



Cloud-Native Ransomware

Attacking availability with cloud services

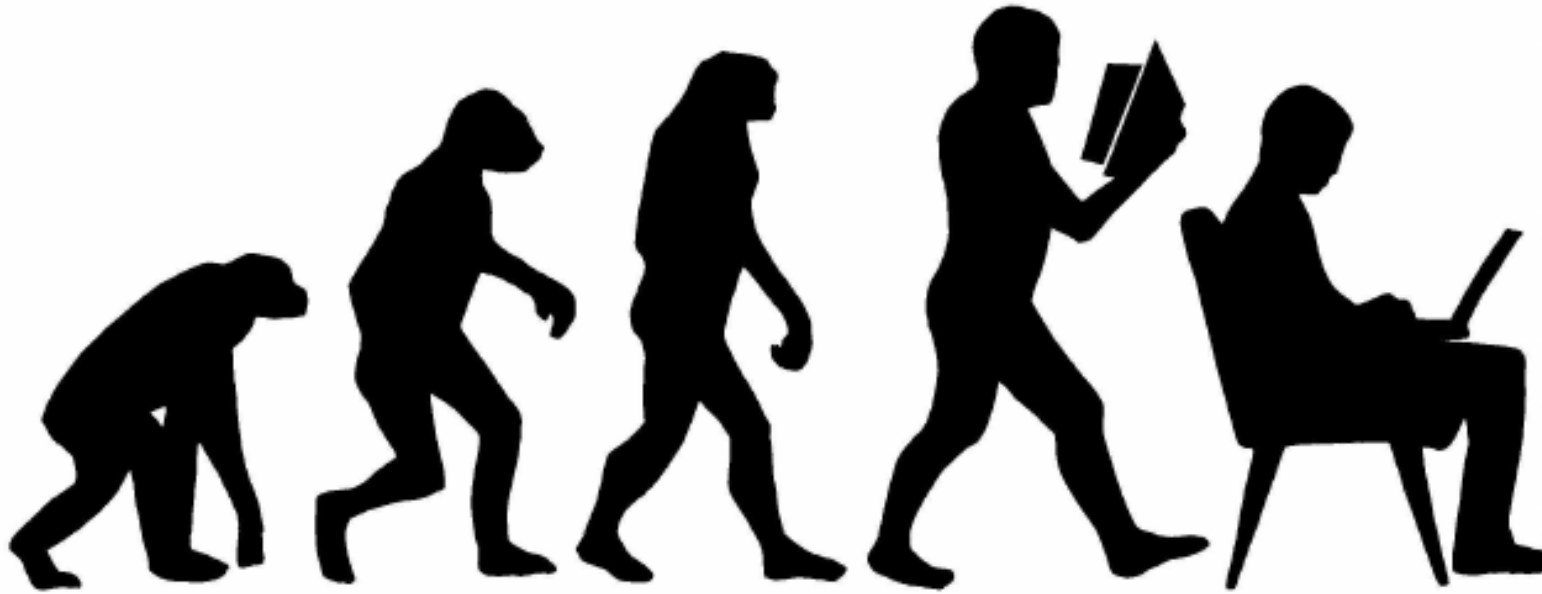
Kat Traxler – Principal Security Research | Public Cloud
@nightmareJs

April 2022




Will Ransomware Evolve to Target Cloud Data?

Wherever critical data lives, ransomware will go.



Subhead line goes here in 18 pt. Arial

Attacking Availability

A decorative graphic on the left side of the slide. It features a large, light gray triangle pointing downwards. Inside this triangle, there are several smaller triangles of different colors and patterns: a light blue triangle, a gray triangle, a blue triangle with a white dot pattern, an orange triangle, a green triangle with a white dot pattern, and a green triangle with a white dot pattern. A white, stylized cloud is positioned in the center of these triangles.

