CYBERSECURITY INCIDENT RESPONSE PLAYBOOK

Version: 1.0

Date: 2024

This playbook serves as a guide for cybersecurity teams to address common security alerts effectively. The aim is to minimise the impact of security incidents through structured response and recovery steps.

BY IZZMIER IZZUDDIN

TABLE OF CONTENTS

INCIDENT RESPONSE ELEMENTS

NIST INCIDENT RESPONSE LIFECYCLE:

1. **Preparation**: Establish roles, responsibilities and resources.
2. **Detection and Analysis**: Investigate alerts and validate incidents.
3. **Containment, Eradication and Recovery**: Limit damage, eliminate threats and restore operations.
4. **Post-Incident Activity**: Review, learn and improve.

INCIDENT RESPONSE

1. CREDENTIAL STUFFING ATTACK

Description: Automated login attempts using stolen credentials detected on your application.

Detection and Analysis:

- Identify unusual login attempts through SIEM alerts or application logs.
- Correlate with threat intelligence for known leaked credentials.
- Monitor login success rates from suspicious IPs or geolocations.

Containment:

- Block suspicious IPs using WAF or firewall rules.
- Enable CAPTCHA or other anti-bot mechanisms for login attempts.
- Enforce temporary account lockouts after a defined number of failed login attempts.

Eradication:

- Identify and neutralise botnet activity.
- Patch vulnerable authentication systems.
- Notify affected users to reset their passwords.

Recovery:

- Enhance MFA enforcement.
- Deploy account anomaly detection mechanisms.
- Conduct a post-event review to fine-tune defenses.

SCENARIO EXAMPLE

Incident Simulation: Credential Stuffing Attack

Date: November 21, 2024
Time: 10:00 AM
Environment: Corporate web application with user authentication portal.

Detection

Alert Details:

- **Alert ID**: SIEM-2024-11-001
- **Source**: SIEM (Splunk)
- **Description**: Multiple failed login attempts detected for user accounts from unusual IP ranges.
- **Severity**: High

Logs:

Timestamp: 2024-11-21T09:55:32

Event: Failed Login

UserID: izzmier@manchesterunited.com

IP: 192.168.50.23

Reason: Invalid password

Timestamp: 2024-11-21T09:56:12

Event: Failed Login

UserID: iffah@manchesterunited.com

IP: 202.56.120.14

Reason: Invalid password

Timestamp: 2024-11-21T09:57:01

Event: Successful Login

UserID: rosnani@manchesterunited.com

IP: 185.23.45.67

Key Indicators:

1. A surge of failed login attempts for multiple accounts within 5 minutes.

2. Logins from IPs associated with geolocations inconsistent with user profiles (different countries).
3. One successful login for a compromised account (rosnani@manchesterunited.com).

Analysis

Key Findings:

1. **Threat Vector**:
    - The attack leverages stolen credentials from a public breach to perform automated login attempts.
    - Tools like **SentryMBA** or similar credential stuffing tools are suspected.
2. **Accounts Impacted**:
    - **Failed Attempts**: izzmier@manchesterunited.com, iffah@manchesterunited.com.
    - **Successful Compromise**: rosnani@manchesterunited.com.
3. **Origin of Attack**:
    - Analysis of IP addresses:
        - 192.168.50.23: Internal corporate range (user might be testing their credentials).
        - 202.56.120.14: Thailand (Anomalous).
        - 185.23.45.67: Associated with a known malicious proxy service (identified via VirusTotal and threat intelligence platforms).
4. **Behavioral Analysis**:
    - The successful login (rosnani@manchesterunited.com) was immediately followed by API calls to export sensitive financial data.
    - Correlation with logs shows unauthorised file download attempts.

Containment

Actions Taken:

1. **User Account Suspension**:
    - rosnani@manchesterunited.com account disabled.
2. **IP Blocking**:
    - Blocked IP ranges associated with malicious activities at the firewall and WAF.
3. **Session Termination**:
    - Active sessions for all impacted accounts forcibly terminated.
4. **Real-time Monitoring**:
    - Enabled real-time alerts for suspicious login attempts.

Eradication

1. **Credentials Rotated**:
    - Forced password resets for rosnani@manchesterunited.com and all accounts showing failed login attempts.
2. **Blacklisting**:
    - Added identified malicious IPs to the threat intelligence blocklist.
3. **Tool Analysis**:
    - Investigated system logs for evidence of credential stuffing tools; no malware found.

Recovery

1. **Data Verification**:
    - Cross-referenced file access logs to ensure no data exfiltration occurred.
2. **Enhanced MFA Deployment**:
    - Enforced MFA for all user accounts, reducing risks of further credential-based attacks.
3. **SIEM Updates**:
    - Added new rules to flag high volumes of failed logins from unusual IPs.

Post-Incident Review

Root Cause:

- Stolen credentials from a publicly available breach used in an automated attack.

