CYBERSECURITY ANALYST INVESTIGATES A CRITICAL ALERT WITH SCENARIO EXAMPLES AND SIMULATIONS

BY IZZMIER IZZUDDIN

TABLE OF CONTENTS

UNUSUAL DNS TUNNELING ACTIVITY DETECTED

Alert Details

- **Alert Name:** Unusual DNS Tunneling Activity Detected
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** SIEM (QRadar)
- **Source:** DNS Logs + Threat Intelligence Integration
- **Affected Asset:** FIN-SERVER-002 (Finance Department Server)
- **User Associated:** Service Account svc-finance
- **Time of Detection:** 10:00 AM

Step 1: Alert Details and Initial Investigation

1. Review Alert Information

- **Description:** DNS tunneling involves encoding data of other programs or protocols in DNS queries and responses. The alert was triggered because:
  - Multiple DNS queries were observed for domains with high entropy (e.g., xy3rf7d6gq8[.]xyz) indicating potential tunneling.
  - The queries were consistent with a known malicious behavior profile in the threat intelligence database.
- **Sources of Suspicion:**
  - Outbound DNS traffic volume is 10 times higher than usual.
  - Destination domains are not on any allowlist and are flagged in threat intelligence as associated with malware.
  - The activity originated from a high-value target: the Finance server.

2. Immediate Checks

- **Check SIEM Dashboard:**
  - Query DNS logs for FIN-SERVER-002:

    ```
    SELECT source_ip, destination_ip, domain, timestamp
    FROM dns_logs
    WHERE source_ip = '192.168.10.5'
    AND timestamp BETWEEN '09:45:00' AND '10:00:00';
    ```

  - Results:
    - 200+ unique DNS queries to suspicious domains in the past 15 minutes.
    - Examples: xy3rf7d6gq8[.]xyz, kl8pz9mf[.]net.
- **Verify Threat Intelligence Correlation:**

- The queried domains match signatures of **"DNSpionage" malware** from the internal threat database.

3. Validate the Asset's Criticality

- **FIN-SERVER-002 Details:**
  - A high-priority finance server hosting payroll data.
  - Compromise risk is **high** due to sensitive data exposure.

Step 2: Incident Response Escalation

1. Notify the SOC Team

- An immediate message is sent to the SOC manager and Incident Response (IR) lead.
- SLA status: **Critical** (Remaining time: 12 minutes).

2. Containment Measures Initiated

- Apply firewall block rules for suspicious domains to halt DNS communication:

  ufw deny out to any port 53

- Isolate the server from the network via NAC policy enforcement.

Step 3: Deep Dive Analysis

1. Investigate the Root Cause

- **Analyse DNS Logs:**
  - Verify the payload size in DNS queries exceeds normal limits (~500 bytes per query).
  - Check for encoded patterns:
    - Query: base64 -d <payload> reveals file paths and credentials being exfiltrated.
- **Endpoint Logs:**
  - Correlate with EDR telemetry:
    - Malware executable found: dns_tunnel_agent.exe.
    - First executed by svc-finance at 09:42 AM.

2. Threat Actor Behavior Profiling

- Match with known Indicators of Compromise (IoCs) from the threat intelligence feed.

- Confirmed: IoCs align with **APT34** (a known cyber-espionage group).

Step 4: Mitigation and Recovery

1. Neutralise Threat

- **Malware Removal:** Push antivirus updates and initiate EDR remediation to remove dns_tunnel_agent.exe.
- **Service Account Action:** Disable svc-finance account temporarily.

2. System Recovery

- Perform disk imaging for forensic analysis.
- Restore the server from a known clean backup.

Step 5: Final Steps and Documentation

1. Communicate the Findings

- Notify stakeholders (Finance team, IT admin) of the issue and containment status.
- Escalate the incident to the Threat Hunting team for further analysis of lateral movement.

2. Create a Detailed Incident Report

Incident Summary:

- **Type:** DNS Tunneling Attack.
- **Source:** APT34-aligned malware using svc-finance service account.
- **Impact:** Potential exfiltration of financial data. Immediate containment successful.

Actions Taken:

1. Isolated the server and blocked malicious domains.
2. Removed malware and disabled compromised account.
3. Restored the server to a clean state..

UNUSUAL BEACONING ACTIVITY DETECTED (SUSPECTED C2 COMMUNICATION)

Alert Details

- **Alert Name:** Unusual Beaconing Activity Detected (Suspected C2 Communication)
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** SIEM (Splunk)
- **Source:** Network Traffic Logs + Intrusion Detection System (IDS)
- **Affected Asset:** ENG-LAP-014 (Engineer's Laptop)
- **User Associated:** izzat@company.com
- **Time of Detection:** 2:00 PM

Step 1: Alert Review and Initial Analysis

1. Review Alert Details

- **Description:** The SIEM triggered an alert for consistent outbound traffic to an external IP 103.45.76.89 every 60 seconds, resembling beaconing behavior.
- **Sources of Suspicion:**
    - External IP flagged in threat intelligence as linked to a known Command-and-Control (C2) server used by the **"CarbonStrike" malware.**
    - Persistent traffic pattern detected (small packets, exact intervals).
    - The asset (ENG-LAP-014) is flagged due to sensitive access levels (design files for an ongoing project).

2. Verify Asset Criticality

- **Asset Details:**
    - Engineer's laptop is part of the R&D team and has access to intellectual property (IP) related to a proprietary project.

Step 2: Initial Containment

1. Escalate to SOC and IR Team

- Inform SOC Manager and Incident Response Lead of a potential active threat targeting critical intellectual property.
- SLA status: **Critical** (Remaining time: 12 minutes).

2. Immediate Containment Actions

- **Block External Communication:** Apply firewall rules to block outbound traffic to IP 103.45.76.89.
- **Isolate Asset from Network:** Use NAC policies to quarantine ENG-LAP-014.

Step 3: Deep Dive Analysis

1. Analyse Network Traffic

- **Query SIEM:**
  - Analyse logs to understand the extent of communication:

    ```
    SELECT timestamp, source_ip, dest_ip, packet_size
    FROM network_logs
    WHERE source_ip = '192.168.20.14' AND dest_ip = '103.45.76.89';
    ```

  - Results:
    - Outbound traffic every 60 seconds since 1:30 PM.
    - Payload size is consistent (512 bytes), indicating potential encoded data.
- **Capture Network Packets:** Use Wireshark to decode payloads. Findings:
  - Encoded data matches Base64 patterns.
  - Decoded payload reveals exfiltrated file names (project_blueprint_v1.pdf, prototype_data.xlsx).

2. Endpoint Analysis

- **Scan for Malware:** EDR detects a suspicious executable (taskhostx.exe) running in the background.
- **Execution Path:** C:\Users\Alex\AppData\Roaming\taskhostx.exe.
- **Execution Timeline:** Created at 12:45 PM and executed at 12:46 PM.

