ANALYST BRIEF – December 2013

International Vulnerability Purchase Program

WHY BUYING ALL VULNERABILITIES ABOVE BLACK MARKET PRICES IS ECONOMICALLY SOUND

Authors – Stefan Frei, PhD; Francisco Artes

Overview

Over the past few decades, the global economy increasingly has come to rely on information systems, and yet society remains in the early phases of adapting to the related opportunities and threats. Criminals, however, are fast adopters (as with any new technology), and worldwide financial losses occurring as a result of cyber crime are estimated in the billions of dollars per year. The continued discovery of new vulnerabilities in software and their subsequent abuse by cyber criminals is the root cause of a considerable portion of the losses experienced by society. Every exploitable security vulnerability in the possession of cyber criminals (particularly those vulnerabilities that affect popular products) subsequently induces significant direct and indirect losses for users and for society as a whole.

There is no indication that the status quo will change any time soon, not least because software manufacturers have yet to produce secure software and, since they do not bear the costs and consequences of the vulnerabilities within their products, there is little to indicate that they ever will. Experience has shown that traditional approaches based on *"more of the same"* do not deliver better overall security. The question to ask is: *"How much are those that bear the costs willing to pay to reduce their losses incurred as a result of cyber crime?"*

It is time to examine the economics of depriving cyber criminals' access to new vulnerabilities through the systematic purchase of *all* vulnerabilities discovered *at or above* black market prices. By comparing the total losses occurring as a result of cyber crime against the costs involved in purchasing all vulnerabilities a compelling case is made for a centralized vulnerability purchase program.

NSS Labs has discovered that the cost of purchasing all of the vulnerabilities of a given software vendor is minimal when compared with that vendor's revenue for the same period of time. Further, the cost of purchasing all of the vulnerabilities for all of the vendors is minimal when weighed against the expected overall reduction in losses incurred as a result of cyber crime. NSS' data reveals that it is economically viable for governments to make large-scale purchases of vulnerabilities to reduce losses, establish proper incentives, provide transparency, and transfer costs to the appropriate parties

NSS Labs Findings

- Either it is fundamentally impossible to produce secure code, or skewed incentives within the industry have resulted in insufficient investment in the production of secure software. Traditional approaches based on *"more of the same"* cannot deliver better overall security.
- The discovery and subsequent disclosure of vulnerabilities by external researchers cannot be prevented.
- Brokers and commercial players increasingly are purchasing vulnerabilities or offering zero-day exploits to their subscribers, and these typically are used for criminal operations or cyber espionage
- Security depends largely on ethical researchers reporting vulnerabilities under the practices of coordinated disclosure. At the same time, the black market is expanding rapidly and offering large rewards for the same information.
- The cost of purchasing all vulnerabilities for all products is considerably lower than the savings that would occur as a result of the expected reduction in losses occurring as a result of cyber crime, even under the conservative estimate that these losses would be reduced by only 10 percent.
- If all of the vulnerabilities for all products are purchased at USD $150,000 each, this still would amount to less than 0.01 percent of the yearly gross domestic product (GDP) for either the US or the European Union (EU).
- The cost for major software vendors to purchase all of their vulnerabilities at USD $150,000 each is less than one percent of their revenue.
- A proposed international vulnerability purchase program (IVPP), whereby all relevant vulnerabilities are purchased, is an economically sound proposal to reduce losses that occur as a result of cyber crime.

NSS Labs Recommendations

- The industry as a whole needs to assess current trends and possible nontechnical solutions, and evaluate new approaches to handling vulnerabilities – failing to take action is not an option.
- Software vendors should run bug bounty programs with *competitive* rewards for vulnerabilities found.
- Governments must evaluate the idea of an international vulnerability purchase program (IVPP) that could reduce losses occurring as a result of cyber crime, and they should establish incentives for the creation of more secure software.
- Governments and the industry as a whole should aim to assign the liability or costs of purchasing vulnerabilities to the parties that are best equipped to manage the risk.
- All software vendors must establish a process for coordinated disclosure of vulnerabilities and communication with researchers.
- Software vendors must invest in mechanisms that allow for the simple, automatic patching of their installed products.

Table of Contents

Overview 1

NSS Labs Findings 2

NSS Labs Recommendations 2

Analysis 4

The Key Role Of Security Vulnerabilities 4

Cyber Criminals Need Vulnerabilities 4

Vulnerability Handling And Exploit Markets 6

Vulnerabilities Are Here To Stay 8

Economics Of Purchasing Vulnerabilities 9

Economic Incentives In Cyber Security 9

Current State 10

International Vulnerability Purchase Program (IVPP) 12

Cost Analysis 12

Operational Benefits 13

Price Dynamics 13

Higher Rewards Lead To More Vulnerabilities Discovered 14

Transparency And Reduced Exposure Time 14

Single Point of Contact 14

Organizational Structure of IVPP 15

Financing The Purchase Program 15

Software Vendors Purchasing Their Vulnerabilities 16

Appendix 17

Organizational Structure Of An IVPP 17

Local Submission Center 18

Submission Qualification Center 18

Transparent Documentation 18

Bounty Programs And Competitions 18

Acknowledgment 19

Reading List 19

Contact Information 20

Analysis

Over the past two decades, it has become apparent that:

A. The industry has been unable to produce universally secure software.
B. The discovery and disclosure of vulnerabilities by third/external parties cannot be prevented or suppressed.
C. Economic and intellectual property losses occurring as a result of cyber crime have soared.
D. *"More of the same"* approaches to security, be they traditional or purely technical, cannot remediate the problem.

