International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:3, 2014

Software Vulnerability Markets: Discoverers and Buyers

Abdullah M. Algarni, Yashwant K. Malaiya

***Abstract*—**Some of the key aspects of vulnerability—discovery, dissemination, and disclosure—have received some attention recently. However, the role of interaction among the vulnerability discoverers and vulnerability acquirers has not yet been adequately addressed. Our study suggests that a major percentage of discoverers, a majority in some cases, are unaffiliated with the software developers and thus are free to disseminate the vulnerabilities they discover in any way they like. As a result, multiple vulnerability markets have emerged. In some of these markets, the exchange is regulated, but in others, there is little or no regulation. In recent vulnerability discovery literature, the vulnerability discoverers have remained anonymous individuals. Although there has been an attempt to model the level of their efforts, information regarding their identities, modes of operation, and what they are doing with the discovered vulnerabilities has not been explored.

Reports of buying and selling of the vulnerabilities are now appearing in the press; however, the existence of such markets requires validation, and the natures of the markets need to be analyzed. To address this need, we have attempted to collect detailed information. We have identified the most prolific vulnerability discoverers throughout the past decade and examined their motivation and methods. A large percentage of these discoverers are located in Eastern and Western Europe and in the Far East. We have contacted several of them in order to collect firsthand information regarding their techniques, motivations, and involvement in the vulnerability markets. We examine why many of the discoverers appear to retire after a highly successful vulnerability-finding career. The paper identifies the actual vulnerability markets, rather than the hypothetical ideal markets that are often examined. The emergence of worldwide government agencies as vulnerability buyers has significant implications. We discuss potential factors that can impact the risk to society and the need for detailed exploration.

***Keywords*—**Risk management, software security, vulnerability discoverers, vulnerability markets.

I. Introduction

POTENTIAL exploitation of software security vulnerabilities has now emerged as a major security threat to organizations, some economic sectors, and national defense. Software vulnerability can be defined as a software defect or weakness in the security system that could be exploited by a malicious user, causing loss or harm [1]. A vulnerability exploit is a code that exploits the vulnerability, and serves as proof that the vulnerability is indeed exploitable. A vulnerability that has not been disclosed and the associated exploit are often termed *zero-day*.A patch, when applied, can remedy a vulnerability. The number of unremedied vulnerabilities in a system represents the degree of security risk. It is important during the software lifecycle development process to evaluate and manage the risk in order to assess how it will impact users, organizations, and society.

Vulnerability discovery models that attempt to model the vulnerability discovery process have been recently proposed [2], [3]. However, there has not been a study of actual vulnerability discoverers and what motivates them. The individuals who discover the vulnerabilities (termed *discoverers* here) and those who exploit them (*exploiters*) are two separate groups. Discovering a vulnerability takes a much higher degree of technical skill and insight. The exploiters do not require a comparable skill—in fact, in the presence of an exploit; a patient hacker may achieve a security breach largely mechanically.

The vulnerability discoverers represent a critical source of security risk, should they choose to sell the vulnerability to malicious organizations or individuals. A vulnerability sold to the developing organization [4] results in a patch that minimizes the risk. However, a vulnerability could also be sold to an organization interested in using it for exploitation. Reports suggest that some exploitable vulnerabilities can command market prices exceeding $100,000[5]-[6].

Many vulnerability discoverers seek to preserve the right to their claim of having discovered a vulnerability; since it serves to acknowledge the discoverer's expertise. For example, the website of well-known University of Cambridge researcher Ross Anderson mentions a vulnerability that he and his student discovered in 2003 [7].A mid-year peak in vulnerability discovery, specifically in Microsoft products, can be explained by the coinciding date of a major conference, wherein security experts often present their vulnerability findings [8].

This study examines real vulnerability markets as they exist. In a market, a commodity (here an undisclosed vulnerability) is made by the producers, and is bought by the consumers or resellers of the commodity. The price is determined by supply and demand. A market may be regulated to some extent or it may be largely unregulated. The presence of a market itself enhances the level of production and consumption. Kannan and Telang [9] present an early mathematical study of the vulnerabilities market, where the discoverers are either benign or malicious, and come to the conclusion that a federally controlled mechanism would be better for society. As we present here, the real markets that have emerged are more complex and are international in nature.

As we discuss below, a large percentage of vulnerabilities are found by experts external to the actual software development organizations. They are free to disclose the vulnerabilities that they discover in any way they like. The hackers who are vulnerability exploiters are often classified as white hat, black hat, and gray hat [10]-[11]. These

A. M. Algarni and Y. K. Malaiya are with the Computer Science Department,Colorado State University, Fort Collins, CO 80523 USA (e-mail: algarni@ cs.colostate.edu, Malaiya@cs.colostate.edu).

classifications do not apply to the vulnerability discoverers who are security researchers engaged in finding vulnerabilities since they may choose different markets for different vulnerabilities. Also note that, in general, the exploiters and the discoverers are distinct groups. Discovering vulnerabilities is not an illegal or anti-social activity, it is a respectable profession; whereas exploiting vulnerabilities is generally the opposite (unless it is part of a service).

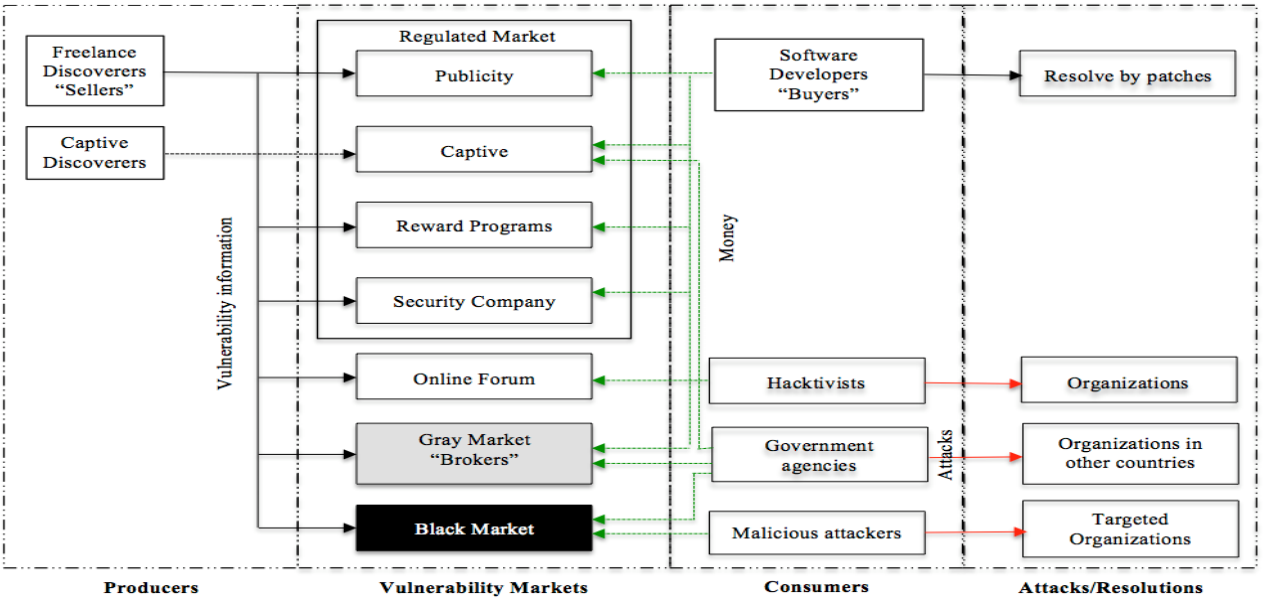

Fig. 1 The current software vulnerability markets

The vulnerability markets, as shown in Fig. 1, may be classified as regulated, where the transactions are properly recorded and disclosed; black, where the transactions are not disclosed and there is no attempt to safeguard the society; or gray, where the transactions can be termed legitimate or improper, depending on the point of view. In the regulated markets the buyers are original software developers, third-party security service organizations follow proper practices for disclosing the vulnerabilities, and the transactions are well-documented [12], [13].

