

HDC

Bueno llegamos al día del Wargame número 2. A diferencia del primero, en el que corrían para lograr descifrar los contenidos antes que los otros competidores, éste no tendría sentido hacerlo de esa manera porque un malware no se crea a costa de presión temporal sino con total ingenio. Así que las reglas cambiarán un poco, en sentido también de experimentar cómo puede salir esto.

Para no hablar más y hacerlo pesado, voy a proponer las reglas que deben leer por completo antes de empezar:

1-El objetivo: Crear un malware (puede ser un PoC). Ganará aquel que haya sido creado con mayor ingenio y tenga la mejor presentación y quedará descalificado el malware que no ande.

2-Sólo se puede mandar un malware por persona. Sólo se validará el primer mail.

3-La fecha de finalización es el Domingo 29/2 a las 23:59hs (GMT-3). El mail que se envíe después será descalificado.

4-El mail debe estar compuesto de:

- Código fuente original del malware
- Comprimido con los archivos, que deben estar sin formato, y un .txt dando a saber los formatos de cada archivo
- Un informe detallado de cómo funciona, qué es lo que les gusta del malware y todo lo que quieran agregar sobre el código, la ejecución y demases. También es necesario hacer un segmento sobre qué le mejorarían al malware para que sea más eficiente o eficaz. Por favor, usen la mejor ortografía y comprensión que puedan.

5-El código debe:

- Ser legible (en caso de que haya una ofuscación de código, agregar el archivo con el código ofuscado y otro con el código legible).
- El núcleo del malware sólo puede ser escrito en Batch o en C. Los demás lenguajes quedan fuera de término.
- Estar bien comentado y ordenado.

6-Seremos 2 jueces (me ayudará un amigo para que no sea algo tan subjetivo) , habrá 3 ganadores, y cada uno se llevará una licencia de Kaspersky AntiVirus original.

Consejos: usen hasta la última hora para mejorar su código y su informe, pero háganlo responsablemente. Nunca un código andará a las primeras, necesitarán pruebas y eso lleva la mayor

parte del tiempo. Modularizen su código, cada función pruébenla por separado para ver qué es lo que no anda. Pueden hacer preguntas sobre las consignas pero no sobre cómo puede funcionar esto o lo otro. No se queden atrás con el informe y busquen en Google cosas que no hayamos visto en el curso para sorprendernos, y no se maten por cosas que no pueden hacer ya que muchas veces es que tenemos un punto de vista errado de la situación. Sean creativos y disfruten estas dos semanas.

¡Happy hacking!:)