



Inside a Cyber Attack: Key Phases and Business Impact

RECONNAISSANCE




The attacker gathers detailed information about your business to identify vulnerabilities. This involves scanning for weak points and obtaining network credentials from stealer logs and combolists. These credentials enhance the attacker's ability to breach your network. This preparation allows for an effective strategy, putting your business at risk. This stage can take from hours to days, depending on the attacker's skills and abilities.

INITIAL BREACH




The attacker gains unauthorized access to your network, often through phishing, exploiting vulnerabilities, or using stolen credentials. This initial breach compromises sensitive data and systems, giving the attacker a foothold in your network. The breach can occur in minutes or seconds, especially if known vulnerabilities are involved, allowing the attacker to set up further exploitation.

MALWARE INSTALLATION/SPREAD




Once inside, the attacker installs malware, such as ransomware or spyware, which spreads through your network. This malware targets critical systems and data, causing significant disruption by encrypting files or stealing information. The malware's spread can take hours to days, depending on its type and how it propagates within your network.

COMMAND & CONTROL (C2) COMMUNICATION




The malware establishes a connection with the attacker's command and control server, sending stolen data or receiving further instructions. This communication allows the attacker to control infected systems, escalate the attack, or demand ransom. C2 communication can occur in real-time or over days, depending on the attack's complexity.

DISCOVERY & INITIAL RESPONSE



Unusual activity, such as slowdowns or encrypted files, prompts an investigation by your IT team. This discovery leads to immediate action to understand the breach, often resulting in system downtime and financial losses. Discovery usually happens within hours to a day after the attack begins, based on monitoring capabilities.

CONTAINMENT, ERADICATION & RECOVERY



Your IT team works to contain and remove the malware, restore systems from backups, and strengthen security measures. This stage involves isolating affected systems and analyzing the attack to prevent future incidents. Recovery can take days to weeks, depending on the attack's severity and response effectiveness, leaving your business dealing with downtime and potential data loss.

To effectively combat cyber threats, it's crucial to be well-prepared for every stage of a potential attack. Proactive measures and a robust incident response plan are essential to minimizing impact and safeguarding your organization. Ensure your cybersecurity strategy is up to date by assessing current practices and seeking expert guidance or resources. By staying vigilant and prepared, you can better protect your business from the evolving landscape of cyber threats.

If you don't know about a threat, you cannot act. SOS Intelligence can be your eyes and ears on the dark web, providing digital risk monitoring to make sure you have the right intelligence, when you need it, to take action to protect your business. Find us at [sosintel.co.uk](https://www.sosintel.co.uk), where you can review our products and request a free demonstration of our services.