

# Mostrame la guita!

Adventures in buying  
vulnerabilities

Pedram Amini  
pamini [at] tippingpoint

HTTP: [dvlabs.tippingpoint.com](http://dvlabs.tippingpoint.com)  
GDoc: <http://bit.ly/eDqjn>  
Twtr: pedramamini



# Talk Overview

- The Marketplace
  - who is buying vulnerabilities?
  - what are they doing with them?
  - how much are they paying?
  - what do they expect?
- The Vendors
  - how do they feel about the marketplace?
  - how are the vendors doing on response?
- The Future

# My Background

- iDEFENSE Vulnerability Contributor Program
  - 2002 - 2005
  - founding member
- TippingPoint Zero Day Initiative
  - 2005 - present
  - founding member

# The Market (s)

Players, Prices, etc...



# Market Breakdown

- Vendor Bug Bounty
- "White" Market
- "Grey" Market
  - .gov resellers
  - .gov
- "Black" Market

# No Fair Market Value?

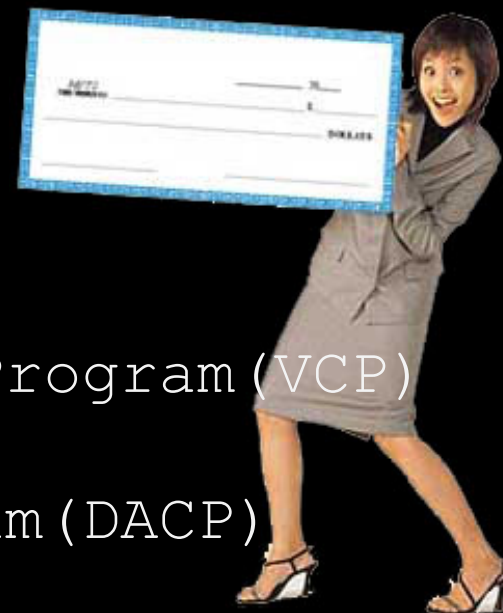
- Frequently voiced opinion
  - i disagree
- ZDI 0.1
  - auction with reputable buyers
  - market determines the price
  - ZDI & affected vendor given first right of refusal



# The Vendor Market

- Mozilla
  - most well known "bug bounty"
  - \$500 a pop
- Ghostscript
  - \$500, \$1000 for priority P1 and P2
  - 94 bugs currently qualify
- D. J. Bernstein QMail and DJBDNS
  - \$500 - \$1000
  - 2005 Georgi Guninski 64bit QMail, denied
  - March 2009 Mathew Dempsy DNS poison, awarded
- Google Native Client Security
  - \$1024, \$2048, \$4096, \$8192
  - Mark Dowd took first
- Google Chrome
  - \$500 a pop
  - \$1,337 for interesting finds

# Advertised Programs



- iDEFENSE Vulnerability Contributor Program (VCP)
- Digital Armaments Contributor Program (DACP)
- TippingPoint Zero Day Initiative (ZDI)
- WabiSabiLabi Marketplace (*defunct*)
- Netragard SNOsoft Exploit Acquisition Program (EAP) (*defunct*)
- iSIGHTPartners Global Vulnerability Partnership (GVP)
- Beyond Security Securiteam Secure Disclosure (SSD)

# 2002: iDEFENSE VCP

- Incentives
  - cash / credit per bug
  - annual competition for 50k/25k/10k/5k prize
- Motivation
  - annual subscription information feed
  - 100k for tier-2, unspecific details / no PoC
- Notes
  - 59 disclosures so far this year
  - >100 disclosures a year on average

# 2004: Digital Armaments DACP

- Incentives
  - cash / credit / equity per bug
- Motivation
  - annual subscription fee ranges from 6k - 120k
  - auction service
  - entertains bulk offers
- Notes
  - <10 disclosures ever?!?
  - 1st iteration of literature lifted from VCP
  - equity program is reportedly flaky
  - appears active, at least on the facade

