--[MISSION BRIEFING]--

Quiero empezar saludando a todos los listeros de CrackSLatinos y a ti que te tomas el tiempo y la molestia de leer este sencillo tutorial. Les cuento que estuve buscando en la red un sistema para consultorio médico y me topé con este programa que me agrado bastante por su sencillez en el diseño y flexibilidad, el autor te permite descargar la versión shareware que tiene algunas limitaciones pero nada del otro mundo, así que me anime a echarle mano y dejarlo completamente funcional.

--[SPECIFICATIONS]--

Víctima:	**Agenda Medica Profesional**
Versión	**v5.6**
URL:	**http://www.agendamedicapro.com/**
Protección:	**Shareware**
Dificultad:	**Newbie**
Herramientas:	**OllyDBG v1.10 / RDG Packer Detector v0.7.2 2014 / Hex Workshop v6.7.3**
Objetivo::	**Registrarlo localmente y en Red.**
Reverser:	**DavicoRm**
Lugar/Fecha:	**Perú - 29/01/2014**

-[VICTIM INFO]-

Agenda Médica es un programa para Windows desarrollado para la administración de pacientes en un consultorio médico.

El programa puede ser utilizado por un único profesional, o por varios que utilicen una misma computadora o varias conectadas en red, permitiendo proteger la información almacenada por cada uno de ellos. Además se destaca el poder implementar como soporte de datos las plataformas Microsoft Access, SQL Server, Oracle y MySQL, para ambientes cliente-servidor más exigente.

Entre sus opciones principales cuenta con la posibilidad de administrar las Historias Clínicas de cada paciente, gestionar Turnos y eventos según fechas y horarios, organizar múltiples imágenes digitales asociadas a cada registro, diseñar Ordinogramas para el seguimiento en consultorios odontológicos, y personalizar los ítems de cada una de las fichas a almacenar permitiendo su utilización en diversas especialidades médicas.

Agenda Medica también cuenta con un completo sistema para la creación y administración de un Vademécum Personal, una guía de consulta de códigos de diagnóstico CIAP-2 (*1), CIE-10 (*2) y DSM-IV (*4), un Discado Telefónico para llamar automáticamente mientras se consulta un registro, un Anotador para pequeños recordatorios, Calendario, acceso directo a un Buscador Web, y muchas otras opciones más..

-[ATTACKING]-

Luego de haber instalado el programa y haberlo probado un rato, procedo a escanearlo con el RDG para ver en que lenguaje esta hecho, vemos que es Visual Basic 6.0 Código Nativo, y no muestra alguna protección a la vista.

[Imagen 1] Escaneo del ExE

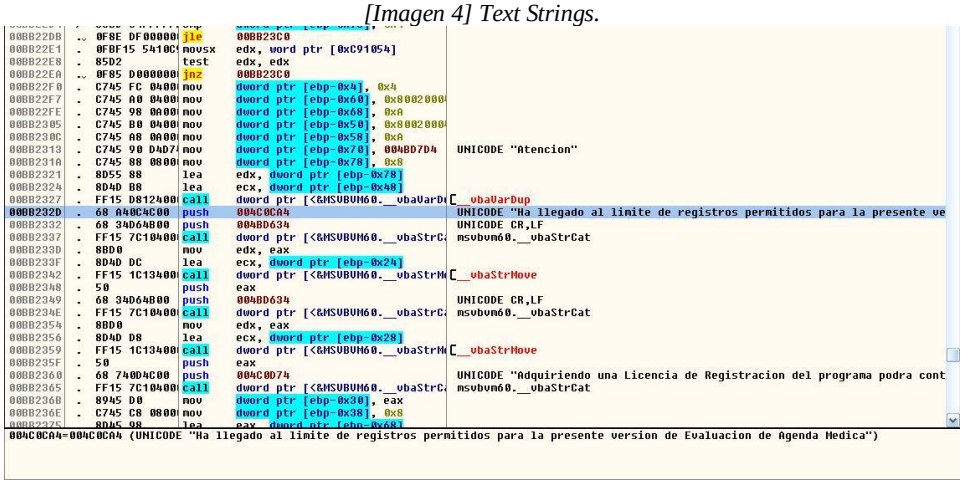
Lo corremos y vemos que nos muestra una NAG que nos pide comprar el programa, damos click en Continuar, una vez dentro del entorno de trabajo, ingresamos varios pacientes y vemos que luego de 5 ingresos nos muestra otra NAG que nos dice que no podemos ingresar más pacientes y que debemos comprarlo, al revisar la documentación de su web vemos que solo nos permite almacenar hasta un máximo de 5 pacientes y 5 medicamentos por ser una versión shareware y que al comprarlo nos enviaran otro instalador registrado a nuestro nombre y apellido, jeje, no creo que sea necesario en este caso.

