ANALYST BRIEF

The Known Unknowns

EMPIRICAL ANALYSIS OF PUBLICLY UNKNOWN SECURITY VULNERABILITIES

Author – Stefan Frei, PhD

Overview

In recent years, there has been increased interest in the way in which security vulnerability information is managed and traded. Vulnerabilities that are known only to privileged closed groups, such as cyber criminals, brokers, and governments, pose a real and present risk to all who use the affected software. These groups have access to critical information that would allow them to compromise all vulnerable systems without the public ever having knowledge of the threats. These privately known vulnerabilities are regarded as the “known unknowns” of cyber security.

NSS Labs has analyzed ten years of data from two major vulnerability purchase programs, and the results reveal that on any given day over the past three years, privileged groups have had access to at least 58 vulnerabilities targeting Microsoft, Apple, Oracle, or Adobe. Further, it has been found that these vulnerabilities remain private for an average of 151 days. These numbers are considered a minimum estimate of the “known unknowns”, as it is unlikely that cyber criminals, brokers, or government agencies will ever share data about their operations.

Specialized companies are offering zero-day vulnerabilities for subscription fees that are well within the budget of a determined attacker (for example, 25 zero-days per year for USD $2.5 million); this has broken the monopoly that nation-states historically have held regarding ownership of the latest cyber weapon technology. Jointly, half a dozen boutique exploit providers have the capacity to offer more than 100 exploits per year.

NSS Labs Findings

- The market for vulnerability and exploit information has grown significantly in recent years
- On any given day between 2010 and 2012, privileged groups had exclusive access to at least 58 vulnerabilities targeting Microsoft, Apple, Oracle, or Adobe; such access would have allowed these groups to compromise all vulnerable systems without public knowledge.
- During the period under investigation, vulnerabilities remained private for an average of 151 days before a vendor patch was made available.
- Jointly, half a dozen boutique exploit providers have the capacity to offer more than 100 exploits per year, resulting in 85 privately known exploits being available on any given day of the year.
- The true number of "known unknowns" is considerably higher than has been estimated, since many groups in possession of such information have no incentive to coordinate with the vendor of the affected software.
- Nation-states no longer have a monopoly on the latest in cyber weapons technology.

NSS Labs Recommendations

- Security professionals should make themselves aware of the clear and present risk presented by "known unknowns."
- Enterprises should assume the network is already compromised, and assume that it will continue to be compromised.
- As prevention is limited, enterprises should deploy tools and processes to quickly detect and remediate successful breaches.
- Enterprises should respond to a breach with a well-defined process rather than considering it to be an exception; have in place an incident response plan that is subject to routine review.
- Software vendors should take advantage of crowd sourcing via the establishment of a bug bounty program that would allow for early and more complete access to vulnerabilities affecting their products.

Table of Contents

Table of Figures

Analysis

The rise in importance of information systems for the economy and for society as a whole has been accompanied by increased interest in the way in which security vulnerability information is managed and traded. Technical advancements within software design and development have not prevented the release of insecure software and consequently the appearance of vulnerabilities. Economic and other non-technical incentives increasingly are perceived as the primary reasons for today's heightened risk exposure. While outside the scope of this analyst brief, it should be noted that there is limited incentive for software vendors to dedicate the time and resources required to adequately secure code before it ships. Thus, NSS expects that enterprise software will continue to ship with significant latent vulnerabilities, which in turn will motivate third parties to hunt for them.

Society is still in the early phase of adapting to the opportunities and threats of information technology. During the embryonic phase of innovation, before the emergence of a dominant design, the industry is characterized by high levels of experimentation among producers and customers. The market for vulnerability and exploit information is a good example of this evolutionary process. Every participant, from producers to customers, is learning. Each time a vulnerability is discovered, diverse groups, often with conflicting motives and incentives, engage to build a security ecosystem. To better understand this ecosystem, it is necessary to examine the *vulnerability life cycle*, which describes the life of a vulnerability from discovery to eventual publication and release of a patch.

The Security Ecosystem & Vulnerability Life Cycle

Vulnerability Life Cycle

The life cycle of a vulnerability can be divided into phases between distinct events. Each phase reflects a specific state of the vulnerability and the associated risk exposure for the users of the affected software. To capture these phases, six events can be defined in the vulnerability life cycle: *creation*, *discovery*, *exploit availability*, *disclosure*, *patch availability*, and *patch installation*, as shown in Figure 1.

