CENTRO CIBERNÉTICO POLICIAL

B@CIB – 006 | Boletín de Análisis en CIBERSEGURIDAD

#Troyano

Suplantan a Facebook para propagar MALWARE - Trojan.MSIL.agid

El Centro Cibernético Policial ha descubierto una nueva campaña de malware que se propaga vía correo electrónico y que trae consigo un peligroso troyano denominado Trojan.MSIL.agid. Este software malicioso es capaz de robar información sencible contenida en el equipo de la víctima, incluyendo nombres de usuarios, claves de acceso a la banca virtual y todo lo que se ingrese por teclado. Este software malicioso funciona como un keylogger y viene acompañado de otro troyano que es capaz de abrir puertas traseras (backdoor) permitiendo al atacante robar los datos de la víctima y tener el acceso remoto de manera no autorizada a la máquina comprometida.

CONCEPTO GLOBAL

Al momento de hablar sobre virus, troyanos y/o gusanos, usualmente hacemos referencia a un programa que tiene efectos nocivos para un sistema informático; estos términos, normalmente se pueden incluir en una sola palabra "malware" (malicious software).

Desde 2015 y lo corrido del 2016 nuestro CaiVirtual ha recibido más de 350 casos asociados al uso de software malicioso.

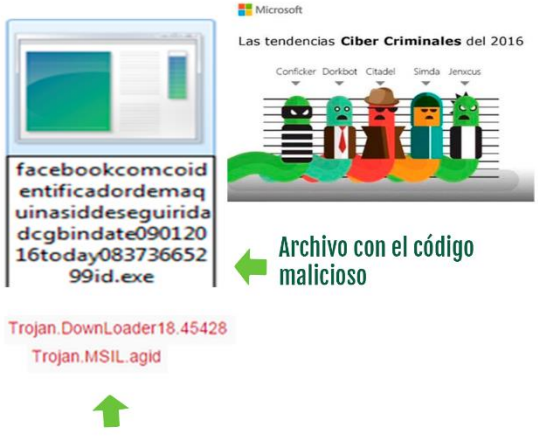
Más información en: www.ccp.gov.co

CENTRO CIBERNÉTICO POLICIAL

B@CIB – 006 | Boletín de Análisis en CIBERSEGURIDAD

Características

Esta modalidad de ataque se lleva a cabo mediante ingeniería social a través del envío de un correo electrónico a nombre de alguna entidad reconocida, en este caso, la propagación del troyano se lleva a cabo desde la cuenta "service@faceonline.com" y lleva como asunto "**SU CUENTA EN FACEBOOK PODRIA SER CANCELADA POR NUESTRO EQUIPO**"; además, contiene una URL que lleva a un sitio web desde donde se descarga un archivo adjunto *.ZIP que contiene un archivo ejecutable *.EXE tal como se puede apreciar la siguiente imagen:



Suma de verificación del código malicioso:

MD5 7fa841cb3ae883b54fed1bf8040b95be

SHA1 b91f6043ca0854d3e55dcbf2b9966b1139ae469f

Como resultado, la víctima al dar clic sobre el archivo ejecutable descarga y descomprime su contenido en una carpeta temporal, para luego ejecutar su payload (daños que causa un virus al activarse) y lograr comprometer la seguridad y privacidad de los usuarios; luego los atacantes cuentan con la capacidad de acceder a la información de las víctimas a través de C2 (Command & Control). Diseñado para Windows, tanto de 32 como de 64 bits.

Recomendaciones

1. Tenga cuidado al abrir archivos adjuntos en correos electrónicos.
2. Evite descargar software pirata o 'crackeado'. Este tipo de programas casi siempre incluyen algún tipo de malware.
3. Tenga programas de antivirus y firewall llamados también cortafuegos instalados en su ordenador, así como anti-espías.
4. Desconecte su ordenador de Internet cuando no lo esté utilizando o si cree estar infectado por algún software malicioso.
5. Mantenga su sistema operativo Windows siempre actualizado y parcheado al igual que su navegador web (browser) y el resto de los programas de su equipo.

@CaiVrtual
@MSFTColombia