Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C

halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c

The Halcyon RISE Team has identified a concerning new ransomware campaign targeting Amazon S3 buckets. This attack leverages AWS's Server-Side Encryption with Customer Provided Keys (SSE-C) to encrypt data, demanding ransom payments for the symmetric AES-256 keys required to decrypt it.

It is important to note that this attack does not require the exploitation of any AWS vulnerability but instead relies on the threat actor first obtaining an AWS customer's account credentials.

With no known method to recover the data without paying the ransom, this tactic represents a significant evolution in ransomware capabilities.

Executive Summary:

Native Resource Abuse: Threat actor dubbed *Codefinger* uses compromised AWS keys to encrypt S3 bucket data via SSE-C, leveraging AWS's secure encryption infrastructure in a way that prevents recovery without their generated key.

Irrecoverable Data Loss: AWS CloudTrail logs only an HMAC of the encryption key, which is insufficient for recovery or forensic analysis.

Urgent Ransom Tactics: Files are marked for deletion within seven days to pressure victims, with ransom notes providing payment details and warnings against altering account permissions.

Campaign Overview

Threat actor *Codefinger* abuses publicly disclosed AWS keys with permissions to write and read S3 objects. By utilizing AWS native services, they achieve encryption in a way that is both secure and unrecoverable without their cooperation.

While SSE-C has been available since 2014, this appears to be a novel use of the feature by ransomware operators. Halcyon has identified two victims in recent weeks (neither were Halcyon customers at time of the attacks) who were impacted by this attack, underscoring its severity and the need for immediate action by organizations utilizing Amazon S3.

How the Attack Works

The threat actor's workflow highlights their technical capabilities:

Identify Vulnerable AWS Keys:

Using publicly disclosed or compromised AWS keys, the threat actor locates keys with permissions to execute *s3:GetObject* and *s3:PutObject* requests.

Encrypt Files Using SSE-C:

The attacker initiates the encryption process by calling the *x-amz-server-side-encryption-customer-algorithm* header, utilizing an AES-256 encryption key they generate and store locally.

AWS processes the key during the encryption operation but does not store it. Instead, only an HMAC (hash-based message authentication code) is logged in AWS CloudTrail. This HMAC is not sufficient to reconstruct the key or decrypt the data.

Set Lifecycle Policies for File Deletion:

Files are marked for deletion within seven days using the S3 Object Lifecycle Management API, adding urgency to the ransom demand.

Ransom Note:

A ransom note is deposited in each affected directory, providing the attacker's Bitcoin address and a client ID associated with the encrypted data. The note warns that changes to account permissions or files will end negotiations.

Why This Matters

This ransomware campaign is particularly dangerous because of SSE-C's design:

Data Loss is Permanent Without the Key: Unlike traditional ransomware that encrypts files locally or in transit, this attack integrates directly with AWS's secure encryption infrastructure. Once encrypted, recovery is impossible without the attacker's key.

Log Evidence is Limited: AWS CloudTrail logs only the HMAC of the encryption key, which is insufficient for recovery or forensic analysis.

Scope for Escalation: If this method becomes widespread, it could pose a systemic threat to organizations using Amazon S3 for critical data storage.

Mitigating the Threat

Organizations can protect themselves by proactively hardening their AWS environments:

Restrict SSE-C Usage:

Use the Condition element in IAM policies to prevent the application of SSE-C to S3 buckets. Policies can be configured to restrict this feature to authorized data and users.

Monitor and Audit AWS Keys:

Regularly review permissions for all AWS keys to ensure they have the minimum required access.

Disable unused keys and rotate active ones frequently.

Implement Advanced Logging:

Enable detailed logging for S3 operations to detect unusual activity, such as bulk encryption or lifecycle policy changes.

Engage AWS Support:

Work with AWS support to identify potential vulnerabilities and implement tailored security measures.