Economic and other nontechnical incentives increasingly are considered the primary reasons for today's heightened risk exposure. An overarching vulnerability purchase program (for example, purchasing *all* vulnerabilities affecting products from *all* software vendors at *competitive* prices) could:

A. Reduce the number of vulnerabilities available for abuse, and thus reduce the overall losses incurred by society as a result of cyber crime
B. Instill incentives that proactively improve security
C. Employ transparency to improve software security
D. Assign liability to the party that can best manage the risk

It is quantifiably demonstrated that purchasing all vulnerabilities at competitive prices is economically viable when juxtaposed against the revenue of the software industry or the resulting reduction in total losses occurring as a result of cyber crime. A solution is proposed (supported by data), by which current unsolved challenges in cyber security may be addressed.

The Key Role Of Security Vulnerabilities

Cyber Criminals Need Vulnerabilities

Cyber criminals depend on software vulnerabilities for operations such as breaking into systems, stealing personal information, or building botnets. Systems targeted by cyber criminals are exploited either directly or via social engineering, whereby a user is tricked into opening an infected document or visiting an infected website in order to compromise the endpoint.

Further, zero-day exploits based on privileged information about security vulnerabilities, or the *"the known unknowns,"* leave users and society in general at risk for extended periods of time.[1] Knowledge of security vulnerabilities is the primary enabler for most cyber crime activities and directly drives the cost of losses incurred as a result of cyber crime.

Below are some of the most prevalent abuse scenarios that are enabled by security vulnerabilities. Reducing the number of vulnerabilities available for exploitation would substantially impair these operations and thus reduce losses incurred as a result of cyber crime.

[1] "*The Known Unknowns In Security*" - https://nsslabs.com/reports/known-unknowns-0

Direct Attack	Exploitable vulnerabilities allow for direct attacks on systems. Systems with permanent access to the Internet, such as servers, networking equipment, or SCADA systems are highly exposed.
Indirect Attack	Endpoints that are on internal networks or that have no permanent connection to the Internet are attacked through infected documents that are opened on a susceptible endpoint or mobile device. Systems or storage devices that are already infected further compromise internal systems when they are connected to internal or private networks/environments.
Social Engineering Attack	Socially engineered malware tricks users into opening or accessing infected documents that they otherwise would not access.
Targeted Attack	Publicly unknown vulnerabilities and derived exploits (zero-day exploits) are the perfect tools for targeted attacks against well-protected, high-value targets. These are often delivered via social engineering. Selectively using an exploit against just a few targets allows for stealthy operations over extended periods of time.
Opportunistic Attack	Fully automated attacks against prevalent software allow for the opportunistic compromise of a large number of susceptible systems in a short time. These are often, although not exclusively, the province of the unskilled attacker.
Staged Attack	While the individual victim of an attack may be of little value, it immediately becomes the staging point for further attacks. For example, a system becomes part of a botnet, which is used to launch and facilitate attacks against further external and internal systems to create leverage for the attacker. By unwittingly acting as a staging point for further attacks, the victim becomes more valuable.
Reinfection/Persistence	A continuous feed of new vulnerabilities allows for the reinfection of previously compromised and cleaned systems, or multiple infections of the same target. The compromises persist, and the victims find themselves in a permanent arms race.

Without knowledge of a critical vulnerability, the operator of a targeted system cannot assess the risk or take remediating action, which results in extended exposure times. Further, the vendor of the affected software cannot release a patch to render systems immune against the vulnerability.

In fact, Symantec found the average zero-day attack persists for almost a full year – 312 days – before it is detected.[2] The McAfee report *"The Economic Impact of Cyber Crime and Cyber Espionage"* discusses the different types of losses.[3]

Security technologies such as firewalls, intrusion prevention systems (IPS), and endpoint protection (EPP), are notoriously ineffective in protecting against unknown attacks.[4]

Cyber crime operations result in collateral losses that are independently estimated to be in the tens to hundreds of billons per year globally.[3] A significant portion of these losses is directly or indirectly related to the criminal exploitation of security vulnerabilities.

Vulnerability Handling And Exploit Markets

The market for information about security vulnerabilities has become more lucrative as society's reliance on information technology has increased, and it is not uncommon for ethical security researchers to demand compensation for time spent uncovering vulnerabilities. Coordinated disclosure, which is the process by which researchers privately report findings to an affected vendor in order for the vendor to produce a security patch, fails to satisfy security researchers who expect financial compensation. On the other hand, cyber criminals or government agencies that are not bound by legal or ethical considerations are willing to invest heavily in acquiring valuable vulnerability information.[1]

The way in which information about a new vulnerability is managed is a direct function of the incentives and ethics of the discoverer. Once a vulnerability is discovered, the following options are available:

Do Nothing	The finder does nothing under the assumption that this is the best way to serve security; this assumption is incorrect, however, because there is no guarantee that other parties have not already discovered the same vulnerability. The likelihood of independent discovery of the same vulnerability by third parties increases with time.
Coordinated Disclosure	The finder privately discloses newly discovered vulnerabilities either to the vendor of the affected product, or to a national CERT program, or other vulnerability program coordinator. The finder gives the vendor opportunity to analyze the vulnerability and provide an update before disclosing detailed information to the public. Upon release of an update, the vendor recognizes the finder's contribution in bulletins or advisories.

