Project Zero

Making 0day hard(er)

Industry context

- To understand the formation of Project Zero, we need to understand some industry shifts;
- Not everyone is taking these shifts on board;
- Failure to consider these shifts can result in suboptimal decisions.

Industry context

Observation #1

Offensive security research done in the open is drying up.

Industry context

Observation #2

Targeted attacks using 0-days are on the increase.

Industry context

Observation #3

Mass malware 0-days are getting rare.

Project Zero

The mission statement:

Make 0day hard.

The Project Zero team:

Attack research.

Vulnerability research
Exploit development
Exploit mitigations
In public

Why build this team?

- Provide dream jobs to top-tier offensive security researchers.
- Provide a source of data to the wider defensive community.
- Be a progressive influence on industry wide policies.

How do we make 0-day hard?

- Tweak the economics, lower supply of “good” bugs.
  - Mop up the “obvious” bugs.
  - Bug collision!
  - Provide a better job for the best offensive researchers.
- Invest in mitigations, tooling and scale.
- Force multiplier: sharing data enable other defenders.
- Industry change.

Technical strategy

Eliminate low-hanging fruit

- utilize machine resources
- to bring an end to dumb-fuzzing
- of ubiquitous software platforms

Last step of the bug chain

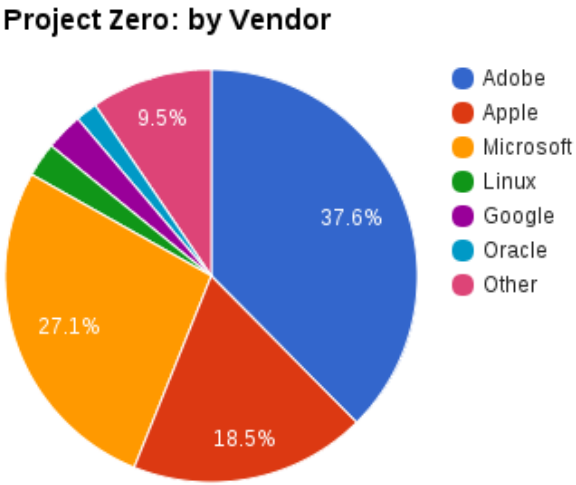
- find surfaces with high contention
- e.g. kernel, sandbox
- use all means possible to find+fix bugs

Target selection

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

- As of today, we focus heavily on endpoint client-side attacks
  - mobile: Android, iOS
  - desktop: Windows, OS X, Linux
  - browser: Chrome, Internet Explorer, Firefox
  - documents: Office, Reader

Results



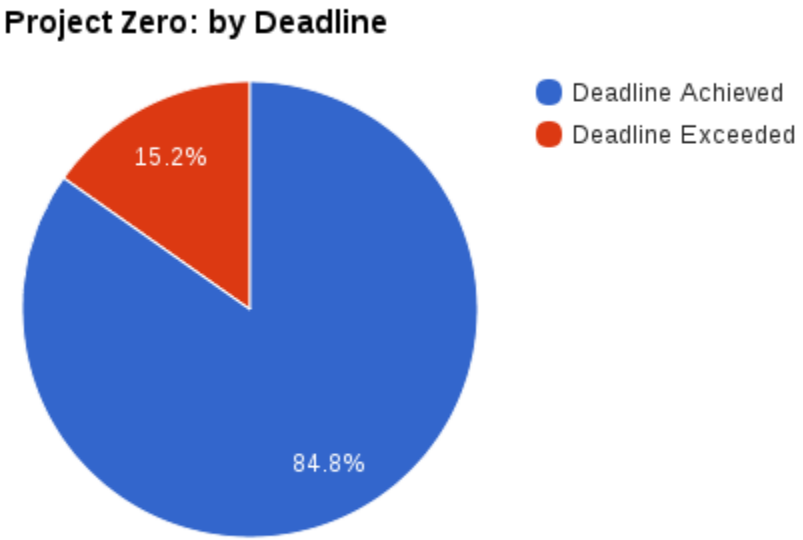
Number of security bugs handled by Project Zero: **427**
Number of blog posts (primarily on vulnerability exploitation) made by Project Zero: **25**

Disclosure deadlines

- Project Zero uses a disclosure deadline.
  - Currently 90 days.
- Starting to become an industry norm.
- The goal: faster patch response times.
  - Acknowledging the reality of independent discovery.
- Results and data suggest deadlines are effective.

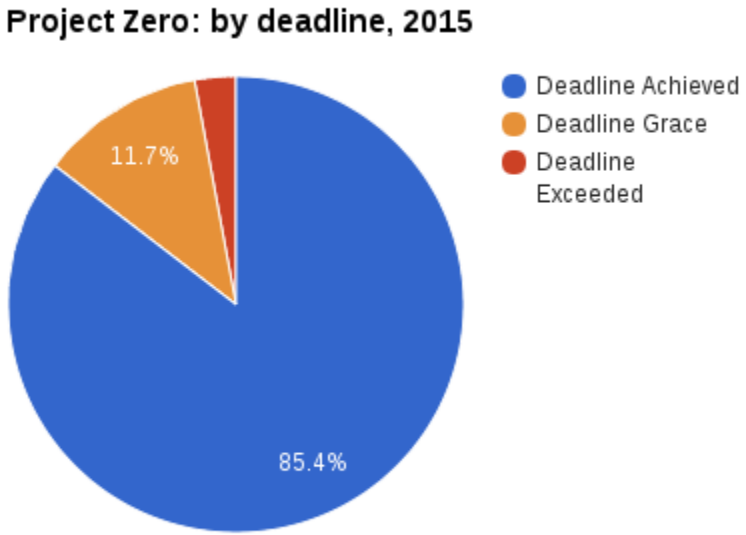
Results: disclosure deadlines

Up to March 2015



Results: disclosure deadlines

All issues filed in 2015



Final thoughts

- **Researchers**: consider applying a disclosure deadline on your findings. Join us under the Project Zero umbrella.
- **Software vendors**: explore the idea of building an open and transparent attack research team of your own.
- **Progressive companies**: consider joining the Project Zero umbrella by spinning up your own teams.

Follow our blog and bug tracker

http://googleprojectzero.blogspot.com/
https://code.google.com/p/google-security-research/

We're hiring!

Questions?