With some restrictions, the exact sequence of these events varies among individual vulnerabilities and the parties involved.

Pre-disclosure Phase

The phase prior to the public disclosure of a vulnerability defines the *pre-disclosure* risk, during which time most of the software users are not aware of the vulnerability and therefore cannot assess the risk or take mitigating action. Within a privileged group, however, the vulnerability is known to exist; therefore, the vulnerability is regarded as a "known unknown."

Post-disclosure Phase

After public disclosure of the vulnerability, the *post-disclosure* phase starts. During this period, the software users are provided with information that will allow them to assess the risk or to take mitigating action until a patch is released and installed, thereby remediating the root cause of the vulnerability.

The individual events defining the vulnerability life cycle are further documented in the Appendix.

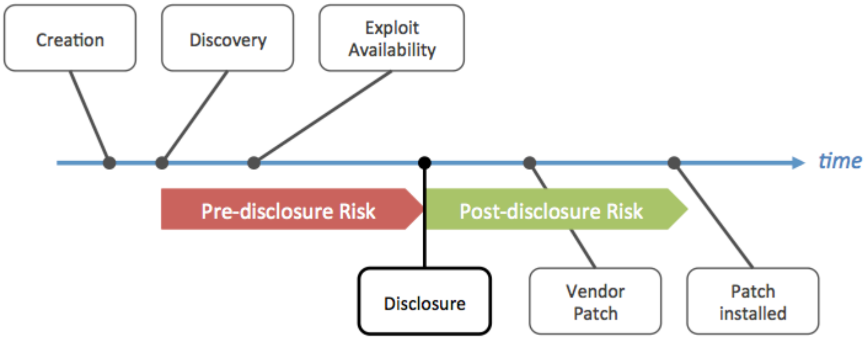

Figure 1 – Life Cycle Of A Vulnerability

The exact sequence of these events is dependent on the manner in which the vulnerability information is managed by the discoverer, and as such, it is a direct function of the incentives and ethics of the discoverer.

Vulnerability Disclosure Debate

Over the past few years, software vendors and security researchers have vigorously debated the social desirability of disclosing vulnerability information. While making the information public will allow all affected parties to assess the risk and take remediating action, the information will also become available to attackers for misuse. The belief that electing to keep vulnerability information private is keeping it from attackers is valid only under the assumption that potential attackers have not yet discovered or otherwise obtained access to this information.

This "disclosure debate," which is the debate over whether or not to divulge security information, is controversial, but it is not new; it has been an issue for locksmiths since the 19th century.[1,2]

As society's reliance on information technology has increased, information about security vulnerabilities has become a valuable asset, and it is not uncommon for ethical security researchers to require compensation for time spent uncovering vulnerabilities. Coordinated disclosure, which describes the scenario where 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. However, reporting vulnerabilities to a software vendor with the expectation of compensation might be viewed as extortion by the vendor. On the other hand, cyber criminals or government agencies that are not bound by legal or ethical considerations are willing to invest considerable amounts in suitable vulnerability information. These conflicting goals, approaches, and mindsets highlight the immature state of the market.

While a market for vulnerabilities has developed, vulnerability commercialization remains a contentious issue that is linked to the concept of vulnerability disclosure. Today, vulnerability information is traded on the underground "black market," is available through commercial service offerings, and is available through brokers where a number of software vendors have begun offering bounties for vulnerabilities that are reported directly to them.

[1] A. Hobbs, "*Locks and Safes: The Construction of Locks*," C. Tomlinson, Ed. Virtue & Co., London, 1853,1868

[2] B. Schneier, *"Locks and Full Disclosure,"* IEEE Security and Privacy, vol. 01, no. 2, p. 88, 2003

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; however, this assumption is incorrect 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 in bulletins or advisories for finding and privately reporting the issue.

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. Examples of typical buyers include:

- *Cyber criminals* who use the information for attacks.
- *Security companies* that 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 interested parties.

Clearly, there are a number of ways for vulnerability information to be made available only to privileged groups (excluding the vendor or users of the affected software) and possibly for extended periods of time.

