

McAfee scopre il cyber-attacco Shady Rat

- Ultima modifica: Giovedì, 01 Dicembre 2011 20:47

Pubblicato: Mercoledì, 03 Agosto 2011 20:23

Scritto da Alessandro Crea



McAfee rivela sul proprio blog di aver scoperto un enorme piano di cyber-spionaggio a livello globale, che dura già da 6 anni e che è ancora in atto contro governi nazionali, istituzioni e aziende multinazionali.

Come utenti siamo spesso portati a immaginare le **attività dei cracker** come principalmente indirizzate nei confronti dei singoli utenti o al massimo di quelle aziende che, operando in alcuni settori strategici di Internet, come i **social network** o i **motori di ricerca**, abbiano database molto appetibili. Pensiamo cioè che le attività illegali online mirino principalmente a sottrarre codici bancari, password e dati personali, attraverso attacchi ai singoli computer o ai ricchi database di aziende e istituzioni pubbliche.



ANONYMOUS

We are Legion. We do not Forgive. We do not Forget.

Ultimamente poi [ci stiamo anche abituando](#) a forme differenti, come quelle portate avanti da crew quali **Anonymous** o **LulzSec**, che hanno come obiettivo principale più che altro quello di sollevare alcuni problemi inerenti alla sicurezza dei dati online e alla loro natura. Ma

McAfee scopre il cyber-attacco Shady Rat

- Ultima modifica: Giovedì, 01 Dicembre 2011 20:47

Pubblicato: Mercoledì, 03 Agosto 2011 20:23

Scritto da Alessandro Crea

difficilmente pensiamo che invece tali attività possano essere svolte anche su una scala molto più grande e con ben altri mezzi, allo scopo di spiare intere nazioni o aziende multinazionali e di sottrarre dati sensibili di altro livello, come ad esempio database protetti, email riservate, trattative commerciali, schemi progettuali, codici sorgente, documenti contrattuali e archivi di documenti legati alla sicurezza nazionale piuttosto che a importanti proprietà intellettuali.

E invece accadono anche queste cose ed è quanto rivelato proprio in questi giorni sul blog di McAfee, nota azienda di sicurezza informatica, che ha svelato di aver scoperto un **enorme piano di cyber-spionaggio** in atto già da ben 5 anni e ancora attivo, indirizzato verso oltre 70 aziende multinazionali, governi e organizzazioni non-profit e denominato **Shady Rat**, con riferimento agli strumenti utilizzati per ottenere l'accesso remoto (Remote Access Tools appunto).

I ricercatori di McAfee Labs hanno scoperto l'operazione raccogliendo ed analizzando i log degli attacchi che hanno colpito alcune organizzazioni anche per **28 mesi continuativi**. Il risultato di questa analisi, una delle più complete mai svolte, è stato pubblicato poco tempo fa ed ha rivelato appunto questa enorme operazione, che tra le vittime coinvolte vede **6 aziende presenti in 14 nazioni**, oltre a **22 governi di tutto il mondo** tra cui il governo federale degli Stati Uniti, quello canadese, vietnamita, e il governo di Taiwan, società di comunicazione satellitare, un'agenzia statunitense non-profit che opera nel settore della sicurezza nazionale e molte altre istituzioni, con attacchi che sono durati da qualche settimana a oltre due anni, per non parlare di quelli ancora in atto, come nel caso della **World Anti-Doping Agency di Montreal**.

Ma la cosa più grave è che moltissime di queste vittime non erano consapevoli dell'attacco, che hanno scoperto soltanto dopo aver ricevuto l'avviso da parte di McAfee. L'ipotesi è che dietro ci sia uno Stato, ma McAfee non ha voluto fare nomi, per chiari motivi di delicatezza politica. Si tratta in ogni caso di una situazione davvero inquietante, che rinnova gli interrogativi riguardo la sicurezza dei dati in Rete e la capacità da parte delle istituzioni preposte di proteggerli efficacemente.