Hola amiguitos, mala gente, infractores de la ley y en general toda esa entrañable ralea de personas que crackeando amplían sus conocimientos y así se van haciendo más libres...

Hoy os he reunido aquí a todos, al calor del fuego y oyendo la lluvia que cae por la ventana mientras el viento azota la noche para contaros un pequeño cuento de terror que os estremecerá. Para vosotros, lo que nadie oyó nunca, lo que los ancianos del lugar callan atemorizados, lo que pocos saben y menos cuentan... Esta es ni más ni menos que (Broummmm, trueno)...

La fabulosa e increíble historia de un crackeo pequeñito

O de cómo enfrentarse a Filebox 3.0 para PalmOs

Pues bien. Ahora que ya he conseguido captar vuestra atención (je je) vamos a meternos en harina y a comenzar este divertido berenjenal.

1- INTRODUCCIÓN:

Como a nadie se le escapa, los dispositivos de mano (llamados PDAs y verdaderos ordenadores chiquirritajos) disponen de varios sistemas operativos al uso, siendo los más importantes EPOC, WindowsCE y PalmOs.

Estupendo. Hace poco X-Grimator (servidor de ustedes) tuvo una noticia muy buena en su vida y decidió regalarse a sí mismo una agenda electrónica de estas con PalmOs como sistema operativo (en mi caso una Handspring Visor Deluxe que supuso todos mis ahorros, pero en fin...) y después de instalar unos programas freeware, que al final son los mejores, se topó de narices con uno que le interesaba pero que era shareware. Ni corto ni perezoso y haciendo uso de la natural inteligencia de los crackers, X-Grimator decidió aprenderlo todo sobre PalmOs y lanzarse así a la aventura de ir destripando cosas ajenas...

2- OBJETIVO:

En este mundo diminuto de las Palm, el programita que me interesaba era Filebox 3.0, que según Softonic es:

"Utiliza tu Palm para transportar cualquier tipo de archivo. FileBox es una aplicación que convertirá a tu Palm en un disquete para transportar cualquier tipo de archivo.
Gracias a su Interface funcionable bajo Windows, podrás seleccionar el archivo deseado para enviarlo en la próxima sincronización a tu Palm. Una vez realizado esto, desde tu dispositivo podrás visualizar ese archivo y indicarle que en la siguiente Sincronización lo envíe al PC.
Como los límites de memoria son escasos en los PDAs, este software te permite activar un sistema de compresión verdaderamente útil. Ahora podrás transportar cualquier tipo de información en tu Palm."

y que archiva en Comunicaciones e Infrared/Windows. Por lo tanto, siguiendo los cánones más clásicos de los tutos de Ingeniería Inversa, habremos de poner algo así:

- OBJETIVO: Filebox 3.0 for PalmOs
- PROTECCIÓN: Serial

3- HERRAMIENTAS:

Bueno, X-Grimator se volvió medio loco buscando las herramientas necesarias para estos menesteres y perdió horas y horas de sueño de su vida buscando en la web páginas inexistentes sobre crackeo de Palm. Al final sólo encontré una de Látigo, argentino, y otra de Quequero, italiano. Un saludo muy grande a ambos por su ayuda y por ser los únicos interesados en este tema.

En fin ¿a qué viene todo esto? pues viene a que en primer lugar XGrimator es un tío que habla por los codos (vale, vale, me di cuenta) y en segundo lugar a que he decidido meteros con este tutorial las herramientas necesarias pues no es fácil encontrarlas.

Por lo tanto ahí os van:

- Prc2bin: un programita para convertir los ejecutables de PalmOs (.prc) en .bin.
- PilotDis: un desensamblador más actualizado que PilDis (este último da problemas)

4- ¡¡ EN GUARDIA!!:

Siguiendo la línea clásica, instalamos el programita en nuestra Palm (para los que aún planeáis comprar una, también podéis usar el emulador gratuito que hay en www.palmos.com y que se llama Pilot) y tras ejecutarlo vemos que en el menú aparece la opción de "Registration". Para los novatos, el menú lo obtienes pulsando el icono del papelito que aparece sobreimpreso en la pantalla de la Palm o del Emulador, abajo a la izquierda. De nada.

Bárbaro. Nos aparece una ventanita preciosa que nos dice que hay que escribir un número para registrarse, y el número aparece dividido en dos campos de cuatro dígitos cada campo... ummmm, ya tenemos una pista...

Pues vale, vamos a meter un numero cualquiera, a ver que pasa: 5223-6651

Generalmente yo meto mi numero de DNI, pues es un número fácil de ver al debugear y que no produce confusión con otras cadenas de número (obviamente, el del ejemplo no es el mío). Es un truquito que os recomiendo.

Le damos a OK... y nos aparece una ventana con un mensaje odioso de error. Típico. Eso es muy positivo, ya sabemos tres cosas:

- el serial es de 8 dígitos.
- hay un mensaje de error.
- todo apunta a que hay otro mensaje de enhorabuena, o thank you o esas cosas que les encantan a los zombi-programadores yanquis...

