Fileless Malware Incident Response Plan

1. Purpose

The purpose of this incident response plan is to provide structured guidelines for identifying, managing, and mitigating fileless malware attacks within Ain shams university.

- **What is fileless attack? →**A fileless attack is a type of cyberattack that does not rely on traditional malware files to compromise a system. Instead, it leverages legitimate software, processes, or built-in tools already present on a victim's computer, making detection more difficult for traditional antivirus software.

2. Scope

This plan covers all IT infrastructure, networks, and endpoints vulnerable to fileless malware attacks. It also applies to all employees, contractors, and third-party service providers involved with IT systems.

3. Roles and Responsibilities

Incident Response Team (IRT):

- **Incident Manager:** Oversees the entire response process, ensures resources are allocated, and maintains communication with stakeholders.

- **Security Operations Center (SOC) Analyst**: Responsible for incident detection, monitoring security alerts, and escalating identified threats.

- **Threat Intelligence Officer**: Gathers threat intelligence, tracks emerging threats, and provides context for ongoing incidents.

- **Forensic Examiner**: Conducts in-depth forensic investigations, analyzes compromised systems, and extracts Indicators of Compromise (IoCs).
- **Incident Handler**: Leads incident response efforts, coordinates team actions, and communicates with stakeholders throughout the incident lifecycle.
- **IT Manager:** Implements technical changes, including isolating and restoring systems.
- **Communications Lead:** Manages internal and external communication, including disclosures to regulatory bodies and customers.
- **Legal Advisor:** Provides guidance on compliance and regulatory reporting.
- **PR Specialist:** Handles public-facing communication to protect the company's reputation.

4. Incident Response Process

4.1. Preparation

Training and Exercises:

Conduct quarterly training, tabletop exercises, and penetration testing.

Cybersecurity Tools:

- Endpoint Detection and Response (EDR) with memory and behavioral analysis.
- Security Information and Event Management (SIEM) with predefined fileless malware rules.
- Network Traffic Analyzers for detecting unusual outbound traffic.
- Regular threat intelligence updates.

System Hardening:

- Enable PowerShell Constrained Language Mode.
- Disable unnecessary administrative tools like Windows Management Instrumentation (WMI) and scripting capabilities.
- Apply least privilege principles to minimize risk.

Communication Protocols:

- Establish clear escalation paths and contact points within the IRT.

Tools to Monitor Common Fileless Malware Tools:

Powershell.exe: Commonly abused for malicious script execution.

Certutil.exe: Used for downloading malicious payloads.

Wmic.exe: Exploited for system reconnaissance.

Mshta.exe: Often used to execute malicious JavaScript or VBScript.

Regsvr32.exe: Abused to execute scripts or load DLLs from remote locations.

Additional Obfuscation Techniques:

Fileless malware often uses encoded scripts, encrypted payloads, or disguised commands to evade detection. For instance, attackers may:

- Use Base64 encoding in PowerShell commands.
- Utilize built-in Windows utilities to bypass traditional defenses.
- Obfuscate payloads with tools like `Invoke-Obfuscation` or `Packers` to hinder analysis.

4.2. Identification

Indicators of Compromise (IoCs):

- Unexpected memory usage spikes.
- Unauthorized PowerShell/script execution.
- Suspicious registry modifications or scheduled tasks.
- Anomalies in process creation (e.g., powershell.exe spawning unexpected processes).
- Unusual outbound traffic to unfamiliar domains or IP addresses.

Detection Tools:

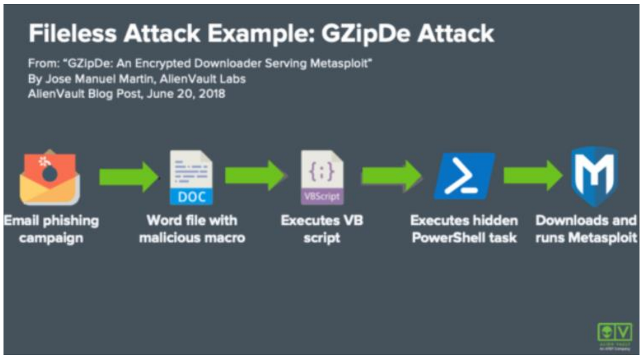
EDR: Identifies behavioral patterns, suspicious scripts, or memory anomalies.

