Monday Monitor

## **Monday Monitor – Endpoint Investigation Report**

### **Scenario Recap**

* Organization: **Swiftspend Finance**
* Goal: Test endpoint monitoring with **Wazuh + Sysmon**
* Timeframe: **Apr 29, 2024 — 12:00:00 to 20:00:00**
* Mission: Identify suspicious process executions, scheduled tasks, credential dumping, and data exfiltration.

### **Findings**

1. **Initial Access**
   * **Method:** Malicious downloaded file.
   * **File Name:**

CopyEdit

SwiftSpend\_Financial\_Expenses.xlsm

1. **Persistence**
   * **Command to Create Scheduled Task:**

pgsql

CopyEdit

"cmd.exe" /c "reg add HKCU\SOFTWARE\ATOMIC-T1053.005 /v test /t REG\_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f & schtasks.exe /Create /F /TN "ATOMIC-T1053.005" /TR "cmd /c start /min \"\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\SOFTWARE\\ATOMIC-T1053.005).test)))" /sc daily /st 12:34"

* + **Scheduled Time:** 12:34
  + **Encoded Payload:**

nginx

CopyEdit

ping www.youarevulnerable.thm

1. **Privilege Escalation / New Account**
   * **Password for New User:**

nginx

CopyEdit

I\_AM\_M0NIT0R1NG

1. **Credential Access**
   * **Credential Dump Tool:**

CopyEdit

memotech.exe

1. **Data Exfiltration**
   * **Flag Extracted:**

bash

CopyEdit

THM{M0N1T0R\_1$\_1N\_3FF3CT}

### **Recommendations**

* Block execution of macros from untrusted Excel files.
* Monitor registry key modifications related to persistence (HKCU\SOFTWARE\...).
* Detect and alert on suspicious scheduled task creations.
* Monitor for unauthorized account creation and password setting.
* Add detection rules for known credential dumping tools (like memotech.exe).
* Inspect outbound DNS/ICMP traffic for data exfiltration attempts.

