

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 alegro 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)

```
00401024 PUSH ExitW.00406070 ASCII "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
```

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

Poned un breakpoint aquí:

```
0040101F . 50 PUSH EAX
00401020 . 6A 02 PUSH 2
00401022 . 6A 00 PUSH 0
00401024 . 68 70604000 PUSH ExitW.00406070
00401029 . 68 02000000 PUSH 00000002
0040102E . 894C24 24 MOV DWORD PTR SS:[ESP+24],ECX
00401032 . 66:895424 28 MOV WORD PTR SS:[ESP+28],DX
00401037 . FF15 00504000 CALL DWORD PTR DS:[&ADVAPI32.RegOpenKeyExA] RegOpenKeyExA
```

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:

```
00401077 . 52 PUSH EDX
00401078 . 6A 01 PUSH 1
0040107A . 6A 00 PUSH 0
0040107C . 68 4C604000 PUSH Copia_de.0040604C
00401081 . 50 PUSH EAX
00401082 . FF15 00504000 CALL DWORD PTR DS:[&ADVAPI32.RegSetValueExA] RegSetValueExA
```

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:

00401341	. 894C24 24	MOV DWORD PTR SS:[ESP+24],ECX	
00401345	. 895424 28	MOV DWORD PTR SS:[ESP+28],EDX	
00401349	. 894424 2C	MOV DWORD PTR SS:[ESP+2C],EAX	
0040134D	. FF15 0C514000	CALL DWORD PTR DS:[&USER32.GetDesktopW	GetDesktopWindow
00401353	. 8BF8	MOV EDI,EAX	
00401355	. 57	PUSH EDI	hWnd
00401356	. FF15 10514000	CALL DWORD PTR DS:[&USER32.GetWindowDC	GetWindowDC
0040135C	. 8D4C24 10	LEA ECX,DWORD PTR SS:[ESP+10]	
00401360	. 8BF0	MOV ESI,EAX	
00401362	. 51	PUSH ECX	pRect
00401363	. 57	PUSH EDI	hWnd
00401364	. FF15 14514000	CALL DWORD PTR DS:[&USER32.GetWindowRe	GetWindowRect
0040136A	. 68 FF000000	PUSH 0FF	Color = <LIGHTRED>
0040136F	. FF15 18504000	CALL DWORD PTR DS:[&GDI32.CreateSolidB	CreateSolidBrush
00401375	. 8D5424 10	LEA EDX,DWORD PTR SS:[ESP+10]	
00401379	. 50	PUSH EAX	hBrush
0040137A	. 52	PUSH EDX	pRect
0040137B	. 56	PUSH ESI	hDC
0040137C	. FF15 18514000	CALL DWORD PTR DS:[&USER32.FillRect]	FillRect
00401382	. 6A 00	PUSH 0	Color = <BLACK>
00401384	. 6A 03	PUSH 3	Width = 3
00401386	. 6A 00	PUSH 0	PenStyle = PS_SOLID
00401388	. FF15 24504000	CALL DWORD PTR DS:[&GDI32.CreatePen]	CreatePen
0040138E	. 50	PUSH EAX	hObject
0040138F	. 56	PUSH ESI	hDC
00401390	. FF15 10504000	CALL DWORD PTR DS:[&GDI32.SelectObject	SelectObject
00401396	. 8B1D 28504000	MOV EBX,DWORD PTR DS:[&GDI32.MoveToEx	GDI32.MoveToEx
0040139C	. 6A 00	PUSH 0	pPoint = NULL
0040139E	. 6A 00	PUSH 0	Y = 0
004013A0	. 6A 00	PUSH 0	X = 0
004013A2	. 56	PUSH ESI	hDC
004013A3	. FF03	CALL EBX	MoveToEx
0040130E	. 8B4424 10	MOV ECX,DWORD PTR SS:[ESP+10]	

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:

00401195	. 6A 02	PUSH 2	BufSize = 2
00401197	. 50	PUSH EAX	ReturnBuffer
00401198	. 8D4C24 28	LEA ECX,DWORD PTR SS:[ESP+28]	
0040119C	. 68 BC600000	PUSH ExitW.004060BC	Default = "0"
004011A1	. 8D5424 10	LEA EDX,DWORD PTR SS:[ESP+10]	
004011A5	. 51	PUSH ECX	Key
004011A6	. 52	PUSH EDX	Section
004011A7	. FF15 EC504000	CALL DWORD PTR DS:[&KERNEL32.GetProfil	GetProfileStringA

Donde vemos información interesante.

0012FE08	0012FEFC	Section = "Chau Windows"
0012FEDC	0012FF0C	Key = "Veces ejecutado"
0012FEE0	004060BC	Default = "0"
0012FEE4	0012FEEE	ReturnBuffer = 0012FEEE
0012FEE8	00000002	BufSize = 2
0012FEEC	003046A2	

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:

The screenshot displays a debugger interface with three main panes:

