Incident Response Playbook Template

Incident Type

Ransomware

Introduction

This playbook is provided as a template to customers using AWS products and who are building their incident response capability. You should customize this template to suit your particular needs, risks, available tools and work processes.

Security and Compliance is a shared responsibility between you and AWS. AWS is responsible for “Security of the Cloud”, while you are responsible for “Security in the Cloud”. For more information on the shared responsibility model, please review our documentation (https://aws.amazon.com/compliance/shared-responsibility-model/).

You are responsible for making your own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) references current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. This document is provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. 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.

Summary

This Playbook

This playbook outlines response steps for handling ransomware incidents. These steps are based on the NIST Computer Security Incident Handling Guide (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) (Special Publication 800-61 Revision 2) that can be used to:

• Gather evidence • Contain and then eradicate the incident • recover from the incident • Conduct post-incident activities, including post-mortem and feedback processes

Interested readers may also refer to the AWS Security Incident Response Guide (https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/welcome.html) which contains additional resources.

Once you have customized this playbook to meet your needs, it is important that you test the playbook (e.g., Game Days) and any automation (functional tests), update as necessary to achieve the desired results, and then publish to your knowledge management system and train all responders.

Note that some of the incident response steps noted below may incur costs in your AWS account(s) for services used in either preparing for, or responding to incidents. Customizing this playbook and testing it will help you to determine if additional costs will be incurred. You can use AWS Cost Explorer (https://aws.amazon.com/aws-cost-management/aws-cost-explorer/) and look at costs incurred over a particular time frame (such as when running Game Days) to establish what the possible impact might be.

In reviewing this playbook, you will find steps that involve processes that you may not have in place today. Proactively preparing for incidents means you need the right resource configurations, tools and services in place that allow you to respond to an incident.

The next section will provide a summary of this incident type, and then cover the five steps (parts 1 - 5) for handling ransomware incidents.

This Incident Type

Ransomware is malicious code designed by threat actors to gain unauthorized access to systems and data and to encrypt the data to block access by legitimate users. Once ransomware has locked users out of their systems and/or encrypted their sensitive data, the actors demand a ransom. In theory, if the ransom is paid, access to the data is returned (such as by providing an encryption key), but equally, some studies have suggested the victim will subsequently be attacked again. Alternatively, if not paid, the organization risks permanent data loss and/or data leaks to the public, competitors or other malicious actors.

There are usually limited options to mitigate a successful ransomware attack once it has occurred. The best mitigation is to reduce the chance that it can happen in the first place. The AWS Well-Architected security pillar provides a framework to implement AWS best practice, including operating workloads security (security foundations section), protecting compute resources (infrastructure protection section) and others. The security pillar encompasses the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security. This playbook covers steps that can be used to deal with ransomware.

Incident Response Process

Part 1: Acquire, Preserve, Document Evidence

1. You become aware that a possible ransomware incident has occurred. This information could come via different means, depending on your configurations in your AWS environment:

2. A colleague reports that an EC2 instance cannot be accessed by SSH or similar, however the instance appears to be correctly configured with appropriate network access in place, and there are no related service issues reported by AWS in the Service Health Dashboard