Traditional ransomware is constrained by the limitations of on-prem environments
With the Cloud, **many more options exist.**

Attacking Availability in the Cloud

Feature abuse rather than vulnerabilities

Feature Abuse

- ▼ The use (or misuse) of cloud APIs to overcome security controls
 - Leveraging built-in features of the tools published by the CSPs
 - No code flaws being manipulated
 - Not detectable with classic vulnerability scanning tools
 - Takes advantage of the public nature of public cloud APIs
 - Best mitigation is defensive architectural patterns and cloud-native detections

Subhead line goes here in 18 pt. Arial



Defending Traditional Data Warehouses

- ▼ Physical Hosts with **broad attack surfaces**
- ▼ **Defense** is informed from decades of experience with ransomware targeting on-prem systems
- ▼ **Network-Controls** has data warehouses tucked deep into internal networks
- ▼ **Monitoring** of these environments include agent-based solutions commensurate with their full-stack nature

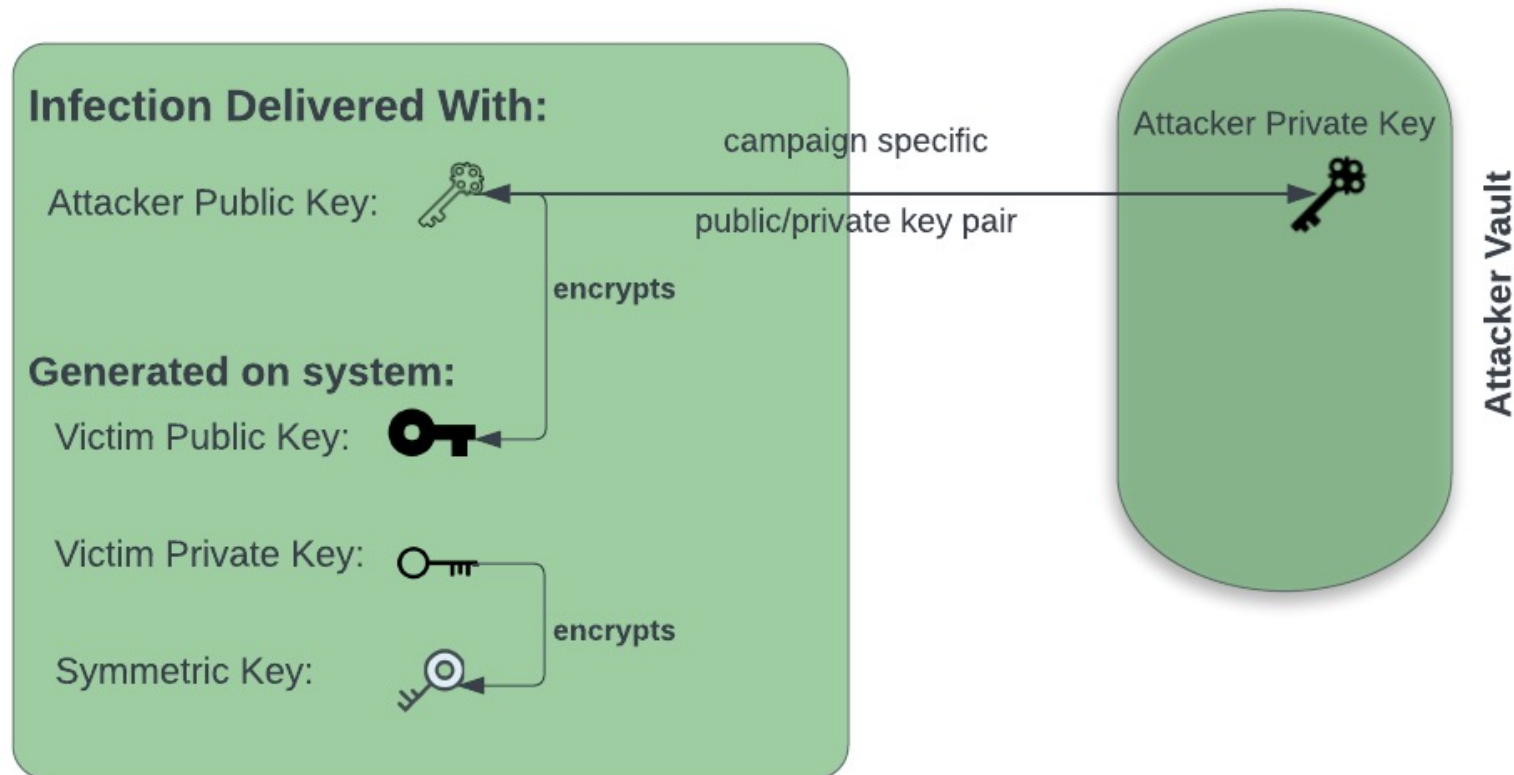


This is why we drink. #infosec

trustoncloud.com/the-last-s3-se...