[2] *"Zero-Day World"* - http://www.symantec.com/connect/blogs/zero-day-world

[3] *"The Economic Impact of Cyber Crime and Cyber Espionage,"* McAfee - http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

[4] *"Correlation Of Detection Failures"* - https://www.nsslabs.com/reports/correlation-detection-failures

Full Disclosure	The finder provides instant, full disclosure of vulnerability information to all affected parties, including potential attackers. While coordinated disclosure is more desirable from the security perspective, the threat of full disclosure helps to motivate software vendors that are not responsive or that fail to act on information about vulnerabilities in their products. Further, full disclosure is a viable option for vulnerabilities discovered in software that is no longer supported by a vendor, or where the vendor no longer exists.
Bug Bounties, ***Selling Information***	The finder sells the information, either directly or through a broker. Typical buyers include: • *Cyber criminals* who will use the information for attacks. • *Security companies* that will coordinate with affected vendors (while providing "ahead of the threat" protection in their products). • *Government agencies* that use the information to protect their countries or to attack other countries. • An increasing number of *software vendors* offer bounties in exchange for reporting product vulnerabilities directly to them. • An increasing number of *specialized companies* research vulnerabilities with the sole purpose of selling them or their derived exploits to subscribers and other interested parties.

Each of these options will affect differently the losses borne by society. Clearly, there are a number of ways for vulnerability information to be made available only to privileged groups (excluding the vendor of the affected software) for abuse, possibly over extended periods of time. While a market for vulnerabilities has developed, the commercialization of vulnerabilities remains a contentious issue that is linked to the concept of responsible disclosure of vulnerabilities. Today, vulnerability information traded on the black market is available through commercial service offerings and through brokers.

Vulnerability markets attract a considerable share of all discovered vulnerabilities that affect major vendors. The long-standing Vulnerability Contributor Program (VCP) of iDefense and the Zero Day Initiative (ZDI) of HP TippingPoint have jointly purchased an average of 17 percent of all vulnerabilities affecting major software vendors (for example, 14 percent of Microsoft, 17 percent of Adobe, 18 percent of Symantec, 10 percent of Oracle vulnerabilities). This in spite of these programs offering prices considerably lower than those offered on the black market.

There are an increasing number of commercial players offering zero-day exploits to their subscribers. Such groups do not reveal their clients, but big buyers reportedly include government agencies. Endgame Systems, for example, offered subscribers 25 zero-day exploits per year for USD $2.5 million, according to its February 2010 price list.[5] The price typically falls between USD $40,000 and USD $160,000.

[5] "*Cyber Weapons: The New Arms Race,"* http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html

Although some firms restrict their clientele, either based on country of origin or on decisions to sell to specific governments only, the ability to bypass this restriction through proxies seems entirely possible for determined cyber criminals. Based on service brochures and public reports, these providers can deliver at least 100 exclusive exploits per year. [1]

Vulnerabilities Are Here To Stay

Software vendors have responded by investing considerably in the security of their products. However, despite their "best" efforts over the past decade, they have been unable to solve the problem, as shown in Figure 1.

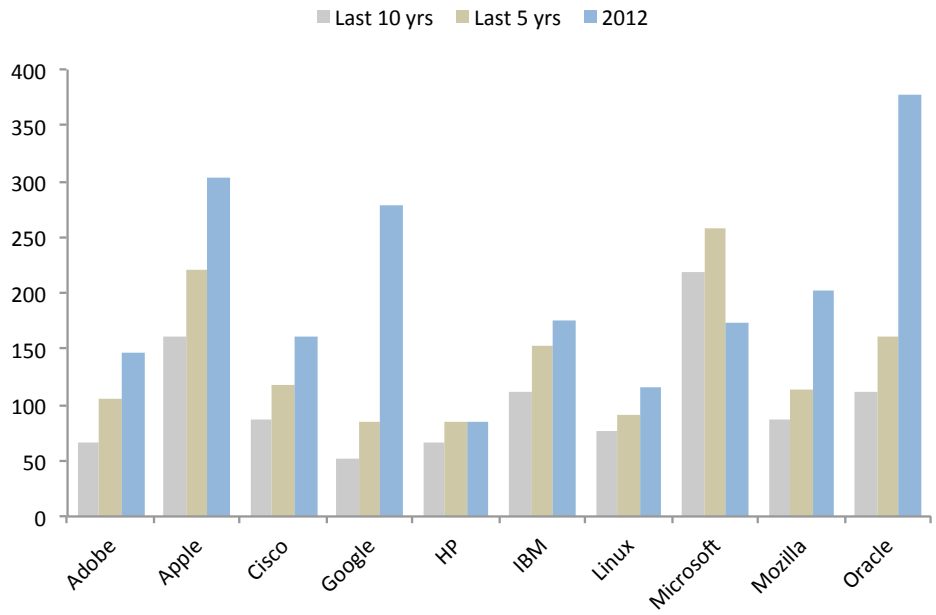

Figure 1 – 2012 Published Vulnerabilities Compared To Averages Of Past 5 Years And Past 10 Years (Oracle Includes Sun)

Software vendors typically find and remediate many vulnerabilities during the software development and testing phase, but it is the exploitation of those vulnerabilities discovered after the release of a product that account for the greatest losses. Typically, these are found not by the vendor but by external individuals and organizations, including cyber criminals. While the successful exploitation of vulnerabilities has become more difficult over time, criminals continue to bypass anti-exploitation techniques, as evidenced by the expanding market for fully weaponized exploits.

