

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

Compatibilidad con API que puede compartir malware!

cuentan

Programas / infecciones

Ejemplos

DB - VX
Heavens

siendo

Maliciosos y bromistas

recopilados

Análisis de ejemplo

revisando

Llamadas al sistema que hizo

```
syscall Op | syscall Name
4S | Get DOS version
61 | Open file
66 | Move file pointer
63 | Read file or device
62 | Close file
4S | Get DOS version
61 | Open file
66 | Move file pointer
63 | Read file or device
66 | Move file pointer
64 | Write file or device
```

Algunos son extraños para el programa actual

```
AX: 0000 BX: DE00 CX: 929F DX: 0116
SI: F918 DI: 0116 SP: 0A66 BP: 0A72
CS: F000 DS: 0116 ES: 0040 SS: 0116

IP: 92BD EIP: 000092BD
CS: IP: F000:92BD (0xF92BD)
SS: SP: 0116:0A66 (0x01BC6)
SS: BP: 0116:0A72 (0x01BD2)
```

Revisando los registros se puede rastrear las interrupciones

Llamadas al sistema

obteniendo

```
syscall Op | syscall Name
4S | Get DOS version
4S | UNKNOWN!
255 | UNKNOWN!
73 | Release memory
72 | Allocate memory
74 | Reallocate memory
74 | Reallocate memory
76 | Terminate with return code
```

generando

TO-DO list por seguir

Tracing checklist

- * Breakpoint on Int 21 handler
- * Save registers
- * Save 100 bytes from (DS * 16 + DX)
- * Also record the screen for quick analysis
- * Grab 4 bytes from SS:SP
- * Grab 100 bytes from the return address

Fuerza bruta

resultando

Cada inicio de año se ejecuta y reinicia el computador

The world's worst x86 emulator

cualidades

BenX86

- * 16 bit only
- * Any pointer memory access ends emulation
- * Fake stack, push = nop, pop = end of emulation
- * 50+ opcodes implemented (Most of them are jumps)
- * Lots every opcode that is ran
- * Can be run with just a x86 code snippet and a register snapshot

Proceso

Al cargar un programa se ejecutan ciertas acciones

pueden

- Ser ocultos
- Mostrar su payload

```
Download / IRun new
IRun infected program IFiles
IGive others Ibecome infected
Infected Files
```

Se requieren condiciones de carga

tal que

Inserte JMP al inicio y existan 3 bytes de diferencia al final del archivo

```
Original program code Malware
3 Byte Jump to end of File Infection
```

usando

Generar persistencia e infección

Llamadas al sistema

para

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

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)

Funcionamiento

Memoria

8086 implementa

Bloques de 16 bits -> 64 KB referenciados

cuenta con

Espacio de memoria de hasta 1 MB

resuelven el problema

Registros

- 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

15	H	7	L	0	15	0
AX						Flag
BX						
CX						
DX						
SP						CS
BP						DS
SI						SS
DI						ES

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

implementa

