Creating a VM instance (version 1.1)

**Cloud Service Label: IaaS**

Description

It may be possible for an adversary to steal credentials that allow him to create IaaS assets like VM’s without granting him access to a user’s data sources or security services. However, by creating a VM inside a user’s account an adversary may be able to use the new VM as a means of achieving those accesses. New VM’s may be created with default IAM roles or be permitted through firewalls based on their presence within an existing VPC or virtual network.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Co-residence identification | As pointed out in a research paper written by the University of CaIifornia San Diego and the Massachusetts Institute of Technology, massive or targeted generation of VM instances could be used to identify a specific availability zone for a target cloud instance. EC2 instances in AWS utilize the Xen hypervisor, and identifying the privileged virtual machine (Domain0 or Dom0) can help determine physical co-residence location. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Adhere to zero trust policies | Inspect hosts for listening ports that are unexpected. |
| Prevent traceroute | Disables adversaries from identifying privileged VM’s (Dom0 in EC2) |

Detection

Detecting the presence of port-knocking command and control might be possible based on an examination of simple network flow records. In the known exploit, source ports of packets were not increasing monotonically as is the custom from the same IP client. An inspection of flow records from the host would reveal odd behavior as the source ports of packets were jumping around and were both increasing and decreasing by huge amounts in short order.

References

1. https://www.threatstack.com/security-operations-center/cloud-attack. Accessed Feb 28,2020.

2. <https://cseweb.ucsd.edu/~savage/papers/CCS09.pdf>. Accessed July 2, 2020.