No matter how large a vendors' security team, it cannot compete with the combined experiences of a global group of individual specialists or organizations with diverse backgrounds, education, culture, and skills. Finding vulnerabilities is a complex endeavor, and the diverse experiences of problem solvers often yield better results than expert or inside knowledge alone.[6] The discovery of vulnerabilities by third parties is unavoidable; the number of software vendors that offer bounties for researchers that submit their findings attests to this. This year

[6] "*The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies,"* Scott E. Page http://press.princeton.edu/titles/8353.html

in particular has seen the emergence of multiple new bug bounty programs, and a recent study reveals that such programs are more economically efficient than hiring full-time security researchers to locate bugs internally.[7] However, the reward offered by software vendors is typically considerably below that which is offered on the black market.

In short, vulnerabilities, which are a critical component for cyber criminals, are in plentiful supply and readily available though external research or on the market. The abuse of these vulnerabilities by cyber criminals induces losses that are estimated in the tens to hundreds of billions of dollars per year.

Economics Of Purchasing Vulnerabilities

Economic Incentives In Cyber Security

Many of the problems in security can be explained using terms typically found in the language of economics: *asymmetric information, network externalities*, and *liability dumping*. [8]

Information Asymmetry	A software vendor has better information on the security of its products (security of design, process for handling vulnerabilities, vulnerabilities found internally, and time to release a patch) than does the user. Users therefore do not have sufficient information to accurately assess the true security of software.
Negative Externality, Liability Dumping	Information security is similar to environmental pollution in that vendors of insecure software do not bear the consequences of their actions. Vulnerabilities in software impose costs on users and on society as a whole, while software vendors internalize profits and externalize costs. Profit-driven businesses do not invest in eliminating negative externalities.
Network Effect	The software industry tends toward dominant firms, largely because of the benefits of interoperability. A larger network, user base, or dominant platform/protocol/format increases the value of the software or service for its members. Thus, time to market and the ability to quickly build a large user base is more important than shipping secure products. More so in light of information asymmetry, where the security of the product or service is not recognizable to the user.
Norms	A norm is a behavioral regulatory in a group. Today it is the norm to tolerate vulnerable software. Buyers are trapped in a suboptimal norm (Nash equilibrium of a game), which ensures that they will continue to demand insecure software.

[7] *"An Empirical Study of Vulnerability Reward Programs,"* http://www.cs.berkeley.edu/~devdatta/papers/vrp-paper.pdf

[8] *"Information Security Economics – and Beyond,"* R. Anderson, T. Moore - http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf

Today, there is no legal liability for the quality of software, and this is unlikely to change anytime soon. Software manufacturers simply do not bear the costs and consequences of vulnerabilities in their products, even though legal theorists have long stated that liability should be assigned to the party that can best manage the risk. Purely technical approaches have proved unable to solve the current security challenges.

The current approaches to address the risks of insecure software and its exploitation are as follows:

Action	Actor
Production of secure software with less vulnerabilities *The industry remains unable or unwilling to release secure software*	Only the vendor can do this
Exploit mitigation techniques *Renders some vulnerabilities irrelevant, buys time and increases cost for exploit development*	Only the vendor can do this
Reduce window of exposure *Expedite development of patch. Provide a robust and easy to use, or automatic, patch installation method on target*	Only the vendor can do this
Competitive vulnerability market *Offer competitive rewards for vulnerabilities, report to vendor*	Vendor, industry, and governments can do this

The first three options rely exclusively on the vendor, but there is no method by which the vendor can be legally enforced to perform these actions. The final option will require a significant change in the way the industry and governments think about software vulnerabilities and the economic losses they induce, but is the one that is likely to have the greatest short-term impact.

Current State

Over the past several decades, the Internet has become a critical infrastructure component on which substantial parts of the society and economy depend, and yet because of technological complexity and skewed economic incentives within the industry, the software being used is inherently insecure. However, when it comes to addressing security vulnerabilities in critical software components, there is almost exclusive reliance on:

- The ethics and altruism of the discoverer to follow coordinated disclosure
- A few vendor-operated bug bounty programs with moderate-to-low rewards

At the same time, more and more brokers or commercial players are purchasing vulnerabilities or offering zero-day exploits to their subscribers; these vulnerabilities can then be used for criminal operations or cyber espionage. To maximize profit and use from the sale of these exploits, subscribers may not report their existence to the vendor of the affected software. Thus, users are exposed to exploitation possibly for extended periods of time, or at least until the issue is independently discovered and reported to the software vendor. Meanwhile, substantial losses occur as a result of cyber operations – as shown in Figure 2.

It is remarkable that society depends on the altruism of so few (discoverers) for the security of a critical infrastructure, while at the same time a market offering considerable rewards is developing rapidly.

For example, full disclosure accounted for around 27 percent and coordinated disclosure for around 64 percent of the vulnerabilities in Microsoft products from 2006 to mid 2010.[9] Considering the global importance of the Internet, the current security ecosystem reveals itself as fragile and increasingly out of balance.

