Anatomy of a Cyberattack

How Modern Cyberattacks Unfold

Cyberattacks rarely happen in a single moment. Most follow a predictable sequence of steps. Understanding these stages helps understand why gaps tend to exist in standalone situations.

1

Reconnaissance

Attackers start by learning about the organization. They look into employees, examine exposed systems, and search for weak points they might exploit.

2

Weaponization

Malicious tools are prepared to exploit weaknesses. Attackers may craft phishing emails, malware, or scripts designed for the specific target.

3

Delivery

The attack is delivered to the victim. This often happens through phishing emails, compromised websites, malicious downloads, or stolen credentials.

4

Installation

Malware installs itself and establishes persistence, allowing attackers to maintain access within the environment.

5

Attack

Once inside, attackers move toward their goal. This may include stealing data, encrypting systems, disrupting operations, or accessing sensitive information.

How a Full Solution Responds at Each Attack Stage

Protection Across the Entire Attack Lifecycle

Attackers move fast, often advancing through several stages before organizations detect the threat. Real Bytes delivers expert-led security through SentinelOne Wayfinder, helping organizations detect suspicious activity earlier, investigate threats faster, and respond with confidence when it matters most.

Security Professionals Monitoring Your Environment at Every Stage

Technology can detect suspicious activity, but investigation and response still require human expertise.

Reconnaissance

1

Threat Intelligence + Threat Hunting

Security analysts use AI-driven insights to hunt for suspicious behavior and indicators of compromise. This helps surface signs of attacker activity before access is attempted.

Weaponization

2

AI-Powered Endpoint Protection

As attackers build their weapons, AI-driven protection works continuously in the background, recognizing and blocking threats before they ever reach the environment.

Delivery

3

Endpoint Detection and Response

As the attack arrives, EDR identifies the threat at the device level and takes immediate action to prevent it from executing and spreading further.

Installation

4

Managed Detection and Response

If something slips through and begins to install, MDR analysts investigate the activity, validate the threat, and take immediate action to remove it before it can establish a lasting presence.

Attack

5

SOC + Breach Response Warranty

If an attacker achieves their objective, expert SOC analysts move quickly to contain and recover, with breach warranty coverage in place to offset the financial impact on the business.

http://realbytes.au

REAL BYTES