
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC402-R

The anatomy of a ransomware event targeting data residing in Amazon S3

Megan O'Neil
Principal Security Solutions Architect
AWS

Kyle Dickinson
Sr. TDIR Solutions Architect
AWS

Agenda

What is ransomware?

Detection & analysis

Response & recovery

Protection

Conclusion

What is ransomware?

Ransomware refers to a business model and a wide range of associated technologies that unauthorized users use to extort money from entities

Unauthorized users use system vulnerabilities to access data and then restrict the rightful owner from accessing it

What is ransomware?

Accomplished by unauthorized user who **encrypts** data using actor-controlled encryption keys, using access controls to **lock out** the rightful owner from a system

Or, unauthorized users may threaten to **reveal data or acts of exfiltration**, which can result in large monetary fines from data privacy authorities and/or litigation from affected parties

Detection

Customer observables: Amazon S3 ransom event

- Decreased amount of objects in an S3 bucket via Amazon CloudWatch metrics
- Ransom letter left in impacted S3 bucket
- Amazon GuardDuty AWS Identity and Access Management (IAM)/Amazon S3 findings
- Objects exist but are encrypted with AWS KMS key not owned by the customer

Unintended disclosure of security credentials and secrets

Detect

- Monitor for identity behavioral changes recorded in AWS CloudTrail events:
  - GuardDuty IAM findings
  - CloudTrail insights for unusual events
- Monitor your AWS account email address for AWS notifications of compromised credentials
- Implement application security scanning for static credentials and secrets to reduce disclosure

Event pattern

Detection and analysis

- S3 objects are deleted or entire S3 buckets are deleted
  - Review CloudWatch metrics and S3 data events to verify data exfiltration to delineate between a ransom or data destruction event
- S3 objects are encrypted using an AWS KMS key not owned by customer
- Ransom note provided as an object within bucket or via email
- Review CloudTrail for destructive API calls
- If S3 server access logs are enabled, look for REST.COPY.OBJECT_GET calls

Event pattern

Event pattern

Discovery API calls

- s3:ListBuckets – Returns a list of all buckets owned by the authenticated sender of the request
- s3:GetBucketAcl – Returns access control list of a bucket
- s3:GetBucketPolicy – Returns bucket policy of a bucket
- s3:ListObjects – Returns list of objects within a specified bucket

---

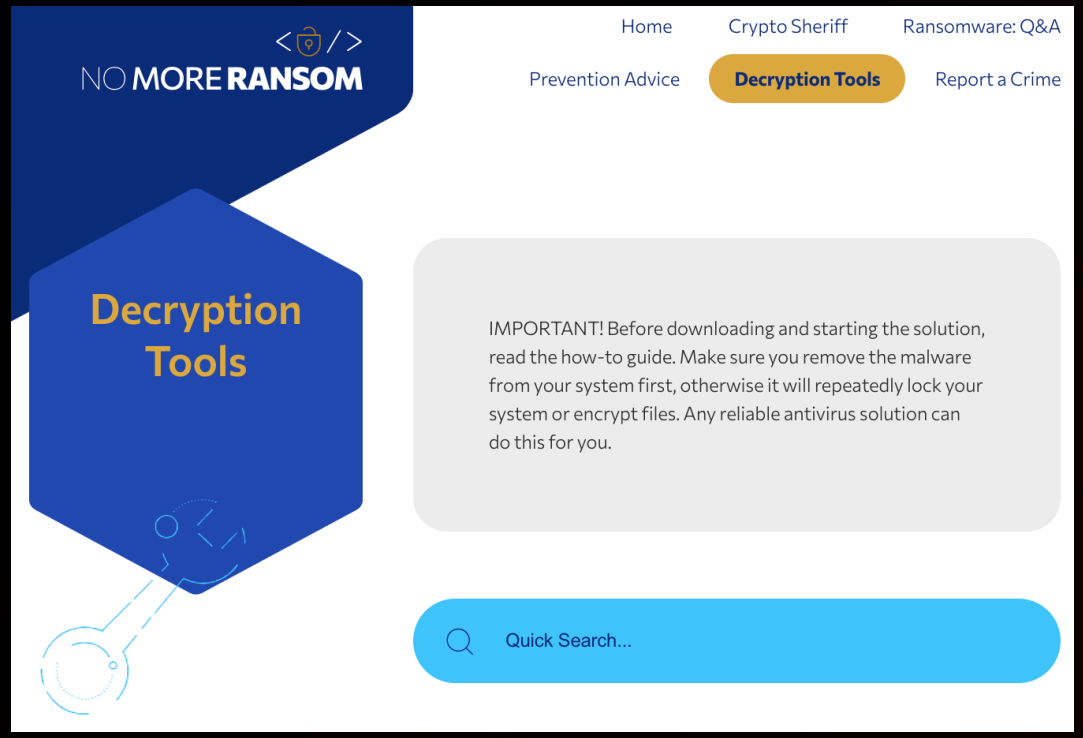
- s3:GetObjects – Retrieves objects from a bucket
- s3:DeleteObjects – Removes the null version (if there is one) and inserts a delete marker

