

STOP MARIPOSA: arrestato il criminale informatico più pericoloso del mondo

2010-08-09 22:01:36



È stato arrestato nei giorni scorsi un giovane di 23 anni ritenuto **il più pericoloso hacker del momento**, tale **“Iserdo”** autore del software per creare la rete di computer zombie chiamata **Botnet Mariposa** (termine che in spagnolo significa farfalla). La notizia la riportano anche i portali di Panda Security e Defence Intelligence hanno collaborato con l’FBI per rintracciare il pericoloso hacker

Gli specialisti delle due aziende interessate all’indagine hanno potuto identificare Iserdo attraverso l’analisi del software utilizzato dalla botnet, responsabile della compromissione e della (inconsapevole per gli utenti) sottomissione di milioni di sistemi in tutto il mondo alle volontà di criminali informatici

Iserdo è stato arrestato la scorsa settimana a Maribor, in Slovenia, e ora è libero su cauzione.

Mariposa, secondo le prime indiscrezioni, sarebbe una rete realizzabile mediante **un kit informatico denominato Butterfly, un pacchetto software rivenduto su internet a un costo tra i 500 e i 1.500 euro**, e che permetteva a persone prive di particolari capacità informatiche, di sferrare micidiali attacchi informatici su ampia scala. Il kit è stato utilizzato per creare almeno 10.000 esemplari unici di software pericolosi e oltre 700 botnet. Centinaia di istituzioni finanziarie e governative e milioni di aziende private e singoli utenti sono stati attaccati in tutto il mondo tramite questo sistema “volante”.

“Negli ultimi due anni, **il software usato per creare la botnet Marisposa è stato venduto a centinaia di criminali**, rendendolo uno dei più famosi in tutto il mondo”, ha spiegato **Robert S. Muller, III, FBI Director**. “Queste cyber intrusioni, furti e frodi minano l’integrità di Internet e delle attività che vi si svolgono e minacciano la privacy e il portafogli dei ‘naviganti’”.

Una botnet è una rete di pc collegati tra loro mediante internet tramite un software nascosto che le mette tutti a disposizione di un unico sistema informatico remoto. Tale connessione può essere realizzata tramite virus informatici o trojan mentre **i controllori della rete possono in questo modo sfruttare i computer compromessi per realizzare attacchi contro portali telematici effettuando accessi simultanei e bloccandone**, così, l’accessibilità per alcune ore (attacchi cosiddetti denial-of-service in sigla DDoS).

Oppure possono essere utilizzati per effettuare attacchi di spamming all’insaputa degli utenti, mediante tecniche di phishing. Od ancora, possono essere utilizzati per effettuare circolazioni illecite di valuta sfruttando le credenziali bancarie degli utenti che siano state incautamente rese disponibili nell’elaboratore compromesso dagli autori del botnet. I computer che compongono la botnet sono chiamati bot (abbreviazione di roBOT) od anche computer zombie.

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