Resource Development

In the attack structure, resource development is **a preparatory phase where attackers gather or create the tools, infrastructure, and credentials needed for an attack**. This phase equips attackers with the resources necessary to initiate and sustain their operation. Here’s a look at specific tactics within resource development, including **getting infrastructure**, **building malware**, and **compromising accounts**.

1. Get Infrastructure (via Compromise or Otherwise)

- Definition: Attackers acquire the physical or virtual infrastructure needed to carry out their attack. This infrastructure **can include compromised servers, domain names, IP addresses, and cloud resources**.
- Methods:
  - **Compromised Infrastructure**: Attackers may hack into servers or devices that are already online and repurpose them for command-and-control (C2), phishing, or hosting malicious files.
  - **Purchased Infrastructure**: Some attackers rent or buy infrastructure like VPS servers, domain names, or cloud services to set up an attack infrastructure that appears legitimate and is harder to track.
- Security Implications: Attackers using compromised or rented infrastructure can blend in with legitimate services, making it harder for defenders to detect malicious activity or trace the infrastructure back to the attackers.

2. Build Malware

- Definition: Attackers develop or modify malicious software to accomplish specific tasks, such as stealing data, encrypting files, or maintaining persistence on a network.
- Malware Types:
  - Custom Malware: Skilled attackers or groups may build tailored malware with unique code to avoid detection by traditional antivirus solutions.
  - Modified Open-Source Malware: Some attackers use or modify publicly available malware to meet their needs, adding features or altering signatures to evade detection.
- **Common Malware Features**:
  - **Persistence**: Ensures the malware remains active even after system reboots.
  - **Stealth**: Uses techniques to evade detection, such as encryption, packing, or code injection.
  - **Command-and-Control (C2)** Communication: Malware often includes C2 capabilities, allowing attackers to control infected systems remotely.
- Implications for Forensics: Custom-built malware may leave unique traces that can help identify its creator or origin, while modified malware can often be detected by comparing it with known malware signatures.

3. Compromise Accounts

- Definition: **Attackers obtain access to user accounts, giving them legitimate credentials that they can use to avoid detection when accessing systems or data**.
- Methods:
  - **Credential Theft**: Attackers may use techniques like **phishing, keylogging, or stealing cached credentials** to obtain usernames and passwords.

    - **Credential Stuffing**: Attackers **test large volumes of stolen credentials from data breaches**, hoping some will match accounts on the target’s systems.
    - **Brute Force**: Attackers repeatedly attempt to guess weak passwords, often targeting accounts with default credentials or simple passwords.
- Implications for Security: Compromised accounts allow attackers to operate under legitimate identities, making it difficult to distinguish between normal and malicious activity. Privileged accounts, if compromised, give attackers broad access, increasing potential damage.

Summary

- **Getting Infrastructure** provides attackers with the necessary hosting resources, either by compromising existing servers or purchasing new infrastructure, to support an attack campaign.
- **Building Malware** allows attackers to develop or customize malicious code tailored for their specific objectives, such as data exfiltration or C2.
- **Compromising Accounts** gives attackers access to legitimate user credentials, helping them bypass security controls and maintain persistence within a network.

By understanding these tactics, defenders can better anticipate the resource preparation phase and implement countermeasures, such as monitoring for unusual infrastructure acquisition and implementing multi-factor authentication to protect accounts.