**Zero-day Attack**  
A zero-day attack takes advantage of a flaw in software, hardware, or firmware that the maker doesn't know about. Zero-day means developers have no time to fix the flaw before it's used in an attack. These attacks are especially dangerous because they're unexpected and there's no quick way to defend against them.

**How It Works**

1. **Vulnerability Discovery**: Attackers find an unknown flaw in software.
2. **Exploit Creation**: They develop a method to take advantage of this flaw.
3. **Attack Execution**: The exploit is deployed, often without detection.
4. **Impact**: The consequences can range from data theft to full system compromise.

**Examples**

* **Stuxnet (2010)**: Targeted Iran's nuclear facilities using multiple zero-day exploits.
* **WannaCry (2017)**: Leveraged the EternalBlue exploit to spread ransomware globally

**Defending Against Zero-Day Attacks**

* **Patch Management**: Regularly update systems to close known vulnerabilities.
* **Behavioral Analytics**: Use tools that detect unusual activities.
* **Security Training**: Educate users to recognize phishing and other attack vectors.

Zero-day attacks are hard to defend against due to their unknown nature and the sophistication of attackers. Organizations must employ proactive and layered security strategies to mitigate risks.