INCIDENCE REPORT FOR KTDA

Prepared by: Loyd Kinoti

Date: 15/09/2024

Contact Information: loyd5kinoti@gmail.com

TABLE OF CONTENT

1. Incidence Response.

This report details the incident response process for a simulated phishing and ransomware attack. It outlines the detection, containment, eradication, and recovery phases, with a focus on the effectiveness of actions taken. Forensic analysis was conducted to identify the root cause, and post-incident lessons were documented to enhance future responses. Finally, the report provides recommendations for improving incident response capabilities based on the findings.

2. Incident Overview

Incident Overview:

Type of Attack: Phishing Attack Leading to Ransomware Deployment

Threat Actor: Organized cybercriminal group targeting financial data.

Entry Point: A targeted spear-phishing email sent to a KTDA finance department employee.

Incident Timeline:

Day 1:

10:00 AM: John receives the phishing email and opens the attachment.

10:05 AM: The macro executes, initiating the ransomware deployment process.

11:30 AM: Critical financial documents are encrypted, and the ransomware begins spreading across shared drives.

Day 2:

08:00 AM: IT department notices unusual activity and begins investigating.

10:00 AM: The ransomware has encrypted a significant portion of the internal systems, and employees report being locked out of key applications.

12:00 PM: A ransom note appears on all affected machines, demanding payment.

Day 3:

08:00 AM: The company's operations are severely disrupted, and KTDA's leadership convenes an emergency meeting to discuss the ransom demand and potential recovery strategies.

- Incident Type: Phishing Attack leading to Ransomware Infection

- Date of Incident: 12/09/2024

- Detection Time: 13/09/2024

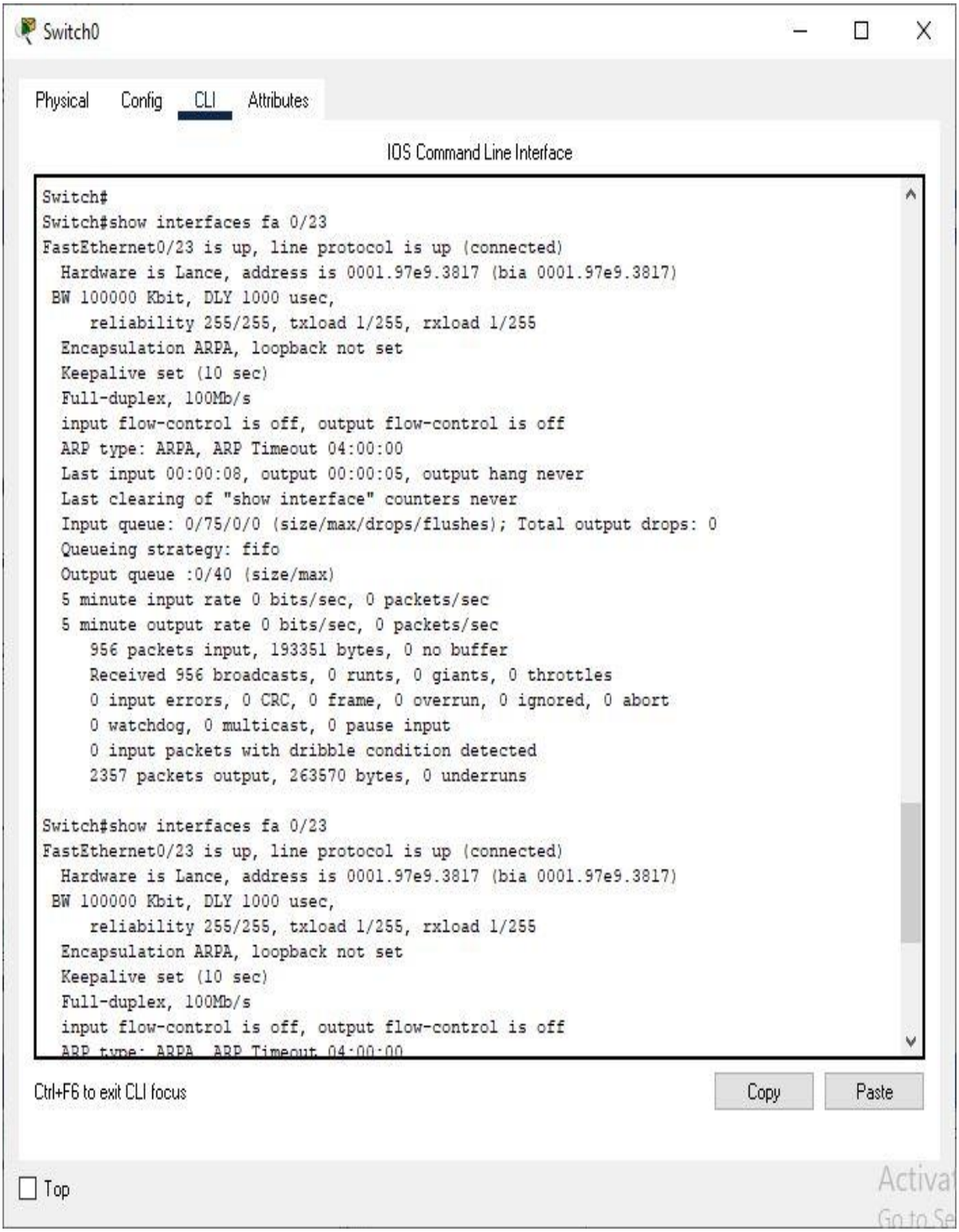
- Affected Systems: Router and Switch Interfaces (e.g., fa0/23)

