Responding to Ransom Attacks within AWS

Notices

This document is provided for informational purposes only. It represents the current product offerings and practices from Amazon Web Services (AWS) as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions, or assurances from AWS, its affiliates, suppliers, or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ransomware

Since the first recorded ransomware attack in 1989 called PC Cyborg, ransomware has become a prominent monetization strategy used by criminal organizations and threat actors across the internet. Other examples of ransomware include:

- CryptoLocker [2014]
- Petya [2016]
- WannaCry [2017]
- NotPetya [2017]
- Ryuk [2019])

Threat actors leverage issues and weaknesses across the customer’s infrastructure, exploiting vulnerable endpoints, insecure services, and socially engineering employees.

Ransomware attacks are costing governments, nonprofits, and businesses billions of dollars and interrupting operations. NotPetya forced shipping giant Maersk to reinstall 4,000 servers and 45,000 PCs for $300M due to “serious business interruption.” The ransomware attack on the City of Baltimore cost over $18M, and local governments from Riviera Beach and Lake City, Florida will pay hackers $1M

combined to get its systems and data back. The U.S. Federal Bureau of Investigation (FBI) anticipates the threat of ransomware to become "more targeted, sophisticated, and costly" in the foreseeable future. These warnings reach beyond U.S. borders, with Europol also calling ransomware the "most widespread and financially damaging form of cyberattack."

What are ransom attacks?

Ransom attacks are a monetization strategy, not a specific technology. Attacks often leverage specific malicious software, or ransomware, which threatens to publish victim information or block access until the ransom is paid.

In theory, if the ransom is paid within the allotted time, systems and data are decrypted and made available once again and normal operations continue. However, if the ransom is not satisfied, organizations risk permanent destruction or public-facing data leaks controlled by the attacker. Attackers [DS(1]can also extort the customer further for release of customer sensitive data and systems to third-parties or to the public.

Ransomware does not care

Many ransom attacks are opportunistic in nature, meaning that ransomware indiscriminately infects any accessible networks through human and/or machine vectors. Security teams for education institutions, state and local governments, and healthcare organizations are ramping up measures to keep their data safe from an increase in ransomware attacks. Threat actors understand how to identify weak spots in industry verticals. Many education and government organizations are more prone to ransomware due to a combination of shrinking budgets, gaps in security resources, and legacy IT systems with known unpatched vulnerabilities. Similarly, ransom attacks may target industries with intolerance for downtime, like hospitals, in hopes of increasing the probability of payout.

Why are ransom attacks effective?

- Security awareness among employees is low
- Organizations are not backing up data, or fail to test existing backups
- Attacks require little skill and result in significant payouts
- Organizations are slow to patch critical common vulnerabilities and exposures (CVE)
- Overburdened technical staff cannot address or anticipate all security gaps
- Multiple vectors or channels are being used in a single attack
- Stealing the data (data exfiltration, unauthorized copying) may not stop a business process, and customers may not react until something does such as encrypting or deleting the information

To pay or not pay?

Active debates exist among cyber security professionals regarding the decision to pay ransoms. Many experts, including the FBI, advise organizations not to pay the ransom, arguing that paying doesn't guarantee that locked systems or encrypted data will be made available and will only continue to motivate nefarious behaviors. Even though system and data access is not guaranteed after paying the ransom, some organizations take a calculated risk to pay in hopes of resuming normal operations. By doing so, they hope to reduce potential ancillary costs of attacks, including lost productivity, decreased revenue over time, exposure of sensitive data, and reputational damage. The ransomware threat is serious but smart preparation and ongoing vigilance are effective counters against it. The full armor of data security includes both human and technical controls but there are features of the AWS Cloud that help to mitigate ransomware attacks. AWS is committed to providing you with tools, best practices, and services to help with high availability, security, and resiliency to address bad actors on the internet.

