Share

Hoodie2: Autoruns – control auto startups

Many places hold auto startup programs:

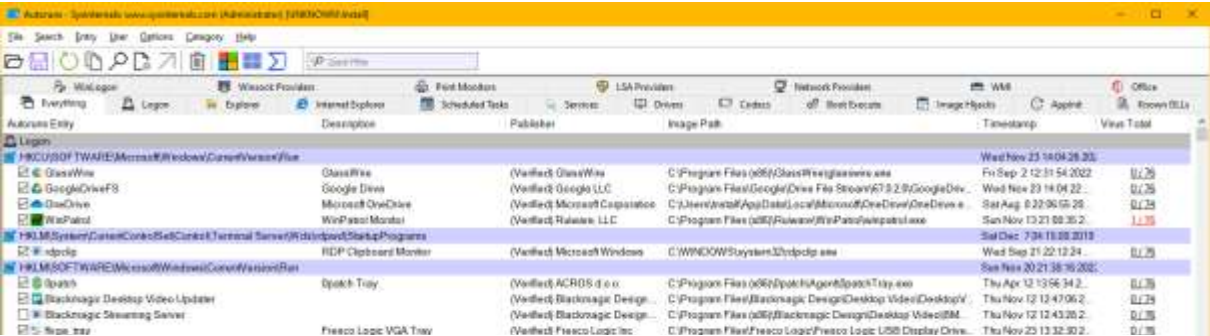
- Startup folder
- Registry – Run, Run Once, ...
- Task manager
- Services & Drivers
- File Explorer extensions
- Winlogon
- ...

So what?
Why delete/disable some autoruns?

- Minimise startup time
- Minimise memory usage
- Remove spyware/malware
- Remove excess background processing
- Remove clutter

NOTE: Run as administrator to make changes

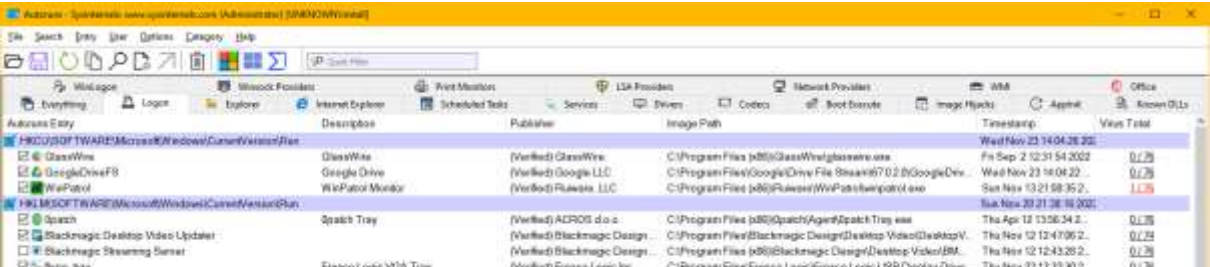
Autoruns screen



- Tabbed layout – Everything, or particular startup categories
- Verified – means Publisher verified by program signature
- Can search by name via “Quick filter” or Find  button

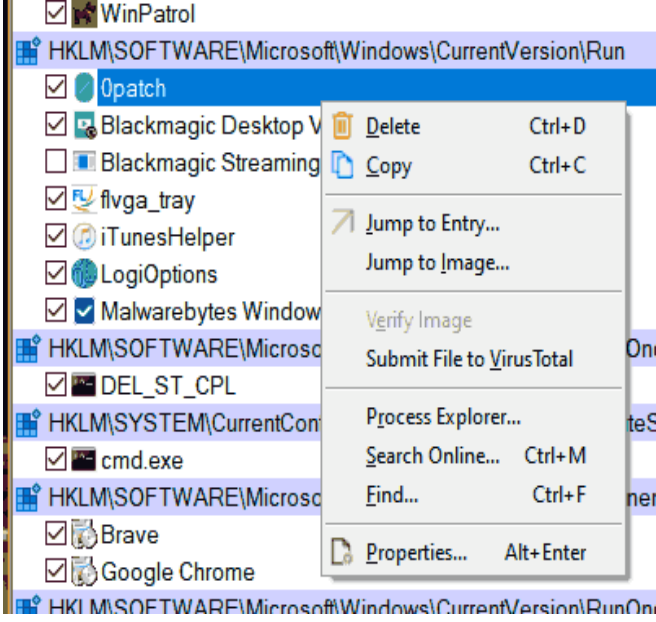
(example) Logons tab

- Everything that starts when a user logs on
  - Program startup locations
  - Run keys
  - Malware often uses