The current software vulnerability reward programs are a major part of the legitimate markets that attempt to attract the vulnerability discoverers who might otherwise resort to selling their findings on the black market. These programs are relatively new and sometimes limited. They attempt to bring a discovery to the legitimate market, which significantly reduces the risk to society. Recent reports suggest that government agencies in several countries have become major player in the gray markets [14], and thus there has been a remarkable change in the vulnerabilities markets.

There are several vulnerability databases organized by government-affiliated or private organizations. They include the National Vulnerability Database (NVD), Open Source Vulnerability Database (OSVDB), the vulnerability data collected by Frei et al. [15] (FVDB), Exploit Database, and IBM X-Force Vulnerability Database. In this paper, we have used OSVDB for some of our investigations. As implied by its name, OSVDB is an open-source, community-organized database associated with the Open Security Foundation, with the stated aim being to provide "accurate, detailed, current, and unbiased technical information". It contains more than 101,350 vulnerabilities found by 4,735 researchers [16].

The first section of this paper discusses the vulnerability markets that have emerged, including the current reward programs. The next section examines the behavior of the vulnerability discoverers by identifying the top discoverers using the OSVDB database, and examines their records and motivation. We examine the data for well-known open-source browsers in order to determine what fraction of the vulnerabilities are discovered internally by the browser development teams in order to assess the relative significance of external vulnerability finders. We have successfully contacted some of discoverers in OSVDB and other, and present what we have discovered about them, even though the vulnerability discovery process is somewhat secretive. Finally, we discuss the implications of the real vulnerability markets along with suggestions for future work.

II. Vulnerability Markets and the Main Players

Vulnerability discoverers can be internal or external to a software development organization. They seek appropriate rewards for their capabilities. The external vulnerability finders (freelancers) are often free to offer their discovery in exchange for a suitable reward. They may attempt to maximize their reward by selling vulnerabilities in the appropriate vulnerabilities markets [9]-[17].

TABLE I
SOME CURRENT VULNERABILITY REWARDS PROGRAMS

Program	# Vulns. type	Max reward	Min reward	# of beneficiaries	Trend
Vulnerability Reward Program for Google web properties	5	$20,000	$100	2010: 51 2011: 122 2012: 189 2013: 226	Increase
Chrome Vulnerability Reward Program	Any security bug	>= 10,000	$500	543	N/A
The Mozilla Security Bug Bounty Program	Certain bugs depending on some criteria	$3000 (US) cash reward and a Mozilla T-shirt	$500	N/A	N/A
Facebook	Certain qualifying security bugs	No maximum	$500	Prior to 2011: 43 2011: 46 2012: 111 2013: 235	Increase
WordPress Security Bug Bounty Program	11	$1000	$25	N/A	N/A
CCBill Vulnerability Reward Program	7	$ 500	$300	42	Hold
Secunia Vulnerability Coordination Reward Program (SVCRP)	Most bugs depending on some criteria	Most Valued Contributor& Most Interesting Coordination Report	N/A	N/A	N/A
ZDI Rewards Program (TippingPoint)	Particular bugs depending on some criteria	$25,000	$1000	N/A	N/A
iDefense (Verisign)	N/A	N/A	N/A	Significant number	N/A

In an ideal situation, the discoverers seek no reward and submit the vulnerabilities found to a responsible disclosure mechanism. Receiving credit for a vulnerability discovered is sufficient compensation for some. However, it is not enough for many discoverers. They know that vulnerabilities can have significant economic value [18] because they can lead to zero-day exploits that might harm organizations, the economy, and ultimately, society [19]. Some exploits have sold for as much as $250,000 [20]. In addition to money, some discoverers find the fame generated by the disclosure attractive, as it can translate into further economic opportunities.

Some organizations, such as Google, have acknowledged the importance of freelance discoverers, and offer a significant monetary award in addition to the possible inclusion in their 'discoverers hall of fame'. A good example of a vulnerability discoverer who has taken advantage of such a reward program is Sergey Glazunov, a Russian student and security researcher who earned $60,000 by discovering a new exploit in Google's Chrome browser [21]. Generally, finding vulnerability exploits is legal, and some legitimate businesses sell them. The price for an exploit sold to business and government agencies in the United States ranges from $20,000 to more than $250,000 [22]. Each market has some attributes that are more attractive for some producers (discoverers) and consumers (buyers) based on their long and short term objectives. A market is defined by its governing rules and conventions. The transactions between discoverers and buyers (software venders, those with malicious intentions, or resellers) involve an exchange of vulnerability information for a suitable price, generally money. The buyers of vulnerabilities derive the value by making their software product safer, or by the rewards a zero-day attack may bring. Below we discuss each of the markets.

A. Regulated Vulnerability Market

This is a regulated market that is controlled by conventions and laws that attempt to prevent any improper actions towards the society as a whole. It includes the four markets discussed below. In all of these markets the vulnerability information is transferred to the software venders, who then patch the vulnerability in their products before it is disclosed.

1. Publicity:

In this case, the discoverer submits the finding to an authority, where it undergoes a well-defined responsible disclosure procedure. The discoverer gets the recognition and the software developer gets the chance to develop a patch before the vulnerability is disclosed. The publicity generated may enhance a discoverer's reputation as a capable researcher. CERT and other similar organizations provide such a market. This market would not be attractive for discoverers who have already established themselves or who need money more than publicity. For some, the recognition received may eventually translate into economic opportunities.

2. Captive Market:

In this market the discoverers are captive to an organization and are thus not permitted to reveal the vulnerabilities externally. This includes vulnerability finders working within a software development organization or those working for them under contracts. Researchers within security service organizations are also, in effect, captive. In some countries the government may be the only permitted buyer, although in that case the government is free to use the vulnerability based on its national priorities.

3. Vulnerability Rewards by Vendors:

The reward programs offered by software venders are a good option for vulnerability discoverers who can sell their finding to the venders directly in an easy, legitimate way. The reward offered for a vulnerability can be significant, although modest in most cases. In addition, the discoverers receive appropriate credit [23].

