Trend Micro's Zero Day Initiative

Who we are, bug bounties and how to get the most bang for your bugs!

Shannon Sabens
ZDI Program Manager
Trend Micro

Agenda

- Introduction
- What's the ZDI?
- Submitting to the ZDI
  - I submitted, now what?
- Pwn2Own
- Questions?

Introduction

Introduction – Shannon Sabens

- Program Manager, ZDI, since 2013
- Formerly Microsoft Malware Protection Center and Symantec
- Purchased and disclosed 3000+ vulnerability reports on behalf of ZDI community

What's the ZDI?

ZDI Objectives

- Augment the TippingPoint product filters and protection for our clients
- Build a community working to secure the greater enterprise ecosphere
- Encourage growth in this space by investing in security research
- Contribute to the maturation of vulnerability disclosure and response processes

Roughly 4000 vulnerabilities have been patched and disclosed to date as a result of the efforts of the ZDI community.

TREND MICRO | ZERO DAY INITIATIVE

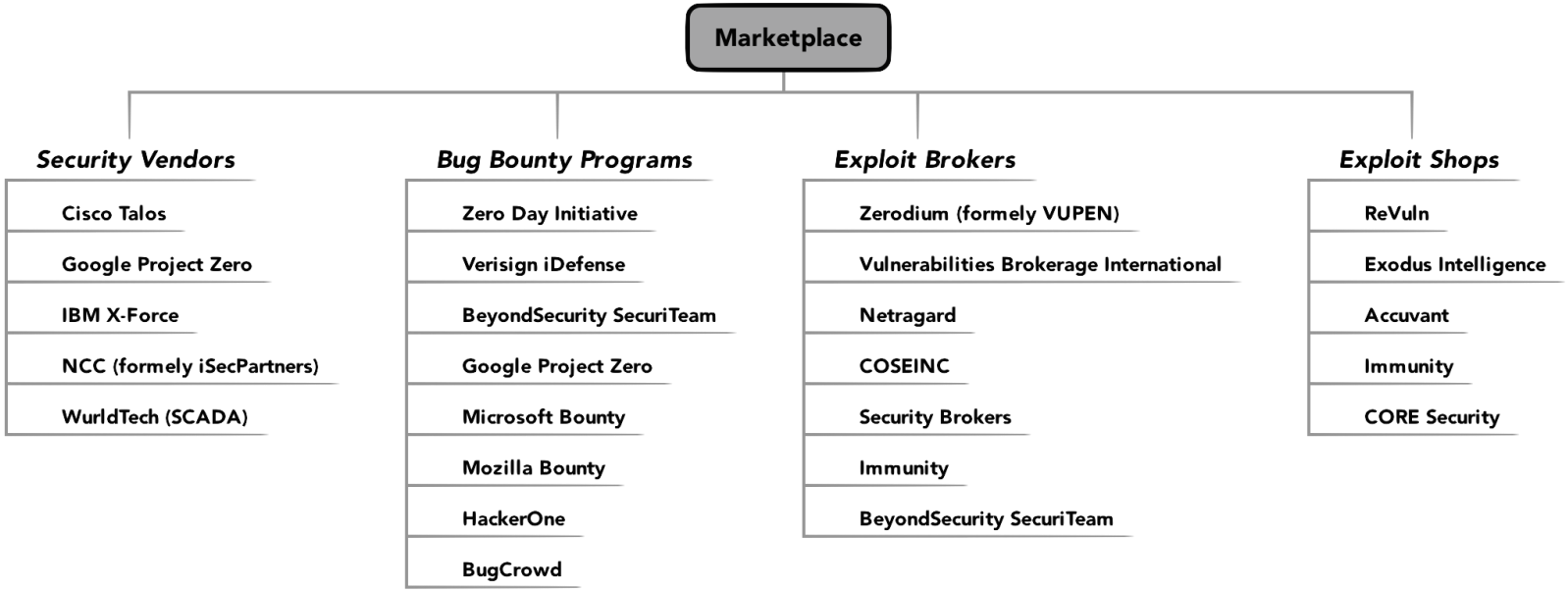
Similar (?) programs

- iDefense
- HackerOne
- BugCrowd
- Cobalt.io

… various vendor and/or product specific bounties…

Some of the tips to follow can help you submit to programs that may be the right fit in your case, or to the vendor, with success!