Such groups range from lone hackers and cyber criminals to government agencies that will want to take advantage of their exclusive knowledge of the vulnerability and thus will have no desire to make the information public.

In order to assess and quantify the risk of the “known unknowns”, NSS analyzed data from two well-known vulnerability purchase programs (VPPs).

Vulnerability Purchase Programs (VPPs)

Traditionally, the primary players in the commercial vulnerability market have been iDefense, which started its Vulnerability Contributor Program (VCP)[3] in 2002 and TippingPoint, which started its Zero Day initiative (ZDI)[4] in 2005. Both vendors publicly advertise their vulnerability handling services and policies. With VPPs, it is a challenge for the sellers to demonstrate and the buyers to ensure that there is no malicious intent. The VCP and ZDI programs typically purchase vulnerability information to protect customers before a vulnerability becomes public knowledge, subsequently informing the vendor of the affected software. The VCP and ZDI programs advertise their ethics and request that security researchers accept lower compensation with the assurance that the information will be used for benevolent purposes.

Upon publication of a purchased vulnerability, both programs provide detailed technical information on the vulnerability and on the timeline from its initial purchase through publication. This information allows for an estimate of the pre-disclosure risk and allows for quantification of the "known unknowns." The VCP and ZDI programs together purchased 2,392 vulnerabilities from their launches up until September 23, 2013. Figure 2 depicts the yearly volume of vulnerabilities published by the VCP and ZDI programs together with the average time from purchase to discovery of these vulnerabilities for the years 2002 to 2012. Figure 3 lists the key aggregates of these two programs.

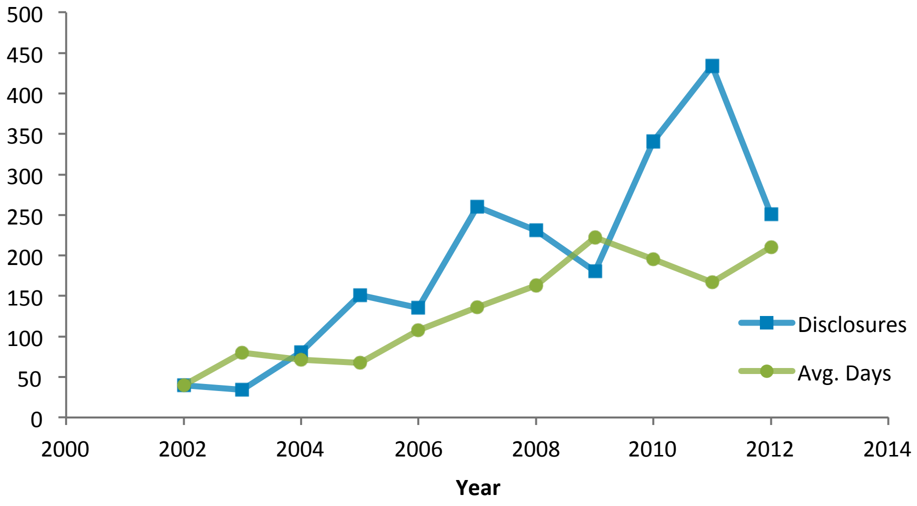

Figure 2 – VCP And ZDI Vulnerability Disclosures And Average Pre-Disclosure Time Of Vulnerabilities In Days

[3] http://www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/idefense

[4] http://www.zerodayinitiative.com

Program	Program Inception	Total Purchases	Targeted Vendors	Time To Disclosure
iDefense VCP	2002	969	195	133 days
TippingPoint ZDI	2005	1,423	92	174 days

Figure 3 – Total Purchases, Affected Software Vendors, And Average Time From Purchase To Publication

It is significant that the average time from *vulnerability purcha*se to *public disclosure* is 133 days for VCP and 174 days for ZDI. This is a lengthy period of time for a process of coordinated disclosure, particularly when considering that an affected vendor would be motivated to release a patch as quickly as possible. It is clear that vulnerabilities acquired by cyber criminals or by government agencies (with an interest in keeping the information private) remain unknown to the public for extended periods of time. In fact, Symantec found the average zero-day attack persists for almost a full year – 312 days – before it is detected.[5]

Both the VCP and the ZDI programs do not purchase all vulnerabilities offered; they prioritize based on type, criticality, and targeted software/vendor, in order to align expenditures with their business objectives. Thus, the majority of vulnerabilities purchased are rated as highly critical and target prevalent software products. Figure 4 lists the software vendors for which both programs have purchased at least 10 vulnerabilities within the past decade. Vulnerabilities in the products of these widely recognized vendors pose a significant risk to enterprises and to society as a whole.

