Case 4

Incident Response

CYBER Security

2020-04-22

**Submitted by:**

Group 15

Ranjana, Efstathios, Justas

# General Information:

|  |  |
| --- | --- |
| **Document Owner** | Ranjana, Efstathios, Justas |
| **Date** | 2020-04-22 |

# Incident

|  |  |
| --- | --- |
| **Date and time of the incident:** | 04/18/2020, 03:43, Local Time. |
| **Who was involved?** | Casino 10-4 manager received a notification that a possible incident has been identified and registered. |
| **Description** | The incident was generated from the server of the financial user, who has authorised access to all the other authorized users. The file transfers were initiated from several authorized users. This directs to Dos/DDoS attacks. Since the incident occurred at non working hours, it seems to be a deliberate Dos/DDoS attack. |

# Detection And Analysis

|  |  |
| --- | --- |
| **Are there any other areas that have been compromised by the incident?** | * Authorized users. * FTP server. * Server where the files were sent. * All the servers connected directly/indirectly to FTP server or the server where the files were sent. |
| **What is the scope of the impact?** | The scope of the impact is throughout the organization as the attack occurred from the financial user’s account who in turn has access to all the authorized users. |
| **What is the business impact?** | The business was down for 5 days causing delay with file transfers. |
| **Have the source(s) of the incident been located? If so, where, when, and what are they?** | File transfers were initiated from an authorised account. The employee has access to the records of all registered accounts. File transfers of several instances were started during non-working hours. |

# Containment

|  |  |
| --- | --- |
| **Short-term containment** | 1. The FTP server and main server where files were sent were removed from the network and isolated. 2. The authorized users were requested to change their credentials. 3. The affected server's snapshots were taken for further analysis. 4. The server where files were sent was reverted back to the last working day snapshot inorder to remove any suspicious file. 5. The FTP servers were kept down until root cause analysis was performed. 6. Antivirus was executed by pushing the code to all the servers/laptops through the central system in order to scan for suspicious activities. |
| **System Back-up** | 1. The system backup was taken in step 3 of short-term cointment by taking a snapshot of the affected servers. 2. The backup was stored in multiple locations including the data center and extra hard copy. 3. The snapshot was then used to create another server which was provided to the forensic team in order to perform forensic analysis. Along with the server, the copy of the snapshot was sent as well. 4. The snapshots ssh values were compared inorder to confirm the integrity of the snapshot. |
| **Long-term containment** | 1. The FTP server and the server where the files were sent are kept in different subnets. The FTP server is separated and kept in DMZ. 2. The access to send files in FTP are now different compared to the authorized users. Only local FTP users for the server are now allowed to send file which are different from authorized users. |

# 

# Eradication & Recovery

|  |  |
| --- | --- |
| **Restoring the server from old snapshot** | The FTP and server where files were sent were restored from old backup to the last working hour before the incident occured. |
| **Applying patches nd changing users** | The patches were updated in all the servers. The patch was pushed from the central server. |
| **Forced change of credentials** | All the authorized users were asked to change the credentials within 72 hours. |
| **Handling artifacts** | The malwares and other artifacts sent via file transfers were removed when restoring the servers from old snapshots. Furthermore, in order to confirm the removal of malware, an antivirus scan was pushed to all the servers in the company. The security patches were pushed to be applied in all the servers and laptops. |

# Post-Incident Actions

|  |  |
| --- | --- |
| **Further investigation if needed**. | * The snapshot and logs of the affected server are sent in forensic analysis for further investigation. |
| **Documentation of the incident that can help in identifying and analyzing future incidents.** | * The incident is reported in Jira service desk and documented in Confluence. An email has been sent to all the clients in order to be aware of the situation. * An alert has been created to send an email and SMS to respective authorized users when the file transfer occurs during non working hours. |
| **Harden and patch the system with regard to future attacks.** | * The system patches were pushed to all the servers within the company. * Compulsory patch is implemented where all the computers are patched once every month. * The password change policy has been implemented once every 3 months * The password strength is increased from length of 7 to 10. |
| **Tools that are going to be used to test, monitor and verify that the affected systems are now resilient to future attacks.** | * Monitoring tool (Nagios) is set up to check activities and logs in the FTP server. * The file transfer is monitored to check how many transfers occur every minute, from which user and from which server. * The log of file transfers are copied every hour from server to log server for future audits. |
| **Monitoring of the affected systems in order to ensure their reliability.** | * Nagios monitoring is set up in all the servers for user login and logout for 3 months and continuation is decided after 3 months of analysis. * The monitoring of FTP and file transfer is permanent and will be monitored through the file transfer process. |
| **Organization of “lessons learnt” meeting with the interested parties and preparation of the incident response report in order to be presented.** | Awareness meeting was conducted in the company and scheduled to be conducted once every 3 months. Following are the topics to be discussed during the meeting:   * A proper incident management process and policy implementation * Importance of changing user credentials within a time frame. * Update on patch application and automation of patch application. * Process creation on receiving monitoring alerts for file transfer during non working hours. |
| **Incident Report** | * The incident report was created and reviewed/approved by the incident management committee during the awareness meeting. * A copy of the incident report is sent to all the clients. Employees received the employee report through an email and the incident report is presented in the Confluence page for further reading. |
| **Further analysis** | * The company is waiting for the forensic department to complete their analysis. Further actions will be created based on the report. |

Questions and Answers Group 10

Well prepared document, but we wanted to point out that the report in general is written in a form of “what could be done” rather than “what you would actually do”. It would have been nice to see what definite steps you would take as a security team otherwise a well written report.

1. Why did you not recommend an actual back-up of the whole system in order to secure its integrity with regard to future attacks?
2. Why did you not choose to present an incident report during the “lessons learnt” meeting in order to inform the interested parties?
3. One of the long term containments included ‘Implement security education against social engineering’, we could not come up with the relation to the incident and this resolution. Can you please elaborate on this.

Regards,

Group 15

Hi ,

Please find out answers:

**Since the attack happened on the database backend server, there is no mention of the FTP server in the document provided. How was this assumption taken up?**

Since the issue occured within file transfer , and the only way to transfer large files is through FTP process so our assumption was that the attack started from other servers but reached FTP server.

**How can it be concluded as a deliberate DoS/DDoS attack, since the impact in the scenario just refers to CPU outage and no network outage?**

The file transfer attack leads to data being exposed so it was our assumption that since data is exposed , there definitely is denial of service until the issue is resolved and the extent of attack is known. So we came with the assumption that it is a DoS attack.

**How is the demarcation between local FTP users and authorized users made?**

Our assumption is the authorized users are active directory users whose credentials are managed through the central system. The local FTP users are the user credentials created only for the sole purpose of file transfer. Differentiating these two won't lead to attacks being generated via a central authorized system as credentials varies from user to user and information is available only to one specific server .

**You mentioned the incident very reasonably, but why did you not mention the responders of an incident?**

According to the instructions, we were the responders of the incident :)

**How do you suggest the business was down for 5 days, given that there is a secondary data center available that works as a backup for the primary data center where the incident happened?**

Even though a secondary data center is present, it is an exact copy of primary. So all the issues in primary are replicated to secondary as well. Secondary also should not be up until all the things are fixed in secondary as well. So it must be down for specific days until a short term fix is implemented. Also it is not reasonable to keep business running during crisis hours nor it creates a good image.

**Have there been any considerations on if this was an internal or external attack?**

Yes but we could not make any assumptions as we decided to wait for the forensics analysis in order to decide about this matter.

Regards,

Group 15