Denial of Data (version 1.1)

**Cloud Service Label: IaaS, PaaS, SaaS**

Description

*Destruction*

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives. Common operating system file deletion commands such as del and rm often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from [Disk Content Wipe](https://attack.mitre.org/techniques/T1488) and [Disk Structure Wipe](https://attack.mitre.org/techniques/T1487) because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.

Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable. In some cases politically oriented image files have been used to overwrite data.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [Credential Dumping](https://attack.mitre.org/techniques/T1003), and [Windows Admin Shares](https://attack.mitre.org/techniques/T1077).

*Encrypted for Impact*

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote stores and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted. In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [Credential Dumping](https://attack.mitre.org/techniques/T1003), and [Windows Admin Shares](https://attack.mitre.org/techniques/T1077).

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Ransomware | Attackers with access to a company’s cloud can encrypt or take data and attempt to ransoms it back to the company. |
| Deleting cloud backups | Before releasing Ransomware onto a company’s environment, attackers have been known to delete backups. Thereby making downtime even longer due to organizations not being able to revert to a backup state quickly. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Data Backup | | Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data. In Azure, data backups can be restored from several points in time if corruption makes its way into an automated backup. The Azure Backup service has built in heuristics to detect potentially suspicious activity regarding Backup service commands. Also note that backups stored in different physical locations also mitigates risk against data loss. |
|  | *AWS* | To have a data backup in an AWS environment, AWS Backup can be used. This is a way to centralize and automate backup services, as well as enforce backup policies that might include aspects such as encryption requirements and audit the activity on the backup. The backup service is PCI and ISO compliant and is HIPAA eligible. There are different backups available: cloud-native (across all AWS services) and hybrid (across AWS and on premise data). To accomplish this a backup plan needs to be created that defines criteria on how to manage the backups (ie. how frequently to backup, how long to keep the backups, etc.), then the resources to backup are assigned. Once the resources are backed up they can be minored, modified, or restored. To get started with this information can be found here: [**https://aws.amazon.com/backup/getting-started/**](https://aws.amazon.com/backup/getting-started/)**.** For more information on the service refer here: [**https://aws.amazon.com/backup/**](https://aws.amazon.com/backup/)**.** Access to and introduction video can be found here: [**https://www.aws.training/Details/Video?id=29646**](https://www.aws.training/Details/Video?id=29646)**.** |
|  | *Azure* | To have a data backup in an Azure environment, Azure Backup service can be used. This allows for on-premises, Azure VMs, Azure file shares, SQL server in Azure VMs, and SAP HANA databases in Azure VMs to be backed up. There are multiple ways this can be accomplished; through the portal, PowerShell, CLI, and ARM template. From the portal a VM to be backed up can be selected, then enable to backup resource, start the backup job, monitor the backup job, and when you no longer need the deployment it can then be cleared up. Using PowerShell and CLI has the same steps (just accomplished through different commands) first a recovery service vault will be created, then the backup will need to be enabled for the service being backed up, then the backup job will need to be started, then monitored, and lastly clean up the deployment. Lastly, to deploy with the ARM template first the template has to be reviewed and edited as needed, then deploy the template, then the deployment must be validated by starting a backup job, monitoring it, and cleaning up the resources.  On this page multiple tutorials can be found for backing up specific resources: [**https://docs.microsoft.com/en-us/azure/backup/tutorial-backup-vm-at-scale**](https://docs.microsoft.com/en-us/azure/backup/tutorial-backup-vm-at-scale). Full details on how to deploy backup services utilizing different resources can be found below:  Portal: [**https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal**](https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal)  PowerShell: [**https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-powershell**](https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-powershell)  CLI: [**https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-cli**](https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-cli)  ARM Template: [**https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-template**](https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-template) |

Detection

Use process monitoring to monitor the execution and command line parameters of binaries involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit. Monitor for the creation of suspicious files as well as unusual file modification activity. In particular, look for large quantities of file modifications in user directories. In some cases, monitoring for unusual kernel driver installation activity can aid in detection. In Azure, monitoring for rest commands sent to the Azure API such as:

Delete https://myaccount.file.core.windows.net/myshare/myparentdirectorypath/mydirectory?restype=directory

This can indicate an attempt to delete multiple files. One place this can be observed is in Azure thru the Activity log blade within the Monitor service.

References

1. <https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/> - Accessed 8/13/21