Curso: IFCT0109 Seguridad informática
Expte.: 29/2020/LJ/0019
Evaluación:
Acción y grupo:
Módulo: MF0488_3 Gestión de incidentes de seguridad informática

Fecha examen:	20/02/2023
Nombre y apellidos:	
NIF:	
Docente:	Juan Antonio Ferrández Rodríguez

Tipo de Evaluación (Señale con una X la que corresponda)			
Evaluación 1	X	Recuperación I	

Referencias:
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2091-ccn-cert-bp-04-ransomware-1/file.html

1) El fichero info.zip incluye la nota de rescate creada por un ransomware tras infectar un equipo, junto con uno de los ficheros cifrados. Para superar este reto deberás identificar el nombre de dicho malware.

Nombre ransoware: _____ Locky_____

2) Dependiendo de la familia de ransomware, es posible recuperar los datos cifrados mediante alguna herramienta.

En el fichero info1.zip se incluye la nota de rescate del ransomware junto con un fichero cifrado tras la infección de un equipo. La solución a este reto está dentro del fichero cifrado.

Nombre ransoware: __ GandCrab v4.0 / v5.0_____

3) La red de tu organización ha sido comprometida por el ransomware WannaCry. Afortunadamente, se realizan copias de seguridad diarias y se han podido restaurar todos los equipos y servidores. Además, se han aplicado los parches de seguridad correspondientes que mitigan la propagación de este malware a través de la red interna.

Este malware presenta la peculiaridad de que dispone de un kill switch, consistente en un dominio al que el malware se conecta antes de hacer nada y, si este dominio existe, para su ejecución.

Tu objetivo consiste en encontrar dicho dominio (sin http://) para poder salvar al mundo.

NOTA: es importante que ejecutes el binario en un entorno virtual. El password del zip es infected

Nombre dominio: www.ccncertnomorecryaadrtifaderesddferrrqdfwa.com

4) Hemos capturado la transmisión de algún tipo de malware en la red de nuestra organización Tenemos que responder a las siguientes preguntas sobre el fichero info2.zip

a) ¿Realmente hay una infección? _____ Si

b) Nombre del fichero infectado _____ gpg4win-2.2.5.exe

c) Tipo de malware _____ Troyano

d) Nombre del malware _____ Redline_Msil

5) Hemos recibido un correo electrónico y sospechamos que pueda ser un spam, ¿puedes contestar a las siguientes preguntas con respecto al fichero correo.eml:

a) ¿Realmente es un spam? _____ Si

b) ¿Qué nos puede hacer sospechar que es spam? _____ Ofuscado base64

c) Dirección URL donde nos remite _____
http://rta3650iorv.doeyrew.buzz/GL26GHSB0L6/577936.PROTESTO

d) Es sospechoso el sitio enlazado _____ No

6) Analizar el fichero uno.xlsb y contestar a las siguientes preguntas:

a) ¿Tiene macros?

b) Container format ←OpenXML

c) ¿Está ofuscado? ← Sí

d) Si está ofuscado con qué tipo ← Base64

e) ¿Tiene contacto con internet? ← Sí