Rewarding security researchers and others who make software products more secure is important. Providing rewards to motivate people to find software defects or weaknesses

before they are exploited by black hat exploiters is critical to improving computer security.

TABLE II
PRICE LIST FOR ZERO-DAY VULNERABILITY EXPLOITS

Products	Minimum price for zero-day exploits "2011"	Minimum price for zero-day exploits "2013"
ADOBE READER	$5,000 - $30,000	N/A
MAC OSX	$20,000 - $50,000	N/A
ANDROID	$30,000 - $60,000	$100,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000 - $100,000	N/A
MICROSOFT WORD	$50,000 - $100,000	N/A
WINDOWS	$60,000 - $120,000	$40,000 - $250,000
FIREFOX OR SAFARI	$60,000 - $150,000	N/A
CHROME OR INTERNET EXPLORER	$80,000 - $200,000	$200,000 - $500,000
IOS	$100,000 - $250,000	$50,000 - $200,000

There are only a few current vulnerability reward programs, and most of them were created a few years ago. The idea of reward programs is still quite new, and needs more development and improvement.

The current reward programs include these listed below. The key information about them is provided in Table I:

- Vulnerability Reward Program for Google web properties [24]: This program was created in November 2010. People who discover one of five types of vulnerabilities, such as remote code execution, SQL injection, and other common web flaws, are rewarded $100 to $20,000. The number of discoverers who have received approval from the reward panel has ranged between 53 winners in the fourth quarter of 2010 to 39 winners in the fourth quarter of 2012.
- Chrome Vulnerability Reward Program (Chromium Security Reward) [25]: All vulnerabilities are considered in this program, provided the vulnerability is identified as being of sufficiently high severity. The rewards range from $500 to $10,000 and up.
- The Mozilla Security Bug Bounty Program [26]: The rewards range from $500 to $3,000 depending on the severity rating of the vulnerability, and the reward includes a Mozilla t-shirt.
- Facebook [27]: This program is similar to most other reward programs. It offers a bounty for certain qualifying security bugs. The reward has a minimum of $500 with no specified maximum, and is based on severity and creativity.
- WordPress Security Bug Bounty Program [28]: This program has two different bounties: one for WordPress and another for WordPress Plugins. The minimum reward is $25, and the maximum reward is $1,000.
- CCBill Vulnerability Reward Program [29]: CCBill is an Internet billing service. The rewards range from $300 to $500, depending on the types of vulnerabilities found, such as SQL Injection, DoS, and persistent XSS.This program has been temporarily placed on hold due to corrections needed in the reported bugs.

Eventually, Microsoft has announced last June 2013 a month-long vulnerability rewards programs for the Internet Explorer (IE11) developer preview [30]. Microsoft was not interested in paying rewards programs since it does use outside consultant organizations to test their software on a contract basis, however [31].

4. Rewards by Security Service Companies:

Some companies that provide security services also acquire vulnerabilities. The vulnerabilities acquired are used to provide a higher degree of safety to their security customers, and may be provided to the software developer using a suitable compensation mechanism. These organizations do not sell the vulnerabilities to others. For example, Microsoft patched at least 17 vulnerabilities reported by the two programs in 2006 [5]. There are some third-party security companies that buy the vulnerabilities and sell them to software makers or vendors such as ZDI and iDefense [32]. Such reward programs include the following:

- Secunia Vulnerability Coordination Reward Program (SVCRP) [33]: There are two special awards: most valued contributor and most interesting coordination report.
- ZDI Rewards Program [34]: The Zero Day Initiative (ZDI) provides reward points each time a vulnerability submission is purchased. These points determine the ZDI status, which are bronze, silver, gold, platinum, and diamond. The rewards range from $1,000 to $25,000.
- iDefense Vulnerability Contributor Program: This is one of the oldest reward programs, and a few top discoverers mention working with iDefense. Detailed reward information is not available.

The security service companies may have their own internal vulnerability researchers. Their discoveries primarily serve to promote the organization.

B. Vulnerability Brokers

As opposed to the security services companies, vulnerability brokers buy as well as sell vulnerabilities. They come closest to an open market, since buyers and sellers can negotiate their prices [35], [36]. It is considered a legitimate, but only partially regulated, market that has some general rules. A vulnerability broker is an organization or person who provides a link between a vulnerability discoverer and the highest bidder. It has been reported that the commission might reach up to 15% of the selling price [32]. Therefore, the broker may sell that information to the software venders or to some government organization, depending on who can pay more.

Several international government organizations are said to have become significant buyers [20] in recent years, but their policies are not generally disclosed.

TABLE III
VULNERABILITY DISCOVERERS FROM JULY 1, 2012 TO DECEMBER 31, 2012: INSIDERS OR OUTSIDERS

Discoverers	Vulnerabilities of Safari	Percentage	Vulnerabilities of Chromium	Percentage
PRODUCT'S COMPANY DISCOVERERS	17	20%	0	0%
PRODUCT'S COMPANY DISCOVERERS AND OTHERS	0	0%	35	35%
OUTSIDE DISCOVERERS	66	80%	63	64%
UNKNOWN DISCOVERERS	0	0%	1	1%

Vupen, located in France, is an example. They can sell vulnerabilities to a government, provided that the government belongs to NATO, ANZUS, or ASEAN alliances [32]. If the software venders buy the vulnerability information, they will use it to patch their products, but if it is purchased by a government agency [37], they might use it for military purposes, to inflict damage to an opponent as a cyber-weapon, or to collect sensitive information (espionage) from opposing governments or organizations. Security experts have claimed that the Stuxnet malware was specifically created by government agencies in the United States and Israel to attack Iran's nuclear facilities in 2010 [38]. We can regard the vulnerability brokers to be a gray market, which can be legitimate from the point of view of national priorities. However, considering the amount of funding that governments can bring to the table, such markets will reduce the number of public disclosures [39]. "The Grugq" a Bangkok-based security researcher, is regarded as an influential global vulnerability broker. He arranges deals between vulnerability discoverers and western government agencies for a 15% commission [6]. A vulnerability auction site WabiSabiLabi was active a few years ago [40].

C. Online Forums

Online forums exist where information about vulnerabilities and exploits can be exchanged. In some cases the exchange may not involve money—rather, the members (called hacktivists) have a special or private agenda to attack specific organizations. LulzSec was a famous hacktivist group that attacked several user accounts and websites in different countries in 2011. Anonymous is a loosely connected network of hacktivists located in different places that choose the same targets to attack. It is likely that such groups do not have access to zero-day vulnerabilities since they would be too valuable to reveal without any financial gain. It is likely that they rely on installations that have not yet applied the patches needed.

D. Vulnerability Black Market

The vulnerability black market is not a regulated market and it is not controlled by any laws. This market allows any groups or organizations such as cyber criminals, terrorists, or government agencies to buy vulnerabilities. The price paid to the vulnerability discoverers is said to be five to ten times the amount of the other vulnerability markets, depending on the attributes of the vulnerabilities [6]-[41]. The estimated price range given by some in-the-field experts for a zero-day exploit is given in Table II [20]-[22]. Many governmental and commercial organizations, such as the International Monetary Fund, Intel, the Indian Defense Ministry, and the Pacific Northwest National Laboratory, have suffered from the malicious attacks [42]. Government agencies in several countries have programs to develop new cyber weapons, and they may be significant players in the black market for zero-day vulnerabilities [43].

