/about/appsecurity/reward-program/

[16] Amini, P., *Mostrame la Guita!*, Tipping Point, October 2009. http://dvlabs.tippingpoint.com/blog/2009/10/29/mostrame-la-guita

[17] Zetter, K., *Gonzalez Accomplice Gets Probation for Selling Browser Exploit*, March 2010. http://www.wired.com/2010/03/jethro-sentencing/

[18] The Economist, *A Walk on the Darkside*, August 2007. http://www.economist.com/node/9723768

[19] Bizeul, D., *Russian Business Network study*, 2007. http://www.bizeul.org/files/RBN_study.pdb

[20] Greenberg, A., *HBGary Federal's Aaron Barr Resigns After Anonymous Hack Scandal*, Forbes.com, February 2011. http://www.forbes.com/sites/andygreenberg/2011/02/28/hbgary-federals-aaron-barr-resigns-after-anonymous-hack-scandal/

[21] *ICA (Indian Cyber Army)*, 2015. https://www.icalab.com/