3. Your ticketing system creates a ticket for unusual metrics or logs from the EC2 instance
4. The instance is reporting network reachability issues in the AWS console, or via Amazon CloudWatch alarms
5. Message from threat actor through alternate communication channel such as email about the ransom demand
6. Findings through services like AWS Security Hub or Amazon GuardDuty.
7. Other alarms or metrics you have configured in your monitoring systems, either internal or external to AWS
8. Once you confirm that an event is a security incident, it is important to determine the scope of impact (quantity of resources as well as sensitivity of data).
9. Determine if there are any known events that could be causing service disruption, or impacting instance metrics (e.g., network CloudWatch metrics increasing due to a sales event, or similar)
10. Use Amazon Detective to investigate any ongoing activity using the time based analysis or a specific period when the incident was identified to identify any deviations from a “normal” operating baseline.
11. Obtain the application’s documented baseline and locate the metrics for standard application performance from the CloudWatch or other application performances monitoring tool used in the organization to compare baseline behavior to anomalous behavior as a result of the incident.
12. Determine the classification level of any data that resides in the EC2 instance, S3 bucket, Amazon Workspaces instance, etc.
13. Confirm a ticket/case has been raised for the incident. If not, manually raise one.
14. If you received an abuse notification from AWS, determine if any cases are already open for the resource that can be correlated to the abuse notification. This may provide indications relating to prior unauthorized activity.
15. If there is a ticket/case already opened, determine what internal alarms/metrics are currently indicating an issue (if automated, what caused the ticket to be created?) If the ticket/case creation was not initiated automatically by an alarm or metric, document the alert/notification that led to identification of the issue if there was one (for example, a ransom demand popping up on the screen, or metrics that indicate the device is no longer on the network). If the incident was identified by an indicator that does not conclusively identify a ransomware incident as the cause, then verify the service disruption is not due to any planned (or other) event and document the actual vector.
16. Identifying the ransomware strain is key to recovery. For example, if objects in S3 buckets are inaccessible with an error of not having encryption key access, the first step would be to review the S3 object properties section to understand the encryption key applied. A similar approach can be leveraged with the Amazon Elastic Block Store (EBS)volumes in situations involving crypto ransomware.
17. Using your preferred monitoring tool, access AWS CloudTrail and search for any API actions which indicates any credential compromise attack vector and refer to the playbook, “Credential Leakage/Compromise”.
18. Determine when the infection occurred using log search. CloudWatch can help you to review logs such as application logs, operating system logs, database logs, etc.

19. Determine the business impact:

a. Identify application(s) impacted; this may be achieved via Resource Tags, or by an internal Configuration Management Database (CMDB)
b. Identify business owner and workload classification (example: mission critical, high risk, etc.)

12. Determine and begin to document end-user impact/experience of the issue. This should be documented in the ticket/case related to the incident. If there are impacted users, determine from them the steps that led to the incident. This will assist you to establish the attack vector used to execute the ransomware. Mitigations against this vector should be placed in later steps of this process.
13. Internal Communications:

a. Identify stakeholder roles from your organization's incident response plan, the application entry in the Configuration Management Database CMDB (if one exists), or via the application's risk register
b. Open an Incident Response bridge to have a regular communication channel about the incident.
c. Notify identified stakeholders including (if required) legal personnel, technical teams and developers and add them to the ticket and the war room, so they are updated as the ticket is updated

14. External Communications:

i. Ensure your organization's legal counsel is informed and is included in status updates to internal stakeholders and especially in regards to external communications.

ii. For colleagues in the organization that are responsible for providing public/external communication statements, ensure these internal stakeholders are added to the ticket so they receive regular status updates regarding the incident and can complete their own requirements for communications within and external to the business.
iii. If there are regulations in your jurisdiction requiring reporting of such incidents, ensure the people in your organization responsible for notifying local or federal law enforcement agencies are also notified of the event. Consult your legal advisor and/or law enforcement for guidance on collecting and preserving the evidence and the chain of custody.
iv. There may not be regulations, but either open databases, government agencies or NGOs may track this type of activity. Your reporting may assist others

Part 2: Contain the Incident

Early detection of anomalous user behavior or network activity is key to reducing the impact of ransomware incidents. The below steps can be taken to help to contain the incident. If applicable, work with the legal and compliance team of your organization on any required response and continue the incident response process outlined here.

1. If possible, determine the type of ransomware used in the incident:

a. Crypto Ransomware - Objects/files will be encrypted
b. Locker ransomware - Locks out access to the device
c. A different type, or previously not observed type

2. For identified AWS resources associated with your impacted workloads, isolate network or internet connectivity by modifying Security groups, S3 bucket Policies or relevant identity and access management policies as applicable to minimize opportunities for the infection to be spread, or for threat actors to have access to those resources.

Keep in mind that sometimes modifying security groups may not have the intended impact, due to connection tracking.

