Incident Response Lifecycle

Simulated Corporate Network

IronGrid Security | Period covered: April 2023 to June 2023

Prepared by Mahdi Ghaznawy

Scenario overview

On July 14, 2025 an endpoint in the lab network began encrypting user profile directories. Wazuh telemetry flagged unusual file rename patterns and Splunk correlation detected ransom note creation. The incident was handled in a controlled environment to demonstrate full lifecycle response.

Assets involved

Asset	Role	IP	OS
DC-LAB-01	Active Directory domain controller	10.10.10.10	Windows Server 2019
WIN10-LAB-07	Affected endpoint	10.10.20.57	Windows 10 Enterprise
EDR-LAB	Telemetry aggregator	10.10.30.5	Ubuntu 22.04
NAS-LAB-01	File share target	10.10.40.12	TrueNAS Core

Lifecycle phases

Preparation

- Playbooks defined for containment and eradication. Gold images stored on NAS-LAB-01.
- EDR isolate capability validated on all Windows endpoints. Backups verified weekly.

Identification

- Splunk alert reported a ransom note pattern on WIN10-LAB-07.
- Wazuh alerted on high volume file writes with a .locked extension.
- Observed sample hash 4f2a9d1b7b0a7f0f69d9db44d38a6a21 for the dropper used in the lab.

Containment

- EDR isolation of WIN10-LAB-07 within 4 minutes of the alert.
- Disabled account lab\a.miller due to anomalous process launches.
- Blocked outbound connections to command and control subnets.

Eradication

- Removed persistence via Run registry keys and a scheduled task.
- Deleted malicious dropper from %ProgramData%.
- Network wide search for indicators using Splunk and OSQuery.

Recovery

- Restored files from the last known good snapshot on NAS-LAB-01.
- Reimaged WIN10-LAB-07 from a gold image and rejoined the domain.
- Monitored for 72 hours with no recurrence.

Lessons learned

- Local admin password reuse enabled lateral movement. Enforced LAPS with unique passwords.
- File share lacked versioning. Enabled snapshots every 2 hours.
- Added detection for shadow copy deletion and suspicious vssadmin usage.

Incident timeline

Time	Event
07:11	Wazuh anomaly on file rename rate
07:12	Splunk ransom note detection triggers
07:15	Incident declared and on call analyst paged
07:16	EDR isolation of WIN10-LAB-07
07:28	Hash triage with no matches in VirusTotal for the sample used in the lab
08:10	Containment verified and scope limited to single host
10:45	Recovery from snapshot completed
Day 3 09:00	Monitoring window concludes and incident closed

MITRE ATT and CK mapping

Tactic	Technique	Evidence
Initial Access	T1566 Phishing	Credential capture in a prior simulation
Execution	T1059 PowerShell	Obfuscated PowerShell script spawned from Outlook

Tactic	Technique	Evidence
Persistence	T1060 Registry Run Keys	HKCU Run entry for updater.exe
Defense Evasion	T1070 Indicator Removal	Cleared Windows event logs using wevtutil
Impact	T1486 Data Encrypted for Impact	Files renamed to .locked and ransom note created

Post incident actions

- Implemented LAPS with 24 hour randomization for local admin accounts.
- Enabled Controlled Folder Access on Windows endpoints in the lab.
- Published a runbook for ransom note detection response steps.
- Scheduled quarterly table top exercises starting September 2025.