

Contents

Introduction	1
Background	1
Rise in Zero Day Vulnerabilities.....	2
Enter the Zero Day Initiative (ZDI).....	2
The ZDI Process	3
Historic Results	5
Summary	8

Introduction

TippingPoint's Zero Day Initiative (ZDI) program has been in operation since August 15, 2005. Recently, concerns have re-surfaced over whether or not 'paid for' security research is in the best interest of the industry – citing that information surrounding software flaws could wind up in the hands of criminals.

The purpose of this paper is to bring light to the intent, process and value of the ZDI program to TippingPoint's customers, legitimate security researchers, software vendors, TippingPoint itself, and the enterprise networking industry at large.

Background

First, it is important to understand the majority of today's security vulnerabilities are disclosed primarily through one of four mechanisms:

- **Product Vendor Discovery**

A product vendor (Oracle®, Microsoft®, Cisco®, etc.) discovers a flaw in one of their products as a result of in-house testing and announces it simultaneous to a patch release. In some cases, the vendor may silently patch the issue without a corresponding security advisory.

- **Responsible Third Party Researcher Discovery**

A third party security researcher discovers a flaw and reports it to the affected vendor "responsibly," allowing time for the vendor to patch the issue and announce the flaw only when a patch is ready. Instead of reporting it directly to the vendor, some researchers go to a third party who will handle the disclosure on their behalf.

- **Zero Day Vulnerability**

A security researcher discovers a flaw and announces it publicly without reporting it to the vendor. These are typically called zero day vulnerabilities since there is no associated patch yet available. This obviously leaves the vendor and its customers alike scrambling for a solution.

- **Zero Day Exploit**

A security researcher discovers a flaw and either sells it to the underground or uses it maliciously, exploiting unpatched users of the affected product. These attacks are typically called zero day exploits, and have been increasingly used by hackers, for example, to silently deliver spyware to their victim's desktops.

While TippingPoint protects its customers from vulnerabilities disclosed through each of these paths, the latter two – zero day vulnerabilities and zero day exploits – tend to create the greatest pain for product vendors and their customers.

Rise in Zero Day Vulnerabilities

Certainly not all flaws that emerge should be treated equally, and the same is true of zero day vulnerabilities. The newest version of the Common Vulnerability Scoring System¹ has a variety of metrics for rating the severity of a vulnerability, only one of which is the availability of a patch. An exploit for a vendor-announced vulnerability can be just as devastating as a zero day exploit thanks to the trend of shrinking windows of time for exploit release. Obviously, for an enterprise that doesn't stay up-to-date with security patches, even historic exploits – like the Code Red worm – can be just as damaging as a fresh zero day exploit in Microsoft's IIS Web server. Nonetheless, zero day vulnerability protection has become increasingly important in the security purchasing process for enterprises who feel frustrated and helpless relative to new and dangerous exploits surfacing while product vendors labor to develop and releases software patches.

An exploit for a vendor-announced vulnerability can be just as devastating as a zero day exploit thanks to the trend of shrinking windows of time for exploit release.

According to the SANS Institute's annual Top 20 Internet Security Attack Targets Update², "zero day attacks saw a significant upward trend in 2006." In 2006, 20 zero day vulnerabilities³ were catalogued for Microsoft and Apple® products alone. One of the more well known exploits emerged December 27, 2005 that was a zero day exploit against Microsoft Windows® computers. This Microsoft Windows MetaFile (WMF) vulnerability was discovered only after being actively used by hackers to exploit users to install adware and spyware. Variations of the exploit were eventually used by hundreds of malicious Web sites at one time⁴ while a patch was still forthcoming from Microsoft. Consequently, TippingPoint shipped updated protection to its IPS customers within 24 hours of the initial vulnerability discovery on December 28, 2005.

Enter the Zero Day Initiative (ZDI)

There remains a perception in the security industry that all security researchers are malicious hackers looking to do harm. While there clearly are malicious hackers with high skills, this remains a very small minority. In reality, the number of benevolent researchers with the expertise required to discover a software vulnerability (and recognize its significance) is

¹ "New Version of Common Vulnerability Scoring System Released." 20 June 2007. Forum of Incident Response and Security Teams. <http://www.first.org/cvss/>.

