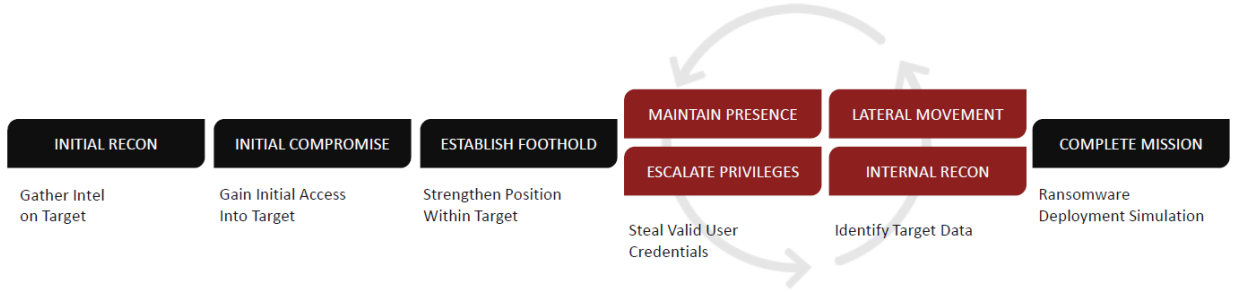
Mandiant

TARGETED ATTACK LIFECYCLE

Cyber attackers are strategic and methodical. They know their mission and they set forth to carry out their attacks in a sequential way in the hopes of going undetected. This predictable sequence of events is the targeted attack lifecycle. As an organization, it is crucial to protect your critical data and cyber assets from all threat actors throughout every stage of the targeted attack lifecycle.

Mandiant experts use their deep knowledge of attackers and the targeted attack lifecycle, combined with an understanding of your unique environment, to determine the preventative measures you need to take throughout the various stages described below.

Mandiant's depiction of the targeted attack lifecycle illustrates the major phases of a typical intrusion. While not all attacks follow the exact flow of this model, the chart below provides a visual representation of the common attack lifecycle.



- **Initial Reconnaissance**: In this stage, the attacker researches the targeted company's systems and employees and outlines a methodology for the intrusion. The attacker may also search for infrastructure that provides remote access to an environment or look for employees to target for social engineering attacks.
- **Initial Compromise**: Here, the attacker successfully executes malicious code on one or more corporate systems. This usually occurs as the result of a social engineering attack or exploitation of a vulnerability on an Internet-facing system.
- **Establish Foothold**: Immediately following the initial compromise, the attacker maintains continued control over a recently compromised system. Typically, the attacker establishes a foothold by installing a persistent backdoor or downloading additional utilities to the compromised system.
- **Escalate Privileges**: At this stage, the attacker obtains further access to corporate systems and data within the environment. Attackers often escalate their privileges through credential harvesting, keystroke logging, or subversion of authentication systems.
- **Internal Reconnaissance**: Next, the attacker explores the organization's environment to gain a better understanding of infrastructure, storage of information of interest, and the roles and responsibilities of key individuals.
- **Lateral Movement**: The attacker uses accounts obtained from the "Escalate Privileges" phase and moves laterally to additional systems within the compromised environment. Common lateral movement techniques include accessing network file shares, remote execution of commands, or accessing systems through remote login protocols such as Remote Desktop Services (RDS) or secure shell (SSH).
- **Maintain Presence**: The attacker ensures continued access to the environment by installing multiple variants of backdoors or by accessing remote access services such as the corporate virtual private network (VPN).
- **Complete Mission**: The attacker accomplishes the objectives of the intrusion such as stealing intellectual property, financial data, mergers and acquisition information, or personally identifiable information (PII). In other cases, the objective of the mission might be a disruption of systems or services or destruction of data within the environment.

Understanding the steps attackers take is important to establish a plan to prevent such attacks and mitigate risks.

Mandiant

Understanding the stages of a targeted attack lifecycle is the first step. To help ensure your organization is prepared and able to prevent attacks, turn to Mandiant's team of experts as your partner in cyber-readiness.