# 2005: TippingPoint ZDI

- Incentives
  - cash / credit / points per bug
  - referral reward
  - 20k/25%/100%, 10k/20%/50%, 5k/15%/25%, 1k/10%  
/na
- Motivation
  - increased filter protection creation time
  - world-wide monitoring of 0day exploitation
- Notes
  - 65 disclosure so far this year
  - ~100 estimated forward moving average
  - 121 upcoming disclosures
  - free information sharing with security vendors  
(yes even our competitors)

# 2007: WabiSabiLabi

- Incentives
  - cash via auction per bug
  - 10% of revenue distributed among researchers
- Motivation
  - vulnerability resales
  - partnership with OneShield UTM appliance
- Notes
  - public bug list was not all encompassing
  - Preatoni's arrest was unrelated to WabiSabiLabi
  - since the arrest, the program has shut down

# 2007: Netragard SNOsoft EAP

- Incentives
  - cash per bug
  - middle man to multiple buyers
- Motivation
  - finders fee
- Notes
  - announcement via SNOsoft blog
    - <http://snosoft.blogspot.com/2007/01/exploit-acquisition-program.html>
  - all buyers are US based
  - >4 month acquisition time
    - and this is why they closed in Mar. 2008

# 2008: iSIGHTPartners GVP

- Incentives
  - cash per bug / credit?
  - no reward program
- Motivation
  - annual subscription information feed
  - resales? feed fees?
- Notes
  - only a single disclosure?!?

# 2009: Beyond Security SSD

- Incentives
  - cash per bug
  - middle man to multiple buyers
- Motivation
  - small finders fee
  - born out of demand from securiteam.com researchers
- Notes
  - one paragraph description on web
    - <http://www.beyondsecurity.com/ssd.html>
  - disclosure process is determined by buyer

# Mostrame la Guita! (USD)

- "White" Market
  - $< \$20,000$
  - average is  $\$5,000 - \$15,000$
- .gov Resellers
  - $\$20,000 - \$100,000$  US
  - average is  $\sim \$50,000$
- .gov
  - $\$100,000 - \$1,000,000$
  - average is  $< \$250,000$
- "Black" Market
  - $\$20,000 - \$100,000$  US
  - average is  $\sim \$50,000$ , seller beware of final hour price fluctuations



