CAPEC-571: Block Logging to Central Repository (Version 3.9)

Archived: 2026-04-06 01:37:51 UTC

Attack Pattern ID: 571 **Abstraction: Standard**		

Description

An adversary prevents host-generated logs being delivered to a central location in an attempt to hide indicators of compromise.

Extended Description

In the case of network based reporting of indicators, an adversary may block traffic associated with reporting to prevent central station analysis. This may be accomplished by many means such as stopping a local process to creating a host-based firewall rule to block traffic to a specific server.

In the case of local based reporting of indicators, an adversary may block delivery of locally-generated log files themselves to the central repository.

Typical Severity

Low

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	Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or techniqu

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, Communications
Mechanisms of Attack	Manipulate System Resources

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

Entry ID	Entry Name
1562.002	Impair Defenses: Disable Windows Event Logging
1562.002	Impair Defenses: Impair Command History Logging
1562.006	Impair Defenses: Indicator Blocking
1562.008	Impair Defenses: Disable Cloud Logs

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, Typical_Severity	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns, Taxonomy_Mappings	
2022-09-29 (Version 3.8)	CAPEC Content Team	The MITRE Corporation
	Updated Description, Extended_Description, Taxonomy_Mappings	

More information is available — Please select a different filter.