Event pattern

Event pattern

Response & recovery

Don’t pay the ransom



https://nomoreransom.org

Response Scenarios

100-200 Level Scenarios

- Compromised IAM Credential(s)
- Denial of Service / Distributed Denial of Service
- Inappropriate Public Resources: S3)
- Inappropriate Public Resources: RDS)
- Unauthorized Network Changes
- Simple Email Service Compromise
- Identifying Exposure of CodeCommit

300-400 Level Scenarios

- Bitcoin and Cryptojacking
- Responding to Ransom in AWS
  - Amazon Elastic Computing (EC2) Linux/Unix
  - Amazon Elastic Computing (EC2) Microsoft Windows
  - Amazon Relational Database Service (RDS)
  - Amazon Simple Storage Service (S3)

https://github.com/aws-samples/aws-customer-playbook-framework

Responding to a credential compromise

What is the first thing you need to do after a credential compromise?

Responding to a credential compromise

- Create a second set of keys, deactivate, record, and then delete
- Delete unauthorized IAM users, policies, and roles
- Revoke active sessions for IAM roles and temporary credentials
- Follow your incident response plan for disclosure and include necessary stakeholders in this conversation

Recover your data in Amazon S3

- Remove delete markers for versioned objects
- Recreate deleted buckets
- Restore from AWS Backup

AWS does not have the ability to recover data that has been deleted

Protection

Amazon S3 protection

- Enable versioning
- MFA required for destructive actions
- Enabling object lock for Write-Once-Read-Many (WORM) objects
- Enabling AWS Backup for Amazon S3
  - Vault lock for AWS Backup
- Enable S3 block public access
- In AWS CloudTrail, enable data events logging for Amazon S3, or enable S3 object logging on a per-bucket basis

Data protection

PROTECTING DATA USING SERVER-SIDE ENCRYPTION

Customer-managed encryption keys (SSE-KMS)

- Customer-managed keys
- Least-privilege key policy
- AWS KMS logs in CloudTrail