² "SANS Top-20 Internet Security Attack Targets (2006 Annual Update)." 15 November 2006. The SANS Institute. <http://www.sans.org/top20/>.

³ "SANS Top-20 Internet Security Attack Targets (2006 Annual Update)." 15 November 2006. The SANS Institute. <http://www.sans.org/top20/#z1>.

⁴ Krebs, Brian. "Windows Security Flaw is 'Severe.'" 30 December 2005. The Washington Post. <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/29/AR2005122901456.html>

a sizeable and growing group. The advancement of publicly available vulnerability analysis and discovery tools has helped foster this group of security enthusiasts. Also, it is not uncommon for “white hat” security researchers to stumble onto a new flaw while doing day-to-day security work.

With this growing network of ‘extended researchers,’ it only made sense for TippingPoint to develop a method to tap⁵ into this network of global researchers in such a manner to benefit the researchers, TippingPoint customers, and the general public all at the same time. The approach was the formation of the Zero Day Initiative (ZDI)⁶ that launched on August 15, 2005. The main goals of the program were then, and continue to be today:

TippingPoint validates the issue in its security labs and makes a monetary offer to the researcher, provided all background checks prove positive.

- Extend TippingPoint’s existing vulnerability research organization – DV Labs – by leveraging the methodologies, expertise and time of others
- Responsibly encourage the reporting of zero day vulnerabilities to the affected vendors by rewarding researchers
- Protect customers through the TippingPoint Intrusion Prevention

Systems (IPS) while the product vendor is working on a patch

The ZDI Process

Interested researchers provide TippingPoint with exclusive information about previously unpatched vulnerabilities they have discovered. TippingPoint collects background information in order to validate the identity of the researcher for ethical and financial oversight. TippingPoint validates the issue in its security labs and makes a monetary offer

- 1 A researcher discovers a vulnerability.
- 2 Researcher logs into the secure ZDI portal and submits the vulnerability for a valuation.
- 3 A submission ID is generated allowing the researcher to uniquely identify and track the vulnerability through the ZDI secure portal.
- 4 TippingPoint verifies the vulnerability and decides whether to make an offer with a week on average.
- 5 TippingPoint makes an offer for the vulnerability. The offer is sent to the researcher via e-mail and is accessible through the ZDI secure portal.
- 6 The Researcher logs into the secure portal, accepts the offer and assigns exclusivity of the information to TippingPoint.
- 7 Researcher is paid in his or her preferred manner. We support a number of payment methods.

TippingPoint responsibly notifies the affected product vendor of the vulnerability.

TippingPoint IPS protection filters are distributed to customers for that vulnerability.
- 8 Later, TippingPoint shares advance notice of the vulnerability details to other security vendors before public disclosure.
- 9 TippingPoint and the affected product vendor coordinate public disclosure through a security advisory when a patch is ready. The researcher is given full credit for the vulnerability discovery or alternatively can remain anonymous to the public.

⁵ <http://dvlabs.tippingpoint.com/blog/2007/07/26/remembering-five-years-of-vulnerability-markets>

⁶ <http://www.zerodayinitiative.com/>

to the researcher, provided all background checks prove positive. If the researcher accepts the offer, he/she will be paid promptly. As a researcher discovers and provides additional vulnerability research, bonuses and rewards can increase⁷ through a loyalty program similar to a frequent flier miles program.

After an agreement has been reached for the acquisition of a researcher's vulnerability, DV Labs simultaneously develops protection filters and notifies the affected vendor so the vendor can develop a vulnerability patch. TippingPoint discloses any and all acquired vulnerabilities to product vendors in accordance with the TippingPoint Vulnerability Disclosure Policy⁸.

The disclosure policy ensures that both researchers and product vendors understand how TippingPoint handles vulnerability information. This policy further reassures researchers that in no case will any of their discoveries be "swept under the rug." It also reassures product vendors that there is a professional and standard set of guidelines they can expect to be utilized throughout the disclosure process.