E. The Consumers of Zero-Day Vulnerabilities

Ultimately, the buyers of vulnerability information are either software developers who intend to eliminate the vulnerability by developing a patch, or an organization that intends to use it for purposes that would seem malicious to its opponents. When a government agency is a buyer, it can bring a substantial amount to money to the market that other buyers may be unable to match. This may raise the prices of the vulnerabilities and in turn encourage more experts to enter the profession of vulnerability discovery.

In the next section, we examine the vulnerability discoverers themselves, and what motivates them. The discussion relies on information about actual individual discoverers rather than abstract characterizations.

III. THE VULNERABILITY DISCOVERERS

The motivation for vulnerability discoverers has been considered briefly by researchers in the past [44], but has never been studied using actual data. The discovery and disclosure of vulnerabilities are processes that are significantly impacted by the economics involved [45]. A few researchers have considered theoretical modeling of the vulnerabilities market. This paper asks these questions: who are the actual vulnerability finders, and what motivates them?

Vulnerability discovery is done by either researchers affiliated with a major organization (and who generally follow proper disclosure policies) or by freelance researchers, who may sell their findings, either in the legitimate or in the gray or black markets.

Software development organizations such as Google or Microsoft have divisions dedicated to security-related work. They are responsible for the development of security patches. They also discover some of the vulnerabilities in their own products. However as Table III shows, a large fraction of the vulnerabilities, perhaps a majority of them, are discovered by outside discoverers. These external discoverers have their own motivation, which may be different from the motivation of those engaged in discovering vulnerabilities internally in a

software development organization. Many external discoverers are freelancers either working on their own or on contract basis. Some of the external discoverers are part of organizations that provide security services.

TABLE IV
THE TOP VULNERABILITIES DISCOVERERS ON OSVDB

Discoverer	Country	Period	# Vuln	# Vuln types	Why they're interested	Stopped/Continued
r0t	Latvia	2005-08-09 to2010-09-16	810	10	N/A	N/A
Janek Vind "waraxe"	Estonia	2003-08-08 to2013-03-21	319	8	Vulnerability website	N/A
Lostmon Lords	Spain	2004-06-20 to2009-08-15	279	8	Security Researcher	Worked until July 2012
rgod	Italy	2005-06-06 to2012-08-29	277	12	Hacker	Worked until Aug. 2012
Luigi Auriemma	Italy	2000-07-08 to2013-03-16	267	9	Hobby	N/A
Russ McRee	USA	2008-01-14 to 2012-03-02	237	4	Specialist in security	N/A
Aliaksandr Hartsuyeu	Lithuania	2005-12-28 to2011-02-03	229	6	Security Company	Still working 2012
James Bercegay	USA	2003-06-03 to2008-09-04	200	12	Web developer	Worked until 2011
Kacper	Poland	2006-05-12 to2007-08-10	199	3	N/A	N/A
luny	N/A	2006-05-18 to 2006-07-13	142	6	N/A	N/A
Diabolic Crab	N/A	2004-09-25 to 2005-07-12	140	6	N/A	N/A
JeiAr	USA	2003-05-29to 2004-05-04	120	7	Web developer	Worked until 2011
Tan Chew Keong	Singapore	2004-07-29 to 2009-09-28	102	9	Information Security Specialist	N/A
Stefan Esser	Germany	2000-11-09 to 2012-06-03	86	10	Security Consultant	Still do jailbreak until 2012
M.Hasran Addahroni	Indonesia	2006-02-09 to 2009-02-07	80	2	Security Gossiper&Bugs Hunter	N/A

A. Top Discoverers

To understand the vulnerability discovery process, we examine the records of the top vulnerability discoverers. Since each of them has successfully discovered a significant number of vulnerabilities, we can presume that they did not just get lucky—rather, they have a system that has been demonstrated to work. To find the top vulnerability discoverers, we obtained data from the OSVDB database(until May 2013).We identified the top fifteen vulnerability discoverers in the database who found the most vulnerabilities, as given in Table IV. The actual names are not identifiable in some cases; they are generally known by the login identifier that they use in their blogs. Table IV includes some of information about them obtained from blogs and discussion boards in addition to OSVDB. The top five discoverers in Table IV are:

- r0t: He is a Latvian associated with a group named Unsecured Systems [46]. He discovered 810 vulnerabilities between Aug. 9, 2005 and Sept. 16, 2010. No additional information about him could be located.
- Janek Vind or "waraxe": He runs an interactive software vulnerability and security website [47]. Janek is from Estonia and his collaborators are from Australia, Turkey, Argentina, and other countries. They discovered 319 vulnerabilities between Aug. 08, 2003 and Mar. 21, 2013.
- Lostmon Lords: He is a security researcher from Spain [48]. He discovered 279 vulnerabilities between June 20, 2004 and Aug. 15, 2009, as recorded by OSVDB. According to his blog [49], he continued to discover vulnerabilities from Nov. 2009 to July 2012, but apparently disclosed them in such a manner that he is not identified as the discoverer in OSVDB.
- rgod: He is Andrea Micalizzi from Catania, Italy. He was 36 years old when he died in 2006 [50]. However, one of his friends has continued to use the rgod login. Together, they discovered 277 vulnerabilities between June 6, 2005 and Aug. 29, 2012. According to rgod's website, rgod's friend is still discovering vulnerabilities but he is not identified as the creditee in OSVDB.
- Luigi Auriemma: He is from Milan, Italy [51]. He discovered 267 vulnerabilities between July 8, 2000 and Mar. 16, 2013.

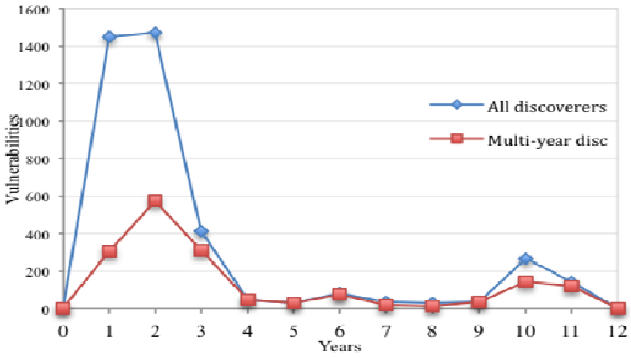

Fig. 2 Vulnerabilities discovered yearly

Fig. 2 gives a plot of the yearly discoveries of all of the top discoverers (line marked with a diamond). Year 1 corresponds to the first year of the discovery. Most of the top discoverers here are credited with discovering the vulnerabilities during the first three years (line marked with a rectangle). However, a few discoverers have continued to discover vulnerabilities for several years. This raises an intriguing question. Why do some very successful discoverers disappear from the scene after two to three years? A possible explanation is that, during those two to three years, they acquire the notoriety of being accomplished vulnerability discoverers. After that, they start offering their services to software developers or security service companies on a contract basis or as employees. Some of them may be able to start their own small organizations. In both cases, they are able to obtain steady and significant remuneration rather than a few rewards from the reward

programs. This is supported by the information that some of them have provided us, as discussed below.

