Trend Micro™

ZERO DAY INITIATIVE™

Promoting coordinated vulnerability disclosure through the world's largest vendor-agnostic bug bounty program

There remains a perception by some in the information security industry that vulnerability researchers are malicious hackers looking to do harm. While there clearly are skilled malicious hackers out there, they represent a very small minority of the total number of people who actually discover new software flaws. In reality, the number of benevolent researchers with the expertise required to discover a software vulnerability is a sizeable group, and it is not uncommon for them to stumble onto a new flaw while doing their day-to-day security work.

According to Gartner, *"IPS vendors should have an R&D capability to perform primary threat, vulnerability and other threat research. This is a critical underpinning capability that enables vendors to fully understand the science of vulnerability exploitation and, therefore, address threats for your organization in a meaningful way. One method that can be used to judge vendors is the ability to provide better than same-day coverage, which is underpinned by investing in research."*[1]

While Trend Micro™ TippingPoint™ has its own world-class security research organization via Digital Vaccine® Labs (DVLabs), it made sense to augment DVLabs with additional zero-day research from Trend Micro Research, our global network of "extended researchers". Our approach resulted in the formation of the Trend Micro™ Zero Day Initiative™ (ZDI) on July 25, 2005. The main goals of the ZDI are to:

The main goals of the ZDI are to:

- Extend our internal research teams by leveraging the methodologies, expertise, and time of others.
- Encourage the responsible reporting of zero-day vulnerabilities to affected vendors by financially rewarding researchers through incentive programs.
- Protect Trend Micro/TippingPoint customers while the affected vendor is working on a patch.

Key Facts

- Founded in 2005
- Over 10,000 researchers worldwide
- Over 6,500 vulnerabilities discovered and publicly disclosed since inception
- Over 25 million USD paid to researchers to date
- Number one in global vulnerability research and discovery since 2007
- Added Pwn2Own Miami with a focus on ICS/SCADA targets

2019 ZDI Statistics

- Acknowledged on **38%** of publicly discovered **Microsoft® vulnerabilities**
- **#1** external supplier of bugs to Microsoft
- Acknowledged on **57%** of publicly discovered **Adobe® vulnerabilities**
- **#1** external supplier of bugs to Adobe
- **1,045** vulnerabilities published
- **Over 1.5 million USD** awarded to researchers

THE MARKETPLACE FOR VULNERABILITIES

The vulnerability market operates within the security industry as a worldwide marketplace, with buyers, sellers, and supply and demand. Security researchers and hackers now have a multitude of options, unlike in the early days, when hackers traded and sold exploits amongst themselves for eminence, disruption of traditional IT and software development pipelines, and once in a while, for ill-gotten profit.

VULNERABILITY MARKET

Bug bounty programs, hacking contests, and direct vendor communication provide opportunities for responsible disclosure.

GOVERNMENT MARKET

Some legitimate companies operate in a legal grey zone within the zero-day market, selling exploits to governments and law enforcement agencies in countries across the world.

UNDERGROUND MARKET

Flaws can be sold to the highest bidder, used to disrupt private or public individuals and groups.

The ZDI pioneered the vulnerability market, with a focus on disrupting the underground market by legitimately purchasing vulnerability research that can then be disclosed to affected vendors. Vulnerabilities are taken off the market for possible abusers and affected vendors are able to address the vulnerabilities before the information is made public. The ZDI uses incentivized coordinated disclosure to affected vendors to prevent blind-sided attacks on corporate environments.

HOW DOES IT WORK?

While the ZDI conducts its own research internally, the external research community continues to be a valuable asset to the program. The amount offered to a researcher for a particular vulnerability depends on the following criteria:

- Is the affected product widely deployed?
- Can exploiting the flaw lead to a server or client compromise? At what privilege level?
- Is the flaw exposed in default configurations/installations?
- Are the affected products high value (e.g. databases, e-commerce servers, DNS, routers, firewalls, SCADA/ICS, etc.)?
- Does the attacker need to social engineer its victim? (e.g. clicking a link, visiting a site, connecting to a server, etc.)

- Vulnerability submitted: A researcher submits a previously unpatched vulnerability to the ZDI, who validates the vulnerability, determines its worth, and makes a monetary offer to the researcher.
- Vendor notified: The ZDI responsibly and promptly notifies the appropriate product vendor of a security flaw with their product(s) or service(s).
- Digital Vaccine® filter created: Simultaneously with the vendor being notified, TippingPoint works to create a Digital Vaccine filter to protect customers from the unpatched vulnerability.
- Vendor response: The ZDI allows the vendor four months to address the vulnerability.
- Vulnerability is patched or remains unfixed: The vendor will either release a patch for the vulnerability, or indicate to the ZDI that it is unable to or chooses not to patch the vulnerability.
- Public disclosure: The ZDI will publicly and responsibly disclose the details of the vulnerability on its website, in accordance with its vulnerability disclosure policy.