SIEM: Correlates logs to generate alerts for fileless malware activity.

Network Traffic Analyzers: Detect data exfiltration or C2 (Command and Control) communication.

Threat Intelligence Feeds: Provide IoC updates for emerging threats.

Visual Example:



Fileless Attack Example: GZipDe Attack

From: "GZipDe: An Encrypted Downloader Serving Metasploit"
By Jose Manuel Martin, AlienVault Labs
AlienVault Blog Post, June 20, 2018

Email phishing campaign → Word file with malicious macro → Executes VB script → Executes hidden PowerShell task → Downloads and runs Metasploit

Explanation: The lifecycle shows stages such as **Initial Access, Execution, Persistence, and Exfiltration**. Attackers exploit built-in tools like powershell.exe during these phases.

4.3. Containment

- Isolate infected systems using network segmentation or endpoint quarantine tools.

- Disable compromised user accounts or credentials.

- Block malicious IP addresses and domains through firewalls and IDS/IPS.

- Notify business unit leaders if containment impacts critical services.

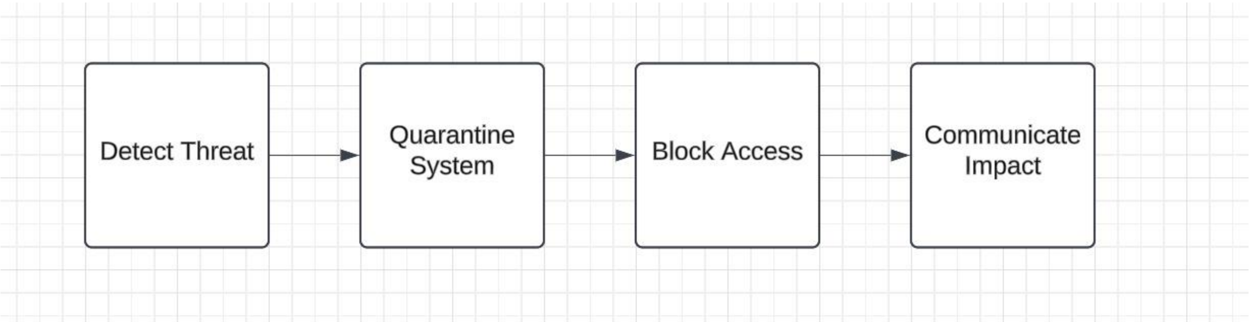
Tools for Immediate Containment:

- Use EDR to suspend processes like powershell.exe or certutil.exe.

- Block domains and URLs linked to suspicious C2 activity.

- Implement SIEM rules to flag and block obfuscated commands or encoded scripts.

Flowchart Example:



4.4. Eradication

Steps to Remove Threat:

1. Terminate Malicious Processes:

- Use EDR to halt processes like powershell.exe, wmic.exe, certutil.exe, mshta.exe, or regsvr32.exe if used maliciously.

2. Remove Persistence Mechanisms:

- Delete unauthorized registry keys or scheduled tasks.
- Remove scripts or executables dropped in temporary directories.

3. Reset Credentials:

- Revoke compromised user accounts and enforce password resets.

4. Apply Security Updates:

- Address vulnerabilities exploited by the attack.

5. Vulnerability Assessment:

- Conduct scans to ensure no additional threats remain.

4.5. Recovery

Steps to Restore Operations:

1. Reinstall Operating Systems:

- Perform clean OS installations on compromised systems if necessary.

2. Restore Data:

- Recover files from verified, malware-free backups.

3. Monitor Restored Systems:

- Use EDR and SIEM tools to monitor for residual activity or reinfection.