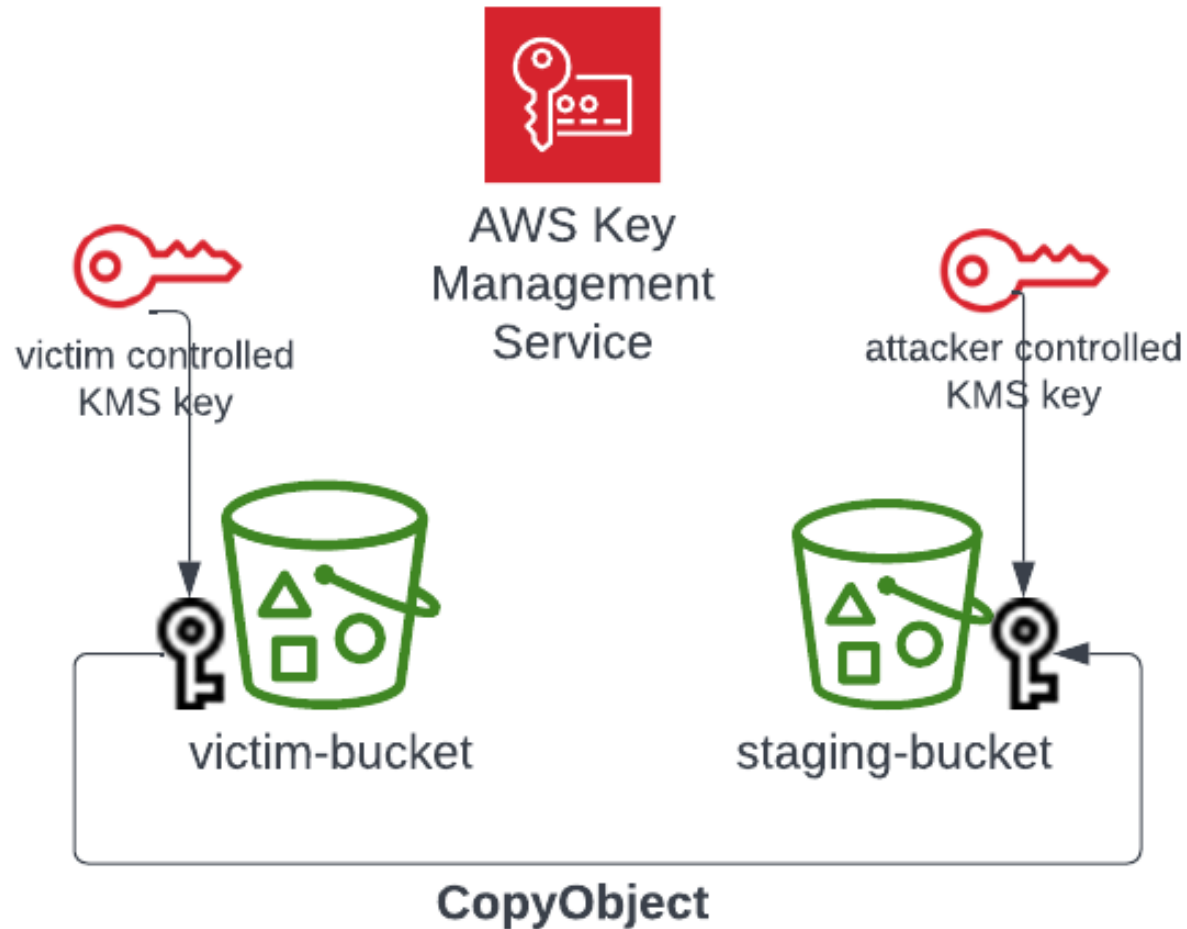
- ▼ Cloud data stores have dramatically different attack surfaces
- ▼ Access to underlying system is limited, curated by the CSP
- ▼ The on-premises approach **does not translate to the cloud**, nor should it
- ▼ S3 Threat Model is 163 pages!
 - [TRUSTONCLOUD](#)
 - #thisIsWhyWeDrink

