0-Day Vulnerabilities and Cybercrime

**Abstract**

This study analyzes 0-day vulnerabilities in the broader context of cybercrime and economic markets. The workisbasedontheinterviewsofseveralleadingexpertsand 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

Este estudo analisa as vulnerabilidades de 0 dias no contexto mais amplo do cibercrime e dos mercados econômicos. O trabalho foi realizado em entrevista aos entrevistados e em uma pesquisa de campo dos autores. Em particular, o cibercrima é considerado quando envolve atividades criminosas tradicionais ou quando as operações militares estão envolvidas. Uma descrição dos diferentes mercados de vulnerabilidades de 0 dias - mercados brancos, negros e governamentais - é fornecida, bem como as características das fábricas de malware e seus principais clientes são discutidos

**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 description1. 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.

O objetivo deste trabalho é estudar como as vulnerabilidades de 0 dias se relacionam ao contexto da cibercriminalidade e dos mercados onde são comercializados. A vulnerabilidade de 0 dias é um tópico sensível e muitas vezes turvo, cujo contexto evolui continuamente, a documentação disponível é escassa e as pessoas envolvidas no comércio ou no desenvolvimento estão relutantes em falar abertamente sobre o problema. A falta de uma visão geral abrangente do fenômeno, foi decidido que o melhor curso de ação para obter informações atualizadas e relevantes era entrevistar alguns especialistas em segurança selecionados com diferentes origens e, a partir de seus diferentes pontos de vista, tentar produzir uma descrição coerente1. Os especialistas selecionados têm autoridade em seus respectivos campos de competência e são empregados diariamente, embora por motivos diferentes, na área de cibercriminalidade a nível nacional e internacional. Além das entrevistas, vários anos de pesquisa possibilitaram analisar a maioria dos documentos disponíveis on-line sobre as vulnerabilidades de 0 dias e discutir o problema com as principais figuras nas várias disciplinas da segurança informática e com o compromisso diário de contrastar o cibercrime.

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

Esta análise serve como base para explorar a dinâmica de negociação de vulnerabilidades de 0 dias nos mercados branco, negro e governamental. Uma seção é dedicada a uma investigação sobre RBN (Russian Business Network), muitas vezes considerada como um exemplo de uma atividade completamente desprovida de ética profissional e, em particular, de seus métodos e serviços operacionais nos últimos anos. Além de redes criminosas como RBN, um papel essencial no desenvolvimento de vulnerabilidades de 0 dias e ciber-armas é desempenhado pela Malware Fábricas.

**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 Licata2 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:

O crime cibernético é uma forma de crime que inclui crimes cometidos através do uso da Internet ou de outras redes informáticas. Um computador (ou outro dispositivo de hardware) ou uma rede de computadores podem desempenhar duas funções diferentes: o instrumento de um crime (se for explorado para cometer) ou a vítima de um crime (se for o alvo). O juiz Fabio Licata2 forneceu um esboço abrangente do cibercrime [1]. Na sua opinião, as ações ilegais realizadas na Internet e através da Internet podem ser classificadas nas seguintes categorias:

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);

Infracções contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos (ou seja, infrações da CIA). Estas ofensas incluem todo o acesso ilegal a sistemas informáticos através de hackers, intercepções ilegais, várias formas de enganação em detrimento dos usuários (por exemplo, phishing), sistema de espionagem (através de spyware ou cavalos de Tróia), até sabotagem projetada para comprometer a disponibilidade do sistema ( Por exemplo através de vírus, ataques de negação de serviço, spam ou bombardeio de correio);

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.;

Delitos informáticos tradicionais, como as fraudes clássicas obtidas pela clonagem de cartões de crédito, cartões de caixa ou outros meios de pagamento, fraudes comerciais on-line, vários tipos de falsificação realizados através do computador, 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 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;

Infracções relacionadas ao conteúdo de informações ou dados transmitidos pela Internet. Pense na pornografia infantil, no racismo e na xenofobia ou na incitação, instigação ou transmissão de instruções para a realização dos mais variados crimes tradicionais (por exemplo, propaganda terrorista). Esta categoria também pode incluir vários tipos de assédio ao computador (o chamado cyberstalking e cyberbullying) e até jogos fraudulentos em linha;

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);

A violação de direitos autorais e propriedade relacionada, como a reprodução ilícita de programas de computador ou todo tipo de trabalho intelectual sobre mídia digital (livros, música, filmes);

The violation of privacy such as the unlawful access to personal data repositories or the unlawful collection and circulation of any such data.

A violação da privacidade, como o acesso ilegal a repositórios de dados pessoais ou a cobrança e circulação ilícitas de tais dados.

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.”

De acordo com o juiz Licata, a segurança informática desempenha um papel essencial "para aumentar a confiança no ciberespaço como um elemento de desenvolvimento econômico, civil e cultural". O juiz Licata continua: "Nos últimos anos, a consciência disso levou a uma proliferação de documentos e Tratados de todas as principais organizações supranacionais: as Nações Unidas e suas organizações colaterais, o G8, a Commonwealth, a Organização dos Estados Americanos, a União Européia, a Cooperação Econômica Paciente Asiática (APEC), a Organização de Cooperação e Desenvolvimento Econômico (OCSE) e a Organização Concelho Europeu."

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.

Na Itália, Lei n. 48/2008, que ratifica a Convenção de Budapeste do Conselho da Europa (2001) sobre o cibercrime [2], está vigente desde 2008. A Convenção de Budapeste foi o primeiro acordo internacional sobre crimes cometidos por meio da Internet ou de outro computador Redes, mesmo que a prova do crime esteja em formato eletrônico; A Convenção prevê uma colaboração extensa e coordenada entre os Estados signatários.

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].

