

Zero-Day Attack

A **Zero-Day Attack** occurs when a **zero-day vulnerability** (a security flaw unknown to the vendor) is **exploited by attackers before a patch or fix is available**.

- These attacks are highly dangerous because defenders (vendors, security teams) have **zero days to prepare or protect systems** from the exploitation.



How a Zero-Day Attack Works:

Vulnerability Exists

A flaw or bug in software/hardware exists but is unknown to the vendor.

Attacker Discovers It

Cybercriminals or malicious hackers identify the flaw before it becomes public.

Attack Launched

The attacker exploits this vulnerability to carry out malicious actions like:

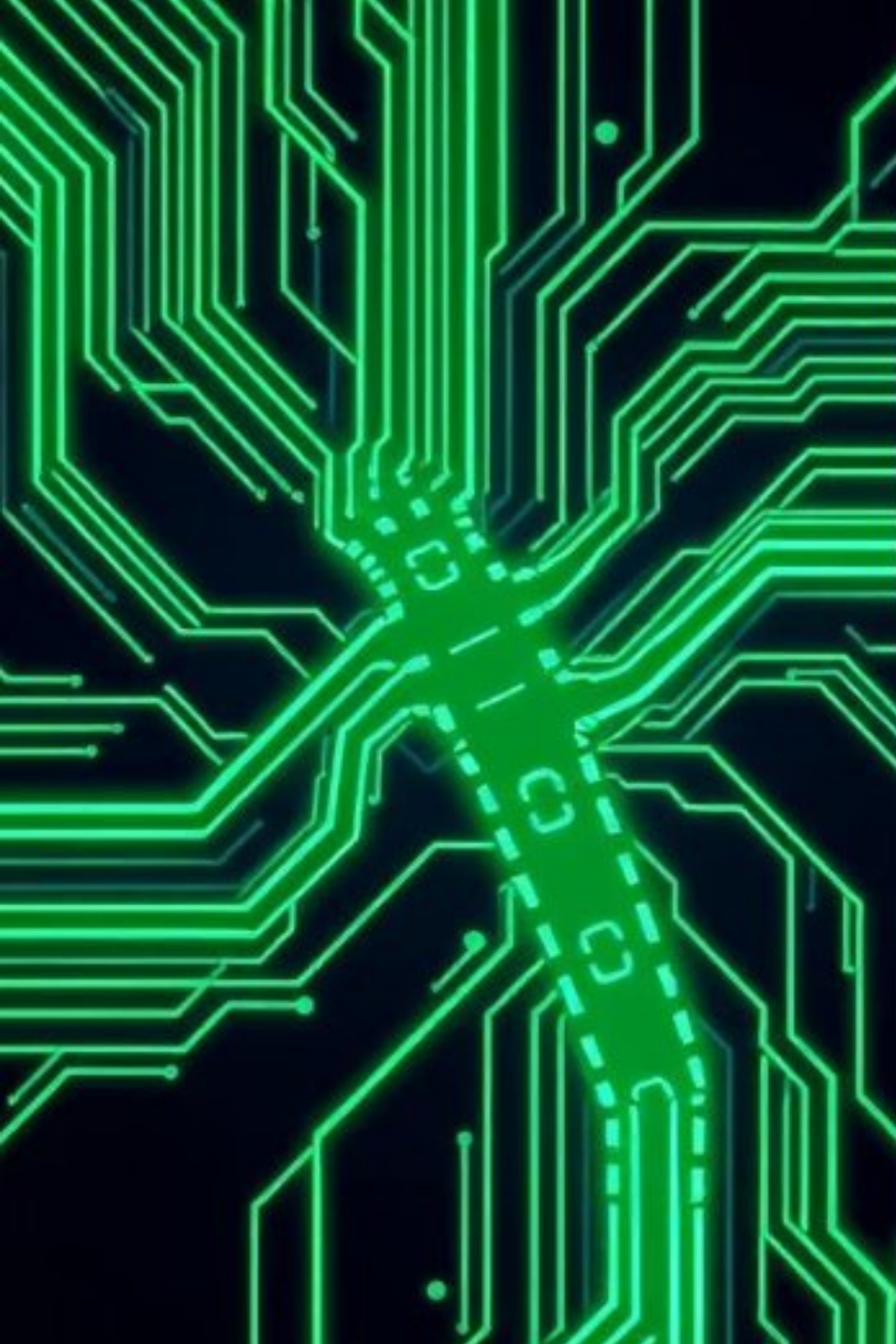
- **Stealing data**
- **Installing malware or ransomware**
- **Gaining unauthorized access or control**

Detection/Disclosure

The attack is discovered either due to security monitoring, breaches, or ethical research.

Patch Released (Post-Attack)

Vendor develops and releases a patch **after the damage may have already occurred.**



Example of Zero-Day Attack:

- **Stuxnet (2010):** One of the most famous zero-day attacks, which exploited multiple unknown Windows flaws to damage Iranian nuclear facilities.
- **2025 WebDAV Exploit (CVE-2025-33053):** Used in the wild before Microsoft patched it in Patch Tuesday June 2025 – APT groups used it for remote code execution on Windows systems.



Mitigation Strategies:

- ☐ Use Zero Trust Architecture.
- ☐ Enable behavior-based intrusion detection systems (IDS/IPS).
- ☐ Subscribe to threat intelligence feeds for early warnings.
- ☐ Apply virtual patching via Web Application Firewalls (WAFs) where possible.

Why Zero-Day Attacks are Dangerous:

No Patch Available	Systems remain unprotected until vendor response.
High Success Rate	Traditional defenses (antivirus, firewalls) often can't detect it.
Often Used by APT Groups	State-sponsored or highly skilled attackers target critical infrastructures.