

A DIVE INTO THE WORLD OF MS-DOS VIRUSES

by Ben Cox "Benjojo"

Rojas Terrazas Laylet
Ruiz Sanchez Miguel Angel

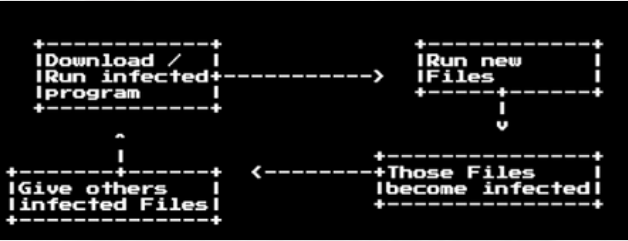
George R R
Martin escribió
Games of
Thrones en DOS

¿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

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

VX HEAVENS MALWARE

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



Cuando se ejecuta el programa el malware tiene dos opciones:

Ocultarse

Mostrar su payload



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

Ejemplo Rápido

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

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

Esto ocurre la mayor parte del tiempo

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

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

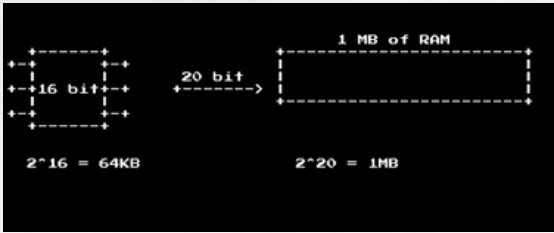
LLAMADAS AL SISTEMA

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

Las llamadas al sistema devuelven los valores como registros al programa

la infección ocurre mediante

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



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



4 registros de segmentación

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

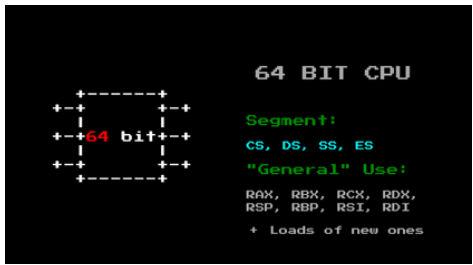
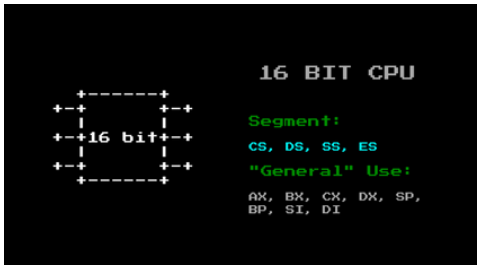
FUNCIONAMIENTO DE SEGMENTOS

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

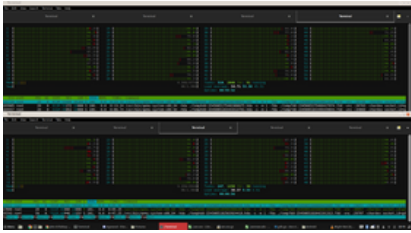
Pasa algo similar en sistemas que usan byte nulo

TRACING CHECKLIST

Tracing checklist

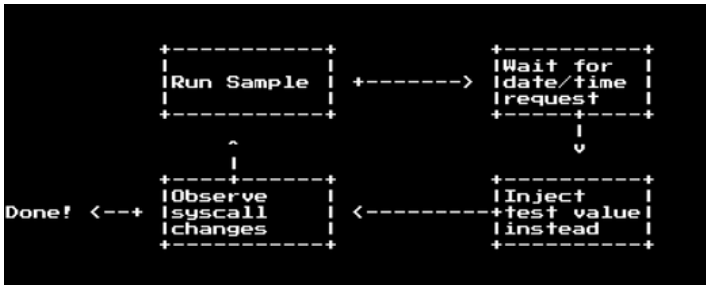
- * Breakpoint on Int 21 handler
- * Save registers
- * Save 100 bytes from (DS * 16 + DX)
- * Also record the screen for quick analysis

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



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

VERIFICAR DOCUMENTACION



Usando fuerza bruta

Int 21h
AH = 2A (Get Date)

on return:
AL = day of the week (0=Sunday)
CX = year (1980-2099)
DH = month (1-12)
DL = day (1-31)

Int 21h
AH = 2C (Get Time)

on return:
CH = hour (0-23)
CL = minutes (0-59)
DH = seconds (0-59)
DL = hundredths (0-99)

Implica un inconveniente el metodo

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

RETURN CODE

Para obtener

CS e IP

Obtener los registros



y creando una nueva checklist

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

```
0x12b69:  cmp  dl, 0x1e
0x12b6c:  je  0x12b70
0x12b6e:  jmp  0x12b69
0x12b70:  mov  ah, 0x4e
0x12b72:  mov  cx, 7
0x12b75:  lea  dx, word ptr [bp + 0x508]
0x12b79:  int  0x21
0x12b7b:  jae  0x12b7f
0x12b7d:  jmp  0x12b9c
0x12b7f:  mov  ax, 0x3d02
0x12b82:  lea  dx, word ptr [bp + 0x55e]
0x12b86:  int  0x21
0x12b88:  xchg ax, bx
0x12b89:  mov  ah, 0x40
0x12b8b:  mov  cx, 0x71
0x12b8e:  lea  dx, word ptr [bp + 0x2b5]
0x12b92:  int  0x21
0x12b94:  mov  ah, 0x3e
0x12b96:  int  0x21
0x12b98:  mov  ah, 0x4f
```

Para analizarlo se hará uso de un emulador

BENX86

Denomnado el peor emulador del mundo x86

Cumple necesidades

Happy New Year !!!

INFORME DE ARCHIVOS

Se le informaba al usuario que todos sus archivos estaban infectados

El 8 de Noviembre de cualquier año

1995

Sin embargo, tenía ventajas en su velocidad

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

3 rutas de código basadas en flechas

Eso nos rinde....

Mensaje perturbador

```
h:\>test.com
I am an assassin, I want to and shall kill you!
I also hate Aladdin and will also kill it!
I will eliminate you with the touch of just one finger
Look at my revenge! Crying wont help you!
I am a dangerous virus, I live! I am created by:
The [HACKING HELL] !!!!
Fear me! I am more powerfull than GOD!
```

```
C:\>rem win
C:\>
C:\>date
Current date is Tue 12-25-2018
Enter new date (mm-dd-yy): 01-01-1995
C:\>a:
A:\>test.com
The previous year you have been infected by a virus
without knowing or removing it. To be gentle to you
I decided to remove myself from your system. I suggest
you better buy ViruScan of McAfee to ensure yourself
complete security of your precious data. Next time you
could be infected with a malevolent virus.
May I say goodbye to you for now....
CyberTech Virus - Strain B
(C) 1992 John Tardy of Trident
```

```
C:\>
C:\>date
Current date is Tue 12-25-2018
Enter new date (mm-dd-yy): 11-08-1988
```