Traditional Ransomware's Encryption Strategy



1. Infection delivered with campaign-specific attacker public key
2. Malware generates new keys:
 - public/private key pair for encryption operation
 - new symmetric key
3. Symmetric encrypts files
4. Private key encrypts symmetric key
5. Attacker public key encrypts malware generated public key
6. Campaign-specific attacker private key required to unencrypt data

Encrypting S3 with Attacker Controlled KMS Keys



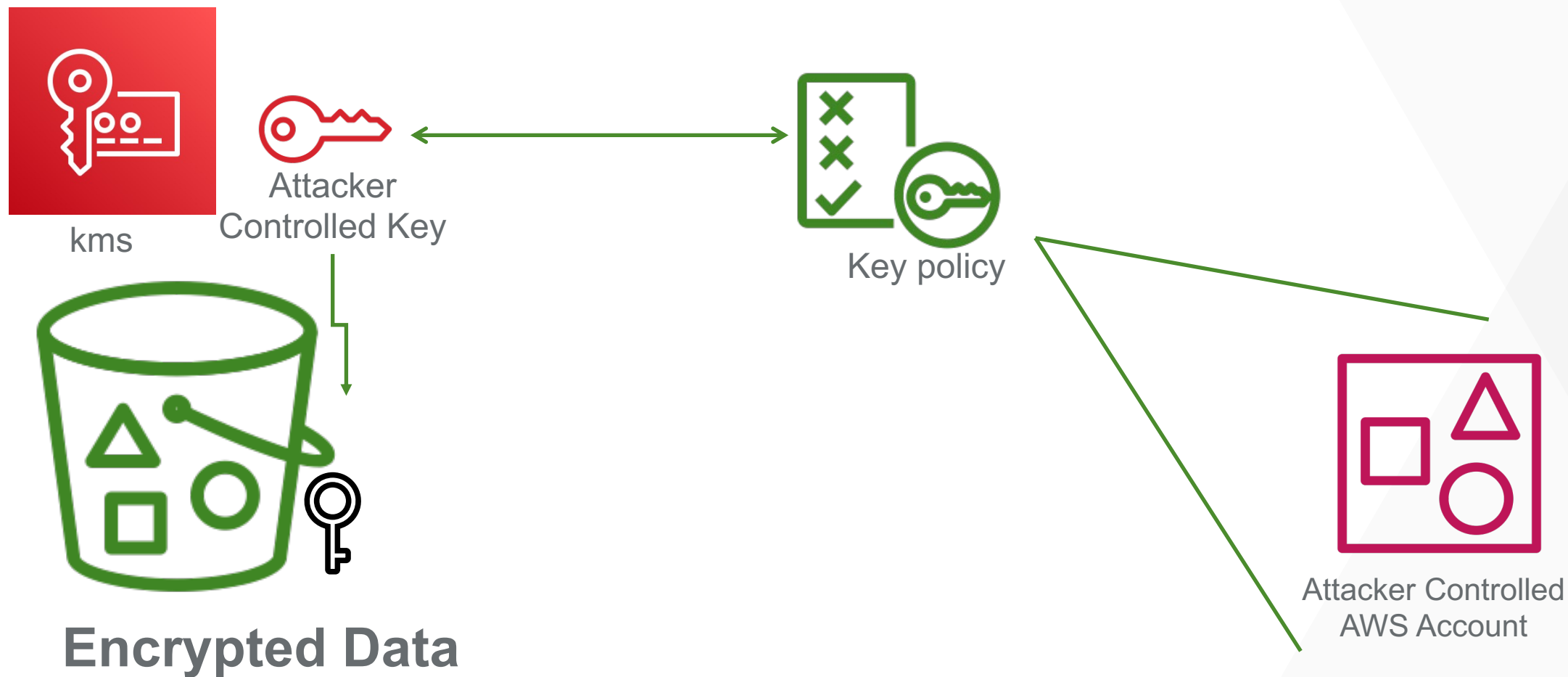
1. Copy objects between two encrypted buckets
2. Control access to key used to encrypt destination bucket
3. Delete original, targeted bucket

Demo 1

Attacking Availability on S3



Key Policy Lockout



DENY, except when; ALLOW, only when

KMS Key Policy Lock Out Technique

- ▼ **DENY** - all actions on the KMS key - except when “*aws:sourceip*” condition key equals the attacker-controlled IP.
- ▼ **ALLOW** - all actions on the KMS key – only when the caller is from the attacker-controlled account
- ▼ Additional condition keys to restrict access to KMS keys include:
 - *aws:PrincipalArn*
 - *aws:PrincipalAccount*
 - *aws:sourceVPC*
 - *aws:SourceVPCE*