Enquanto o cibercrima assusta cada vez mais os cidadãos e pequenos funcionários que temem incorrer em perdas econômicas ou em danos aos seus dados [3], as empresas e as transações comerciais são o principal alvo do cibercrima, como vários estudos recentes confirmaram [4].

In Italy the authority responsible for investigating and pro secuting cybercrimes is the Postaland 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.

Na Itália, a autoridade responsável por investigar e perseguir os crimes contra o crime na Polícia Pública e de Telecomunicações, cujas atividades de investigação realizadas em 2013 sobre pornografia infantil levaram a 55 prisões em relação a 344 acusações. Em uma entrevista que aconteceu em novembro de 2014 [Int-8], alguns funcionários da Polícia de Correios e Comunicações declararam que o aumento da disseminação de crimes por computador deve-se a um ROI muito elevado (Return On Investment) derivado desse tipo De atividade criminosa.

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.

Outros especialistas entrevistados [Int-6, Int-7, Int-10] afirmam que o aumento da disseminação do cibercrime não é apenas devido à facilidade de renda imediata, mas também à crise econômica internacional e ao desemprego nos últimos anos, o que Empurrou profissionais qualificados nas mãos de criminosos. Em contrapartida, nossa opinião é diferente: não é a recessão econômica que desencadeou o aumento da venda de vulnerabilidades no mercado negro, mas as vendas de vulnerabilidades aumentaram principalmente devido a um mercado mais amplo criado por desenvolvedores de vulnerabilidades principais e correntes de guerra cibernética / cibernética governamental Percepções.

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.

O recrutamento de cibercriminosos também é frequentemente atenuado pela percepção incorreta das implicações e consequências do cibercrime. As pessoas envolvidas em cibercrimas muitas vezes não conseguem entender completamente o significado e as conseqüências de ações ilegais realizadas com o auxílio de equipamentos de TI ou na Internet quando, ao contrário dos criminosos tradicionais, eles sentem que estão em um ambiente seguro com regras soltas.

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 informações pessoais e corporativas representam um grande valor para os criminosos e alimentam um mercado altamente próspero, mas não é fácil estimar a extensão do volume de negócios do cibercrime.

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 [].”

Como Alessio Pennasilico afirma [Int-7]: "[] Russian Business Network, em 2009, teve um volume de negócios maior que a Microsoft, não conheço o volume de negócios de outros mercados, mas o malware e o cibercrime geralmente são altos e aumentam rapidamente [ ]. "

Como Alessio Pennasilico afirma [Int-7]: "[] Russian Business Network, em 2009, teve um volume de negócios maior que a Microsoft, não conheço o volume de negócios de outros mercados, mas o malware e o cibercrime geralmente são altos e aumentam rapidamente [ ]. "

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 [].”

De acordo com Boris Sharov [Int-10], o mercado de cibercrimas é na sua maioria invisível, subterrâneo e silencioso: "[] Embora seja mais ou menos conhecido no campo da droga, permanece inexplorado no campo cibernético. Dito fortemente que ultrapassou as principais indústrias criminosas tradicionais [] ".

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.”

Stefano Mele, um advogado que trabalha em questões de tecnologia, privacidade, segurança da informação e inteligência, explica por que é particularmente difícil estimar o volume de negócios do cibercrime [Int-6]: "[] Não há dados públicos nos quais podemos encontrar essa informação Por várias razões, incluindo danos à reputação, perda de mercado e perda de confiança. Como não há obrigação de publicar relatórios de incidentes quando houve vítimas de ataques de computador, deixando de lado as empresas de telecomunicações, as empresas atacadas não fazem anúncios públicos. O código de silêncio não é apenas um problema na Itália, em qualquer caso, não podemos saber se o cibercrima superou os mercados mais tradicionais em termos de volume de negócios. Pode-se certamente dizer que é um mercado altamente próspero no qual o ROI é muito alto, com pouco investimento; Se o ataque certo, o phishing certo ou o ransomware direito vem ao longo dos ganhos pode ser muito alto, centenas de milhares de 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.”

A Polícia Italiana de Correios e Comunicações compartilha a mesma visão de Stefano Mele, mas especifica que a dificuldade no cálculo do volume de negócios não depende apenas do fato de ser produzida em um mercado subterrâneo [Int-8]: "[é] muito Difícil de estabelecer devido à variedade dos crimes perpetrados através da Internet: do ransomware ao phishing, spam, roubo de identidade, e assim por diante. Todos esses crimes contribuem para aumentar o volume de negócios do cibercrime ".

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.”

Steve Santorelli, sublinha dois aspectos significativos relativos ao debate sobre a extensão do volume de negócios do cibercrime [Int-9]: "Há um grande debate sobre esse número todos os anos e está ficando mais complexo já que os crimes tradicionais estão empregando aspectos cibernéticos o tempo todo . Você não pode colocar um número confiável sobre isso, mas eu sei que todo sindicato criminoso organizado no mundo está gravitando em relação ao cibercrima, pois os riscos são praticamente zero e as recompensas são pelo menos tão altas quanto com seu trabalho tradicional ".

**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.

O cibercrime em um cenário militar (também chamado de Cyberwar) deve ser considerado de forma diferente: os investimentos são mais altos, ataques mais direcionados e focados em objetivos estratégicos e seu sucesso é menos certo e, conseqüentemente, o ROI é consideravelmente menor. A estimativa do volume de negócios do cibercrima no campo militar é ainda mais complicada, neste caso, os fatores geopolíticos entram em jogo e tornam o ganho puro um elemento não essencial. O objetivo do Stuxnet, um malware descoberto em 2010 que infestava várias usinas nucleares, por exemplo, não era tanto os ganhos derivados de um ato de cibercrime quanto retardar o desenvolvimento nuclear do Irã.

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[...].”