[Imagen 2] NAG 1 – Continuar.

[Imagen 3] NAG 2 – Límite de Registros.

Ahora lo abrimos con OllyDBG, y damos click derecho dentro de la ventana de desensamblado y Search for / All referenced text strings y buscamos el texto que nos muestra la NAG.

[Imagen 4] Text Strings.



Luego de Tracear un rato y jugar con algunas condicionales, veo que en la dirección,

00BB22DB /0F8E DF000000 jle 00BB23C0 (Salta si es menor o igual o salta si no es más grande.)

[Imagen 5] JLE a JMP.

Es el punto de quiebre de la limitación, ya que si logra saltar si o si, evitaría que se muestre la NAG del "Chico Malo", por lo tanto lo reemplazaremos por un JMP que haría que siempre salte sin importar el valor que este tenga, y saltaría directamente a la dirección 00BB23C0, y continuaría con su recorrido.

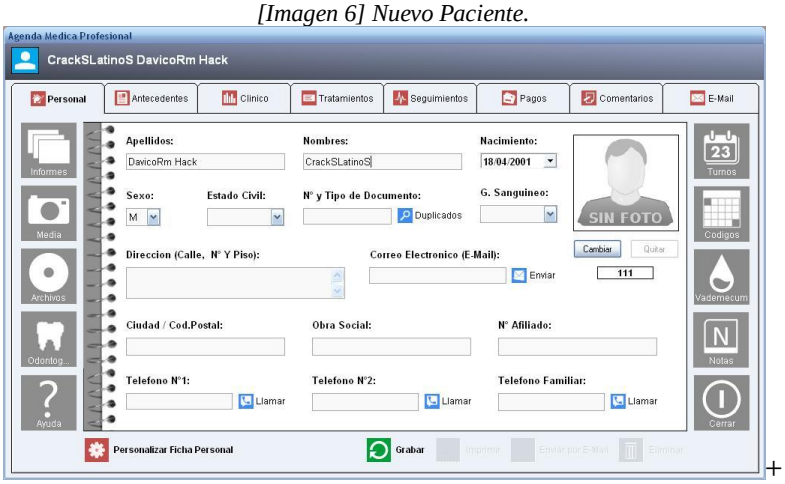
00BB23C0 > \C745 FC 06000>mov dword ptr [ebp-0x4], 0x6

Por lo tanto reemplazamos todos los JLE por JMP en las siguientes direcciones de memoria donde encontré al "Chico Malo".

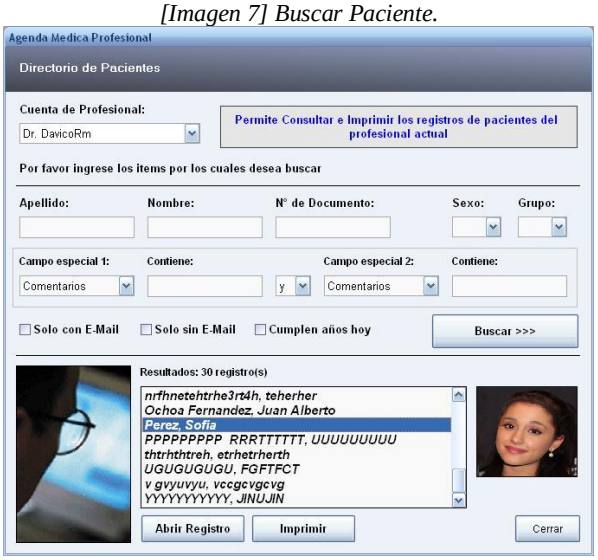
00BB22DB	. /0F8E DF000000	jle	00BB23C0
00BEB38C	. /0F8E ED000000	jle	00BEB47F
00C105AA	. /0F8E F3000000	jle	00C106A3
00C240A9	. /0F8E 0B010000	jle	00C241BA
00C479DE	. /0F8E 0F010000	jle	00C47AF3
00C70C49	. /0F8E ED000000	jle	00C70D3C

Ahora teniendo el nuevo ExE parcheado lo corremos y probamos si aún aparecen las limitaciones que teníamos.