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

	Vendor		Total Purchases		Days	Vendor
#	Affected	VCP	ZDI	VCP+ZDI	Private	Share
1	Microsoft	153	237	390	181	14%
2	Apple	38	171	209	129	10%
3	HP	17	157	174	233	19%
4	Adobe	59	102	161	119	17%
5	Oracle	29	114	143	166	8%
6	Novell	30	112	142	142	10%
7	IBM	58	67	125	226	8%
8	RealNetworks	19	73	92	262	49%
9	Sun	34	26	60	159	5%
10	Symantec	20	39	59	198	18%
11	Mozilla	8	51	59	80	5%
12	CA	23	30	53	151	29%
13	EMC	11	35	46	131	38%
14	Cisco	10	20	30	229	2%
15	WebKit	13	14	27	138	5%
16	Trend Micro	15	10	25	94	24%
17	Samba	9	14	23	65	28%
18	Ipswitch	15	8	23	58	25%
19	SAP	4	10	14	143	13%
Total		**565**	**1290**	**1855**		
Average					**153**	**17%**

Figure 4 – Software Vendors For Which VCP And ZDI Purchased Vulnerabilities In The Last 10 Years (With Average Pre-Disclosure Time And Share Of The Purchases On All Vulnerabilities Of Given Vendor)

The average pre-disclosure time for these vendors again is considerable: 153 days, or five months, over the past 10 years. Further, Figure 4 reveals that the VCP and ZDI programs together feed a remarkable number of vulnerabilities to the affected software vendors. For example, 14 percent of all Microsoft vulnerabilities, 10 percent of all Apple vulnerabilities, and 17 percent of all Adobe vulnerabilities published in the past 10 years were reported to the software vendor through the VCP or ZDI programs. These numbers demonstrate that VPPs attract a considerable share of the vulnerabilities of a given software vendor, despite the fact that the VPP rates are considerably lower than those offered by the black market.

In order to quantify the “known unknowns,” the following sections further explore the aggregate statistics of the vulnerabilities purchased by VCP and ZDI programs and of their targeted vendors.”

The Known Unknowns

Over the past 12 months, there have been reports regarding changes within and expansion of the vulnerability and exploit markets. New entrants to the vulnerability or exploit markets, as well as existing companies, have received considerable media attention, either because of their findings or because they have won highly-publicized hacking contests. It has long been accepted that cyber criminals operate with privileged vulnerability information; however, the Stuxnet attack in 2010 and other more recent revelations have exposed to a wider audience the existence and operations of suppliers of critical vulnerability information, and also of government-sponsored programs. During the pre-disclosure phase, these groups have exclusive access to critical information, which would allow for the compromise of all vulnerable systems without the public ever being aware of the threat.

These privately known vulnerabilities are the “known unknowns,” as depicted in Figure 5: A vulnerability is known to exist and to pose a security threat, but the public does not know about it therefore cannot assess or remediate the risk.

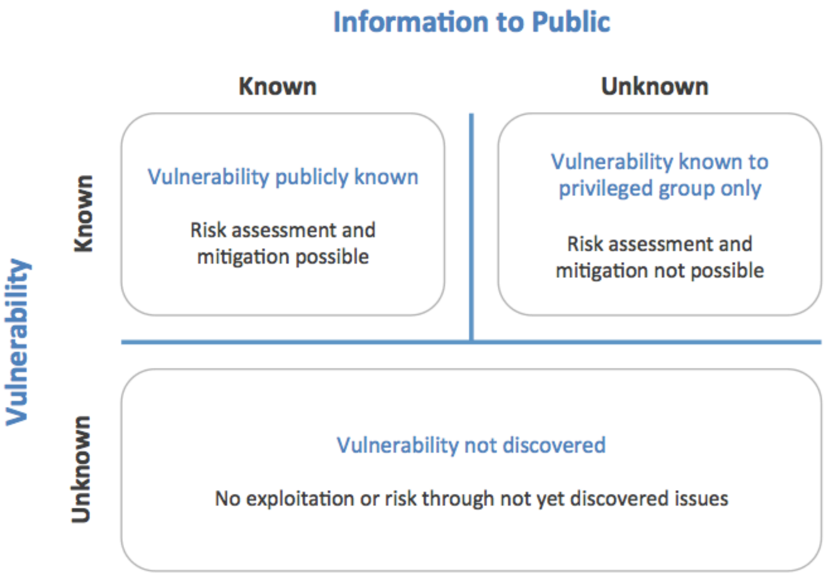
Information to Public
Known
Unknown
Vulnerability
Known
Unknown
Vulnerability publicly known
Risk assessment and mitigation possible
Vulnerability known to privileged group only
Risk assessment and mitigation not possible
Vulnerability not discovered
No exploitation or risk through not yet discovered issues