5- DEFENSA EN CUARTA Y MARCHANDO HACIA EL ENEMIGO:

Vale, todo esto es muy bonito pero ¿qué coño hago?. Pues parece ser que lo que más nos interesa ahora es ver ese filebox.prc que hemos instalado en la maquinita. No estaría nada mal abrirle los intestinos y ver que tiene dentro ¿no?. Para ello usaremos nuestro mejor sable: Prc2bin. Su uso es fácil. Metemos el filebox.prc en el mismo directorio que Prc2bin y abriendo una consola DOS nos dirigimos a ese directorio y tecleamos

prc2bin filebox.prc

con esto logramos que el directorio se nos llene de archivos con extensión .bin... fijaos el dichoso mini-programa lo que tenía dentro, el muy condenado... pero al menos ganamos ya nuestro primer asalto ¡touché!. Muy bien chavalotes, lo estáis haciendo bárbaro.

El problema que se nos plantea ahora es elegir algo de todo eso que nos sea de utilidad. Para ello recurriremos a nuestro amado Zen-Cracking (¡loor a +Orc!).

Estiro las piernas, manteniendo siempre la defensa, y apunto con mi florete al corazón de mi contrario. Veamos, lo más obvio en esta lucha es un mensajito de "error, tonto del capirote, que no sabes ni meter un número sin nuestra ayuda". Pues busquemos ese mensaje en el destripe que le hicimos al filebox a ver que aparece. NOTA: en Palm, los mensajes de aviso y error se llaman Talt**xxxx** de modo que al haber separado los componentes de filebox.prc, tendremos varios Talt**xxxx**.bin. Uno de ellos nos interesa.

Así las cosas, los miramos con el block de notas y encontramos que Talt076c.bin nos suelta el mensaje de "wrong registration code" y cual será nuestra sorpresa al ver que Talt0154.bin nos dice que "Thank you...bla bla bla". Juas juas, vamos por buen camino, ¡hoy nuestro florete está bien afilado!.

Acabado el primer asalto, señores. A nuestro favor, que el serial es de 8 dígitos en dos campos y que los mensajes de error y éxito son Talt076c y Talt0154. A favor de los zombi-programadores, nada.

Me chifla ser cruel.

5- SEGUNDO ASALTO: MARCHAR, FONDO Y TOCADO:

Ahora viene lo más divertido para los programadores e informáticos que me leéis, y lo más duro para XGrimator que es un pobre tirador de esgrima que fue por Humanidades. Me refiero al código puro y duro.

Necesitamos un código en listado muerto para acabar el estudio forense del tema ¿verdad?. Pues eso lo conseguiremos con la maravilla de desensamblador llamado PilotDis.

De nuevo, vamos a una consola de DOS y entramos en el directorio de PilotDis, donde previamente habremos metido el archivo llamado Code0001.bin. Ese es el meollo de la cuestión, porque para eso hemos separado los mensajitos de otras vainas. Ese es el código puro y duro, el gran enemigo, el malo y feo de la película.

Pues tecleamos

PilotDis code0001.bin

y el malo de la película se convierte en code0001.bin.s en el mismo directorio de PilotDis. Ya veis, con lo fuertote y gordo que parecía y se nos quedó en nada. En fin, la vida es que es muy mala. Nuestro aguerrido enemigo, ese diminuto programa en el diminuto mundo de Palm está ya sin arma. De una rápida estocada se la hemos tirado al suelo e indefenso tiembla viendo acercarse su suerte. Huelo ya la sangre...

6- PRIMERA SANGRE Y FIN DEL ACTO. MUERTE MIRANDO AL SOL:

Abrir code0001.bin.s con el block de notas no tiene ninguna complicación. Una vez dentro usamos el comando “buscar” del block de notas y le ponemos

$076c <---------- que hace referencia a Talt076.bin

y hago una pequeña pausa para explicaros esto, aunque reconozco que de ensamblador no tengo pero es que ni idea, o sea que tened paciencia conmigo.

Parece ser que la historia es que aparece el símbolo de dólar ($) cuando se mete en la pila un mensaje de alerta. Se metería justo cuando está comenzando la ID de Alerta. Bueno, eso me dijeron, al menos para el ASM de PalmOs que se basa en Motorola, que como sabéis tiene sus diferencias con x86. Pero eso no viene al caso.