Statement from Amazon Web Services:

Halcyon provided AWS with advance notice of the findings in this report, and they provided the following statement and guidance:

> *AWS helps customers secure their cloud resources through a shared responsibility model. Anytime AWS is aware of exposed keys, we notify the affected customers. We also thoroughly investigate all reports of exposed keys and quickly take any necessary actions, such as applying quarantine policies to minimize risks for customers without disrupting their IT environment.*
>
> *We encourage all customers to follow security, identity, and compliance best practices. In the event a customer suspects they may have exposed their credentials, they can start by following the steps listed in this post. As always, customers can contact AWS Support with any questions or concerns about the security of their account.*
>
> *AWS provides a rich set of capabilities that eliminate the need to ever store credentials in source code or in configuration files. IAM Roles enable applications to securely make signed API requests from EC2 instances, ECS or EKS containers, or Lambda functions using short-term credentials that are automatically deployed, frequently rotated, requiring zero customer management. Even compute nodes outside the AWS cloud can make authenticated calls without long-term AWS credentials using the Roles Anywhere feature. Developer workstations use Identity Center to obtain short-term credentials backed by their longer-term user identities protected by MFA tokens. All these technologies rely on the AWS Security Token Service (AWS STS) to issue temporary security credentials that can control access to their AWS resources without distributing or embedding long-term AWS security credentials within an application, whether in code or configuration files. Even secure access to non-AWS technologies can be protected using the AWS Secrets Manager service. The purpose of that service is to create, manage, retrieve, and automatically rotate non-AWS credentials like database usernames and passwords, non-AWS API keys, and other such secrets throughout their lifecycles.*

January 16, 2025: AWS published more guidance in response to our report

For more information:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/security_iam_service-with-iam.html#security_iam_service-with-iam-id-based-policies-conditionkeys

Additional Resources:

Using server-side encryption with customer-provided keys (SSE-C) - Amazon Simple Storage Service

