Colegio Santo Domingo
Nivel secundario

COMPUTACIÓN
Cursos: 2dos "A" y "B"

Profesor: Sergio Baigorria
e-mail: profesorsergiobaigorria@gmail.com
Fecha de entrega: lunes 09/05/2022.

Esta ya es la última guía de malware. Haz lectura comprensiva del texto. Si tienes dudas, consulta a tu profesor. Al final, hay un cuestionario de preguntas sobre este texto.

Botnet

Las **botnets** son redes formadas por equipos infectados por **bots**: aplicaciones maliciosas que permiten a un usuario malintencionado controlar esos equipos a distancia. Los equipos infectados son llamados **zombies**.
Con una botnet, el atacante puede generar muchísimas acciones delictivas como el envío masivo de correo electrónico o spam (correo no deseado) usando todos los equipos de la red infectada. Las botnets también pueden enviar órdenes a otras computadoras y enviar mensajes en redes sociales a través de las cuentas de los usuarios infectados.
(Observa la imagen de la derecha. Verás un ejemplo de cómo se contagia una red usando un troyano, luego se controla dicha red pues es una botnet, y por último, se la usa para enviar spam.)

Adware */ád-uer/*

El **adware** es un malware que tiene síntomas muy visibles: muestra constantemente ventanas más pequeñas, llamadas pop-ups, o muestra páginas web con publicidad de manera repetitiva. Para que aparezcan, basta con solo abrir el navegador o tener conexión a Internet. Son malwares de poca peligrosidad ya que su principal objetivo no es dañar el dispositivo o su software sino incitar al usuario compulsivamente a la compra de productos o a la visita de páginas web.

Rootkit */rút-kit/*

El **rootkit** es un malware que usa un conjunto de técnicas que le permiten permanecer indetectable ocultando los síntomas de la infección. Su objetivo es permitirle al ciberdelincuente, desde otro equipo, comandar acciones o extraer información importante sin ser descubierto.

Rogue */róuk/*

El **rogue** es una de las categorías más despreciables de malware. Prometen remover malwares y en realidad sólo sirven para infectar aún más el equipo o pretenden cobrar por limpiar infecciones que jamás ocurrieron.

Keylogger

Un **keylogger** es un tipo específico de spyware que se caracteriza por registrar concretamente las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un archivo en el dispositivo o enviarlas a través de internet. Suele ser aprovechado por ciberdelincuentes para obtener datos importantes de quienes usan el dispositivo.

Ransomware */ránsom-uer/*

El **ransomware** es un malware que usa **técnicas criptográficas o de cifrado**: cambia los datos para que no puedan ser leídos excepto por quien tenga la clave para volverlos legibles, (como hace Whatsapp con los mensajes que enviamos para que los hackers no puedan leerlos) junto con algunas técnicas que usan los ciberdelincuentes para engañar a los usuarios.

Cuando nuestro equipo se infecta con un ransomware, sus datos son encriptados para que no podamos leerlos, ni nosotros ni el dispositivo. Nos presenta un aviso que nos dice que todos nuestros datos en el dispositivo han sido encriptados. Nos pide que enviemos dinero a una cuenta para que el ciberdelincuente nos dé la clave que nos permitirá desencriptar nuestros datos, lo cual casi nunca ocurre.

Actividades

A continuación, te dejo un enlace a un Formulario de Google. Responde las preguntas allí mismo y con eso habrás cumplido toda la tarea de esta guía:

https://forms.gle/DEqsqB9nbpDuojZS6

No dudes en preguntarme sobre cualquier duda o problema que tengas.

Estoy para ayudarte.