Stefano Mele afirmou que [Int-6]: "[...] Os governos investem enormes montantes no campo da cibercriminalidade militar, particularmente no setor de ciberespionagem. Embora a espionagem seja uma prática ilegal, não existem leis que a condenem explicitamente. Não é apenas a China ou os EUA que monitoram ilegalmente outros países, mas também países europeus como a França e o Reino Unido estão envolvidos na mesma atividade [...] ".

**The ambiguous nature of vulnerabilities**

**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.

O conceito de violação do sistema remonta aos anos 80, o período em que provavelmente ocorreram as primeiras vulnerabilidades de 0 dias. Nos anos 80, a segurança informática foi principalmente estudada e debatida a nível acadêmico e não havia percepção do papel fundamental que desempenharia no futuro imediato.

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.

Hoje a situação é radicalmente diferente: os sistemas são protegidos com software e hardware cada vez mais avançados. Para atacar um sistema, é essencial estudá-lo, compreender sua estrutura, identificar o tipo de proteção instalada e o sistema operacional em uso e, por fim, identificar suas vulnerabilidades. O objetivo das violações é saquear informações que possam fornecer um ganho substancial ou explorar ativos de TI.

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

Conforme especificado por Vulnerabilidades e exposições comuns (CVE): "Uma vulnerabilidade de segurança da informação é um erro no software que pode ser usado diretamente por um hacker para obter acesso a um sistema ou rede. A CVE considera um erro uma vulnerabilidade se permitir que um invasor use isso para violar uma política de segurança razoável para esse sistema. "Para CVE, uma vulnerabilidade é um estado em um sistema de computação (ou conjunto de sistemas) que permite que um invasor

• 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.

• Execute comandos como outro usuário;

• Acesse dados contrários às restrições de acesso especificadas para esses dados;

• Posicionar como outra entidade;

• Realizar uma negação de serviço.

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)

Exemplos de vulnerabilidades incluem:

• phf (execução de comando remoto como usuário ninguém);

• rpc.ttdbserver (execução de comando remoto como root);

• arquivo de senha com gravação mundial (modificação de dados críticos do sistema);

• senha padrão (execução de comando remoto ou outro acesso);

• problemas de negação de serviço que permitem que um invasor cause uma tela azul da morte;

• smurf (negação de serviço inundando uma rede)

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.

Também deve ser observado que as vulnerabilidades podem resultar da configuração incorreta de sistemas computacionais cada vez mais complexos ou do descuido dos usuários do sistema, por exemplo, o uso de senhas fracas ou o compartilhamento de senhas com colegas e amigos.

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 cana0-dayattackbeusedbeforeitisnolongerconsidered 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.).

Para definir o conceito de vulnerabilidades de 0 dias, é essencial esclarecer o papel do termo zero. Quando o zero realmente começa? A partir do momento em que a vulnerabilidade é descoberta e divulgada, ou o tempo que é usado pela primeira vez sem que ninguém perceba? E quantas vezes o tempo de ataque pode ser usado como tal? A maioria das pessoas entrevistadas concordou com a seguinte de fi nição [5]: "o termo exploração de 0 dias descreve uma exploração que não é conhecida publicamente. Ele descreve ferramentas de hackers de elite que descobriram um novo bug e compartilhavam apenas com amigos íntimos. Ele também descreve algumas novas explorações para comprometer serviços populares (os suspeitos habituais: BIND, serviços de FTP, distros de Linux, Microsoft IIS, etc.).

Many 0-day exploits are discovered by the victims when hackers use them, or by honeypots. The term 0day 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.

Muitas explorações de 0 dias são descobertas pelas vítimas quando os hackers as usam ou por honeypots. O termo 0day descreve o fato de que o valor das façanhas diminui rapidamente assim que são anunciadas. Em termos gerais, no dia seguinte, uma vulnerabilidade de 0 dias foi anunciada publicamente, as diferenças de valor econômico. O 2º dia é um quarto tão valioso. Dez dias depois, o valor poderia ser 1/1000 do que no dia 0. Isso ocorre porque os criadores de scripts usam rapidamente a exploração em computadores em toda a Internet, comprometendo os sistemas antes que qualquer outro possa chegar a eles. Portanto, uma exploração de 0 dias é uma vulnerabilidade de segurança do computador que está sendo praticada ativamente antes que o conhecimento da exploração se torne uma informação pública.

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 certainlyexistedbefore2000,but they were not considered as distinct from common computer attacks so they did not haveaspeciﬁcname;theyweresimplyknownas’attacks’.

As vulnerabilidades de 0 dias são cada vez mais um tema de discussão na comunidade de segurança de TI, e desde 2000 o termo se tornou uma parte regular do vocabulário da comunidade científica. As vulnerabilidades de 0 dias, que hoje ganham um interesse considerável entre pesquisadores e empresas, também certamente existiram antes de 2000, mas não foram consideradas como distintas dos ataques comuns de computador, então eles não tinham um nome específico, eles são conhecidos como "ataques".

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).

A qualificação de 0 dias é usada tanto quando se refere a uma vulnerabilidade (do ponto de vista da vítima) quanto quando se refere a um ataque (do ponto de vista do invasor).

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.”

Em uma entrevista, Cesar Cerrudo [Int-2], declarou: "As vulnerabilidades de 0 dias existem há muito tempo e foram ativamente usadas, você pode vê-lo nos últimos incidentes Stuxnet [6]. Acho que, no futuro, continuaremos a ver ataques mais específicos que usam explorações de 0 dias ".

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.

Como Cesar Cerrudo explica, os ataques e as vulnerabilidades de 0 dias sempre existiram: é provável, como já mencionado, que, antes de 1986, não fossem explorados para fins lucrativos, mas que violassem a propriedade intelectual do 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.

As definições definidas acima fornecem uma compreensão de quão interessantes e estratégicas vulnerabilidades de 0 dias podem ser para criminosos, governos e a comunidade científica.