Figure 5 – The Known Unknowns In Information Security

Quantification And Exposure Time

Due to the inaccessibility, privacy, or unavailability of data, only certain aspects of the “known unknowns” can be measured with the information that is publicly available. It is unlikely that cyber criminals or government agencies will ever share data about their operations, and software manufacturers are reluctant to publish data about their internal processes for managing vulnerabilities. However, the empirical data presented in the previous section provides valuable insight, including a minimum estimate of the amount of “known unknowns” that users are exposed to, as well as the length of time during which they are exposed.

The number of vulnerabilities known exclusively to these programs can be calculated for each day since 2002. For example, on August 1 2012:

- VCP had 20 purchased, but not yet published, vulnerabilities in its processing queue
- ZDI had 93 purchased, but not yet published, vulnerabilities in its processing queue

Figure 7 plots the number of vulnerabilities known exclusively by the VCP and ZDI programs for every day since 2002. The darkly shaded area depicts the subset of vulnerabilities affecting only Microsoft, Apple, Oracle, Sun, and Adobe products . Figure 6 lists average numbers for 2010, 2011, and 2012.

Targeted Vendors	Vulnerabilities	Time to Disclosure	Known Unknowns
2010, 2011, and 2012		average in days	average per day
All Vendors	1,026	187	152
Microsoft, Apple, Oracle, Sun, Adobe	452	151	58

Figure 6 – Summary Of The Known Unknowns For 2010 – 2012

From 2010 to 2012, the VCP and ZDI programs together published 1,026 vulnerabilities, of which 425 (44 percent) target Microsoft, Apple, Oracle, Sun, and Adobe products. The average time from purchase to publication is 187 days (or 151 days for the five vendors). On any given day during these three years, the VCP and ZDI programs possessed 58 unpublished vulnerabilities affecting the five vendors, or 152 vulnerabilities in total. As no public information is available regarding the quantity of vulnerabilities possessed by cyber criminals, different brokers, or government agencies, these numbers are considered a minimum estimate of the total number of privately known vulnerabilities existing on any given day.