The experience of past decades has shown that traditional approaches based on *"more of the same"* cannot deliver adequate security. The question to ask is this: *"How much are those that bear the costs willing to pay to reduce their losses incurred as a result of cyber crime?"*

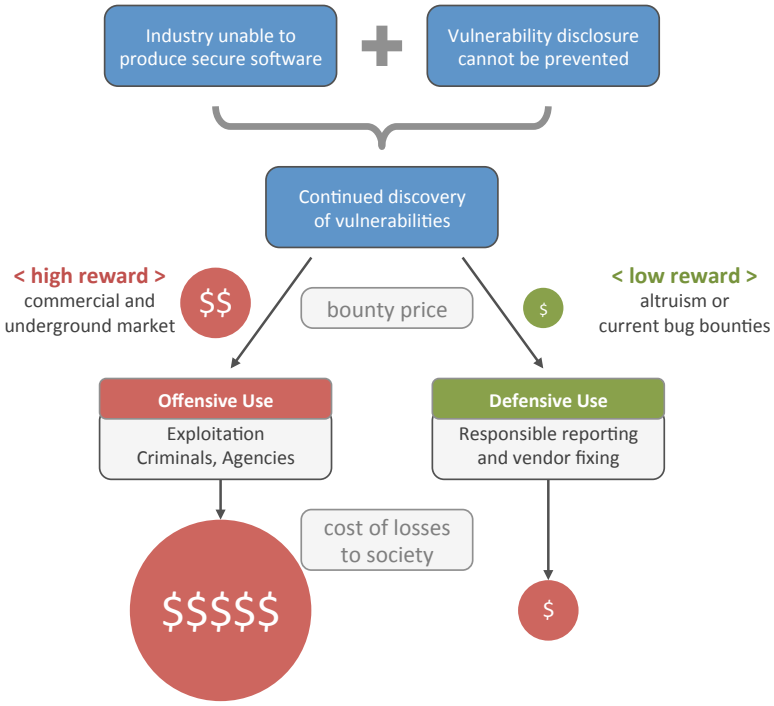

Figure 2 – How Handling Of Vulnerability Information Influences Cyber Crime Losses

The discovery and disclosure of new vulnerabilities cannot be prevented. The model depicted in Figure 2 demonstrates that information about a vulnerability can be used defensively or it can be used offensively (which will result in society incurring losses as a result of cyber crime). The defensive option can be made more attractive by offering higher rewards for vulnerabilities and within a more complete range of software products. It should be noted that investment in such a purchase program is justified so long as the total cost of the rewards is less than the cost of the losses prevented.

The benefits of such a program include:

- Inclusion of products that are not currently covered by existing bug bounty programs
- Vulnerabilities that otherwise would be acquired for illicit use are reported to the vendor
- Competitive pricing increases vulnerability research, thereby increasing the chance of the independent discovery and reporting of vulnerabilities that are already privately used by criminals or for cyber espionage

[9] *"How To Get Along With Vendors Without Really Trying"* Katie Moussouris - http://bit.ly/1b77qYv

International Vulnerability Purchase Program (IVPP)

An international vulnerability purchase program (IVPP) would offer competitive prices for all new and relevant vulnerabilities; coordinate this information with the vendor in order for a patch to be released; and publish all relevant information on the vulnerability. In this context, *relevant vulnerabilities* describes all vulnerabilities that pose a risk and have the potential to incur losses. The IVPP thereby covers vulnerabilities in products that are not covered by existing bug bounty programs (including free or open source programs).

Cost Analysis

The cost of purchasing all vulnerabilities in a given year, and at competitive prices, is remarkably low compared to the losses that are estimated to occur as a result of cyber crime, or the economic output of major countries, or the revenue of the software industry for the same time period. Figure 3 compares the cost of purchasing all vulnerabilities published in 2012 (regardless of criticality) for USD $150,000 per vulnerability with the GDP of both the United States and the EU and with the total revenue of the software industry for the same period. Purchasing all of the vulnerabilities of all vendors for this price is an unlikely scenario that is used only to demonstrate this proposal, since it includes non-critical vulnerabilities as well as vulnerabilities found in software that is neither well known nor widely used. The software industry tends to be dominated by a few key players, and, not surprisingly, most vulnerabilities are found within these products.

		Cost in Million $				Percentage Cost of			Percentage Cost of	
	Vuln.	Cost by Risk				GDP	GDP	Revenue	Cyber Crime Estimates	
Vendors	Total	High	Med	Low	Total	US	EU	SW Ind.	10 Billion	100 Billion
All	**5,218**	265	441	76	**783**	0.005%	0.005%	0.268%	7.827%	0.783%
Top 100	**3,332**	192	257	51	**500**	0.003%	0.003%	0.171%	4.998%	0.500%
Top 50	**2,959**	176	224	44	**444**	0.003%	0.003%	0.152%	4.439%	0.444%
Top 10	**2,065**	147	134	29	**310**	0.002%	0.002%	0.106%	3.098%	0.310%

Figure 3 – Cost To Purchase All Vulnerabilities In 2012 For USD $150,000 Each Compared To GDP Of US, EU, And Total Revenue Of Software Industry, And Losses Estimated As A Result Of Cyber Crime

Figure 3 also lists the cost of purchasing all of the vulnerabilities of those top 10, top 50, and top 100 vendors whose software resulted in the most known vulnerabilities in 2012. The software products of these vendors are the most critical since they are the most globally prevalent. For example, the top ten vendors (Oracle, Apple, Google, Mozilla Foundation, IBM, Microsoft, Cisco, Adobe, Linux, and HP) account for more than one third of all vulnerabilities published in 2012 and represent more than 80 percent of the market share of operating systems, web browsers, mail clients, and office applications.

Even in the unlikely event that *all* 2012 vulnerabilities of *all* vendors are purchased, the cost is ***less than 0.01 percent of the GDP*** of either the United States or the EU and ***less than 0.3 percent*** of the total revenue of the software industry. This includes the purchase of all known vulnerabilities in free and open source software. It should be noted that for retail companies within the United States, the accepted rate of "pilferage" or "inventory shrinkage," (considered a cost of doing business) falls between 1.5 percent and 2.0 percent of annual sales.

