**Malware.**

Para poder llegar a comprender la definición de malware oculto, primero debemos analizar el significado de Malware. La palabra malware proviene de la unión de dos palabras en inglés **mal**icious soft**ware** (su traducción sería programa malicioso); es por ello que lo podemos entender como todo tipo de software que ha sido creado con la intención de dañar cualquier sistema. El malware suele ser confundido por la mayoría de las personas con los virus, sin embargo, es importante destacar que los virus informáticos son un tipo específico de malware.

El malware por lo general es creado por hackers, podemos encontrar diversas intenciones para las cuales pueden ser creados, algunas de ellas son: dañar los dispositivos, robar datos de información personal de los usuarios, apropiarse de los recursos informáticos o contagiar a otros sistemas que se encuentren en la red. Por otra parte, el objetivo de su creación está relacionado con la persona que lo diseña; normalmente son creados para buscar algún beneficio económico, pero también han sido utilizados como una herramienta para protestas, o para poner en prueba la seguridad y en algunos casos incluso se ha llegado a usar como arma de guerra entre gobiernos.

En la actualidad, este tipo de programas ha encontrado en Internet el medio predilecto para poder propagarse, ya sea mediante páginas web infectadas, correo electrónico sospechoso (conocido también como Spam), archivos compartidos en línea, demos de videojuegos, barras de herramientas o de cualquier otra cosa que se descargue de internet. En los últimos años debido a la revolución que han tenido los dispositivos móviles, estos también se han convertido en un vector de ataque importante. La evolución y el aumento del uso ilegal de estos programas maliciosos ha derivado en la necesidad, casi obligatoria de que los usuarios utilicen alguna herramienta que sirva para combatir este software malicioso, a esta herramienta la conocemos como antimalware.

Como hemos comentado con anterioridad existe una gran variedad de malwares, y dependiendo de las características de cada uno de ellos se han clasificado en los siguientes tipos de malware: infeccioso, oculto, espía, publicitario, que realicen ataques distribuidos o para secuestro de información y engaño. En nuestro caso hablaremos del malware oculto, y abarcaremos los diferentes tipos que existen, su respectivo método de propagación y las medidas de prevención y defensa que se deben tomar para evitar el ataque de estos programas.

**Malware oculto.**

Un malware podrá alcanzar sus objetivos, siempre y cuando permanezca oculto a la vista del usuario. Es por ello que llamaremos malware oculto cuando hablemos de programas nocivos cuyo ingreso al sistema y posterior ataque ocurra de manera silenciosa, es decir, sin que el usuario lo perciba y sin su consentimiento. Dentro de esta clasificación de malware oculto podemos de igual forma encontrar diversos malwares como es el caso de Troyanos, Backdoors, Drive-by downloads, Rootkits.

Unas de las mejoras que han ido perfeccionando los ciberdelincuentes en los últimos años es la posibilidad de ocultar el malware, por lo que este logra permanecer por bastante tiempo en nuestro dispositivo y ejecutándose en un segundo plano.

Algunos lugares que han sido utilizados por los hackers para ocultar los malwares son los siguientes:

* **El registro de Windows,** varios programas han sido creados con la posibilidad de modificar este registro para poder controlar el tiempo en el que quieran que se ejecute el software, ya sea al iniciar el sistema, después de cada tiempo programado, entre otros.
* **Archivos y carpetas temporales**, es uno de los lugares donde casi siempre son ocultados los malwares, estos pueden ser tanto la caché de Internet o datos de las aplicaciones; ya que desde estos lugares pueden realizar otras amenazas con la facilidad de que pueden recopilar información del usuario.
* **Accesos directos,** abarca las páginas web que han sido modificadas para realizar sus ataques, de igual forma pueden incluir archivos ejecutables modificados que ha vista del usuario sea difícil encontrar las diferencias con respecto al original.
* **Descarga de archivos**, en estos casos pueden ocurrir al intentar descargar música, una aplicación o un simple documento Word o de Excel, los cuales pueden haber sito modificados para albergar un malware y poder atacar de esta forma al sistema.
* **El e-mail,** en general puede llegar a ser el tipo de amenaza más frecuente en la actualidad. Pueden venir ocultos en los SPAMS, estos tipos de correos son un peligro inactivo hasta que el usuario por error entre en ellos y descargue algún archivo o entre en una página maliciosa.

El Malware oculto también ha llegado al internet de las cosas (IoT en sus siglas en inglés) y es que es bastante la cantidad de equipos que se han ido incorporando a la red de dispositivos que se conectan a Internet, sin embargo, esta llegada no ha venido con un aumento de seguridad frente a ciberataques, por lo que en la actualidad pueden llegar a convertirse en los puntos débiles dentro de nuestra red por lo que pueden servir de puente para realizar ataque a nuestros ordenadores o móviles.

**Bibliografía:**

Cardozo, L. y García B. (2012). *Malware: Historia y Clasificación*.

<https://www.redeszone.net/2018/11/24/lugares-esconder-malware/>

<https://www.avast.com/es-es/c-malware>

<https://www.ionos.es/digitalguide/servidores/seguridad/como-identificar-y-eliminar-malware/>

<https://www.avg.com/es/signal/what-is-malware>

<https://es.m:alwarebytes.com/malware/>