In 2019, through exclusive access to vulnerability information provided by the ZDI, TippingPoint customers were protected **an average of 81 days** before the vendor issued a patch *(that's if the vendor issued a patch at all)*. Customers are protected during any potential exploit campaign that may arise, especially during the initial phase, when it's most likely to affect users. In addition, customers gain control of their patch management life cycle through preemptive coverage for a vulnerability between its discovery and patch availability.

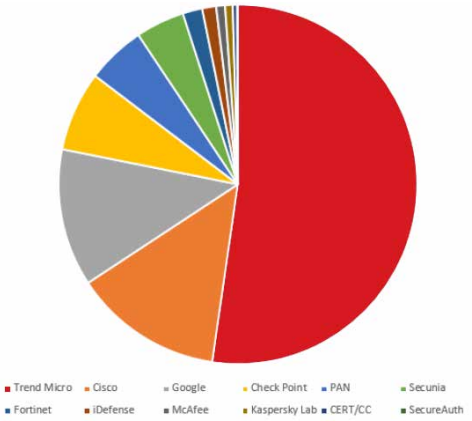
> "Pwn2Own is truly valuable because it shows how different researchers will try to bypass the existing mitigations to create the fully weaponized exploit. That insight into different attack approaches inspires us as vendors to come up with the next generation of defenses."[3]

Peleus Uhley,
Principal Scientist, Adobe Systems

THE LEADER IN GLOBAL VULNERABILITY RESEARCH AND DISCOVERY

Since 2007, Frost & Sullivan has recognized the ZDI as the leading global vulnerability research organization4. For 12 years, Frost & Sullivan gathered public vulnerability data to identify the most reliable vulnerability vendors and research organizations. In 2019, IHS Markit (now OMDIA) took over this research, tracking both software vulnerabilities and the organizations that publicly disclose them.

IHS Markit Vulnerability Disclosure Market 2019



Pwn2Own™

The ZDI has sponsored the Pwn2Own computer hacking contest since 2007. Contestants are challenged to exploit widely-used software and systems with previously unknown vulnerabilities. The Pwn2Own contest serves to demonstrate the vulnerability of devices and software in widespread use, while also providing a checkpoint on the progress made in security since the previous year. 2020 marked the 13th anniversary of Pwn2Own, with 250,000 USD in prizes awarded and the first virtual contest held due to the COVID-19 pandemic.

Pwn2Own™ Tokyo

Pwn2Own Tokyo was born to address the growing attack surface on mobile devices, smart speakers, TVs, and NAS servers. Valuable data that is stored on a mobile device is just as vulnerable to compromise directly by attackers or indirectly by malware, as the data stored anywhere else. Pwn2Own Tokyo shows that vulnerabilities do exist and can be exploited to see the same kinds of resulting compromises and payloads seen on more traditional platforms. The real difference is users don't expect these attacks on mobile platforms or consumer devices, and aren't modifying their behavior accordingly.

HOW DOES THE ZDI BENEFIT TREND MICRO CUSTOMERS?

The vulnerability research and bug bounty program conducted by the ZDI ultimately leads to more secure products and customers. Without the ZDI, many vulnerabilities would continue to either remain behind closed doors, or sold to the underground market and used for nefarious purposes.

- Customers receive preemptive protection ahead of a vendor patch through exclusive access to vulnerability information submitted to the ZDI, as well as added protection for legacy, out-of-support software.
- Our long-standing relationships with leading-software vendors and the research community continue to influence the importance of security in the product development life cycle.

For more information on the ZDI, visit **www.zerodayinitiative.com**

TREND MICRO™

Securing Your Connected World

©2020 Trend Micro Incorporated and/or its affiliates. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners. [OVV01_ZDI_Overview_200914US]

For details about what personal information we collect and why, please see our Privacy Notice on our website at: **https://www.trendmicro.com/privacy**

[1] Gartner, Inc. "Defining Intrusion Detection and Prevention Systems." 20 September 2016.

[2] Omdia report "Quantifying the Public Vulnerability Market" July 2020, https://resources.trendmicro.com/Public-Vulnerability-Market-Report.html

[3] Uhley, Peleus. "Reflections on Pwn2Own." Security @ Adobe (blog), April 16, 2016

[4] Frost & Sullivan Report: Analysis of the Global Public Vulnerability Research Market