Lección 7: F-Secure antivirus 2.0

O lo ridículo de hacer una protección insultante

¡Hola de nuevo, mis pequeños y alocados secuaces!. Bueno, últimamente he estado un poco ausente pero eso fue debido al crackme que hice en prc y a un keygen también en formato para Palm, que es que aprender a programar, aunque sea un poquito, lleva su tiempo. Así que he decidido escribiros este tuto para ir poco a poco dejándoos alguna lección por ahí.

1- Aburrido estaba yo en ircnet:

Cuando apareció un pobre chico llamado TaeBo- de Dakota del Sur todo agobiado porque no era capaz de crackear este antivirus, y sospechaba que un monstruo horrible y feo se había colado en su pobre Palm a fin de devorarle la codiciada estabilidad de su S.O. Tanto era su sufrimiento para crackear el antivirus que decidí ayudarle, así que cogí las herramientas de siempre y me puse a mirar...

Lo primero que hice fue cargar el programa en el Palm Emulator del que tanto os hablé y comprobar sus mensajes. Efectivamente, vi que había uno clásico:

Juas juas, así que un trial... en fin, el crack no podía ser difícil pero como no había escrito nada sobre trials, decidí que tenía que escribir uno, así que se me ocurrió adelantar la fecha para ver qué mensaje me salía, y hete aquí que me espeta esto a la cara:

Dios, cómo se puede ser tan previsible... lastimoso esto, de verdad, es que ofende a la inteligencia... :o(

En fin, ya algo desanimado por lo sencillo del crack y casi deprimido de que una empresa tan seria como debería ser una antivirus haga este tipo de protecciones, decidí cargar el programa en el prcExplorer y comprobar, como efectivamente fue, que el mensaje de "Fin de Trial" era el 1500 decimal (empezaremos a acostumbrarnos a ponerlo como #1500) o lo que es igual, el 05dc hexa ($05dc). Estupendo. Me hizo gracia ver un mensaje #1600 ($0640) que te daba las gracias por registrarte y que luego no aparecía en ningún lado del código, además, es que ni siquiera aparecía una casilla de register, lo que me hizo pensar que el programador es

un tío vago (lazy en inglés) que reutilizó trozos de código y recauchutó cosas varias... lo cual me da más y más que pensar que este antivirus es de todo menos fiable... pedazo chapuza macho.

Ya no sabía si enfadado o deprimido, utilicé el pilotdis para desensamblar (más cómodo si se usa con el prcedit del dr_funk, quizá la mejor herramienta de crackeo para Palm ahora mismo en el mercado), en concreto el code0001, que es el único interesante (respecto al code0000, es uno estándar en todas las aplicaciones de Palm, y podéis buscar información en google, en un texto llamado Prc Format). Así que ya tenemos desensamblado el code y nos disponemos a crackear.

2- Ay, TaeBo-, mon ami...:

Lo que te llevó a ti, estimado lector, a leer estas líneas, fue más o menos lo que me llevó a mí, pobre newbie, sospechar por dónde iban los tiros. Y el bueno del de Dakota del Sur, perdidísimo en código. En fin, abro el code0001.bin.s con el notepad (block de notas en lengua no-hereje) y tras buscar el mensaje de "gracias por registrarse" y ver que ni existía, busqué el de "caducado como los billetes con los que X-Grimator intenta pagar las cervezas", o sea, la Talt #1500 ($05dc) en la forma en que vimos en los tutoriales anteriores. Pues bien, nos interesaba que hubiese un sysTrapFrmAlert justo debajo. Eso nos apareció aquí:

```
000020d2  4eba05fc        L278      JSR   L334
000020d6  3600                      MOVE.W D0,D3
000020d8  3003                      MOVE.W D3,D0
000020da  673c                      BEQ   L281
000020dc  5340                      SUBQ.W #1,D0
000020de  670a                      BEQ   L279; branch if equal
000020e0  5340                      SUBQ.W #1,D0
000020e2  676c                      BEQ   L282
000020e4  5340                      SUBQ.W #1,D0
000020e6  6712                      BEQ   L280; branch if equal
000020e8  6066                      BRA   L282
000020ea  3f3c05dc        L279      MOVE.W  #1500!$5dc,-(A7) ; Your evaluation version of F-
Secure Anti-Virus 2.0 has expired.
000020ee  4e4fa192                  sysTrapFrmAlert
000020f2  303c3039                  MOVE.W #12345!$3039,D0
000020f6  544f                      ADDQ.W #2,A7
000020f8  606a                      BRA   L283
000020fa  3f3c000e        L280      MOVE.W  #14!$e,-(A7)
000020fe  4eba0286                  JSR   L310
00002102  3600                      MOVE.W D0,D3
00002104  544f                      ADDQ.W #2,A7
00002106  6710                      BEQ   L281
00002108  3f3c05dc                  MOVE.W #1500!$5dc,-(A7) ; Your evaluation version of F-Secure
Anti-Virus 2.0 has expired.
0000210c  4e4fa192                  sysTrapFrmAlert
```