**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.

A diferença entre ameaça e vulnerabilidade, muitas vezes ignorada por muitos que se referem a eles como sinônimos, é, em vez disso, essencial para identificar as possíveis medidas de proteção contra vulnerabilidades de 0 dias. Como exemplo, considere Zeus e Heartbleed, dois dos ataques mais conhecidos dos últimos anos.

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, includingPRG,Zbot andInfostealer.IntheUSaloneithas 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].

Zeus é uma família de malware especialmente criada para explorar as vulnerabilidades dos sistemas Windows, a fim de roubar credenciais bancárias. Funciona como um registro de teclas de um homem no navegador e captura de formulário. Também é capaz de criptografar as informações de sistemas infectados para permitir que seus usuários exijam um resgate. Tem muitos aliases, incluindo PRG, Zbot e Infostealer. Nos Estados Unidos, afetaram mais de 3,6 milhões de computadores pessoais. O malware se espalhou globalmente, em filtrar mais de 74 mil contas bancárias e afetar empresas como Amazon, Oracle, Bank of America e NASA. Variações capazes de infectar os sistemas Blackberry e Android também foram descobertas [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].

Heartbleed, por outro lado, explora um bug de segurança da biblioteca criptográfica open-open OpenSSL, amplamente utilizado para implementar o protocolo TLS (Transport Layer Security) [8]. A vulnerabilidade foi causada por uma verificação de limites perdidos no gerenciamento da extensão Heartbeat do protocolo TLS. Estima-se que cerca de 17%, ou seja, meio milhão dos servidores web seguros, certificados pelas autoridades confiáveis, eram vulneráveis ao ataque. A vulnerabilidade Heartbleed permitiu o roubo de chaves privadas do servidor, bem como senhas de usuários e 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.

Tanto a Zeus como a Heartbleed exploram as vulnerabilidades, mas enquanto a Zeus é composta por uma série de programas ad hoc desenvolvidos para tirar proveito de flocos em sistemas Windows, Heartbleed é uma lista de instruções escritas em linha de comando que explora um erro de programação em uma biblioteca essencial de um Serviço amplamente utilizado, sem a ajuda de software. Portanto, pode-se concluir que a Zeus é uma ameaça, enquanto o Heartbleed é uma exploração que aproveita uma vulnerabilidade.

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.

Ameaças e vulnerabilidades compartilham a característica de tornar um sistema informático aberto a ataques, mas pode haver menos vulnerabilidades se o desenvolvimento e manutenção de software tiverem sido realizados com especial atenção à segurança. Se a análise de software das bibliotecas do Heartbeat fosse realizada com maior cuidado, o erro de software que causava o erro Heartbleed provavelmente seria corrigido antes da liberação do software.

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.

Uma boa prática para aqueles que produzem software pode ser sujeitar os módulos desenvolvidos a uma nova análise estática do código em intervalos regulares, na tentativa de minimizar o número de erros.

0-day vulnerabilities are able to expose computer systems to planned ad hoc attack scapable 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.

As vulnerabilidades de 0 dias são capazes de expor os sistemas informáticos a ataques ad hoc planejados de causar danos com conseqüências difíceis de prever: por isso são de grande interesse para aqueles que visam desenvolver ciber-armas visando entre outras organizações governamentais e críticas Infra-estruturas.

**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.

Fábricas de Malware são empresas que criam malwares sob demanda em troca de uma taxa. Nessas empresas, como em qualquer casa de software, grupos de desenvolvimento específicos são configurados, cujo trabalho pode ser definido como malware como um serviço. Como é essencial que um malware seja disponibilizado no prazo mais curto, para aumentar a eficácia do seu uso, é plausível assumir que as mudanças de trabalho são organizadas para permitir o desenvolvimento 24 horas por dia. É difícil estabelecer com certeza quantas fábricas de malware existem e onde estão localizadas.

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.”

Alessio Pennasilico afirma que "esta informação não é conhecida" [Int-7], enquanto Boris Sharov [Int-9] afirma: "Nós nunca tentamos avaliar o número dessas fábricas. Do nosso ponto de vista, não é tão importante - temos nossas estatísticas de arquivos suspeitos recebidos (mais de 200.000 por dia) e o número de novos malwares que adicionamos às nossas bases de assinatura ou tratamos de diferentes maneiras ".

Steve Santorelli explains why it is not simple to obtain precise information on Malware Factories [Int-9]: ”[...] these people dont want to be found: the yal ready 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 [...].”

Steve Santorelli explica por que não é simples obter informações precisas sobre Fábricas de Malware [Int-9]: "[...] essas pessoas não querem ser encontradas: o YAL pronto tem sua rede de contatos, nada de bom viria para eles Publicando em qualquer coisa que se aproxime de um fórum público. Embora o que eles possam estar fazendo não seja tecnicamente ilegal, eles não precisam da atenção dos governos, agências de inteligência, policiais e outros pesquisadores e tipos de mídia [...] ".

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.

Em nossa opinião e, em particular, de acordo com o co-autor Armin, na Rússia e na China existem duas principais fábricas de malware, que são empresas para todos os efeitos e propósitos com uma localização precisa e um quarto principal. No entanto, é um erro pensar em Malware Factories como organizações tradicionais de colarinho branco configuradas com cabines e horas de trabalho fixas. O país que uma Fábrica de Malware pertence depende da localização da comunidade que oferece suporte e que pode ser considerada origem do malware. O malware mais avançado e desenvolvido nos últimos anos refere-se principalmente ao software de espionagem, Advanced Persistent Threat (APT), malware de intrusão e ciber-armas. Por estas razões, existem Fábricas de Malware nos Estados Unidos, Rússia, China, Reino Unido, França, Turquia, Paquistão e Índia; Essas organizações devem ser contatadas através de intermediários, pois geralmente não podem ser alcançados diretamente.

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.

