Estudio completo de virus simples

por

AkirA

Información

Programa:	Virus del Kazaa (ponerse contacto conmigo)
Tamaño:	El tamaño no importa XDDDDD
Herramientas:	1. Ollydbg 1.09c
Dificultad:	NewBie avanzado

Introducción

Hola amigos!!!! Bienvenidos a la 36 entrega del curso de AkirA sobre protecciones comerciales.

Hoy vamos a hablar de un tema curioso. Hace poco un amigo se quiso instalar unos parches para sus juegos (de entre ellos, un Parche NO-CD de praetorinas (62 K) y uno para el Pax Payne -no recuerdo exactamente que nombre-).

El caso es que este chico tenia el Norton Antivirus 2003 sin actualizar. Y no dijo nada. Cuando lo probamos en casa de otro amigo el antivirus (que era el mismo pero actualizado hasta la fecha) salto como un cosaco y dijo que no le dejaba meter el parche al ordenador porque tenia un virus.

Mi primer colega actualizo el antivirus, y ahora si que lo reconoció, pero el programa ya estaba instalado y el antivirus decía que no podía ni borrarlo, ni ponerlo en cuarentena, ni nada de nada (y se quedó sin solución) Ya entenderéis porque...

En ese mismo instante me dije, ¿porqué no intentarlo? ¿Por qué no abrirlo con el Olly e intentar estudiarlo?

Y me puse manos a la obra XDD

Por suerte eran virus sin demasiadas protecciones. (no tenían encriptaciones especial de la tabla de datos, ni se anexaban a ningún archivo, y por supuesto nada de polimorfismo ni nada de eso (ya lo veréis).

Mas que virus, son programas maliciosos. Los dos son muy semejantes, incluso puede que estén hechos por la misma persona, aunque uno te reinicia una y otra vez el Pc y otro te instala una BackDoor.

Desconozco si tienen nombre. Yo los he llamado Mscvrt32.exe y ExitW.exe

Me alegre mucho cuando comprendí lo que hacían estos virus y cuando por lógica supe la manera de quitarlos del PC (ahora primer colega, escanea el Pc y ya indica Virus = 0 XDD)

Quiero dedicarle este tuto, (muy especial para mi, porque supone un paso más en los temas importantes por hablar) a JOE CRACKER al que tengo una gran admiración (mirad su pagina y sus mas de 60 tutos!!! XD) y también se lo quiero dedicar a un gran colega y cracker SPARK, (el cual debe escribir muy rápido ya que trabaja en varios Ezines XDD)

Sobre cualquier duda, escribirme a mi email atalasa@hotmail.com

Nota: si necesitáis información sobre Ollydbg buscar en la pagina de Joe Cracker: www.iespana.es/ollydbg esta es la mejor página que hay sobre el tema, de hecho gracias ha ella yo hago todos es tos proyectos en olly

Comentario del Programa

Por supuesto el disclaimer de turno. Vamos a ver, no es que no me haga responsable de la utilización de esta información, es que directamente paso del tema, el único propósito de todo esto es de carácter educativo.

A fin de cuentas, si lo que quieres es crackear un programa, pues te bajas el crack y punto, pero si vas a leer este tutorial es porque tu objetivo es aprender. Eso es lo que nos motiva, el comprender como funcionan las cosas o como están hechas por dentro, y por supuesto el subidón de haberle ganado a un equipo de ingenieros diseccionando un objeto que ellos habían diseñado y del cual no sabemos nada.

Manos a la Obra
Comienza el asedio....

Hola a todos y bienvenidos a la 36 entrega del curso de AkirA.

Para analizar un virus debemos tomar una serie de precauciones.

Lo primero es instalar una maquina virtual, yo utilizo VMware-workstation-4.0.5-6030, aunque tu deberías bajarte la última versión. Bien, aquí podremos hacer todas las particiones que queramos, ya que lo que pase en ellas no afectaran a la maquina real, pues que se tratan de particiones “virtuales”.

Una vez instalado el programa haz una partición para windows (yo te aconsejo para windows Me, 98 o 95, que son los mas vulnerables a todo) e instala dicho sistema operativo como si lo estuvieses haciendo en una maquina real.

Sobre VMware-workstation-4.0.5-6030 puedes encontrar muchos manuales en internet. La verdad es que es un programa tan fácil e intuitivo que no perderé el tiempo explicándolo. Es un programa que vale lo que cuesta.