Key Policy Lockout with Sourcelp Address Condition

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Deny all actions on key from all AWS Principals if that are not coming from attacker controlled IP",
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Action": "kms:*",
      "Resource": "*",
      "Condition": {
        "NotIpAddress": {
          "aws:sourceIp": ["18.118.5.221"]
        }
      }
    },
    {
      "Sid": "Allow all actions on kms from attacker AWS Account, as long as traffic eninates from attacker controlled IP",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::184767987163:user/attacker-account"
      },
      "Action": "kms:*",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:sourceIp": ["18.118.5.221"]
        }
      }
    }
  ]
}
```

Turning Over The Keys

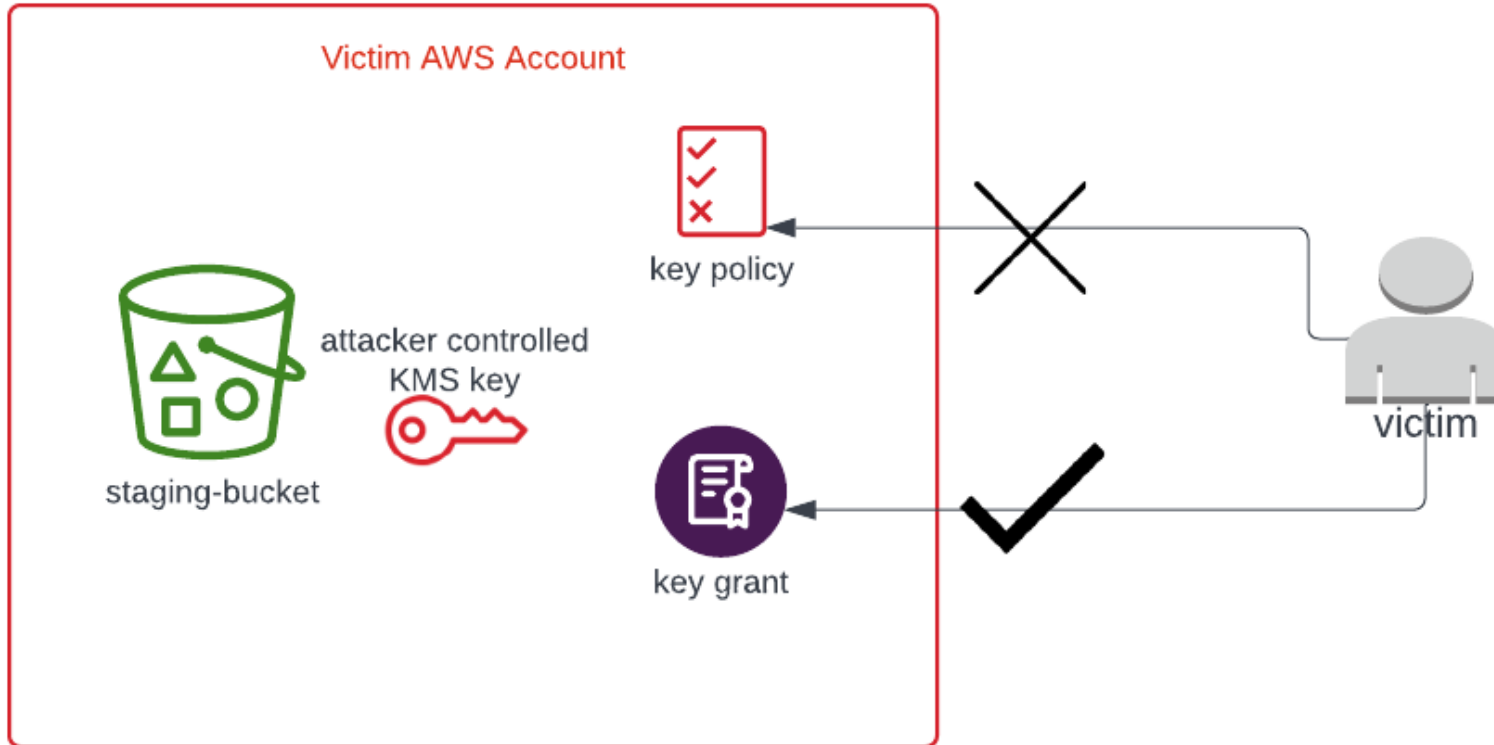
Completing the Ransomware Lifecycle

Like any other business, ransomware operators need a reliable and trusted means to deliver products to their 'customers.'



KMS Key Grants

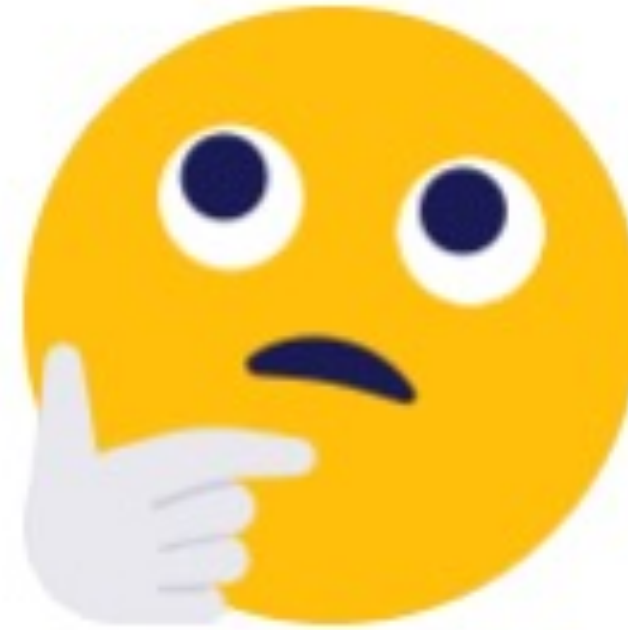
A separate authorization mechanisms for KMS Keys



- Only callers from the attackers account can perform operations on the key per AWS IAM
- Attacker is allowed to generate a key grant for the victim
- Cryptographic operations are allowed by the grantee even when explicitly denied in policy

Could AWS assist during a ransomware event ?

1. Could AWS access KMS key material from an AWS HSM?
2. Does AWS have a 'hand-of-god' to update resource-based key policies?
3. Can AWS seize control over the resources of a rogue account?



Ransomware Mitigations on S3

▼ Bucket Configurations

- Object Lock
- Object Versioning
- MFA Delete

▼ Service Control Policy

- Enforce Server-Side Encryption on S3 Buckets with a pre-defined list of KMS Keys
