Data from VM Local File System (version 1.0)

**Cloud Service Label: IaaS**

**Description**

Sensitive data can be collected from VM local (ephemeral) file systems or resident databases residing on the system prior to Exfiltration.

Adversaries will often search the file system on computers they have compromised to find files of interest. They may do this using a [Command-Line Interface](https://attack.mitre.org/techniques/T1059), such as cmd, which has functionality to interact with the file system to gather information. Some adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

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

Monitor processes and command-line arguments for actions that could be taken to collect files from a system. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) and [PowerShell](https://attack.mitre.org/techniques/T1086).

Reference