Anno XI n. 3214 di martedì 28 aprile 2009 - PI / News

GAPTCHA AGGIRA I CONTROLLI GMAIL

Un worm si annida nelle pieghe del Web per infettare un PC e sfruttarlo per spammare a destra e manca. Nulla possono le protezioni per impedire ai bot di riprodursi

Roma - Una società vietnamita specializzata in sicurezza ha individuato un worm in grado di aggirare il sistema di CAPTCHA di Gmail, creando nuovi *fake* account in serie. Il *malware*, chiamato **W32.Gaptcha.Worm**, consente agli spammer di moltiplicare le *bocche di fuoco* dalle quali inviare scam ed altre forme di pubblicità indesiderata.

Erano già diversi mesi, in effetti, che la quantità di spam proveniente da Gmail - e dall'ambiente Google in generale - sembrava continuasse ad aumentare. Con un post sul loro blog aziendale, gli analisti di Bach Koa Internetwork Security (BKIS) hanno annunciato la scoperta di uno worm in grado di forzare le barriere anti-bot di Gmail.

Una volta che il computer è infettato con Gaptcha, il malware lancia automaticamente Internet Explorer e lo reindirizza verso la pagina di creazione di nuovo account su Gmail. Gaptcha riempie automaticamente i campi con nomi casuali, e quindi invia l'immagine CAPTCHA a un server remoto. Quest'ultimo, a sua volta, decodifica il codice e lo reinvia alla macchina infettata, dove il processo di iscrizione può così essere completato.

Dopo che che il nuovo account è stato creato, lo spammer di turno lo può impiegare per inviare da esso messaggi pubblicitari o *scam* in quantità. Il gioco si esaurisce soltanto quando l'eccessiva frequenza di *signup* dalla stessa macchina "insospettisce" i server di Gmail, portando ad un blocco nei confronti del computer in questione. A quel punto il worm si auto- distrugge.

I CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) sono le stringhe alfanumeriche random tipicamente impiegate nei processi di iscrizione ai servizi online. In passato i CAPTCHA risultavano estremamente difficili da aggirare per bot e malintenzionati in genere. Di recente,

i miglioramenti nelle tecnologie di riconoscimento ottico dei caratteri (OCR) e l'impiego di operatori umani hanno portato al superamento di tali ostacoli. Al punto che forse è giunto il momento di cercare modi nuovi e diversi per tenere i bot lontani da questi servizi.

Gli account gratuiti di gruppi come Yahoo! e Google sono particolarmente ambiti dagli spammer, in quanto la provenienza da domini conosciuti aumenta la probabilità per le mail di superare i filtri antispam. Le *internet firm* d'altra parte, promuovono ogni sforzo per tenere i propri sistemi aggiornati rispetto ai tentativi di aggiramento. Solo pochi giorni fa, la stessa Google aveva introdotto una nuova tecnica di gestione dei CAPTCHA, in grado secondo i responsabili di ridurre l'incidenza di bot e malware.

Nel caso di Gaptcha, i responsabili di Mountain View per il momento hanno declinato le richieste di un commento ufficiale.

Giovanni Arata

Punto Informatico è testata giornalistica quotidiana - Tribunale di Roma n. 51 del 7.2.1996
Fondato da Andrea De Andreis nel 1995
De Andreis Editore Srl - P.IVA: 06696301008 - ROC: 7983