Once a patch is ready from the affected vendor, TippingPoint

collaborates with that vendor to notify the public of the vulnerability through a joint advisory that provides full credit to the originating researcher, unless the researcher chooses to remain anonymous. Before public disclosure of the vulnerability, TippingPoint also shares the technical details of the vulnerability with other security vendors so that they too may prepare an appropriate security response for their customers. TippingPoint maintains a competitive advantage with respect to their customers while facilitating the protection of a customer base outside their own.

In order to maintain the secrecy of a researcher's vulnerability discovery until a product vendor can develop a patch, TippingPoint customers are only given a generic description of the filter provided, not the vulnerability itself. Once details are made public in coordination with the product vendor, TippingPoint's Digital Vaccine[®] service for the Intrusion Prevention System provides an updated description so customers can identify the appropriate filters that were protecting them. In other words, TippingPoint customers will be protected from the vulnerability in advance, but they will not be able to discern the vulnerability itself.

Before public disclosure of the vulnerability, TippingPoint also shares the technical details of the vulnerability with other security vendors so that they too may prepare an appropriate security response for their customers.

⁷ <http://www.zerodayinitiative.com/benefits.html>

⁸ <http://www.zerodayinitiative.com/legal.html>

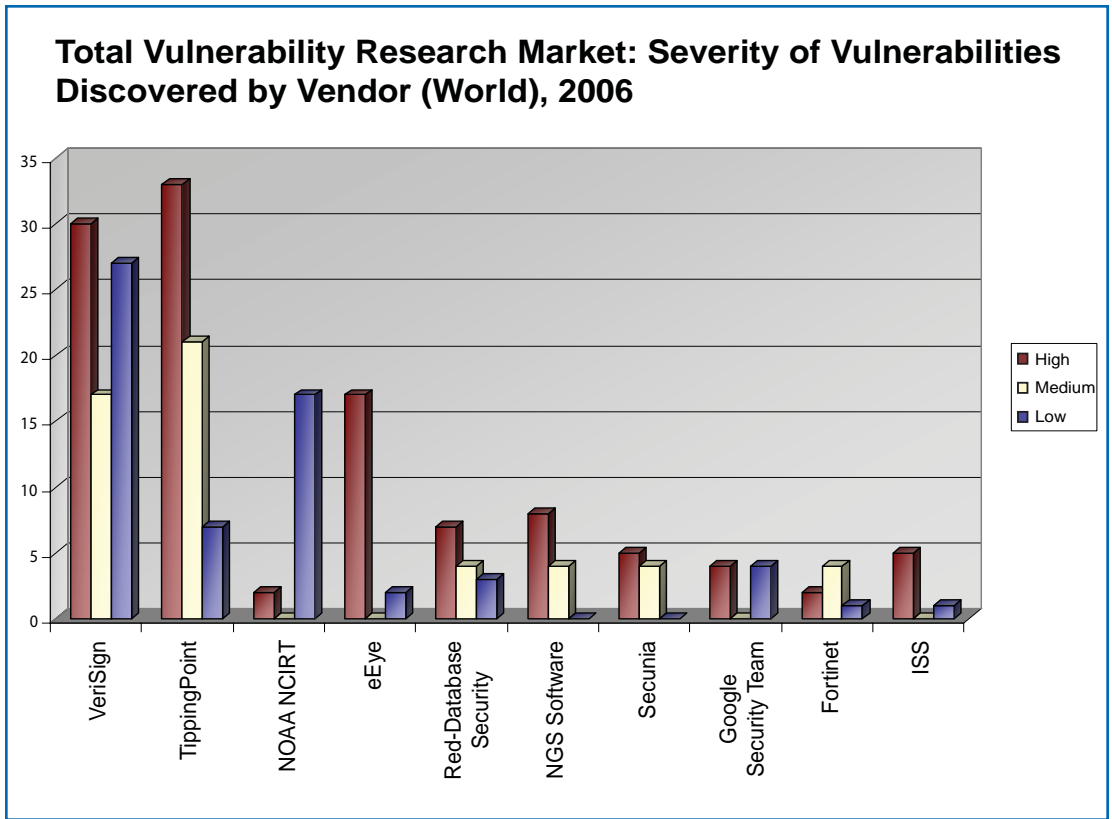
Coverage Overview	Disclosure	Patch	TippingPoint
Symantec VERITAS NetBackup Remote Code Execution(ZDI-05-001)	10.12.05	10.12.05	09.15.05
Microsoft Excel File Format Parsing Vulnerability (MS06-012) (ZDI-06-004)	03.14.06	03.14.06	02.21.06
Symantec VERITAS NetBackup DB Manager Vulnerability (ZDI-06-006)	03.27.06	03.27.06	01.23.06
Symantec VERITAS NetBackup vnetd Vulnerability(TSRT-06-01)	03.27.06	03.27.06	01.23.06
Symantec VERITAS NetBackup Vol. Manager Vulnerability(ZDI-06-005)	03.27.06	03.27.06	12.19.05
Microsoft Outlook WAB File Vulnerability (MS06-016)(ZDI-06-007)	04.11.06	04.11.06	04.03.06
