The Zero Days

A zero-day vulnerability is a security flaw in software that is unknown to the software vendor and being actively exploited by attackers before a patch or fix is available

Imagine you have a house with a broken lock on the front door. If a burglar discovers this flaw and breaks in, before you can fix the lock, that would be like a zero-day vulnerability. The burglar is exploiting the vulnerability before you even know about it.

Zero-day vulnerabilities are valuable to attackers because there are no defenses or patches available to protect against them. Vendors need time to analyze the vulnerability, develop a fix, and release it to users. During this window, systems remain exposed to potential attacks.

Some key characteristics of zero-days:

- They are unknown to the vendor and public until disclosed or exploited.
- Attackers like advanced persistent threat (APT) groups reserve zero-days for high-value targets.
- Exploits can fetch millions of dollars on the black market.
- Antivirus and intrusion detection systems struggle to detect zero-day attacks

There are many zero days brokers and marketplaces where zero days are being sold to nation state actors, governments and private corporations. Not all of them are in the Dark Net, some are on the surface web too and can be easily accessible but the price is not affordable for an average andy.

Zerodium - https://www.zerodium.com/program.html

0day - https://0day.today/

In short, if you have a zero day of a particular software let say Android 13. Then, you can hack all the android phones running with that particular version. Even if it is latest one with all the security features and whatever sugarcoating they use in the name of security. Until the bug is there and not reported to the vendor, it is a zero day and it cannot be stop.

While zero-days are difficult to prevent, staying vigilant and patching systems quickly can help reduce the window of exposure when they are discovered. Vendors also work with security researchers to identify and fix zero-days before they are exploited in the wild.