3. Determine whether the EC2 instance actually needs to be recovered, or not. For example, if the impacted instance is part of an AWS Application Auto Scaling group, removing the instance from the group will trigger a scaling action. If the incident is linked to a vulnerable package on the host's operating system, updating the AMI used in the Launch configuration and confirming the vulnerability has been patched (check the Mitre CVE database) will also be required.
4. Check your CloudTrail log for unauthorized activity such as creation of unauthorized IAM users, policies, roles or temporary security credentials. Delete any unauthorized IAM users, roles, and policies, and revoke any temporary credentials.
5. If you're dealing with this incident as part of a broader security incident in the account, a drastic approach could be to use AWS Organizations Service Control Policies (SCPs) to restrict any API call to be made from that AWS account (assuming it is not the master account of the Organization). Please note this may impact other running workloads as SCPs applied at the account level will be enforced on all the IAM entities associated in it. This may prevent malicious actors from inflicting further damage on the account's resources and data.
6. If the attack vector was made possible by un-patched software, operating system updates, out-of-date malware/anti-virus tools, ensure that all EC2 instances are either updated to the latest version of operating system, all software packages and patches are up-to-date and virus signatures and definition files on all EC2 instances are up-to-date. This may be done by several methods:

a. Patch-in-place for mutable architectures
b. Re-deploy for immutable architectures

7. Depending on what occurred in Step 6 above, remove any remaining resources that are identified as being at risk of infection (that may have accessed the same vector that downloaded the ransomware, whether that be via email, visiting an infected website, or something else). If it is part of a larger fleet managed by Auto Scaling, containment efforts may be better focused on establishing the attack vector and then placing mitigations that will prevent other resources in the fleet from becoming infected via the same vector.

Part 3: Eradicate the Incident

1. It is important to understand if the impact from the incident is contained to a subset of the environment. If there is an ability to restore the ransomed data from backups/snapshots, you can refer to the recover from the incident section. Note that there may still be value in exploring the incident under an isolated environment to run the root cause analysis and use controls to avoid situation in the future.
2. Investigate potential use of up-to-date antivirus or anti-malware software to clean the ransomware. Refer to this step with caution as it may alert the actor (see earlier steps to remove network access from the impacted EC2 instance). You can review the locked/encrypted objects in an isolated forensic environment.
3. Review any GuardDuty findings if there are any high or medium severity alerts that can help to reduce the additional effort required to search application level logs. GuardDuty findings provide recommendations on how to remediate the finding.
4. Remove any malware that was identified during the forensic analysis and identify Indicators of Compromise.
5. If the ransomware strain has been identified, determine if any 3rd party decryption tools are available, or if any other online resources may help

Part 4: Recover from the Incident

1. Identify the restore point for any restore operation performed from backup.
2. Review the backup strategy and see if you can recover all the objects and files. This will depend on the lifecycle policies applied on the resources.
3. Restore the data from your backup, or revert to an earlier snapshot of the EC2 instance's volumes. Apply forensic methods to confirm that data is clean before restoring it. Ensure any spread vectors are identified & resolved.
4. Alternatively, if you have been successful in using any open source de-crypter tool to retrieve the data, remove that data from the instance and perform any required analysis to ensure the data is clean. Then, recover the instance, terminate it or quarantine it and create a new one, and restore the data to a new instance.
5. If restoring from a backup and de-crypting the data is not an option, consider whether to start from entirely new environment is a possibility .

Part 5: Post-Incident Activity

1. Documenting and cycling lessons learned during simulations and live incidents back into "new normal" processes and procedures allows organizations to better understand how an incident occurred with their configurations and processes – 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.
2. If you identified the initial attack vector or point of entry, determine how best to mitigate the risk of a re-occurrence. For example, if the malware gained initial entry due to an un-patched public-facing EC2 instance, and assuming you applied the missing patch to all current instances, how can you improve your patching process to ensure that patches are tested and applied sooner and with more consistency and reliability?
3. If you've developed set technical steps to take for a given threat, assess opportunities to automate those actions upon detection to mitigate the threat as quickly as possible to minimize scope and severity of impact.
4. Ensure you collect lessons learned from all stakeholders and update your incident response plan, disaster recovery plans, and this playbook as necessary. And where appropriate, consider priorities and funding for new technical capabilities and personnel skills to fill any gaps.