Recommendations:

1. Implement a CAPTCHA mechanism after multiple failed login attempts.
2. Educate users on the risks of reusing passwords across platforms.
3. Integrate threat intelligence feeds for proactive alerting of suspicious IPs.

Visualisation of Data

Login Attempts Heatmap:

- Red zones indicate high activity from IPs 202.56.120.14 and 185.23.45.67.
- Normal user activities showed no prior interaction from these regions.

Timeline:

Time	Event	Action Taken
09:55 AM	Failed logins detected	Alert triggered in SIEM
09:57 AM	Successful login for Alex Brown	Account disabled
10:05 AM	API data export attempt blocked	IP blocked, session killed

2. LATERAL MOVEMENT DETECTED

Description: Unauthorised internal reconnaissance activities detected in the network.

Detection and Analysis:

- Analyse alerts from EDR or network traffic analysis tools for lateral movement patterns.
- Use logs to identify unusual account access to multiple systems.

Containment:

- Isolate affected systems and segments.
- Disable compromised accounts.

Eradication:

- Remove unauthorised tools or malware enabling movement (Mimikatz, PsExec).
- Conduct a thorough review of user privileges and roles.

Recovery:

- Restore affected systems from clean backups.
- Strengthen segmentation policies.
- Deploy additional lateral movement detection mechanisms.

SCENARIO EXAMPLE

Simulated Scenario: Lateral Movement Detected

Date: November 21, 2024
Time: 3:30 PM
Environment: Corporate Active Directory (AD) network with shared drives and email servers.

Detection

Alert Details:

- **Alert ID**: SIEM-2024-11-002
- **Source**: EDR and SIEM
- **Description**: Lateral movement detected between systems Finance-PC01 and HR-Server01.
- **Severity**: Critical

Logs:

Timestamp: 2024-11-21T15:15:42

Source: Finance-PC01

Event: Suspicious SMB Traffic

Destination: HR-Server01

Description: Unusual process (`wmiexec`) initiated communication.

Timestamp: 2024-11-21T15:18:27

Source: HR-Server01

Event: Credential Dumping Detected

Description: Process `lsass.exe` accessed by `procdump.exe`.

Timestamp: 2024-11-21T15:22:50

Source: HR-Server01

Event: Privilege Escalation Attempt

User: finance-admin

Description: Added to local administrators group.

Analysis

Key Findings:

1. **Attack Method**:

- Adversary gained initial access to Finance-PC01 and used tools (wmiexec) for lateral movement to HR-Server01.
- Indicators suggest the use of known techniques like **Pass-the-Hash** or **Credential Dumping** to compromise HR-Server01.

2. **Compromised Accounts**:
   - finance-admin: Elevated privileges on HR-Server01.
   - Hashes from Finance-PC01 and HR-Server01 were potentially dumped.
3. **Malicious Tools Used**:
   - wmiexec: Detected in SMB logs for executing commands remotely.
   - procdump.exe: Used to access lsass.exe for credential dumping.
4. **Threat Actor's Goal**:
   - Likely exfiltration or compromise of sensitive HR data from HR-Server01.

Containment

Actions Taken:

1. **Network Isolation**:
   - Isolated Finance-PC01 and HR-Server01 from the corporate network.
2. **Account Lockdown**:
   - Disabled the finance-admin account to prevent further misuse.
3. **Real-Time Blocking**:
   - Updated firewall rules to block suspicious SMB traffic across the network.
4. **Session Termination**:
   - Forced logouts and session terminations for finance-admin.

Eradication

1. **Tool Removal**:
   - Removed wmiexec and procdump.exe from compromised systems.

- Performed a full scan using EDR to identify and remove additional artifacts.

2. **Patch and Updates**:
    - Applied patches for any vulnerabilities exploited in Finance-PC01 and HR-Server01.
    - Hardened configurations to disable remote SMB execution for non-administrative users.
3. **Access Review**:
    - Revoked all elevated privileges granted during the attack.
    - Conducted a full audit of Active Directory accounts and permissions.

Recovery

1. **System Restoration**:
    - Restored Finance-PC01 and HR-Server01 from the last known good backups.
2. **Credential Reset**:
    - Forced password resets for all users whose credentials were potentially compromised.
3. **SIEM Fine-Tuning**:
    - Updated detection rules to better monitor:
        - Lateral movement attempts.
        - Unusual privilege escalation activities.

Post-Incident Review

Root Cause:

- Initial compromise of Finance-PC01 occurred through phishing or exploitation of an unpatched vulnerability.

Recommendations:

1. **Enhance Monitoring**:

- Deploy honeypots to detect lateral movement.
- Improve logging and alerting for SMB and RDP activity.

2. **Zero Trust Architecture**:
    - Implement stricter segmentation and access policies across departments.
3. **Awareness Training**:
    - Conduct targeted phishing training for Finance team employees.