The cost of cyber crime is estimated in the tens to hundreds of billions of dollars per year. As it is inherently difficult to measure losses occurring as result of cyber crime, Figure 5 compares the cost of the IVPP to a lower (USD $10 billion) and higher (USD $100 billion) estimate of losses incurred as a result of cyber crime. The cost of the IVPP is found to be one or two orders of magnitude lower (between 0.8 and 8 percent) than the current

estimates of the cost of cyber crime. These figures demonstrate that even with a large margin for error, there is a solid business case for an IVPP: the IVPP is cost effective even if it is assumed that losses incurred as a result of cyber crime will be reduced by only 10 percent.

A more realistic scenario would be to link the reward of the program to the criticality of the vulnerability, for example, by offering USD $50,000 for low-risk vulnerabilities, USD $100,000 for medium-risk vulnerabilities, and USD $150,000 for high-risk vulnerabilities. With this pricing schema, the total cost of the IVPP as listed in Figure 3 would on average be reduced by approximately 25 percent – further validating the business case.

Operational Benefits

Existing bug bounty programs demonstrate the operational feasibility of a vulnerability purchase program. This summer, even Microsoft, which has long resisted the notion of paying for vulnerabilities, introduced its bug bounty program. While recent research has shown such programs to be economically efficient,[10] existing bug bounty programs suffer from a narrow scope of products for which they reward researchers, and low rewards compared to that which is offered on the black market. The exceptions are hacking contests, which, however, only reward their few winners once a year, and Microsoft, which offers USD $100,000 for new hacking techniques and less for individual vulnerabilities.

The IVPP extends the concept of rewarding researchers for reporting vulnerabilities in two dimensions: the scope (all relevant products) and the price (outbidding cyber criminals).

Price Dynamics

Some argue that with an IVPP offering competitive rewards for vulnerabilities, cyber criminals will raise the price that they offer for vulnerabilities. However, cyber criminals cannot afford to offer more for vulnerabilities than the *return they expect from their investment*. The IVPP on the other hand cannot offer more than the *expected reduction of the* losses.

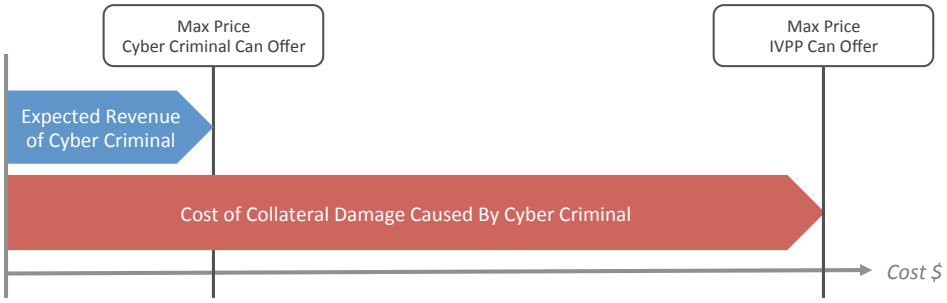

Figure 4 – Maximum Affordable Vulnerability Price For Cyber Criminal And IVPP

The huge collateral losses that are induced by cyber crime far *exceed the criminal's return*, typically by orders of magnitude. An IVPP therefore could systematically outbid cyber criminals and still be economically sound because the cost of the losses that are prevented would outweigh the return for cyber criminals.

[10] *"An Empirical Study of Vulnerability Reward Programs"* http://www.cs.berkeley.edu/~devdatta/papers/vrp-paper.pdf

Higher Rewards Lead To More Vulnerabilities Discovered

The high rewards and wide scope of an IVPP will likely lead to more researchers scrutinizing the security of products, which would result in more vulnerabilities being discovered in the short term. Often, a new vulnerability indicates a weakness in the code for a class of new attacks.

Early discovery, coordinated reporting, and knowledge of such vulnerabilities would allow for remediation of the root case and thereby would prevent a class of attacks or a number of future vulnerabilities. This is preferable to learning about a vulnerability after its exploitation in the wild.

The exploitation of a vulnerability that affects a known or even preventable class of attack (for example, a buffer overflow or sql-injection) indicates flaws in that software vendor's development process. Allocating the burden of remediating such vulnerabilities to the vendor is appropriate and the subsequent publicity surrounding the discovery of these vulnerabilities will create incentive for increased investment in the development process in order to prevent such vulnerabilities in-house. The vendor will also be motivated to investigate and remediate the root cause of the vulnerability, not only the reported attack vector.

An IVPP would also signal to vendors that numerous diverse researchers will be thoroughly evaluating the security of their products, and this will further motivate vendors to discover vulnerabilities during the development phase. Given the rapid expansion of commercial vulnerability and exploit markets, doing nothing is no longer an option.

Over the long term, the increased scrutiny will result in more secure products.

Transparency And Reduced Exposure Time

Research has shown that software vendors produce patches more quickly when external parties submit vulnerability information. An IVPP could force vendors to expedite development of a patch within a specified period of time, from first reporting to patch release, for example, 60 days. Failure to comply within this period of time will result in publication of the vulnerability information. In rare circumstances, the deadline may be extended, for example, if the issues requiring patching are highly complex. The broad scope of the IVPP will allow for information regarding the performance and responsiveness of different vendors to be collected over time, including those that consistently delay responses and patch development. This information can be used to rank vendors, which will incentivize them to improve their security. With this transparency of information, good security practices may be rewarded; poor security practices may be exposed; and actuarial data may be analyzed.

Information asymmetry, which allows software vendors to conceal poor security practices, would be reduced with the IVPP.