3. Match Indicators of Compromise (IoCs)

- **IoCs Correlation:**
  - 103.45.76.89 → Matches CarbonStrike C2 IP.
  - taskhostx.exe → Hash matches a known malicious sample in VirusTotal.

4. Investigate Initial Infection Vector

- **Email Logs:** Check for suspicious emails sent to izzat@company.com. Findings:
  - Phishing email received at 12:30 PM with subject: "Updated Project Timeline."
  - Malicious attachment: project_timeline.docx containing a macro that drops taskhostx.exe.

Step 4: Mitigation and Recovery

1. Eradicate Malware

- **Terminate Processes:** Kill taskhostx.exe via EDR console.
- **Delete Malicious Files:** Remove files and associated registry keys.

2. Disable Compromised Account

- Temporarily disable izzat@company.com to prevent further misuse.

3. Recover Asset

- Perform a full re-image of ENG-LAP-014 to ensure no residual malware.

Step 5: Documentation and Reporting

1. Communicate Findings

- Notify stakeholders, including the Engineering Manager and IT Admin, about the containment and next steps.

2. Document Full Incident Report

Incident Summary:

- **Type:** C2 Beaconing and Exfiltration.
- **Source:** taskhostx.exe dropped by a malicious email attachment.
- **Impact:** Potential exfiltration of sensitive project files.

Actions Taken:

1. Blocked C2 communication and quarantined the asset.
2. Removed malware and restored the system.
3. Disabled compromised account temporarily.

UNAUTHORISED CLOUD STORAGE UPLOAD DETECTED

Alert Details

- **Alert Name:** Unauthorised Cloud Storage Upload Detected
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** SIEM (Splunk) + Cloud Security Monitoring Tool (AWS GuardDuty)
- **Source:** Outbound Data Exfiltration Rule Violation
- **Affected Asset:** FIN-SRV-002 (Finance Server)
- **User Associated:** iffah@company.com
- **Time of Detection:** 11:00 AM

Step 1: Alert Review and Initial Analysis

1. Review Alert Details

- **Description:** The SIEM triggered an alert for unusual data upload activity from the Finance Server (FIN-SRV-002) to an unauthorised cloud storage bucket hosted on Amazon S3 (s3://malicious-bucket123).
- **Sources of Suspicion:**
    - Data transfer exceeded the baseline threshold of 10MB per hour, reaching 500MB in 5 minutes.
    - S3 bucket not listed in the company's approved AWS resources.
    - Suspicious domain malicious-bucket123.s3.amazonaws.com flagged by AWS GuardDuty.

2. Verify Asset Criticality

- **Asset Details:**
    - Finance server hosts sensitive financial data, including payroll, tax filings and client payment records.
    - Impact of compromise: High, given the nature of stored data and compliance regulations (e.g., GDPR, SOX).

Step 2: Initial Containment

1. Escalate to SOC and Incident Response Team

- Notify SOC Manager and Incident Response Lead about a possible exfiltration attempt on sensitive financial data.

2. Immediate Containment Actions

- **Block Network Traffic:**
  - Use firewall policies to block outbound traffic to the S3 bucket's IP address and domain.
- **Quarantine Server:**
  - Temporarily isolate FIN-SRV-002 from the network to prevent further data transfer.

Step 3: Deep Dive Analysis

1. Investigate Network Traffic

- **Query SIEM Logs:**

```
SELECT timestamp, source_ip, dest_ip, file_size, protocol
FROM network_logs
WHERE source_ip = '10.10.10.20' AND dest_ip = '52.216.100.89';
```

  - Findings:
    - Large file uploads (e.g., payroll_2023.xlsx, client_financials_2023.pdf) between 10:50 AM and 10:55 AM.
    - Destination IP belongs to AWS infrastructure linked to the suspicious S3 bucket.

2. Investigate Server Activity

- **Endpoint Detection and Response (EDR):**
  - Detects execution of a script (upload_script.py) under the user account iffah.
  - **Execution Path:** C:\Users\JaneDoe\Documents\Scripts\upload_script.py.

3. Investigate User Behavior

- **Last Login:** User iffah logged in at 10:45 AM from an external IP address 198.51.100.25 (unrecognised).
- **GeoIP Check:** Originates from a foreign country not associated with the employee.
- **Credential Misuse:** Suggests account compromise.

4. Match Indicators of Compromise (IoCs)

- IoCs identified:
  - S3 bucket: malicious-bucket123.
  - Script name: upload_script.py.
  - External IP: 198.51.100.25.
  - Files Exfiltrated: Financial data, employee payroll.

Step 4: Mitigation and Recovery

1. Disable User Account

- Immediately disable the account iffah to prevent further misuse.

2. Remove Malicious Script

- Use EDR to terminate and delete upload_script.py.

3. Audit Uploaded Data

- Perform a quick audit using AWS CloudTrail logs to verify which files were uploaded:

  aws s3api list-objects --bucket malicious-bucket123

  - Files detected in the bucket:
    - payroll_2023.xlsx.
    - client_financials_2023.pdf.

4. Notify Cloud Provider

- Contact AWS Security to freese access to the bucket and request a takedown.

Step 5: Documentation and Reporting

1. Communicate Findings

- Inform the Finance Team and Compliance Officer about the incident.
- Notify the company's Data Protection Officer (DPO) to assess regulatory implications.

2. Document Full Incident Report

Incident Summary:

- **Type:** Unauthorised Cloud Data Exfiltration.
- **Source:** Compromised user credentials and malicious script execution.
- **Impact:** Partial data exfiltration (payroll and financial records).

Actions Taken:

1. Blocked unauthorised uploads to AWS S3.
2. Quarantined affected server.
3. Disabled compromised user account and removed malicious script.

4. Engaged AWS Security to freese the unauthorised bucket.

DNS TUNNELING DETECTED

Alert Details

- **Alert Name:** DNS Tunneling Detected
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** SIEM (Splunk) + Network Threat Detection Tool
- **Source:** High Volume of DNS Queries to Rarely Seen Domains
- **Affected Host:** ENG-SRV-004 (Engineering Server)
- **User Associated:** service_account@company.com
- **Time of Detection:** 14:00

Step 1: Alert Review and Initial Analysis

1. Review Alert Details

- **Description:** SIEM flagged abnormal DNS query behavior originating from ENG-SRV-004. Over 1,000 DNS queries to suspicious domains (abcd[.]example[.]com) in the past 10 minutes.
- **Source of Concern:**
    - **Rare Domain:** The domain abcd.example.com has no known association with the organisation.
    - **Query Pattern:** Repeated queries with randomised subdomains (e.g., xyz123.abcd.example.com).
    - **Usage:** DNS tunneling often facilitates covert data exfiltration or C2 communication.

