

Pc a rischio per i Software fasulli, ma la colpa è nostra

2009-10-23 21:19:20



scareware Tecnicamente vengono chiamati “**Scareware**”, o anche “**rogue security software**”. Dei programmi per elaboratore fasulli che non forniscono alcuna utilità a chi li scarica e che vengono installati per via dell’ansia che generano con i loro finti messaggi d’allarme, reclamizzati da inserzioni che preannunciano falle o anomalie nel pc di chi si imbatte in loro. **Ma il problema è che la falla, sono in grado di generarla proprio loro, con l’inconsapevole complicità della stessa vittima.** Un nuovo inquietante caso di ingegneria sociale con finalità criminali, raccontata nel nuovo reporto della Symantec che tira un ballo l’irresponsabilità degli stessi utenti.

Questo il comunicato presente nel sito della nota azienda produttrice di **software antivirus come Norton:**

Symantec, nota azienda fra i cui prodotti troviamo Norton Antivirus ma anche Norton Ghost presenta un nuovo studio sui “rogue security software” o per meglio dire “scareware”. **I scareware sono software fasulli, che non forniscono alcun benefit all’utente che li scarica.** La metodologia attraverso cui vengono diffusi i scareware è suscitare ansia, apprensione, shock magari attraverso messaggi sullo schermo in cui si dice che il proprio PC ha una falla di sicurezza. Ma il proprio PC è invece perfetto e ci sono molte probabilità che, dopo aver proceduto al download del scareware (falso antivirus o antispyware), il proprio PC venga infettato. Eseguito il scareware **il prodotto si presenta solitamente in versione “trial”, l’utente avrebbe da pagare una licenza per l’utilizzo del sw** che ripetiamo, non apporta alcun beneficio.

Ebbene, Symantec, nota società specializzata nella sicurezza afferma che i scareware sono stati scaricati nel periodo fra luglio 2008 e giugno 2009 per la maggior parte dagli utenti (i principali 50 tipi di scareware). Si tratta quindi di un allarme sicurezza ma ancor più di un allarme informatizzazione. **Non esiste un singolo “luogo” di diffusione scareware, li possiamo trovare in Blogs a dir poco legittimi, social network, siti per adulti ma anche come link nei risultati delle ricerche.** Il consiglio è come al solito procurarsi un Browser che integri funzionalità Anti Phishing ma anche un Antivirus che controlli attentamente i processi in e out del nostro PC, stando attenti che non avvengano scaricamenti in background.

Si tratta di un argomento complesso su cui è intervenuto anche il Professor David Wall, PhD, del Centro sui Studi Criminali dell’Università di Leeds:

“Scareware creators can scam thousands of people for comparatively small amounts of money all at the same time and make huge aggregate profits,” “This type of fraud works because the fake security software tricks users into believing they have an immediate threat which only their program can resolve. Ultimately, it’s a con. I would advise Internet users to be careful while online and only download from trusted sources.”

Anti-Phishing Italia: il portale contro le truffe on-line

Pc a rischio per i Software fasulli, ma la colpa è nostra

Concludiamo che il miglior contrattacco ai creatori di scareware è fare uso di un sistema aggiornato, con le ultime patch di sicurezza. Si raccomanda infine di tenere il proprio Antivirus e Antispyware (antispyware con protezione realtime processi in e out) sempre aggiornati oltre ovviamente al non andare a scaricare nuovi antivirus, qualora abbiamo già uno sul nostro PC.

Fonte: Anti-Phishing Italia – www.anti-phishing.it