

# ATHANASIUS J.K GADOSEY

## Week 6

### Practical Task: Finding Persistence

#### 1. Process Analysis

##### Suspicious process:

- *powershell.exe* (PID 1720)

##### Parent process:

- *chrom.exe* (PID 1652)

##### What likely happened:

Powershell which was launched by Chrome strongly suggests that the user clicked a malicious link or download in the browser. This matches

#### 2. Persistence Hunt–Registry

Yes. Most of the Registry Run entries look normal and expected for a regular user system. Things like *OneDrive*, *Chrome*, and *AdobeUpdater* all do point to legitimate programs being installed in the usual locations.

##### Suspicious Registry Run Key:

- Value Name: *UpdateSVC*
- Path: *C:\Users\Public\Music\update.vbs*

##### Why this shows suspicious:

- The *UpdateSVC* name is being designed to look like a system service
- *.vbs* files are commonly or usually used by malware for persistence
- The *Public\Music* folder is not the place where legitimate software can run scripts from.

#### 3. Persistence Hunt – Scheduled Tasks

Looking at the scheduled tasks, it seems none of them stand out as malicious.

All the tasks listed appear to belong to legitimate software (*Adobe*, *Microsoft Edge*, *Google*, *OneDrive*), whereby their paths and triggers are consistent with normal behavior.

#### 4. Trying It all Together

- The filename of the persistence malware is *update.vbs*
- The full path is *C:\Users\Public\Music\update.vbs*
- The persistence mechanism the attacker used is *Registry Run Key (User logon persistence)*
- MITRE ATT&CK Technique: *T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder*

## 5. Final Recommendation

### Is the machine clean after killing the process?

No. Stopping the PowerShell process only fixed what we could see at the moment. The persistence is still there, so the malware would come back the next time the user logs in.

### Immediate next steps

- Remove the malicious *UpdateSVC* registry run entry.
- Delete the *update.vbs* file from the system.
- Run a full EDR scan to make sure nothing else was dropped.
- Reset the user's credentials in case they were exposed.
- Other machines must be checked for the same indicators to rule out wider spread.