Exported from Obsidian – Formatting retained for Obsidian Compatibility

###Malware Analysis Checklist###

\*\*1. Identification & Confirmation\*\*

- \*\*File Analysis:\*\* Obtain the file hash, metadata, and digital signatures.

- Device

- User:

- Path:

- SHA1

- SHA256

- MD5

- Virus Total Results:

- Determine file origin and compare against threat intelligence databases.

- Device:

- Quarantine Status:

- \*\*Process Execution Review:\*\*

- Analyze execution logs and system events to trace the malicious process lifecycle.

- File Executed on Disk:

- Process Execution Tree:

- Identify any network connections, registry modifications, or system changes.

- HTTP/TLS/SSH/RDP Connections:

- \*\*Preserve Evidence:\*\* Secure memory dumps, disk images, and audit logs.

\*\*2. Containment\*\*

- \*\*Isolate Affected Systems or Users:\*\* Disconnect impacted devices from the network if necessary.

- Device Isolation / Notification Sent:

- DLP Restrictions Increased:

- User Account Password Reset:

- Sessions Revoked:

- \*\*Stop Malicious Processes:\*\* Terminate the malicious process(s) and block further execution.

- Stop and Quarantine File:

- Download Safe/Zip File:

- Sandbox File:

\*\*3. Eradication\*\*

- \*\*Remove Malicious Artifacts:\*\* Delete the file and any related scripts or payloads.

- \*\*Patch & Reconfigure:\*\* Update system patches, close exploited vulnerabilities, and rotate compromised credentials.

- \*\*Verify Forensic Cleanup:\*\* Ensure no remnants of the malicious file remain across the network.

\*\*4. Recovery\*\*

- \*\*Restore Systems:\*\* Reintegrate cleaned systems back into the network with enhanced monitoring.

- Follow Up AV and/or Vulnerability Scans:

- \*\*Monitor for Re-Infection:\*\* Increase logging and continuous threat detection on the affected endpoints.