- Explicitly deny key creation and policy modification except from designated crypto operations team

▼ S3 Backups

- Balancing the freshness of backups | time to recovery | securing the integrity of backups

Detection Strategies

Detecting Suspect Conditions in Policy

- ▼ Elements in policy can be used to conditionally allow and conditionally deny access to keys.
- ▼ Captures all variants
 - Key-policy lockout with **new key**
 - Key-policy lockout with **existing key**
 - Encryption with **external key**

Detecting Non-Approved KMS Keys Use

- ▼ If your organization has a clear view of which keys should be used for encryption, the use of non-approved KMS keys should raise alarms.
- ▼ Captures variants
 - Key-policy lockout with **new key**
 - Encryption with **external key**

Detection External KMS Key Use

- ▼ Developing a clear view of what external means to your organization is critical to implementing this detection strategy.
- ▼ Captures variants
 - Encryption with **external key**

In Conclusion.....



Acknowledgements and Further Reading

- ▼ “S3 backups and other strategies for ensuring data durability through ransomware attacks”
 - Scott Piper – Summit Route Blog
 - “Ensuring S3 data cannot be deleted by an attacker is not entirely trivial, but hopefully this guide has explained the better options (s3 object locking and replication policies) and pointed out some common problems to watch out for.”
- ▼ “Ransom in the Cloud”
 - Spencer Gietzen – DEFCON Cloud Village
 - KMS Key Policy Lockout Technique described in depth.
- ▼ “S3 Ransomware Part 1 – Attacker Vectors”
 - Spencer Gietzen – Rhino Security Blog
- ▼ “Threat Model for Amazon S3”
 - Trust On Cloud



Questions

..... Comments or Concerns



VECTRA[®]
SECURITY THAT THINKS.[®]