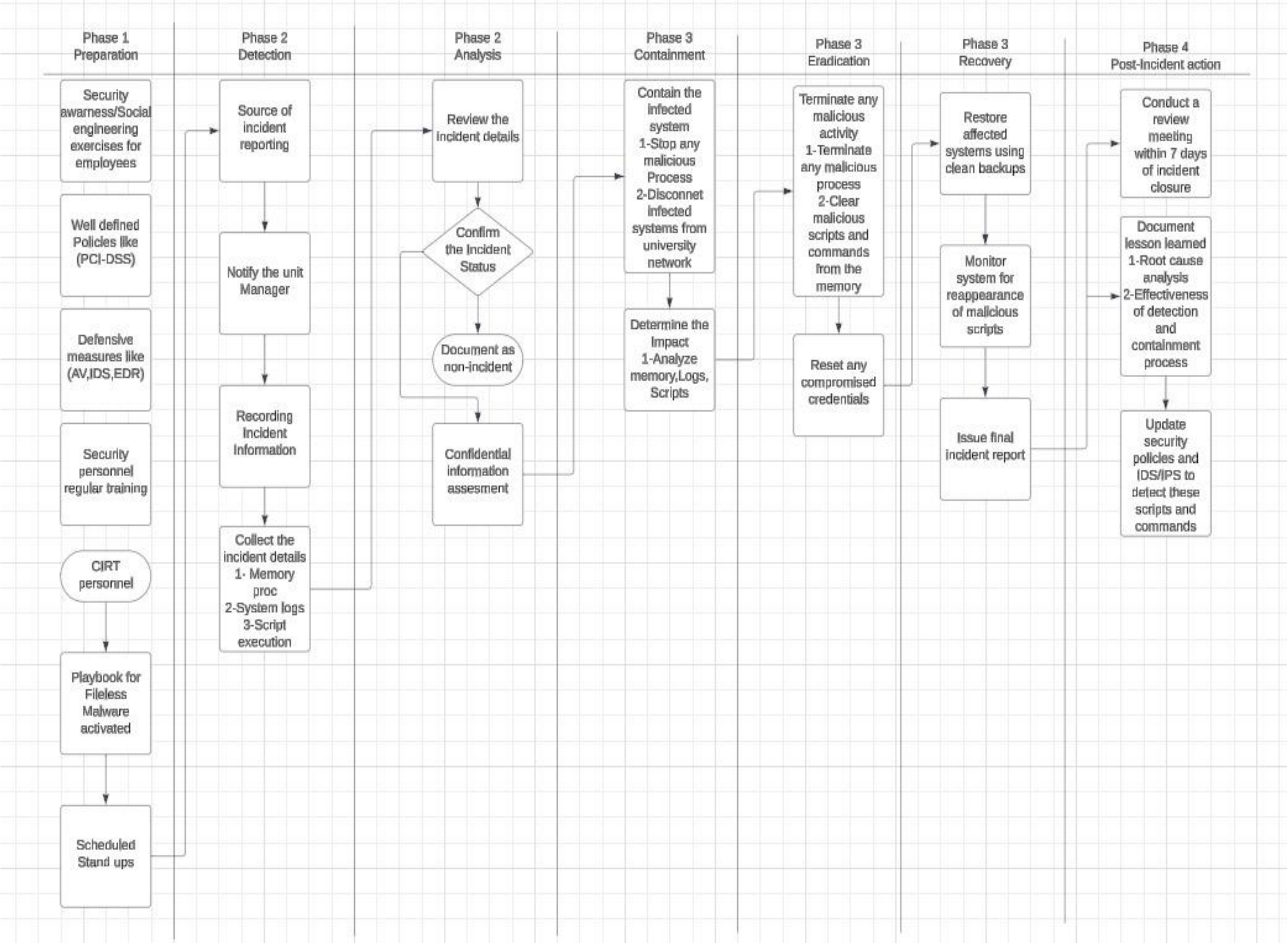
4. Verification:

- Confirm systems are clean before reconnecting them to the network.

4.6. Post-Incident Review

- Conduct a review meeting within seven days of incident closure.
- Document lessons learned, focusing on:
  - Root cause analysis.
  - Detection and containment process effectiveness.
  - Detection gaps or weaknesses in policies.
- Update security policies and incident response procedures.
- Organize additional training sessions based on findings.

Refer to the flowchart below for a summarized visualization of the entire incident response process, including Preparation, Detection, Analysis, Containment, Eradication, Recovery, and Post-Incident Review.