Securing systems and data on AWS is a shared responsibility [DS(2)] [HJ3]

When you deploy applications and infrastructure in the AWS Cloud, AWS helps by sharing the security responsibilities with you. AWS engineers the underlying cloud infrastructure using secure design principles and customers must implement their own security architecture for workloads deployed on AWS. AWS is responsible for protecting the infrastructure that runs all of the services offered on the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. The AWS Cloud services that a customer selects determine the amount of configuration work the customer must perform as part of their security responsibilities. Customers are always responsible for managing and securing their data, classifying their assets, and using AWS Identity Access Management (IAM) to apply the appropriate permissions.

AWS Support

If you or your customer(s) believe an account is under an active ransom attack, the impacted customer should create a case from the AWS Support Center from within the impacted account. If the root user cannot be accessed or is compromised, then the customer should open a new AWS account and open a support ticket from there. [DS(4)] This process allows AWS to perform identity verification with the customer and also begin engaging internal resources to best help with remediating the event. [HJ5]

AWS Security Reference Architecture (AWS SRA)

The Amazon Web Services (AWS) Security Reference Architecture (AWS SRA) is a holistic set of guidelines for deploying the full complement of AWS security services

in a multi-account environment. It can be used to help design, implement, and manage AWS security services so that they align with AWS best practices.

U.S. Cybersecurity & Infrastructure Security Agency

The Ransomware Guide (Sept. 2020) provides best practices and references to help manage the risk posed by ransomware and support an organization's coordinated and efficient response to a ransomware incident.

The European Union Agency for Cybersecurity (ENISA)

The ENISA Threat Landscape 2020 - Ransomware outlines the findings on ransomware, provides a description and analysis of the domain, and lists relevant recent incidents. A series of proposed actions for mitigation is provided.

Australian Cyber Security Centre (ACSC)

The ACSC provides several guides including response to Ransomware in Australia, RANSOMWARE ATTACKS EMERGENCY RESPONSE GUIDE, and RANSOMWARE ATTACKS PREVENTION AND PROTECTION GUIDE.

NIST Cybersecurity Framework

The guide, NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud, is designed to help commercial and public sector entities of any size and in any part of the world align with the CSF by using AWS services and resources.

Ransomware mitigation: Top 5 protections and recovery preparation actions

AWS has provided a public Security Blog covering Ransomware mitigation: Top 5 protections and recovery preparation actions. These include:

- Set up the ability to recover your apps and data
- Encrypt your data
- Apply critical patches
- Follow a security standard
- Make sure you're monitoring and automating responses

You should also use strong authentication for exposed remote access services, notably remote desktop protocol and secure shell. Multifactor authentication combined with single sign-on is a technical mechanism that enables protection of remote connections and resource requests.

Amazon Elastic Compute Cloud (*Amazon EC2*) - Microsoft Windows

Identify

- Assess the security posture of the account to identify and remediate security gaps
    - AWS developed a new open source Self-Service Security Assessment tool that provides customers with a point-in-time assessment to gain valuable insights into the security posture of their AWS account.
- Maintain a complete asset inventory of all resources including domain controllers, Microsoft Windows EC2 instances, Microsoft Windows Servers and Databases, and any integration with external identity providers.
- Perform recurring vulnerability analysis of your hosts using utilities such as Amazon Inspector
- To protect your organization, Microsoft recommends that you use the information in the **Human-Operated Ransomware Mitigation Project Plan** PowerPoint presentation, which includes securing privileged access.
- Use CloudWatch metrics, specifically NetworkPacketsOut, to look for data exfiltration "spikes." It is possible an attacker performed data destruction and left a ransom note, and in these cases there is no opportunity for data recovery by working with the malicious actor

