**Ataques reales con Malware Oculto.**

Para que podamos comprender mejor el alcance que pueden llegar a tener este tipo de malware, hemos decidido recopilar información de algunos ataques reales que han sido realizados bajo la técnica del malware oculto y que han afectado a un gran número de usuarios, los cuales en algunos casos probablemente ni si quiera se han dado cuenta de que estaban bajo amenaza.

Coronavirus informático:

Uno de los ataques más recientes con el uso de malware oculto está siendo el llamado Coronavirus informático y es que los hackers están aprovechando la pandemia sobre el COVID-19 para ocultar malwares dentro de todo tipo de documentos y vídeos. Este ataque esta siendo realizado por lo general en informaciones que nos llegan a nuestros dispositivos sobre cómo protegernos del coronavirus, los métodos de detección y actualizaciones sobre el estado de alarma; y el usuario al estar interesado en ellos accede a abrirlos sin esperarse que estos archivos estén infectados.

Según la empresa Kaspersky (empresa de ciberseguridad), hasta la fecha han sido encontrados por los momentos 10 archivos distintos con malwares ocultos; sin embargo, se estima de que la tendencia aumente debido es considerado un cebo perfecto, ya que es una información que se puede propagar de manera extraordinaria dentro de la población.

Aplicaciones móviles ocultas:

Según un estudio realizado por la compañía McAfee para el año 2019, las aplicaciones móviles ocultas generaron aproximadamente el 50% de todos los ataques a móviles de ese mismo año. El problema viene dado porque los hackers han ido mejorando las formas de ocultar sus ataques, logrando que cada vez sean más difíciles de identificar y de eliminar.

Los hackers aprovechan generar versiones falsas de WhatsApp, Spotify, entre otras aplicaciones debido al alto impacto de descargas que estás pueden llegar a obtener. De igual forma se aprovechan de la popularidad de algunos juegos para engañar a los usuarios, y es que una vez el cliente haga uso de la app, el atacante adquiere la capacidad de controlar todo el dispositivo y muchas veces el usuario ni se da cuenta de que esto está pasando.

Los troyanos bancarios:

Uno de los ataques más frecuentes en la actualidad es el de los troyanos bancarios, debido a que le permite al hacker sustraer toda la información bancaria que desee. Este malware por lo general, se esconde mediante programas aparentemente legítimos; sin embargo, pueden acceder a la información mediante programas que hemos descargado e instalado.

Este tipo de malwares por lo general van dirigidos para atacar nuestros dispositivos móviles o también a ordenadores que tengan el sistema operativo Windows. Las maneras de obtener estos troyanos por lo general son descargando algún software malicioso, mediante archivos malignos que nos han sido enviados por e-mail o también al ingresar a páginas web infectadas.

Troyano Eurograbber:

Durante el año 2012, en Europa se vivió bajo la acción de un troyano conocido como Eurograbber; este ataque ha sido uno de los grandes asaltos informáticos ya que se saldó con la sustracción de 36 millones de euros en toda Europa, y es que este ataque afectó cerca de unos 30 mil usuarios de banca de países como Alemania, Italia, Países Bajos y España.

En España cerca de 11.000 personas vieron sus cuentas bancarias afectadas, lo que le permitió el robo a los ciberdelincuentes con un botín estimado de 5.8 millones de euros. Los ataques por lo general eran realizados a dispositivos bajo Android y BlackBerry

Troyano en dispositivos móviles:

En el año 2019 se descubrió la existencia de un malware (troyano) oculto en la aplicación de Android CamScanner, la cual cuenta con más de 100 millones de descargas en Google Play Store. Este ataque fue descubierto gracias a las investigaciones de la empresa de seguridad Kaspersky Lab.

El ataque se realizaba mediante una biblioteca de publicidad, la cual contenía a este componente malicioso. Al descargar la aplicación y ejecutarla, los hackers ya podían acceder al dispositivo infectado y beneficiarse de la manera que quisieran, desde mostrarle publicidad intrusiva o hasta robar dinero de su cuenta móvil mediante el cobro de suscripciones.

Este es uno de los casos de mayor alerta debido a que se trataba de una aplicación legítima de Android que usaba compras integradas y que su monetización provenía de los anuncios. La aplicación en su momento fue eliminada por Google de la Play Store para evitar que los usuarios se siguieran viendo afectados.

Referencias Bibliográficas:

<https://www.elespanol.com/omicrono/20200131/coronavirus-informatico-hackers-aprovechan-epidemia-infectar-dispositivos/463953911_0.html>

<https://www.muyseguridad.net/2020/03/06/aplicaciones-moviles-ocultas/>

<https://www.europapress.es/portaltic/internet/noticia-troyano-roba-58-millones-euros-clientes-banca-online-espana-20121205182549.html>

<https://www.lavanguardia.com/tecnologia/20190828/478235982/descubren-troyano-app-android-100-millones-descargas.html>