Phase 1
Preparation
Security awarness/Social engineering exercises for employees
Well defined Policies like (PCI-DSS)
Defensive measures like (AV,IDS,EDR)
Security personnel regular training
CIRT personnel
Playbook for Fileless Malware activated
Scheduled Stand ups
Phase 2
Detection
Source of incident reporting
Notify the unit Manager
Recording Incident Information
Collect the incident details 1- Memory proc 2-System logs 3-Script execution
Phase 2
Analysis
Review the incident details
Confirm the Incident Status
Document as non-incident
Confidential information assesment
Phase 3
Containment
Contain the infected system 1-Stop any malicious Process 2-Disconnet infected systems from university network
Determine the Impact 1-Analyze memory,Logs, Scripts
Phase 3
Eradication
Terminate any malicious activity 1-Terminate any malicious process 2-Clear malicious scripts and commands from the memory
Reset any compromised credentials
Phase 3
Recovery
Restore affected systems using clean backups
Monitor system for reappearance of malicious scripts
Issue final incident report
Phase 4
Post-Incident action
Conduct a review meeting within 7 days of incident closure
Document lesson learned 1-Root cause analysis 2-Effectiveness of detection and containment process
Update security policies and IDS/IPS to detect these scripts and commands

5. Communication Plan

Internal Communication:

- Notify executives, affected teams, and the board.
- Provide regular updates during the response process.

External Communication:

Regulatory Compliance:

- Engage legal counsel for guidance on ISO27001, PCI-DSS, or other applicable regulations.

Public Disclosures:

- Work with the PR team to manage external messaging and protect reputation.

6. Metrics and Reporting

Key Metrics:

Dwell Time : The length of time that threat actors have access to a network before they are detected, and their access is stopped

Incident Detection Time (MTTD): Time from attack initiation to detection.

Containment Duration (MTTC): Time from detection to containment.

Total Recovery Time (MTTR): Time from containment to full recovery.

Number of Affected Systems: Count of infected or quarantined systems.

Incident Costs: Estimated financial impact, including system downtime and data loss.

7. Review and Maintenance

- **Annual Review:**

  - Review the plan annually or after significant incidents.

- **Updates:**
  - Update tools, procedures, and training programs regularly.

- **Testing:**
  - Conduct quarterly threat simulations and incident response drills to assess readiness.

8. Appendices

Contact Directory:

1- CSIRT contacts

Role	Name	Phone	Email
Incident handler (lead)	Abdelrahman Khaled	[redacted]	AK@ainshams.com
Incident handler (backup)	Ziad Mahmoud	[redacted]	ZM@ainshams.com
Note-taker	Abdelrahman Sohsah	[redacted]	AS@ainshams.com
Communications	Nour Amr	[redacted]	NA@ainshams.com
Network	Salma Abdelmonem	[redacted]	SA@ainshams.com
Legal	Moamen Mahmoud	[redacted]	MM@ainshams.com

2-ISP contacts

Role	Name	Phone	Email
Help desk	Ahmed khaled	[redacted]	AK@ISP.com

Incident Details Summary Template:

- Incident type
- Timeline
- Affected systems
- Resolution steps
- Follow-up actions

Security Tools Reference Guide:

- List of tools (EDR, SIEM, traffic analyzers) with configuration and version details.

Learning from Real-World Incidents

To enhance our incident response capabilities against fileless attacks, we recognize the importance of studying real-world incidents. These cases provide valuable insights into attack methods, detection challenges, and effective response strategies.

For example, the following incidents demonstrate various aspects of fileless attack execution:

- **Equifax Data Breach (2017):** Showcases how exploitation of vulnerabilities can lead to large-scale data breaches through fileless methods.
- **Operation Cobalt Kitty (2017):** Demonstrates advanced persistent threat (APT) tactics using legitimate system processes.
- **FIN7 Cybercrime Campaign:** Highlights how financial data theft can be executed using PowerShell scripts.
- **DarkHotel APT:** Explores targeted attacks on executives through in-memory payloads.
- **Sodinokibi (REvil) Ransomware Attacks:** Shows how attackers leverage remote access and malicious scripts for ransomware deployment.
- **APT29 (Cozy Bear) SolarWinds Attack:** Demonstrates supply chain compromise using fileless techniques for stealthy lateral movement.

Date: [12/16/2024]

References:

https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

https://www.sans.org/white-papers/33901/

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

https://www.cybereason.com/blog/operation-cobalt-kitty-apt

https://www.forbes.com/councils/forbestechcouncil/2020/05/04/defending-against-the-new-reality-of-fileless-malware-attacks/

https://www.trendmicro.com/en_us/research/21/d/carbanak-and-fin7-attack-techniques.html

https://www.zscaler.com/blogs/security-research/new-darkhotel-apt-attack-chain-identified

https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack

https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know