Impact:

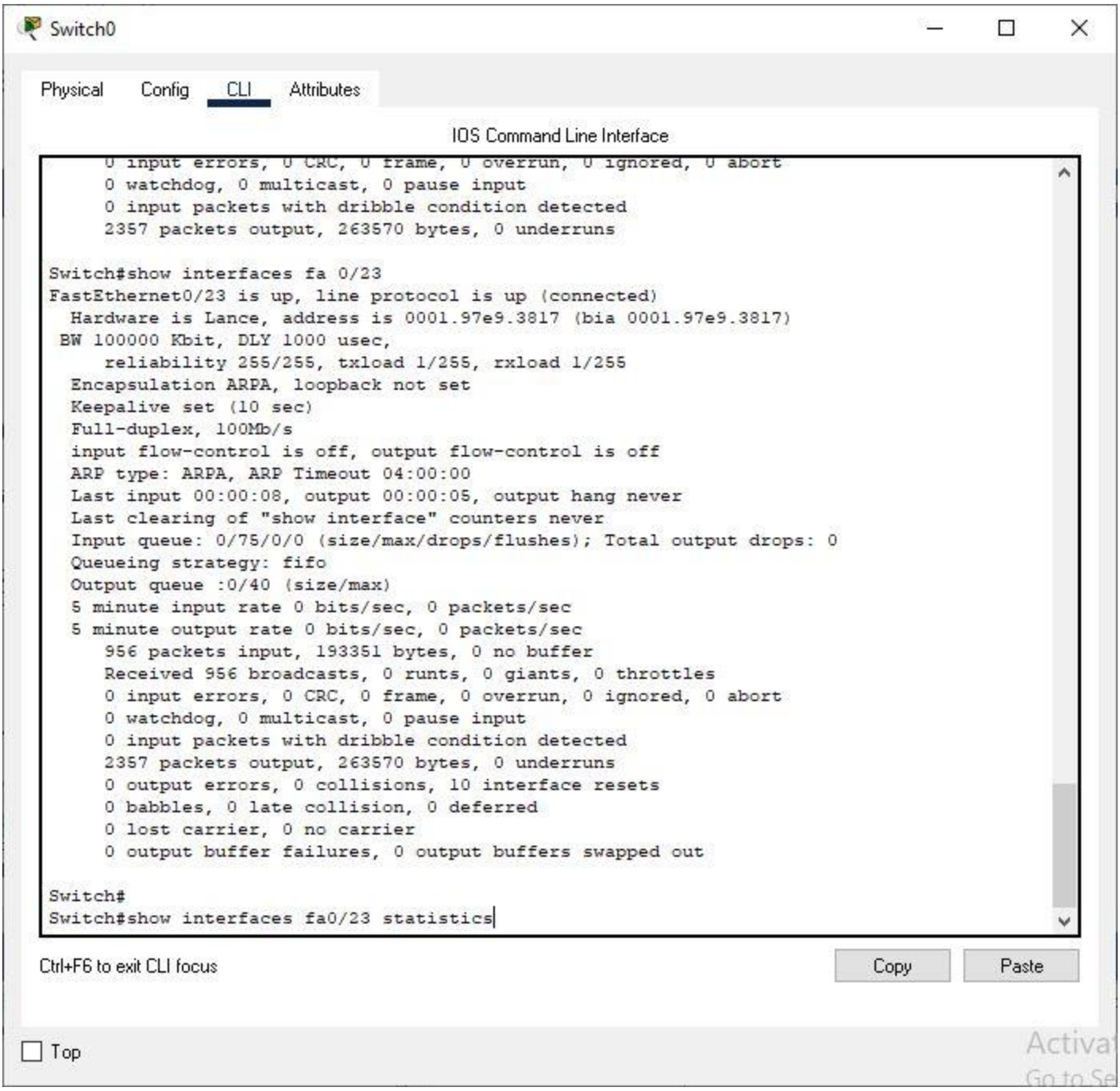
- Compromised network infrastructure
- Encrypted files on key systems
- Potential exposure of sensitive data

3. Incident Response Process

a) Detection



b)



- **Trigger**: The incident was detected through monitoring logs from the router and switch interfaces showing unusual activity, with ARP tables displaying anomalous entries and compromised interfaces showing high traffic with no legitimate source.

- **Detection Tools**: I stimulated Packet Tracer to simulate network scenarios and run tests similar to those conducted with tools like TheHive for incident response and GRR Rapid Response for live remote forensics.

c) Containment and Mitigation

Containment Actions:

- Immediate Isolation: Affected systems (fa0/23 switch interfaces) were isolated from the network to prevent further spread of the ransomware.

