CAPEC-270: Modification of Registry Run Keys (Version 3.9)

Archived: 2026-04-06 01:09:15 UTC

Attack Pattern ID: 270 **Abstraction: Detailed**		

Description

An adversary adds a new entry to the "run keys" in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to operate and run on the target system with the authorized user's level of permissions. This attack is a good way for an adversary to run persistent spyware on a user's machine, such as a keylogger.

Likelihood Of Attack

Medium

Typical Severity

Medium

Relationships

This table shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as ChildOf and ParentOf, and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as CanFollow, PeerOf, and CanAlsoBe are defined to show similar attack patterns that the user may want to explore.

Nature	Type
ChildOf	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attac
CanFollow	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attac
CanPrecede	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attac
CanPrecede	D Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific techni
CanPrecede	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attac

This table shows the views that this attack pattern belongs to and top level categories within that view.

View Name	Top Level Categories
Domains of Attack	Software
Mechanisms of Attack	Manipulate System Resources

Execution Flow

Explore

1. **Determine target system:** The adversary must first determine the system they wish to target. This attack only works on Windows.

Experiment

1. **Gain access to the system:** The adversary needs to gain access to the system in some way so that they can modify the Windows registry.

Techniques
Gain physical access to a system either through shoulder surfing a password or accessing a system that is left unlocked.
Gain remote access to a system through a variety of means.

Exploit

1. **Modify Windows registry:** The adversary will modify the Windows registry by adding a new entry to the "run keys" referencing a desired program. This program will be run whenever the user logs in.

Prerequisites

The adversary must have gained access to the target system via physical or logical means in order to carry out this attack.

Consequences

This table specifies different individual consequences associated with the attack pattern. The Scope identifies the security property that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in their attack. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a pattern will be used to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	Impact	Likelihood
Integrity	Modify Data Gain Privileges	

Mitigations

Identify programs that may be used to acquire process information and block them by using a software restriction policy or tools that restrict program execution by using a process allowlist.

Example Instances

An adversary can place a malicious executable (RAT) on the target system and then configure it to automatically run when the user logs in to maintain persistence on the target system.
Through the modification of registry "run keys" the adversary can masquerade a malicious executable as a legitimate program.

Taxonomy Mappings

CAPEC mappings to ATT&CK techniques leverage an inheritance model to streamline and minimize direct CAPEC/ATT&CK mappings. Inheritance of a mapping is indicated by text stating that the parent CAPEC has relevant ATT&CK mappings. Note that the ATT&CK Enterprise Framework does not use an inheritance model as part of the mapping to CAPEC.

Relevant to the ATT&CK taxonomy mapping (also see parent)

Entry ID	Entry Name
1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Start Folder
1547.014	Boot or Logon Autostart Execution: Active

Content History

Submissions		
Submission Date	**Submitter**	**Organization**

2014-06-23 (Version 2.6)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2015-11-09 (Version 2.7)	CAPEC Content Team	The MITRE Corporation
	Updated References	
2018-07-31 (Version 2.12)	CAPEC Content Team	The MITRE Corporation
	Updated Attack_Motivation-Consequences, Attack_Prerequisites, Description Summary, Examples-Instances, Solutions_and_Mitigations, Typical_Likelihood_of_Exploit, Typical_Severity	
2019-04-04 (Version 3.1)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Weaknesses	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Description, Mitigations, Taxonomy_Mappings	
2021-10-21 (Version 3.6)	CAPEC Content Team	The MITRE Corporation
	Updated Description, Execution_Flow, Related_Attack_Patterns	
2022-09-29 (Version 3.8)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	

More information is available — Please select a different filter.