Una vez que hayáis hecho esto, copias el Ollydbg y el primer virus. El ExitW.

Cargamos el Olly y damos a open y seleccionamos el virus. (cada uno el nombre del archivo que tenga)

Bien, lo primero que observé del virus es que si das al botón derecho y pinchas en search for – all referens strings veréis dos cosas muy llamativas. Una es una dirección del registro de windows y otra es una frase que dice Runtime VC++ etc, Ya sabemos dos cosas. Una, que el virus fue compilado en VC++ (lo cual es muy raro porque casi todo lo que he visto suele estar hecho en VB) y que el virus debe acceder al registro de windows (en concreto a una dirección muy importante que luego veremos)

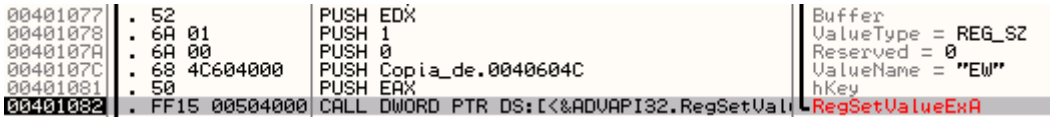
Id haciendo paso a paso lo que os digo e iremos rápido:

Poned un breakpoint aquí:

Esta api ya la hemos visto anteriormente, se utiliza para acceder a una key del registro de windows. (recordar que el registro de windows es una especie de base de datos donde se guarda toda la información y configuración de windows en forma de árbol jerárquico. Seguro que en los ezines de DISIDENTS encontrareis mucha información si queréis profundizar en este tema, o consultar los tutos anteriores AkirA que hablan del registro)

Observar detenidamente la dirección. Esa dirección es muy importante. Cada clave de esa dirección es un programa que windows debe cargar en el arranque del ordenador.

Seguimos trazando con f8 hasta llegar a esta dirección:



Esa api, que también hemos visto anteriormente, se utiliza para establecer una clave dentro de una key del registro de windows.

Al parecer, el dichoso programita, está metiendo una entrada llamada EW y que contiene un nombre de archivo ExitW.exe. Pues a partir de ahora, cada vez que se inicie el ordenador se cargará un programa llamado de esa manera, aunque el programa todavía no existe.

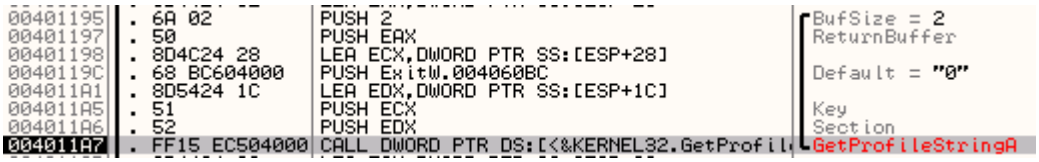
Sigamos observando...

Ahora tracemos con f7 hasta llegar a esta dirección:

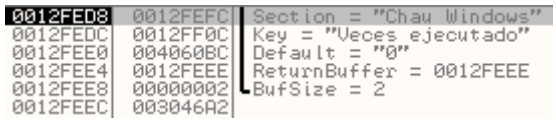
Estas apis que tenéis ante vosotros son las típicas apis de GDI (interfaces para dispositivos gráficos) Aquí no hace falta que lo analicemos muy a fondo, porque se ve claramente que el programa va a pintar algo en pantalla y sobretodo cuando trazando con f8 llegamos a "Textout" y sale ese mensaje de "bye, bye, .." etc

Es para poner un mensajito en bonito.

Si seguimos ejecutando con f7 llegamos hasta esta zona:



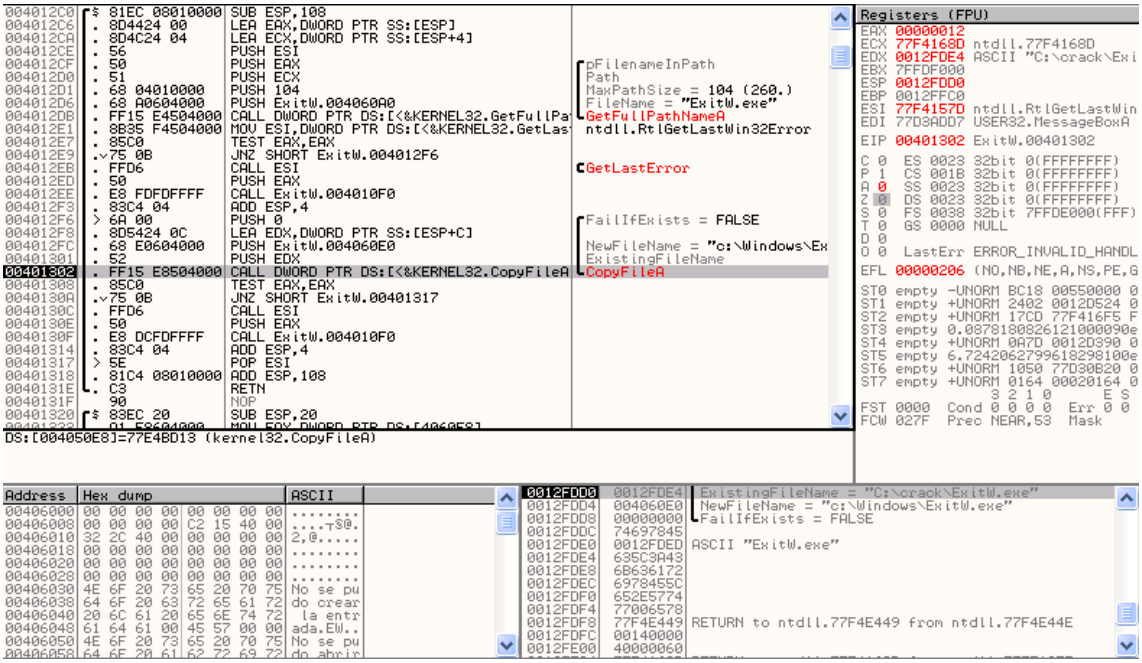
Donde vemos información interesante.



Esa api se utiliza para recoger valores de tipo string tanto en archivos INI como en el registro de windows, también las hemos visto con anterioridad en otros tutos.

Parece ser que el virus lleva la cuenta de cuantas veces se ha accedido al programa, y que contiene esos valores con estas apis.

Seguimos trazando con f7 (saltarse las apis con f8 claro) y llegamos a la zona más importante del virus:



Fijaos bien en ese “GetFullPathName” y en la siguiente Api “CopiFile”

Bien, una posible interpretación sería la siguiente (aunque no tiene porque ser definitiva):

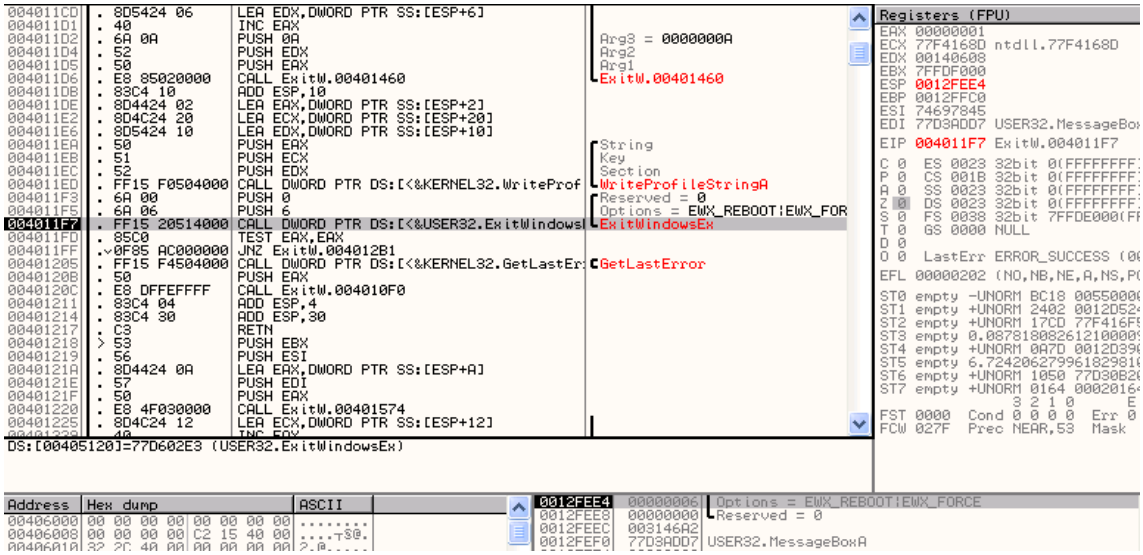
El virus controla si se ejecuta por primera vez con GetProfileString, si es así, obtiene la dirección donde se está ejecutando que GetFull... y después hace una copia del archivo a C:\windows\ExitW.exe

En caso de que no sea la primera vez, se salta eso de copiarse.

