A DIVE INTO THE WORLD OF MS-DOS VIRUSES

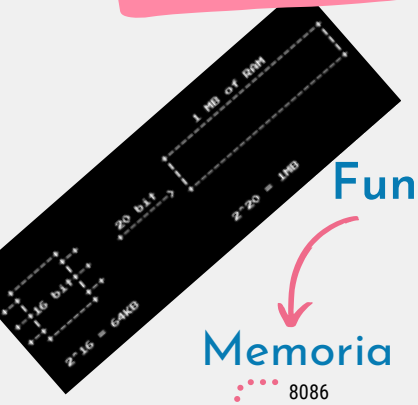
Elaborado por: Carranza Ochoa José David

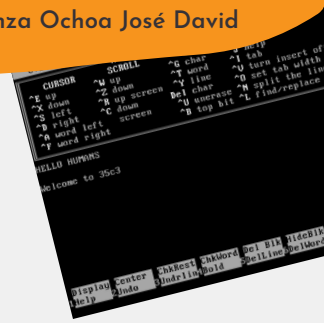
¿Qué es DOS?

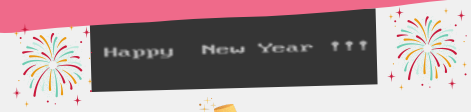
Sistema operativo antecesor a Windows creado para las computadoras personales

implementa → QBASIC - IDE de BASIC dentro de DOS como lenguaje de programación

cuentan → Compatibilidad con API que ¡puede compartir malware!







Funcionamiento

Memoria

8086 implementa

Bloques de 16 bits -> 64 KB referenciados

cuenta con

Espacio de memoria de hasta 1 MB

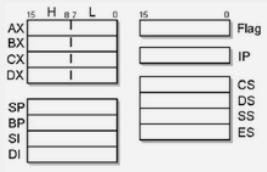
resuelven el problema

Registros

Propósito general

- Guardan datos e instrucciones
- Tamaño 16 bits
- Usados como parámetros
- AX, BX, CX, DX (parte alta y baja)
- BP, DI, SI

IP: apuntador a posición
FLAG: estado de componente



Segmento

- Redirecciona la dirección de cada bloque en ejecución
- Amplia el rango de 16 bits
- Presenta desplazamientos
- CS (code), DS (data), SS (stack), ES (extra)

Llamadas al sistema

Interrupción controlada del SO para atender un evento

Int 21h

Salto de acuerdo al registro IP la cual tiene varios parámetros

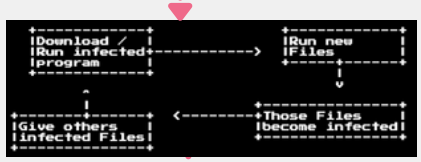
ofrece → Agregar/modificar llamadas

Programas / infecciones

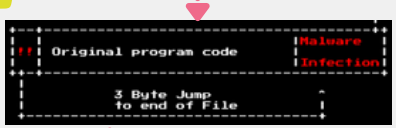
Proceso

Al cargar un programa se ejecutan ciertas acciones

pueden →
- Ser ocultos
- Mostrar su payload



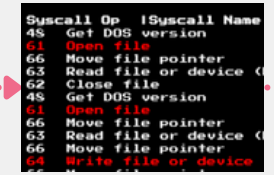
Se requieren condiciones de carga tal que Inserte JMP al inicio y existan 3 bytes de diferencia al final del archivo



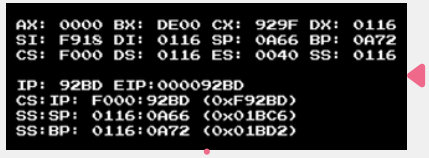
usando Llamadas al sistema para Generar persistencia e infección

Análisis de ejemplo

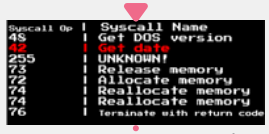
revisando Llamadas al sistema que hizo



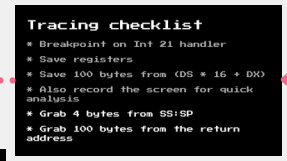
Algunos son extraños para el programa actual



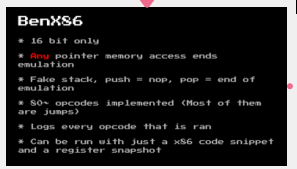
Revisando los registros se puede rastrear las interrupciones → Llamadas al sistema obteniendo



generando TO-DO list por seguir



apoyados The world's worst x86 emulator cualidades



mediante Fuerza bruta resultando Cada inicio de año se ejecuta y reinicia el computador

Ejemplos

recopilados DB - VX Heavens siendo Maliciosos y bromistas

Fuentes: 1) https://blog.benjojo.co.uk/post/dive-into-the-world-of-dos-viruses. 2) IBM PC Assembly language & programming -Peter Abel