Cyber Crime: infettati più di 3 milioni di pc nel mondo

Più di tre milioni di computer in tutto il mondo erano sottoposti ad attacchi informatici di cyber criminali, attraverso una vera e propria rete di computer "zombie", smantellata dalla Polizia di Stato con l'operazione "Rubbly".

Il server della rete pirata, localizzato nell'area milanese, è stato sequestrato dai poliziotti del CNAIPIC (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche) e verrà messo a disposizione dell'European Cyber Crime Center di Europol per gli approfondimenti dell'attività investigativa.

Gli esperti della Polizia postale e delle comunicazioni hanno verificato che infettati i pc con il virus malevolo (malware), attraverso link contenuti nelle e-mail di spam o siti web, i cyber criminali sottraevano informazioni relative ad account bancari, password di accesso alla posta elettronica nonchè credenziali dei più noti social network.

Il malware associato alla botnet è noto con il nome "Ramnit" e colpisce computer con sistema operativo Microsoft Windows, riuscendo, tra le altre cose, a disabilitare i sistemi di protezione antivirus.

Inoltre, il virus sfrutta un meccanismo di generazione automatico di nomi di dominio (Dga) che successivamente vengono registrati ed utilizzati come server di comando e controllo (C&C) codificato all'interno del malware, cosa che ne rende molto difficoltosa l'individuazione.

L'operazione che ha consentito di neutralizzare i server di comando e controllo utilizzati dai cyber criminali, è il frutto di una stretta collaborazione tra la Polizia di Stato e l'European Cyber Crime Center (EC3) di Europol oltre alle unità specializzate nel cyber crime di Germania, Paesi Bassi e Regno Unito.

English

25/02/2015