A DIVE INTO THE WORLD OF MS-DOS VIRUSES

by Ben Cox "Benjojo"

Rojas Terrazas Laylet
Ruíz Sanchez Miguel Angel

George R R Martin escribió Games of Thrones en DOS

¿QUÉ ES DOS?

- Es el padre de un sistema Operativo más antiguo CP/M
- Es compatible con API, por lo que pueden compartir malware
- Forma parte de la era beige

23 DE MARZO

VX HEAVENS MALWARE

Debido a una investigración crimianll la policia Ucraniana interceptó la creación de programas maliciosos en un inteno de venta o distribución para la irrupción no autorizada en computadoras

FLUJO DE PROPAGACIÓN TÍPICA

Al tener un archivo infectado, este buscará instalar llamadas al sistema de manera sutil y no visible para que se ejecute después y no ser detectado

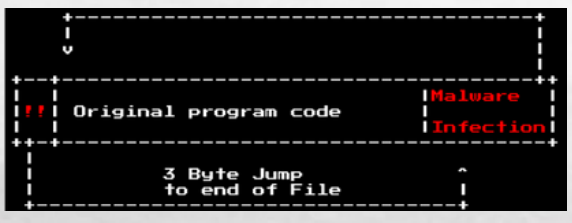
Cuando se ejecuta el programa el malware tiene dos opciones:

Ocultarse

Esto ocurre la mayor parte del tiempo

Mostrar su payload

HAVOC THE CHAOS



INFECCIÓN

Se inserta el JMP al comienzo del programa y agrega datos al final del programa o encuentra espacios vacios parra evitar que un binario se haga más grande, el cual alertaria al antivirus

FUNCIONES SYSCALL

Funcionan a través de un llamado a una interrupción, donde el programa le pedira a la CPU que salte a otra seccion de la memoria para manejar algo

Agrega/Modifica
↓
Llamadas
↓
Amplia el sistema

Ejemplo Rápido

```
[org 100h]
mov dx,msg
mov ah,9
int 21h

mov ah,4Ch
int 21h
msg db 'Hello, World!',0Dh,0Ah,'$'
```

Int 21h Syscalls

0 - Terminate	2A - Get Date
1 - Keyboard input	2C - Get Time
2 - Display output	31 - TSR
3 - Wait for device input	40 - Write to File
...	41 - Delete File
9 - Print string	48 - Allocate RAM
F - Open File	4C - Exit with return code

Carga de controladores

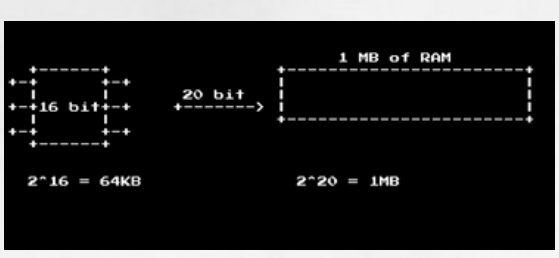
LLAMADAS AL SISTEMA

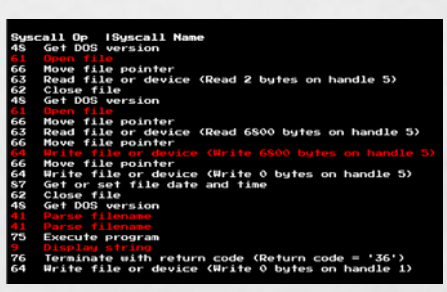
Se puede interrumpir el inicio del controlador de interrupción y verificar cuál es el valor de ah. el controlador de interrupciones siempre está en una ubicación fija en MS-DOS

la infección ocurre mediante

Goat files, es un archivo diseñado para ser infectado, como una cabra de sacrificio.

Las llamadas al sistema devuelven los valores como registros al programa





MEMORY LAYOUTS

La CPU 8086 tiene 16 bits, mientras que en su memoria de direccionamiento tiene 20 bits.
Su CPU puede contener valores a 64 KB, lo cual puede ser un problrma cuando la memoria es mayor

Para evitar eso necesita

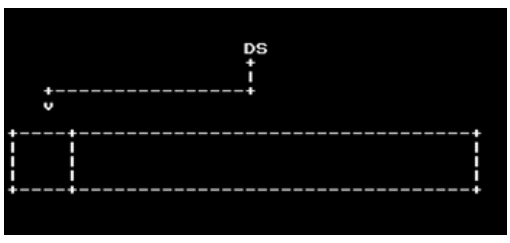
Registros de Segmentación

4 registros de segmentación

CS - Segmento de código
DS - Segmento de datos
SS - Segmento de pila
ES - Segmento adicional

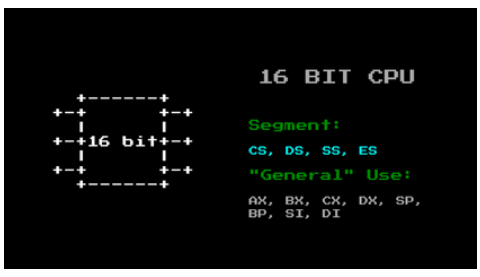
FUNCIONAMIENTO DE SEGMENTOS

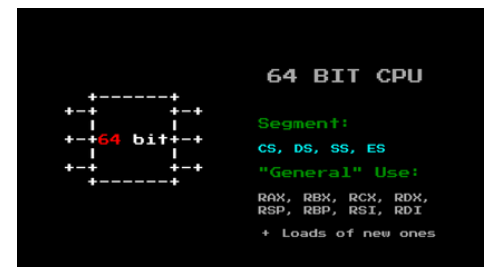
Esos segmentos funcionan variando la RAM



