T1583 Access to Cloud Infrastructure or MEC

Description: An adversary may purchase access to cloud infrastructure or Multi-access Edge Computing (MEC) resources that will also be hosting the operator’s infrastructure.

Mobile Network Operators are looking to commercial cloud and MEC providers to deploy 5G Core and RAN functions. Similar resources may also be utilized to offer compute services for time latency sensitive enterprise/user applications. Adversaries may attempt to target victims by creating co-residency in cloud or MEC resources for bridging network, or lateral movements by using software and configuration vulnerabilities. These are sometimes referred to as colocation attacks.

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: resource-development

Metadata:

* Architecture Segment: OA&M, MEC
* Platforms: 5G Network
* Permissions required: None
* Data Sources:
* Theoretical/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Locate cloud resources of target | [2] is a university research showing how an attacker can locate an entity’s systems in the cloud and work to instantiate profiling and other malicious hosts on the same physical platform. |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1030 | Network isolation. Deployment architecture should consider physical and virtual isolation from other tenants |
| M1041 | Any traffic going from a security zone to another security zone must be protected with encryption. Key based user and resource authentication and authorization |
| FGM5504 | Cloud compute, cloud storage and any serverless activity should be isolated from other tenants |
| FGM5505 | Hardware mediated execution environment |

Pre-Conditions

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

Critical Assets

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

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
|  |  |
|  |  |

Post-Conditions

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

References

|  |  |
| --- | --- |
| Name | URL |
| S. Sahoo, S. K. Mishra, B. Sahoo & A. K. Turuk, “*Co-resident Attack in Cloud Computing: An Overview*”, Encyclopedia of Big Data Technologies, March 2018 | https://link.springer.com/content/pdf/10.1007%2F978-3-319-63962-8\_322-1.pdf |
| T. Ristenpart, E. Tromer, H. Shacham, S. Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds”, In CCS '09: Proceedings of the 16th ACM conference on Computer and communications security, November 2009 Pages 199–212 | https://dl.acm.org/doi/10.1145/1653662.1653687 |