2. Verify Asset Criticality

- **Asset Details:**
    - Engineering server hosts intellectual property, including product designs and patents.
    - Data exfiltration could compromise competitive advantage and lead to legal issues.

Step 2: Initial Containment

1. Escalate to SOC and Incident Response Team

- Notify SOC Manager and Incident Response Lead about potential DNS tunneling activity and affected server.

2. Immediate Containment Actions

- **Restrict Network Access:**
  - Block outbound DNS traffic from ENG-SRV-004 to abcd.example.com using firewall rules.
- **Isolate Host:**
  - Place ENG-SRV-004 in quarantine to prevent further data leakage.

Step 3: Deep Dive Analysis

1. Investigate Network Traffic

- **Query SIEM Logs:**

```
SELECT timestamp, source_ip, dest_ip, query_name, query_type, response_size
FROM dns_logs
WHERE source_ip = '10.10.50.15'
 AND query_name LIKE '%.abcd.example.com';
```

  - **Findings:**
    - Over 1,000 queries to abcd.example.com within 10 minutes.
    - Queries include randomised subdomains, indicating potential tunneling.
    - Responses carry encoded data (response sizes vary between 300–600 bytes).

2. Analyse Host Activity

- **Endpoint Detection and Response (EDR):**
  - Detects a suspicious process (dns_tunnel.exe) running under service_account.
  - File hash flagged by VirusTotal as associated with DNS tunneling malware.
  - Malware path: C:\Temp\dns_tunnel.exe.

3. Investigate User Account

- **Account Behavior:**
  - service_account is a non-human account used for scheduled tasks.
  - No scheduled tasks should generate DNS traffic from this host.
  - Indicates compromise of the service account.

4. Match Indicators of Compromise (IoCs)

- **IoCs Identified:**
  - Domain: abcd.example.com.
  - File hash: Known malware sample dns_tunnel.exe.

- Account: service_account.

Step 4: Mitigation and Recovery

1. Disable Compromised Account

- Disable service_account to prevent further misuse.

2. Terminate Malicious Process

- Use EDR to terminate dns_tunnel.exe and delete the file.

3. Block Malicious Domain

- Update DNS filtering rules to block abcd.example.com and its subdomains across the organisation.

4. Review Exfiltrated Data

- Analyse the DNS queries and payloads to identify potentially exfiltrated data:

  ```
  # Example script to decode Base64 payloads
  import base64
  encoded_payload = "dGhpcyBpcyBhIHNlY3JldCBkYXRhIGZyYWdtZW50"
  decoded_payload = base64.b64decode(encoded_payload).decode('utf-8')
  print(decoded_payload)
  ```

  - **Result:** Decoded data includes filenames such as patent_designs.docx.

5. Notify Relevant Teams

- Inform the Engineering team and Legal/Compliance teams about the potential compromise.

Step 5: Documentation and Reporting

1. Incident Report Summary

Incident Type: DNS Tunneling for Data Exfiltration.
Affected Asset: ENG-SRV-004.
Compromised Account: service_account.
Impact: Potential exposure of intellectual property.

Actions Taken:

1. Blocked outbound DNS traffic to malicious domain.
2. Isolated the affected server.
3. Disabled compromised account.
4. Terminated malicious process and removed malware.

SHADOW IT DETECTED - UNAUTHORISED CLOUD STORAGE USAGE

Alert Details

- **Alert Name:** Shadow IT Detected - Unauthorised Cloud Storage Usage
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** SIEM + CASB (Cloud Access Security Broker)
- **Source:** Traffic to unauthorised cloud storage service (shadydrive[.]com)
- **Affected Host:** HR-LAPTOP-024
- **User Associated:** izzmier@company.com (HR Manager)
- **Time of Detection:** 10:45

Step 1: Alert Review and Initial Analysis

1. Review Alert Details

- **Description:**
  - CASB flagged suspicious uploads to shadydrive[.]com from an HR employee's laptop.
  - Over 500 MB of data transferred in the past 30 minutes.
- **Initial Indicators of Concern:**
  - Domain (shadydrive.com) is not whitelisted or part of approved services.
  - Significant data transfer volume is abnormal for HR personnel.

2. Verify Asset and User Context

- **Asset Details:**
  - HR Laptop containing employee records, payroll data and other sensitive information.
- **User Details:**
  - izzmier@company.com has elevated privileges for accessing sensitive HR files.

Step 2: Initial Containment

1. Escalate to Incident Response Team

- Notify SOC Manager and escalate to Incident Response Team due to potential data exfiltration.

2. Immediate Containment Actions

- **Block Network Access:**

    - Use firewall or CASB to block outbound traffic to shadydrive.com.
- **Isolate Host:**
    - Quarantine HR-LAPTOP-024 to prevent further uploads or external communication.

Step 3: Deep Dive Analysis

1. Investigate Network Logs

- **Query SIEM Logs:**

```
SELECT timestamp, source_ip, dest_ip, file_name, file_size
FROM network_logs
WHERE dest_ip = '192.168.200.50' AND dest_domain = 'shadydrive.com';
```

    - **Findings:**
        - Upload of multiple files: payroll_2025.xlsx, employee_benefits.docx, HR_Audit.pdf.
        - Cumulative upload size: ~500 MB.

2. Investigate Host Activity

- **Endpoint Detection and Response (EDR):**
    - Active process: Unauthorised file-sharing application (shadydrive_uploader.exe).
    - File path: C:\Users\Mary\Downloads\shadydrive_uploader.exe.

3. Investigate User Actions

- **HR Access Logs:**
    - Review logs for sensitive file access by izzmier:
        - Files accessed: Payroll data, employee benefits and audit records in the last 24 hours.
    - **Unusual Behavior:** User accessed these files at odd hours (midnight).

4. Validate Indicators of Compromise (IoCs)

- **IoCs Identified:**
    - Domain: shadydrive.com.
    - Application: shadydrive_uploader.exe.
    - Files: Sensitive HR documents.

Step 4: Mitigation and Recovery

1. Disable User Account

- Temporarily disable izzmier@company.com to prevent further unauthorised access.

2. Terminate Malicious Process

- Kill the shadydrive_uploader.exe process using EDR.

3. Remove Unauthorised Application

- Delete the application and associated files from the host.

4. Forensic Analysis

- Create a snapshot of the system for further forensic analysis.
- Hash the uploaded files for future tracking and investigation.

Step 5: Documentation and Reporting

Incident Report Summary

Incident Type: Unauthorised Cloud Storage Usage (Shadow IT) for Data Exfiltration.
Affected Asset: HR-LAPTOP-024.
Compromised User: izzmier@company.com.
Impact: Potential exposure of payroll and employee data.

