Leveraging SaaS Applications (version 1.0)

**Cloud Service Label: SaaS, IaaS**

Description

The adversary is trying to communicate with compromised systems to control them.

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim’s network structure and defenses.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| SLUB | Malware spreading unique watering hole websites and through [CVE-2018-8174](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8174) and [CVE-2019-0752](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0752). Command and Control vectors include GitHub and Slack, with much more focus on the latter. Utilizes TLS from API’s to evade detection since it is presented as normal network traffic. |
| [SaaSy\_boi](https://github.com/netskopeOSS/saasy_boi) | Proof-of-Concept project presented at DEFCON27. Purpose is to establish CnC vectors through various SaaS and social media services. Examples include Slack, Twitter, and GitHub and starts by retrieving their respective API keys. SaaSy\_boi offers file upload, download, and execute functionality, creating reverse shells, and actively taking screenshots of the compromised machine. |
| [Gcat](https://github.com/byt3bl33d3r/gcat) | Python based backdoor that uses G-mail as a CnC server. |
| [Twittor](https://github.com/PaulSec/twittor) | Python based backdoor that uses Twitter direct messages (DM’s) as a CnC server. |
| [Slackor](https://github.com/Coalfire-Research/Slackor) | A GoLang project that uses Slack as a CnC server. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Manage log data like other sensitive data | Ensure log data is protected and managed like any other confidential data source with encryption at rest and positive control. |
| Cloud Access Security Broker | Implement CASB solutions to ensure cloud resources are being properly accessed. |
| Endpoint Detection | Anti-virus or malware detection services will flag and protect against any suspicious information and files. |
| Disable unnecessary SaaS | Adversaries could potentially exploit available Enterprise SaaS the same as an open port or service on a machine. Harden, lockdown, or outright disable any SaaS that is not needed. |

Detections

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Create Log Metric Filters and Alarms for AWS | To create a metric filter and alarm:   1. Create a metric filter that checks for IAM policy changes and the *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter and SNS topic created in steps 1 and 2 respectively |
| Monitor Activity in AWS Account | Various services in AWS offer logging features that allow for detection capabilities. These include CloudFront, CloudTrail, CloudWatch, Config, and S3. |
| Monitor for Suspicious Activity in Azure | Azure AD can generate anomaly reports than can be run on a daily basis. Azure AD Identity Protection show current risks in its dashboard and provides daily email summary notifications. Policies can also be configured to alert to specific issues. |
| Create Log Metric Filters and Alarms for CloudTrail | To create a metric filter and alarm:   1. Create a filter that checks for CloudTrail changes and the specific *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic that the alarm will notify 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter from step 1 and SNS topic in step 2 |
| Create Activity Log Alerts in Azure | To create log activity alerts for deletion in the Azure Console:   1. Navigate to *Monitor’ / ‘Alerts* 2. Select *Manage alert rules* 3. Click on the Alert *Name* where Condition contains *operationName equals Microsoft.Network/networkSecurityGroups/securityRules/delete* 4. Hover a mouse over *Condition* to ensure it is set to *Whenever the Administrative Activity Log “Delete Security Rule (networkSecurityGroups/securityRules)” has “any” level with “any” status and event is initiated by “any*” |
| Create, View, and Manage Activity Alerts in Azure Monitor | To create a log alert in the Azure portal:   1. Select **Monitor -> Alerts** 2. Select **New alert rule** of the **Alerts** window 3. Provide information in **Define alert condition** 4. Provide details in **Define alert details** 5. Specify action group for new alert rule under **Action group**, or create a new action group with + **New group** 6. Select **Yes** for the **Enable rule upon creation** option 7. Select **Create alert rule**   To view and manage alerts:   1. Select **Monitor -> Alerts -> Manage alert rules** 2. Select the rule you want to modify and double-click to edit the rule options 3. Click **Save** |
| Azure Resource Manager Templates | Azure Resource Manager templates in the format of JSON files that can be used to configure metric alerts in Azure Monitor. These templates can be used for simple static and dynamic threshold metric alerts, availability tests, and monitoring multiple resources. |
| Enable CloudTrail across all regions in AWS | To enable CloudTrail across all regions:   1. Sign into the AWS Management Console and open the CloudTrail console 2. Click on *Trails* 3. Set necessary Trails to All option in the I column 4. Click on a trail via the link *Name* column 5. Set *Logging* to *ON* 6. Set *Apply trail to all regions* to *Yes* |
| Configure log profile to capture activity logs for all regions in Azure | To set up activity logs for all regions:   1. Navigate to Azure console 2. Go to *Activity log* 3. Select *Export* 4. Select *Subscription* 5. Check *Select all* in *Regions* 6. Select *Save* |

References

1. <https://blog.trendmicro.com/trendlabs-security-intelligence/slub-gets-rid-of-github-intensifies-slack-use/>. Accessed July 9, 2020.
2. <https://www.youtube.com/watch?v=m5NxE9yZjR4>. Accessed July 9, 2020.
3. <https://github.com/netskopeOSS/saasy_boi>. Accessed July 9, 2020.
4. <https://github.com/byt3bl33d3r/gcat>. Accessed July 9, 2020.
5. <https://github.com/PaulSec/twittor>. Accessed July 9, 2020.
6. <https://github.com/Coalfire-Research/Slackor>. Accessed July 9, 2020.