TWITTER Y FACEBOOK NUEVAMENTE UTILIZADAS PARA LA PROPAGACIÓN DE CÓDIGOS MALICIOSOS

Durante este mes, se ha detectado la propagación de un gusano vía Twitter y un ataque multi-stage a través de Facebook. Sin importar eso. Además, apareció un troyano para los equipos móviles que utiliza los sistema operativo Android.

Durante enero la red social microblogging twiter fue utilizada para propagar malwares Por su parte Facebook sufrió un ataque multi-stage, confirmando la tendencia a utilizar las redes sociales como plataforma de ataque. Asi mismo, se descubrió un nuevo troyano para la plataforma de dispositivos móviles Android que convierte al equipo infectado en parte de una botnet, según informa la compañía de seguridad la informática ESET.

El mismo día que se dio a conocer la noticia más de 200 millones de cuentas de usuarios estaban infectadas con este nuevo malware se encontró un gusano que utilizaba el acordador de direcciones url de google para poder ingresa a la popular red social de microblogging.

Durante el envió de mensajes en twitter utilizaban mensajes muy cortos y atractivos la cual llamaba la atención de los usuarios con un acordador de url les invitan a los usuarios a hacer clic y directamente ingresan a diferentes sitios web y ya supuesta mente les alerta sobre una posible propagación de virus en sus equipos y les ofrecen un programa el cual va a proteger a el equipo

Llamado Security Shield y esto es un troyano el cual va directo a dañar el computador sin que el usuario se dé cuenta de que abrió y lo descargo.

Este programa que ofrecen aparentan ser un programa de seguridad para el computador y en realidad lo que hace es instalar códigos maliciosos en el computador de la victima a un que en twitter ya han sido bloqueados es necesario que el usuario este pendiente de lo está aceptando ya que vienen de diversas formas a un que la mayoría han sido bloqueados a un se siguen presentando casos de malware en los computadores atra vez de twitter

Durante diez meses Facebook fue protagonista de un ataque multi-stage en este caso se esforzaron mucho en crearlo fue una amenaza muy elaborada que por medio de diferentes dispositivos de ataque recopilo muchísimos datos de las victimas este resulto ser muy interesante ya que permitió observar como es que los atacantes se las ingenian y combinan diversas técnicas de ataque las cuales les permite recopilar demasiados datos y también se pueden ocultar muy bien sin que el usuario se de de cuenta de que es un virus que puede causar demasiado daño ya que está hecho con técnicas muy avanzadas una vez el dispositivo a sido activado el malware envía cada un período aproximado

de 5 minutos información tanto del usuario como del equipo y la posibilidad de recibir comandos esto corre el riesgo de activar y de esta manera puede ejecutar la descarga o aplicaciones de dispositivos no deseados en el envió y borrado de mensajes de texto o la realización de llamadas o el acceso a paginas web

Twitter y Facebook nuevamente utilizadas para la propagación de códigos maliciosos

Shalom Jireth Amaya Sepúlveda
Luz Ángela Ruiz Corredor
T-114