Single Point of Contact

Many software vendors still have no well-documented or established process by which they communicate with or respond to researchers, or they do not wish to engage with researchers at all. This frustrates researchers who otherwise are willing to follow the process for coordinated disclosure.[11] The IVPP can simplify the process and facilitate communication by becoming a single point of contact between vendors and researchers.

[11] *"Disclosure ethics apply to BOTH parties,"* Robert Graham - http://blog.erratasec.com/2007/01/disclosure-ethics-apply-to-both-parties.html

This is particularly relevant in the case of multivendor vulnerabilities, for example, vulnerabilities in a protocol or widely used software library, which are critical in that they affect multiple products. Coordinating the disclosure with a large number of different vendors exceeds the resources of an individual researcher.

Organizational Structure of IVPP

Independence, efficiency, and the highest degree of trust are key to establishing the IVPP as the accepted partner for a global community of researchers. For this reason, the IVPP should have a multitier organizational structure. *The Organizational Structure Of An IVPP* (see *Appendix*) discusses a proposed high-level model for an IVPP organization. A multitier structure prevents any part of the organization, or legal entity within which it is operating, from monopolizing the process or the information being analyzed.

Financing The Purchase Program

A solid business case for an IVPP has been presented, which demonstrates that the benefits outweigh the cost. The following are options for the financing of the program:

Governments	Any reduction in macroeconomic loss is beneficial to society and governments. Society bears the aggregated and collateral losses, and governments are the entities in charge of the wellbeing of nations. Governments could finance the IVPP either with a tax on related software products or services, or through legislation that would link software sales to the recovery of the cost of the program.
Finance Industry Or Other Specific Industry Sectors	The finance industry is heavily exposed to losses incurred as a result of cyber crime, and is also a major purchaser of software. The finance industry collectively could finance the IVPP to reduce its losses, and could leverage this when renegotiating software renewals. First-hand access to timely data regarding the security of software vendors would also be of particular value to insurance carriers offering cyber security policies. Benefits would include: • Use IVPP expenditures and results for vendor selection or in software contract negotiation • Actuarial data facilitates the assessment and pricing of cyber insurance
Software Industry	The software industry could itself: • Demonstrably increase investment in software security to make the IVPP redundant • Choose to self regulate by creating and financing an IVPP program, which would preempt its subjection to a future program beyond its control

Software Vendors Purchasing Their Vulnerabilities

The software industry tends to be dominated by a few key players, and, not surprisingly, most vulnerabilities are found in their products. Figure 5 depicts the cost for each of the top ten vendors (ranked by number of vulnerabilities in 2012) to purchase all vulnerabilities within their products (for USD $150,000 per vulnerability) and compares this to their revenue for the same period. Only three of these ten vendors currently run their own bug bounty program.

		Cost in Million $				Revenue in Million $	
	Vuln.	Cost by Risk					
Vendor	Total	High	Med	Low	Total	Revenue	Cost in %
Oracle	427	9.8	37.4	17.0	64.1	37,120	0.173%
Apple	303	25.1	18.3	2.1	45.5	164,700	0.028%
Google	279	24.9	16.2	0.8	41.9	49,770	0.084%
Mozilla	202	18.0	11.6	0.8	30.3	n/a	
IBM	175	6.9	16.5	2.9	26.3	104,500	0.025%
Microsoft	173	18.2	7.2	0.6	26.0	72,930	0.036%
Cisco	160	13.8	9.5	0.8	24.0	46,680	0.051%
Adobe	146	19.8	2.1	0.0	21.9	4,404	0.497%
Linux	116	3.5	10.5	3.5	17.4	n/a	
HP	84	6.8	5.0	0.9	12.6	120,400	0.010%
Total w/o Mozilla, Linux	(Open Source, No Revenue)				**262.1**	**600,504.0**	**0.044%**

Figure 5 – Cost For Vendors To Purchase All Vulnerabilities vs. Vendor Revenue In Same Year

NSS has found that the average cost to a vendor of purchasing all vulnerabilities is less than one percent of its yearly revenue. Figure 5 demonstrates that these vendors could purchase their vulnerabilities at competitive prices, and without any risk to their business.

These ten vendors are responsible for more than one third of all vulnerabilities published in 2012, and they represent the most critical and prevalent software products. If vendors were required to internalize the cost of such a program, they would be motivated to review and/or enhance the security of their software development processes.

Appendix

Organizational Structure Of An IVPP

Independence, efficiency, and the highest degree of trust are key to preventing sensitive information from being leaked and to establishing the IVPP as the accepted partner for a global community of researchers. For this reason, the IVPP should have a multitier organizational structure. Figure 6 depicts a high-level model of an IVPP structure.

The first tier of the model presents multiple *local submission centers* that are located in different world regions and that accept submissions from researchers. Contracted *technical qualification centers* (the second tier) qualify these submissions and share information with relevant vendors. Most critical is that the IVPP employs an organizational structure with multiple entities at each tier; this will ensure the automatic and consistent sharing of all relevant process information with all *local submission centers*, thus guaranteeing that the IVPP operates independently and is trustworthy.

This structure allows a researcher to check the status of a submission with any submission center, and it allows each submission center to verify that it possesses all information, including submissions from other centers. Because the IVPP would be handling highly sensitive information, checks and balances are critical. They would make it difficult for any party to circumvent the published policy of vulnerability handling. A multitier structure prevents any part of the organization, or legal entity within which it is operating, from monopolizing the process or the information being analyzed. Governments could still share vulnerabilities with their agencies, but they would no longer have exclusive access to this information and for extended periods of time. Detection of such a breach of the IVPP policy would bear the risk of expulsion for the offending submission center.