Os señalo el quid de la cuestión en negrita. Como una de las más importantes bazas para ser cracker es la intuición, el zen palming (jeje), X-Grimator todo chulo fue y puso un nop en ambos saltos, quedando algo así:

```
000020d2  4eba05fc        L278      JSR   L334
000020d6  3600                      MOVE.W D0,D3
000020d8  3003                      MOVE.W D3,D0
000020da  673c                      BEQ   L281
000020dc  5340                      SUBQ.W #1,D0
000020de  4e71                      NOP
000020e0  5340                      SUBQ.W #1,D0
000020e2  676c                      BEQ   L282
000020e4  5340                      SUBQ.W #1,D0
000020e6  4e71                      NOP
```

cosa que hizo gracias a un editor hexadecimal, buscando la secuencia 670a5340, que me llevó directo a ese trozo de código.

3- En Dakota del Sur alucinan con los europeos:

Guardo el cambio en el programa y con la chulería que caracteriza a los lamers como yo, le envío el crack al dakotiano, o dakotiense o como se llame, y le digo que ya está. El chico lo prueba y le funciona perfectamente. No sólo eliminé la primera Talt que nos recordaba que eso era un trial sino que eliminé la que decía que fecha expirada, pues adelantó el calendario y todo iba perfecto. Esta vez no os voy a explicar el por qué del crack, baste decir que fue una mezcla de intuición y suerte y salió a la primera. Supongo que analizando con más calma la cosa veríamos que el cambio no sólo afectó al mensaje de "time expired" sino que por una serie de saltos también afectó al mensaje de inicio. Ver para creer... el bueno de mi amigo yanqui no era capaz de creer que en 15 minutos escasitos sacase lo que a él le estaba llevando ya 1 hora (y eso que a la vez yo me dedicaba a chatear con mis amigos de #codex del irc-hispano). Ver para creer... asco de trial, asco de crack, asco de tutorial que escribo... ¡¡¿pero alguien puede fiarse de un antivirus que está así de protegido?!!... si cuando +Orc decía "zombi-programmers" lo decía por algo... en fin... y yo con un empleo que da grima...

4- Resumiendo chis-pum punto final:

Acabamos de reventar un trial sin comerlo ni beberlo. Bueno, sirva pues este tutorial como alivio a mi silencio temporal y a los últimos, que fueron más complicados. Lo que conseguimos fue: un yanqui de Dakota con los ojos como platos (ojiplático) de mi velocidad crackeando, un antivirus que nos dice que no tenemos virus (ja ja, tú fíate de la Virgen pero por si acaso no corras...), y X-Grimator con un poco de suerte por una vez en su vida (quedé como un gurú del crack ante el chico). ¡Ah! y tú, lector, con cara de haba de ver un crack tan tonto y un tuto igual de tonto.

Hasta otra.

X-Grimator; UE 01/09/02
"Pensad, pensad. Siempre pensad..."

Saludos especiales a ablaze y TaeBo-, por ser mis dos primeros alumnos extanjeros y admirarme, que eso siempre gusta. También a InLimbo por su ayuda programando, a Sunevil por ser el primero en creer en mí y a todo Disidents por apoyarme cuando lo necesitaba y hacer algo serio y con futuro esto de los estudios de seguridad en los programas (entre ellos, w3ndig0, wendell, remains, S-P-A-R-K, LuZZer, }-XpyXt-{, Low, FEAR, etc etc...) ¡ah! y Marconi y Ziritione por ser, sencillamente, tan majos.
eSn-mIn, olvidarme de ti sería, sencillamente, un insulto a la comunidad cracker.