Actions Taken:

1. Blocked outbound traffic to unauthorised cloud storage service.
2. Isolated the affected laptop.
3. Disabled the user account.
4. Removed unauthorised file-sharing application.

ADVANCED PERSISTENT THREAT (APT) ACTIVITY DETECTED - UNAUTHORISED DOMAIN FRONTING

Alert Details

- **Alert Name:** Advanced Persistent Threat (APT) Activity Detected - Unauthorised Domain Fronting
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** IDS + SIEM + Threat Intelligence Platform
- **Source:** Inbound/Outbound traffic utilising a legitimate CDN (Content Delivery Network) for malicious communication.
- **Affected Host:** DEV-SRV-101 (Development Server hosting proprietary applications).
- **Time of Detection:** 13:25

Step 1: Alert Review and Initial Assessment

1. Review Alert Details

- **Description:**
  - IDS flagged anomalous encrypted communication from DEV-SRV-101 to a benign-looking domain cdn-legitimate[.]com, associated with APT campaigns.
  - High entropy in traffic suggests potential tunneling or encrypted command-and-control (C2) communication.
- **Key Indicators of Suspicion:**
  - Domain (cdn-legitimate[.]com) flagged by Threat Intelligence for domain fronting activities linked to known APT groups.
  - Traffic volume and patterns mimic beaconing behavior (e.g., periodic short bursts).

2. Correlate Asset and Context

- **Host Details:**
  - DEV-SRV-101: A critical asset with access to proprietary application source code and development tools.
- **Potential Impact:**
  - Exfiltration of intellectual property or introduction of malicious code into the development pipeline.

Step 2: Initial Containment Actions

1. Escalate Incident to IR Team

- Notify SOC Manager and escalate to the Incident Response Team due to APT-level threat indicators.

2. Immediate Containment Actions

- **Block Communication:**
  - Use firewall and IDS to block outbound traffic to cdn-legitimate[.]com.
- **Isolate Host:**
  - Quarantine DEV-SRV-101 using EDR to halt any ongoing communication.

Step 3: Advanced Analysis and Investigation

1. Analyse Network Traffic

- **Traffic Analysis via SIEM:**
  - Query traffic logs:

    ```
    sql
    SELECT timestamp, source_ip, dest_ip, dest_port, protocol, data_size
    FROM network_traffic
    WHERE source_ip = '10.10.20.101'
      AND dest_domain = 'cdn-legitimate.com';
    ```

  - **Findings:**
    - Outbound traffic every 15 seconds over port 443.
    - Data packets with high entropy indicating encrypted payloads.

2. Investigate Host Activity

- **EDR Investigation:**
  - Active process: svchost.exe running under an unusual directory (C:\Temp\) and spawning periodic outbound connections.
  - New file created: C2-agent.dll in C:\Temp\.

3. Analyse Threat Intelligence

- **Threat Feed Lookup for Domain:**
  - cdn-legitimate[.]com confirmed as a C2 domain used by APT-29.
  - Related IoCs include:
    - File hash: d2e5f55bfa8c9e3120efc2b51a089e77 (matches C2-agent.dll).

        - Encrypted payload mimics known tunneling techniques (domain fronting).

4. Analyse Logs for Lateral Movement

- **SIEM Analysis for Lateral Connections:**
    - Check for any RDP, SMB or other connections originating from DEV-SRV-101.
    - Findings:
        - Lateral connections detected to DEV-SRV-103 and DB-SRV-05.

Step 4: Mitigation and Recovery

1. Disable Host Communication

- Ensure DEV-SRV-101 remains quarantined and unable to reach any internal or external systems.

2. Terminate Malicious Processes

- Use EDR to kill svchost.exe and delete associated malicious files (C2-agent.dll).

3. Investigate Lateral Impact

- Quarantine DEV-SRV-103 and DB-SRV-05 for further analysis.

4. Enhance Network Rules

- Block all traffic to cdn-legitimate[.]com across the organisation.
- Deploy enhanced IDS rules to flag high-entropy traffic patterns.

Step 5: Documentation and Post-Incident Actions

Incident Summary

Type: APT Activity - Domain Fronting
Affected Assets:

- Primary: DEV-SRV-101
- Secondary: DEV-SRV-103, DB-SRV-05

Indicators of Compromise (IoCs):

- Domain: cdn-legitimate[.]com
- File Hash: d2e5f55bfa8c9e3120efc2b51a089e77

- Malicious Process: C2-agent.dll executed by svchost.exe.

Actions Taken:

1. Blocked outbound communication to the malicious domain.
2. Quarantined affected systems (DEV-SRV-101, DEV-SRV-103, DB-SRV-05).
3. Terminated malicious processes and removed malicious files.

DATA EXFILTRATION VIA COVERT CHANNEL DETECTED

Alert Details

- **Alert Name:** Data Exfiltration via Covert Channel Detected
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** NDR (Network Detection and Response) + SIEM Correlation Rules
- **Source:** Rogue IoT device communicating with an unknown external IP over DNS.
- **Affected Host:** Unregistered IoT device on the corporate network (IoT-Unknown-37).
- **Time of Detection:** 14:15

Step 1: Alert Review and Initial Assessment

1. Review Alert Details

- **Description:**
  - Unusual spike in DNS traffic from IoT-Unknown-37 (not part of the corporate asset inventory).
  - NDR flagged repeated DNS queries with suspicious subdomain patterns indicative of data exfiltration.
  - Traffic directed to malicious[.]domain.

2. Context Analysis

- **Device Profile:**
  - MAC address indicates a generic IoT sensor, likely connected to the guest or insecure VLAN.
  - Device is bypassing established network segmentation policies.
- **Potential Impact:**
  - Stealthy exfiltration of sensitive information.
  - Use of DNS as a covert channel to avoid traditional monitoring tools.

3. Verify Business Relevance

- **Action Taken:**
  - Cross-reference the MAC address in asset inventory and CMDB.
  - **Finding:** No record exists. The device is unauthorised.

Step 2: Initial Containment Actions

1. Escalate Incident

- Notify SOC Manager and incident response stakeholders of a possible rogue IoT device being used for data theft.

2. Contain the Threat

- **Action Taken:**
  - Quarantine the rogue device using NAC (Network Access Control) to block all network traffic from IoT-Unknown-37.
  - Apply DNS sinkhole rules in the firewall to block access to malicious[.]domain.

Step 3: Advanced Analysis and Investigation

1. Investigate DNS Queries

- **DNS Query Patterns (SIEM Query):**

```
SELECT timestamp, source_ip, query_name
FROM dns_logs
WHERE source_ip = '192.168.10.237';
```

  - **Findings:**
    - High volume of DNS queries with dynamically generated subdomains:
      - abcd1234.malicious[.]domain
      - efgh5678.malicious[.]domain
    - Pattern suggests DNS tunneling using Base64-encoded data.

