Polizia di Stato

Internet:operazione "Rubbly", oltre 3mln pc sottoposti ad attacco

Si è conclusa oggi l'operazione "*Rubbly*" che ha permesso di smantellare una *botnet* ovvero una rete di computer "zombie"" controllata da un amministratore, il c.d. "*Botmaster*" e utilizzata dai cyber criminali per effettuare attacchi informatici di varia natura in danno di 3,2 milioni di computer in tutto il mondo. L'operazione è il frutto di una stretta collaborazione tra la Polizia di Stato e l'European Cyber Crime Center (EC3) di Europol e le unità specializzate nel *cyber crime* di Germania, Paesi Bassi e Regno Unito. Gli esperti della Polizia Postale e delle Comunicazioni hanno potuto verificare che, una volta acquisito il pieno controllo da remoto dei computer infettati dal virus malevolo (*malware*), i cyber criminali sottraevano informazioni relative ad account bancari, password di accesso alla posta elettronica nonché credenziali dei più noti social network. Durante le attività sono stati "spenti" i server di Comando e Controllo che venivano utilizzati come parte fondamentale del sistema di comunicazione della *botnet* ed allo stesso tempo Microsoft ha effettuato il *sinkhole,* prendendo quindi il controllo del traffico diretto ai C&C, di circa 300 nomi di dominio con estensione ".com". Il *malware* associato alla *botnet* è noto con il nome "*Ramnit*" e colpisce computer con sistema operativo Microsoft Windows, riuscendo tra le tante cose a disabilitare i sistemi di protezione antivirus. Inoltre, 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) che è codificato all'interno del *malware*, rendendo così molto difficoltosa l'individuazione degli stessi C&C. I vettori di infezione con cui la *botnet* si è diffusa, sono costituiti da link contenuti nelle e-mail di spam o siti web il cui contenuto è stato compromesso con l'inserimento di "*exploit kit*" che sono in grado di scaricare ed eseguire il codice malevolo sulla macchina dell'ignaro visitatore. Per questo motivo all'operazione hanno preso parte *stakeholder* dell'industria privata specializzati nella sicurezza IT (Microsoft, Symantec e AnubisNetworks) sulla scorta del già consolidato modello operativo che si fonda sul principio della *partnership* pubblico-privato. Microsoft e Symantec, in particolare, hanno rilasciato un tool per pulire e ripristinare i computer infetti raggiungibile agli indirizzi internet cyberstreetwise.com e getsafeonline.org.

Sul territorio italiano, il C.N.A.I.P.I.C. (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) della Polizia Postale e delle Comunicazioni ed il Compartimento Polizia Postale e delle Comunicazioni di Milano hanno sequestrato un server di comando e controllo localizzato nell'area milanese, che verrà messo a disposizione dell'European Cyber Crime Center (EC3) di Europol di EC3 per il prosieguo dell'attività investigativa.

"Il C.N.A.I.P.I.C.- dichiara Antonio Apruzzese Direttore del Servizio Polizia Postale e delle Comunicazioni - *interviene in favore della sicurezza delle Infrastrutture (istituzionali ed aziendali) connotate sempre più da una criticità intersettoriale per via dei vincoli di interconnessione ed interdipendenza esistenti tra i differenti settori e su una tipologia di minaccia che ha un'origine transnazionale e che potrebbe essere sfruttata anche per scopi di cyber-spionaggio/cyber-terrorismo".*

L'operazione - aggiunge Apruzzese- *è l'ulteriore risultato della proficua collaborazione tra Forze di Polizia europee e le partnership pubblico privato".*

Per ulteriori informazioni si invita a visitare il sito www.getsafeonline.org o www.cyberstreetwise.com.

25/02/2015