CAPEC-552: Install Rootkit (Version 3.9)

Archived: 2026-04-06 00:15:27 UTC

Attack Pattern ID: 552 **Abstraction: Detailed**		

Description

An adversary exploits a weakness in authentication to install malware that alters the functionality and information provide by targeted operating system API calls. Often referred to as rootkits, it is often used to hide the presence of programs, files, network connections, services, drivers, and other system components.

Likelihood Of Attack

Medium

Typical Severity

High

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

Prevent adversary access to privileged accounts necessary to install rootkits.

Example Instances

A rootkit may take the form of a hypervisor. A hypervisor is a software layer that sits between the operating system and the processor. It presents a virtual running environment to the operating system. An example of a common hypervisor is Xen. Because a hypervisor operates at a level below the operating system it can hide its existence from the operating system.
Similar to a rootkit, a bootkit is a malware variant that modifies the boot sectors of a hard drive, including the Master Boot Record (MBR) and Volume Boot Record (VBR). Adversaries may use bootkits to persist on systems at a layer below the operating system, which may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

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
1014	Rootkit
1542.003	Pre-OS Boot:Bootkit
1547.006	Boot or Logon Autostart Execution:Kernel Modules and Extensions

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 Description Summary, Examples-Instances, References, Solutions_and_Mitigations, Typical_Likelihood_of_Exploit, Typical_Severity	
2019-04-04 (Version 3.1)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Weaknesses, Taxonomy_Mappings	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	

More information is available — Please select a different filter.
