PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 321 di giovedì 19 aprile 2001

Scoperta una nuova vulnerabilita' dei software Microsoft?

Il baco potrebbe essere sfruttato da hacker e creatori di virus. Qualche consiglio per evitare brutte sorprese...

Un famoso " "bug hunter", Georgi Guninski, avrebbe individuato in Windows Explorer e Internet Explorer una vulnerabiliata' facilmente sfruttabile da hacker e creatori di virus.

Si tratta della possibilita' di celare l'estensione di un file dietro ad estensioni fittizie; questo consentirebbe ad esempio, di nascondere un programmino "pericoloso", mediante un'estensione innocua quale quella dei file di testo.
L'utente che apre il file, convinto che nulla possa accadere perche' "si tratta solo di un file di testo...", in realta' potrebbe attivare un file che di innocuo ha ben poco.

Il quotidiano di informatica che ha riportato la notizia ha illustrato i dettagli "tecnici" della scoperta.
Guninski afferma che aggiungendo dopo un'estensione di un file un CLSID (Class Identifier), che in Windows individua univocamente una classe di oggetti, Windows Explorer e Internet Explorer mostera' all'utente solo la prima estensione.

Considerando ad esempio il file testhta.txt.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}, Windows Explorer e Internet Explorer non mostrano l'estensione CLSID (.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}), ma solo 'estensione .txt: un file ".hta" (HTML Application) potrebbe essere cosi' nascosto in un file .txt.

Un piccolo consiglio per prevenire sgradite sorprese: non aprite i file se l'icona non e' associata correttamente all'estensione, in particolare se e' visualizzata l'icona generica con il logo di Windows.

---

www.puntosicuro.it