Redundant Access (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Adversaries may use more than one remote access tool with varying command and control protocols or credentialed access to remote services so they can maintain access if an access mechanism is detected or mitigated.

If one type of tool is detected and blocked or removed as a response but the organization did not gain a full understanding of the adversary's tools and access, then the adversary will be able to retain access to the network.  Adversaries may “backdoor” user accounts by adding additional permissions or access keys associated with otherwise valid accounts. Adversaries may also retain access through cloud-based infrastructure such as creating their own bastion host within a virtual network.

Use of a [Web Shell](https://attack.mitre.org/techniques/T1100) is one such way to maintain access to a network through an externally accessible Web server.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Pacu Backdoor Modules | Publicly available modules that make creating hard to find backdoors easy if AWS account access has been established even briefly. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Account Exploitation | Prevent initial exploitation of Cloud accounts. |
| Network Monitoring | Network intrusion detection and prevention systems that use network signatures to identify traffic for specific traffic entering and leaving cloud virtual networks can be monitored via flow logs to identify network traffic that does not belong. Both AWS and Azure have capabilities to also capture PCAP from virtual machines. In Azure this capability is called Network Watcher. PCAP can be run through a signature tool such as Snort to search for tell tale signs of past beacons. |

Detection

Existing methods of detecting remote access tools are helpful. Backup remote access tools or other access points may not have established command and control channels open during an intrusion, so the volume of data transferred may not be as high as the primary channel unless access is lost.

Detection of tools based on beacon traffic, Command and Control protocol, or adversary infrastructure require prior threat intelligence on tools, IP addresses, and/or domains the adversary may use, along with the ability to detect use at the network boundary. Prior knowledge of indicators of compromise may also help detect adversary tools at the endpoint if tools are available to scan for those indicators.

If an intrusion is in progress and sufficient endpoint data or decoded command and control traffic is collected, then defenders will likely be able to detect additional tools dropped as the adversary is conducting the operation.

References

1. https://medium.com/@rzepsky/playing-with-cloudgoat-part-5-hacking-aws-with-pacu-6abe1cf5780d Accessed August 14,2020