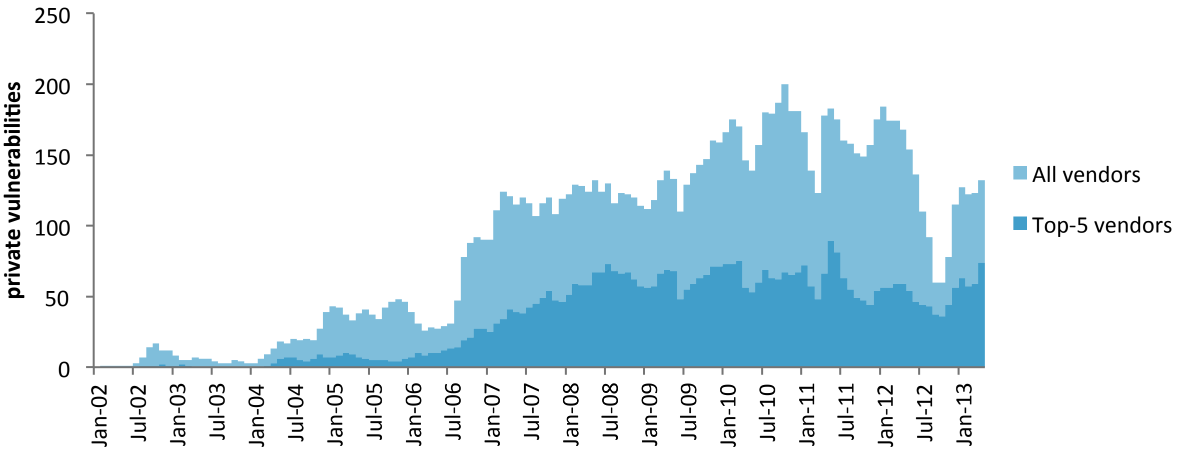

Figure 7 – Number Of Vulnerabilities Known Only To VCP And ZDI On Any Given Day Between 2002 And 2013

Figure 7 illustrates the number of “known unknowns” from July 2002 to February 2013. In September 2006, vulnerabilities increased to more than 100 per day, and in mid-2012, there was a significant decrease in vulnerabilities followed by a quick recovery.

This data reveals that on any given day over the past three years, the VCP and ZDI programs have had exclusive knowledge of 58 vulnerabilities targeting the products of major software vendors. This would have allowed them to attack most of the private and corporate users of these software products, and with a high probability of success, given that the attacks were not yet known. Since the VCP and ZDI programs use this information only for the purpose of building better protection for their customers, and since they share the information with the software vendors in order to develop and release patches, the overall risk is comparatively low. This analysis, however, clearly demonstrates that critical vulnerability information is available in significant quantities for private groups, for extended periods and at a relatively low cost.

Expanding The Minimum Estimate

It is NSS’ belief that the previous figures represent only a *minimum estimate* of the number of “known unknowns” and of the amount of time that users are exposed to them. Some of the parties involved in the exploitation of vulnerabilities have no desire to coordinate vulnerability information with the affected vendors, potentially using this information for offensive operations.

Internal Discovery By Software Vendor

Software vendors conduct internal vulnerability research either with their internal researchers or by contracting third-party code reviews and assessments. The findings remain internal knowledge and the software vendor makes the decisions regarding which vulnerabilities will be remediated and when this remediation will occur. This results in a number of vulnerabilities being known only privately and remaining unpatched for extended periods of time. Such vulnerabilities are often silently patched in new software releases following their discovery. Such delayed and silent patching not only exposes software users to the vulnerabilities for extended periods of time, it also denies users the opportunity to perform independent risk assessment or to take mitigating actions. Occasionally, these vulnerabilities that are discovered internally are later re-discovered by an independent third party that will then coordinate with the vendor. In such cases there will appear to be a truncated delay between "discovery" (by the second finder) and patch availability.

Bug Bounty Programs By Software Vendor

Over the past few years, a growing number of software vendors have introduced bug bounty programs, in which finders are compensated for reporting vulnerabilities directly to the software vendors, rather than going public with the information or selling it on the black market. The Mozilla Foundation was one of the first to introduce a bounty program, and since then Google, Facebook, PayPal, and others have followed. This summer, Microsoft, which has long resisted such a system, introduced its bug bounty program.

- Google paid approximately USD $580,000 over three years for 501 vulnerabilities discovered in the Chrome browser (= 28 percent of the patched vulnerabilities in same period)
- Mozilla paid approximately USD $570,00 over three years for 190 vulnerabilities discovered in its Firefox browser (= 24 percent of the patched vulnerabilities in same period)
- Facebook has paid approximately USD $1 million since the 2011 inception of its program
- Microsoft has paid approximately USD $100,000 since the June 2013 inception of its program for reporting new exploitation techniques

Recent research has found such programs to be economically efficient, comparing favorably to the cost of hiring full-time security researchers to locate bugs internally.[6] Bug bounty programs offered by software vendors generally benefit security as they can attract many vulnerabilities that might otherwise be used offensively. A software vendor has less time to delay remediation of vulnerabilities that are reported through a bug bounty program than if the vulnerabilities had been discovered internally.

Boutique Exploit Providers

There is an increasing number of commercial players that offer zero-day exploits for 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.[7] According to a recent article in *The New York Times*, firms such as VUPEN (France), ReVuln (Malta), Netragard, Endgame Systems, and Exodus Intelligence (US) advertise that they sell knowledge of security vulnerabilities for

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

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

cyber espionage.[8] The average price lies between USD $40,000 and USD $160,000. 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 (see Appendix for sources).