Protect

- Apply the latest updates to your operating systems and apps
- Back up your files with File History if your PC's manufacturer hasn't already turned it on. Learn more about File History
- Back up important files regularly. Use the 3-2-1 rule. Keep three backups of your data, on two different storage types, and at least one backup offsite
- Block Known Ransomware File Types
- Block Macros in Office Documents
- Educate your employees so they can identify social engineering and spear-phishing attacks
- Follow Best Practices for securing your Active Directory Services
- Follow Top 10 Most Important Group Policy Settings for Preventing Security Breaches
- Implement controlled folder access. It can stop ransomware from encrypting files and holding the files for ransom
- Perform backups of EC2 instances
    - Consider using AWS Backup or AWS CloudEndure
- The Microsoft 365 Defender Threat Intelligence Team has provided a comprehensive report identifying actions to secure your Microsoft resources prior to a ransomware event
    - Harden internet-facing assets and ensure they have the latest security updates. Use threat and vulnerability management to audit these assets regularly for vulnerabilities, misconfigurations, and suspicious activities.

    - Monitor for brute-force attempts. Check excessive failed authentication attempts (Windows security event ID 4625)
    - Monitor for clearing of Event Logs, especially the Security Event log and PowerShell Operational logs. Microsoft Defender ATP raises the alert "Event log was cleared" and Windows generates an Event ID 1102 when this occurs
    - Practice the principle of least-privilege and maintain credential hygiene. Avoid the use of domain-wide, admin-level service accounts. Enforce strong randomized, just-in-time local administrator passwords. Use tools like LAPS
    - Secure Remote Desktop Gateway using solutions like Azure Multi-Factor Authentication (MFA). If you don't have an MFA gateway, enable network-level authentication (NLA)
    - Turn on AMSI for Office VBA if you have Office 365
    - Turn on attack surface reduction rules, including rules that block credential theft, ransomware activity, and suspicious use of PsExec and WMI. To address malicious activity initiated through weaponized Office documents, use rules that block advanced macro activity, executable content, process creation, and process injection initiated by Office applications. To assess the impact of these rules, deploy them in audit mode
    - Turn on cloud-delivered protection and automatic sample submission on Windows Defender Antivirus. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats
    - Turn on tamper protection features to prevent attackers from stopping security services
    - Utilize the Windows Defender Firewall and your network firewall to prevent RPC and SMB communication among endpoints whenever possible. This limits lateral movement as well as other attack activities
- Turn on and update Windows Defender Antivirus - commericial, subscription paid Endpoint Detection and Response (EDR) solutions are preferred
- Turn on Controlled Folder Access in Windows 10 to protect your important local folders from unauthorized programs like ransomware or other malware
- Use Systems Manager and Amazon Inspector to check if EC2 instances running Microsoft Windows contain any common vulnerabilities and exposures (CVEs)
- Verify your backups and ensure the infection has not spread into them

Detect

- The Microsoft 365 Defender Threat Intelligence Team has provided a comprehensive report identifying things to look for against multiple ransomware variants

- Use VPCFlowLogs to identify inappropriate database access from external IP addresses
    - You can investigate VPC Flow with Amazon Detective or Amazon Athena

Respond

- Enforce NACLs based on network IoCs to prevent further traffic
- Isolate the infected systems
- Inspect backups for potential infection
- Remove any compromised systems from the network.
    - Follow regulatory requirements or internal company policy to determine if forensics of the EC2 instance is required
    - If forensics of the instances are required OR data needs to be recovered, then quarantine the EC2 instance
- Remove compromised Domain Controller metadata from the domain
- Use flow logs to determine the exfiltration IP, look for any other instances communicating with the IPs that data was exfiltrated to / access from CloudTrail

Recover

- It is recommended not to pay the ransom
    - Paying the ransom is a gamble as to whether the criminal will honor the transaction after receiving payment
    - If no data backups exist, then you should do a cost benefit analysis and weigh the value of the data/reputational compromise against the payment to the attacker
    - You directly enable the attacker to continue their operations against your company or others if you choose to pay the ransom
- Create new EC2 instances from a trusted AMI
- Use CloudEndure Disaster Recovery to select the latest recovery point before the ransomware attack or data corruption to restore your workloads on AWS
    - If using an alternate data backup strategy, validate the backups have not been infected and restore from the last scheduled event prior to the ransomware event
- Visit https://www.nomoreransom.org/ to identify if a decryptor is available for the malware variant the infected your data

Amazon Elastic Compute Cloud (*Amazon EC2*) - Unix/Linux

Identify

- Assess your security posture to identify and remediate security gaps
    - AWS developed a new open source Self-Service Security Assessment tool that provides customers with a point-in-time assessment to quickly gain valuable insights into the security posture of their AWS account.

