Troyanos y Backdoors

3CM20
IT Governance
Martínez Coronel
Brayan Yosafat

Conceptos básicos

¿Cómo afectan?
Dependiendo del tipo, algunos pretenden robar información comunmente, sin alertar. Pero, podemos encontrar algunos que buscan dañar el equipo.

Son muy difíciles de detectar, por lo que, lo mejor es evitar encontrarnos con ellos.

¿Qué son?
Son programas disfrazados, por ejemplo, un correo o alguna descarga que aparenta ser otro programa. Suelen ser enviados mediante correo.

Mientras que los backdoors son accesos creados con algún troyano, para entrar más tarde en otra ocasión o robar datos de forma sigilosa.

Prevenir & corregir

Los expertos en seguridad dicen que una vez que entra un troyano:

Dependiendo del caso, se desconecte de la red, y se repare, encontrarlos sueles ser díficil, si ya se encontró, seguramente ya creó backdoors para atacar más tarde

La mejor de las recomendaciones es evitarlos, esto se puede hacer evitando descargar programas de sitios poco confiables, y no usar links de correos electrónicos.

Sin embargo, esas dos son en un mundo ideal, se recomienda también restringir el acceso a solo lo esencial según los roles de trabajo, la mayoría de los ataques de este tipo se presentan por personas internas, las razones son diversas (como enojo)

Se recomienda realizar pentesting con el apoyo de una consultoría, esto varía de precio según el tamaño de lo que se vaya a probar, pero resulta mucho más barato

¿De verdad?

Un caso muy conocido fue el del youtuber Fedelobo, que recibió un correo con los siguiente: Oye, mira mi juego, somos de una nueva desarrolladora, y queremos que lo pruebes, creemos que es un gran juego, no nos respondas, confiamos mucho en nuestro juego, pruébalo, y luego nos dices, no importa si nos rechazar, pero pruébalo

No se dio cuenta de que le robaron las credenciales de su canal y le secuestraron la cuenta.

Tomado de UNAM Seguridad en Cómputo y una entrevista con un consultor en seguridad informática http://blogs.acatlan.unam.mx/lasc/2016/02/11/troyanos-y-backdoors/