Los registros de segmentación funcionan cambiando una ventana deslizante a través de la RAM, lo que permite que una CPU de 16 bits vea los 20 bits de RAM, asegurando que para cada valor de DS, la ventana se desplace 16 bytes.

Podemos ver todas las llamadas al sistema que hizo un programa, interrumpiendo el inicio del controlador de interrupción y verificando cuál es el valor de ah.

La CPU 8086 tiene 4 registros de segmentación de los que tendremos que preocuparnos:
CS - Segmento de código.
DS - Segmento de datos.
SS - Segmento de pila.
ES - Segmento extra.

Es un sistema operativo que ofrece una API completa para evitar que las aplicaciones necesiten sus propias implementaciones de sistemas de archivos.

George R. R. Martin, quien escribió Game of Thrones, supuestamente usó Wordstar en DOS para escribir el libro.

Es el sucesor de CP/M, otro sistema operativo muy antiguo.

La familia DOS cubre una amplia gama de vendedores, y el hecho de que sea DOS no significa que vaya a ejecutarse en un procesador 8086 o mejor.

Algunos de estos proveedores DOS comparten compatibilidad con API, lo que significa que algunos tienen malware compartido.

Esta es la era de la "computing beige" y del teclado Model M.

MS-DOS

¿Qué es DOS?

Un clavado en el mundo de los virus MS-DOS

DOS no siempre era tan bueno

A veces se usaba DOS y de repente aparecía la palabra techno en toda tu terminal mientras se reproducía una canción.

O se mostraba una ambulancia ASCII que se desplaza por la pantalla, y luego te permitía que el programa que se ejecutó continúe.

Historial de malware de DOS

Gracias a un grupo de archivistas de malware que funcionan bajo el nombre de “VX Heavens”, se obtuvo un buen archivo histórico de malware de DOS, hasta que la policía ucraniana asaltara el sitio por el artículo 361-1 del Código Penal de Ucrania: la creación de programas maliciosos con la intención de venderlos o difundirlos.

El servidor fue confiscado por la policía por la investigación criminal basada en una denuncia sobre "la colocación en acceso libre de programas maliciosos diseñados para la entrada no autorizada en computadoras, sistemas automatizados, redes de computadoras".

Todavía hay copias de la base de datos de este sitio en sitios web populares de torrents (tipo de archivo que se utiliza para compartir grandes cantidades de datos a través de Internet. Es un archivo pequeño que contiene información sobre la ubicación de los archivos que se desean compartir y cómo descargarlos.)

Entendimiento de la propagación del malware DOS

Generalmente el malware permanece en silencio e intentará encontrar archivos para infectar.

Primero se necesita comprender proceso de propagación de estas muestras, ya que estos programas se ejecutaban en una era pre-Internet:

En el momento de ejecución, el malware tiene dos opciones; puede quedarse oculto e infectar nuevos archivos, o puede mostrar su payload.

El malware buscará o instalará syscall hooks en los programas que ejecuta después. A menudo lo hará de manera sutil y no visible para evitar la detección. La importancia de la sutileza es importante ya que para que se propague este malware, debe darse a otro sistema a través de copias de medios (disco floppy) o cargarse en otro punto de distribución como un BBS (Sistema de Tablón de Anuncios).

Syscall hooks

Los syscall hooks también pueden ser utilizados con fines malintencionados, como la inyección de código malicioso en los procesos del sistema, la modificación del comportamiento de las aplicaciones legítimas o la ocultación de actividades maliciosas. Por lo tanto, es importante implementar medidas de seguridad adecuadas para evitar que sean utilizados de forma malintencionada.

Son una técnica de seguridad y análisis utilizada en sistemas operativos para interceptar y controlar las llamadas al sistema realizadas por los programas en ejecución.

Los syscall hooks permiten interceptar estas llamadas antes de que lleguen al kernel del sistema operativo. Esto permite a los programadores agregar una funcionalidad adicional a las llamadas del sistema o modificar su comportamiento.

En un sistema operativo, los programas no pueden realizar directamente ciertas tareas del sistema operativo, como acceder a los archivos. Sino que deben solicitar la realización de estas tareas mediante llamadas al sistema. Cuando un programa realiza una llamada al sistema, se produce una transición del modo de usuario al modo kernel, y el kernel del sistema operativo se encarga de realizar la tarea solicitada y devolver el resultado al programa.