- Maintain a complete asset inventory of all resources including servers, networking devices, network/file shares and developer machines
- Perform recurring vulnerability analysis of your hosts using utilities such as Amazon Inspector
- Use CloudWatch metrics, specifically NetworkOut, to look for data exfiltration "spikes." It is possible an attacker performed data destruction and left a ransom note, and in these cases there is no opportunity for data recovery by working with the malicious actor

Protect

- Apply the latest updates to your operating systems and apps
- Back up important files regularly. Use the 3-2-1 rule. Keep three backups of your data, on two different storage types, and at least one backup offsite
- Block Known Ransomware File Types
- Consider using AWS Config to create rules to monitor for changes to AWS services. AWS Config has several managed rules prebuilt to monitor EBS and EC2 including:
    - ebs-in-backup-plan
    - ebs-optimized-instance
    - ebs-snapshot-public-restorable-check
    - ec2-ebs-encryption-by-default
    - ec2-imdsv2-check
    - ec2-instance-detailed-monitoring-enabled
    - ec2-instance-managed-by-systems-manager
    - ec2-instance-multiple-eni-check
    - ec2-instance-no-public-ip
    - ec2-instance-profile-attached
    - ec2-managedinstance-applications-blacklisted
    - ec2-managedinstance-applications-required
    - ec2-managedinstance-association-compliance-status-check
    - ec2-managedinstance-inventory-blacklisted
    - ec2-managedinstance-patch-compliance-status-check
    - ec2-managedinstance-platform-check
    - ec2-security-group-attached-to-eni
    - ec2-stopped-instance
    - ec2-volume-inuse-check
- Educate your employees so they can identify social engineering and spear-phishing attacks
- Have malware detection and antivirus enabled on all systems - commercial, subscription paid Endpoint Detection and Response (EDR) solutions are preferred.
    - An example guide can be found at How to Install and Use Linux Malware Detect (LMD) with ClamAV as Antivirus Engine
- Perform backups of EC2 instances
    - Consider using AWS Backup or AWS CloudEndure

- The Microsoft 365 Defender Threat Intelligence Team has provided a comprehensive report identifying actions to secure Microsoft resources prior to a ransomware event. Many of these recommendations can be adapted for Unix & Linux including:
    - Determine where highly privileged accounts are logging on and exposing credentials.
    - Harden internet-facing assets and ensure they have the latest security updates. Use threat and vulnerability management to audit these assets regularly for vulnerabilities, mis-configurations, and suspicious activities.
    - Monitor for brute-force attempts. Check excessive failed authentication attempts (/var/log/auth.log or /var/log/secure)
    - Monitor for clearing of Event Logs
    - Practice the principle of least-privilege and maintain credential hygiene. Avoid the use of domain-wide, admin-level service accounts. Enforce strong randomized, just-in-time local administrator passwords.
    - Turn on tamper protection features to prevent attackers from stopping security services
- Use an endpoint security agent such as Wazuh
- Use a file integrity monitor such as Tripwire to detect changes to critical files
- Use Systems Manager and Amazon Inspector to check if EC2 instances contain any common vulnerabilities and exposures (CVEs)
- Verify your backups and ensure the infection has not spread into them

