Detecting ransomware activities within AWS environments

Applicability

- Product: Splunk Cloud Platform or Splunk Enterprise
- Feature: Monitoring
- Technology: Splunk App for AWS and Splunk Add-on for AWS
- Data: Amazon Web Services: CloudTrail and CloudWatch

Scenario

You are an Amazon Web Services (AWS) admin who manages AWS resources and services across your organization. As part of your role, you need to be able to detect potential ransomware attacks that occur via your AWS resources.

Cloud ransomware can be deployed when attackers obtain high-privileged credentials from targeted users or resources. The searches in this use case help you to detect when users in your AWS environment are performing activities that are commonly associated with ransomware attacks, namely through the creation of KMS keys and encryption activities.

- To run these searches, install the Splunk App for AWS (version 5.1.0 or later) and Splunk Add-on for AWS (version 4.4.0 or later).
- Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.

Detection searches

► Detect AWS users creating KMS keys where kms:Encrypt is publicly accessible

This search provides detection of newly created Key Management Service (KMS) keys or keys that have been assigned a policy for access, where the action kms:Encrypt is accessible for everyone, even people outside of your organization. This is an indicator that your account is compromised and the attacker is using the encryption key to compromise another company.

```
| search (sourcetype=aws:cloudtrail (eventName=CreateKey OR eventName=PutKeyPolicy))
| spath input=requestParameters.policy output=key_policy_statements path=Statement{}
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Detect AWS users with KMS keys performing encryption in S3 buckets

This search provides detection of users with KMS keys performing encryption specifically against S3 buckets.

Additional resources

This use case is included within Splunk Enterprise Security, a Splunk app that provides prebuilt content and searches to help answer root-cause questions in real-time about malicious and anomalous events in your IT infrastructure. In addition, Splunk Enterprise Security provides a number of other searches to help reinforce your cloud security posture, including:

- Detecting a ransomware attack