Governments & Defense Contractors

Long before the advent of the Internet, leading defense contractors (from all of the Group Of Twenty [G20] countries) used information warfare techniques. Many of these defense contractors have extended their services to include "cyber warfare" capabilities and offering these for sale to their long-standing government customers. Defense contractors generally avoid media attention (unlike the boutique exploiters), but based on their resources and on their current scale of recruitment, they serve a considerable share of the exploit market.[9] Recently, it was revealed that the National Security Agency (NSA) plans to spend USD $25 million on exploit purchases this year.[10] Given the average street price for zero-day exploits, this translates to more than 100 exploits. Countries such as Israel, Britain, Russia, India, and Brazil are some of the bigger spenders.[8]

Commercial Security Consulting

A commercially effective way to acquire zero-day exploits is through reverse engineering. Many large security consulting organizations employ teams of highly skilled reverse engineers and can deliver exploits for any software package. Instead of purchasing exploits on the market, an organization contracts with a team of reverse engineers that it deploys on-site to locate and weaponize vulnerabilities in specified software products.[9] At the end of the engagement, the vulnerabilities, exploits, and reports belong exclusively to the client. How the client chooses to use this information is entirely its business.

Exploit Brokers

Specialized, well-connected brokers offer to connect buyers and sellers for a percentage of the transaction price. Trades are assumed to be exclusive, and the vendor is not informed about the affected software. Some fees are paid in installments over periods of time in order to ensure that the seller of the vulnerability does not also sell the vulnerability to other interested parties, thus increasing the risk of the information leaking to the affected software vendor. Brokers package exploits for sale to buyers and, much like selling commercial software, the exploits are professionally marketed and include documentation and support. In the past year, this market has exploded, with more buyers emerging and with these buyers willing to pay higher prices.[11]

[8] "*Nations Buying as Hackers Sell Flaws in Computer Code*," *New York Times*, July 13, 2013
http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html

[9] "*The Business Of Commercial Exploit Development*," *DarkReading*, November 20, 2013
http://www.darkreading.com/hacked-off/the-business-of-commercial-exploit-devel/240142392

[10] "*The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities*," *Washington Post*, August 31, 2013
http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities

[11] "*Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits*," *Forbes*, March 23,2012
http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits

Connecting The Dots

As the analysis shows, on any given day for the past three years, the VCP and ZDI programs have had private knowledge of at least 58 vulnerabilities targeting Microsoft, Apple, Oracle, Sun, or Adobe, or of 152 vulnerabilities targeting the 19 vendors for which either program purchased more than 10 vulnerabilities. Given the average risk ratings, it can be reasonably assumed that a considerable number of these vulnerabilities are exploitable. Information on these vulnerabilities is coordinated with the affected software vendors.

Add to this the number of vulnerabilities/exploits that are not publicly traded or discovered and that are definitively not coordinated with the software vendor. Together, the boutique exploit providers mentioned previously are able to offer in excess of 100 exploits per year. Assuming an average of 312 days[5] before a zero-day exploit is publicly discovered results in at least another 85 exploits privately known on any given day.

Given the NSA budget of USD $25 million for the purchase of exploits in 2013 and given that the documented price of an exploit ranges from USD $40,000 to USD $250,000, it can be assumed that this will result in at least another 100 to 625 exploits per year[11] – or 86 to 541 known unknowns on any given day, provided the market can satisfy the demand.

Since there is no reliable information to further quantify “known unknowns” that are in the hands of cyber criminals or that are privately developed through consulting contracts, the assertion that there are 100 exploits available to privileged groups on any given day must be considered a reasonable minimum estimate of the “known unknowns.”

It is safe to assume that cyber criminals and government agencies primarily purchase vulnerabilities and exploits that target prevalent products from major vendors. Therefore, these “known unknowns” pose a real and present threat to the security of corporate and private software users.

The statistics presented in this brief do not include vulnerabilities in online services such as Facebook, Twitter, Google, e-Bay, and Salesforce. As more software becomes available as online services, i.e., software as a service (SAAS), there will be increased risk.