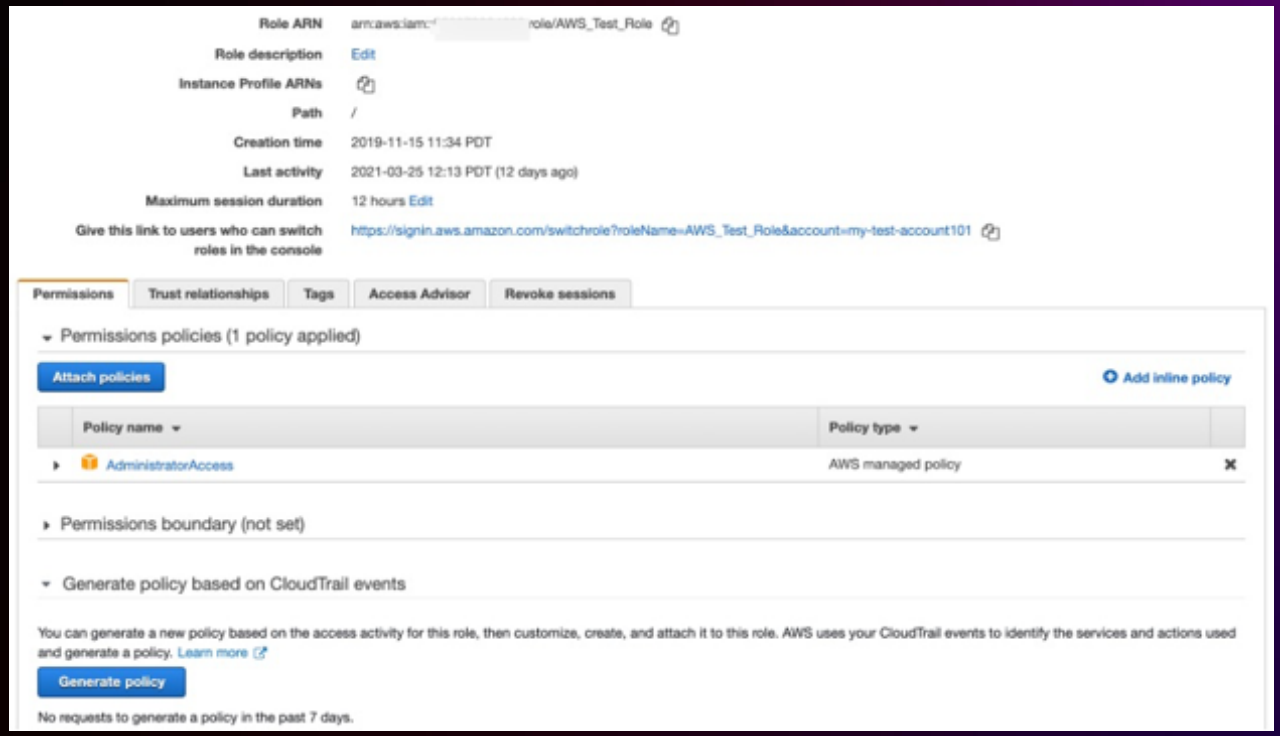
Identity protection

- Least-privilege access practices
- Require MFA for your most sensitive operations and privileged access
- Eliminate static credentials as much as possible
- Use AWS Secrets Manager to vault and audit use of non-IAM credentials/secrets

Example: Tools for least privilege access

Use IAM Access Advisor
Enabled per IAM principal by default in IAM service
Review which AWS services have been used up to last 400 days per IAM principal

Use IAM Access Analyzer to generate least-access policy
- Requires that CloudTrail trail is enabled
- Evaluates last 90 days of specific IAM principal access from selected CloudTrail trail S3 bucket
- Generates a suggested IAM policy from evaluation to use



Additional resources

aws-customer-playbook-framework – aws-samples GitHub
https://github.com/aws-samples/aws-customer-playbook-framework

Security best practices in IAM – AWS Documentation (Updated July 2022)
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Top 10 Security Best Practices for securing data in Amazon S3 – Blog Post
https://aws.amazon.com/blogs/security/top-10-security-best-practices-for-securing-data-in-amazon-s3/

git-secrets – awslabs GitHub
https://github.com/awslabs/git-secrets

nomoreransom.org
https://nomoreransom.org

Ransomware related sessions

Name	SessionID	Type
Data protection & application recovery strategies for ransomware events	STG305	Chalk Talk
Mitigate ransomware risk using AWS security controls	WPS305	Chalk Talk
Protect against ransomware with a Zero Trust architecture	STG208	Breakout Session
Beyond 11 9s of durability: Data protection with Amazon S3	STG338	Breakout Session

Thank you!

Megan O'Neil
megoneil@amazon.com

Kyle Dickinson
kdsecure@amazon.com