Port Knocking – C&C (version 1.1)

**Cloud Service Label: IaaS, PaaS**

Description

Malicious rootkits on a host in the cloud still require a method of command and control to accomplish adversary objectives. If a compromised cloud host happens to be hosting a public web server or other publicly accessible network service, it is possible to secretly communicate with a rootkit that resides on this host by sending application packets to the service with carefully encoded source ports. In this way the traffic will pass through any firewalls or network security groups which are programmed to let port traffic destined to the service through. Once the packet is delivered to the cloud host, the rootkit can sniff the packet and interpret the source ports as directives.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Cloud Snooper | Publicly published attack on AWS hosted web servers that already had been implanted with malware. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Audit | | Frequently check permissions on cloud storage to ensure proper permissions are set to deny open or unprivileged access to resources. Consider using automated resource checkers such as CloudSploit or Divvycloud. |
|  | AWS | To perform an audit via AWS it is suggested to review information such as account details (credentials, users, groups, roles, etc), mobile applications, EC2 configurations, policies, and account activity. How to audit these different factors can be found in detail at: **https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html.** |
|  | Azure | To perform an audit via Azure an administrator can review the audit logs that are recorded under Azure’s monitoring for active directory. The audit logs allow for filtering, as well as looking at users, groups, and enterprise specific information. Full details on how to access this information can be found at: **https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs.** |
|  | GCP | To perform an audit via GCP the logs can be reviewed. GCP breaks this down into three categories; admin activity, data access, and system events. The audit logs can be viewed a few different ways- the console, API, or gcloud. Full details on how to view these logs, how to export, and for how to configure the retention period can be found here: **https://cloud.google.com/logging/docs/audit.** |

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://news.sophos.com/wp-content/uploads/2020/02/CloudSnooper\_report.pdf. Accessed Feb 28, 2020.