Mitre att&ck

Index

Reconnaissance

#MITRE/1-Reconnaissance

- *Gather info* they can use to plan future operations
- techniques that involve active or passive gathering info that can be used to support targeting.
- info includes details of the victim like
  - org
  - infrastructure
  - staff/personnel

Resource Development

#MITRE/2-Resource-Development

- Adversary trying to *establish resources* they can use to support operations.
- techniques that involve creating, purchasing, or compromising/stealing resources that can be used to support targeting.
- Such resources include infrastructure, accounts, or capabilities.

Initial Access

#MITRE/3-Initial-Access

- The adversary is trying to *get into your network*.
- exploiting weaknesses on public-facing web servers.
- Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Execution

#MITRE/4-Execution

- The adversary is trying to *run malicious code*.
- adversary-controlled code running on a local or remote system.
- Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data.
- For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

In Remote System Discovery, the adversary might be interested in obtaining information such as:

1. **System Names and IP Addresses:** Identifying what systems are present on the network.
2. **System Configuration:** Gathering details about the configuration of remote systems, including operating system version, installed software, and system settings.
3. **Network Topology:** Understanding how systems are interconnected within the network.

Persistence

#MITRE/5-Persistence

- The adversary is trying to *maintain their foothold*.
- Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
- Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

Privilege Escalation

#MITRE/6-Privilege-Escalation

- The adversary is trying to *gain higher-level permissions* on a system or network.
- often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives.

- Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include:
  - SYSTEM/root level
  - local administrator
  - user account with admin-like access
  - user accounts with access to specific system or perform specific function

---

Defense Evasion

#MITRE/7-Defense-Evasion

- The adversary is trying to *avoid being detected*.
- Techniques that adversaries use to avoid detection throughout their compromise.
- Techniques used for defense evasion include
  - uninstalling/disabling security software
  - obfuscating/encrypting data and scripts.
  - leverage and abuse trusted processes to hide and masquerade their malware.

Credential Access

#MITRE/8-Credential-Access

- The adversary is trying to *steal account names and passwords*.
- Techniques used to get credentials include
  - keylogging or credential dumping.
- Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Discovery

#MITRE/9-Discovery

- The adversary is trying to *figure out your environment.*
- To gain knowledge about the system and internal network.
- Adversaries observe the environment themselves before deciding how to act.
- Explore what they can control and what's around their entry point in order to discover how it could benefit their current objective.
- Native operating system tools are often used toward this post-compromise information-gathering objective.

Lateral Movement

#MITRE/10-Lateral-Movement

- The adversary is trying to *move through your environment*.
- use to enter and control remote systems on a network.

Collection

#MITRE/11-Collection

- The adversary is trying to *gather data of interest* to their goal.
- Frequently, the next goal after collecting data is to steal (exfiltrate) the data.
- Common target sources include
  - various drive types,
  - browsers,
  - audio,
  - video,
  - email.
- Common collection methods include capturing screenshots and keyboard input.

Command and Control

#MITRE/12-Command-and-Control

- The adversary is trying to *communicate with compromised systems* to control them.
- use to communicate with systems under their control within a victim network.
- Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.
- Many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

Exfiltration

#MITRE/13-Exfiltration

- The adversary is *trying to steal data*.
- Avoid detection while *removing it*.
- Techniques for getting data out of a target network typically include.
  - Include putting size limits on the transmission.

Impact

#MITRE/14-Impact

- The adversary is trying to *manipulate, interrupt, or destroy your systems and data*.
- Destroying or tampering with data.
- In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals.
