Integrated Cyber Threat Intelligence

Operational Incident Response Plan

Name: Seerat E Marryum

Bytewise Limited Cyber Security Track

Submitted to: Sir Tayyab

Submission date: 4 September, 24

Contents

1. Introduction

This operational incident response plan outlines containment, remediation, and recovery strategies for the multi-stage attack on TechGuard Inc. by the Specter APT group. The plan addresses each stage of the malware attack—SpecterDrop, ShadowFrost, and FrostLock ransomware—focusing on real-time alert prioritization and coordination, as well as internal and external communication strategies.

2. Containment Strategies

Stage 1: SpecterDrop (Initial Access)

- **Priority Alerts:**
    - Unusual login attempts or successful logins from suspicious IP addresses.
    - Suspicious file execution from unexpected locations (e.g., downloads or email attachments).
- **Containment Actions:**
    - **Immediate Quarantine:** Isolate affected endpoints from the network to prevent further communication.
    - **Account Lockdown:** Disable compromised accounts and require multi-factor authentication (MFA) for all access points.
    - **Email Filtering:** Block similar phishing emails across the organization and flag incoming suspicious emails for review.

Stage 2: ShadowFrost (Lateral Movement and Data Exfiltration)

- **Priority Alerts:**

    - Unexpected internal traffic between endpoints, especially from non-admin accounts.
    - Unusual use of administrative tools like PowerShell, PsExec, or Remote Desktop Protocol (RDP).
- **Containment Actions:**
    - **Network Segmentation:** Segment the network to limit malware movement and isolate affected subnets.
    - **Privilege Revocation:** Revoke administrative privileges for non-essential users to minimize lateral movement.
    - **Encryption Monitoring:** Monitor encrypted outbound traffic to identify potential data exfiltration activities.

Stage 3: FrostLock Ransomware (File Encryption)

- **Priority Alerts:**
    - Sudden file encryption activities and mass file modifications across multiple systems.
    - Access attempts to backup storage and server files.
- **Containment Actions:**
    - **Immediate Disconnection:** Disconnect infected systems from the network and power down affected servers to prevent further encryption.
    - **Backup Isolation:** Secure and isolate backup systems to ensure they remain unaffected by the ransomware.
    - **Critical Systems Priority:** Focus on protecting critical systems that support business operations and revenue streams.

3. Remediation Steps

Stage 1: SpecterDrop

- **System Cleanup:** Deploy advanced threat detection tools to scan and remove SpecterDrop from infected endpoints. Focus on cleaning up persistence mechanisms such as registry keys, scheduled tasks, and malicious executables.
- **Credential Reset:** Require a password reset for affected accounts and audit all user credentials for signs of compromise.
- **Security Awareness Training:** Provide employees with immediate training on identifying phishing attacks and responding to suspicious emails.

Stage 2: ShadowFrost

- **Privilege Escalation Mitigation:** Patch vulnerabilities used by ShadowFrost to gain elevated privileges. Review access controls and disable unnecessary administrative tools.
- **Network Traffic Analysis:** Conduct a detailed analysis of network traffic logs to determine the extent of lateral movement and identify compromised systems.
- **Data Loss Prevention:** Implement additional data loss prevention (DLP) measures to monitor sensitive data and prevent further exfiltration attempts.

Stage 3: FrostLock Ransomware

- **File Restoration:** Utilize available decryption tools if possible. If decryption is not feasible, recover encrypted files from clean backups.
- **System Rebuild:** For systems where recovery is not possible, rebuild affected machines with fresh installations, applying hardened security configurations.

- **Future Prevention:** Implement advanced ransomware protection measures, such as real-time behavioral detection and automated response protocols.

4. Recovery Procedures

Stage 1: SpecterDrop

- **Endpoint Restoration:** Reinstall operating systems on infected endpoints if necessary, ensuring that all malware remnants are removed.
- **Security Enhancements:** Strengthen security measures, such as enhancing email filtering rules and implementing endpoint detection and response (EDR) tools to catch future phishing attempts.

Stage 2: ShadowFrost

- **System Restoration:** Restore compromised systems from clean backups, verifying that no malicious code persists in the restored environments.
- **Network Reconfiguration:** Rebuild network segments to limit potential attack vectors and strengthen internal firewall rules to prevent unauthorized access between segments.

Stage 3: FrostLock Ransomware

- **Backup Recovery:** Restore critical data and systems from backups. Implement regular backup testing to ensure that backups are functional and can be restored quickly.
- **Business Continuity Plan Activation:** Activate the business continuity plan to ensure minimal disruption to operations during the recovery process, prioritizing essential services.

5. Coordination Strategies and Alert Prioritization

1. Centralized Incident Response Team (IRT):

- Form a centralized incident response team to coordinate containment, remediation, and recovery efforts. This team will manage real-time alert prioritization, assign roles, and oversee the execution of the response plan.

2. Prioritization Framework:

- **High Priority Alerts:** Focus on alerts related to initial access, lateral movement, and ransomware deployment. Ensure that these are addressed immediately to limit the spread of malware and data exfiltration.
- **Medium Priority Alerts:** Monitor alerts related to suspicious internal activities and abnormal use of administrative tools. These should be addressed promptly but after containing high-priority threats.
- **Low Priority Alerts:** Routine security alerts that do not indicate immediate threats can be reviewed during the post-incident analysis phase.

3. Communication Protocols:

- Establish clear communication channels between the IRT, IT staff, management, and external stakeholders. Implement regular status updates and situation reports to ensure everyone is informed and aligned.
- Use secure communication tools to coordinate response efforts and avoid compromising sensitive information during the incident.

6. Communication Plan

Internal Communication:

- **Incident Updates:** Regularly update the executive team, department heads, and affected staff on the status of the attack, containment efforts, and recovery progress.
- **Incident Reports:** Prepare detailed incident reports for internal review, highlighting the steps taken and lessons learned.

External Communication:

- **Client Notifications:** Inform clients of the breach in compliance with relevant data protection regulations. Provide transparent information on the scope of the breach, the data affected, and the steps taken to mitigate the impact.
- **Regulatory Notifications:** Report the incident to relevant regulatory bodies, following the required timelines and protocols. Ensure that all documentation is thorough and aligns with legal requirements.

7. Conclusion

By implementing this operational incident response plan, TechGuard Inc. can effectively manage the Specter APT attack, mitigate its impact, and recover critical operations. Prioritizing alerts, ensuring coordinated response efforts, and maintaining transparent communication with both internal and external stakeholders are key to minimizing damage and building resilience against future attacks.