A cura di: **ing. Sommruga Andrea Guido**
Versione **1..0**
del: 24 gen 2005

DESCRIZIONE

Winpooch è un programma di utilità che si installa come servizio e controlla se ci sono modifiche nelle aree critiche del sistema per piattaforma windows2000 ed XP.

- E' compatto e non carica eccessivamente il sistema
- E' software libero distribuito con sorgenti
- Controlla alcune chiavi del registry ed il direttorio system32

Il programma è di semplicissima installazione: basta lanciare l'eseguibile e confermare il direttorio in cui installare il programma. Winpooch si scarica liberamente da internet dal sito http://winpooch.sourceforge.net.
Il programma attualmente prevede solo la lingua inglese e francese, questo non è comunque un problema perché le interazioni con il programma sono minime.

Il programma si avvia automaticamente all'avvio di windows e crea una simpatica icona con un cagnolino vicino all'orologio. Winpooch vigila costantemente sull'attività dei programmi, controlla alcune chiavi del registry ed i direttori system32 e system32\driver\etc. Se si verificano modifiche al contenuto delle chiavi o al contenuto dei direttori visualizza immediatamente il simpatico sceriffo che, anticipato da un suono, elenca le modifiche rilevate. Tutte le modifiche sono comunque registrate su un comodo file di log in formato testo.

Durante il normale funzionamento di windows non si dovrebbero avere modifiche nei file di system32 e nelle chiavi del registry della sezione run. Se si riscontrano modifiche è un possibile campanello di allarme per segnalare delle attività sospette di software che magari cerca di installarsi all'insaputa dell'utente. Questo è il tipico modo con cui lo spyware infetta le macchine. Winpooch può quindi essere di grande aiuto nello scovare software indesiderato.

Per avere la massima efficacia è un programma da utilizzarsi abbinato ad un antivirus e ad un programma per la rimozione dello spyware.

Come antivirus segnalo l'ottimo prodotto di AVAST disponibile da http://www.avast.com , non è un prodotto OpenSource ma per uso personale è gratuito. Gli antivirus sono quasi tutti prodotti commerciali.

Per la rimozione dello spyware segnalo Spyware Search & Destroy scaricabile da http://www.safer-networking.org/it/index.html classico prodotto libero ed opensource.

CARATTERISTICHE

Winpooch non si presenta come alternativa ai programmi antivirus o anti spyware. E' solo un utile compagno che aiuta ad identificare i problemi e a smascherare immediatamente i programmi che cercano di fare troppo i furbi.

Attenzione: winpooch si limita a segnalare l'attività sospetta e non cancella i programmi spyware o virus.

- rileva immediatamente le modifiche al contenuto di system32 e di system32\driver\etc
- rileva immediatamente le modifiche alle chiavi del registry HKEY_LOCALMACHINE RUN*
- registra tutte le modifiche sospette su un file di log in formato testo consultabile a posteriori

REQUISITI

Attualmente winpooch è disponibile solo per la piattaforma windows a 32 bit quindi per windows 2000 e windows XP.

DA USARE CON

spyboot search & destroy: GPL
antivirus

LINK

http://winpooch.sourceforge.net/home