Fijaos que la dirección de destino (lo que es el nombre del archivo) coincide con la entrada que creo el virus en la key RUN al principio (eso es fijo, estático).

Sigamos trazando con f7 (saltarse las apis con f8) para ver que más va haciendo el virus.

Entonces llegaremos a esta zona:



Vemos que ejecuta la función ExitWindowsEx y vemos que los flags son" Reboot y force.

Osea, que lo que el virus hace es forzar al ordenar a que se reinicie una y otra vez y como cada vez que se reinicia se vuelve a cargar el programa porque tiene una entrada en el registro.... pues vuelta a empezar. ".

Anda!!!!!! como el Blaster!!! Que jodio!!

Ya sabemos lo que hace el virus y lo tenemos totalmente pillao, ahora vamos a por él.

Vamos a solucionar el problema (vamos a quitar el virus):

1. Reiniciar windows (el virtual infectado claro) y mantener presionado f8. Y seleccionar arrancar en "modo seguro" . Lo primero, será borrar el archivo C:\windows\ExitW.exe.
2. Ahora ya dejaríamos de estar infectados, pero por limpieza vamos a limpiar también el registro.
3. Pinchad en Inicio-ejecutar y escribid Regedit, y dirigíos como en el explorador de windows a esta dirección
4. Allí encontrareis una entrada llamada EA y contiene el nombre del archivo ExitW.exe. Suprimirlo.

Alguno podrá pensar. Oye ¿y no te olvidas de las entradas donde se guardan las veces que se ha ejecutado el virus? Muy bien, pero es que esas entradas precisamente no las borramos, porque como el virus ya se ha ejecutado mas de una vez, no se copiará con CopyFile y seremos totalmente inmunes al virus en futuros descuidos (osea, archivos con otro nombre pero mismo virus).

Ahora podéis probar vosotros mismo con el mscvrt32.exe. Es muy extendido por el Kazaa (más de lo que pensáis) ocupa unos 62 k y tiene muchos nombres, sobretodo tipo Parche No-CD Praetorians.exe o el nombre que sea XDD

Cosas a tener en cuenta para los que no tengáis miedo a analizarlo.

1. el virus se copia en C:\windows\system32\mscvrt32.exe (deberíais hacer un buscar el archivo, no vaya a ser que estéis infectados)

2. este virus no te reinicia el ordenador, te instala una BacKdoor donde te pueden robar archivos a incluso instalarte cosas de forma remota.

3. En el registro se guarda en dos sitios. (el primero ya lo habéis visto arriba), el segundo es también un ... algo/algo/..RUN pero este Run arranca los servicios de windows.

Esto es muy importante. Los antivirus no pueden eliminar ni tocar este programa porque son servicios, de windows, es decir el propietario del programa (el que lo lanza) es SYSTEM, y aunque tu seas administrador no podrás tocar este archivo, porque el SYSTEM es el Dios de tu ordenador. Por eso el antivirus no puede ni tocarlo, ni borrarlo, ni ponerlo en cuarentena.

4. Para borrarlo sigue el mismo procedimiento que con el otro (osea arranca en MODO SEGURO, borra el archivo y borra todas las entradas del registro que tengan algo que ver con el programa XD)

Nota:

Bueno espero que te hayas divertido y sobre todo que hayas aprendido mucho que es de lo que se trata, que te sirva de ejemplo para que tu también puedas hacerlo, desde luego no hay comparado como coger un programa, abrirlo, ver un montón de código por todas partes y manejar lo que otros ingenieros han hecho, tu solo, por ti mismo.

Bueno, si quieres comentarme algo escríbeme a atalasa@hotmail.com

Quiero agradecer a Ricardo Narvaja y a Makkako por su increíble esfuerzo de escribir tantísimos y buenos tutoriales que nos han llevado a aprender tanto, agradecer al Profesor X por sus famosas compilaciones, Y también agradecer a Joe Cracker su pagina muy, muy actualizada, y el esfuerzo de divulgación de olly que esta haciendo, ha sido muy importante en mis progresos como cracker.

Chao!!

Espero que hayan disfrutado leyendo este tutorial y que les sirva para incrementar sus habilidades, pero recuerden, lean muchos tutoriales, practiquen, estudien y CRACKEAR será mucho más.