2. INVESTIGACIÓN.

a. ENTORNO CONTROLADO DE TRABAJO.

Antes de ejecutar cualquier tipo de análisis sobre una muestra malware, es necesario disponer de un entorno de trabajo seguro y controlado. Se utilizará la ayuda de máquinas virtualizadas en un dispositivo anfitrión que será configurada de una manera determinada dependiendo del tipo de análisis que se quiera realizar en cada momento.

La virtualización se llevará a cabo con el software "VirtualBox", "una potente herramienta de uso empresarial y doméstico, rico en funciones y de alto rendimiento para clientes empresariales. Además, se trata de la única solución profesional que está disponible de manera gratuita como software de código abierto bajo los términos de la licencia publica general GNU (GLP) versión 2".

El sistema operativo utilizado para montar la maquina virtual será "IE11 on Windows7 (x86)", obtenido de la pagina oficial de desarrollo de Microsoft, que proporciona el servicio gratuito con un limite de uso de 90 días.

Una vez creado de manera correcta el servicio virtualizado, es necesario configurar la maquina con las herramientas necesarias para llevar a cabo los análisis estáticos y dinámicos de los ejemplares ransomware.

Las búsquedas en Internet se podrán realizar de dos maneras, aunque para algunas serán exclusivamente necesario utilizar el navegador TOR *explicación* Browser, un navegador que protege la provacicidad de los usuarios y mejora la seguridad online, además de proporcionar acceso a la "Deep Web", lugar en el cual se encuentran la mayoría de grupos ransomware.

b. MUESTRAS

Antes de llevar a cabo un análisis estático o dinámico de una muestra ransomware, es necesario realizar una recopilación de información sobre el malware, obteniendo datos como el hash del archivo, cabeceras, librerías (DLLs) utilizadas…

Ciertas plataformas ofrecen servicios de este tipo, siendo de gran utilidad para entender el funcionamiento y comportamiento del individuo.

VIRUS TOTAL

Se trata de una herramienta en la web, ya que inspecciona el elemento proporcionado con más de 70 escáneres antivirus y servicios de listas de bloqueos de dominios/URL, además que variedad de herramientas para extraer señales del contenido y la propia base de datos de la empresa.

Permite al usuario insertar la consulta a realizar de varios métodos diferentes, pudiendo elegir entre un archivo, una URL o una búsqueda identificada por dirección IP, dominio, hashes…

ANY RUN

Se trata de una herramienta que ofrece un servicio de sandboz para el analsiis malware que permite analizar una muestra de malware de forma segura sin ningún tipo de riesgo para los equipos.

Los resultados obtenidos en esta prueba son los registros de red, actividad de archivos y cambios de registro, además de permitir observar el comportamiento que sigue la muestra.

c. ANALISIS ESTATICO DE MUESTRAS

Se denomina “análisis estático” al estudio realizado sobre una muestra sin detonar, es decir, sin ejecutar la función establecida dependiendo del tipo de archivo o elemento a analizar.

Las herramientas utilizadas en este proceso permiten extraer información sin necesidad de ejecutar la muestra. La información está disponible para el usuario de manera inmediata y puede servir como base para guiar la investigación.

En el análisis estático se estudia el código ensamblador, strings, dependencias, cabeceras, etc… Este proceso se encuentra dividido en fases, dependiendo de la función que se realice en ese momento

Alguna información relevante que obtenemos es el consumo de la memoria del archivo, recorriendo sus sistemas de ficheros en busca de posibles amenazas, etc…

HERRAMIENTAS DE IDENTIFICACION DEL BINARIO

TECNICAS ANTIDETECCION Y ANTIINGENIERIA INVERSA

OBTENCION DE STRINGS

DEBUGGERS

El análisis estático se realizará sobre dos familias de Ransomware as a Service, conocidas como “REvil” o “Sodinokibi” y “Avaddon”.

d. ANALISIS DINAMICO DE MUESTRAS

Se denomina “análisis dinámico” al estudio realizado sobre una muestra detonandola, es decir, llevando a cabo la función del archivo que se haya ejecutado.

De esta forma se puede observar en primera persona cual es el comportamiento y funcionamiento del malware. Este estudio es necesario realizarlo en un entorno de pruebas aislado y seguro, para no dañar ninguna unidad importante de nuestro dispositivo anfitrión.

Para aislar la maquina virtual para que la ejecución sea totalmente segura es necesario:

- Bloqueamos la salida a Internet (Todos los adaptadores)
    - Configuración/Red/Deshabilitar adaptador de red.
    - Conectado a: No conectado.
- Deshabilitar las carpetas compartidas entre las máquinas virtuales y el host si existen.
- Deshabilitar portapapeles y arrastrar y soltar:
    - Configuración/General/Avanzado/Compartir portapapeles: Inhabilitado.
    - Configuración/General/Avanzado/Arrastrar y soltar: Inhabilitado.
- Prevenir la conexión de dispositivos de memorias extraíbles.
    - Configuración/USB/Deshabilitar USB.
- Mantener actualizado el software de virtualización.
    - Archivo/Comprobar actualizaciones.
- Realizar un snapshot que permita recuperar la máquina.
    - Instantáneas/Tomar Instantánea.

- Comprobar que no se tiene conexión a Internet.