Permitiendo a la CPU de 16 bits, ver los 20 bits de RAM para cada valor de DS

Si nuestra llamada DS se usa como puntero dentro de la ventana de 16 bits



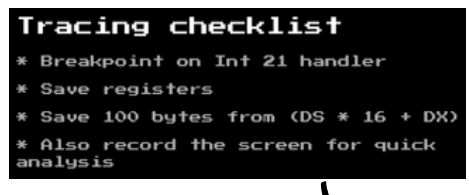


Escanea hasta encontrar el simbolo $ para detenerse

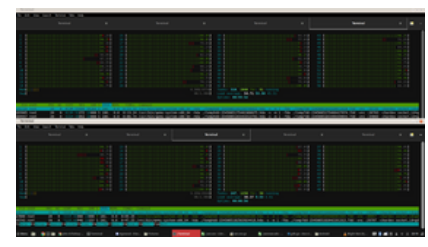
Pasa algo similar en sistemas que usan byte nulo

TRACING CHECKLIST

podemos construir una lista de "cosas por hacer" para rastrear estos programas

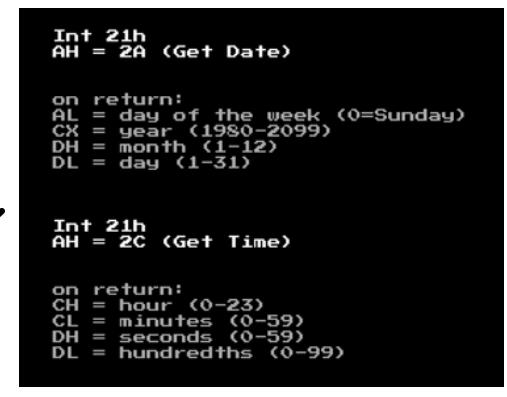


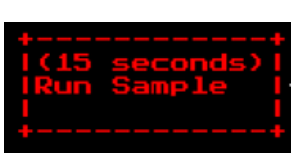
Se manda a analizar el problema mediante algunas computadoras grandes y recopilar los resultados



VERIFICAR DOCUMENTACION

Usando fuerza bruta





Implica un inconveniente el metodo

Su etapa de prueba realiza un proceso de emulación de quemu completo, el cual provoca 15 segundos en ejecutarse en la maquina virtual

EXAMINAR CODIGO

Una forma de ver el problema es observando el codigo de ejecución despues de una solicitud de fecha/hora

Nuestro DOS no posee funciones de ahorro de energia

Por lo tanto

DOS inactivo → Esta en bucle ocupado

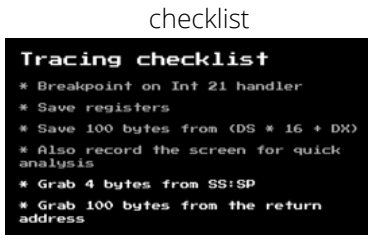
Para obtener

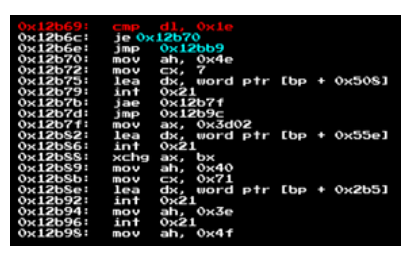
CS e IP

Obtener los registros

RETURN CODE

y creando una nueva checklist



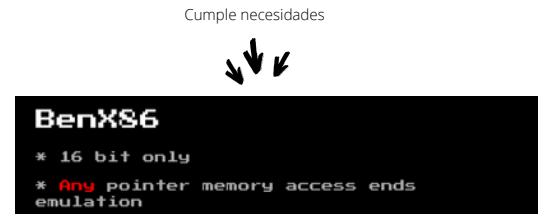


Para analizarlo se hará uso de un emulador

BENX86

Denomnado el peor emulador del mundo x86

Cumple necesidades



Sin embargo, tenía ventajas en su velocidad

Desde 1980-2005 se puede probar en 100 [ms]

3 rutas de codigo basadas en flechas

Eso nos rinde.....

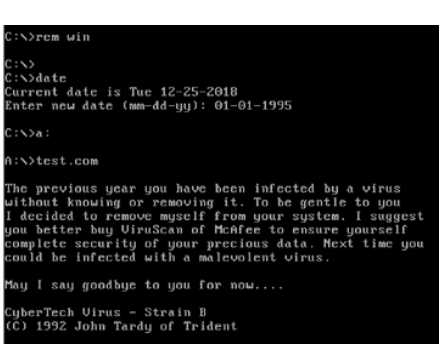
EJEMPLOS

1. Se activa el día de año nuevo e inhabilita el sistema después de mostrar un saludo.

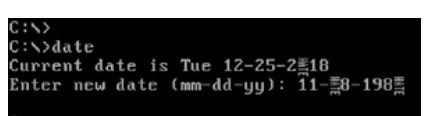
INFORME DE ARCHIVOS

1995

Se le informaba al usuario que todos sus archivos estaban infectados



El 8 de Noviembre de cualquier año



Mensaje perturbador