

## 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

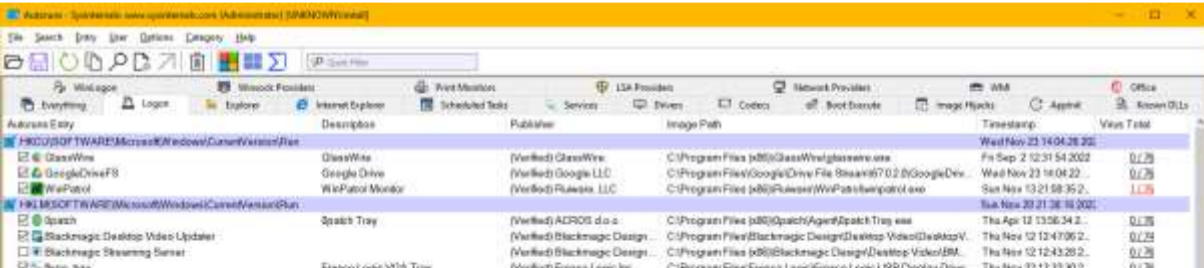
The screenshot shows the Autoruns application window. The title bar reads "Autoruns - System32\www.system32.com (Administrator) [1980x1080]". The menu bar includes "File", "Search", "Entry", "User", "Options", "Category", and "Help". The toolbar contains icons for "Everything", "Logon", "Explorer", "Internet Explorer", "Scheduled Tasks", "Services", "Drivers", "Context", "Boot Events", "Image Hooks", "Applet", and "Known DLLs". The main area displays a table of startup items with columns for "Autoruns Entry", "Description", "Publisher", "Image Path", "Timestamp", and "View Total".

Autoruns Entry	Description	Publisher	Image Path	Timestamp	View Total
<b>Logon</b>					
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run					
GlassWire	GlassWire	(Verified) GlassWire	C:\Program Files (x86)\GlassWire\glasswire.exe	Fri Sep 2 12:31:54 2022	0/25
GoogleDriveFS	Google Drive	(Verified) Google LLC	C:\Program Files\Google\Drive File Stream\67323\GoogleDev...	Wed Nov 23 14:04:22	0/25
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\mwh\AppData\Local\Microsoft\OneDrive\OneDrive.e...	Sat Aug 8 22:06:00 20...	0/25
WinPaint	WinPaint Monitor	(Verified) Rulaire, LLC	C:\Program Files (x86)\Rulaire\WinPaint\winpaint.exe	Sun Nov 13 21:00:35 2...	1/25
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\Programs					
rdpclip	RDP Clipboard Monitor	(Verified) Microsoft Windows	C:\WINDOWS\system32\rdpclip.exe	Wed Sep 21 22:12:24	0/25
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run					
Spacth	Spacth Tray	(Verified) ACROS s.o.c.	C:\Program Files (x86)\Spacth\Agent\SpacthTray.exe	Thu Apr 12 13:56:34 2...	0/25
Blackmagic Desktop Video Updater		(Verified) Blackmagic Design	C:\Program Files\Blackmagic Design\Desktop Video\Desktop\...	Thu Nov 12 12:47:06 2...	0/25
Blackmagic Streaming Server		(Verified) Blackmagic Design	C:\Program Files (x86)\Blackmagic Design\Desktop Video\BM...	Thu Nov 12 12:43:26 2...	0/25
Freecc	Freecc Logic VGA Tray	(Verified) Freecc Logic, Inc	C:\Program Files\Freecc Logic\Freecc Logic USB Display Drive...	Thu Nov 25 13:32:30 2...	0/25

- 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

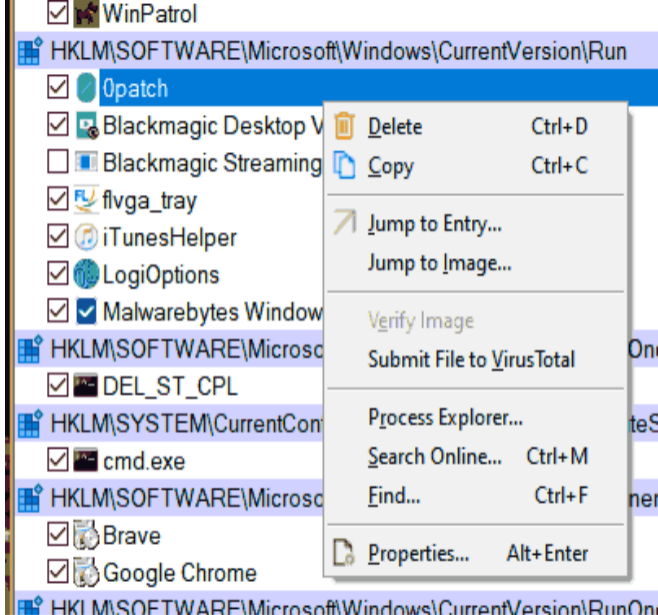


The screenshot shows the Windows Task Manager application with the 'Logons' tab selected. The window title is 'Admin: SystemInfo www.systeminfo.com (Administrator) [3880x1080]'. The taskbar includes icons for Start, Search, Task View, Settings, File Explorer, Internet Explorer, Scheduled Tasks, Services, Drives, Cortana, Boot Executive, Image Hooks, Appbar, and Known DLLs. The Logons tab displays a table with the following columns: 'Autostart Entry', 'Description', 'Publisher', 'Image Path', 'Timestamp', and 'Virus Total'.