Detect

- Table 1 from No Strings on Me: Linux and Ransomware, by Richard Horne, identifies multiple indicators to monitor for including:
    - A new process that has never been seen on the endpoint prior that has external network connectivity requests
    - Attempted communications with DNS names where entropy is found or directly with bare IPs
    - Change in distribution Yum or Apt repositories
    - Creation of .sh files inside of non-user-based home directories
    - Enumeration of shared web, database, or file storage directory trees
    - Escalation of privileges or attempts to gain sudo access
    - External as well as internal network communications
    - File names generated with entropy or that are in a quick succession
    - Files being renamed multiple times in the same directory tree
    - Files created with odd file extensions
    - Focus being given to outliers and events that fall outside of the typical day to day operations
    - High memory usage for short or sustained periods of time
    - Large process tress where the Parent Process is terminated prior to the child processes

    - Modification of boot options
    - Multiple copies of the same file in multiple directories
    - Multiple modifications within a single directory
    - Possible calls for encryption libraries
    - Possible creation and running of processes inside of the/tmp directory
    - Quick and successive directory enumeration
    - Removal of files from directories using wildcards or without confirmation
    - The use of chmod with wildcards (or chmod 777)
    - The use of wget or curl cmds
    - Use of the chmod cmd to change executable files to overly permissive rights
    - Use of the strings cmd to attempt to encode communications prior to or during infection
- Use VPCFlowLogs to identify inappropriate database access from external IP addresses
    - You can investigate VPC Flow with Amazon Detective or Amazon Athena

Respond

- Inspect backups for potential infection
- Isolate the infected systems
- Remove any compromised systems from the network.
    - Follow regulatory requirements or internal company policy to determine is forensics of the EC2 instance is required
    - If forensics of the instances are required OR data needs to be recovered, then quarantine the EC2 instance

Recover

- It is recommended not to pay the ransom
    - Paying the ransom is a gamble as to whether the criminal will honor the transaction after receiving payment
    - If no data backups exist, then you should do a cost benefit analysis and weigh the value of the data/reputational compromise against the payment to the attacker
    - You directly enable the attacker to continue their operations against your company or others if you choose to pay the ransom
- Create new EC2 instances from a trusted AMI
- Follow regulatory requirements or internal company policy to determine if forensics of the EC2 instance is required
- Use CloudEndure Disaster Recovery to select the latest recovery point before the ransomware attack or data corruption to restore your workloads on AWS

    - If using an alternate data backup strategy, validate the backups have not been infected and restore from the last scheduled event prior to the ransomware event
- Visit https://www.nomoreransom.org/ to identify if a decryptor is available for the malware variant the infected your data

Amazon Simple Storage Service (S3)

Identify

- Assess your security posture to identify and remediate security gaps
    - AWS developed a new open source Self-Service Security Assessment tool that provides customers with a point-in-time assessment to gain valuable insights into the security posture of their AWS account.
- Consider implementing AWS GuardDuty to continuously monitor for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3
- Consider using AWS Config, which is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources
- Darkbit provides an example of AWS S3 Data Loss Prevention that can be used to identify unauthorized copying of objects. Other specific operations could be added in the pattern as well based upon your business use case(s)
- Maintain a complete asset inventory of all resources including servers, networking devices, network/file shares and developer machines

Protect

- Consider enabling replication - same region or cross region. Cross region replication protects data against application defects and operator errors by maintaining a second copy in another region
- Consider using AWS Config to create rules to monitor for changes to AWS services. AWS Config has several managed rules prebuilt to monitor EBS and EC2 including:
    - s3-account-level-public-access-blocks
    - s3-account-level-public-access-blocks-periodic
    - s3-bucket-blacklisted-actions-prohibited
    - s3-bucket-default-lock-enabled
    - s3-bucket-level-public-access-prohibited
    - s3-bucket-logging-enabled
    - s3-bucket-policy-grantee-check
    - s3-bucket-policy-not-more-permissive
    - s3-bucket-public-read-prohibited
    - s3-bucket-public-write-prohibited
    - s3-bucket-replication-enabled
    - s3-bucket-server-side-encryption-enabled
    - s3-bucket-ssl-requests-only
    - s3-bucket-versioning-enabled
    - s3-default-encryption-kms