Microsoft IE DXImage ActiveX Vulnerability (MS06-021)(ZDI-06-018)	04.27.06	06.13.06	06.13.06
Novell NetMail IMAPD Buffer Overflow Vulnerability(ZDI-05-003)	10.24.05	11.18.05	10.24.05
Adobe Macromedia ShockWave Code Execution (ZDI-06-002)	11.22.05	02.23.06	11.22.05
Novell GroupWise Messenger Accept-Language Vulnerability(ZDI-06-008)	03.16.06	04.13.06	03.14.06
Mozilla Firefox Tag Parsing Vulnerability (ZDI-06-009)	12.13.05	04.14.06	12.13.05
Mozilla Firefox CSS Letter-Spacing Vulnerability (ZDI-06-010)	01.31.06	04.14.06	01.23.06
Sophos Anti-Virus CAB Unpacking Vulnerability(ZDI-06-012)	02.28.06	04.25.06	03.14.06
Verisign I-Nav ActiveX Control Vulnerability (ZDI-06-014)	03.27.06	05.10.06	03.20.06
Apple QuickTime H.264 Parsing Vulnerability (ZDI-06-015)	03.20.06	05.11.06	03.20.06
Novell eDirectory 8.8 NDS Server Vulnerability (ZDI-06-016)	03.20.06	05.22.06	03.14.06
Microsoft IE UTF-8 Decoding Vulnerability (MS06-021)(ZDI-06-017)	01.20.06	06.13.06	06.13.06
HTTP: GraceNote CDDBControl Buffer Overflow (ZDI-06-019)	04.17.06	06.27.06	04.03.06
Apple iTunes AAC File Parsing Integer Overflow Vulnerability (ZDI-06-020)	04.07.06	06.29.06	04.03.06
WebEx Downloader Plug-in Code Execution Vulnerability (ZDI-06-021)	04.11.06	07.06.06	04.03.06
Microsoft Server Service Vulnerabilities (MS06-035)(TSRT-06-02)	07.11.06	07.11.06	07.11.06
Microsoft Excel Unspecified Code Execution (MS06-037)(ZDI-06-022)	07.11.06	07.11.06	07.11.06
MS Security Update for IE (MS06-042) (ZDI-06-026) (ZDI-06-027)	08.08.06	08.08.06	08.08.06
Microsoft HTML Help BO Vulnerability (MS06-046) (TSRT-06-08)	08.08.06	08.08.06	08.08.06
Microsoft Hyperlink Object Library Vulnerability (MS06-050) (TSRT-06-10)	08.08.06	08.08.06	08.08.06
Mozilla Firefox Javascript navigator Object Vulnerability (ZDI-06-025)	07.26.06	07.26.06	07.26.06
PowerPoint Remote Code Execution (MS06-058) (ZDI-06-032)	10.10.06	09.27.06	10.10.06
Excel Remote Code Execution Vulnerability (MS06-059) (ZDI-06-033)	10.10.06	10.10.06	10.10.06
Microsoft Office Remote Code Execution (MS06-062) (ZDI-06-034)	10.10.06	10.10.06	10.10.06
Server Service DOS & Remote Code Execution (MS06-063) (TSRT-06-02)	10.10.06	10.10.06	07.11.06
Cumulative Security Update for Internet Explorer (MS06-067) (ZDI-06-041)	11.14.06	11.14.06	10.10.06
CA Multiple Product Discovery Service Remote BO (ZDI-06-030)	10.05.06	10.05.06	04.03.06