O Grupo de Equações certamente deve ser contado como uma das Fábricas de Malware; As características deste grupo foram discutidas pela Kaspersky Lab em um documento publicado em 16 de fevereiro de 2015 [10] e assim chamado com referência à criptografia usada no desenvolvimento de malware. O malware desenvolvido pelo Equation Group é altamente sofisticado e capaz de infectar a segurança de discos rígidos produzidos por empresas específicas. É importante ressaltar que eles podem permanecer ativos mesmo após o sistema operacional ter sido reinstalado.

**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.

Quem descobre uma vulnerabilidade de 0 dias tem várias possibilidades para o curso de ação a seguir. Primeiro, o pesquisador pode decidir divulgar publicamente a vulnerabilidade somente depois que o fornecedor lançou um patch (divulgação coordenada). Por exemplo, como descrito por Feliciano Intini [Int-4]. Ele / ela poderia apresentar a descoberta em uma conferência de segurança ou o mesmo fornecedor poderia dar créditos ao pesquisador quando anunciar a atualização do software. Caso contrário, por qualquer motivo, o descobridor da vulnerabilidade pode compartilhá-lo sem que o fornecedor seja informado e, em seguida, capaz de liberar um patch ou, eventualmente, ele / ela pode querer monetizar seu trabalho ao decidir vender a vulnerabilidade no mercado. Este caso é cada vez mais frequente, bem como o número de pessoas que se alimentam de pesquisas de vulnerabilidades. Além disso, o mercado poderia ser o mercado branco, o mercado negro ou o mercado do governo.

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.

O mercado branco é um mercado legal que não está escondido, em que as empresas de tecnologia da informação oferecem um pagamento aos pesquisadores dispostos a vender uma vulnerabilidade de 0 dias que descobriram. Seja qual for a opção que o pesquisador escolha, ele / ela está bem ciente de que o valor (ou seja, para o reconhecimento técnico ou o preço de mercado) de uma vulnerabilidade de 0 dias pode cair rapidamente de muito alto para quase 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].

O valor está estritamente vinculado à notoriedade das vulnerabilidades: se fosse divulgado e negociado também por outros ou se um remendo fosse repentinamente divulgado, o valor da vulnerabilidade cairá até que não valesse nada e o pesquisador arriscaria sofrer um financeiro fiável Perda porque seu trabalho se torna inútil. Para algumas vulnerabilidades críticas, as figuras podem chegar a centenas de milhares de dólares e mais, um ganho potencial que poderia desaparecer apenas desperdiçando um dia demais argumentando sobre o preço de venda. O tempo é uma variável que dificulta até encontrar um comprador confiável [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.

Os compradores, por sua vez, desejam proteger seu investimento em relação a dois aspectos, pelo menos: a vulnerabilidade deve ser tecnicamente efetiva, o que significa que ele realmente deve permitir o que é suposto permitir, e a compra deve ser exclusiva, isto é A vulnerabilidade não deve ser revendida no futuro ou já foi vendida a terceiros. Se um pesquisador revenda uma vulnerabilidade a mais do que um único comprador, isso seria percebido como uma fraude e causaria danos financeiros aos compradores. Por esta razão, é costume que os compradores de vulnerabilidade realizem a devida diligência no vendedor e o acordo inclui a compra da propriedade intelectual da vulnerabilidade de 0 dias e todos os direitos conexos [12]. Como é facilmente previsível, o mercado de vulnerabilidades de 0 dias é em grande parte baseado em reputação como meio para gerenciar sua falta de confiança intrínseca.

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.

O efeito das ações do comprador é duplo: por um lado, eles garantem aos pesquisadores de vulnerabilidade maiores ganhos, melhorando sua reputação e, por outro lado, regulam o mercado de vulnerabilidades, reduzindo o número de golpes.

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

Como é facilmente previsível, o mercado de vulnerabilidades de 0 dias é em grande parte baseado em reputação como meio para gerenciar sua falta de confiança intrínseca.

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.

Existem empresas que compram vulnerabilidades de 0 dias para assumir a responsabilidade de informar o fornecedor de um novo bug e, entretanto, proteger seus clientes através do desenvolvimento de um patch temporário pendente do definitivo. Este é o caso da Zero Day Initiative (ZDI) riu por Tipping Point, que começou a comprar vulnerabilidades usando este método em 2003 [13]. O ZDI não é o único programa que adquire vulnerabilidades de 0 dias para garantir aos seus clientes: iDefense e Securiteam, por exemplo, também oferecem pagamento a pesquisadores que, em troca, estão dispostos a atribuir todos os direitos sobre a vulnerabilidade.

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].

Muitas grandes empresas lançaram programas Bounty oficialmente para recompensar pesquisadores que encontraram vulnerabilidades em seus produtos. O Facebook, por exemplo, introduziu uma página dedicada em seu site onde explica como comprar as vulnerabilidades e as vulnerabilidades que considera adequadas para relatar [14]. O pagamento mínimo prometido pela rede social é de US $ 500 por vulnerabilidade. Em 2010, também o Google lançou um Programa Bounty para a compra de vulnerabilidades de seus produtos [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:

Em geral, as informações fornecidas até agora mostram que não existe uma tarifa uniforme para vulnerabilidades de 0 dias compartilhadas no mercado. Em várias conferências dedicadas ao cibercrime, foi possível obter algumas informações úteis sobre esse recurso específico. Por uma questão de simplicidade, é apresentado um breve questionário abaixo que pode servir de guia para determinar o valor da vulnerabilidade:

• 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?

• Quão generalizado é o uso da aplicação que é vulnerável?

• O aplicativo vem por padrão com o sistema operacional?

• O aplicativo está ativado por padrão?

• A autenticação é necessária para explorar o aplicativo?

• Quão bem as configurações de depuração típicas bloqueiam o acesso ao aplicativo?

