Project Zero

Make 0day Hard

The mission statement:

Make 0day hard.

The Project Zero team:

Attack research.

Vulnerability research
Exploit development
Exploit mitigations
In public

The philosophy:

Offense guides defense.

Good defense makes offense more costly.

Why?

- Private exploit markets exist. Software exploits are bought and sold for offensive purposes.
- Proactive efforts to make this harder were limited.
- Let's try to do something to protect Google, our partners, and our users.

How?

- First and foremost, devise a technical strategy:
  - Give defenders relevant and actionable information about offense
  - Disrupt private offensive research through specific collisions and incremental increases in attack research difficulty
- But also: challenge outdated policy and process norms.

Technical Strategy

Eliminate low-hanging fruit

- utilize machine resources
- bring an end to dumb-fuzzing
- incrementally improve fuzzing state-of-the-art

Last step of the bug chain

- find surfaces with high contention
- e.g. kernel, sandbox
- use all means possible to find+fix bugs

Target Selection

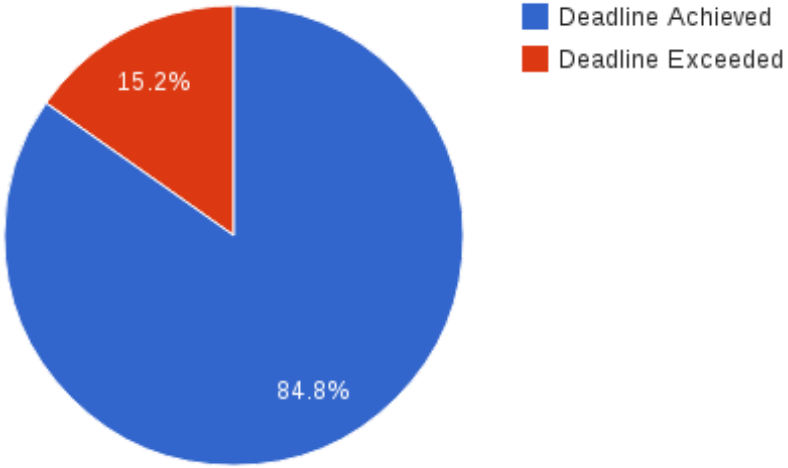
- Balance of:
  - observed attacks
  - external feedback
  - internal deduction

- As of today, we focus heavily on endpoint attacks
  - mobile: android, ios
  - desktop: windows, osx, linux
  - browser: chrome, internet explorer, firefox
  - documents: office, reader

Disclosure Deadlines

- Project Zero uses a 90-day disclosure deadline.
- Disclosure deadlines are a standard industry practice.
- The goal: faster patch response times.
- Our initial results suggest that deadlines are effective.

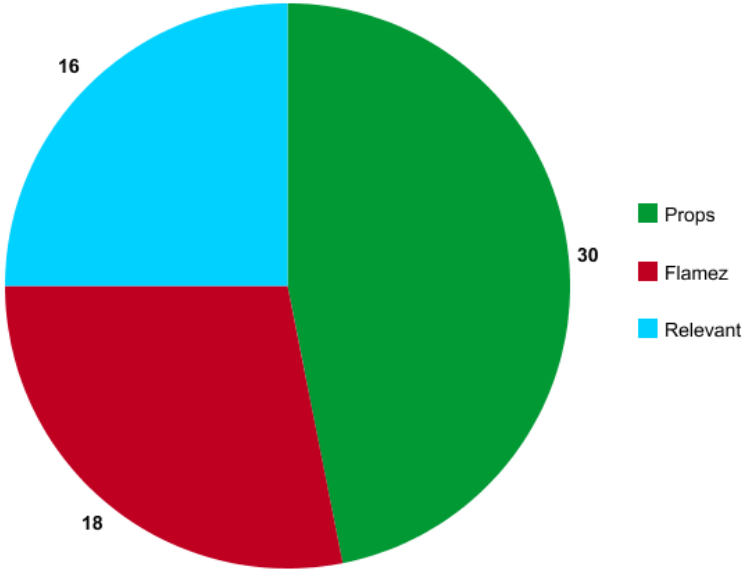
Deadline Statistics



Total bug count: 150+

Google

Feedback Statistics



Deadline Misses

- Disclosure deadlines acknowledge the reality of independent discovery.
- For certain high profile targets, our discoveries are often already known by advanced and stealthy actors.
- Opportunistic reuse of deadline misses is constrained by:
  - the limited window of exposure
  - the higher cost of modern exploit development
  - the nature of the issues we're finding: parts of bug chains

Openness and Transparency

- Great things have been accomplished in public research.
- We want to strengthen and rebuild the community of attack researchers who are working in the open.
- Project Zero provides an attractive alternative to working in the private exploit market.

Final Thoughts

- Project Zero is an ambitious initiative, but the early signs are promising - *"make 0day hard" is achievable as a community.*
- **Researchers**: consider applying a disclosure deadline on your findings.
- **Software vendors**: explore the idea of building an open and transparent attack research team of your own.

Project Zero

http://googleprojectzero.blogspot.com/