Vulnerability/Exploit Intelligence Marketplace



Looking at what we know about bug bounties – What do they tell us about themselves?

- An agnostic bug bounty like ZDI vs. Vendors and web businesses with bounties
- ZDI see a higher quality bar
  - 57% of all submissions were accepted in 2016
  - On par with previous years and is much higher than the rate of other programs

ZDI is prolific compared to similar entities

- 2015 –666 vulnerability reports to patches
- 2016 –700 vulnerability reports to patches
- 2017 - 848 vulnerability reports to patches, so far!

ZDI contributors

- ZDI contributors are a global community of security/vulnerability researchers. Our network includes 3000+ researchers in 80 countries!

- *We rightly and very gladly share the credit for this work!*

More about the ZDI

- #1 Supplier of vulnerability reports to Microsoft 2014, 2015, 2016
- #1 Supplier of vulnerability reports to Adobe 2015, 2016
- And considerable contributions in the overall SCADA space as well!
- *75% of ZDI disclosed reports come from contributors and 25% is ZDI's own research

ZDI's Focus

1. Highly-Deployed
2. Enterprise
3. SCADA
4. Security
5. Development
6. Point-of-Sale
7. Networking
8. Architecture
9. Mobile
10. Infrastructure

American infrastructure's cybervulnerabilities again in the spotlight

Share this content:

The fear of a state or terror-group-sponsored cyberattack on the nation's infrastructure was again highlighted by a pair of news stories this week that indicated such groups may have accessed the United States' electrical grid as well as a dam in New York State.

The Associated Press reported that hackers, possibly from Iran, had opened a pathway into the nation's power grid and taken passwords and schematic drawings enabling a strong follow-up attack. In addition, another group, again possibly Iranian, may have attempted to gain access to a dam located in New York. While there was no sign a breach took place, this incident was described as a probe of the dam's defenses, according to The Wall Street Journal.

American infrastructure cybervulnerabilities again in the spotlight and changes need to be made to protect the system.

Report: 1,700 malware-infected mobile devices per company connect to networks

Share this content:

A new study demonstrates the prevalence of many data breaches caused by employee mobile devices. The report, conducted by The Ponemon Institute and Lookout, polled 588 information technology and security professionals at Global 2,000 companies, and found that the economic risk of mobile breaches can be as high as $26.4 million.

The report also noted a startling gap between the information that employees say they have access to on their mobile devices, compared to the information that IT security pros believe they can access on their devices.

A new report demonstrates the prevalence of data breaches caused by employee mobile devices.

Lethal smart device hack possible, nastier online blackmail in 2016: Trend Micro

Share this content:

A potentially fatal hack of a smart device, a change in tactics for ransomware attacks, and more destructive hacktivist attacks will be in the mix, according to the good folks at Trend Micro who are not waiting until the end of December to issue their cybersecurity predictions for 2016.

The team, led by Trend Micro Chief Technology Officer Raimund Genes, came up with seven thoughts on what they see as 2016's big cyber issues.

TREND MICRO

Trend Micro's cybersecurity predictions for 2016 foresees events ranging from a smart device hack that leads to fatality to more personalized ransomware attacks.