- Consider using AWS Key Management Service (KMS) keys to encrypt all objects and to prevent an attacker from applying their encryption key
- Consider using AWS S3 Block Public Access Feature to mitigate unintentional exposure of objects
- Consider using S3 Intelligent Tiering for object backups and cost optimization
- Consider using S3 Object Lock so you can store objects using a *write-once-read-many* (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely.
    - In Object Lock Compliance Mode**,** a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode ***ensures*** that an object version can't be overwritten or deleted for the retention period's duration.
- Enable CloudTrail event logging for S3 buckets and objects containing sensitive or critical information. By default, CloudTrail trails don't log data events, but you can configure trails to log data events for S3 buckets that you specify, or to log data events for all the Amazon S3 buckets in your AWS account.
- Enable CloudTrail server level logging for S3 buckets and objects containing sensitive or critical information. Server access logging provides detailed records for the requests that are made to a bucket
- Enable S3 Object Versioning to allow restoral of modified objects
    - To set the number of versions kept, set a lifecycle policy to apply to noncurrent versions
- Enable S3 MFA delete to prevent an attacker from disabling versioning and overwriting all objects within a bucket
- Enforce multi-factor authentication (MFA)
- Enforce password complexity requirements and establish expiration periods
- Implement CIS AWS Foundations including expiration of accounts and mandatory credential rotations
- Run an IAM Credential Report to list all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices
- Take steps to prevent any new credentials from being publicly exposed
- Use AWS IAM Access Analyzer to identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles that are shared with an external entity. This lets you identify unintended access to your resources and data, which is a security risk
- Use IAM roles to manage permissions
    - Implement least-privilege and do not allow s3:* permissions
- Use and routinely audit bucket policies
    - Only make public what *needs* to be, and ensure all of objects are protected by being private

- While we cannot recommend specific third-party solutions, there are also products from our Partners, including Veritas and CommVault, and other backup software providers that have the native capability to backup objects in S3 to their managed backup storage locations inside or outside of S3

Detect

- Check your CloudTrail log for unsanctioned activity such as creation of unauthorized IAM users, policies, roles or temporary security credentials
- Check your CloudTrail log to review your AWS account for any unauthorized AWS usage, such as unauthorized EC2 instances, Lambda functions, or EC2 Spot bids. You can also check usage by logging into your AWS Management Console and reviewing each service page. The "Bills" page in the Billing console can also be checked for unexpected usage
    - Please keep in mind that unauthorized usage can occur in any region and that your console may show you only one region at a time. To switch between regions, you can use the dropdown in the top-right corner of the console screen
- Ransom note provided either as an object within the bucket or via e-mail to the customer
- S3 Objects are deleted or entire S3 buckets are deleted
    - Note: With data destruction events, a ransom note may or may not be provided. Also ensure you check CloudWatch metrics and CloudTrail S3 events to verify if data exfiltration occurred or not to delineate between a ransom or data destruction attack
- S3 Objects are encrypted using a key from an account not owned by the customer

Respond

- Delete or rotate IAM User Keys and Root User Keys; you may wish to rotate all keys in your account if you cannot identify a specific key or keys that has been exposed
- Delete unauthorized IAM Users
- Delete unauthorized policies
- Delete unauthorized roles
- If your application uses exposed Access Keys, you need to replace the Key. To replace the Key, first create a second Key (at that point, both Keys will be active) and then modify your application to use the new Key. Then disable (but do not delete) exposed Keys by clicking on the “Make inactive” option in the console. If there are any problems with your application, you can reactivate exposed Keys. When your application is fully functional using the new Key, please delete exposed Keys
- Revoke temporary credentials. Temporary credentials can also be revoked by deleting the IAM User. *NOTE:* Deleting IAM Users may impact production workloads and should be done with care

