CAPEC-564: Run Software at Logon (Version 3.9)

Archived: 2026-04-06 01:04:48 UTC

Attack Pattern ID: 564 **Abstraction: Detailed**		

Description

Operating system allows logon scripts to be run whenever a specific user or users logon to a system. If adversaries can access these scripts, they may insert additional code into the logon script. This code can allow them to maintain persistence or move laterally within an enclave because it is executed every time the affected user or users logon to a computer. Modifying logon scripts can effectively bypass workstation and enclave firewalls. Depending on the access configuration of the logon scripts, either local credentials or a remote administrative account may be necessary.

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 attack. It

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	Inject Unexpected Items

Mitigations

Restrict write access to logon scripts to necessary administrators.

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
1037	Boot or Logon Initialization Scripts
1543.001	Create or Modify System Process: Launch Agent
1543.004	Create or Modify System Process: Launch Daemon
1547	Boot or Logon Autostart Execution

Content History

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

2015-11-09 (Version 2.7)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2018-07-31 (Version 2.12)	CAPEC Content Team	The MITRE Corporation
	Updated References	
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 Taxonomy_Mappings	
2020-12-17 (Version 3.4)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	
2021-06-24 (Version 3.5)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	
2022-09-29 (Version 3.8)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	

More information is available — Please select a different filter.