CA Message Engine RPC Server BO (ZDI-06-031)	10.05.06	10.05.06	04.11.06
Novell eDirectory NDS Server Host Header BO (ZDI-06-035)	10.26.06	11.08.06	10.26.06
Novell Netmail User Authentication BO (ZDI-06-036)	10.31.06	11.08.06	10.31.06
AOL ICQ ActiveX Control Code Execution (ZDI-06-037)	11.06.06	10.31.06	10.31.06
Citrix IMA Management Module Remote Heap Overflow (ZDI-06-038)	11.09.06	11.09.06	11.09.06
WinZip FileView ActiveX Control Unsafe Method Exposure (ZDI-06-040)	11.14.06	11.14.06	09.05.06
Verity Ultraseek Request Proxying Vulnerability (ZDI-06-042)	11.15.06	11.01.06	04.03.06
Novell Netware Client Print Provider BO (ZDI-06-043)	11.29.06	11.29.06	07.04.05
Adobe Download Manager AOM Parsing BO (ZDI-06-044)	12.06.06	12.05.06	04.03.06
Cumulative Security Update for Internet Explorer (MS06-072) (ZDI-06-048)	12.12.06	12.12.06	02.27.06
Visual Studio 2005 Remote Code Execution (MS06-073) (ZDI-06-047)	12.12.06	12.12.06	11.06.06
Sophos Anti-virus CPIO Archive Buffer Overflow Vulnerability (ZDI-06-045)	12.12.06	12.12.06	12.12.06
Sophos Anti-Virus SIT Archive Buffer Overflow Vulnerability (ZDI-06-046)	12.12.06	12.12.06	12.12.06
Symantec Veritas NetBackup Buffer Overflow Vulnerability (ZDI-06-049)	08.14.06	12.13.06	11.20.06
Symantec VERITAS NetBackup CONNECT_OPTIONS BO Vul(ZDI-06-050)	12.13.06	12.13.06	11.20.06
Mozilla Firefox SVG Processing Remote Code Exec. Vuln. (ZDI-06-051)	12.19.06	12.19.06	12.14.06
Novell NetMail NMAP STOR Buffer Overflow Vulnerability (ZDI-06-052)	12.22.06	12.22.06	11.21.05
Novell NetMail IMAP Verb Literal Heap Overflow Vuln (ZDI-06-053)	12.22.06	12.22.06	12.21.06
Novell NetMail IMAP APPEND Buffer Overflow Vulnerability (ZDI-06-054)	12.22.06	12.22.06	10.24.05
CA BrightStor ARCserve Tape Engine Vulnerability (ZDI-07-002)	11.01.06	01.11.07	11.22.06
CA BrightStor ARCserve Backup Message Engine Vuln. (ZDI-07-003)	11.08.06	01.11.07	11.22.06
CA BrightStor ARCserve Backup Tape Engine Vulnerability (ZDI-07-004)	11.08.06	01.11.07	11.22.06
Sun Microsystems Java GIF File Memory Corruption Vuln (ZDI-07-005)	06.16.06	01.16.07	12.18.06
Citrix Metaframe Presentation Server Print Provider BO Vuln. (ZDI-07-006)	10.02.06	01.24.07	07.04.05
HP Mercury LoadRunner Agent Stack Overflow Vulnerability (ZDI-07-007)	10.27.06	02.08.07	11.10.06