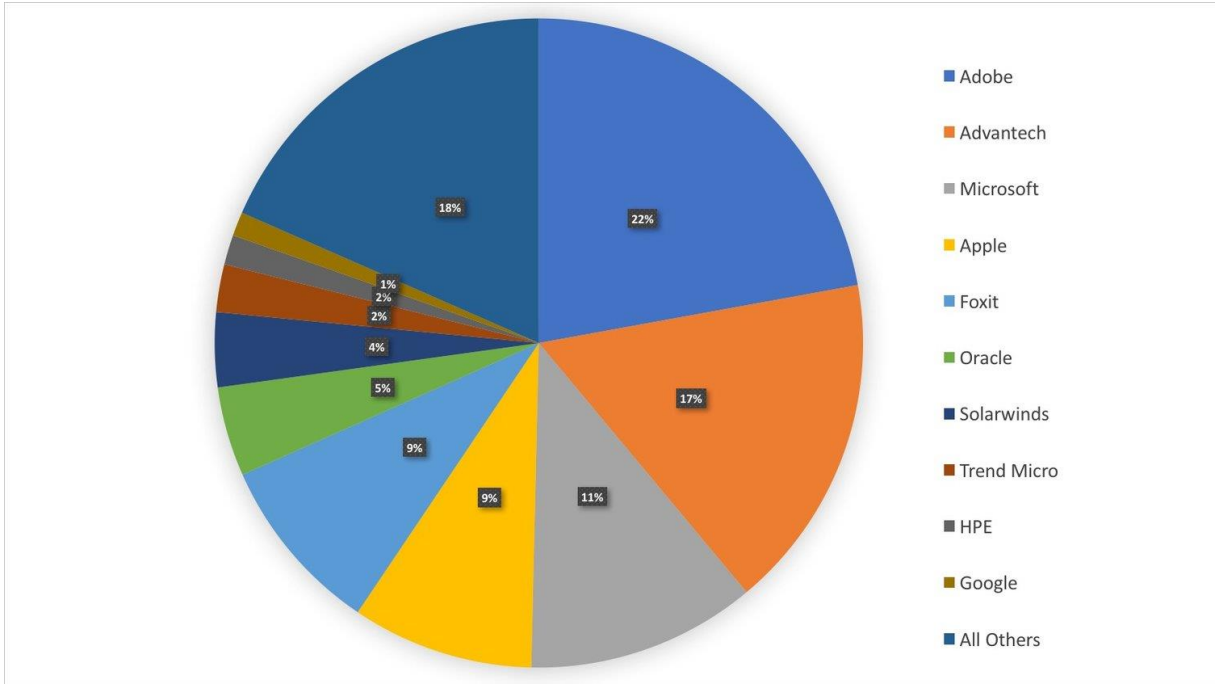
TREND MICRO | ZERO DAY INITIATIVE

2016 Statistics and Trends

Top Vendors
1. Adobe
2. Advantech
3. Microsoft
4. Apple
5. FoxIt

Top Products
1. Advantech WebAccess
2. Adobe Acrobat Reader
3. FoxIt Reader
4. Apple OS X
5. Microsoft Browsers

Totals
700 Bugs Mitigated
433 Pre-disclosure Filters
49 Different Vendors
88 Different Products



ZDI Contributor Rewards Program

For regular contributors, a ‘kicker’ appended to bounty payouts is an added incentive.

The following are the various levels of ZDI Reward membership:

ZDI Reward Points	Status
15,000	ZDI Bronze
25,000	ZDI Silver
45,000	ZDI Gold
65,000	ZDI Platinum

For example, if you have ZDI Platinum status and receive a vulnerability offer of $5,000, then you would receive a payment of $6,000 (25% multiplier) and 10,000 reward points (100% multiplier).

Submitting to the ZDI

Getting started

- Review our Upcoming and Published pages to see what we are buying
- Detail, root cause analysis and/or proving exploitability will increase your payout
- Be mindful! Use encryption!

Do

- What we DO really want to see is bug reports in our queues featuring qualities like:
  - Browser Vulnerabilities (IE/Edge/Chrome/Firefox)
  - Server Side Vulnerabilities (SSH/HTTP/DNS etc..)
  - SCADA
  - VM Escapes (VMware, VirtualBox, Hyper-V etc..)
  - EOP – (Windows Kernel, Linux Kernel, macOS etc..)

Don’t

- We are NOT currently offering on bug reports involving:
  - Non-default configurations
  - Cross-Site Scripting (XSS)
  - DLL planting
  - Denial of Service (DOS)
  - Web-based or online tools
  - ActiveX
  - Post-authentication
  - Most consumer products (widely used security products and some IoT may be the exception)

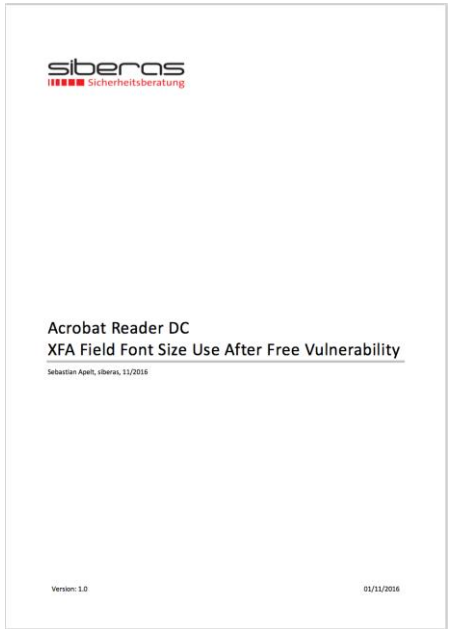
Additional criteria

- RCE/Information Leak/Privilege Escalation
- Latest version of the software
- Latest available supported version of the OS
- Previously unknown

