¿qué es el Crimeware?

CrimeWare es el termino con el que se denomina al software que se utiliza para llevar a cabo actividades Criminales, como son Fraudes Cibernéticos y Robos de Identidad, uno de los ejemplos más claros de sus aplicaciones negativas es el llamado "Phishing", técnica basada en el envío de correos falsos para obtener fraudulentamente información sensible de usuarios de servicios financieros.

Los Phishers (delincuentes que envían estos correos) utilizan una combinación de engaños por medio del uso de Ingeniería Social, y elementos técnicos para robar información sensible a los usuarios.

Por otro lado, la Anti-Phishing Working Group, organismo que se dedica a la Prevención, Detección, Combate y Monitoreo del Phishing en varios países, ha informado que la tendencia de los delincuentes es a alejarse de los esquemas de Ingeniería Social concentrándose principalmente en el uso de Software especializado para llevar a cabo su labor criminal.

Esta tendencia que se ha venido monitoreando desde hace 3 años ha sufrido un incremento constante, lo que deriva en la aparición de infinidad de códigos troyanos tendientes a secuestrar la información sensible de los usuarios.

Los detalles de estos hallazgos se publican mensualmente aquí..

Hace tiempo Panda Software detecto un código malicioso, el trj/Bancos.NL, que incluía una lista específica de dominios de entidades financieras, con el fin de identificar cuando el usuario entraba en contacto con alguna de ellas para en su caso almacenar todos los detalles de la actividad realizada, y reportarlo a sitios controlados por los delincuentes.

La APWG esta convencida de que los Phishers continuaran en su tendencia de automatizar en mayor grado sus intentos de este tipo para robar las credenciales de usuarios de Comercio y Banca Electrónica, alejándose de los esquemas de Ingeniería Social. Es por ello que ha creado el PROYECTO CRIMEWARE, una iniciativa de colaboración para capturar, registrar y clasificar los incidentes de daños causados por el tipo de software conocido como CrimeWare.

A esta fecha, la APWG tiene las siguientes clasificaciones para el Crimeware:

KeyLoggers Tipo de código troyano que se diseña con el objeto de recolectar información del usuario. A diferencia de los Keyloggers genéricos, los que están orientados al Phishing cuentan con componentes de rastreo que se activan para monitorear la actividad de instituciones financieras y de comercio electrónico muy especificas.

Redirectors Tipo de código troyano que intenta redirigir a un usuario hacia un sitio al que el no pretendía ir, esto incluye crimeware que cambia archivos e información local del servicio de DNS del equipo para lograr modificar la ubicación del sitio a visitar para obtener información sensible del usuario.

Pharming Tipo de ataque que intercepta la información enviada entre tu equipo y el servidor DNS de tu proveedor de acceso a Internet para redirigir a un usuario hacia un sitio fraudulento.

Alianza por la SEGURIDAD en internet