Visualisation

Timeline of Attack:

Time	**Event**	**Action Taken**
15:15 PM	SMB traffic detected (Finance-PC01)	Alert triggered in SIEM
15:18 PM	Credential dumping on HR-Server01	Systems isolated
15:22 PM	Privilege escalation on HR-Server	Account disabled
15:30 PM	Forensic analysis initiated	Tools removed, logs reviewed

Network Heatmap:

- Red lines indicate suspicious traffic between Finance-PC01 and HR-Server01.

3. PRIVILEGE ESCALATION ATTEMPT

Description: An attacker tries to elevate their privileges on a critical system.

Detection and Analysis:

- Review SIEM logs for privilege escalation indicators ("sudo" commands, new account creations).
- Cross-check logs with endpoint alerts on suspicious registry changes or policy modifications.

Containment:

- Revoke elevated privileges and disable compromised accounts.
- Block associated malicious IP addresses.

Eradication:

- Patch vulnerabilities exploited for escalation.
- Audit user roles and access permissions to identify gaps.

Recovery:

- Reinforce least-privilege principles.
- Enable automated alerts for privilege changes.
- Educate users and administrators about privilege abuse.

SCENARIO EXAMPLE

Simulated Scenario: Privilege Escalation Attempt

Date: November 21, 2024
Time: 10:00 AM
Environment: Corporate IT environment with Active Directory, application servers and endpoint security.

Detection

Alert Details:

- **Alert ID**: SIEM-2024-11-003
- **Source**: Endpoint Detection and Response (EDR)
- **Description**: Privilege escalation attempt detected on AppServer01.
- **Severity**: High

Logs:

Timestamp: 2024-11-21T09:55:12

Source: AppServer01

Event: Process Execution

User: dev-user01

Description: Execution of `exploit.exe` (SHA256: abc123...) flagged as suspicious.

Timestamp: 2024-11-21T09:57:45

Source: AppServer01

Event: Privilege Modification

User: dev-user01

Description: Added to Local Administrators group.

Timestamp: 2024-11-21T09:58:30

Source: AppServer01

Event: Registry Change

User: dev-user01

Description: Registry key modified:
`HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System`.

Timestamp: 2024-11-21T09:59:50

Source: AppServer01

Event: Persistence Mechanism Detected

User: dev-user01

Description: Startup item added to
`HKLM\Software\Microsoft\Windows\CurrentVersion\Run`.

Analysis

Key Findings:

1. **Attack Method**:
    - Privilege escalation attempt used a known exploit (exploit.exe) targeting a misconfigured service or unpatched vulnerability on AppServer01.
    - Logs show dev-user01 gained local administrator privileges.
    - Persistence established via registry modifications.
2. **Compromised Account**:
    - dev-user01: Regular user account used for daily operations, elevated privileges to access sensitive systems.
3. **Tools and Indicators**:
    - **Exploit Executable**: exploit.exe flagged by EDR as malicious (hash matched with public databases).
    - Registry keys and startup folder modifications indicate persistence setup.
4. **Potential Impact**:
    - Access to sensitive application and database resources.
    - Ability to move laterally across the network with elevated privileges.

Containment

Actions Taken:

1. **Account Suspension**:
    - Disabled dev-user01 account immediately.

2. **Network Isolation**:
    - Isolated AppServer01 from the network to prevent further exploitation.
3. **Session Termination**:
    - Forced termination of all active sessions for dev-user01.

Eradication

1. **Malware Removal**:
    - Deleted exploit.exe from AppServer01.
    - Scanned system using antivirus and EDR for other artifacts.
2. **Patch Management**:
    - Applied missing patches to address the exploited vulnerability.
3. **Registry Cleanup**:
    - Reverted unauthorised registry changes:
        - Removed persistence mechanisms.
        - Reset modified policies.
4. **Privilege Review**:
    - Verified and reset local administrators' group membership to exclude unauthorised accounts.

Recovery

1. **System Restoration**:
    - Restored AppServer01 from a clean backup image.
2. **Credential Reset**:
    - Reset credentials for dev-user01 and other accounts that may have been exposed.
3. **Validation**:

- Verified no additional unauthorised changes were made using file integrity monitoring tools.

Post-Incident Review

Root Cause:

- Exploitation of a known vulnerability in an unpatched service on AppServer01.

Recommendations:

1. **Patch Management**:
   - Enforce automated patch updates for critical servers.
2. **Access Control**:
   - Implement strict role-based access control (RBAC) policies.
3. **Monitoring**:
   - Enhance detection for registry changes and privilege modifications.
4. **Training**:
   - Conduct security awareness training to educate users on risks and secure behavior.

Visualisation

Timeline of Attack:

Time	Event	Action Taken
09:55 AM	Execution of exploit.exe	Alert triggered in SIEM
09:57 AM	Privilege escalation detected	Account disabled
09:58 AM	Registry modification detected	Server isolated
10:05 AM	Persistence mechanism found	Malicious tools removed

Heatmap of Activity:

- Red indicates suspicious privilege modifications and registry changes concentrated on AppServer01.

4. DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

Description: A flood of malicious traffic is impacting the availability of services.

Detection and Analysis:

- Detect unusually high traffic using network monitoring tools.
- Analyse traffic patterns to identify the type and source of the DDoS attack.

Containment:

- Enable rate-limiting on affected endpoints.
- Use a content delivery network (CDN) or anti-DDoS services to filter malicious traffic.

Eradication:

- Block traffic from specific attack sources using firewall rules.
- Deploy protective measures, such as geo-blocking or application-layer firewalls.

Recovery:

- Validate service performance post-attack.
- Conduct stress tests to ensure resilience.
- Improve capacity planning and implement DDoS mitigation tools.

SCENARIO EXAMPLE

Simulated Scenario: Distributed Denial of Service (DDoS) Attack

Date: November 21, 2024
Time: 2:30 PM
Environment: Corporate e-commerce platform hosted on a cloud infrastructure (AWS).

Detection

Alert Details:

- **Alert ID**: SIEM-2024-11-004

- **Source**: Web Application Firewall (WAF) and Cloud Monitoring
- **Description**: High volume of inbound traffic detected targeting the e-commerce login API endpoint (/api/v1/login).
- **Severity**: Critical

Logs:

Timestamp: 2024-11-21T14:15:32

Source: WAF

Event: Excessive HTTP Requests

IP: 185.23.45.90

Endpoint: /api/v1/login

Request Rate: 1,200 requests/sec

Timestamp: 2024-11-21T14:16:01

Source: Cloud Monitoring

Event: Resource Spike

CPU Utilisation: 98%

Memory Utilisation: 95%

Load Balancer Queue Length: 5,000 connections

Timestamp: 2024-11-21T14:18:45

Source: CDN

Event: Throttling Triggered

Blocked IP: 192.168.1.101

Blocked IP: 101.45.23.67

Analysis

Key Findings:

1. **Attack Type**:
    - **Application Layer (Layer 7)** DDoS attack targeting the /api/v1/login endpoint with a flood of HTTP POST requests.
    - Traffic exceeded normal thresholds by 500%, causing server resource exhaustion.
2. **Attack Origin**:
    - Multiple source IPs observed, indicating the use of a botnet.
    - Geo-IP analysis showed malicious traffic originating from multiple countries (Russia, Thailand and the U.S.).
3. **Impact**:
    - Service disruption: Legitimate users unable to access the login page due to resource exhaustion.
    - Backend database latency increased to 8 seconds/query.

Containment

Actions Taken:

1. **Traffic Filtering**:
    - Deployed WAF rules to block malicious IPs and patterns associated with the attack.
    - Enabled rate limiting to throttle excessive requests to /api/v1/login.
2. **Geofencing**:
    - Restricted traffic from countries not served by the platform.
3. **Load Redistribution**:
    - Adjusted CDN settings to cache non-sensitive static content aggressively, reducing server load.
4. **Blackhole Routing**:

- Diverted attack traffic to a sinkhole to prevent further load on production servers.

Eradication

1. **Botnet Analysis**:
   - Collaborated with threat intelligence feeds to analyse malicious IPs for botnet behavior.
   - Reported the identified botnet to relevant ISPs and law enforcement agencies.
2. **System Hardening**:
   - Strengthened backend API security with stricter input validation and rate limiting.
   - Updated firewall rules to detect and block unusual request patterns dynamically.
3. **Code Review**:
   - Reviewed the login API for vulnerabilities that could be exploited in the attack.

Recovery

1. **Service Restoration**:
   - Scaled up backend resources temporarily to handle residual traffic.
   - Rebalanced the load across servers to ensure service availability.
2. **Monitoring**:
   - Enabled enhanced monitoring for high-traffic endpoints.
   - Set up real-time alerts for abnormal traffic spikes.
3. **Post-Attack Verification**:
   - Conducted penetration testing to validate the resilience of the updated system.

Post-Incident Review

Root Cause:

- Lack of rate limiting and WAF rules for the affected endpoint made it susceptible to a Layer 7 DDoS attack.

Recommendations:

1. **Traffic Management**:
    - Deploy advanced anti-DDoS solutions like AWS Shield or Cloudflare.
    - Implement request authentication mechanisms such as CAPTCHA for login requests.
2. **Network Architecture**:
    - Optimise load balancers and use auto-scaling to handle unexpected traffic surges.
3. **Incident Response Readiness**:
    - Create a dedicated playbook for DDoS incidents to reduce response time.
    - Conduct periodic drills to test the effectiveness of mitigation strategies.

Visualisation

Timeline of Attack:

Time	Event	Action Taken
14:15 PM	Spike in login requests detected	WAF rules applied
14:16 PM	Resource exhaustion observed	Traffic throttled
14:18 PM	Attack escalated	Geofencing implemented
14:30 PM	Attack traffic mitigated	CDN caching optimised

Traffic Analysis:

- **Normal Traffic**: ~50 requests/sec.
- **Attack Traffic**: Spiked to 1,200 requests/sec.