Recover

- It is recommended not to pay the ransom
    - Paying the ransom is a gamble as to whether the criminal will honor the transaction after receiving payment
    - If no data backups exist, then you should do a cost benefit analysis and weigh the value of the data/reputational compromise against the payment to the attacker
    - You directly enable the attacker to continue their operations against your company or others if you choose to pay the ransom
- Implement procedures under Protect before attempting to restore data or objects
- Remove delete markers for versioned objects
- Re-create deleted buckets
- Restore objects from using S3 Intelligent Tiering object backups or replicated region bucket
- *Note:* There is currently no "undelete" capability for S3, and AWS does not have the ability to recover data that has been deleted. In the current era of data storage compliance and regulations such as GDPR and CCPA, Amazon S3 cannot continue to store customer data explicitly deleted from the customer's account. Once an object is deleted, it can no longer be recovered by AWS regardless of how quickly the unintended deletion is reported to AWS

Relational Database Service (RDS)

Identify

- Assess your security posture to identify and remediate security gaps
    - AWS developed a new open source Self-Service Security Assessment tool that provides customers with a point-in-time assessment to gain valuable insights into the security posture of their AWS account.
- Consider using AWS Config, which is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources
- Consider implementing AWS GuardDuty to continuously monitor for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon RDS
- Maintain a complete asset inventory of all resources including servers, networking devices, network/file shares and developer machines

Protect

- Additional references and steps are available in Security in Amazon RDS
- Consider using AWS Config to create rules to monitor for changes to AWS services. AWS Config has several managed rules prebuilt to monitor RDS including:
    - rds-automatic-minor-version-upgrade-enabled
    - rds-cluster-deletion-protection-enabled
    - rds-cluster-iam-authentication-enabled

    - rds-cluster-multi-az-enabled
    - rds-enhanced-monitoring-enabled
    - rds-instance-deletion-protection-enabled
    - rds-instance-iam-authentication-enabled
    - rds-instance-public-access-check
    - rds-in-backup-plan
    - rds-logging-enabled
    - rds-multi-az-support
    - rds-snapshots-public-prohibited
    - rds-snapshot-encrypted
    - rds-storage-encrypted
- Have a third-party host-based intrusion detection system (HIDS) solution (such as OSSEC, Tripwire, Wazuh, Amazon Inspector)
- Run your DB instance in a virtual private cloud (VPC) based on the Amazon VPC service for the greatest possible network access control. For more information about creating a DB instance in a VPC, see Amazon Virtual Private Cloud VPCs and Amazon RDS.
- Use AWS Identity and Access Management (IAM) policies to assign permissions that determine who is allowed to manage Amazon RDS resources. For example, you can use IAM to determine who is allowed to create, describe, modify, and delete DB instances, tag resources, or modify security groups.
- Use Amazon RDS encryption to secure your DB instances and snapshots at rest. Amazon RDS encryption uses the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your DB instance. For more information, see Encrypting Amazon RDS resources
- Use Secure Socket Layer (SSL) or Transport Layer Security (TLS) connections with DB instances running the MySQL, MariaDB, PostgreSQL, Oracle, or Microsoft SQL Server database engines. For more information on using SSL/TLS with a DB instance, see Using SSL/TLS to encrypt a connection to a DB instance
- Use security groups to control what IP addresses or Amazon EC2 instances can connect to your databases on a DB instance. When you first create a DB instance, its firewall prevents any database access except through rules specified by an associated security group.
- Use network encryption and transparent data encryption with Oracle DB instances; for more information, see Oracle native network encryption and Oracle Transparent Data Encryption
- Use security features of your DB engine to control who can log in to the databases on a DB instance. These features work just as if the database was on your local network.