Protecting data with server-side encryption - Amazon Simple Storage Service

GetObject - Amazon Simple Storage Service

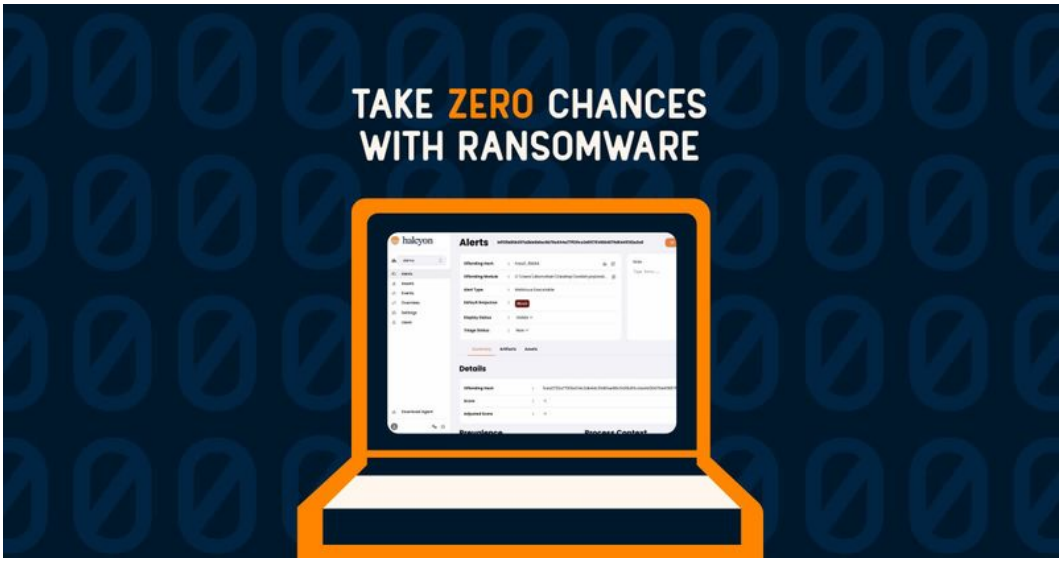
Takeaway

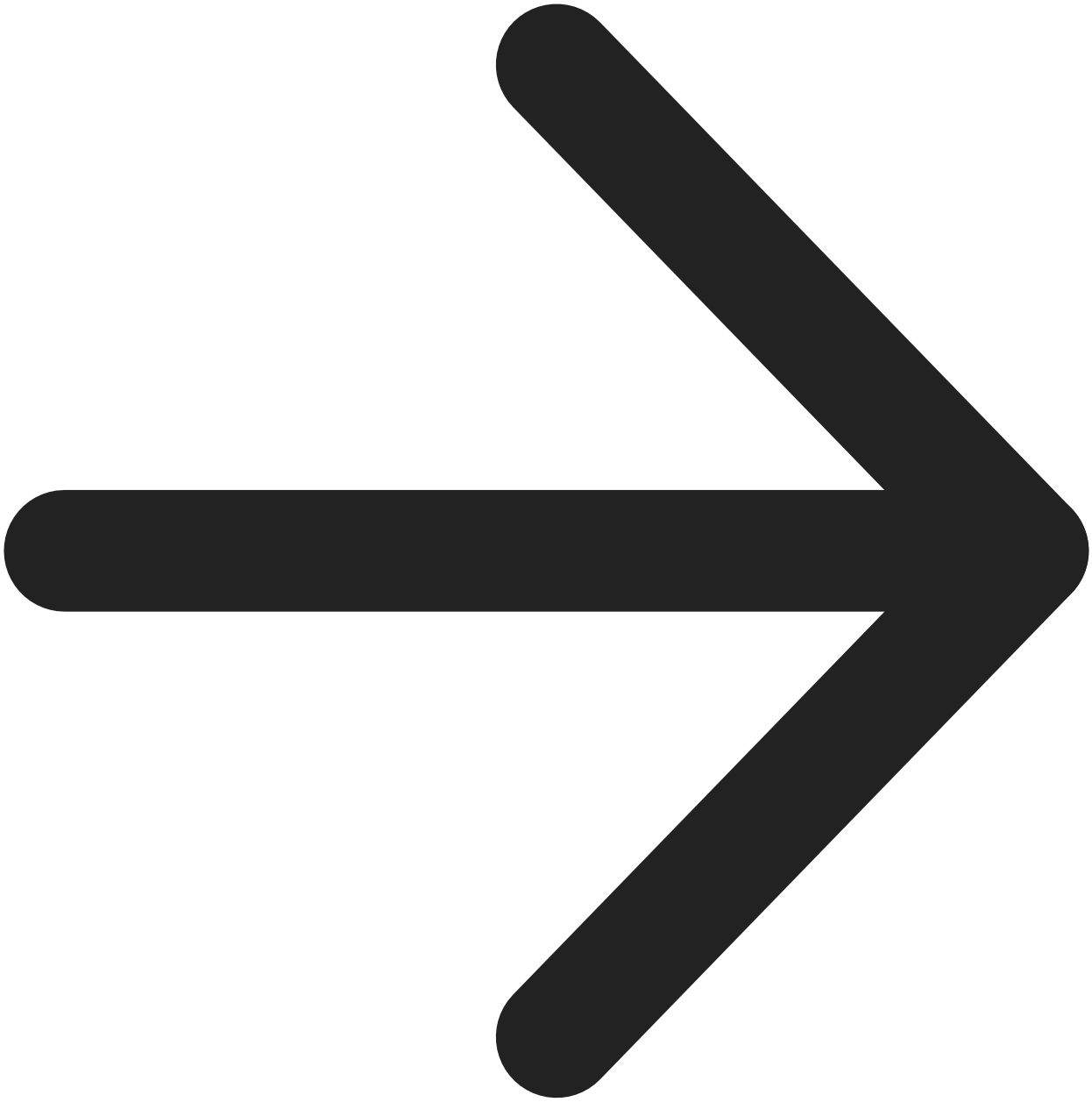
Halcyon intelligence indicates that while this attack is currently targeted, the technique may soon gain traction among other threat actors. This campaign highlights the need to secure AWS keys or access tokens by organizations relying on Amazon S3 for data storage. Immediate mitigation measures include restricting SSE-C usage, auditing AWS keys, implementing advanced logging, and engaging AWS support to bolster defenses.

Halcyon urges organizations to act swiftly, as this attack method could gain broader adoption, posing a systemic threat to cloud data security. All major cloud service providers offer similar client-side encryption functionality that could be abused.