Apache Tomcat JK Web Server Connector Vulnerability (ZDI-07-008)	02.16.07	03.02.07	02.26.07
Novell Netmail WebAdmin Buffer Overflow Vulnerability (ZDI-07-009)	12.12.06	03.07.07	12.14.06
Apple QuickTime UDTA Parsing Heap Overflow Vulnerability (ZDI-07-010)	08.14.06	03.07.07	05.23.06
IBM Lotus Domino IMAP Server Authentication Vulnerability (ZDI-07-011)	08.31.06	03.28.07	01.05.06
Yahoo! Messenger AudioConf ActiveX Control BO Vulnerability (ZDI-07-012)	10.27.06	04.03.07	11.10.06
Kaspersky AntiVirus Engine ARJ Heap Overflow Vulnerability (ZDI-07-013)	11.09.06	04.05.07	12.12.06
Kaspersky AntiVirus ActiveX Control Vulnerability (ZDI-07-014)	01.08.07	04.05.07	02.02.07
Novell Groupwise WebAccess Stack Overflow Vulnerability (ZDI-07-015)	03.19.07	04.18.07	04.19.07
Oracle E-Business Suite Node Deletion Vulnerability (ZDI-07-016)	01.29.07	04.18.07	12.14.06
Oracle E-Business Document Download Vulnerability (ZDI-07-017)	01.29.07	04.18.07	12.14.06
Microsoft Language Pack Vulnerability (MS07-033)(ZDI-07-037)	11.08.06	06.12.07	06.10.06
Microsoft Uninitialized Memory Vulnerability (MS07-033)(ZDI-07-038)	02.15.07	06.12.07	06.12.07
Microsoft Excel BIFF Record Vulnerability(MS07-023)(ZDI-07-026)	11.16.06	05.08.07	05.08.07
Microsoft Uninitialized Memory Vulnerability (MS07-027) (ZDI-07-027)	05.08.07	05.09.07	05.08.07
CA BrightStor ArcServe Media Server Vulnerabilities (ZDI-07-022)	03.08.07	04.24.07	04.19.07
Apple QuickTime Java Extension Vulnerability (ZDI-07-023)	04.23.07	05.01.07	04.23.07
Trend Micro ServerProtect EarthAgent Vulnerability (ZDI-07-024)	02.01.07	05.07.07	05.02.07
Trend Micro ServerProtect Module Vulnerability (ZDI-07-025)	02.01.07	05.07.07	05.07.07
CA eTrust AntiVirus Server inoweb Vulnerability (ZDI-07-028)	11.06.07	05.09.07	11.20.06
Samba LSA RPC Parsing Vulnerability (ZDI-07-029)	04.25.07	05.15.07	05.02.07
Samba DFS RPC Parsing Vulnerability (ZDI-07-030)	04.25.07	05.15.07	05.02.07
Samba SPOOLSS Parsing Vulnerability (ZDI-07-031)	04.25.07	05.15.07	05.02.07
Samba SRVSVC RPC Vulnerability (ZDI-07-032)	04.25.07	05.15.07	05.02.07
Samba LSA RPC Parsing Vulnerability (ZDI-07-033)	05.04.07	05.15.07	05.14.07
CA CAB File Parsing Vulnerability (ZDI-07-034)	08.11.06	06.05.07	11.30.06
Symantec AV Engine RAR File Parsing Vulnerability (ZDI-07-039)	11.01.06	07.12.07	11.20.06