TABLE V
TOP VULNERABILITY DISCOVERERS' ANSWERS TO SPECIFIC QUESTIONS ABOUT THEIR VULNERABILITY DISCOVERING AND REWARD PROGRAMS

Discoverer	Motivating Factors	Stop Discovering	Impact of Rewards Programs	Applying to Rewards Programs
DISCOVERER 1	Hobby and lifestyle choice	No	N/A	No
DISCOVERER 2	Make his website more popular	No	Limited impact	No
DISCOVERER 3	Curiosity	No. He has a company	Not much impact	ZDI and iDefense
DISCOVERER 4	Enjoyment	Yes. Not enough time	Mostly, yes	No
DISCOVERER 5	Fun, profit, auditing	No	Yes	ZDI and iDefense
DISCOVERER 6	Lean new discovering skills	No	Yes	All major programs
DISCOVERER 7	Enjoyment	No. Part of his job	Mostly, yes	Many programs
DISCOVERER 8	Passion, profit, learn new technologies	Yes. Not enough time	Yes	Many programs

Table IV illustrates the global distribution of vulnerability finders. A significant number of them are in eastern and western Europe, with a few in the Far East, in addition to some in the United States. This shows why the legal framework within a single country cannot regulate the vulnerability markets. Thus, while ideal vulnerability markets can be proposed, they cannot be implemented. Ultimately, economics will govern the markets.

B. Outsider and Insider Discoverers

One key question in understanding the vulnerability discovery process is whether a discoverer is part of the software product team or is an outsider. This will help us to understand what motivates discoverers to find and report software vulnerabilities. To address this question, we examined two well-known open-source software products (as example): Safari and Google Chromium (Table III). The period we investigated was from July 1, 2012 to December 31, 2012, and we used the OSVDB as the data source.

As shown in Table III, for these two products, the majority of the vulnerabilities discovered were found by outsiders. Finifter et al. [52] have also found this to be true for particularly for Google Chrome although not for Firefox. This demonstrates the importance of outsider discoverers and the potential significance of providing discoverers with more enticing vulnerability reward programs, or other forms of a legitimate market. It is definitely worth knowing what would motivate the discoverers to participate in such reward programs.

C. Direct Information

Some of the vulnerability markets are secretive, specifically the gray market, where the brokers serve as intermediaries, and the black market. They are, however, believed to be of great significance, and government agencies are emerging as vulnerability buyers. To understand the motivations and mechanics of different markets, we decided to directly contact the top discoverers of OSVDB to seek information. We were able to locate contact information for many of them. We then contacted them and asked some key questions, including the following:

1) What motivates you to discover software vulnerability?
2) How and when did you start?
3) What specific tools do you use for discovering vulnerability?
4) Did you stop working as a vulnerability discoverer? If so, when and why did that happen? If not, why not?
5) Do you think that vulnerability reward programs will help reduce black market transactions and encourage the use of legitimate markets? Please explain.
6) Did you apply to one of the current vulnerability reward programs, and if so, why?
7) If you have discovered a vulnerability, when would you consider selling your vulnerability to a broker? Please explain.
8) In your view, are there any specific steps that software developers or government agencies can do to reduce the security risk to society? Please explain.
9) Do you have any other comments?

Considering that freelance vulnerability discoverers can sometimes be secretive, we were pleasantly surprised when several of them actually responded; although most of them did not reply to us. The following section includes some of the answers to the above questions. To ensure their privacy, we have replaced the discoverers' names with aliases. Table V summarizes the responses.

- Discoverer 1: He uses his own tools, "specifically [his] hands and mind, in preference to automated tools". He has not sold a vulnerability in the past ten years. He does not find the reward program to be attractive. He never sold his own discovered vulnerability to brokers or any buyers, but he has sent vulnerabilities directly to the software venders.
- Discoverer 2: The main reason he became a vulnerability discoverer was that he wanted to promote his own website and his source code review service. He only uses his own tools, which are offered on his organization's website. He states that that vulnerability reward programs are of limited use, as the black markets offer more money. Like Discoverer 1, he does not apply for any reward programs.
- Discoverer 3: He started in 2002 while following Bugtraq and other mailing lists. He uses both public and proprietary tools to discover vulnerabilities. Although he now runs his own company, he still finds the time for discovery work. He states that reward programs pay very little for exclusive information and bug patches, which can be sold for much more on the black market. Nevertheless, he has submitted some vulnerabilities to the ZDI and iDefense reward programs in the past.