# Zero Day Initiative

An Inside Look

# The Researchers

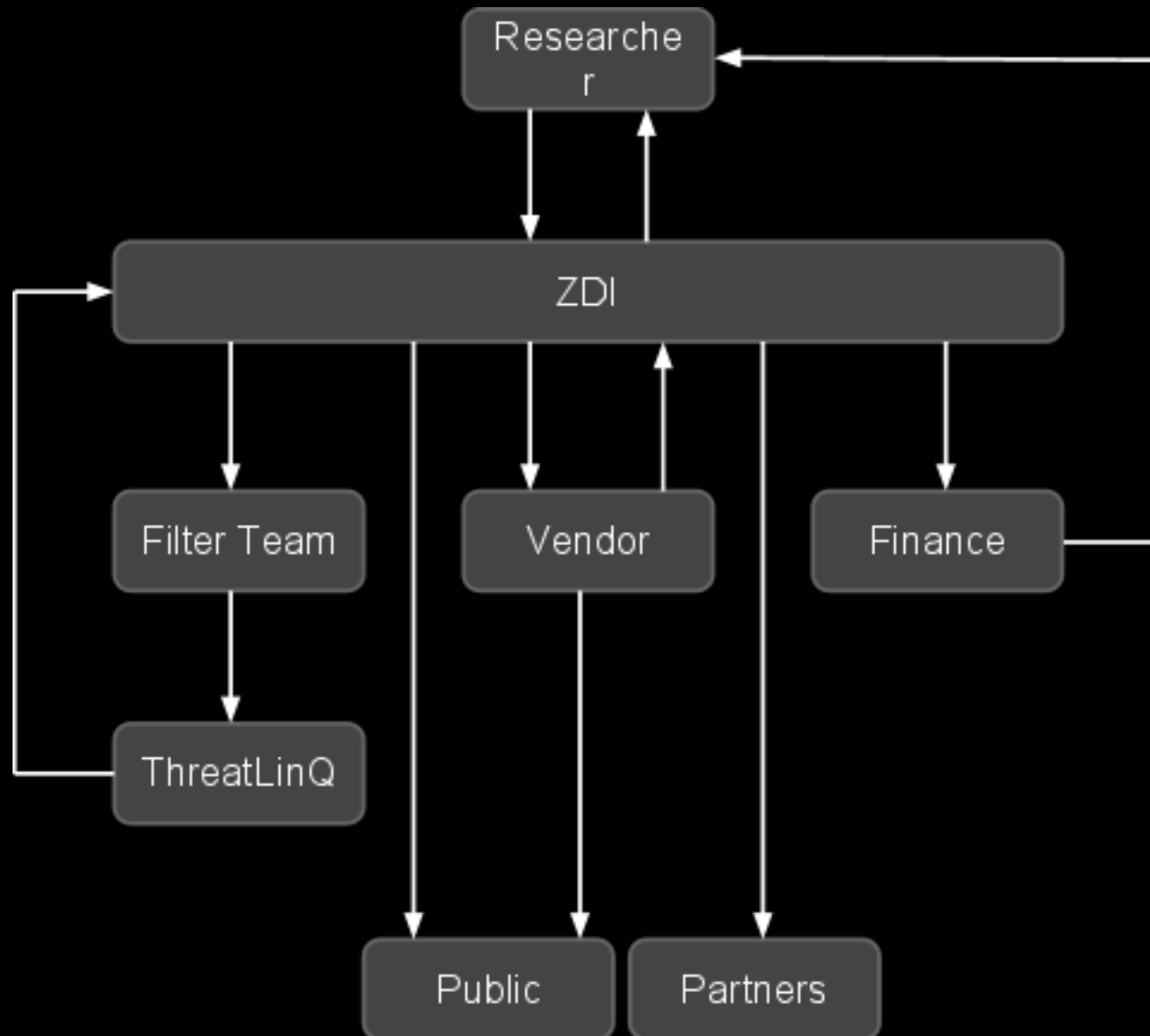
- >1,000 researchers registered
  - ~500 have opened at least one case
    - follows power law distribution
  - male, teen to mid twenties, hobbyist
- ~1,900 cases seen total
  - >500 accepted (30%)
  - avg. 10 a month
- Top origins
  - 25% United States
  - 5% United Kingdom
  - 4% Germany, India
  - 3% France, Brazil, Spain
  - 2% Italy, China

# The ZDI Team (TSRT+k8)

- 19 days average verification time
- 14 days average payment time



# The Lifecycle



# The Research\*

Vendor	# Accepted	% Accepted	% Budget
Adobe	18	28%	3%
Apple	55	44%	8%
CA	21	26%	2%
EMC	10	56%	1%
HP	20	29%	2%
IBM	26	32%	4%
Microsoft	133	30%	30%
Mozilla	13	31%	2%
Novell	35	52%	5%
Oracle	11	34%	1%
Real	20	39%	3%
Sun	12	24%	3%
Symantec	30	45%	5%

\*covers only our most prominent vendors

# The Partners

- Fortinet
- SecureWorks
- Sophos
- Stonesoft (almost)
- Third Brigade (Trend Micro)
- ZScalar
- Where is everyone else? Good question.

# Trends

- Increasing rate of overlapping discoveries
- Most research is on the client-side
  - Browsers, QuickTime, PDF, SWF
- Increasing interest off the Windows platform
- Main motivation shifting towards profit

# No More Free Bugs (NMFB)

- <http://nomorefreebugs.com/>
- March 2009 Charlie Miller, Alex Sotirov and Dino Dai Zovi
- LinkedIn group has >50 members now



# Vulnerabilities

Stories, Musings, Mishaps...

