Paper - Incident Response Playbook

Rama Krishna Sumanth Gummadapu

Foundations of Information Assurance

November 27, 2019

Abstract:

The following are the incident response playbooks created in case of incident. We assume that there is a Incident response database created which keeps track of the database. The SIEM is working fine and all systems are kept up to date with all the updates. No known vulnerabilities are kept un-patched. The system is not compromised is being assumed. We also pre-assume that the spam filter we use can be updated with custom input and configurable and honeypots are present on the network.

Phishing email with malware in attachment

Introduction:

This is a playbook to follow in case of incident of detection of a malware attachment received to user and detected before or after the incident has occurred. Follow step by step for resolution and improvise if you need to.

Identification:

1. Monitoring of all emails using Email Gateway with Anti spam protection is present on the network and Anti malware Endpoint protection present on all devices.
2. The Security Information and Event Management(SIEM) gathers all the logs on the system which triggers an alert using keyword detection method.
3. The user reports email as phishing email.

Notification:

1. Update the Security Analyst team about the incident with information about the incident.

2. Add the Incident to the Incident database.
3. Update user if the number of similar incidents are occurring frequently.
4. If the mail originated from the trusted company update the company and request clarification.
5. Update to HR and Technology and Operations Team Lead if this is happening again with the user after first contamination was done.
6. If more than a threshold of users receives phishing email the issue should be escalated to Technology and Operations Team Lead, Incident Response Manager, CISO and CIO.
7. If it is a mass attack is carried out against the company notify the senior management.

Analysis:

1. Get the PTR record of the host.
2. Check the email recipients if the incident reported by user and start the process from notification.
3. Check for the patterns of the email and add to spam filter.
4. Check for the type of attachment sent.
5. If reported by user check for malware and add the new malware strain to the database.
6. Check for the origin of the malware and the type of it.
7. Previously did the host from which the email is received has passed through the filters without raising any trigger. If passed undetected check the previous

email/emails for malware. Repeat the process from Notification for the undetected email.

8. If this is a false trigger from the system update the same in incident database.

Containment/Eradication:

1. Email is striped of it's malware attachments if not detected by user and the email is removed from SMTP server.
2. If user updates the issue check for the email recipients and start process from the notification.
3. Update the incident status in the incident database.
4. Add the origin of the email to the list of blacklisted addresses to the perimeter firewall on the network.
5. If a user gets targeted frequently then contact user and ask the user to change the email address of his account.
6. Monitor the old email address of the user for more phishing emails.
7. Advance scan user system for malware.
8. Scan affected users system for malware or rootkit. If rootkit found start incident response process for rootkit.

Recovery:

1. For mass Phishing email add the origin to the blacklist.
2. For individual user make sure the user gets trained about phishing email.
3. Advance System Scan for malware for frequent phishing targeted user.

4. For false trigger update the system.

Phishing email with credential harvesting web link

Introduction:

The following playbook is used if a incident occurs when user receives email to credential harvester web link.

Identification:

1. Monitoring of all emails using Email Gateway with Anti spam protection is present on the network.
2. The Security Information and Event Management gathers all the logs on the system which triggers an alert using keyword detection method.
3. The user reports email as phishing email.
4. If the Perimeter firewall detects a unusual activity for multiple users originated from a link sent from single email address.

Notification:

1. Update the Security Analyst team about the incident with information about the incident.
2. Add the Incident to the Incident database.
3. Update user if the number of similar incidents are occurring frequently for same user.
4. If the mail originated from the trusted company update the company and request clarification.

5. Update to HR and Technology and Operations Team Lead if this is happening again with the user after first contamination was done.
6. If more than a threshold of users receives phishing email the issue should be escalated to Technology and Operations Team Lead, Incident Response Manager, CISO and CIO.
7. If it is a mass attack is carried out against the company notify the senior management.

Analysis:

1. Get PTR record of the host and
2. Check network logs for the outward data towards the host of the link if phishing detected by the user and start the process from notification.
3. What data is being harvested.
4. What is the method being used to harvest the data.
5. Is any malware is being installed on the user system.
6. Previously did the host from which the email is received has passed through the filters without raising any trigger. If so check immediately previous email/emails and scan for harvesting links and check network logs if any credentials are harvested for the previous undetected email. Repeat the process from Notification for the undetected email.
7. If this is a false trigger update the system and

Containment/Eradication:

1. Strip the link of the phishing email if not detected by user.
2. If user updates the issue check for the email recipients and start process from the notification.
3. Add host of the link to blacklist on the Firewall.
4. Update incident in the incident database.
5. update the network admins to block traffic from the host of phishing site on entire network.
6. Add the origin of the email to the list of blacklisted addresses to the perimeter firewall on the network.
7. Scan targeted systems for malware installed. If credentials were compromised update users to update passwords and update system admins to update the affected users account password expiration.
8. Run system Integrity test and confirm for no rootkit. If rootkit found start Incident response procedure for rootkit.

Recovery:

1. Update the method to Anti-malware Endpoint Protection and incident database used if systems are compromised.
2. Send phishing awareness to user who are affected by the credential extractor.
3. Send users update to update the password.

Lost Laptop incident from an employee

Introduction:

The employee lost laptop on which the company sensitive data is stored. The laptop is an asset of the company and needs to be protected. Follow the procedures to recover the asset and avoid any major fallout. Laptop is equipped with tracking and VPN is being assumed. All the laptop disks are fully encrypted. Update every step in Incident Database. Incident data recovery server holds employee laptop data for inspection in case of recovery.