5. INSIDER THREAT INCIDENT

Description: Malicious or unintentional activities from an internal user jeopardising data security.

Detection and Analysis:

- Monitor user behavior analytics for anomalies.
- Investigate alerts for unauthorised data access, exfiltration or deletions.

Containment:

- Suspend the user account involved in the incident.
- Block access to sensitive data or systems.

Eradication:

- Identify and address security gaps in user access permissions.
- Remove unauthorised tools or software used by the insider.

Recovery:

- Reinforce security awareness training programs.
- Implement strict logging and monitoring of privileged user activities.
- Establish a whistleblower mechanism for reporting internal threats.

SCENARIO EXAMPLE

Simulated Scenario: Insider Threat Incident

Date: November 21, 2024
Time: 11:00 AM
Environment: Corporate Active Directory network with sensitive financial and HR systems.

Detection

Alert Details:

- **Alert ID**: SIEM-2024-11-005

- **Source**: User Behavior Analytics (UBA) and SIEM
- **Description**: Unusual data access patterns detected from user.internal@company.com.
- **Severity**: Critical

Logs:

Timestamp: 2024-11-21T10:30:12

Source: File Server (HR-Shared)

Event: File Access

User: user.internal@company.com

Files Accessed: payroll-2024-Q3.xlsx, termination-list.docx

Timestamp: 2024-11-21T10:40:45

Source: Email Server

Event: Email Sent

User: user.internal@company.com

Recipient: personaluser@gmail.com

Attachment: payroll-2024-Q3.xlsx

Timestamp: 2024-11-21T10:50:32

Source: VPN Logs

Event: Data Transfer Spike

User: user.internal@company.com

Data Transferred: 1.5 GB in 10 minutes.

Timestamp: 2024-11-21T10:55:10

Source: Endpoint Monitoring (Laptop-1001)

Event: USB Device Plugged

User: user.internal@company.com

Files Copied: HR-confidential-strategy.pdf.

Analysis

Key Findings:

1. **Behavioral Indicators**:
    - Access to sensitive HR documents without a valid business reason.
    - Large data transfer over VPN in a short time span.
    - Attempted exfiltration using email and USB devices.
2. **Insider Profile**:
    - **User**: user.internal@company.com (Finance Department).
    - **Access Level**: Standard employee access with read-only permissions for HR and finance shared drives.
3. **Impact**:
    - Potential exposure of sensitive HR and payroll data.
    - Risk of data being sold or disclosed to unauthorised parties.
4. **Motivation**:
    - Likely disgruntled employee; no prior performance reviews indicate dissatisfaction.

Containment

Actions Taken:

1. **Immediate Account Suspension**:
    - Disabled the account user.internal@company.com in Active Directory.
2. **Endpoint Isolation**:
    - Isolated the laptop (Laptop-1001) from the network using EDR.

3. **Email and VPN Lockdown**:
    - Quarantined the suspicious email in the email server.
    - Revoked VPN access and terminated active sessions.
4. **USB Device Audit**:
    - Identified and blocked the USB device's serial number in endpoint protection policies.

Eradication

1. **Data Recovery**:
    - Retrieved and deleted the email with attachments sent to unauthorised external addresses.
    - Identified and mitigated the potential leakage by reviewing logs and blocking further data transfer channels.
2. **Policy Updates**:
    - Enforced stricter controls over sensitive file access, including Just-In-Time (JIT) permissions.
    - Implemented USB device restrictions for non-administrative users.
3. **User Access Review**:
    - Audited all access permissions granted to user.internal@company.com and removed unnecessary privileges.

Recovery

1. **System Restoration**:
    - Reintegrated isolated systems (laptop) into the network after forensic analysis confirmed no malicious persistence.
2. **Access Control Reinforcement**:
    - Applied role-based access controls (RBAC) to shared folders to minimise exposure risk.

- Implemented user-specific file activity monitoring for high-risk areas.

3. **Awareness Training**:
    - Conducted insider threat awareness training for employees and managers.

Post-Incident Review

Root Cause:

- Lack of continuous monitoring for abnormal user behavior and delayed detection of unauthorised access.

Recommendations:

1. **Enhanced Monitoring**:
    - Deploy user behavior analytics (UBA) across all endpoints.
    - Automate alerts for large data transfers or abnormal access to sensitive files.
2. **Zero Trust Security**:
    - Limit access to sensitive files based on business need.
    - Enforce stricter controls for remote and local data transfer.
3. **Periodic Audits**:
    - Regularly audit permissions and user access logs for anomalies.
4. **Reporting and Hotline**:
    - Establish an anonymous reporting mechanism for employees to report potential insider threats.

