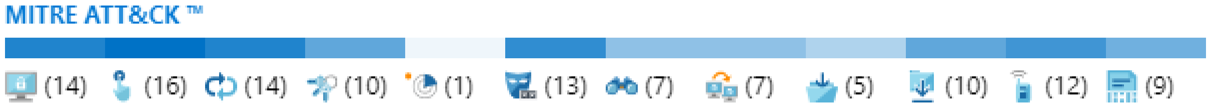
MITRE ATT&CK Framework Reference for Azure Sentinel



•**Initial access**—Techniques used by the adversary to obtain a foothold within a network, such as targeted spear-phishing, exploiting vulnerabilities or configuration weaknesses in public-facing systems.

•**Execution**—Techniques that result in an adversary running their code on a target system. For example, an attacker may run a PowerShell script to download additional attacker tools and/or scan other systems.

•**Persistence**—Techniques that allow an adversary to maintain access to a target system, even following reboots and credential changes. An example of a persistence technique would be an attacker creating a scheduled task that runs their code at a specific time or on reboot.

•**Privilege escalation**—Techniques leveraged by an adversary to gain higher-level privileges on a system, such as local administrator or root.

•**Defense evasion**—Techniques used by attackers to avoid detection. Evasion techniques include hiding malicious code within trusted processes and folders, encrypting or obfuscating adversary code, or disabling security software.

•**Credential access**—Techniques deployed on systems and networks to steal usernames and credentials for re-use.

•**Discovery**—Techniques used by adversaries to obtain information about systems and networks that they are looking to exploit or use for their tactical advantage.

•**Lateral movement**—Techniques that allow an attacker to move from one system to another within a network. Common techniques include "Pass-the-Hash" methods of authenticating users and the abuse of the remote desktop protocol.

•**Collection**—Techniques used by an adversary to gather and consolidate the information they were targeting as part of their objectives.

•**Command and control**—Techniques leveraged by an attacker to communicate with a system under their control. One example is that an attacker may communicate with a system over an uncommon or high-numbered port to evade detection by security appliances or proxies.

•**Exfiltration**—Techniques used to move data from the compromised network to a system or network fully under control of the attacker.

•**Impact**—Techniques used by an attacker to impact the availability of systems, networks, and data. Methods in this category would include denial of service attacks and disk- or data-wiping software.