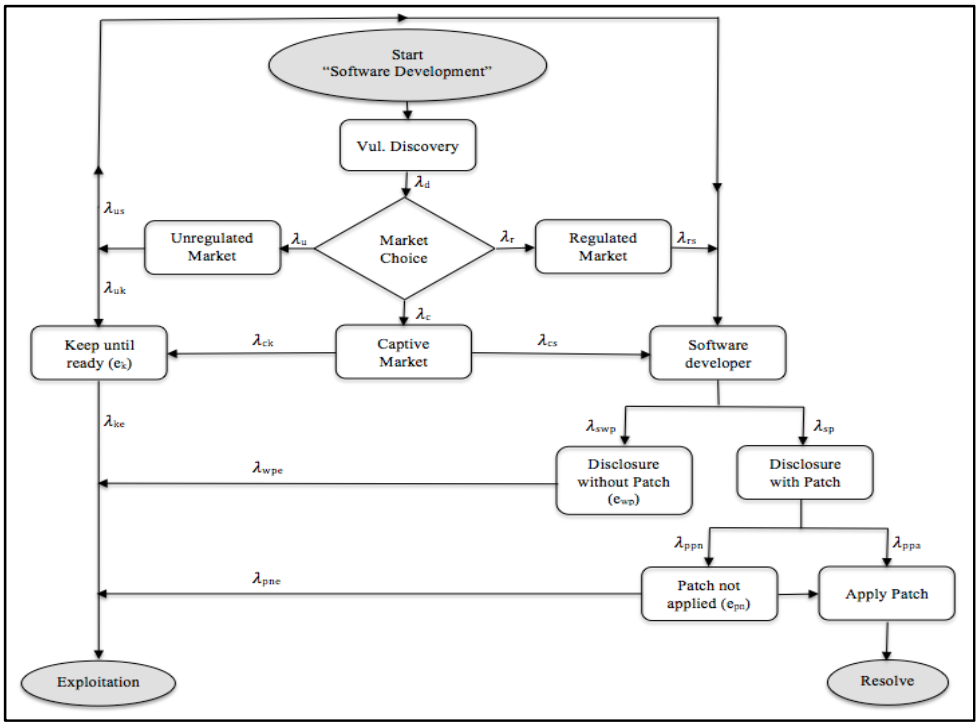

Fig. 3 Vulnerability flow through markets to zero-day exploitation or patching

- Discoverer 4: He started in 2008 and focuses entirely on web application security flaws, largely specific to free and open source applications. To discover vulnerabilities, he uses a combination of tools such as Burp Suite, OWASP ZAP, and a number of Firefox plugins (Tamper Data), as well as simple manual testing. He thinks that, for the most part, vulnerability reward programs will help to reduce black markets and encourage legitimate markets. He acknowledges that money is always a motivator and if vulnerability discoverers are paid well via the legitimate market, hopefully they will be less likely to sell the bug on the black market. He claims that he does not sell vulnerabilities. He always coordinates his findings with Secunia but does not take any further action regarding the vulnerability.
- Discoverer 5: He believes that the most profitable option for a vulnerability discoverer is to offer software security auditing services. His first discoveries were done between 1992 and 1993. The tools that he uses for discovering vulnerabilities are Notepad++ for PHP and other scripting languages, which allow him to search specific text strings through multiple files and color-coding. He also uses Apache/PHP/MySQL on his home PC, and all of his web application research is done using @localhost. Discoverer 5 usually works manually, without automatic vulnerability scanners. He believes that vulnerability reward programs will surely lessen damage, and is aware of hundreds of zero-day findings sold to ZDI and other vulnerability reward programs. He has worked with ZDI and iDefense because they pay for findings, arrange all communications with developers, and give him credit in the public advisory.
- Discoverer 6: He began to delve further into discovering after he did an interesting exercise during a computer security lab when he was a university student. He uses popular open-source tools, such as the ones distributed with Kali Linux, as well as his own scripts. He is still working in vulnerability discovering as a web application security pentester. He thinks that vulnerability rewards programs should be lucrative since pentesting requires a great deal of time, which results in a personal output of money and effort. Therefore, if one cannot earn money through legitimate channels, he will sell his discovered vulnerabilities on the black market. He is an active participant in all major bug bounty programs for two reasons: money and renown in the community. However, he claims that he himself has never considered selling the bugs he discovers to a broker.
- Discoverer 7: He began doing so in his early teens by finding security issues in the online games that he played. He used various intercepting proxy/tools for replaying requests, such as LiveHTTPHeaders or Burp Proxy, for vulnerability discovering. He is still involved in vulnerability discovering as a full-time employee on the Product Security team at Facebook. He has submitted issues to many of the bug bounty programs that currently exist; he believes that these programs are a great way to apply his skills and have his efforts rewarded and recognized. As a responsible vulnerability discoverer, he always tries to disclose an issue to the vendor before selling the vulnerability to a broker.

- Discoverer 8: He used HttpWatch and Burp Suite to capture the http traffic and did the rest of the work manually. He has taken a break from discovering vulnerabilities since he did not get enough time. He thinks that legal rewards programs offer white-hats good money, so there are fewer chances that white-hats will become black-hats. He has been participating in rewards programs for the past year and a half. He only reports vulnerabilities to vendors, and claims that he never thinks about selling vulnerabilities to brokers or anyone else. If a vendor does not respond properly, he discloses the vulnerability in a blog post, but he does not sell it. He believes that government agencies should support and encourage new rewards programs, such as HackerOne (a bug bounty program for the internet).

We note that many of the discoverers acknowledge the significance of the gray market and the black market in vulnerabilities. Many of them have found it profitable to engage in contract work after having established credentials as expert vulnerability finders.

Another notable observation from this study is the fact that the freelance discoverers appear to rely on their expertise more than on specific tools. Some of them have developed their own tools based on their experience. This suggests that the discovery of previously unknown vulnerabilities is a research activity requiring considerable technical skill, rather than something that can be completely automated using algorithmic methods. This should be contrasted with vulnerability scanning tools that look for known, i.e. already disclosed, vulnerabilities.

D. Study Limitations

There is not yet enough data to start development of key hypotheses regarding the mechanics of multiple vulnerability markets. Considering the nature of the field, it will not be possible in the near future to obtain representative samples. Here, we explore some potential limitations of this research due to the size of the sample and its potential bias.

Sample Size: We tried to analyze the OSVDB dataset to find the top discoverers there because other databases do not include the names of discoverers. Unfortunately, the OSVDB database is not available for direct analysis. We relied on some manual analysis in addition to their reports to identify a larger number of top discoverers. We thus left out the discoverers who have discovered only a small number of vulnerabilities. We attempted to locate the email addresses of the top discoverers on OSVDB and sent emails to the individuals. We were happy to note that several of the discoverers were willing to share information with us. It is unlikely that a significantly larger sample of top discoverers would be willing to participate in a study. We have also contacted some of the discoverers who have been active in several vulnerability rewards programs. Only three of them have responded so far.

Sample Bias: It is likely that those who responded to the questions were much more likely to be on the "white hat" side of the business. However, some of the respondents candidly acknowledged the lure of the black market, although none of them actually directly acknowledged having been a part of it. Innovative methods need to be developed that would allow researchers to better assess the black market in vulnerabilities.

E. Potential Impact of Money Flow

In the past few years, several government agencies associated with different countries have started investing in offensive and defensive capabilities for engaging in cyber warfare and espionage [20]. In comparison with conventional military hardware, the cyber capabilities are potentially much more cost-effective. Reports suggest that some vulnerabilities, along with their exploits, can bring a significant amount of money. This could cause a significant shift in the markets. As we discuss, it might lead software developers to be more aggressive in their reward programs.

IV. Vulnerability Markets and the Risks to Society

A few researchers have recently evaluated security risk based on the vulnerability life-cycle [53].However, they have not considered the impact of the vulnerability markets. Fig. 3 shows the vulnerability flow involving the markets.

As Fig. 3 shows, even disclosed vulnerabilities can be a source of risk. Some vulnerabilities can be disclosed without a patch either because of logistics reasons or because they are judged to be inconsequential (state e_{wp} Disclosure without Patch). When the patch is available, some users may not apply it, immediately leaving it in an exposed state (state e_{pn} Patch not Applied). Some of the conventional vulnerability scanning products offer protection against such states.

There is no protection against zero-day vulnerabilities, however, which have not been publically disclosed (state e_k Keep until Ready).We can note that the captive market has two options: sell the vulnerability to software developers or keep it until it can be used for an attack, for example. Even highly secured systems can be potentially exploited using the zero-day. They can be expensive to acquire, but can be used for cyber warfare, cyber terrorism, espionage, or an attack on vital institutions of an opposing nation.

Fig. 3 shows the three states e_k, e_{wp}, e_{pn}, in which the vulnerability is exposed. The risk due to an exploitation of a vulnerability during a time window (t1, t2) is given by [53] as in (1):

$$Risk(t_1,t_2) = \int_{t_1}^{t2} \sum_i P(e_i)\lambda_i \; dt.Exploitation\ impact \qquad (1)$$

where i is one of the one of the exposed states (e_k, e_{wp}, e_{pn}) and λ_i is the transition rate from that state to the exploitation state. $P(e_i)$ is the probability of being in the state e_i.