Detect

- AWS GuardDuty machine learning can detect suspicious behavior including Generating Amazon Relational Database Service (Amazon RDS) snapshots as

part of data exfiltration attempts. An example is provided in the AWS Security Blog How you can use Amazon GuardDuty to detect suspicious activity within your AWS account

- Review EC2 operating system and application logs for inappropriate logins, installation of unknown software, or the presence of unrecognized files
- Use VPCFlowLogs to identify inappropriate database access from external IP addresses
    - You can investigate VPC Flow with Amazon Detective or Amazon Athena
    - The AWS Security Analytics Bootstrap enables customers to perform security investigations on AWS service logs by providing an Amazon Athena analysis environment that's quick to deploy, ready to use, and easy to maintain

Respond

- Delete or rotate IAM User Keys and Root User Keys; you may wish to rotate all keys in your account if you cannot identify a specific key or keys that has been exposed
- Delete unauthorized IAM Users
- Delete unauthorized policies
- Delete unauthorized roles
- Delete unrecognized or unauthorized public snapshots or databases
- Identify an EC2 instances that had permissive access to the database(s) and investigate those as well
- If your application uses exposed Access Keys, you need to replace the Key. To replace the Key, first create a second Key (at that point, both Keys will be active) and then modify your application to use the new Key. Then disable (but do not delete) exposed Keys by clicking on the "Make inactive" option in the console. If there are any problems with your application, you can reactivate exposed Keys. When your application is fully functional using the new Key, please delete exposed Keys
- Revoke temporary credentials. Temporary credentials can also be revoked by deleting the IAM User. *NOTE:* Deleting IAM Users may impact production workloads and should be done with care

Recover

- It is recommended not to pay the ransom
    - Paying the ransom is a gamble as to whether the criminal will honor the transaction after receiving payment
    - If no data backups exist, then you should do a cost benefit analysis and weigh the value of the data/reputational compromise against the payment to the attacker
    - You directly enable the attacker to continue their operations against your company or others if you choose to pay the ransom
- Delete the compromised database and create new RDS databases

- Follow regulatory requirements or internal company policy to determine if forensics of the RDS database is required
- Visit https://www.nomoreransom.org/ to identify if a decryptor is available for the malware variant the infected your data
- Use CloudEndure Disaster Recovery to select the latest recovery point before the ransomware attack or data corruption to restore your workloads on AWS
    - If using an alternate data backup strategy, validate the backups have not been infected and restore from the last scheduled event prior to the ransomware event

Following an Incident

Report Ransom Attacks to Authorities

The FBI encourages organizations to report ransom incidents to law enforcement. The Internet Crime Complaint Center (IC3) accepts online internet crime complaints either from the actual victim or from a third party to the complainant and will work with them to determine the best course of action going forward. Be prepared to share:

- Any relevant information you believe is necessary to support your complaint
- Email header(s)
- Financial transaction information (account information, transaction date and amount, recipient details)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- Victim's name, address, telephone, and email

Perform root cause analysis

In most cases, your existing forensics tools will work in the AWS environment. Forensic teams will benefit from the automated deployment of tools across AWS Regions and the ability to collect large volumes of data quickly with low friction using the same robust, scalable services their business-critical applications are built on.

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects AWS service log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to conduct faster and more efficient security investigations.

Update security program with lessons learned

Documenting and cycling lessons learned during simulations and live incidents back into "new normal" processes and procedures allows organizations to better

understand how they were breached – such as where they were vulnerable, where automation may have failed, or where visibility was lacking – and the opportunity to strengthen their overall security posture.

Train your employees

Train your employees through an effective security awareness program. This needs to be made entertaining and engaging. Focusing on reporting phishing, notification procedures, and how to report “bad” things then awarding that behavior can be very effective.

Conclusion

Ransom attacks are evolving, but so can your security awareness and preparedness. Government agencies, nonprofits, and businesses around the world trust AWS to power their infrastructure and keep their systems and data secure. Using the AWS services and best practices shared in this guidebook, you can take proactive measures to reduce the likelihood and impact of ransom in your AWS environments.