Historic Results

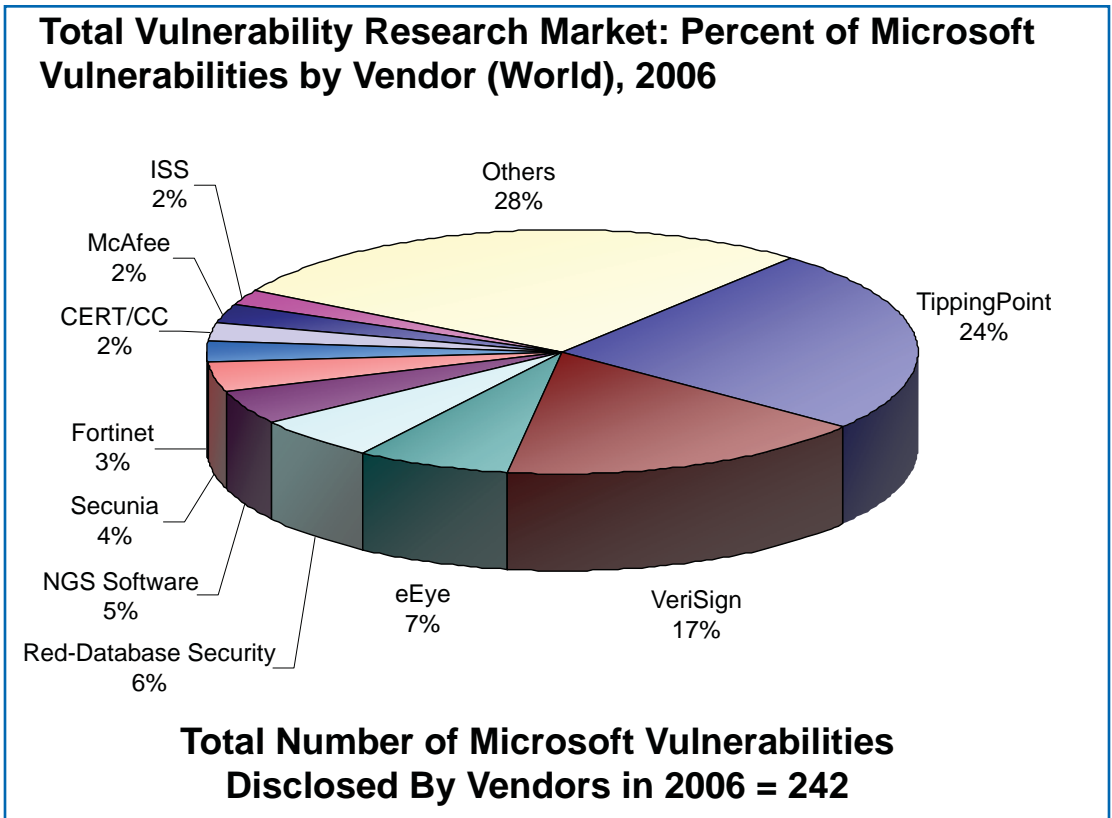
The Zero Day Initiative celebrated its two year anniversary⁹ in August 2007. Within its first two

years, ZDI has grown to over 600 researchers who have collectively contributed over 1,000 vulnerability submissions. TippingPoint has

⁹ <http://dvlabs.tippingpoint.com/blog/2007/07/26/happy-birthday-zdi>



Source: Frost & Sullivan 2006 World Vulnerability Research Market (N1B2-74)



Source: Frost & Sullivan 2006 World Vulnerability Research Market (N1B2-74)

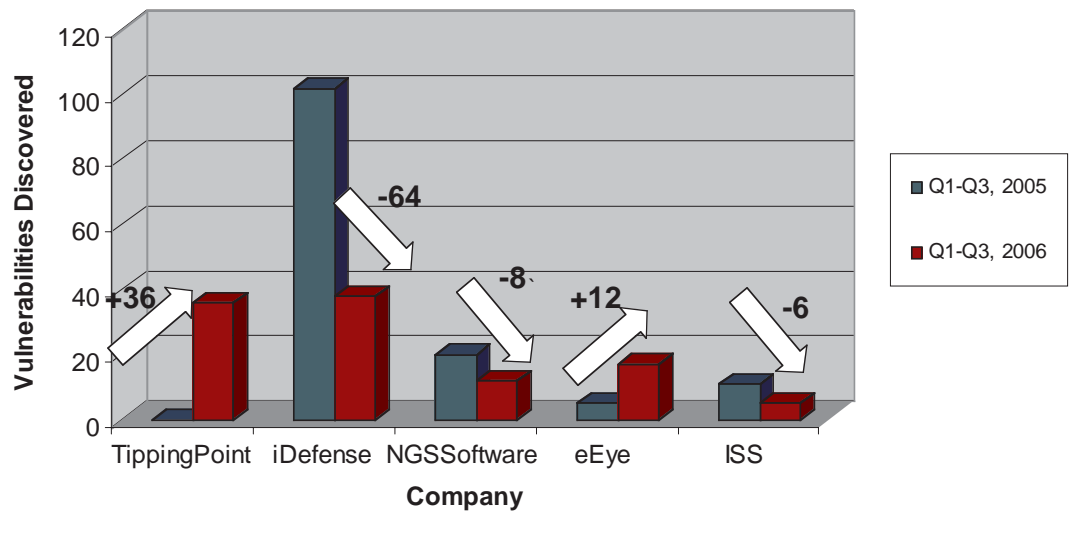
purchased the exclusive rights to over 250 of these submissions in that time. A random sampling of over one third of the vulnerabilities purchased in that timeframe shows TippingPoint customers have received, on average, 37 days of protection through the Digital Vaccine service in advance of a vendor supplied patch.

