**DFIR – Caso #1**

1. ¿Cuál es el hash sha256 para el archivo adjunto malspam?
2. ¿Cuál es la línea de comando del proceso secundario cuando el usuario habilitó la macro?
3. ¿Cuál es el hash sha256 del archivo de la aplicación HTML de la pregunta anterior?
4. ¿cuál es el método de ejecución de DLL?
5. ¿Cuáles son la dirección IP y su nombre de dominio instalador alojado DLL?
6. ¿Cuál es la URL completa del instalador de DLL?
7. ¿Cuáles son las dos direcciones IP identificadas como servidores C2?
8. ¿Cuáles son los cuatro dominios C2 identificados en el archivo PCAP?
9. El malware generó tráfico a una dirección IP a través del puerto 8080 con dos solicitudes SYN, ¿cuál es la dirección IP?
10. El archivo license.dat se usó para crear persistencia en la máquina del usuario, ¿cuál es el método de ejecución de dll para la persistencia?

Herramientas necesarias

Wireshark, Network Miner, Virus Total, AnyRun

**DFIR Ransomware – Caso #2**

1. Identifique los procesos sospechosos
2. ¿Cuál es el nombre del archivo que utiliza el atacante?
3. ¿Cuál es el DLL identificado y la ruta asociada?
4. ¿Cuál es el hash MD5 para el dll?
5. ¿Cuál es el nombre de la nota de ransomware que se eliminó?
6. ¿Cuál es la URL desde la que se descargó la carga útil inicial? (Incluya la URL completa con la carga útil)
7. ¿Cuál es el nombre del archivo descargado por el usuario y la ruta?
8. ¿Cuál es el nombre del ransomware?

**Herramientas utilizadas**

Redline – FireEye

**Análisis de Malware – Caso #3**

1. ¿Cuál es el valor hash SHA1 de la muestra?
2. ¿Cuáles son las URL utilizadas por la muestra?
3. ¿Cuál es el nombre del archivo XML que almacena la URL extraída?
4. ¿Cuál es el CVE asociado a la vulnerabilidad explotada?

**Resultado AnyRun**<https://app.any.run/tasks/3908d3a9-54e0-4c49-8de3-c9e8c3a42169>

**Análisis de Phishing – Caso #4**

1. ¿Cuál es la dirección de correo electrónico de envío?
2. ¿Cuál es la dirección de correo electrónico del destinatario?
3. ¿Cuál es el asunto del correo electrónico?
4. ¿Qué empresa está tratando de imitar el atacante?
5. ¿Cuál es la fecha y hora en que se envió el correo electrónico?
6. ¿Cuál es la URL del botón principal de llamada a la acción?
7. Al mirar el contenido del cuerpo principal en un editor de texto, ¿qué esquema de codificación se está utilizando?
8. ¿Cuál es la URL utilizada para recuperar el logotipo de la empresa en el correo electrónico?
9. Por alguna razón desconocida, una de las URL contiene una URL de perfil de Facebook. ¿Cuál es el nombre de usuario (no necesariamente el nombre para mostrar) de esta cuenta, según la URL?

**Herramientas utilizadas**

CyberChef, Editor de texto, Outlook, HTML Viewer

**Análisis de Powershell – Caso #5**

1. ¿Cuál es el valor hash SHA256 para el archivo de script de PowerShell?
2. ¿A que categoría pertenece el malware?
3. ¿Qué dirección de correo electrónico se utiliza para enviar y recibir correos electrónicos?
4. ¿Cuál es la contraseña de esta cuenta de correo electrónico?
5. ¿Qué puerto se utiliza para SMTP?
6. ¿Qué DLL se importa y cuál es la función que cumple asociada a la categoría del malware identificado?
7. ¿En qué directorio se coloca el archivo txt generado?

**Herramientas utilizadas**

Editor de texto

**Análisis de Ransomware Script – Caso #6**

1. ¿Cuál es la dirección IP maliciosa a la que se hace referencia varias veces en el script?
2. El script usa apt-get para recuperar dos herramientas y usa yum para instalarlas. ¿Cuál es la línea de comando para eliminar los registros de yum después?
3. Este mensaje también contiene una dirección de correo electrónico de contacto para reparar el sistema. ¿cuál es?
4. Cuando los archivos están encriptados, se usa una extensión de archivo inusual. ¿cuál es?
5. Hay 5 funciones asociadas con el proceso de encriptación que comienzan con encrypt. ¿Cuáles son, en el orden en que realmente se ejecutan en el script?
6. El script verificará un archivo de texto alojado en el servidor C2. ¿Cuál es la URL completa de este archivo?

**Herramientas utilizadas**

Editor de texto

**DFIR – Fuerza Bruta – Caso #7**

1. ¿Cuántos eventos de falla de auditoría hay?
2. ¿Cuál es el nombre de usuario de la cuenta local a la que se dirige?
3. ¿Cuál es el motivo de falla relacionado con los registros de fallas de auditoría?
4. ¿Cuál es el ID de evento de Windows asociado con estas fallas de inicio de sesión?
5. ¿Cuál es la IP de origen que realiza este ataque?
6. ¿Con qué país está asociada esta dirección IP?
7. ¿Cuál es el rango de puertos de origen que utilizó el atacante para realizar estas solicitudes de inicio de sesión?

**Herramientas utilizadas**

Editor de texto, Excel, Visor de evento Windows

**DFIR – Ransomware Dump Memory – Caso #8**

1. ¿Cuál es el perfil del sistema operativo?
2. ¿Cuál es el nombre del proceso sospechoso?
3. ¿Cuál es el ID del proceso?
4. ¿Cuál es el ejecutable que creó el proceso?
5. ¿Qué proceso se utiliza para eliminar los archivos?
6. ¿Cuál es la ruta donde se ejecutó por primera vez el archivo malicioso?
7. ¿Cuál es el nombre del ransomware?
8. ¿Cuál es el nombre del archivo con la clave pública del ransomware que se usó para cifrar la clave privada con extensión .eky?

**Herramientas utilizadas**

Volatility, PowerShell, Editor de textos

**Análisis de tráfico malicioso – Caso #9**

1. ¿Cuál es el sistema operativo del host desde el que se capturó el tráfico de red?
2. ¿Cuál es la URL completa desde la que se descargó el ejecutable del ransomware?
3. Nombre el archivo ejecutable ransomware
4. ¿Cuál es el hash MD5 del ransomware?
5. ¿Cuál es el nombre del ransomware?
6. ¿Cuál es el algoritmo de cifrado utilizado por el ransomware?

**Herramientas utilizadas**

Wireshark, Virus Total.

**Análisis de PowerShell malicioso – Caso #10**

1. ¿Qué protocolo de seguridad se está utilizando para la comunicación con un dominio malicioso?
2. ¿Qué directorio crea el PowerShell ofuscado?
3. ¿Qué archivo se está descargando?
4. ¿Qué se usa para ejecutar el archivo descargado?
5. Cuál es el nombre de dominio del URI que termina en '/6F2gd/'
6. Según el análisis del código ofuscado, ¿cuál es el nombre del malware?

**Herramientas utilizadas**

Editor de texto

CyberChef