- Network Segmentation: Network traffic between affected segments was blocked.

- Account Locking: User accounts showing unusual activity were disabled, and password resets were initiated.

Mitigation Actions:

- Updated antivirus and endpoint protection software across systems.

- Applied system patches to vulnerable machines identified in the incident.

- Backup files were secured, ensuring data recovery post-incident.

d) Eradication

Root Cause Eradication:

- Ransomware infection was traced to the phishing email that bypassed spam filters. The infected systems were cleaned using advanced malware removal tools.

- Persistent malware traces were eradicated from the network infrastructure (routers and switches), and network configurations were reset to a clean state.

e) Recovery

- Data Restoration: Systems were restored from clean backups, and encrypted files were replaced.

- Verification: Affected systems were scanned thoroughly to confirm that no malicious activity remained.

- System Hardening: Additional security layers were applied to endpoints and the network to prevent re-infection.

4. Forensic Analysis

a) Evidence Gathering

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
dhcp-server>
dhcp-server>
dhcp-server>
dhcp-server>
dhcp-server>
dhcp-server>
dhcp-server>en
dhcp-server#
dhcp-server#
dhcp-server#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             -   00E0.8F5E.A302  ARPA   GigabitEthernet0/1
Internet  192.168.1.3            23   0009.7C32.9B89  ARPA   GigabitEthernet0/1
Internet  192.168.2.1             -   00E0.8F5E.A301  ARPA   GigabitEthernet0/0
Internet  192.168.2.2            34   0001.9736.A201  ARPA   GigabitEthernet0/0
dhcp-server#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:15, GigabitEthernet0/0

dhcp-server#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Key Logs Reviewed:

- ARP tables from routers and switches showing rogue IP addresses and hardware bindings.

- Switch interface logs (fa0/23) revealing abnormal packet flow and unauthorized traffic patterns.

Forensic Analysis Tools:

- Memory dumps and disk imaging tools were used to capture snapshots of compromised systems.

- Network traffic analysis to trace the source and spread of ransomware.

b) Root Cause Analysis

- Phishing Email: The incident began with a phishing email that tricked a user into downloading a malicious attachment.

- Ransomware Spread: The malware encrypted files and attempted to propagate via the network, exploiting vulnerabilities in network segmentation and outdated endpoint security measures.

5. Post-Incident Assessment

a) Effectiveness of Response

- Detection: The phishing attack was detected within a reasonable time frame, but some delay in identifying lateral movement was observed. Alerts were accurate, but improving timeliness could have prevented broader infection.

- Containment: Systems were isolated effectively, but initial containment took longer than expected due to gaps in automated network segmentation.

- Eradication: The eradication process was thorough, but updating outdated security configurations prior to the incident would have reduced the infection spread.

- Communication: Internal communication was mostly effective. However, more structured communication protocols are needed for crisis situations to streamline incident updates and decision-making.

- Recovery: The recovery process was smooth, with systems restored from clean backups and network services fully operational within the expected recovery time.

b) Areas for Improvement

- Phishing Defenses:

- Enhance email filtering systems to better detect and block phishing emails.

- Regularly train employees with simulated phishing tests to raise awareness and reduce the risk of social engineering attacks.

Network Segmentation:

- Implement stricter segmentation policies to limit the spread of malware between network segments.

- Deploy more granular access control lists (ACLs) on critical interfaces.

Incident Response Playbook:

- Update the incident response playbook to address gaps in containment processes. Introduce more detailed steps for ransomware incidents, focusing on faster containment.

Backup and Recovery:

- Regularly test the backup and restoration process to ensure minimal data loss during future incidents.

- Keep backup systems offline or on separate, secured networks to prevent ransomware from encrypting backup files.

6. Final Recommendations

a) Enhance Detection and Monitoring

- Implement more advanced Intrusion Detection/Prevention Systems (IDS/IPS) and ensure they are properly configured to detect phishing attempts and ransomware activity earlier.

- Increase log retention to capture more historical data for effective forensic analysis.

b) Strengthen Endpoint and Network Security

- Deploy stronger endpoint detection and response (EDR) solutions on all endpoints to improve malware detection and isolation.

- Apply frequent updates and patches to all systems, especially critical infrastructure such as routers and switches.

- Implement zero-trust security architecture to reduce the lateral movement of malware.

c) Improve Incident Response Training

- Conduct regular incident response drills simulating ransomware and phishing attacks to improve the team's readiness.

- Assign specific roles in the incident response team and ensure each team member is clear on their responsibilities during a real incident.

d) Optimize Communication and Collaboration

- Establish a communication plan for crises, ensuring all relevant stakeholders (internal and external) are informed quickly.

- Set up a centralized dashboard for tracking and managing security incidents in real time.

7. Conclusion

The incident highlighted both the strengths and weaknesses in the organization's incident response process. While the containment, eradication, and recovery phases were successful, there were areas that need improvement, especially in detection speed and phishing defense. By implementing the recommendations outlined in this report, the organization can enhance its security posture and improve its ability to respond to future incidents.