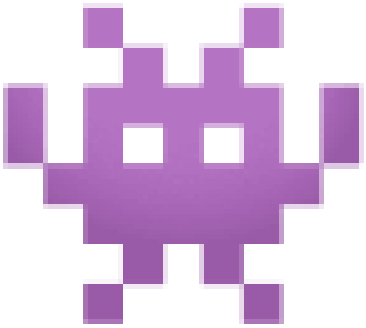

Malware Infection Playbook

1. Identify and contain the malware

Quickly detect, isolate, and limit the spread of malware to minimize damage while performing a **thorough but cautious analysis** in a controlled environment..

1.1 Identify and observe infected systems

Infected systems should not remain online on the production network. Instead, isolate them immediately to prevent lateral movement or additional compromise, while keeping them powered on (if needed) to preserve volatile evidence.

1.2 Conduct preliminary analysis

Gather initial indicators of compromise (IOCs) such as suspicious files, processes, registry changes, or outbound connections to inform containment and eradication strategies.

2. Perform static analysis of the malware sample

Analyze the malware file without executing it to understand its characteristics.

2.1 Inspect file structure and metadata

Examine the malware file's properties, including size, hash values, and embedded metadata.

2.2 Extract embedded strings and suspicious code

Use tools like Strings, VirusTotal, or PEStudio to identify readable text, URLs, or code fragments that provide insight into the malware's intent and behavior.

3. Perform dynamic analysis in a controlled environment

Never run malware on a production system — it must be executed in a sandbox or isolated virtual lab.

This is critical to prevent unintentional spread or damage

3.1 Execute malware on a clean system

Run the malware in a controlled virtual lab or sandbox, not in production, to safely observe its behavior and capture forensic data.

3.2 Record system modifications and activities

Document all system changes, including registry edits, file creation/deletion, process launches, and network connections made during execution.

4. Conduct network traffic analysis

Analyze communication attempts made by the malware to uncover external connections.

4.1 Capture network traffic

Use packet-capturing tools to monitor network activity generated by the malware.

4.2 Identify external entities

Look for connections to command-and-control (C2) servers or data exfiltration endpoints.

5. Investigate behavioral patterns and persistence mechanisms

Determine how the malware survives and operates over time.

5.1 Identify persistence techniques

Investigate changes such as registry modifications, scheduled tasks, or startup files.

5.2 Examine behavioral indicators

Look for recurring patterns, such as periodic network requests or file executions.

6. Eradicate the malware and recover systems

Remove the malware and restore affected systems to their original state.

6.1 Deploy cleanup tools

Use antivirus or specialized malware removal tools to eradicate infections.

6.2 Restore from clean backups

Reinstall or rebuild affected systems and data using backups confirmed to be malware-free.

6.3 Apply mitigations to prevent reinfection

Address any vulnerabilities that permitted the original infection to occur by applying the appropriate mitigation.

7. Post-incident reporting and prevention

Document lessons learned and strengthen defenses against future incidents.

7.1 Generate incident report

Detailed findings, response steps, and impact assessment in a comprehensive report.

7.2 Implement prevention measures

Update security policies, patch vulnerabilities, and educate staff to avoid recurrence.