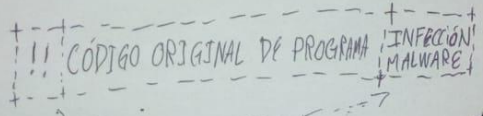
- Syscalls = llamados al sistema
- Int 21h Syscalls
  - Estas funciona llamando interrupciones en las que el programa le pedirá al CPU saltar a otra sección del sistema de memoria para manejar algo

TRACING CHECKLIST

* Punto de Interrupción en el manejador 21
* Guardar registros
* Guardar 100 bytes desde CDS * 16 + DX)
* Grabar pantalla para análisis rápido
* Tomar 4 bytes desde SS:SP
* Tomar 100 bytes desde la dirección de devolución

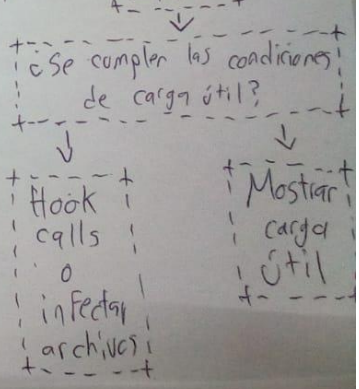
- Infectar archivos es súper sencillo
- Sólo tienes que insertar un JMP al inicio del programa y agregar los datos al final



Salto de 3 bytes al final del Archivo

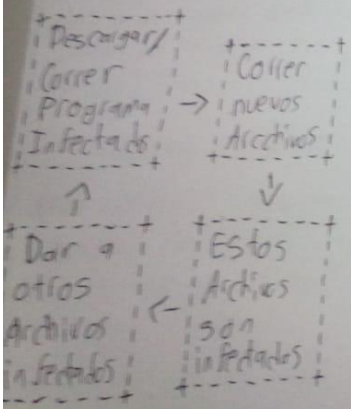
- Algunos códigos son más listos y buscan "espacio libre" en un binario y se reescriben ahí, evitando hacer más grande el archivo una posible señal de alerta para los antivirus

- En tiempo de ejecución el malware tiene 2 opciones
  - permanecer oculto e infectar nuevos archivos
  - Mostrar su carga útil



UNA INMERCIÓN EN EL MUNDO DE LOS VIRUS MS-DOS

- Flujo de Propagación

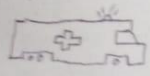


La sotileza es sencial para evitar detección

- DOS es el sistema operativo siguiente a CP/M
- Algunos proveedores de DOS compartían API, lo que significa que han compartido Malware
- Esta es la era de la "Computadora beige" y del teclado Modelo M
- ¡George R R Martin utilizó WordStar en DOS para escribir el libro!

- Pero a veces la vida usando DOS no era tan buena y pasaban cosas extrañas
- En algunos ejemplos se reproducía una pequeña melodía en el altavoz de la PC mientras se imprime TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO

• Otros son un poco más "lindos" como por ejemplo una ambulancia en arte ASCII desplazandose a través de la pantalla



• Gracias a un grupo de activistas "VX Heaven" tenemos un gran archivo histórico de DOS malware hasta que la Policía Ukraniana asaltó el sitio

• Afortunadamente, todavía podemos encontrar bases de datos en sitios web todavía pagulais

• ¡Algunas cargas útiles son bastante bonitas!

HAVOC THE CHAOS

256 colores

Happy New Year!!!

Este ejemplo se activa en año nuevo y solo te muestra lo de arriba entonces ahí

• Soy un asesino; Quiero matarte y te mataré!
¡Además odio a Aladdin y también lo mataré!
Te eliminaré con el toque de un solo dedo
¡Obstruiré mi Venganza!
¡Llorar no te ayudará!
Soy un virus peligroso
¡Yo vivo! Fuí creado por
¡¡¡; El INFIERNO ~~DE LA~~ PIRATERIA!!!!
¡Témeme! ¡Soy más poderoso que DIOS!

• Esta es la versión Navy Seal Copy-pasta del malware DOS