Notas sobre Altar 797

La descripcion del virus se puede encotrar en:

> https://www.virusign.com/details.php?hash=c99cedd1cf3092155ff9e332414be9573f7ce70f83fe27b22525947

Escaneando el virus de forma estatica con la herramienta PPEE, podemos ver que:

- Esta compilado para una arquitectura de 32bits. (x86) Intel 386
- Se le han quitado absolutamente todas las propiedades posibles
- En la cabecera *NT header > optional header* aparecen:
  - Member Value Comment
  - *Magic:* `010B` PE32
  - *AddressOfEntryPoint:* 00001000 CODE (last section)
- La lista de secciones consta de una unica seccion, llamada: CODE
  - Aparecen los siguientes campos interesantes:
    - *VirtualAddress:* `00001000`
    - *VirtualSize:* `00001000`
    - *RawAddress:* `00000600`
    - *RawSize:* `00000600`
- Buscando cadenas en el archivo, vemos que hay:
  - *[Altar] by T-2000 / Immortal Riot:* Parece la atribucion del archivo a los usuarios/grupos
  - *Awaiting the sacrifice. . . :* Parece algun tipo de texto que se le muestra al usuario, para que ingrese dinero. Puede que este malware sea alguna especie de Ransom?
  - *.EXE:* De alguna forma, se genera un ejecutable, o se clona el existente.
- Escaneando el virus de forma dinamica con x64dbg nos crashea en el debugger.
  - Investigando el posible motivo de este problema, buscando el nombre del virus en internet, es un virus que se ha hecho para windows 9X. entonces, ese puede ser el principal motivo por el que no nos funcione.