Uno de los administrativos de nuestra organización lleva temas económicos con empresas internacionales y ha recibido un email relativo a una factura que tiene un enlace para descargarla. En la captura sanclemente-forense-01.pcap[1] está el tráfico de la organización generado después de abrir el email.

Como analista del SOC (Security Operations Center) haz una investigación del tráfico de red para determinar si hubo un incidente relativo a los emails recibidos por el administrativo. Usando tus conocimientos de Wireshark responde a las siguientes cuestiones:

1. Prepara el entorno:
   a. Crea un perfil llamado TH.
   b. Configura la columna tiempo para mostrar la fecha en formato UTC.
   c. Oculta la columna Length.
   d. Añade columnas para mostrar el puerto origen y puerto destino.
   e. Añade una columna para ver el contenido del campo Host de los paquetes http.
2. ¿Cuántos paquetes tiene la captura?.
3. ¿A qué hora se capturó el primer paquete?. NOTA: tiempo UTC y formato de respuesta: aaaa-mm-dd hh:mm:ss.
4. ¿Duración de la captura?.
5. ¿Cuál es el equipo más activo a nivel de enlace?.
6. ¿Fabricante de la NIC del equipo más activo a nivel de enlace?.
7. ¿Ciudad dónde está la sede de la compañía que fabricó la NIC del equipo más activo a nivel de enlace?.
8. La organización trabaja con direccionamiento privado y máscara de red /24, ¿cuántos equipos de la organización intervienen en la captura?.
9. ¿Cuál es el nombre del equipo más activo a nivel de red?.
10. ¿Cuál es la IP del servidor DNS de la organización?.
11. ¿Por qué dominio pregunta la víctima en el paquete 204?.
12. ¿Cuál es la IP del dominio de la pregunta anterior?.
13. Indica el país y la organización a la que pertenece la IP del apartado anterior.
14. ¿Qué sistema operativo corre el equipo víctima?.
15. ¿Cuál es el nombre del archivo malicioso descargado por el contable?.
16. Extrae el archivo malicioso, súbelo a Virustotal e indica el nombre del malware según malwarebytes.
17. ¿Cuál es el hash md5 del fichero descargado?.
18. Repite la búsqueda en Virustotal pero esta vez usando el hash md5. ¿Da el mismo resultado?.
19. ¿Qué software corre el servidor web que aloja el malware?.
20. ¿Cuál es la IP pública del equipo víctima?.
21. Haz un *display filter* para ver los paquetes dns y smtp donde interviene el equipo víctima.
22. ¿En qué país está ubicado el servidor de correo electrónico al que se le envía la información robada? .
23. Fecha en la que se creó el dominio al que se le envía la información exfiltrada.[2]
24. Analizando la primera extracción de información ¿Qué software corre el servidor de correo electrónico al que se le envía la información robada?.
25. ¿A qué cuenta de email se le envía la información robada?
26. ¿Cuál es la contraseña usada por el malware para enviar el email?[3]
27. ¿Qué variante del malware exfiltra la información?
28. ¿Cuáles son las credenciales de acceso a bankofamerica?
29. ¿Cada cuántos minutos se exfiltra la información recopilada?
30. Haz un display filter para ver los paquetes dns, http y smtp donde interviene el equipo víctima y repasa lo ocurrido. Una vez que tengas una idea global de lo ocurrido, escribe un informe sobre el incidente. El informe ha de tener 3 apartados:
    a. Resumen ejecutivo: usando un lenguaje sencillo explica de forma clara que sucedió (cuándo, quien y qué).
    b. Detalles de la víctima (nombre equipo, dir. IP, dir. MAC, nombre de usuario).
    c. IoC (Indicators Of Compromise): dir. IP, dominios y URLs asociadas con la infección, hashes SHA256 o MD5 en caso de ficheros maliciosos.

1 El fichero pcap es una captura de Bran Duncan miembro de la Unit 42 de PaloAlto Newtorks.
2 Usa la utilidad whois o alguna web especializada con información sobre dominios.
3 En los protocolos de correo electrónico es muy habitual el uso de la codificación base64 para el envío de adjuntos o texto con caracteres más allá de los caracteres ASCII imprimibles.