Problemas Bancarios

LABORATORIO #2

Escenario

Introducción

El CEO de la compañía ETOLEPSED S.A. se ha puesto en contacto con usted para realizar un análisis forense sobre un incidente que ha ocurrido recientemente.

Uno de sus empleados habría recibido un correo electrónico de un compañero de trabajo con un PDF adjunto. Si bien al abrirlo no le pareció notar nada extraño, más tarde descubrió cierta actividad inusual en su cuenta bancaria.

La compañía ETOLEPSED S.A. ha logrado obtener una imagen de la memoria RAM de la máquina del empleado afectado y se sospecha que podría estar infectada con algún tipo de malware.

Le solicitan a usted que analice la evidencia e informe sobre cualquier actividad sospechosa encontrada.

Para resolver el presente laboratorio el alumno debe contar con el archivo de evidencia **memory-dump.zip** el cual puede ser descargado aquí. Dicha evidencia se corresponde con una captura de la memoria RAM de la computadora afectada.

Preguntas a responder

Para resolver el laboratorio, el alumno deberá responder las siguientes preguntas justificando en cada caso las respuestas y especificando las herramientas utilizadas:

1. Validar el hash de la evidencia. Continuar con las siguientes preguntas sólo en caso que la evidencia se encuentre validada.

Archivo	md5	sha1
memory-dump.zip	9ccedbb0683cc49ba7b2623007f930bb	50b4e7b18ee33dc0faea72a39a35ff05cdc86765
memory-dump.vmem	20d420729287026a3f55704154bd6163	aee1a80fed6671f3c3bb7d8bbe069c94f16fac09

2. Enumere los procesos que se estaban ejecutando en la máquina de la víctima. Según lo expresado por el empleado, ¿Qué proceso debió haber sido el responsable del exploit inicial?

3. Enumere los puertos de red que estaban abiertos en la máquina de la víctima durante la infección. ¿Hay algún proceso sospechoso que tenga sockets abiertos?

4. ¿Existen URLs en la memoria? En caso afirmativo enumere las URLs sospechosas que encuentre en el proceso.
5. ¿Existen otros procesos que contengan URLs que puedan indicar actividad en un Banco? Si es así, ¿cuáles son estos procesos y cuáles son las URLs?
6. Verifique si el proceso sospechoso tiene archivos embebidos. En caso afirmativo intente extraerlos.
7. Si se extrajo un archivo del proceso inicial, ¿qué técnica utilizaron estos archivos para efectuar el exploit?
8. Enumere los archivos sospechosos que fueron cargados por cualquier proceso en la máquina de la víctima. A partir de esta información, ¿cuál fue el payload del exploit que afectó a la cuenta bancaria de la víctima?
9. Si se pueden extraer archivos sospechosos de algún proceso inyectado, ¿algún producto antivirus detecta el ejecutable sospechoso? ¿Cuál es el resultado general de los productos antivirus?

Herramientas sugeridas

A continuación se listan un conjunto de herramientas sugeridas para resolver el laboratorio.

- **Volatility Framework** es una colección de herramientas completamente abierta, implementada en Python bajo la Licencia Pública General GNU, para la extracción de artefactos digitales de muestras de memoria volátil (RAM). https://github.com/volatilityfoundation/volatility
- **Foremost** es un programa de consola para recuperar archivos en función de sus encabezados, pies de página y estructuras de datos internas. Este proceso se conoce comúnmente como datacarving. http://foremost.sourceforge.net/
- **strings** es un comando de linux que para cada archivo dado, imprime las cadenas de caracteres imprimibles que tienen al menos 4 caracteres de largo.
- **VirusTotal** es un servicio en línea para analizar archivos y URLs sospechosas para detectar tipos de malware y compartirlos automáticamente con la comunidad de seguridad. https://www.virustotal.com/gui/
- **Pdf tools** analiza un documento PDF para identificar los elementos fundamentales utilizados en el archivo analizado sin procesarlo. https://blog.didierstevens.com/programs/pdf-tools/

Desafíos potencialmente peligrosos

Algunos desafíos forenses que vamos a realizar pueden contener piezas de código realmente maliciosas.

Tomar todas las precauciones del caso dado que

¡El profe no arreglará tu computadora!