Nombre: Fecha:

Seguridad informática– Examen 4

Parte 1 (3.2)

1.1) Define virus y ransomware (2 puntos)

1.2) Nombra los tipos de malware que conoces. (2 puntos)

1.3) Indica, según la información proporcionada, qué tipo de malware es más probable que se esté ejecutando en cada situación (1 punto cada una):

a) En la pantalla del cliente aparece un mensaje informando de que los datos están cifrados y la única manera de volver a acceder a ellos es pagando un rescate.

b) Mientras el cliente navega por la red, aparecen demasiadas ventanas intrusivas llenas de publicidad.

c) El cliente indica que el ordenador tiene un comportamiento lento y errático desde que ejecutó un programa para piratear su suite ofimática.

d) El cliente está preocupado porque ha recibido un correo electrónico de un banco en el que no tiene cuenta corriente, indicando que hay un descubierto a su nombre.

e) El cliente te dice que sus contactos han recibido un correo de su parte que él no ha enviado, indicando que abran las fotos que adjunta en ese correo.

f) El cliente te informa de que el led de la webcam de su ordenador se activa aunque no esté usándola en ese momento.

Parte 2 (4.2)

2.1) ¿Qué distingue un ataque de ingeniería social frente a otros tipos de ataques maliciosos? (2 puntos)

Material elaborado por David Romero Santos

2.2) ¿Cómo protegerías una organización frente a ataques de ingeniería social? (3 puntos)

2.3) Nombra las técnicas de ingeniería social que conozcas. (2 puntos)

2.4) Expón un ejemplo de un ataque de ingeniería social, lo más detalladamente posible. (3 puntos)

Material elaborado por David Romero Santos