Visualisation

Timeline of Attack:

Time	Event	Action Taken
10:30 AM	Access to HR files detected	Account flagged in SIEM
10:40 AM	Email with attachment sent	Email quarantined

10:50 AM	Large data transfer over VPN	Account disabled, VPN revoked
10:55 AM	USB data exfiltration attempt	Endpoint isolated

Activity Heatmap:

- High-risk actions concentrated on shared drive access, email activity and external device usage.

6. SUPPLY CHAIN ATTACK

Description: An external vendor's compromised software or service affects your infrastructure.

Detection and Analysis:

- Identify the compromised vendor or software via alerts or advisories.
- Investigate logs for unusual changes or connections to vendor systems.

Containment:

- Disconnect affected systems from the compromised vendor's infrastructure.
- Disable access to affected software or services.

Eradication:

- Patch affected software with vendor-provided updates.
- Remove compromised applications or configurations.

Recovery:

- Validate the integrity of critical systems post-remediation.
- Audit vendor security practices and revise contracts for better security guarantees.
- Establish a vendor risk management program.

SCENARIO EXAMPLE

Simulated Scenario: Supply Chain Attack

Date: November 21, 2024
Time: 9:00 AM
Environment: Corporate IT infrastructure with cloud services, vendor connections and third-party software integrations.

Detection

Alert Details:

- **Alert ID**: SIEM-2024-11-006
- **Source**: SIEM (Splunk) and Threat Intelligence Platform
- **Description**: Suspicious connection established from a trusted third-party vendor's IP, potentially indicating an exploitation of a supply chain vulnerability.
- **Severity**: High

Logs:

Timestamp: 2024-11-21T08:45:32

Source: Cloud Provider API

Event: New API Key Generated

User: third-party-vendor@company.com

IP: 203.0.113.45 (Vendor IP)

Action: API key used to access internal resources without valid authorisation.

Timestamp: 2024-11-21T09:00:12

Source: SIEM

Event: Data Exfiltration Detected

User: third-party-vendor@company.com

Files Accessed: financial_records_Q3.xlsx, customer_db_backup.zip

Data Transfer: 1 GB to external IP.

Timestamp: 2024-11-21T09:02:17

Source: Email Server

Event: Email Sent

User: third-party-vendor@company.com

Recipient: personalemail@gmail.com

Attachment: financial_records_Q3.xlsx

Analysis

Key Findings:

1. **Attack Vector**:
    - The attack originates from a trusted third-party vendor (third-party-vendor@company.com) who had valid API access to company systems. This vendor appears to have been compromised.
    - The vendor's compromised credentials were used to generate a new API key and access internal systems, exfiltrating sensitive data (financial records and backups).
2. **Compromised Vendor**:
    - **Vendor Name**: Third-Party Software Solutions Inc. (provides software integration for payment processing and reporting).
    - **Vulnerabilities**: Unpatched vulnerabilities in the vendor's software allowed an attacker to gain access to the vendor's systems, enabling the breach of their credentials.
3. **Exfiltrated Data**:
    - **Files Exfiltrated**: Payroll data, customer database backups and confidential financial documents.
    - **Amount of Data**: 1 GB transferred to an external IP. This is an indication of large-scale data theft.
4. **Evidence of Exploitation**:
    - The attacker used the vendor's API access to bypass traditional authentication methods.
    - Unauthorised email sent with the same data attached, indicating potential collaboration or further compromise.

Containment

Actions Taken:

1. **Immediate API Access Revocation**:
    - All API keys associated with the vendor’s account were revoked.
    - Disconnected all active sessions and disabled the vendor's access to internal resources.
2. **Blocking Vendor IP**:
    - Blocked the IP address 203.0.113.45 from accessing any company infrastructure.
    - Implemented geo-blocking to prevent further unauthorised access from unfamiliar geolocations.
3. **Email Quarantine**:
    - Quarantined the email containing exfiltrated data.
    - Investigated the recipient email (personalemail@gmail.com) to determine if the data was further distributed.
4. **User and Device Isolation**:
    - Isolated the vendor’s device and accounts involved in the attack.
    - Analysed the devices and network traffic from the vendor’s systems.

Eradication

1. **Vendor Compromise Investigation**:
    - Worked with the vendor to perform a full forensic analysis of their systems to identify the root cause of the breach.
    - Found that the vendor had outdated software and failed to implement the latest security patches, which were exploited by attackers.
2. **Patching and Secure Configuration**:
    - Applied all critical patches and updates to the vendor’s software to prevent further exploitation.
    - Strengthened the security measures on the company’s side to limit access from third parties using least privilege access controls.

3. **Data Integrity and Recovery**:
    - Conducted an audit of the exfiltrated data to assess its impact.
    - Recovered data from backups and verified the integrity of the unaffected systems.
4. **Access Review**:
    - Re-evaluated all third-party vendor access privileges and implemented a more rigorous vetting process for vendor security.

