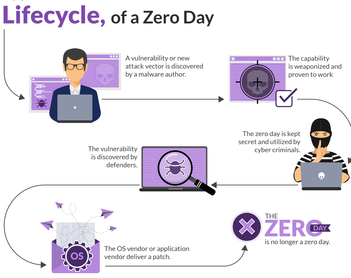
What is a ZERO DAY, REALLY?

The term "zero day" has come to describe one thing: A vulnerability or an attack vector that is known only to the attackers, so it can work without interruption from the defenders. You can think about it is a flaw in a piece of software, or even sometimes hardware.

Typical Lifecycle, of a Zero Day



Responsible Disclosure

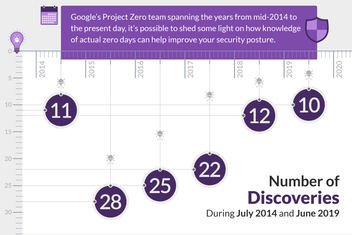
While the technical ability to discover a zero day (some would call it the ability to break things) is quite similar in both scenarios, the first is a crime that can cause huge damage, both financially and to a brand, the latter is the right path to choose.

What is Not A Zero Day

- Malware with an unknown hash or reputation
- Malware that evades legacy AV string-based scans (e.g., 'Yara' rules)
- Attacks against unpatched vulnerabilities

In-the-Wild, Zero Day Attacks

Google's Project Zero team spanning the years from mid-2014 to the present day, it's possible to shed some light on how knowledge of actual zero days can help improve your security posture.



Number of Discoveries
During **July 2014** and **June 2019**

108 ZERO DAY
Exploits discovered between July 2014 and June 2019.

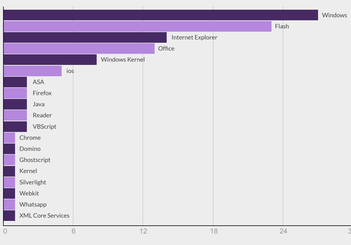
20 ZERO DAY
Exploits are detected in the wild each year, which naturally leads to the question:

- How many go undetected?
- What percentage of the total are being detected?

Assocuation	Actor	Claimed Attributions
Russian-Backed State Actor	APT28/Fancy Bear	10
US-Backed State Actor	Equation Group	8
Private Hack for Sale Firm (disbanded)	Hacking Team	7
Middle East-Backed State Actor	Black Oasis	4
Private Hack for Sale Firm	NSO Group	4
Noth Korean Backed State Actor	APT 37 Scar Cruft	3
Chinese Based Actor	APT 19, APT 3	2

ZERO DAY EXPLOITS
The dataset includes zero day exploits that were either detected in the wild or were found in circumstances where in the wild use is a reasonable inference.

Number of Zero Day by Product



Source: "Google's Project Zero team"

How Can You Protect Against Zero Day Exploits?

E: Ahmed.Sharaf@xband.net or P: (617) 922-6346 Ext. 1

GET OUR FREE DEMO

SentinelOne™