• Quais versões de sistemas operacionais / aplicativos são vulneráveis?

• A vulnerabilidade em um servidor ou aplicativo cliente?

• A interação do usuário é necessária para explorar a vulnerabilidade?

• Quão difícil é encontrar a vulnerabilidade (que é uma medida de proxy de quanto tempo será antes de ser descoberta por outra pessoa)?

• Quantas pessoas conhecem a vulnerabilidade?

• Quão confiável é a exploração?

• Um único recurso funciona contra várias versões?

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.”

Cesar Cerrudo [Int-2] affirms: "O valor de 0 dias depende do produto afetado e de quantas pessoas e / ou servidores executem esse produto. 0 dias para o software amplamente utilizado será o mais valioso. O valor mais alto dependendo dos mais valiosos 0 dias são aqueles que permitem que você remova remotamente servidores sem autenticação e também vulnerabilidades no software do lado do cliente, como Internet Explorer, Adobe Reader, Microsoft Office, etc. "

In conclusion, a researcher who has identiﬁed a vulnerability 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.

Em conclusão, um pesquisador que identificou uma vulnerabilidade e decide vendê-lo não pode saber com certeza o quanto ele ganhará da descoberta, pois, na ausência de uma tarifa específica, cada caso é avaliado individualmente e de forma independente por cada comprador potencial ; Com base em uma ordem de grandeza de que ambas as partes estão cientes, estabelece-se uma negociação comercial tradicional, cujo objetivo é a satisfação mútua.

**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.

As vulnerabilidades de 0 dias também são negociadas no Mercado Negro, um mercado de bens e serviços ilegais, onde as operações comerciais ocorrem de duas maneiras principais: praticamente, realizadas através de contatos e vendas on-line, e fisicamente, que ocorre através de reuniões pessoais entre criminosos que compram e / ou vendem vulnerabilidades digitais.

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

O Black Market, portanto, tem diferentes facetas: há um mercado negro menos escondido, onde a maioria das transações envolvem a venda de bens e serviços ilegais, como números de cartões de crédito roubados, documentos falsos, mas não vulnerabilidades de 0 dias. No mercado negro há um mercado ainda mais oculto, onde as vulnerabilidades de 0 dias são vendidas

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].

A venda de vulnerabilidades de 0 dias neste mercado subterrâneo mais isolado ocorre de maneiras que não estão claramente documentadas e também as opiniões dos especialistas entrevistados são misturadas. Boris Sharov acredita que, para realizar transações, você precisa primeiro ser introduzido em fóruns específicos da Darknet [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.

De acordo com a nossa experiência, para acessar o mercado negro de vulnerabilidades de 0 dias, é necessário passar por empresas intermediárias específicas, portanto usando o mesmo método de abordagem descrito para Fábricas de Malware.

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].

Um elemento que torna o Black Market particularmente atraente para aqueles que desejam vender uma vulnerabilidade de 0 dias é o lucro que pode ser obtido. Pedram Amini, um pesquisador de segurança, por exemplo, afirma que, no mercado negro, os preços das vulnerabilidades individuais variam de 20.000 a 100.000 dólares, com um preço médio de cerca de 50.000 dólares [16].

Intriguingly, there is also the possibility of the same 0day vulnerability being sold on both the White Market and the Black Market by the same researcher. An interviewee whopreferstoremainanonymous[Int-1]afﬁrmsthatthose 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 vulnerabilitiesﬁrsttohis/her government, which uses them to complete targeted attacks, then, once some time has passed, to the Black Market.

Curiosamente, há também a possibilidade de vender a mesma vulnerabilidade de 0day no mercado branco e no mercado negro pelo mesmo pesquisador. Um entrevistado que responde que [Int-1] afirme que aqueles que trabalham no setor podem adivinhar quais pesquisadores estão envolvidos nesse tipo de jogo de con, tanto através de conhecimentos pessoais desenvolvidos em um mundo tão apertado quanto o padrão de vida que alguns pesquisadores mostram. O entrevistado anônimo continua, afirmando estar diretamente familiarizado com pelo menos um pesquisador que vende vulnerabilidades de 0 dias antes do seu governo, que os usa para completar ataques direcionados, e depois, algum tempo depois, para o Mercado Negro.

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.

Ioan Landry [Int-5] não descarta a existência de pessoas que vendem suas vulnerabilidades para mais mercados: Landry, no entanto, adverte esses indivíduos das conseqüências terríveis que podem incorrer. Se o esquema de vendas duplas se tornasse conhecido, os vendedores arriscariam sua reputação e poderiam ser expulsos do círculo altamente selecionado de pesquisadores confiáveis, além de sofrerem consequências criminosas.

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].

Um exemplo documentado de falta de atenção é o envolvimento de Jeremy Jethro, um profissional de TI que vendeu uma exploração por 60 mil dólares para a gangue Gonzalez de Chicago, que permitiu o acesso não autorizado às redes de TI. O grupo Gonzalez roubou mais de 90 milhões de números de cartão de crédito e débito. Jeremy Jethro foi condenado a três anos de liberdade condicional e uma quantia de 10.000 dólares. Jethro não é o único especialista em TI que colaborou com a gangue Gonzalez: Stephen Watt, antigo programador da Morgan Stanley, forneceu um fuzileiro que permitiu que a gangue Gonzalez roubasse dados corporativos da empresa TJX. Watt foi condenado a dois anos de prisão e o pagamento de 171,5 milhões de dólares como compensação pelos danos sofridos pela empresa americana. Finalmente, Humza Zaman, ex-chefe de segurança de rede no Barclays Bank, foi condenada a 46 meses de prisão e uma lei de 75 mil dólares por ter lavado entre 600.000 e 800.000 dólares para o grupo Gonzalez [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 thelargestproviderofillegalInternetservicesintheworld. According to a Verisign estimate, the turnover of RBN derived from scams alone perpetrated through phishing amounts to 150 million dollars per year [18].

