Caso real

ALERTA → trojan:script/wacatac.b!ml

RUTA →
C:\Users\xxxxx
\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu_79rhkp1fndgsc\LocalState\rootfs\home\xxxxxxxx\.local\lib\py
packages\arsenal\data\cheats\Password
extraction\mimikatz.md

Mimikatz

¿que es?

Mimikatz es una herramienta para Windows que permite extraer las contraseñas de inicio de sesión, tickets de kerberos, hashes NTLM y certificados en Windows.

Destaca su capacidad de extraer las contraseñas sin cifrar directamente de la memoria de Windows y por esta razón es usada como una herramienta de post-explotación por pentesters, red teamers así como por parte de actores maliciosos.