2. Decode DNS Payload

- **Action Taken:**
  - Extract subdomain values and decode them:

```
import base64
data = "abcd1234"  # Example subdomain
decoded = base64.b64decode(data)
print(decoded.decode('utf-8'))
```

  - **Decoded Data:** Partial document fragments containing internal IPs and login credentials.

3. Network Traffic Analysis

- **PCAP Review (NDR):**

    - Outbound DNS queries contain packet payloads larger than standard DNS requests.
    - No legitimate traffic from the IoT device prior to the anomaly.
- **Key Indicators:**
    - DNS queries match known tunneling toolkits used by threat actors (e.g., Iodine or DNScat2).

4. Investigate Device Origin

- **MAC Address Lookup:**
    - Manufacturer: Generic IoT vendor.
    - Deployment in unauthorised areas, likely plugged in by an insider or unauthorised personnel.

5. Cross-Check External Domain

- **Threat Intelligence Analysis:**
    - malicious[.]domain associated with known threat actors conducting IoT-based attacks.
    - Domain registered less than 30 days ago.

Step 4: Mitigation and Recovery

1. Remove Rogue IoT Device

- Physically locate and disconnect IoT-Unknown-37 from the network.

2. Threat Neutralisation

- Continue DNS sinkhole operation and monitor for residual traffic patterns.

3. Validate System Integrity

- Review logs for signs of lateral movement or additional compromised devices.
- Conduct vulnerability scans on the VLAN to identify potential risks.

4. Notify Affected Stakeholders

- Inform asset owners and IT team to enforce stricter IoT access policies.

Step 5: Documentation and Post-Incident Actions

Incident Summary

- **Type:** Data Exfiltration via Rogue IoT Device.
- **Affected Assets:** None directly compromised, but potential insider negligence or malicious intent detected.

Indicators of Compromise (IoCs):

- Domain: malicious[.]domain
- DNS Query Pattern: Dynamically generated subdomains (Base64 encoded).
- MAC Address: Unregistered IoT device.

Actions Taken:

1. Quarantined rogue device.
2. Blocked malicious domain at DNS level.
3. Physically removed unauthorised IoT device.

SQL INJECTION DETECTED IN CUSTOMER WEB PORTAL

Alert Details

- **Alert Name:** SQL Injection Attempt Detected
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** WAF (Web Application Firewall) + SIEM Correlation Rules
- **Source IP:** 185.143.223.99
- **Target URL:** https://customer-portal.example.com/login
- **Time of Detection:** 15:00

Step 1: Alert Review and Initial Assessment

1. Review Alert Details

- **Description:**
  - Multiple SQL injection attempts detected from a single source IP targeting the login endpoint.
  - Malicious payloads identified in the HTTP POST parameters.
  - WAF blocked several requests with the signature: SQL Injection - UNION SELECT.

2. Context Analysis

- **Potential Impact:**
  - If successful, the attacker could access sensitive customer data, manipulate the database or execute administrative commands.

3. Verify Business Relevance

- **Action Taken:**
  - Confirm the target is a live production web application handling customer data.
  - **Finding:** The web portal is critical to business operations and the database contains Personally Identifiable Information (PII).

Step 2: Initial Containment Actions

1. Escalate Incident

- Notify SOC Manager, application owner and database administrator (DBA).

2. Contain the Threat

- **Action Taken:**
  - Use WAF to temporarily block the offending IP address (185.143.223.99).
  - Enable enhanced SQL injection protection rules across the application.

Step 3: Advanced Analysis and Investigation

1. Review WAF Logs

- **WAF Logs (Sample):**

  [Time: 14:58] POST /login HTTP/1.1
  User-Agent: Mozilla/5.0
  Payload: username=admin'--&password=123456
  Result: BLOCKED

  [Time: 14:59] POST /login HTTP/1.1
  Payload: username=admin' UNION SELECT 1,2,3--&password=123456
  Result: BLOCKED

  - **Findings:**
    - Multiple SQL injection payloads targeting the username field.
    - The attacker attempted common patterns, including UNION SELECT and comment-based SQL injection (--).

2. Database Logs

- Query database logs for suspicious activity:

  ```
  SELECT * FROM logs
  WHERE query LIKE '%--%'
    OR query LIKE '%UNION SELECT%'
    OR query LIKE '%admin%';
  ```

  - **Findings:**
    - No successful malicious queries detected.
    - WAF successfully blocked all attempts before they reached the database.

3. Correlate Threat Intelligence

- Search for the IP (185.143.223.99) in a threat intelligence database:
  - **Finding:**
    - The IP is linked to previous SQL injection campaigns targeting financial institutions.

4. Investigate Source IP

- Perform reverse DNS lookup and geo-location for 185.143.223.99:
    - **Location:** Known proxy service provider in Eastern Europe.
    - **Risk:** High likelihood of being used by attackers for anonymisation.

5. Analyse Application Vulnerability

- Verify if the login endpoint has proper sanitisation and parameterised queries.
    - **Action Taken:** Conduct quick static code analysis:
        - **Finding:** The username field is not properly sanitised, making it vulnerable to injection.

Step 4: Mitigation and Recovery

1. Patch the Vulnerability

- Collaborate with the development team to:
    - Implement parameterised queries in the affected endpoint.
    - Add input validation to prevent malicious payloads.

2. Update WAF Rules

- Enhance WAF rules to block specific SQL injection signatures more effectively.

3. Monitor and Validate

- Continue monitoring the application for further suspicious activity.

Step 5: Documentation and Post-Incident Actions

Incident Summary

- **Type:** SQL Injection Attempt.
- **Affected Endpoint:** https://customer-portal.example.com/login.
- **Source:** Malicious IP address (185.143.223.99).

Indicators of Compromise (IoCs):

- IP Address: 185.143.223.99
- SQL Injection Payloads:
    - admin'--
    - UNION SELECT 1,2,3--

Actions Taken:

1. Blocked malicious IP address via WAF.
2. Identified and patched the vulnerable endpoint.
3. Updated WAF rules for enhanced protection.

DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK

Alert Details

- **Alert Name:** DDoS Attack Detected on Web Server
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** IDS/IPS + SIEM Correlation
- **Source IPs:** Multiple (suspected botnet traffic)
- **Target:** https://api.customer-service.example.com
- **Time of Detection:** 14:00

Step 1: Alert Review and Initial Assessment

1. Review Alert Details

- **Description:**
  - Sudden spike in traffic targeting the /api/login endpoint on the customer service API server.
  - Traffic exceeds normal thresholds, with over 10,000 requests per second.

2. Context Analysis

- **Potential Impact:**
  - API unavailability for legitimate users.
  - Degraded performance or a full system crash if unmitigated.

