

test.au3

especimen

- keylogger
- data mining
- oculta su presencia en el explorador de tareas (usar alternativa - herramientas)

localización física

- HKCU/Microsoft/Windows/CurrentVersion/Run
- carpeta inicio: `shell:startup` → `c:\users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
- carpeta oculta: `c:\<NOMBRE_EQUIPO>`
- carpeta oculta: `c:\programData\<sha1>`
- carpeta oculta: (capturas log + mining): `c:\users\<user>\appData\Roaming\<sha1>`

herramientas

- [Process Explorer](#), Sysinternals
- [cmdr](#), CMD mejorado, portable
- [foldermonitor](#)

extirpación

- eliminar procesos **systeminfo**, **vbc**, mirando previamente su ubicación
- eliminar localizaciones físicas

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/windows:virus:test.au3?rev=1570374014>

Last update: **06/10/2019 08:00**