The list on page five indicates when each vulnerability was disclosed by TippingPoint to the affected vendor, when the vendor finally patched the issue, and when TippingPoint protected its customers with a corresponding IPS filter.

In the July-August 2006 timeframe alone, TippingPoint and ZDI were credited with helping Microsoft patch more vulnerabilities than any other individual or group. Another validation of the success of the ZDI comes from the analyst firm Frost and Sullivan. In May of 2007, Frost & Sullivan selected TippingPoint as the recipient of the 2007 Global Frost & Sullivan Award for Market Penetration Leadership in the vulnerability research market¹⁰.

Frost and Sullivan also disclosed in their January 2007 report, "Analysis of Vulnerability Discovery and Disclosure," that TippingPoint was the fastest growing discoverer of new vulnerabilities and the

Change in Total Vulnerability Discoveries by Vendor (Q1 2005 - Q3 2006)



Source: Frost & Sullivan "An Analysis of Vulnerability Discovery and Disclosure"

¹⁰ Frost & Sullivan. "Frost and Sullivan Recognizes TippingPoint's Valuable Contribution to Vulnerability Research." 11 May 2007. Frost & Sullivan. <http://www.frost.com/prod/servlet/press-release.pag?docid=98552761&ctxixpLink=FcmCtx1&ctxixpLabel=FcmCtx2>

leader in the discovery of both high-severity and Microsoft vulnerabilities.

Summary

With zero-day vulnerabilities on the rise and the window of time between discovery and exploit shrinking, it is increasingly important that security solutions be powered by next-generation security intelligence. With carefully managed security research commerce, the extended community of security research minds can be tapped to offer greater vulnerability protection for all technology users by ensuring that affected vendors have the time they need to address product flaws.

TippingPoint has one of the strongest internal research organizations via DV Labs¹¹. However, augmenting that organization with additional zero day research through the Zero Day Initiative enables TippingPoint to continue providing industry-leading IPS protection for its customers.

An untrained eye may view a program like ZDI as introducing risk that information surrounding software flaws will get into the hands of criminals, or even provide payment to criminals for finding vulnerabilities. In actuality, the facts clearly show that a well-controlled process of submission, validation, timely vendor disclosure, and advanced customer protection is a valid way of extending benevolent security research to the industry at large.

"TippingPoint continues to prove its security leadership by becoming the first intrusion prevention system vendor with a vulnerability research incentive program. The fact that TippingPoint has more vulnerability discoveries than any other IPS vendor confirms the program's success. Although the ZDI program has drawn controversy, TippingPoint has successfully demonstrated its competence in responsibly working with vendors to disclose the vulnerability with a corresponding patch. In turn, TippingPoint's customers have some of the greatest zero day protection an IPS can provide. With a program like ZDI, everyone benefits: the research community is compensated for their efforts, the vendors are provided knowledge of security flaws, and TippingPoint customers are protected well in advance of a threat."

Robert Ayoub, Frost & Sullivan

¹¹ <http://dvlabs.tippingpoint.com/>