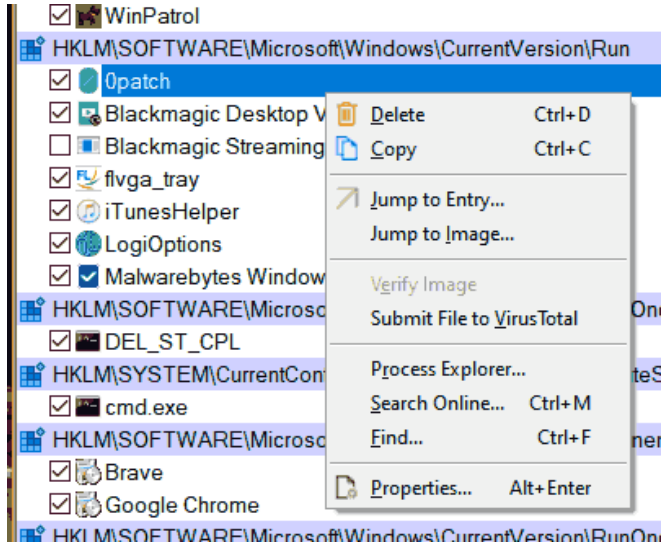
Strategies

- Delete obsolete entries – file not found
- Delete or disable programs you do not want running now
- Beware deleting/disabling programs you know nothing about! Programs you want may depend on them.



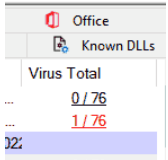
Right-click actions

- Jump to entry – goes to registry
- Jump to image – shows file in folder
- Process Explorer – opens details of the running process
- Properties – shows file properties
- Search online for the file

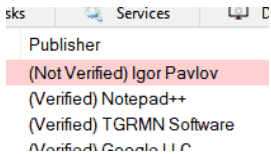


Suspicious entries

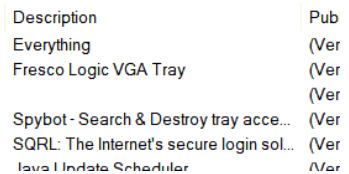
- Virus Total as a hit



- Publisher not verified



- No Description

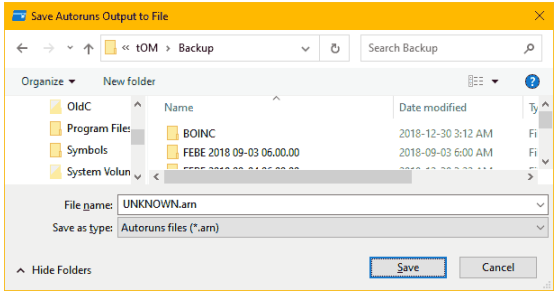


Investigate suspicious files

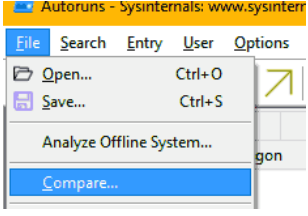
- Many hits in Virus Total?
- Check file name online for virus reports
- Is Description good English?
- Is the file in a *temporary* folder? Why???

Compare against previous checkpoints to see changes

- Save to a file:



- Compare current autoruns vs. Previous checkpoint:



Summary

- Autoruns is useful to:
  - Find malware/spyware
  - Remove memory/cpu hogs
- Autoruns source
  - https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
- Detecting/removing malware:
  - https://www.varonis.com/blog/how-to-use-autoruns