Suggested template

1. Vulnerability Title
   - (e.g. Vendor Product Module Component Vulnerability Type)
2. High-level overview of the vulnerability and the possible effect of using it
3. Root Cause Analysis
   - Detailed description of the vulnerability
   - Code flow from input to the vulnerable condition
   - Buffer size, injection point, etc.
   - Suggested fixes are also welcomed
4. Proof-of-Concept
   - A test case to trigger the vulnerability
   - Optional: exploit code
5. Software Download Link
   - For vetting purposes
6. Optional: Detection Guidance
   - Identify what the vulnerability looks like across the wire
   - Pinpoint filterable conditions like protocol, ports, URI, buffer lengths, allowed character sets, etc.
   - Identify alternative attack vectors

Sample good submission



Sample poor submission

Average report, average bug, average bounty

The value in the params parameter get used in a SQL query.

```
0:068> du poi(esp+10);
0cfc87c0 "SELECT AVG(NValue) FROM log_14;"
0:068> r
eax=ffffffff ebx=00000001 ecx=00b761b8 edx=00bc07f0 esi=0cfe9cb4 edi=0f04f358
eip=080e8c0e esp=0f04f2e0 ebp=0cfe97e8 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000206
igwebs!IgQueryUserDatabaseEx:
080e8c0e ff2548540f08 jmp dword ptr [igwebs!_imp__IgQueryUserDatabaseEx (080f5448)] ds:0023:080f5448=
{igmgr!IgQueryUserDatabaseEx (00795300)}
```

I have create PoC that abuses the new SQL injection.

1. Create file called test.txt on the c:\ drive with the text HACK in it.
2. Issue this command:

```
http://192.168.252.149:7131/DEM0/getdata?dbgroup=-1&amp;function=sql&amp;name=-6357%27%20OR%203083=3083--
```

3. See response:

```
[{"expr1000":"76.6742825936255"},{"expr1000":"HACK"}]
```

I submitted now what?

What determines a reports value?

- How much can you expect to be paid for your submission?
- Expect bounty payments will vary by:
  - Vendor/Product desirability/Distribution
  - Criticality/Effect of the vulnerability
  - Quality of the write-up
  - PoC is required, but exploits help!
  - Availability on the market of vulnerability reports in the given product target

Sometimes people are nervous about submitting their findings

- "What happens if we don't accept an offer from ZDI?" is a question we see often from new submitters
- If we reject your report, or if an offer is made and you reject our offer:
  - The report is simply closed: ZDI would not take any action on it and would make no claims to the rights to your research.
- For complete information:
  - https://zerodayinitiative.com/documents/zdi_researcher_agreement.pdf

What to expect from the process

- Acceptance or rejection after vetting
- Case vetting times can vary
- We reply to every submission
- Be credited or be anonymous
- Provide identity documents
- Be paid (in USD, GBP or Euros)
- After your acceptance,
  - Templating
  - Disclosure

What to expect from the vendor

- ZDI reports receive higher priority with some vendors If the vendor has questions about the report, they will contact ZDI and ZDI will ensure they are answered
- Almost all vendors give credit to finders
- Not all vendors are CNAs to assign CVEs
- Our focus is not to shame nor punish a vendor

What to expect as a vendor

- Vendors should expect a thoroughly detailed report including:
  - Affected product/version
  - Proof-of-concept
  - Analysis
  - Steps to reproduce
  - CWE, CVSS
  - Clear expectations regarding timeliness
  - Support in reproducing

Patch cycles

- What is typical?
- While we see patches from some vendors every month,
- *90 day sustaining cycles are typical
- But what happens if you miss your flight?

So, you want to publish, but you sold your report for a bounty…

- When you sell your research you have sold the rights
- To publish about it, you need permission
- We would like to see what you intend to publish
- To date, we have never declined

Pwn2Own

Pwn2Own

- So, as you become a more experienced vulnerability researcher, consider Pwn2own as place to really showcase your skills and earn more money!
- **Pwn2Own** is a white hat hacking contest hosted by ZDI and held annually at the CanSecWest and PacSec security conferences
- ZDI typically gives away a several hundred thousand dollars in prize monies. Last Pwn2Own, we paid out $833,000!