Recovery

1. **System and Vendor Collaboration**:
    - Collaborated with the vendor to restore services and ensure that their systems were secured before re-establishing access.
    - Monitored the restored systems for any further anomalous activity.
2. **Notification and Legal Compliance**:
    - Notified affected parties (customers, employees) in accordance with data protection laws (GDPR, CCPA).
    - Informed regulatory bodies about the data breach as required by law.
3. **Enhanced Monitoring**:
    - Implemented enhanced monitoring on APIs and vendor access points to detect unusual activities in the future.
    - Deployed advanced SIEM rules to correlate vendor activity with internal systems for early detection.
4. **Data Loss Prevention (DLP)**:
    - Strengthened DLP controls to monitor and block sensitive data from being transmitted to unauthorised locations.
    - Implemented stronger email filtering mechanisms to prevent data leaks.

Post-Incident Review

Root Cause:

- Exploitation of a vulnerable third-party vendor's software, leading to the compromise of their credentials and subsequently, unauthorised access to sensitive company data.

Recommendations:

1. **Vendor Risk Management**:
    - Establish a rigorous third-party risk management program that includes regular security audits and checks for vendors.
    - Ensure that all vendors follow a minimum security standard and are regularly assessed for vulnerabilities.
2. **Zero Trust for Third-Party Access**:
    - Adopt a zero-trust security model for all third-party interactions, limiting their access to only the essential data and systems.
    - Implement more granular access controls to minimise the impact of a potential breach.
3. **Supply Chain Monitoring**:
    - Continuously monitor and verify all data exchanges with third-party vendors.
    - Use threat intelligence feeds to track the security posture of all partners and vendors.
4. **Incident Response Plan Update**:
    - Update the incident response plan to include specific steps for addressing supply chain attacks and breaches involving third-party vendors.

Visualisation

Timeline of Attack:

Time	**Event**	**Action Taken**
08:45 AM	Vendor API key generated	Alert triggered
09:00 AM	Data exfiltration attempt detected	API access revoked

09:02 AM	Unauthorised email sent	Email quarantined
09:30 AM	Vendor systems isolated	Vendor collaboration for investigation
10:00 AM	Data recovery and system restoration	Systems and access restored

Activity Heatmap:

- Increased access to sensitive data from the vendor's account, along with outbound data transfer spikes.

7. ADVANCED PERSISTENT THREAT (APT)

Description: Coordinated and stealthy attack targeting high-value systems and data.

Detection and Analysis:

- Detect using threat intelligence feeds, unusual persistence mechanisms or behavioral analysis.
- Analyse artifacts (malicious scripts, lateral movement) using sandbox environments.

Containment:

- Isolate affected systems and networks.
- Restrict access to sensitive data immediately.

Eradication:

- Remove malicious software, backdoors and other persistence mechanisms.
- Rotate credentials and enforce MFA for all affected accounts.

Recovery:

- Rebuild compromised systems from a trusted baseline.
- Implement advanced detection mechanisms (honeypots, machine learning models).

Post-Incident:

- Conduct a deep-dive forensic analysis to identify TTPs (Tactics, Techniques and Procedures).
- Share findings with threat intelligence platforms.

SCENARIO EXAMPLE

Simulated Scenario: Advanced Persistent Threat (APT)

Date: November 21, 2024
Time: 12:00 PM

Environment: Corporate environment with a mix of on-premises and cloud infrastructure (Azure, AWS), sensitive intellectual property and research data.

Detection

Alert Details:

- **Alert ID**: SIEM-2024-11-007
- **Source**: SIEM (Splunk), Network Intrusion Detection System (IDS) and Endpoint Detection and Response (EDR)
- **Description**: Suspicious network traffic and lateral movement detected across multiple internal systems, likely indicating an APT in progress.
- **Severity**: Critical

Logs:

Timestamp: 2024-11-21T11:30:15

Source: Network IDS

Event: C2 Traffic Detected

Description: Outbound encrypted traffic detected to external IP (192.0.2.10) over port 443 (HTTPS).

Timestamp: 2024-11-21T11:45:52

Source: EDR

Event: Suspicious PowerShell Command Execution

Description: PowerShell script executed on `DevServer01`, downloading a payload from a known APT C2 server.

Timestamp: 2024-11-21T11:50:33

Source: Active Directory

Event: Suspicious Account Privilege Escalation

Description: `user.john.doe@company.com` added to `Domain Admins` group without proper authorisation.

Timestamp: 2024-11-21T11:58:12

Source: SIEM

Event: Lateral Movement Detected

Description: `DevServer01` accessing `HRServer02`, which holds sensitive payroll data.

Analysis

Key Findings:

1. **Attack Type**:
    - The attack shows signs of a sophisticated **Advanced Persistent Threat (APT)**, characterised by stealthy, long-term access with specific goals (intellectual property theft or system disruption).
    - The attacker used **credential dumping** to escalate privileges and gain access to critical infrastructure.
2. **Initial Entry Point**:
    - The APT likely began through **phishing**, which allowed the attacker to gain a foothold via user.john.doe@company.com.
    - This account, although with regular privileges, was exploited to escalate privileges to **Domain Admin** and gain control of key systems.
3. **Persistence Mechanism**:
    - **PowerShell scripts** and **encrypted communication (C2)** with an external server were used for persistence.
    - The use of a **secure shell** (SSH) and **VPN tunneling** made it difficult to detect the movement.
4. **Lateral Movement**:
    - The attacker moved laterally from DevServer01 to HRServer02, which contains sensitive payroll data.

