CONCLUSIÓN

Dentro de los diversos ataques que pueden afectar a nuestros sistemas, el de malware oculto es uno de los más utilizados y peligrosos debido a su capacidad de pasar desapercibido. Pueden acceder a través de un archivo descargado de apariencia inofensivo como es el caso de los troyanos para infectar y conseguir crear un backdoor que permita un posterior acceso al sistema o máquina por parte del atacante. O ni siquiera hace falta descargar ningún elemento de forma consciente de internet como en el caso de los drive-by download, que aprovechan las webs donde está escondido su código y realizan la descarga de malware de forma camuflada. Hay diversas maneras de detectar este tipo de malware que se pueden compaginar para garantizar su éxito, pero lo más importante es la prevención puesto que pueden ser muy complicados de eliminar incluso una vez detectados, como sucede con los rootkit. Para ello es bueno tener las directrices de seguridad bien implementadas y tanto los programas como el SO actualizados y con sus correspondientes parches de seguridad instalados.