3. Verify Business Relevance

- **Action Taken:**
  - Confirm the API endpoint is business-critical for customer support.
  - **Finding:** This API handles authentication for over 1 million daily users.

Step 2: Initial Containment Actions

1. Escalate Incident

- Notify SOC Manager, DevOps and network engineering teams.

2. Contain the Threat

- **Immediate Actions Taken:**
  - Redirect suspicious traffic to a sinkhole.
  - Apply rate limiting at the firewall and load balancer.

- Activate mitigation features in the DDoS protection system (e.g., Cloudflare, AWS Shield).

Step 3: Advanced Analysis and Investigation

1. Traffic Analysis

- Inspect traffic patterns using SIEM and network monitoring tools:
  - **Observations:**
    - Requests are originating from over 500 IPs globally.
    - Common User-Agent strings used by bots.
    - Large volume of HTTP GET and POST requests targeting /api/login.

2. Threat Intelligence Correlation

- Query source IPs against threat intelligence databases:
  - **Findings:**
    - Many IPs are flagged as part of known botnets (e.g., Mirai).

3. Check for Amplification

- Identify if the attack is leveraging amplification techniques like DNS or NTP reflection:
  - **Findings:**
    - No amplification detected; attack uses direct botnet traffic.

4. System Performance Logs

- Review system performance logs:
  - **Findings:**
    - CPU utilisation at 95%.
    - API response times degraded significantly (from 300ms to 5 seconds).

5. Behavioral Indicators

- Analyse if legitimate users are affected:
  - **Finding:** Several customer complaints about timeouts and unresponsiveness.

Step 4: Mitigation and Recovery

1. Fine-Tune Mitigation Controls

- Adjust rate-limiting thresholds to balance traffic and avoid blocking legitimate users.
- Deploy CAPTCHA challenges for suspicious traffic.

2. Divert Traffic

- Enable traffic redirection to an alternative data center.

3. Strengthen DDoS Protection

- Enable advanced DDoS mitigation modes in the CDN and WAF.

Step 5: Documentation and Post-Incident Actions

Incident Summary

- **Type:** Distributed Denial-of-Service (DDoS) Attack.
- **Affected Resource:** https://api.customer-service.example.com.
- **Source:** Over 500 IPs globally, suspected botnet activity.

Indicators of Compromise (IoCs):

- Source IPs: Various, flagged as botnet.
- User-Agent Strings: Common botnet headers (e.g., "curl/7.x").

Actions Taken:

1. Applied rate-limiting and sinkholing techniques.
2. Activated CDN-based DDoS mitigation.
3. Redirected traffic to a secondary data center.

PHISHING CAMPAIGN DETECTED

Alert Details

- **Alert Name:** Targeted Phishing Campaign
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** Email Gateway + SIEM Correlation
- **Target Users:** Finance Department (10 users)
- **Phishing Domain:** secure-finance-payments[.]com
- **Time of Detection:** 10:00

Step 1: Alert Review and Initial Assessment

1. Review Alert Details

- **Description:**
  - An email impersonating the company CFO was sent to 10 users in the finance department.
  - The email contains a malicious link to a phishing site mimicking a corporate payment system.

2. Context Analysis

- **Potential Impact:**
  - Unauthorised access to financial accounts.
  - Data theft (e.g., login credentials, financial transactions).
  - Possible compromise of sensitive payment data.

3. Verify Business Relevance

- **Action Taken:**
  - Confirm that the email domain impersonates a legitimate payment system used by the organisation.
  - **Finding:** Domain closely resembles the organisation's official vendor payment portal.

Step 2: Initial Containment Actions

1. Escalate Incident

- Notify SOC Manager, IT Security and finance department leadership.

2. Contain the Threat

- **Immediate Actions Taken:**
    - Block the phishing domain (secure-finance-payments[.]com) on email gateways and firewalls.
    - Quarantine the phishing emails in affected users' mailboxes.
    - Disable any links embedded in the phishing emails using URL re-write features.

Step 3: Advanced Analysis and Investigation

1. Email Header Analysis

- **Email Headers (Sample):**

  From: cfo@company.com
  To: finance-team@company.com
  Subject: Urgent: Payment Approval Required
  SPF: Fail
  DKIM: Fail
  DMARC: Fail

    - **Findings:**
        - Sender address spoofed as the company CFO.
        - Failed SPF, DKIM and DMARC validation indicate forgery.

2. Phishing Link Analysis

- Extracted link: https://secure-finance-payments[.]com/login.
- Perform sandbox analysis:
    - **Observations:**
        - The page mimics the legitimate payment system's login portal.
        - JavaScript captures keystrokes (indicative of credential harvesting).

3. Threat Intelligence Correlation

- Search for the domain in threat intelligence feeds:
    - **Finding:** Newly registered domain flagged as malicious in multiple sources.

4. User Activity Investigation

- Check if any users clicked on the link:
    - Review SIEM and proxy logs for HTTP GET requests to the phishing domain.
    - **Findings:**
        - Two users accessed the phishing site but did not submit credentials.

5. Identify Additional Threat Indicators

- Look for related phishing domains or IPs:
    - **Finding:** The domain resolves to IP 192.168.45.33, part of a known malicious IP range.

Step 4: Mitigation and Recovery

1. Block Additional Threats

- Add the phishing IP and related domains to the organisation's blocklist.

2. Protect Affected Users

- Contact the two users who accessed the site to verify no credentials were entered.
- Force password resets for these users as a precaution.

3. Strengthen Email Security

- Adjust email filtering rules to detect similar phishing patterns.
- Conduct an immediate review of email security policies (e.g., SPF, DKIM, DMARC enforcement).

Step 5: Documentation and Post-Incident Actions

Incident Summary

- **Type:** Targeted Phishing Campaign.
- **Affected Users:** 10 users in the finance department.
- **Phishing Domain:** secure-finance-payments[.]com.
- **Threat Vector:** Email impersonation of CFO.

Indicators of Compromise (IoCs):

- Phishing Domain: secure-finance-payments[.]com.
- Malicious IP: 192.168.45.33.

Actions Taken:

1. Quarantined phishing emails and blocked malicious domain/IP.
2. Prevented credential submission by affected users.
3. Enhanced email gateway rules for improved detection.

VULNERABILITY EXPLOITATION IN CLOUD ENVIRONMENT

Alert Details

- **Alert Name:** Suspicious Activity on Cloud Storage Bucket
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** CSP Security Monitoring + SIEM Correlation
- **Target:** Cloud Storage Bucket sensitive-customer-data
- **Indicators:**
    - Publicly accessible storage bucket.
    - Unusual access from an external IP (172.31.24.15).
    - Large-scale data download detected.
- **Time of Detection:** 13:00

Step 1: Alert Review and Initial Assessment

1. Review Alert Details

- **Description:**
    - A publicly exposed cloud storage bucket containing sensitive customer information is being accessed from an external IP.
    - Large volumes of data have been downloaded.