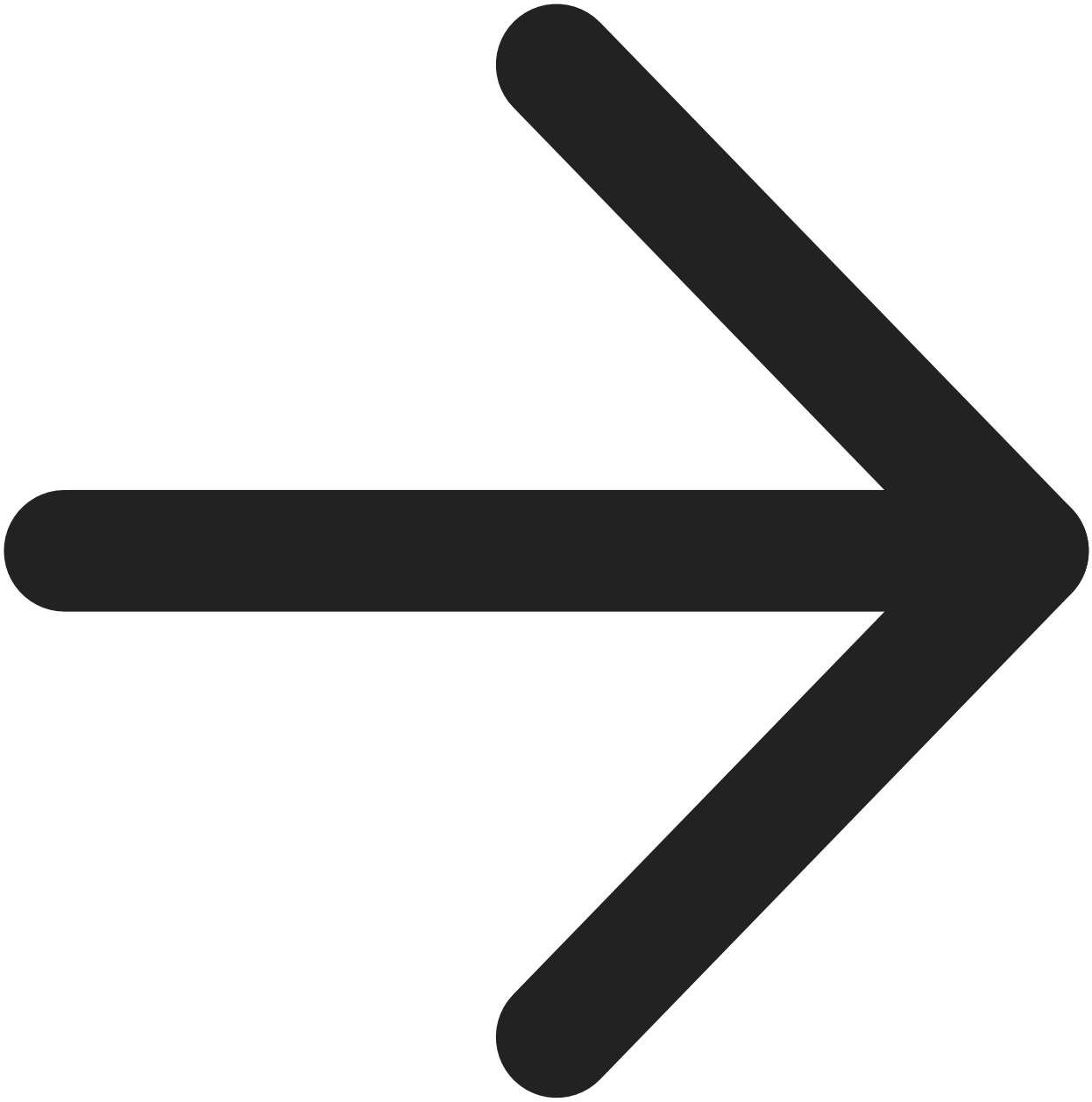
Stay vigilant and ensure your environment is resilient against emerging ransomware techniques. The Halcyon RISE Team will continue to monitor and provide updates as this campaign develops.

Halcyon.ai eliminates the business impact of ransomware. Modern enterprises rely on Halcyon to prevent ransomware attacks, eradicating cybercriminals' ability to encrypt systems, steal data, and extort companies – talk to a Halcyon expert today to find out more and check out the Halcyon Attacks Lookout resource site. Halcyon also publishes a quarterly RaaS and extortion group reference guide, Power Rankings: Ransomware Malicious Quartile.





Get a Demo



stay updated on news

The world of ransomware is always changing. Subscribe and stay in the know.

Thank you! Your submission has been received!

Oops! Something went wrong while submitting the form.

Thanks for subscribing, you're now on the inside!

Oops! Something went wrong while submitting the form.

By subscribing you agree to with our Privacy Policy.
Share this post