Autostart Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run				Wed Nov 23 14:04:28 2011	
GlassWire	GlassWire	(Verified) GlassWire	C:\Program Files (x86)\GlassWire\glasswire.exe	Fri Sep 2 12:31:54 2012	0/29
Google Drive FB	Google Drive	(Verified) Google LLC	C:\Program Files\Google\Drive File Sharing\7.0.2\GoogleDriveFS.exe	Wed Nov 23 14:04:28 2011	0/29
WinPatrol	WinPatrol Monitor	(Verified) Plaxco, LLC	C:\Program Files (x86)\Plaxco\WinPatrol\winpatrol.exe	Sun Nov 13 21:58:35 2011	1/25
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run				Tue Nov 23 21:38:18 2011	
Spacth	Spacth Tray	(Verified) ACROS d.o.o.	C:\Program Files (x86)\Spacth\Agent\Spacth Tray.exe	Thu Apr 12 13:56:34 2011	0/29
Blackmagic Desktop Video Updater		(Verified) Blackmagic Design	C:\Program Files\Blackmagic Design\Desktop Video\Desktop Video Updater.exe	Thu Nov 12 12:47:06 2011	0/29
Blackmagic Streaming Server		(Verified) Blackmagic Design	C:\Program Files\Blackmagic Design\Desktop Video\Blackmagic Streaming Server.exe	Thu Nov 12 12:43:29 2011	0/29
Blackmagic Desktop Video Updater		(Verified) Blackmagic Design	C:\Program Files\Blackmagic Design\Desktop Video\Desktop Video Updater.exe	Thu Nov 12 12:43:29 2011	0/29

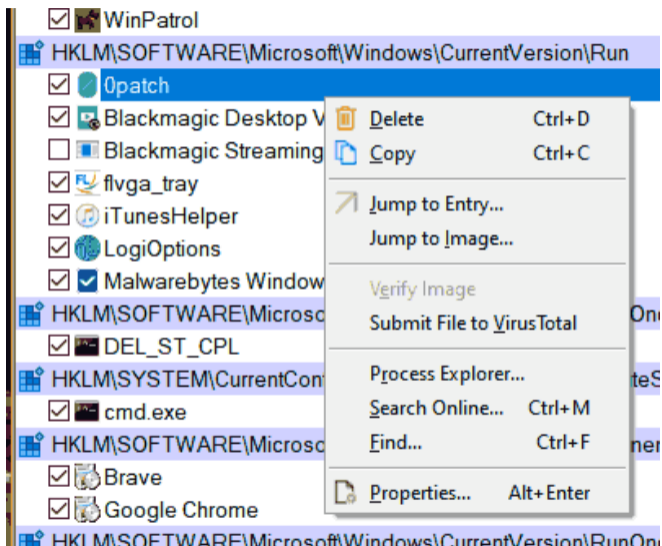
# Strategies

- 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.



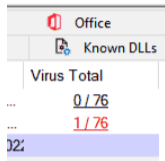
# Right-click actions

- 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

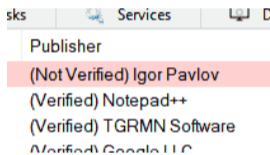


# Suspicious entries

- Virus Total as a hit



- Publisher not verified



- No Description

Description	Pub
Everything	(Ver
Fresco Logic VGA Tray	(Ver
	(Ver
Spybot - Search & Destroy tray acce...	(Ver
SQRL: The Internet's secure login sol...	(Ver
Java Update Scheduler	(Ver

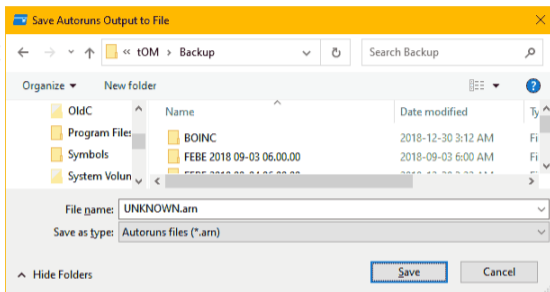
# Investigate suspicious files

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

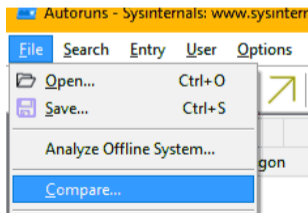


# Compare against previous checkpoints to see changes

- 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>