VÍDEO intypedia006es

LECCIÓN 6: MALWARE

EJERCICIOS

AUTOR: Bernardo Quintero

Hispasec – VirusTotal Founder

EJERCICIO 1

Descubrimos en un sistema un malware que captura el usuario y contraseña cuando el usuario teclea esa información en procesos de autenticación. Según esa característica, podríamos decir que se trata de un:

a) Virus
b) Gusano
c) Keylogger
d) Backdoor

EJERCICIO 2

Los rootkits se caracterizan por:

a) Auto-enviarse por correo electrónico
b) Implementar técnicas para permanecer ocultos
c) Infectar a otros ejecutables
d) Presentar publicidad no deseada

EJERCICIO 3

Hay más posibilidades de infectarse navegando por la web si:

a) Usamos un navegador vulnerable, no actualizado con los últimos parches de seguridad

b) Visitamos webs para descargar películas y contenidos multimedia

c) Utilizamos software gratuito en vez de comercial

d) Vistamos dominios ".es" en vez de ".com"

EJERCICIO 4

Una vez hemos instalado un antivirus, podemos:

a) Olvidarnos del malware, porque el antivirus previene cualquier infección

b) Evitar las actualizaciones de seguridad del sistema, ya que el antivirus se encarga de la seguridad integral

c) Abrir y ejecutar cualquier tipo de programa, independientemente de su procedencia, y estar seguros de que no seremos infectados

d) Prevenir mejor las infecciones ya que, si bien no son infalibles, proporcionan una capa adicional a nuestra seguridad

EJERCICIO 5

Encontramos un fichero sospechoso en nuestro sistema, tras enviarlo a un servicio de análisis online descubrimos que se trata de un malware denominado "Win32.Adware.gen", según su nomenclatura podríamos deducir que:

a) Ha infectado a otros ejecutables y documentos de nuestro sistema

b) A los 32 días el sistema operativo Windows será formateado

c) Es el culpable de la aparición de ventanas con publicidad no deseada en nuestro sistema

d) Un atacante está controlando nuestro ordenador de forma remota y capturando nuestras contraseñas

RESPUESTAS

1. c
2. b
3. a
4. d
5. c

Madrid, España, marzo de 2011

http://www.intypedia.com

http://twitter.com/intypedia