CYBER VT2022

Case 4 Cyber Security Incident Response

Group #10

Jawdat Kour
Hideo Tommaso Nishimura
Anas Kwefati
Munish Sharma

The incident:

High CPU usage on one of two database backend servers because of running multiple instances of remote copy operation outside the work time by one of the authorized financial accounts that have access to all account records.

We follow the incident handling steps mentioned in NIST SP 800-61/ Table 3-5 to handle the Casino's security incident.

Table 3-5. Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Classification

We classify the event as a critical computer security incident, as it is done from an account with access to records of all registered accounts and those accounts contain personally identifiable information and payment card information.

Following the Incident taxonomy, the incident has been classified as deliberate action. If the incident was carried out by an employee it would be unauthorized use of resources. It could also be a masquerade if someone illegitimately assumed the identity of an employee in order to gain access to the information.
The severity of the attack is very high, as it is personally identifiable information and payment card information, and consequently, the priority of the incident handling is high. Though there is no functional impact and the recoverability effort at this stage is viewed as regular as defined by NIST Sp 800-61, the incident is a privacy breach, and the level and amount of information demand a high priority.

Detection and analysis

This step includes determining whether an action deviates from normal operations within the organisation. Someone with an authorized account has been transferring information from all registered accounts:

1. Analyze the precursors and indicators

- High usage of CPU power on one of the database backend servers
- Multiple instances of /bin/scp
- Activity outside of normal work hours

1.1 Perform research (i.e. search engines, knowledge base)

1.2 Determine/identify the breach by collecting information such as:

- What was the time of the event: 03.43
- How was it discovered and by whom: the incident response manager
- What is the scope of the compromise: all registered accounts
- What was the entry point discovering: Database backend servers
- What are the potential effects on the operations: loss of customers, loss of reputation, possible civil lawsuits

2. Prioritize handling the incident based on the relevant factors:

- As the severity of the attack is very high (due to being about personally identifiable information and payment card information) the priority of the incident handling is high.

3. Report the incident to the appropriate internal personnel and external organizations:

- Following the security incident management plan we contact the IRT team members and appropriate stakeholders in the organization, including escalation information.

Containment, Eradication & Recovery

4. Acquire, preserve, secure, and document evidence

Potential evidence regarding the incident should be acquired, and preserved by making a forensic disk image or copies of log files and login sessions that might contain evidence that is related to the incident. Make sure that established procedures for gathering and handling evidence are followed, and all acquired evidence is clearly documented, listed, and stored in a secure location. When evidence is later handled, the chain of custody forms should be signed by the people handling the evidence.

5. Contain the incident

In order to contain the potential security incident, the following steps are taken:

- Isolating the backend server
- Potentially breached user account is disabled and passwords reset/restored
- Any additional account that is found to be compromised during evidence gathering should be disabled and passwords reset/restored
- Make forensics copies of logs and other crucial information of the affected system and carry out another analysis to trace and prove what happened.

Long term measures:

- Make a screening of all employees
- Limit access only during office hours for all employees to remove the risk of it happening again. Withdraw access rights.

6. Eradicate the incident

In order to eradicate the security incident, the following steps are taken, including documentation of all actions taken:

- Discovered vulnerabilities should be fixed
- Identification and removal of potential malware
- Scan the affected systems to make sure that all potential illicit content has been removed
- Restore the systems back to normal
- Make notes on where improvements should be implemented

7. Recover from the incident

The following steps need to be taken to recover from the incident:

- Affected systems are to be returned to an operationally ready state
- Testing the fixes made in accordance with the eradicate face - to make sure the systems are now functioning as they should
- Implement monitoring if needed

Post-incident Actions

8. Follow-up Report

Gathering all documentation from the incident and see if any additional information needs to be written down in the incident response report.
The intention of the report is to describe the process of how the incident was handled as well as a summary of what has happened.

9. Lessons Learnt - Meeting

Lessons Learnt meeting should be held. The meeting should include a briefing on what happened, and the performance of staff and management in terms of how well they performed in dealing with this incident and if there were any deviations in following the procedures, or if there were any steps in the procedures that needed to be improved as well as what could be done differently next time a similar incident occurs.
Further discussions on what could be done to prevent similar incidents in the future as well as what precursors or indicators should be looked out for to be able to detect similar incidents before they could become an incident. In this case high usage of CPU power and multiple instances of /bin/scp.

During this meeting, it is also recommended to review the implemented controls as well as the information security incident management policy to see if further improvements are necessary. For example, adjust the access control to only allow access to data during office hours. It is also necessary to review how effective the processes, procedures etc were in dealing with the incident and if necessary improvements need to be done to the information security incident management plan.

Proposed improvement actions:

- Improved access control
- Keep information for six months instead of three.
- Employee screening
- No access outside of office hours
- The incident response team will perform exercises to minimize risks and incidents from happening again.
- Employees need to review the security policy continuously.
- Management need to review and update policies and provide these to the employees
- Systems and files will be monitored

References

NIST-SP 800-61r2 Incident Handling Guide
ISO/IEC 27035-1 Information security incident management