JRA *de la* EGURIDAD

MALWARE

La palabra malware procede del acrónimo "malicius software", software malicioso. Su nombre lo dice todo. Es todo tipo de programas con finalidad maliciosa, de causar daño. Al principio se hablaba de virus, gusanos, troyanos, spyware, adware,... diferenciando cada programa malicioso en función de su finalidad u operativa. Pero muchos fueron evolucionando y adquiriendo más funcionalidades, por lo que resultaba difícil distinguir, por ejemplo, si era troyano o spyware. Por ello, se empezó a hablar genéricamente de malware.

PHISHING

Es una técnica por la cual el ciberdelincuente, mediante engaño, suplanta la identidad de un tercero (de confianza) para recabar de un usuario información sensible, o para que realice a su vez una acción que no debería realizar.
El phishing nació sobre el año 2002 y se centró en suplantar la identidad de entidades bancarias para que la víctima facilitara sus datos bancarios (nº de cuenta y de tarjeta, titular, claves de acceso). A medida que las entidades bancarias fueron adoptando medidas de seguridad y la información personal cada vez adquiría mayor valor, las técnicas de phishing se fueron perfeccionando y abriendo a otros escenarios. Así, hoy en día, podemos sufrir un ataque de phishing para robarnos nuestros datos bancarios o nuestros datos de acceso a Netflix, Amazon, Facebook, Twiter, Gmail, o cualquier servicio personalizable o de pago.

RANSOMWARE

Se trata de un malware que una vez acceden a los equipos informáticos víctima, cifra toda la información, incluido el sistema operativo, de forma que si la clave de descifrado no se puede acceder al equipo. Esto es, el ciberdelincuente toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos. La exigencia económica siempre es en criptomonedas, lo que dificulta el seguimiento del dinero y facilita la impunidad del ciberdelincuente.

SMISHING

Es otra variante de phishing. En este caso el canal de engaño son los mensajes de SMS y hoy en día, en la que cada vez se utiliza menos el servicio de SMS, los mensajes a través de redes sociales o servicios de mensajería, como el WhatsApp.
El nombre proviene del acrónimo de SMS y Phishing).
Desde que el teléfono móvil o smartphone es nuestro principal canal de acceso a la mensajería y redes sociales, lo utilizan para inducir a la víctima para que instale programas maliciosos en su móvil. La mayoría de los programas que se instalan tienen fines defraudatorios, para acceder a nuestra cuentas bancarias y robarnos dinero.

SPOOFING

Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de malware. Los ataques de seguridad en las redes usando técnicas de spoofing ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

TROYANO

Uno de los programas maliciosos más conocidos son los troyanos. Su funcionalidad es entrar en el ordenador de la víctima y controlarla remotamente, a través de internet. Los primeros que surgieron eran prácticamente inofensivos. Te permitían, por ejemplo, abrir remotamente las disqueteras o apagarte el ordenador. Con el crecimiento del **fraude en banca** electrónica, y las contramedidas de seguridad que establecieron los bancos, la solución más efectiva para superarlas era estar dentro del equipo informático de la víctima, donde poder copiar sus contraseñas. Así creció el uso de los troyanos, tipo keylogger, que copiaban las pulsaciones de teclado o las pantallas del equipo informático víctima. El crecimiento fue muy importante y ya se empezó a hablar de troyanos bancarios. Y cuando el acceso a banca electrónica se traspasó mayoritariamente a la telefonía móvil, los delincuentes también empezaron a crear troyanos bancarios para los distintos sistemas operativos de móviles, Android, iOS.

VISHING

colabora@guardiacivil.org

DIRECCIÓN GENERAL DE LA GUARDIA CIVIL

Oficina de Información y Atención al Ciudadano
C/ Guzmán El Bueno 110 - 28003 Madrid

NIPO (ED. PAPEL): 126-21-112-9
NIPO (ED. EN LÍNEA): 126-21-113-4
DEPÓSITO LEGAL: M-29554-2021

Papel
FSC® C015305
RECICLADO

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

EDITA: SECRETARÍA GENERAL TÉCNICA DEL MINISTERIO DEL INTERIOR
CATÁLOGO DE PUBLICACIONES DE LA ADMINISTRACIÓN GENERAL DEL ESTADO
https://page.mpr.gob.es
REALIZADO POR LA UNIDAD DE COORDINACIÓN DE CIBERSEGURIDAD
IMPRIME: ARTES GRÁFICAS COYVE, S.L.

guardiacivil.es

@guardiacivil.062

@guardiacivil.062

@guardiacivil

062

www.guardiacivil.es

Oficina de Información y Atención al Ciudadano
C/ Guzmán El Bueno 110 - 28003 Madrid

DIRECCIÓN GENERAL DE LA GUARDIA CIVIL

GUARDIA CIVIL

CULTURA *de la* CIBERSEGURIDAD

colabora@guardiacivil.org

DIRECCIÓN GENERAL DE LA GUARDIA CIVIL

Oficina de Información y Atención al Ciudadano
C/ Guzmán El Bueno 110 - 28003 Madrid