Appendix

Vulnerability Life Cycle Events

Analysis and empirical data on the sequence of these events can be found here.[12]

Vulnerability Creation	Vulnerabilities typically are the result of a coding error. If the vulnerability remains undetected throughout the development and testing phases, it will be included in the code that is released publically. The exact time that a vulnerability is created is by definition typically unknown; it may, however, be retrospectively determined, i.e., once it has been discovered or disclosed. If a vulnerability is malicious and thus intentionally created, discovery and creation time coincide.
Vulnerability Discovery	The time of discovery is the earliest time that a software vulnerability is recognized as posing a security risk. Vulnerabilities do exist before they are discovered, but prior to the discovery of the vulnerability, the underlying defect is not recognized as a security risk. Usually the time of discovery is not publicly known until after the vulnerability's disclosure, if at all.
Exploit Availability	An exploit is a piece of software, set of data, or sequence of commands that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur in the targeted software. Exploits for vulnerabilities that are not yet known publicly are known as zero-day exploits, or "0-days."
Vulnerability Disclosure	The time at which information about a vulnerability is made freely available, and in an understandable format, to the general public. From a security perspective, only free and public disclosure of vulnerability information can ensure that all interested, affected, or concerned parties receive the relevant security information.
Patch Availability	The earliest time that the software vendor releases a patch that can provide protection against the exploitation of the vulnerability. Software vendors cannot make security patches available instantly upon the discovery of new vulnerabilities or exploits. While some vendors publish patches as soon as they are available, others publish patches on a predefined schedule for planning purposes.

[12] *"Modeling the Security Ecosystem"* - http://www.techzoom.net/papers/weis_security_ecosystem_2009.pdf

The Microsoft Approach To Coordinated Vulnerability Disclosure

"Under the principle of Coordinated Vulnerability Disclosure, finders disclose newly discovered vulnerabilities in hardware, software, and services directly to the vendors of the affected product, to a national CERT or other coordinator who will report to the vendor privately, or to a private service that will likewise report to the vendor privately. The finder allows the vendor the opportunity to diagnose and offer fully tested updates, workarounds, or other corrective measures before any party discloses detailed vulnerability or exploit information to the public. The vendor continues to coordinate with the finder throughout the vulnerability investigation and provides the finder with updates on case progress. Upon release of an update, the vendor may recognize the finder in bulletins or advisories for finding and privately reporting the issue. If attacks are underway in the wild, and the vendor is still working on the update, then both the finder and vendor work together as closely as possible to provide early public vulnerability disclosure to protect customers. The aim is to provide timely and consistent guidance to customers to protect themselves."[13]

Exploit Offerings

Minimum estimate of exploits offered by boutique exploit providers

Provider	Offering	Remark / Source
Endgame Systems	25 exploits/year USD $2.5 million	*Business Week* http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html
Exodus Intelligence	60 exploits/year	Service Offering https://www.exodusintel.com/rsrc/ExodusIntelligence_EXP.pdf
ReVuln	> 9 exploits/year	Minimum estimate by counting exploits demonstrated here: http://vimeo.com/53806381 (2013-09-27)
VUPEN	> 7 exploits/year > 15 to 20 binary analysis and private 1-day exploits/month	Minimum estimate by counting list of published exploits here: http://www.vupen.com/blog/ (2013-09-27) Service Offering: http://www.vupen.com/english/services/ba-gov.php

[13] http://www.microsoft.com/security/msrc/report/disclosure.aspx#

Reading List

The Targeted Persistent Attack (TPA) – The Misunderstood Security Threat Every Enterprise Faces. NSS Labs
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
https://www.nsslabs.com/reports/top-20-best-practices-help-reduce-threat-targeted-persistent-attack

Correlation Of Detection Failures. NSS Labs
https://www.nsslabs.com/system/files/public-report/files/Correlation%20Of%20Detection%20Failures.pdf

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.

Please note that access to or use of this report is conditioned on the following:

1. The information in this report is subject to change by NSS Labs without notice.

2. The information in this report is believed by NSS Labs to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at the reader's sole risk. NSS Labs is not liable or responsible for any damages, losses, or expenses arising from any error or omission in this report.

3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY NSS LABS. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY NSS LABS. IN NO EVENT SHALL NSS LABS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet the reader's expectations, requirements, needs, or specifications, or that they will operate without interruption.

5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.

6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.