Um exemplo impressionante do Black Market é representado por RBN (Russian Business Network), um provedor de serviços de Internet ilegal com sede em São Petersburgo. É um provedor completamente anônimo, sem identidade jurídica, em que os papéis principais são ocupados por pessoas anônimas. Os sites registrados oferecem um endereço de e-mail de contato anônimo e os serviços oferecidos não são anunciados, incluindo a venda de ataques de computador, serviços voltados ao roubo de dados pessoais e serviços relacionados à pornografia infantil. Finalmente, os pagamentos podem ser feitos sem deixar rastro. A RBN expandiu sua atividade também através de acordos entre criminosos fora das fronteiras russas, tornando-se o maior fornecedor de serviços internacionais de internet no mundo. De acordo com uma estimativa da Verisign, o volume de negócios do RBN derivado de golpes sozinho perpetrados através de phishing é de 150 milhões de dólares por ano [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 andc redentials 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:

Jart Armin, um desses co-autores de papel, em uma pesquisa independente ainda não publicada mostra que o volume de negócios da RBN é de cerca de 200 milhões de libras por ano. Ele também especificou que a maioria dos golpes foram perpetrados on-line e que um site de apostas foi especialmente criado para lavar o dinheiro roubado ilegalmente. Atrás do RBN existem criminosos e antigos agentes da KGB, onde a identidade do fundador é desconhecida. Ele é conhecido apenas por seu pseudônimo Flyman. Durante suas investigações, a Armin e alguns de seus colaboradores tiveram a oportunidade de inspecionar alguns servidores RBN, onde identificaram 200 a 300 pastas contendo identidades, contas bancárias e redes sociais para computadores comprometidos, com um valor estimado de 5 milhões de libras por pasta. Antes do trabalho de Armin, a única investigação conhecida sobre RBN era até 2007, quando RBN aparentemente desmantelou suas operações [19]. Agora, graças à nova investigação, é possível reconstruir a história dessa gangue criminosa que traçou sua atividade desde sua fundação, em 2000, até março de 2015:

Origins (2000-2003) and Structure: Russian Business Network (RBN) was originally a cellular structured cybercrime operation. It was established as a collaborative activity based in St. Petersburg and ﬁnanced and sheltered by the organized crime enterprise the Tambov Gang. The initial operations centred around TooCoin Software and the earlier ValueDot/SBT Telecom Network.

Origens (2000-2003) e Estrutura: Russian Business Network (RBN) era originalmente uma operação de cibercrime estruturada celular. Estabeleceu-se como uma atividade colaborativa baseada em São Petersburgo e financiada e protegida pela empresa de crime organizado, o Tambov Gang. As operações iniciais foram centradas em torno do software TooCoin e da rede de telecomunicações ValueDot / SBT anterior.

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 atthecentre of a networkofSt.Petersburg-basedorganizationsengaged 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.

Principais atividades operacionais abertas (2003-2007): RBN foi melhor descrito durante esse período como um host à prova de balas. O servidor era possuído / controlado e operado pelo RBN: servia de phishing, código / ferramentas maliciosas, comandos de comando e controle de botnet (C & C) e ataques de negação de serviço distribuídos (DDoS) e pornografia infantil. Era tão significativo que o ISP aparentemente hospedasse praticamente todos os grandes cavalos de Tróia que visavam informações bancárias em algum momento. O RBN não era uma entidade autônoma, e suas atividades ilegais não se encerraram na sua área de IP. Em vez disso, o RBN foi atribuído a uma rede de organizações baseadas em São Petersburgo envolvidas em atividades que poderiam ser classificadas como RBNs. A organização criminosa não estava apenas localizada na Rússia, mas também tinha filiais no Panamá, Seychelles, Hong Kong e Turquia.

Cloaked and Related Spin-off Operations (20082015): 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.

Operações Spin-Off Cloaked e Relacionadas (20082015): Foi visto na época (novembro de 2007), o RBN foi de folga. No entanto, o RBN pode até mesmo estar se dividindo em peças menores criadas para as infra-estruturas da Internet de vários países. Embora pouca informação tenha sido divulgada publicamente, uma das áreas-chave das atividades distribuídas pelo RBN foi a pornografia infantil. Como descobriu mais tarde em 2010, essa atividade, embora tenha criado uma conscientização pública aumentada e negativa sobre RBN em 2007, foi uma ação importante e contínua. Foi principalmente para fins de extorsão e proteção contra a aplicação da lei e a investigação, já que conhece um banco de dados de 18.000 usuários, com membros-chave da Duma russa, funcionários governamentais, funcionários legais e pessoas de outros 25 países nomeados no DB.

**Government Market**

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

Além dos mercados brancos e negros, existe um mercado que pode ser definido como mercado governamental ou mercado cinza.

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

Um entrevistado confidencial afirma que o governo americano compra vulnerabilidades de 0 dias para não se proteger, mas antes atacar [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 recipientes 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.

Os e-mails roubados por Anonymous da empresa privada HBGary, uma empresa especializada em segurança de TI, parecem testemunhar tais atividades governamentais. Os e-mails contêm comunicações entre membros da empresa de segurança informática e membros do governo dos EUA. Entre os conteúdos dos e-mails, vale a pena mencionar um plano para desacreditar o WikiLeaks através da introdução de documentos falsos em seu site, a suposta identi ficação de alguns membros da Anônimo, mas sobretudo algumas vulnerabilidades de 0 dias e sua operação; Neste último caso, alguns e-mails possuem anexos contendo as vulnerabilidades reais discutidas nos e-mails. Alguns e-mails ainda dão a impressão de que uma empresa privada, como a HBGary, realizou operações de guerra cibernética no lugar do exército regular. Parece que os e-mails foram roubados devido a um erro de configuração do servidor de e-mail que foi pirateado através de uma operação de injeção SQL greenberg2011. Os e-mails roubados não são criptografados e escritos em linguagem simples e, na verdade, são muito claros e explícitos. Os recipientes variam de empresas privadas conhecidas a instituições públicas e os e-mails foram enviados para pessoas que desempenham papéis fundamentais dentro da organização. Alguns contêm anexos que podem ser documentos privados e exemplos de documentos falsos, ou mesmo vírus, enviados como arquivos comprimidos sem senhas e, portanto, são fáceis de descompactar e analisar.

