Revert Cloud Instance (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

An adversary may revert changes made to a cloud instance after they have performed malicious activities in attempt to evade detection and remove evidence of their presence. In highly virtualized environments, such as cloud-based infrastructure, this may be easily facilitated using restoration from VM or data storage snapshots through the cloud management dashboard. Another variation of this technique is to utilize temporary storage attached to the compute instance. Most cloud providers provide various types of storage including persistent, local, and/or ephemeral, with the latter types often reset upon stop/restart of the VM.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
|  | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |

Detection

Establish centralized logging of instance activity, which can be used to monitor and review system events even after reverting to a snapshot, rolling back changes, or changing persistence/type of storage. Monitor specifically for events related to snapshots and rollbacks and VM configuration changes, that are occurring outside of normal activity. To reduce false positives, valid change management procedures could introduce a known identifier that is logged with the change (e.g. tag or header) if supported by the cloud provider, to help distinguish valid, expected actions from malicious ones.

References