2. Context Analysis

- **Potential Impact:**
    - Data breach leading to loss of sensitive customer information.
    - Non-compliance with regulations (e.g., GDPR, CCPA).

3. Verify Business Relevance

- **Action Taken:**
    - Check the bucket's intended permissions.
    - **Finding:** The bucket is intended for internal use only and should not be public.

Step 2: Initial Containment Actions

1. Escalate Incident

- Notify the SOC Manager, Cloud Security Team and relevant stakeholders.

2. Contain the Threat

- **Immediate Actions Taken:**
    - Restrict public access to the bucket by updating permissions.
    - Block the suspicious external IP address (172.31.24.15) via the CSP's firewall.
    - Rotate the access keys for any service accounts linked to the bucket.

Step 3: Advanced Analysis and Investigation

1. Investigate Access Logs

- **Access Log Findings:**
    - External IP (172.31.24.15) accessed the bucket using a compromised API key.
    - Data transfer logs show a download of 5GB of sensitive customer data.

2. Threat Intelligence Correlation

- Query the external IP in threat intelligence feeds:
    - **Finding:** The IP is linked to known malicious activity (e.g., cryptojacking campaigns and data exfiltration).

3. Cloud Configuration Review

- Audit the bucket configuration using CSP tools:
    - **Findings:**
        - Bucket was misconfigured with public read access.
        - An API key with excessive privileges was not rotated for over 12 months.

4. Assess Data Sensitivity

- Identify data stored in the bucket:
    - **Finding:** The bucket contained PII (e.g., customer names, addresses and payment details).

5. Investigate Internal Activity

- Check for unauthorised actions by internal users:
    - **Finding:** No evidence of insider activity; the compromise likely occurred externally.

Step 4: Mitigation and Recovery

1. Implement Configuration Fixes

- Restrict access to sensitive buckets to internal IP ranges.
- Enable strict IAM policies with the principle of least privilege.

2. Enhance API Security

- Rotate API keys and implement key usage monitoring.
- Enforce Multi-Factor Authentication (MFA) for API access.

3. Monitor for Further Threats

- Set up enhanced alerts for any future access attempts from the malicious IP.

Step 5: Documentation and Post-Incident Actions

Incident Summary

- **Type:** Vulnerability Exploitation in Cloud Storage.
- **Affected Resource:** Cloud Storage Bucket sensitive-customer-data.
- **Threat Vector:** Misconfigured public access combined with a compromised API key.

Indicators of Compromise (IoCs):

- Malicious IP: 172.31.24.15.
- Unauthorised Access Times: 12:45 to 13:00.

Actions Taken:

1. Blocked public access and malicious IP.
2. Rotated API keys and enforced stricter IAM policies.
3. Enhanced cloud storage monitoring for abnormal activities.

EXPLOITATION OF THIRD-PARTY VULNERABILITY

Alert Details

- **Alert Name:** Unauthorised Activity via Third-Party Application
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** SIEM Correlation + Endpoint Detection and Response (EDR) Tool
- **Target Application:** Employee Expense Management Tool (Cloud-based)
- **Indicators:**
    - Unauthorised access from external IP: 185.43.12.200.
    - Use of an unpatched third-party application vulnerability (CVE-2025-XXXX).
    - Privilege escalation leading to data exfiltration attempts.
- **Time of Detection:** 14:00

Step 1: Alert Review and Initial Assessment

1. Review Alert Details

- **Description:**
    - Exploitation of a known vulnerability in a third-party expense management application used by employees.
    - Unauthorised access detected with signs of privilege escalation.

2. Context Analysis

- **Potential Impact:**
    - Exposure of sensitive employee financial data.
    - Lateral movement into the corporate environment via API integrations.
    - Regulatory non-compliance risks.

3. Verify Business Relevance

- **Action Taken:**
    - Confirm the application’s role and integration points in the organisation.
    - **Finding:** The application is used for expense approvals and is integrated with HR systems.

Step 2: Initial Containment Actions

1. Escalate Incident

- Notify SOC Manager, Application Security Team and the vendor's security contact.

2. Contain the Threat

- **Immediate Actions Taken:**
  - Disable API keys associated with the application to halt integrations temporarily.
  - Apply web application firewall (WAF) rules to block requests from the malicious IP (185.43.12.200).
  - Restrict access to the application for all users until further investigation.

Step 3: Advanced Analysis and Investigation

1. Vulnerability Identification

- **Known CVE:** CVE-2025-XXXX.
  - **Description:** Unauthenticated remote code execution vulnerability in the third-party application.
  - **Patch Status:** Vendor released a patch two weeks ago; the organisation has not applied it.

2. Threat Intelligence Correlation

- Search for exploit activity related to CVE-2025-XXXX:
  - **Finding:** Exploits for this CVE are publicly available and active campaigns are targeting cloud applications.

3. Log Analysis

- **Application Logs:**
  - Show access to sensitive HR data (employee salary and bank details).
  - Unauthorised API requests from IP 185.43.12.200.
- **SIEM Logs:**
  - Evidence of privilege escalation from regular user accounts to administrative access.
  - Large data transfer logs flagged at 13:50.

4. Assess Scope of Compromise

- **Impact Assessment:**
  - Data exfiltration confirmed for 200 employee records.
  - No evidence of lateral movement beyond the application environment.

Step 4: Mitigation and Recovery

1. Apply Patches

- Deploy the vendor-released patch to remediate the CVE in the application.

2. Secure Access

- Rotate API keys and reconfigure IAM policies to enforce the principle of least privilege.
- Require MFA for accessing the application.

3. Monitor for Further Activity

- Set up enhanced monitoring for access attempts targeting the application.
- Block known malicious IPs associated with campaigns targeting CVE-2025-XXXX.

Step 5: Documentation and Post-Incident Actions

Incident Summary

- **Type:** Exploitation of Third-Party Vulnerability.
- **Affected Application:** Employee Expense Management Tool.
- **Threat Vector:** Known vulnerability (CVE-2025-XXXX) exploited by an external IP.

Indicators of Compromise (IoCs):

- Malicious IP: 185.43.12.200.
- CVE Exploited: CVE-2025-XXXX.
- Unauthorised Access Time: 13:50 to 14:00.

Actions Taken:

1. Disabled application access and API integrations.
2. Blocked malicious IP and applied firewall rules.
3. Deployed critical patch and rotated credentials.