- Assembly Window:** Shows assembly instructions. Key instructions include:
 - 004012C0: SUB ESP, 108
 - 004012C2: LEA EDI, DWORD PTR SS:[ESP]
 - 004012C4: LEA ECX, DWORD PTR SS:[ESP+4]
 - 004012CE: PUSH ESI
 - 004012D0: PUSH EAX
 - 004012D2: PUSH ECX
 - 004012D4: PUSH 104
 - 004012D6: PUSH ExitW.004060A0
 - 004012D8: CALL DWORD PTR DS:[<&KERNEL32.GetFullPa
 - 004012DA: MOV ESI, DWORD PTR DS:[<&KERNEL32.GetLas
 - 004012E0: TEST EAX, EAX
 - 004012E2: JNZ SHORT ExitW.004012F6
 - 004012E4: CALL ESI
 - 004012E6: PUSH EAX
 - 004012E8: CALL ExitW.004010F0
 - 004012EA: ADD ESP, 4
 - 004012EC: LEA EDI, DWORD PTR SS:[ESP+C]
 - 004012EE: PUSH ExitW.004060E0
 - 004012F0: PUSH EDX
 - 004012F2: CALL DWORD PTR DS:[<&KERNEL32.CopyFileA
 - 004012F4: TEST EAX, EAX
 - 004012F6: JNZ SHORT ExitW.00401317
 - 004012F8: CALL ESI
 - 004012FA: PUSH EAX
 - 004012FC: CALL ExitW.004010F0
 - 004012FE: ADD ESP, 4
 - 00401300: POP ESI
 - 00401302: ADD ESP, 108
 - 00401304: RETN
 - 00401306: NOP
 - 00401308: SUB ESP, 20
 - 0040130A: MOV EDI, DWORD PTR DS:[004060E0]
- Registers (FPU) Window:** Shows register values:
 - EAX: 00000012
 - ECX: 77F41680 ntdll.77F41680
 - EDX: 0012FDE4 ASCII "C:\crack\Exi
 - EIP: 00401302 ExitW.00401302
- Hex Dump Window:** Shows memory contents with ASCII interpretation:
 - Address 00406000: Hex 00 00 00 00 00 00 00 00, ASCII "....."
 - Address 00406010: Hex 32 2C 40 00 00 00 00 00, ASCII ".t30."
 - Address 00406018: Hex 00 00 00 00 00 00 00 00, ASCII "2.B...."
 - Address 00406020: Hex 00 00 00 00 00 00 00 00, ASCII "....."
 - Address 00406028: Hex 00 00 00 00 00 00 00 00, ASCII "....."
 - Address 00406030: Hex 4E 6F 20 73 65 20 70 75, ASCII "No se pu
 - Address 00406038: Hex 64 5F 20 63 72 65 61 72, ASCII "do creat
 - Address 00406040: Hex 20 6C 61 20 65 6E 74 72, ASCII "la entr
 - Address 00406048: Hex 61 64 61 00 45 57 00 00, ASCII "ada.EW..
 - Address 00406050: Hex 4E 6F 20 73 65 20 70 75, ASCII "No se pu
 - Address 00406058: Hex 64 5F 20 61 62 72 63 72, ASCII "do abstr

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:

The screenshot shows a debugger window with the following assembly code:

```

004011C0 . 8D5424 06 LEA EDX,DWORD PTR SS:[ESP+6]
004011C1 . 48 INC EAX
004011C2 . 6A 0A PUSH 0A
004011C4 . 52 PUSH EDX
004011C5 . 58 PUSH EAX
004011C6 . E8 95020000 CALL ExitW.00401460
004011C8 . 83C4 10 ADD ESP,10
004011DE . 8D4424 02 LEA EAX,DWORD PTR SS:[ESP+2]
004011E2 . 8D4C24 20 LEA ECX,DWORD PTR SS:[ESP+20]
004011E6 . 8D5424 10 LEA EDX,DWORD PTR SS:[ESP+10]
004011EA . 50 PUSH EAX
004011EB . 51 PUSH ECX
004011EC . 52 PUSH EDX
004011ED . FF15 F0504000 CALL DWORD PTR DS:[&&KERNEL32.WriteProf
004011F3 . 6A 00 PUSH 0
004011F5 . 6A 06 PUSH 6
004011F7 . FF15 20514000 CALL DWORD PTR DS:[&&USER32.ExitWindows
004011FD . 85C0 TEST EAX,EAX
004011FF . 70F85 AC000000 JNZ ExitW.004012B1
00401205 . FF15 F4504000 CALL DWORD PTR DS:[&&KERNEL32.GetLastEr
0040120B . 50 PUSH EAX
0040120C . E8 0FFEFFFF CALL ExitW.004010F0
00401211 . 83C4 04 ADD ESP,4
00401214 . 83C4 30 ADD ESP,30
00401217 . C3 RETN
00401218 > 53 PUSH EBX
00401219 . 56 PUSH ESI
0040121A . 8D4424 0A LEA EAX,DWORD PTR SS:[ESP+A]
0040121E . 57 PUSH EDI
0040121F . 50 PUSH EAX
00401220 . E8 4F030000 CALL ExitW.00401574
00401225 . 8D4C24 12 LEA ECX,DWORD PTR SS:[ESP+12]
00401227 . 48 INC EAX

```

The registers window shows the following values:

```

Registers (FPU)
EAX 00000001
ECX 77F4168D ntdll.77F4168D
EDX 00140608
EBX 77FDF000
ESP 0012FEE4
EBP 0012FFC0
ESI 74697845
EDI 7703A007 USER32.MessageBox
EIP 004011F7 ExitW.004011F7

```

Below the assembly code, there is a hex dump of memory at address 0012FEE4:

```

Address Hex dump ASCII
00406000 00 00 00 00 00 00 00 00 .....
00406008 00 00 00 00 C2 15 40 00 .....t30.
00406010 3F 2F 4B 0A 0A 0A 0A 0A >.B.....

```

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 escíbeme 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.