Obtain Capabilities: Exploits, Sub-technique T1588.005 - Enterprise

Archived: 2026-04-05 15:02:47 UTC

Adversaries may buy, steal, or download exploits that can be used during targeting. An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. Rather than developing their own exploits, an adversary may find/modify exploits from online or purchase them from exploit vendors.[1][2][3]

In addition to downloading free exploits from the internet, adversaries may purchase exploits from third-party entities. Third-party entities can include technology companies that specialize in exploit development, criminal marketplaces (including exploit kits), or from individuals.[4][5] In addition to purchasing exploits, adversaries may steal and repurpose exploits from third-party entities (including other adversaries).[2]

An adversary may monitor exploit provider forums to understand the state of existing, as well as newly discovered, exploits. There is usually a delay between when an exploit is discovered and when it is made public. An adversary may target the systems of those known to conduct exploit research and development in order to gain that knowledge for use during a subsequent operation.

Adversaries may use exploits during various phases of the adversary lifecycle (i.e. Exploit Public-Facing Application, Exploitation for Client Execution, Exploitation for Privilege Escalation, Exploitation for Defense Evasion, Exploitation for Credential Access, Exploitation of Remote Services, and Application or System Exploitation).

Source: https://attack.mitre.org/techniques/T1588/005