Pwn2Own

- Individual researchers used to make up the majority of entries, but for the last few years, teams make up the majority of entries
- This has made for more aggressive competition
- Recently, we have seen teams filing bug reports with vendors prior to the contest in the hopes of disqualifying competitor's exploits
- An independent researcher must sort all aspects of the vulnerability chain on their own
- It is not unusual for successful contestants to see a few job offers after P2O - *Wins at Pwn2Own don't exactly make a career, but it certainly highlights talent and solidifies reputations*

Pwn2Own Targets and Awards

- **Virtual Machine Escape (Guest-to-Host)**
  - VMware Workstation [$100,000]
  - Microsoft Hyper-V [$100,000]
- **Local Escalation of Privilege**
  - Microsoft Windows 10 [$30,000]
  - Apple macOS [$20,000]
  - Ubuntu Desktop [$15,000]
- **Web Browser and Plugins**
  - Microsoft Edge [$80,000]
  - Google Chrome [$80,000]
  - Mozilla Firefox [$30,000]
  - Apple Safari [$50,000]
  - Adobe Flash in Microsoft Edge [$50,000]
- **Enterprise Applications**
  - Adobe Reader [$50,000]
  - Microsoft Office Word [$50,000]
  - Microsoft Office Excel [$50,000]
  - Microsoft Office PowerPoint [$50,000]
- **Server Side**
  - Apache Web Server on Ubuntu Server [$200,000]

TREND MICRO | ZERO DAY INITIATIVE

Winning!

- It used to be that one vulnerability could be used to exploit common software, but mitigations have made it harder
- It is typical to see a vulnerability chain used to exploitation

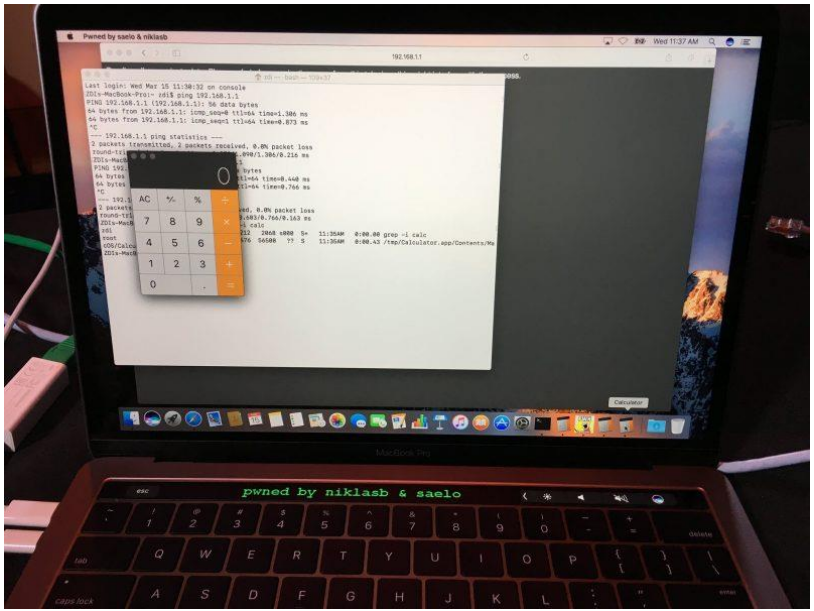
- Last Pwn2own, we bought 51 bugs!
- We love to be impressed!:
  - We saw a Microsoft Edge to VMWare escape that was only 3 vulnerabilities, a very smooth chain…

Master of Pwn “ridiculous smoking jacket”

TREND MICRO | ZERO DAY INITIATIVE

Spring Pwn2Own 2017 - Results

- Spent $833,000 total on
  - 20 Microsoft bugs
  - 20 Apple bugs
  - 6 Adobe bugs
  - 3 VMware bugs
  - 1 Linux kernel bug
  - 1 Mozilla bug



Due to considerable visibility…

- And demonstrated exploitability…
- Pwn2Own bugs are generally fixed by vendors very quickly
- Most were patched within a month
- All were patched within the allotted 120-days

Questions?