Cybercrime: scacco alla rete degli zombie

Infettavano pc in tutto il mondo con il virus Zeus, che permetteva ai cybercriminali di controllare da remoto il computer delle vittime. Questo consentiva agli hacker di carpire informazioni sensibili e utilizzare la macchina infestata a proprio piacimento, contro la volontà del proprietario.

L'operazione "Game Over Zeus" è stata portata a termine dagli agenti del Centro nazionale anticrimine Informatico per la protezione delle infrastrutture critiche (Cnaipic) della Polizia postale, in collaborazione con il Federal bureau of investigation (Fbi) statunitense, con il coordinamento dell'European cyber crime centre (EC3) di Europol.

L'indagine ha permesso di smantellare una Botnet, cioè una rete di pc "Zombie", chiamati in questo modo perché agiscono senza la volontà del legittimo proprietario, bensì con quella dell'hacker che li ha infestati con un virus.

Oltre a Italia e Stati Uniti, l'operazione ha coinvolto le polizie di Ucraina, Regno Unito, Germania, Giappone, Francia, Olanda e Canada. In questi ultimi due paesi, in particolare, è stato eseguito il sequestro di alcuni server dell'infrastruttura creata per la diffusione di zeus e cryptolocker.

Infatti il virus Zeus era utilizzato anche per diffondere il ransomware (dall'inglese ransom che significa riscatto, estorsione) denominato Cryptolocker, programma malevolo in grado di criptare i dati presenti sui computer delle vittime alle quali veniva poi richiesto il pagamento di un riscatto per la decriptazione.

In Italia sono stati individuati 160 nodi trust della rete Game Over Zeus, con almeno 10 mila pc infettati, che salgono a un numero compreso tra 500 mila e 1 milione in tutto il mondo, con un danno economico che si aggira intorno ai 100 milioni di euro.

Con questo sistema i cybercriminali potevano impadronirsi di dati come credenziali e password per l'autenticazione a servizi di banking online, oppure utilizzavano i pc controllati per effettuare attacchi di tipo Distributed denial of service (Ddos), cioè effettuati da più fonti contemporaneamente, evitando così di esporsi ed essere rintracciati dalle Forze dell'ordine.

English

03/06/2014