INCIDENT RESPONSE USE CASE

AI-Spawned Malware Controller on Enterprise Endpoint

An incident response use case showing how REMI turns enterprise IT event logs and source records into a cyber SITREP with confirmed findings, unresolved questions, and immediate next steps.

At 8:16 AM, the security operations analyst at Metro Health Administration noticed that an endpoint alert did not match a normal malware pattern. The workstation was online, but the pattern was wrong: generated scripts appeared in a user profile, a child process launched from a temporary directory, and outbound traffic repeated in short bursts to an external IP.

The analyst reported it to the incident response lead, who reviewed EDR telemetry and found **C:\Users\Public\svc-runner.exe** launched from **FIN-WS-09** at **3:28 AM**. The process created scripts under **C:\ProgramData\cache**, spawned **tasklink.exe**, accessed cached browser tokens, and connected to **203.0.113.73**. Firewall records then showed internal traffic from **10.72.44.18** toward **APP-SRV-03** and **FILE-FIN-02**.

That changed the concern from an endpoint alert to an AI-spawned malware controller with movement into application and file-server systems. The warning signs were connected behaviors: generated script creation, controller process activity, token access, outbound callback traffic, internal network movement, and file-server access outside the expected user activity window.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **Metro Health Administration**. The investigator speaks with the security operations analyst who noticed the endpoint alert, the incident response lead who reviewed EDR telemetry, the application owner responsible for **APP-SRV-03**, and the file services owner responsible for **FILE-FIN-02**.

After those conversations, the investigator requests copies of the available event logs and source records so they can be analyzed in REMI. The goal is to determine how the malware controller, generated scripts, endpoint activity, token access, callback traffic, application server traffic, and file-server access fit together as a cyber attack path. The more complete the log package is, the wider the investigative coverage becomes.

Event Logs to Request

- **EDR and endpoint telemetry** showing process launches, parent-child process chains, generated scripts, file creation, token access, and persistence indicators.
- **PowerShell, command, and Windows event logs** showing script execution, encoded commands, scheduled tasks, service creation, and local account activity.
- **Firewall, proxy, and DNS logs** showing outbound callbacks, internal destinations, blocked traffic, allowed traffic, and domain resolution activity.
- **Identity and token records** showing account use, session timing, browser token activity, MFA events, and privilege changes.
- **Application server logs** showing administrative access, service calls, failed logons, API activity, and timestamps.
- **File-server access logs** showing folder enumeration, reads, exports, writes, and timestamps.
- **Help desk tickets, change records, asset ownership, and support schedules** showing whether the activity matched authorized work.

REMI Flagged

- **Malware controller execution** involving **C:\Users\Public\svc-runner.exe** on **FIN-WS-09**.
- **Generated script creation** under **C:\ProgramData\cache** during the same overnight window.
- **Child process activity** involving **tasklink.exe** after the controller launched.
- **Cached token access** from the same workstation session.
- **Outbound callback** from **10.72.44.18** to **203.0.113.73**.
- **Internal movement** toward **APP-SRV-03** and **FILE-FIN-02**.
- **Shared evidence links** across workstation, file path, process chain, token access, source IP, destination IP, application logs, and file-server records.

Correlation and SITREP Output

The raw logs are imported into REMI for analysis. REMI identifies the flagged behaviors inside the evidence package, then correlates records that share the same workstation, file path, process chain, token event, source IP, callback destination, application server event, file-server record, and timestamp.

REMI Correlated

- **Controller file and endpoint** linked through **FIN-WS-09**, **C:\Users\Public\svc-runner.exe**, and EDR process history.
- **Generated scripts and child process activity** linked through **C:\ProgramData\cache**, **tasklink.exe**, PowerShell logs, and file creation records.
- **Token access and outbound callback** linked through browser token events, **10.72.44.18**, and **203.0.113.73**.
- **Endpoint activity and internal destinations** linked to **APP-SRV-03** and **FILE-FIN-02** through firewall and server logs.
- **Shared evidence path** connecting workstation, malware file, generated scripts, process chain, token access, callback traffic, application activity, and file-server records.

SITREP Output Includes

- **Confirmed findings** showing what the evidence proves.
- **Unresolved questions** showing what still needs confirmation.
- **Additional source data needed** to close specific answer gaps.
- **Questions to ask IT, security, cloud, identity, vendors, and system owners.**
- **Artifacts to preserve or sandbox** before cleanup.
- **Malware paths, generated scripts, services, or scheduled tasks to remove** after preservation.
- **Verification steps** to confirm the activity does not return.

How REMI Reconstructs It

The following simulated incident response excerpt shows the level of case-specific detail REMI can produce inside a SITREP. Names, accounts, IP addresses, systems, files, and records are examples, but the structure reflects the level of detail REMI is designed to generate from the evidence package.

AI-Spawned Malware Controller on Enterprise Endpoint

REMI confirmed that **FIN-WS-09** launched **C:\Users\Public\svc-runner.exe** at **3:28 AM**. The process created generated scripts under **C:\ProgramData\cache**, spawned **tasklink.exe**, accessed cached browser tokens, and established outbound traffic from **10.72.44.18** to **203.0.113.73**.

REMI correlated the **controller file**, **generated scripts**, **child process chain**, **token access**, **callback destination**, **application server traffic**, and **file-server access** into one evidence path. The activity occurred during the same overnight window in which user activity records showed access outside the expected work pattern.

The SITREP identified confirmed findings, including the **malware controller**, **generated script directory**, **child process**, **token access**, **source workstation**, **callback IP**, **application server traffic**, and **file-server access**. It also identified unresolved questions: which account launched the controller, whether the controller was staged by a prior remote session, whether tokens were reused on other systems, and whether files were exported from **FILE-FIN-02**.

REMI generated immediate next steps: preserve EDR telemetry, PowerShell logs, firewall flows, proxy logs, DNS records, token records, application logs, file-server audit logs, and a forensic copy of **svc-runner.exe**; sandbox the controller and generated scripts; isolate **FIN-WS-09** after preservation; remove unauthorized scripts, scheduled tasks, and services; and verify that outbound traffic and server access return to expected behavior.