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.

Os governos de alguns países são organizados para implementar programas de treinamento técnico para futuros hackers, o melhor dos quais terá a oportunidade de trabalhar em agências de inteligência. As seguintes informações e dados foram fornecidos anonimamente, portanto, não há fontes documentadas.

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 attacksonthirdpartiesandtoimprovetheirownprotection systems.

Na China, na Universidade Xangai Shao Cond, estudantes que são particularmente talentosos em ciência da computação e matemática são ensinados a espionagem industrial contra governos estrangeiros e como criar malwares para usar tanto para ataques de terceira partes como para proteger os sistemas de proteção.

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.

A Índia tem uma organização governamental chamada NTRO (Organização Nacional de Pesquisa Técnica), que uma lei autoriza, em caso de ataque, a retaliar usando técnicas de hacking; O governo também incentiva seus jovens talentos a entrar em um programa para proteger o país.

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.

Há também um grupo, chamado ICA (Indian Cyber Army) [21], que, diariamente, enfrenta um grupo de hackers paquistaneses, o PCA (Pakistan Cyber Army) [16]. O objetivo de ambos os grupos é proteger a segurança nacional do Estado que representam e tentar conquistar o oponente.

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 [...].”

Stefano Mele [Int-6] afirmou que: "[...] um ataque é feito em um país hostil e, fingindo que a informação vazou, o autor do ataque é conhecido. Desta forma, todos os governos podem verificar que esse país tem o poder econômico de criar ciber-armas efetivas. Na prática, é um aviso porque, neste momento, os outros países terão medo da vingança se for tentado um ataque. Manter o segredo de ataque não produziria o mesmo efeito de aviso [...] ".

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.

A compra de vulnerabilidades de 0 dias é uma estratégia cibernética importante para um governo, tanto para tornar a sua infra-estrutura crítica segura, como confirmada pelos entrevistados [Int-6, Int-7, Int-8, Int-9] e para ataque. Um número crescente de países está disposto a gastar consideráveis somas de dinheiro para adquirir vulnerabilidades de 0 dias.

On this issue members of the Italian Postal andCommunications 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 [...].”

Sobre esta questão, membros da Polícia de Correios e Comunicações italianas afirmaram que [Int-8]: "[...] a Itália não compra qualquer tipo de vulnerabilidade, pelo menos de acordo com a nossa informação, nada disso ocorre. Outros governos compram essas vulnerabilidades [...] ".

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.

As forças policiais também são empregadas no controle das vulnerabilidades compradas e vendidas e, para esse fim, além de sites de consultoria como o Shodan, um mecanismo de pesquisa capaz de indexar os dispositivos conectados à Internet, eles visitam fóruns da Dark Web.

**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 nonmilitary cybercrime, or in government settings, to obtain a strategic advantage over adversaries.

O presente estudo mostrou que as forças do mercado e as atividades de cibercrime que envolvem vulnerabilidades de 0 dias conduzem a pesquisa sobre a vulnerabilidade de 0 dias. Vimos que o objetivo poderia ser o maior lucro econômico ou a exploração oportunista da vulnerabilidade no cibercrime não militar, ou em ambientes governamentais, para obter uma vantagem estratégica em relação aos adversários.

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.

O cibercrime não militar atinge frequentemente tantos alvos quanto possível através de um ou mais ataques que exploram o mesmo tipo de vulnerabilidade, com o único objetivo de maximizar o lucro. Pelo contrário, o cibercrime militar investe montantes substanciais de dinheiro no desenvolvimento de ataques altamente sofisticados e sigilosos especialmente projetados para atingir metas específicas.

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.

A informação recolhida no estudo permitiu delinear uma imagem relativamente precisa e detalhada dos três mercados conhecidos como mercados brancos, negros e governamentais em que ocorre a venda deste tipo de vulnerabilidade, bem como os mecanismos que regem a Relações entre as diversas entidades participantes.

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?

Considerando a informação coletada e os testemunhos diretos dos entrevistados, uma questão ainda está aberta e pode ser objeto de novas especulações: em que medida as vulnerabilidades de 0 dias são parte de relações geopolíticas complexas que marcam os conflitos militares, políticos e econômicos internacionais em Quais as cibercapilas são usadas?

To conclude, we wish to attempt a prediction on the future course of actions in this area. The market of 0days 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.

Para concluir, desejamos tentar uma previsão sobre o curso futuro das ações nesta área. O mercado de vulnerabilidades de 0 dias provavelmente se expandirá e se tornará ainda mais orientado para o governo, emergindo das águas enlameadas de hoje darknets ou fóruns subterrâneos. Isso talvez leve a novos regulamentos semelhantes às leis que controlam o comércio de armas. Desta forma, as empresas especializadas em pesquisa de vulnerabilidade tornar-se-ão mais transparentes, uma tendência que já estamos percebendo com algumas empresas anunciando abertamente sua atividade, às vezes especificando que seus clientes são governos para a segurança nacional e as agências de aplicação da lei para contrastar o crime organizado. No entanto, se essa tendência persistir, é possível que a diferença entre cybercrime, ciberwar, legal ou ciberarmes ilegais se torne ainda mais confusa do que hoje.

**Acknowledgment**

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

Os autores estão profundamente em dívida com todos os especialistas que aceitaram ser entrevistados.