Buscáis eso en el block de notas para ver cuando el mensajito de error se mete en la pila y nos encontramos con este pedazo de código:

```
00001f6e  2800            L185     MOVE.L    D0,D4
00001f70  0c8300001b6d             CMPI.L    #7021!$1b6d,D3
00001f76  661a                     BNE       L186
00001f78  0c8400000cfd             CMPI.L    #3325!$cfd,D4
00001f7e  6612                     BNE       L186
00001f80  3f3c0514                 MOVE.W    #1300!$514,-(A7)
00001f84  4e4fa192                 sysTrapFrmAlert
00001f88  1b7c0001fe82             MOVE.B    #1,-382(A5)
00001f8e  544f                     ADDQ.W    #2,A7
00001f90  600a                     BRA L187
00001f92  3f3c076c       L186      MOVE.W    #1900!$76c,-(A7)
00001f96  4e4fa192                 sysTrapFrmAlert
```

Os he resaltado en negrita lo que os señala el buscador del block de notas. Aunque aún tenéis otra referencia más, esta es la que nos interesa por la sencilla razón de que justo debajo nos aparece **sysTrapFrmAlert** que es la API que muestra los mensajes de alerta. Si a eso le sumamos que el registro A7 es la pila...¡¡tocado en el corazón y herido de muerte!!.

Nuestro enemigo agoniza. Tose sangre. Vemos claro que en

00001f92 3f3c076c L186 MOVE.W #1900!$76c,-(A7)

una ID de alerta se está metiendo en la pila, y que es una instrucción de move que decrementa A7. Vaya, vaya, y además tenemos

00001f80 3f3c0514 MOVE.W #1300!$514,-(A7)

Si mi memoria no me falla, y no lo hace, ese $514 era el Talt514 del mesajito de “Thank you”. Muchacho, has sido un caballero peleando, pero ahora llega tu fin.

Repasemos de nuevo esto:

```
00001f6e  2800              L185     MOVE.L    D0,D4
00001f70  0c8300001b6d               CMPI.L    #7021!$1b6d,D3
00001f76  661a                       BNE       L186
00001f78  0c8400000cfd               CMPI.L    #3325!$cfd,D4
00001f7e  6612                       BNE        L186
00001f80  3f3c0514                   MOVE.W    #1300!$514,-(A7)
00001f84  4e4fa192                   sysTrapFrmAlert
00001f88  1b7c0001fe82               MOVE.B    #1,-382(A5)
00001f8e  544f                       ADDQ.W    #2,A7
00001f90  600a                       BRA L187
00001f92  3f3c076c          L186     MOVE.W    #1900!$76c,-(A7)
00001f96  4e4fa192                   sysTrapFrmAlert
```

Por poco que nos fijemos, vemos en

```
00001f6e  2800              L185     MOVE.L    D0,D4
```

que algo habla esa máquina de L185. Eso es una LABEL (etiqueta) y es algo que hace referencia a un punto en algún momento de la ejecución del programa. Más abajo tenemos la L186, que puse en negrita porque es una llamada a una Talt, la de error. La cosa está clara. El enemigo cae de rodillas agarrándose el pecho...

Fijaos en

```
00001f70  0c8300001b6d               CMPI.L    #7021!$1b6d,D3
00001f76  661a                       BNE       L186
00001f78  0c8400000cfd               CMPI.L    #3325!$cfd,D4
00001f7e  6612                       BNE        L186
```

Eso tiene toda la pinta de decir “compárame nosequé y si no es igual salta a L186” (en este ASM, bne = branch not equal) y luego compara nosequé y lo mismo.

No hay duda, el pobre chico pone una mano en el suelo. Está de rodillas y sangra en abundancia por el pecho. Nuestra estocada lo ha matado. Escupe sangre y musita: “Mi mujer, mi mu...”. Limpiamos nuestro florete y con una mirada fría y sabia, distantes, recordamos que el serial de 8 numeritos se guardaba en dos campos, que son estos:

```
00001f70  0c8300001b6d               CMPI.L    #7021!$1b6d,D3
00001f78  0c8400000cfd               CMPI.L    #3325!$cfd,D4
```

y que comprueba el primero (y de no cumplirse salta a L186, que es la carga en pila el mensaje de error) y hace igual al segundo. ¿Qué podrá ser el primer término de la comparación? Ese precioso 7021 y 3325 (resaltados en negrita).

El triste adversario muere mirando al sol.

7- DUELO POR SU MUERTE:

Enciendo mi Palm, voy al programa y meto en el “Register” 7021-3325. De nada por registrarme. Lo compruebo en el emulador y también funciona. Es lógico: ordenador pequeño y programa pequeño = protección pequeña. Tan triste que estoy por desinstalarlo. En fin...

8- AGRADECIMIENTOS:

Por supuesto al canal IRC-HISPANO #crackers por aguantarme y por su apoyo y a todos ellos (ahora mismo, por lo que veo, Mr White, el bueno de Ziritione, el genio de eSn-mIn, Viktory,

The Pope que es una autoridad, Sunevil, TGILITO, Blackdog, MetalSlug, Offset, birk, Seroculto y bueno, miles de ellos que no pongo porque, para que negarlo, me aburro) (jeje).

Y ya sabéis, leed, leed, leed y pensad, pensad, pensad... sólo así seréis fuertes y libres.

X-Grimator

25/01/02

PD: Por cierto, para ser mi primer tuto no me he enrollado mucho ¿no?. Es que en el canal de crackers me insistieron mucho que fuese muy muy clarito explicando. Bueno, perdonad si no os enterasteis de nada...