Atomic Red Team Cleanup Report

1. Executive Summary

This document records the identification, investigation, and remediation of unintended Atomic Red Team artifacts on a personal Windows laptop. The artifacts were causing abnormal startup behavior, including multiple administrative windows opening automatically. The activity was confirmed to be non-malicious but inappropriate for a personal, non-lab environment. A full sanitization was performed.

---

2. Initial Observation

Symptoms observed: - Two Notepad windows opening automatically - Computer Management console opening automatically - Event Viewer opening automatically - Behavior triggered when the laptop was plugged into AC power

Impact: - Unexpected administrative tools launching at startup/logon - Indication of persistence mechanisms active on the system

---

3. Investigation

3.1 Task Scheduler Analysis

Task Scheduler revealed multiple suspicious scheduled tasks. Key findings:

Task Name	Trigger	Action	Author
T1053_005_WMI	At logon	notepad.exe	AtomicRedTeam
T1053_005_OnStartup	At startup	cmd.exe /c calc.exe	AtomicRedTeam
T1053_005_OnLogon	At logon	cmd.exe /c calc.exe	AtomicRedTeam
EventViewerBypass	At logon	eventvwr.msc	AtomicRedTeam
CompMgmtBypass	At logon	compmgmt.msc	AtomicRedTeam
ATOMIC-T1053.005	Daily	Obfuscated PowerShell (Base64)	AtomicRedTeam
atomic red team	At logon	calc.exe	AtomicRedTeam

Assessment: - Tasks mapped directly to MITRE ATT&CK technique **T1053.005 – Scheduled Task / Job** - Confirmed as Atomic Red Team adversary emulation artifacts - No evidence of real malware payloads

---

4. Root Cause Analysis

The system previously had Atomic Red Team tests executed (likely for training or lab purposes). Cleanup was not performed afterward, leaving persistence mechanisms active on a personal laptop.

Why it triggered on AC power: - Power state changes can trigger logon/startup/WMI-based scheduled tasks - Plugging in AC power caused task execution

---

5. Remediation Actions

5.1 Scheduled Task Removal

- Deleted all tasks containing:
- `Atomic`
- `ATOMIC`
- `T1053`
- `Bypass`

5.2 Registry Cleanup

Executed as Administrator:

```
Remove-Item -Recurse -Force HKCU:\SOFTWARE\ATOMIC* -ErrorAction SilentlyContinue
Remove-Item -Recurse -Force HKLM:\SOFTWARE\ATOMIC* -ErrorAction SilentlyContinue
```

Verified no remaining Atomic-related registry keys.

5.3 File System Cleanup

- Searched for and removed:
- Atomic Red Team directories
- Invoke-AtomicRedTeam scripts
- Residual `.ps1` test files

5.4 Startup & Persistence Review

- Verified empty startup folders:
- `shell:startup`
- `shell:common startup`
- Reviewed registry Run keys
- Checked Windows services for non-standard entries

---

6. System Integrity Validation

6.1 Windows Integrity Checks

Executed:

```
sfc /scannow
DISM /Online /Cleanup-Image /RestoreHealth
```

6.2 Security Scan

- Performed Microsoft Defender Offline Scan
- No malicious findings detected

---

7. Final Status

System State: Clean

- No remaining Atomic Red Team artifacts
- No unauthorized persistence mechanisms detected
- System suitable for personal daily use

---

8. MITRE ATT&CK Mapping

The following table maps the observed Atomic Red Team artifacts to the corresponding MITRE ATT&CK techniques.

ATT&CK ID	Technique Name	Tactic	Evidence on System	Notes
T1053.005	Scheduled Task / Job: Scheduled Task	Persistence, Privilege Escalation	Multiple scheduled tasks (At logon, At startup, Daily)	Primary persistence mechanism used by Atomic Red Team
T1059.001	Command and Scripting Interpreter: PowerShell	Execution	Base64-encoded PowerShell command executed via scheduled task	Simulated obfuscated in-memory execution

ATT&CK ID	Technique Name	Tactic	Evidence on System	Notes
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Execution	cmd.exe /c calc.exe tasks	Demonstrates LOLBin-based execution
T1036.005	Masquerading: Match Legitimate Name or Location	Defense Evasion	eventvwr.msc and compmgmt.msc	Abuses trusted Windows management consoles
T1218	System Binary Proxy Execution	Defense Evasion	MMC snap-in execution	Simulates bypass of application controls
T1112	Modify Registry	Defense Evasion	HKCU\SOFTWARE\ATOMIC-T1053.005	Registry-based payload storage

9. Lessons Learned

- Adversary emulation tools must only be used in isolated lab environments (VMs)
- Post-lab cleanup is critical
- Scheduled Tasks are a high-risk persistence vector and should be routinely reviewed

9. Recommendations

- Use dedicated virtual machines for red team / blue team labs
- Periodically audit Task Scheduler and startup locations
- Maintain regular system backups
- Document lab activity and cleanup steps for future reference

Prepared by: Personal system owner (Cybersecurity-focused remediation)