The Zero Day Initiative (ZDI) was founded in 2005 to encourage the responsible reporting of zero-day vulnerabilities to affected vendors by financially rewarding researchers through incentive programs. It enables Trend Micro to extend its internal research teams by leveraging the methodologies, expertise and time of external researchers, and protect customers while an affected vendor is working on a patch.

Since 2007, the Zero Day Initiative (ZDI) has been the world's largest bug bounty program and the leader in global vulnerability research and discovery. ZDI's long-standing relationships with software vendors and the research community help influence the importance of security in the product development lifecycle, leading to more secure products and more secure customers.

In the February 2018 report, “Analysis of the Global Public Vulnerability Research Market, 2017,” the Zero Day Initiative was named #1 in vulnerability disclosure. The report covers vulnerabilities that have been disclosed by public vulnerability reporting agencies. In 2017, Trend Micro customers were protected ahead of patch on average 72 days.

**Key Statistics**

- 4,500+ vulnerabilities published since inception
- Over $17 million USD awarded since inception
- 1,522 total number of publicly disclosed vulnerabilities
- 66.3% of the 2017 publicly disclosed vulnerabilities were discovered by ZDI
- 61% of all reported vulnerabilities were “Critical-severity” (26%) or “High-severity” (35%)
- 67.8% of the 929 vulnerabilities categorized as “Critical-severity” and “High-severity” were disclosed by ZDI
- 66% of the 624 vulnerabilities across the top three application classes were disclosed by ZDI
- 64.5% of the 574 vulnerabilities across the top three flaw types were disclosed by ZDI
- 1,009 vulnerabilities published in 2017
- 72 days average preemptive protection for Trend Micro customers ahead of vendor patch in 2017
- Top provider of vulnerabilities to ICS-CERT, Adobe and Microsoft

**Process**

1. An unpatched vulnerability is submitted to ZDI for validation and purchase.
2. ZDI allows the vendor four months to address the vulnerability.
3. The vendor either releases a patch or indicates to ZDI that the vulnerability will not be patched.
4. ZDI will publicly and responsibly disclose the details of the vulnerability online simultaneously. Trend Micro creates a security filter to protect customers from the unpatched vulnerability.
5. ZDI responsibly and promptly notifies the vendor of the vulnerability found in their product.

**Without ZDI,**

many vulnerabilities would continue to remain behind closed doors, or sold to the black market and used for nefarious purposes.

**With ZDI,**

security research and development help influence the importance of security in the product development lifecycle, leading to more secure products and more secure customers.