# Bugs We Have Turned Away

- Non remote issues
  - can't protect our customers
  - no post-auth for the most part either
- Hosted Services
  - GMail, LinkedIn, etc..
  - verification legality issue
  - Salesforce.com has reached out to us
  - some scary bugs out there
- Non Fortune 100
  - nginx (twice), despite its 4% market share

# Behind the Hype

- 2008 CansecWest Pwn2Own two-minute pwn
  - Apple zealots are intense
- Firefox 3.0 five-hour discovery
  - <http://dvlabs.tippingpoint.com/blog/2008/06/18/vulnerability-in-mozilla-firefox-30>
- MS09-043 Microsoft OWC
  - 2.5 year patch turnaround time
- 2009 Pwn2Own IE8 twelve-hour pwn
  - Great find by Nils
  - DEP bypass via .NET DLL load ineffective

# PDF JBIG2 0day

- Sept. 2008 we received the report
  - so did 3 other potential buyers
  - unfortunately we didn't win the bid war
- Feb. 2009 exploitation seen in wild
  - <http://research.eeye.com/html/alerts/zeroday/20090212.html>
- Snagged a sample from ThreatLinQ and it was undeniably based on the same PoC
- ???

# Microsoft IE 0day Triplet

- MS08-031, ZDI-08-039
  - DOM object substringData() heap corruption
  - Affects IE 6 and 7
- Oct. 22, 2007 first report received
- Apr. 23, 2008 second report received
- May 19, 2008 third report received
- June 10, 2008 public disclosure
- No foul play

# Free Sirius Bug

- Fun bug
- Not something we normally handle, but the researcher feared approaching the vendor
- July 10, 2008 sent report to the vendor
- First attempt was misconceived to be a job application
- Second attempt was met with legalese
  - Sirius / XM merger
- Fixed but never publicized... until now

# Dishonorable Mention

- Software so bad, we simply couldn't afford to keep supporting it
- Trend Micro Server Protect
- Computer Associates ARCserve Backup
- Hewlett-Packard OpenView Network Node Manager



# Vendors

Reactions and Statistics

# Vendor Sentiments

- Our relationships with vendors start on the right foot as we don't resell information
- Overall, the vendors like us and what we stand for. Not easy to get that in writing though
- Drastic contrast from my iDEFENSE days
- Some really approve
  - <http://www.netiq.com/support/ReportPotentialSecurVulner.asp>

# BMC

- 2007 Pwnie nominee for "Lamest Vendor Response"
- ZDI-07-019 and ZDI-07-020
  - April 2007 vendor didn't want to address issues reported from non "legit" customers
- ZDI-08-082
  - December 2008 drastic improvement in response
- Ironically, they have an office down the block from us

# Vendor Response Times\* (days)

Vendor	2006	2007	2008	2009	Overall	Upcoming**
Adobe	242	67	215	-	179	269
Apple	166	46	106	59	91	92
CA	239	291	12	-	224	478
EMC	-	129	72	146	103	412
HP	295	264	-	-	291	276
IBM	267	117	170	-	190	434
Microsoft	170	311	171	100	197	171
Mozilla	50	29	32	-	48	314
Novell	82	161	163	28	125	170
Oracle	-	364	281	145	306	165
Real	-	261	199	-	234	205
Sun	214	180	156	121	160	34
Symantec	143	486	80	-	307	127

\*covers only our most prominent vendors

\*\*these numbers get skewed with recent reports

# 10 Most Outstanding

Hewlett-Packard	1071+	days
Hewlett-Packard	911+	days
Microsoft	875	days
Microsoft	866	days
IBM	847+	days
Hewlett-Packard	791+	days
Borland	733+	days
Symantec	706	days
Microsoft	697	days
CA	693	days
...		



# What 's Coming?

- Zero Day Initiative
  - full vendor report card roll-out
  - credit on upcoming advisories
  - researcher profile pages
  - collaboration between researchers
  - advisory comments and maybe timed release
  - expansion to researcher insights
- The Market (IMHO)
  - increase in programs, later tapering off
  - regulations (US)?
  - exploit derivatives market, Rainer Bohme
    - not enough liquidity

# Open Discussion

Questions? Comments.

Pedram Amini

pamini [at] tippingpoint

<http://dvlabs.tippingpoint.com>

Google Doc: <http://bit.ly/eDqjn>

Don't forget to participate in our contest