test.au3

especimen

- encontrado en Minerva
- keylogger
- data mining
- oculta su presencia en el explorador de tareas (usar alternativa - herramientas)
- posible punto de entrada: USB con fichero **Archivos.lnk** y **explorer.vbe**
    - parece que mueve el contenido del USB a una carpeta **usbdata** oculta y permite el acceso a esa carpeta a través del link que monta en la raiz, que evidentemente ejecuta el .vbe

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
- cmder, CMD mejorado, portable
- foldermonitor: monitoriza cambios en un directorio y/o subdirectorios
- DeskDrive, montar unidades USB en escritorio

extirpación

- eliminar procesos **systeminfo**, **vbc**, mirando previamente su ubicación
- eliminar localizaciones físicas
- eliminar claves registro (buscar **test.au3**)