IOT DEVICE COMPROMISE IN CORPORATE NETWORK

Alert Details

- **Alert Name:** Unauthorised IoT Device Activity Detected
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** Network Behavior Analysis (NBA) Tool + SIEM Correlation
- **Target Device:** Smart Office Camera (IP: 10.10.5.12)
- **Indicators:**
    - Unauthorised outbound connections to an external IP: 204.45.77.19.
    - Unusual traffic volume originating from the IoT device.
    - Suspected command-and-control (C2) communication detected.
- **Time of Detection:** 10:30

Step 1: Alert Review and Initial Assessment

1. Review Alert Details

- **Description:**
    - An office IoT camera is exhibiting suspicious behavior, including initiating outbound connections to a known malicious IP.

2. Context Analysis

- **Potential Impact:**
    - Compromise of the IoT device for use in a botnet or exfiltration of video streams.
    - Potential lateral movement within the corporate network.

3. Verify Business Relevance

- **Action Taken:**
    - Confirm the device type, ownership and function.
    - **Finding:** The IoT camera is used for monitoring office spaces and is connected to the corporate network.

Step 2: Initial Containment Actions

1. Escalate Incident

- Notify the SOC Manager, IT Network Team and Physical Security Team.

2. Contain the Threat

- **Immediate Actions Taken:**
    - Isolate the IoT camera (IP: 10.10.5.12) from the corporate network.
    - Block outbound traffic to the malicious IP (204.45.77.19) at the network firewall.
    - Disable the device's remote access features.

Step 3: Advanced Analysis and Investigation

1. Analyse Network Traffic

- **Network Logs:**
    - Traffic analysis reveals the device communicating with 204.45.77.19 on port 8080, which is commonly used for C2 servers.
    - A high volume of outbound traffic suggests potential data exfiltration or botnet activity.

2. Investigate Device Logs

- **Device Findings:**
    - Logs indicate an unauthorised login from an external IP (194.32.56.21) using default credentials.
    - The device firmware is outdated, with known vulnerabilities.

3. Threat Intelligence Correlation

- Query malicious IP (204.45.77.19) in threat intelligence feeds:
    - **Finding:** The IP is linked to a Mirai-like IoT botnet campaign.

4. Assess Impact and Scope

- **Findings:**
    - No lateral movement detected into the corporate network.
    - Device appears to have been hijacked for botnet participation.

Step 4: Mitigation and Recovery

1. Remediate Device Vulnerabilities

- Reset the device to factory settings and apply the latest firmware update.
- Change default credentials and enforce strong passwords.

2. Enhance Network Security

- Segregate IoT devices into a dedicated VLAN.

- Implement strict firewall rules for IoT traffic, limiting outbound connections to approved destinations.

3. Monitor for Further Activity

- Continue monitoring network traffic for signs of other compromised devices.
- Enhance alerting for suspicious IoT activity.

Step 5: Documentation and Post-Incident Actions

Incident Summary

- **Type:** IoT Device Compromise.
- **Affected Device:** Smart Office Camera (IP: 10.10.5.12).
- **Threat Vector:** Unauthorised access using default credentials, followed by botnet enlistment.

Indicators of Compromise (IoCs):

- External IP: 204.45.77.19 (C2 server).
- Unauthorised login IP: 194.32.56.21.
- Ports: 8080.

Actions Taken:

1. Isolated the compromised IoT device.
2. Blocked malicious IPs and applied stricter network controls.
3. Updated firmware and secured the device with strong credentials.

SOCIAL ENGINEERING ATTACK

Alert Details

- **Alert Name:** Potential Credential Harvesting via Spear Phishing
- **Severity:** Critical
- **SLA:** 15 minutes
- **Generated by:** Email Security Gateway + SIEM Correlation
- **Indicators:**
    - Phishing email sent to 50 employees from external sender: ceo@company-hr-secure.com.
    - Subject: “Mandatory HR Policy Update - Immediate Action Required.”
    - Malicious link: http://hr-policy-update.com/login.
    - 5 users clicked on the link and submitted credentials.
- **Time of Detection:** 11:15

Step 1: Alert Review and Initial Assessment

1. Review Alert Details

- **Description:**
    - A phishing email designed to impersonate HR communications has been sent to multiple employees.
    - Link leads to a phishing site mimicking the company’s single sign-on (SSO) login page.

2. Context Analysis

- **Potential Impact:**
    - Compromise of corporate accounts, leading to unauthorised access to sensitive systems or data.
    - Lateral movement within the corporate environment using harvested credentials.

3. Verify Business Relevance

- **Action Taken:**
    - Confirm the email domain company-hr-secure.com is not legitimate.
    - **Finding:** The domain is newly registered and unrelated to the organisation.

Step 2: Initial Containment Actions

1. Escalate Incident

- Notify SOC Manager, IT Security Team and HR.

2. Contain the Threat

- **Immediate Actions Taken:**
  - Block the sender's email domain (company-hr-secure.com) via the email security gateway.
  - Add the malicious link (http://hr-policy-update.com/login) to the organisation's URL blocklist in the web proxy and DNS firewall.
  - Identify and temporarily suspend accounts of the 5 users who submitted credentials.

Step 3: Advanced Analysis and Investigation

1. Analyse Email Metadata

- **Headers Review:**
  - Sender IP: 203.0.113.45 (linked to known phishing campaigns).
  - SPF, DKIM and DMARC records: All fail, confirming spoofed domain.

2. Analyse SIEM Logs

- **Findings:**
  - Logs confirm 50 recipients received the phishing email.
  - 5 users accessed the phishing site and submitted credentials between 11:05 and 11:10.

3. Threat Intelligence Correlation

- **Malicious Domain:**
  - Query in threat intelligence tools confirms hr-policy-update.com is associated with known phishing activity.

4. Assess Impact and Scope

- **Compromised Accounts:**
  - Credentials of 5 employees are likely harvested.
  - No evidence of unauthorised activity using those accounts yet.

Step 4: Mitigation and Recovery

1. Secure Compromised Accounts

- Force password reset for the affected accounts.

2. Enhance Email Security

- Configure stricter email security filters to identify similar phishing patterns.
- Conduct a retrospective search to ensure no additional malicious emails from the domain were received.

3. Educate Employees

- Send an immediate alert to all employees warning them about the phishing campaign.
- Remind them not to click links or share credentials from unsolicited emails.

4. Monitor for Further Activity

- Set up advanced monitoring for the compromised accounts to detect potential unauthorised access.
- Monitor for failed login attempts indicating brute force activity.

Step 5: Documentation and Post-Incident Actions

Incident Summary

- **Type:** Social Engineering (Spear Phishing).
- **Attack Vector:** Phishing email impersonating HR communications.
- **Target:** Employees across multiple departments.

Indicators of Compromise (IoCs):

- Malicious email domain: company-hr-secure.com.
- Malicious URL: http://hr-policy-update.com/login.
- Sender IP: 203.0.113.45.

Actions Taken:

1. Blocked phishing domain and sender.
2. Disabled compromised accounts and reset their credentials.
3. Alerted employees and conducted awareness training.