Appendix A

Preparation

As with other incident response scenarios, mitigating ransomware threats requires a strong preventative strategy and preparation is very important. More so than others though, mitigation techniques rely on adequate preparation prior to a ransomware incident. Implementing best practices based on the AWS Well-Architected Framework will help you in your preparation. If key preventative measures are not already in place, these must be considered as part of any post-incident activity including any tools or techniques that failed during the incident response process itself, such as automation, integration with partner offerings, application and systems observability, etc. The below points cover some key preparation steps.

1. Adopt foundational best practices: Leverage AWS Cloud Adoption Framework (CAF) and AWS Well-Architected best practices to your organization's cybersecurity framework such as the NIST CyberSecurity Framework for

AWS, a framework focused on security outcomes organized around five functions (Identify, Protect, Detect, Respond, Recover) and foundational activities that map to existing standards, accreditations and frameworks.

2. Training: Cybersecurity awareness training for your employees. Social engineering is one of the common methods used to induce end users to download an infected file.
3. Deep dive on assets and configurations: Identifying your IT assets is a vital component of governance and security. You must have visibility into all your data storage services and resources in order to evaluate their security posture and effectively configure them. Reduce potential attack surface, for instance, by analysing your public data footprint. If you use Amazon Simple Storage Service (S3), ensure that your S3 buckets use the correct policies and are not publicly accessible. Implement the idea of least privilege enterprise-wide. With S3 Versioning, existing versions of your data are immutable: actors cannot change existing objects, and any modification is going to result in a new version. Use MFA delete to require a second element of authentication for S3 data deletion. In addition, S3 includes a number of security controls to consider when developing and implementing your own security policies; for more information, please see security best practices for Amazon S3 (https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html).
4. Stay up-to-date with system patches: Ransomware often relies on exploit kits to gain access to a system or network using known threats. Amazon Elastic Compute Cloud (Amazon EC2) resources can use AWS Systems Manager to automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems. These capabilities enable automated configuration and ongoing management of systems at scale, and help maintain software compliance for instances running in EC2.
5. Continuous monitoring:

a. Use Amazon Inspector to assess your deployed EC2 instances for CVEs and deviation from best practice. Build a CI/CD pipeline to remediate security findings automatically & periodically. Amazon Inspector finds applications by querying the package manager or software installation system on the operating system where the agent is installed. This means that software that was installed through the package manager is assessed for vulnerabilities. You can also leverage AWS Security Competency Partner offerings to help inspect your application deployments for security risks and vulnerabilities, while providing priorities and advice to assist with remediation.
b. AWS developed a new open source Self-Service Security Assessment tool (with ransomware analysis modules) that provides customers with a point-in-time assessment to quickly gain valuable insights into the security posture of their AWS account. For continuous monitoring of your security posture, AWS recommends enabling AWS Security Hub's Foundational Security Best Practices standard, which also provides automated security checks.

6. Data back-up: Create secure backups of your data on a regular basis. AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services. If backups are not a requirement, ensure that there are regular snapshots or an up-to-date AMI that can be used either for recovery or replacement of the impacted EC2 instance. Amazon S3 and Amazon Glacier are durable, low-cost storage platforms. Both offer unlimited capacity and require no volume or media management as backup data sets grow. Backup and Recovery Approaches Using AWS.
7. Testing: Implement, review and test disaster recovery scenarios for your organizational needs. This will help you determine the path for implementing recovery mechanisms and mitigate risks. Disaster recovery is about preparing for and recovering from an event that has a negative impact on your business goals. You can use CloudEndure Disaster Recovery to quickly recover your environment, minimizing data loss and downtime in the case of a ransomware incident.

8. Automation: Where you identify fixed technical procedures that don’t deviate or require a human to make a decision, explore the opportunity to automate protections and response actions to mitigate the threat as quickly as possible to minimize scope and severity of impact. Communication channels: Identify communication channels such as an Incident Response bridge that you will need to use during the incident to communicate with the internal and external stakeholders.