- Data access patterns suggest an attempt to exfiltrate payroll and employee data.

5. **Impact**:
    - Risk of sensitive data (intellectual property, payroll information) being exfiltrated.
    - Potential for system and infrastructure disruption if the attack is allowed to continue.

Containment

Actions Taken:

1. **Account Isolation**:
    - Immediately disabled the user.john.doe@company.com account to prevent further escalation.
    - Isolated any accounts with newly escalated privileges (i.e., Domain Admin rights).
2. **Network Segmentation**:
    - Isolated DevServer01, HRServer02 and other systems involved in lateral movement from the rest of the network.
    - Blocked outbound C2 traffic by updating firewall and IDS rules to drop packets to the external IP (192.0.2.10).
3. **Real-time Monitoring**:
    - Enabled network and endpoint monitoring on the affected systems to detect further malicious activity.
    - Enforced **multi-factor authentication (MFA)** for all privileged accounts.
4. **Credential Revocation**:
    - Reset passwords for all potentially compromised accounts.
    - Rolled back changes to the Domain Admins group and performed an audit to ensure no other unauthorised privilege escalations occurred.

Eradication

1. **Malware Removal**:
    - Deployed **EDR tools** to scan DevServer01, HRServer02 and other potentially impacted endpoints to identify and remove the malware.
    - Analysed the **PowerShell scripts** to identify indicators of compromise (IOCs) and wiped any backdoors left behind by the attacker.
2. **Patch Vulnerabilities**:
    - Applied critical security patches to all systems, especially on those with exposed remote access (RDP, SSH).
    - Hardened the configurations of servers and services vulnerable to remote code execution.
3. **C2 Server Blocking**:
    - Utilised threat intelligence to confirm the **C2 server** IP address (192.0.2.10) as known for APT activity, blocking it permanently and adding it to threat feeds.
4. **Privileged Account Review**:
    - Conducted a full audit of all domain admin accounts and access permissions.
    - Removed all unnecessary administrative rights and enforced least privilege access policies.

Recovery

1. **System Restoration**:
    - Restored the affected systems from clean, known good backups.
    - Validated the integrity of the restored data to ensure no data corruption or unauthorised changes were made during the attack.
2. **Incident Logging and Reporting**:
    - Documented all actions taken during the containment, eradication and recovery phases for compliance and internal analysis.
    - Reported the incident to law enforcement and regulatory bodies (where applicable).
3. **Strengthened Monitoring**:

- Implemented additional **network intrusion detection systems (NIDS)** and **endpoint monitoring** to detect any follow-up attempts or new threats.
- Enhanced internal visibility and logging to improve response times for future incidents.

Post-Incident Review

Root Cause:

- **Initial Phishing Attack**: The attacker gained initial access via phishing and escalated privileges by exploiting weak access controls and poor network segmentation.
- **Insufficient Detection**: The APT remained undetected for an extended period due to encrypted communication channels and the stealthy nature of the attack.

Recommendations:

1. **Improved Endpoint Protection**:
   - Deploy advanced **behavioral anomaly detection** on all endpoints to detect unusual activity (PowerShell scripts, file downloads, lateral movement).
   - Strengthen **EDR tools** and **SIEM integrations** for deeper visibility into endpoint actions.
2. **Zero Trust Model**:
   - Implement a **Zero Trust Security** framework, especially for critical resources and privileged accounts.
   - Reevaluate remote access methods and use technologies like **Privileged Access Management (PAM)** to control and audit admin access.
3. **Multi-Factor Authentication (MFA)**:
   - Enforce MFA for all **privileged accounts**, especially for those accessing critical systems and services.
   - Implement stricter network access policies for high-risk systems.
4. **Ongoing Threat Intelligence**:

- Integrate threat intelligence feeds into SIEM systems to keep track of emerging TTPs (Tactics, Techniques and Procedures) associated with APT groups.
- Regularly review threat intelligence for signs of new vulnerabilities or exploited software in your environment.

Visualisation

Timeline of Attack:

Time	Event	Action Taken
11:30 AM	C2 traffic detected (outbound)	Firewall rules updated
11:45 AM	PowerShell script executed	Account disabled, endpoint isolated
11:50 AM	Privilege escalation detected	Group membership revoked
11:58 AM	Lateral movement detected	Systems isolated and monitored
12:30 PM	Systems restored from backup	Systems and network recovery complete

Network Heatmap:

- Outbound traffic towards external IP (192.0.2.10) from compromised internal systems and lateral movement across internal servers.