Note that a zero-day attack is only possible for a vulnerability passing through the unregulated markets, with the exception of a captive market (such as a defense lab) where the objective is to discover vulnerabilities for exploitation.

A significant fraction of the cyber-attacks on systems belonging to individuals or organizations occur though e_{wp}, $e_{pn.}$ An attack through e_{wp} is through a known risk, and one through e_{pn} could be considered a consequence of negligence. However, an attack through e_k would be completely

unexpected, and, depending on the target and the type of breach, can have devastating consequences on an organization or a society.

As we observe, a large fraction of successful vulnerability discoverers are from regions that are not as industrially developed. Some of these regions are also known for their sophisticated vulnerability exploiters [54]. This suggests that economics might play a significant role in potential approaches for keeping the society safe.

An attractive reward program based on vulnerability criticality can provide a significant alternative to the gray and the black markets. A few software developers and security organizations now run a small number of such programs. These programs ensure time for patch development before a disclosure. Some of the top discoverers that we contacted suggest that sometimes the reward programs do not pay enough, and a better reward may be obtained on the black market (although none of them admitted to selling any vulnerabilities in such a market.)

We note that after a few years of very successful vulnerability discovery, many of the top discoverers apparently disappear from the scene as credited discoverers. Some of them suggest that they find it more profitable to contract out their security auditing services to software developers. This can also significantly reduce the risk to the society.

Companies and organizations need to design attractive vulnerability reward programs for their products. This will allow the legitimate markets to compete with the black market.

Some reward programs, such as the one for Google Chrome, appear to have been successful. While the amount of money committed to the reward programs is only a tiny part of the company's revenues, Google is giving out some of the best monetary rewards.

A significant part of the global vulnerabilities market is quite opaque. Even the emerging legitimate markets have not been studied in detail, although some mathematical studies based on the classical market theories have appeared. There is a need to examine actual data and practices in order to understand the vulnerability discovery and disclosure.

The zero-day vulnerabilities with exploits are a serious issue. The number of high-profile attacks that use the zero-day has increased sharply during the first three months of 2013 [55], demonstrating the amount of risk associated with the unregulated markets [56]. Mechanisms need to be developed to make it more profitable for researchers to sell their discovered vulnerabilities in the legitimate markets, therefore reducing trading in the unregulated markets.

VI. Conclusion and Future Works

This paper has identified multiple vulnerability markets where the exchange between the discoverers and the buyers of the vulnerabilities takes place. We have examined the motivation and methods of vulnerability discoverers by studying the motivation and methods of discoverers. The most successful vulnerability discoverers are identified, and their motivation and techniques have been examined.

While vulnerability discoverers use some tools— including those that they have developed themselves—they rely on their expertise and insight to a considerable extent. It must be kept in mind that tools for finding known vulnerabilities are completely different, and are not of use for discovering new vulnerabilities.

We find that a large fraction of the discoverers are from outside of the software development organizations, and that their key motivation is a monetary reward. The vulnerabilities are disclosed in a proper and responsible way when they are traded though the legitimate markets. Reward programs and contract-based software review services are the major components of the legitimate markets. Organizations that act as vulnerability brokers may deal in either the legitimate or the black market. The vulnerability discoverers acknowledge that the black markets can often be attractive. Reports suggest that government agencies from different countries may make up an increasingly significant part of the black market buyers. This suggests a need for expanded and more attractive legitimate markets.

The research reported in this paper demonstrates the needs for further examination of the markets in more detail. There is a need to collect data about the transactions in the regulated and the unregulated markets so that the processes can be modeled accurately. Because this is a dynamically changing field, studies such as this need to be repeated in order to see if there are any observable trends in terms of the vulnerabilities that end up in the legitimate and black market periodically, and the subsequent risks to society.

Acknowledgment

We would like to thank all of the discoverers who chose to answer our questions. Their answers and comments have provided us with a much clearer understanding of the field. This work was partly supported by a scholarship from King AbdulAziz University in Saudi Arabia.

References

[1] C. P. Pfleeger and S. L Pfleeger. Security in Computing, 3rd ed. Prentice Hall PTR, 2003.
[2] O. H. Alhazmi and Y. K. Malaiya, "Application of Vulnerability Discovery Models to Major Operating Systems," IEEE Trans. Reliability, March 2008, pp. 14-22
[3] S.-W. Woo, H. Joh, O. H. Alhazmi and Y. K. Malaiya, "Modeling Vulnerability Discovery Process in Apache and IIS HTTP Servers", Computers & Security, January 2011, Pages 50-62.
[4] "Teen Exploits Three Zero-Day Vulns for $60K Win in Google Chrome Hack Contest | Threat Level | Wired.com," Threat Level. [Online]. Available: http://www.wired.com/threatlevel/2012/03/zero-days-for-chrome/. [Accessed: 06-Oct-2013].
[5] "Bug brokers offering higher bounties." [Online]. Available: http://www.securityfocus.com/news/11437. [Accessed: 06-Oct-2013].
[6] "Be a Millionaire: The Market for Zero-Day Software Exploits | Critical Start." [Online]. Available: http://www.criticalstart.com/2012/04/be-a-millionaire-the-market-for-zero-day-software-exploits/. [Accessed: 06-Oct-2013].
[7] R, Anderson, University of Cambridge, Home page. [Online]. Available: http://www.cl.cam.ac.uk/~rja14/ [Accessed: 06-Oct-2013].
[8] H.-C. Joh and Y. K. Malaiya, "Seasonal variation in the vulnerability discovery process," in Software Testing Verification and Validation, 2009. ICST'09. International Conference on, 2009, pp. 191–200.