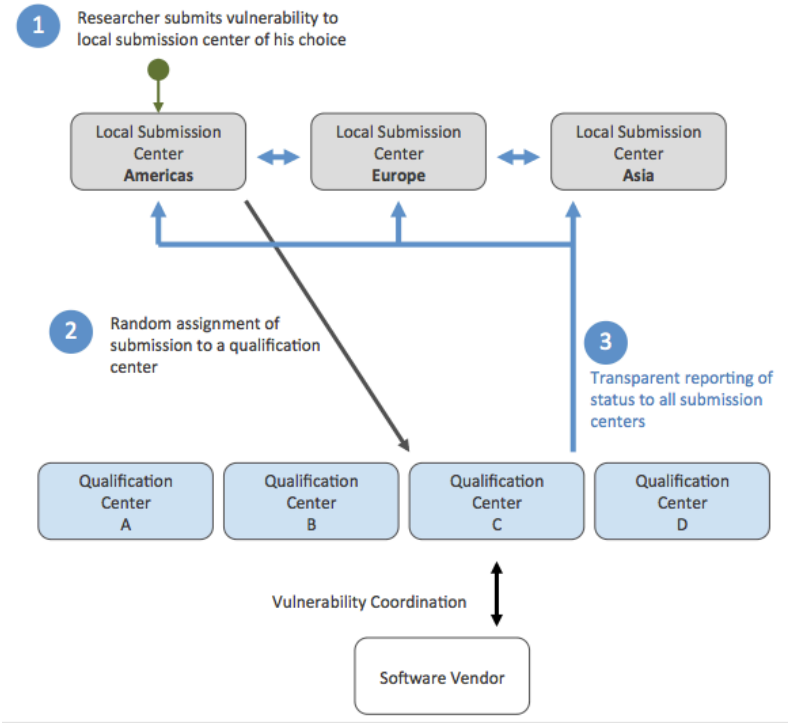

Figure 6 – Proposed Organizational Structure Of The IVPP

Local Submission Center

Local submission centers in different world regions accept vulnerability submissions and establish secure communications with researchers submitting new vulnerabilities. Having multiple centers in different world areas ensures as well as demonstrates independence from any specific government or industry, as well as facilitates communication in different languages. Candidates would be new organizations or local CERTs.

After their initial screening, submissions would be time stamped, documented, and shared with the other submission centers in order to create transparency, ensure independence, and prevent suppression of information. Every submission would be documented, which would create an audit trail from the document's submission to its rejection or its acceptance and subsequent publication, and, finally, the reward payment to the researcher. The researcher could access any submission center online to verify that the information is being processed and shared with the other centers.

Submission Qualification Center

A qualification center would have the deep technological competence to analyze and qualify submissions and to communicate with researchers at an advanced level. Once a submission is accepted, the center would share the information with the vendor of the affected software. All relevant actions would be documented and shared with all submission centers to provide an audit trail and to ensure independent checks and balances throughout the process.

Qualification centers could comprise specialized organizations or existing security companies that are contracted by the IVPP and therefore bound by its strict policy. Qualification centers would be subject to thorough screenings prior to their admittance into the program. Contracting with multiple qualification centers ensures independence and scalability. Submissions would be randomly assigned to qualification centers to ensure independence and to prevent bias.

Transparent Documentation

In the interests of transparency, the IVPP would on a regular basis provide the public with information concerning the vulnerabilities that have been processed. Working with a recognized entity such as the IVPP will allow researchers to enter into legally enforceable contracts rather than conducting transactions with cyber criminals. Selling the same vulnerabilities to cyber criminals and to the IVPP is not sustainable as cyber criminals will not accept such behavior.

Bounty Programs And Competitions

BugSheet maintains a list of bug bounty and reward programs, listing software vendors according to whether they offer a reward, an entry in the *"Hall Of Fame,"* or nothing at all.[12]

Sponsored by Microsoft and Facebook, the Internet Bug Bounty program rewards researchers for reporting vulnerabilities in a dozen open source programs.[13]

[12] http://www.bugsheet.com/bug-bounties

[13] https://hackerone.com/ibb

Acknowledgment

NSS thanks Professor Bernhard Plattner, head of the Communication Systems Group, and Professor Didier Sornette, Chair of Entrepreneurial Risks, both from ETH Zürich, for early feedback and their contributions to this research.

Reading List

"The Known Unknowns in Cyber Security" NSS Labs, November 2012
https://www.nsslabs.com/reports/known-unknowns-0

"Correlation Of Detection Failures" NSS Labs, May 2013
https://www.nsslabs.com/reports/correlation-detection-failures

"The Targeted Persistent Attack (TPA) – When the Thing That Goes Bump in the Night Really Is the Bogeyman" NSS Labs, August 2012
https://www.nsslabs.com/reports/targeted-persistent-attack-tpa-misunderstood-security-threat-every-enterprise-faces

"Top 20 Best Practices To Help Reduce The Threat Of The Targeted Persistent Attack" NSS Labs, October 2012
https://www.nsslabs.com/reports/top-20-best-practices-help-reduce-threat-targeted-persistent-attack

"Vulnerability Threat Trends" NSS Labs, February 2013
https://www.nsslabs.com/reports/vulnerability-threat-trends

Contact Information

NSS Labs, Inc.
206 Wild Basin Rd
Building A, Suite 200
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com

This analyst brief was produced as part of NSS Labs' independent testing information services. Leading products were tested at no cost to the vendor, and NSS Labs received no vendor funding to produce this analyst brief.