Identification:

1. User reports the loss of device from his possession.
2. User present at office location and laptop is bouncing on the internet at different locations and user logged into the system on office location. CCTV footage shows employee not using laptop but still there is a activity on the laptop.
3. The SIEM reports a possible malware on employee system and the system is not on the VPN or not on on-ground location of the office.

Notification:

1. Notify the incident response manager and superior of the employee about the incident.
2. Add the Incident to the Incident Database.
3. Update and get confirmation from the employee if the employee didn't report the loss of device.
4. Notify CISO, CIO and HR if the asset is in custody of government.

Analysis:

1. Try to remote access the system.
2. If remote access worked and the asset is inside the office location or secure location(Government Custody) get the location and update in Incident database and inform the CISO to secure the employee laptop.
3. Go through the SIEM to check for the software update and version of the employee laptop.
4. Add the system MAC details to watch list on the firewall.
5. Analyse the system activity from the moment the employee reports loss of device and keep a tab on suspicious activity from the system.

Containment/Eradication:

1. If the system is reachable and inside the office location. Lock the system down.
2. If the system is reachable and in government custody try to get the important data updated to the incident data recovery server.
3. If the data gets updated in the incident data recover server and complete wipe the employee laptop or rewrite the entire disk with random data.
4. If the user laptop is not found report local law enforcement about the theft/loss.
5. Add the laptop MAC address to watch list on network Firewall and update network admins to route all the traffic from the employee lost laptop to honeypots.
6. Any activity of lost laptop online try coping the data to incident data recovery server and wipe the laptop or writing the full disk with random data.
7. If data recovery is not possible wipe the disk.

8. Update the Intrusion Prevention sensors with the MAC address of the lost employee laptop.

Recovery:

1. Inform employee, HR and CISO about the status of the incident.
2. Monitor the network for the MAC address of the laptop lost and try to wipe the disk.
3. Keep track of the incident for future references.

System alert for USB inserted on employee machine

Introduction:

This is a scenario in which the user has plugged in the USB inserted into the employee machine of the laptop. This scenario is to identify and neutralise any attack if present.

Identification:

1. Alert from the SIEM based on storage peripheral attachment detection.
2. Anti Malware endpoint protection.
3. Another dutiful employee reporting about the employee inserting USB in the system.

Notification:

1. Notify employee.
2. If not responded and repeated then notify Technology and Operations Team Lead and HR after analysis.

3. Update incident in the Incident database.

Analysis:

1. What type of the device is inserted.
2. what is the capability of the device.
3. Can the device store data on it.

Containment/Eradication:

1. Send alert to the user about the incident as on screen popup.
2. If the device found to be storage device block the device and lock the system and ask employee to visit security analyst for unlocking.
3. If false trigger check and sort that out.

Recovery:

1. If there is a false trigger then add the peripheral id to the trusted id.
2. Update Incident database as false trigger.

Ransom note received in email with threat of DDOS attack on company

Introduction:

Note about threat of DDOS attack on the company. A payment in bitcoins is demanded to stop the attack from starting.

Identification:

1. Note from the attacker about DDOS on the company network.

Notification:

1. Notify the following people:
    - Incident Response Manager
    - Security Analyst
    - CISO
    - CIO/CTO
    - Technology and Operations Team Lead
    - Senior Management
    - Business Line Head of Departments
    - Legal / General Counsel
    - Public Relations Officer

Analysis:

1. Get PTR records of the host from which the email is received.
2. Update the incident in incident response database.
3. Check for suspicious activity on the network.
4. Check SIEM for any security events.
5. Check System for health and get the stats.

Containment/Eradication:

1. If the threat is from a account where previous attack occurred or a legit source.
2. Update network admins to take down network if there is a sudden spike in network activity.

3. Prepare backup systems in case of attack.
4. Inform system, Database admins to take backup and disconnect the backup systems from network.
5. Contact ISP for additional bandwidth.
6. Update the whitelist of IP's crucial for business function and allow only them in case of DDOS attack starts.

Recovery:

1. Update Law enforcement about the attack.
2. Release the restrictions and allow normal usage.
3. Check the attack type used in case of DDOS attack occurred.

References

F5, "The F5 DDOS Playbook", https://f5.com/Portals/1/Premium/Architectures/RA-DDoS-Playbook-Recommended-Practices.pdf (accessed November 27, 2019).

Incident Response consortium, "DDOS—Incident Response Playbook", https://www.incidentresponse.com

(accessed November 27, 2019).

Brian Prince, "Creating DDOS Playbook", https://www.darkreading.com/creating-a-ddos-response-playbook/d/d-id/1316008 (accessed November 27, 2019).

Demistro, "Phishing Incident Response Playbook", https://www.demisto.com/phishing-incident-response-playbook/ (accessed November 27, 2019).

Incident Response consortium, "Phishing—Incident Response Playbook", https://www.incidentresponse.co

(accessed November 27, 2019).

Paul Rose, ”Whitepaper: Best Practices for Developing a Cyber Security Playbook”, https://www.cnsgroup hub/news/news-article/2017/05/02/whitepaper-best-practices-for-developing-a-cyber-security-playbook (accessed November 27, 2019).

Josh Mayfield, ”LOST OR STOLEN DEVICES: WHAT TO DO IN 4 STEPS”, https://blogs.absolute.com/ stolen-devices-4-steps/ (accessed November 27, 2019).

Rapid7, ”How to Securely Handle a Lost or Stolen Device: A Practical Workflow”, https://blog.rapid7.com/ to-securely-handle-a-lost-or-stolen-device-a-practical-workflow/ (accessed November 27, 2019).