[9] Karthik Kannan and Rahul Telang, Market for Software Vulnerabilities? Think Again, Management Science, Vol. 51, No. 5 (May, 2005), pp. 726-740.
[10] "White hat," Search security. [Online]. Available: http://searchsecurity.techtarget.com/definition/white-hat [Accessed: 06-Oct-2013].
[11] "HacK, CouNterHaCk | New York Times Magazine," [Online]. Available: http://www.nytimes.com/library/magazine/home/19991003mag-hackers.html. [Accessed: 06-Oct-2013].
[12] C. Miller, "The legitimate vulnerability market: the secretive world of 0-day exploit sales," in Workshop on the Economics of Information Security (WEIS), 2007, pp. 7–8.
[13] D. McKinney, "Vulnerability Bazaar," IEEE Security Privacy, vol. 5, no. 6, pp. 69–73, 2007.
[14] Andy Greenberg, Meet The Hackers Who Sell Spies The Tools To Crack Your PC, Forbes, March 21, 2012, bit.ly/11cbLC6
[15] M. Shahzad, M. Z. Shafiq, and A. X. Liu, "A large scale exploratory analysis of software vulnerability life cycles," in 2012 34th International Conference on Software Engineering (ICSE), 2012, pp. 771–781.
[16] The Open Source Vulnerability Database. [Online]. Available: http://www.osvdb.org. [Accessed: 06-Oct-2013].
[17] Arora, A.; Rahul Telang, "Economics of software vulnerability disclosure," Security & Privacy, IEEE, vol.3, no.1, pp.20, 25, Jan.-Feb. 2005.
[18] R. Böhme, "Vulnerability markets," Proc. of 22C3, vol. 27, p. 30, 2005.
[19] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in 11th Workshop on the Economics of Information Security, 2012.
[20] "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits - Forbes," Forbes. [Online]. Available: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/. [Accessed: 06-Oct-2013].
[21] "Google throws stacks of cash at hackers to publicly crack its Chrome browser," VentureBeat. [Online]. Available: http://venturebeat.com/2012/03/08/hackers-crack-chrome-in-publi/. [Accessed: 06-Oct-2013].
[22] "Cyber-security: The digital arms trade | The Economist." [Online]. Available: http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade. [Accessed: 06-Oct-2013].
[23] A. Ozment, "Bug auctions: Vulnerability markets reconsidered," in Third Workshop on the Economics of Information Security, 2004.
[24] Vulnerability Reward Program for Google web properties. [Online]. Available: http://www.google.com/about/appsecurity/reward-program/. [Accessed: 21-Jan-2014].
[25] Chrome Vulnerability Rewards Program. [Online]. Available: http://www.chromium.org/Home/chromium-security/vulnerability-rewards-program. [Accessed: 21-Jan-2014].
[26] The Mozilla Security Bug Bounty Program. [Online]. Available: http://www.mozilla.org/security/bug-bounty.html. [Accessed: 21-Jan-2014].
[27] Facebook rewards program. [Online]. Available: https://www.facebook.com/whitehat/bounty/. [Accessed: 21-Jan-2014].
[28] Wordpress rewards program. [Online]. Available: http://www.whitefirdesign.com/about/wordpress-security-bug-bounty-program.html. [Accessed: 06-Oct-2013].
[29] CCBill Vulnerability Reward Program. [Online]. Available: http://www.ccbill.com/developers/security/vulnerability-reward-program.php. [Accessed: 21-Jan-2014].
[30] Microsoft Bounty Programs. [Online]. Available: http://technet.microsoft.com/en-US/security/dn425036. [Accessed: 21-Jan-2014].
[31] "Microsoft Says No to Paying Bug Bounties," *Threatpost*. [Online]. Available: http://threatpost.com/microsoft-says-no-paying-bug-bounties-072210/. [Accessed: 06-Oct-2013].
[32] "The Shadowy World Of Selling Software Bugs - And How It Makes Us All Less Safe," ReadWrite. [Online]. Available: http://readwrite.com/2012/10/04/the-shadowy-world-of-selling-software-bugs-and-how-it-makes-us-all-less-safe. [Accessed: 06-Oct-2013].
[33] Secunia Vulnerability Coordination Reward Program (SVCRP). [Online]. Available: http://secunia.com/community/research/svcrp/. [Accessed: 21-Jan-2014].
[34] ZDI Rewards Program. [Online]. Available: http://www.zerodayinitiative.com/about/benefits/. [Accessed: 21-Jan-2014].
[35] Ryan Gallagher, "Cyberwar's Gray Market- Should the secretive hacker zero-day exploit market be regulated?" Slate, Jan. 16, 2013.
[36] Michael Riley and Ashlee Vance "Cyber Weapons: The New Arms Race" BloomsbergBusinessWeek, July 20, 2011.
[37] "Schneier on Security: The Vulnerabilities Market and the Future of Security." [Online]. Available: https://www.schneier.com/blog/archives/2012/06/the_vulnerabili.html. [Accessed: 06-Oct-2013].
[38] "Stuxnet was work of U.S. and Israeli experts, officials say - The Washington Post." [Online]. Available: http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. [Accessed: 06-Oct-2013].
[39] "Black hat greed reducing software vulnerability report rate • The Register." [Online]. Available: http://www.theregister.co.uk/2013/02/26/grey_market_cuts_vulnerability_reporting/. [Accessed: 06-Oct-2013].
[40] "WabiSabiLabi may close 0day auction site." [Online]. Available: http://www.networkworld.com/news/2008/103008-wabisabilabi-may-close-0day-auction.html. [Accessed: 06-Oct-2013].
[41] S. Ransbotham, S. Mitra, and J. Ramsey, "Are markets for vulnerabilities effective?," MIS Quarterly-Management Information Systems, vol. 36, no. 1, p. 43, 2012.
[42] "Cyber Weapons: The New Arms Race - Businessweek." [Online]. Available: http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html. [Accessed: 06-Oct-2013].
[43] "Welcome to the Malware-Industrial Complex | MIT Technology Review." [Online]. Available: http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/. [Accessed: 06-Oct-2013].
[44] Alhazmi, O.H.; Malaiya, Y.K., "Quantitative vulnerability assessment of systems software," Reliability and Maintainability Symposium, 2005. Proceedings. Annual, vol., no., pp.615, 620, Jan. 24-27, 2005.
[45] Ross Anderson and Tyler Moore, The Economics of Information Security, Science, 27 October 2006: 314 (5799), 610-613.
[46] Blog of r0t. [Online]. Available: http://pridels-team.blogspot.com. [Accessed: 06-Oct-2013].
[47] main website of Janek Vind "waraxe". [Online]. Available: http://www.waraxe.us. [Accessed: 06-Oct-2013].
[48] Facebook's account of Lostmon. [Online]. Available: https://www.facebook.com/lostmon. [Accessed: 06-Oct-2013].
[49] Blog of Lostmon Lords. [Online]. Available: http://lostmon.blogspot.com. [Accessed: 06-Oct-2013].
[50] Personal website of rgod. [Online]. Available: http://retrogod.altervista.org. [Accessed: 06-Oct-2013].
[51] Personal website of Luigi Auriemma. [Online]. Available: http://aluigi.altervista.org. [Accessed: 06-Oct-2013].
[52] Finifter, Matthew,Devdatta Akhawe, and David Wagner." An empirical study of vulnerability rewards programs."In USENIX Security.2013, 273-288
[53] H. Joh and Y. K. Malaiya, "Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics," SAM'11, The 2011 International Conference on Security and Management, pp.10-16, 2011.
[54] Report: Eastern European Hackers More Sophisticated Than Asian Counterparts. [Online]. Available: http://blogs.wsj.com/digits/2012/09/18/report-eastern-european-hackers-more-sophisticated-than-asian-counterparts/. [Accessed: 06-Oct-2013].
[55] "GCHQ Establishes Cyber Unit to Detect Software Vulnerabilities - IBTimes UK." [Online]. Available: http://www.ibtimes.co.uk/articles/448951/20130321/gchq-establishes-cyber-research-unit-search-software.htm. [Accessed: 06-Oct-2013].
[56] L. Allodi, W. Shim, and F. Massacci, "Quantitative assessment of risk reduction with cybercrime black market monitoring". The 2013 IEEE Security and Privacy Workshops, pp. 165-172, 2013.