[Imagen 6] Nuevo Paciente.



[Imagen 7] Buscar Paciente.



Que bien ¡!! Hemos saltado las limitaciones del programa, ahora nos muestra la ventana de Nuevo Paciente, la cual podemos llenar sin problemas, y cuando vamos la ventana de Directorio de Pacientes, podemos ver los 30 registros que ya tenemos ingresados, en la ventana Vademécum también podemos crear nuevos medicamentos, por lo tanto podemos decir que hemos vencido las limitaciones del shareware.

Por cuestiones estéticas y de comodidad, voy a NOPEAR la NAG de inicio para que directamente se abra la ventana del Login del Sistema y voy a cambiar la NAG de la parte superior "Version de Demostracion" por otra mejor.

Usando la técnica de COCO, mostrada en la teoría "061-OLLYDBG Y VISUAL BASIC III por COCO", cargamos nuestro ExE en OllyDBG y le damos click derecho dentro de la ventana de desensamblado y Search for / All constants y buscamos "2B0" y enter.

[Imagen 8] Buscar 2B0.

Nos aparecen varios resultados, colocamos un BP en cada una de las CALL y presionamos F9, y caemos en esta dirección que es la que llama a la NAG de inicio.

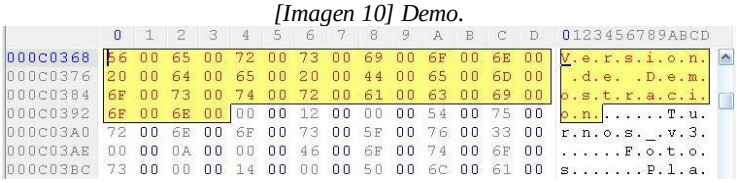
00BB0D5D |. FF90 B0020000 call dword ptr [eax+0x2B0] ; msvbvm60.72A44218

Como no me gusta complicarme la vida, lo que hago es NOPEAR esa CALL y así evitar la NAG, luego guardamos los cambios y corremos el programa.

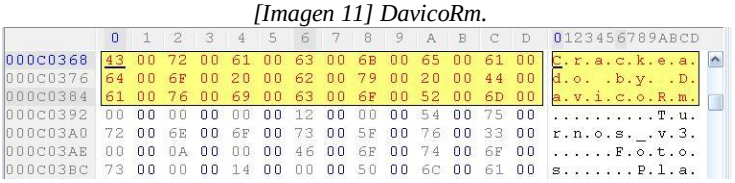
[Imagen 9] Login.

Por último y para terminar, abrimos el ExE con el Hex Workshop v6.7.3, buscamos el texto "Version de Demostracion" y lo reemplazamos por "Crackeado por DavicoRm" y guardamos el ExE.

[Imagen 10] Demo.



[Imagen 11] DavicoRm.



Ahora si podemos decir que hemos alcanzado nuestra meta, el programa está totalmente funcional y se ve estéticamente bien. Para los que les gusta usar el dUP de diablo2oo2, les adjunto el proyecto y el Patch que hice para que lo revisen.

-[MISSION ENDING]-

Al final de todo nuestro trabajo, logramos alcanzar nuestra meta trazada, dejar totalmente funcional esta aplicación, soy consciente de que el método utilizado no es el más adecuado para este fin, pero es el que actualmente está a mi alcance y del que tengo conocimiento, por favor que me disculpen los maestros si he cometido varios errores o quizás no he utilizado de forma adecuada las enseñanzas, aún estoy en proceso de aprendizaje, y espero que en un futuro cercano poder hacer mejores tutoriales como los hay en la lista de CrackSLatinoS.

Agradezco a todos los Maestros que dedican su tiempo a escribir y compartir su conocimiento en la lista y te agradezco a ti que estás leyendo este tutorial, ya que sé que todo mi esfuerzo no es en vano.

Para terminar quiero agradecer a todos los amigos y compañeros de la lista que comparten sus conocimientos diariamente conmigo y que responden mis insistentes preguntas en cada tema, esta vez no los voy a nombrar ya que haría aún más extenso este tutorial, pero Uds. saben quiénes son y espero que sigan así.

DavicoRm
CrackSLatinos
Lima-Perú
2014