LA NUOVA BUSSOLA QUOTIDIANA DOMENICA
Direttore Riccardo Cascioli

MINACCIA FANTASMA

Virus WannaCry, antipasto di una cyber guerra

CRONACA 16_05_2017

WannaCry, il supervirus che nello scorso weekend ha colpito reti informatiche in 150 Stati del mondo, ha fatto parlare di sé e ha scatenato nuove polemiche sulle misure di sicurezza contro il cyber crime ma non ha certo arricchito gli hacker che lo hanno scatenato.

Secondo Ransom Tracker, il profilo Twitter creato dal ricercatore italiano Michele Spagnuolo

(che è Information Security Engineer presso la sede di Google a Zurigo) che in automatico traccia i singoli pagamenti, a ieri pomeriggio le vittime di WannaCry avevano pagato riscatti per un ammontare di soli 51mila dollari. I riscatti pagati dai diversi utenti colpiti nel mondo vanno da un minimo di 190 dollari ma toccano anche punte di 300 e 600 dollari nella “valuta virtuale” bitcoin.

Se il bottino finanziario è magro in compenso la bufera scatenata ha raggiunto i vertici governativi. Vladimir Putin, in visita a Pechino, non ha perso l’occasione per ricordare che “il management della Microsoft ha detto chiaramente che il virus è nato dai servizi d'intelligence degli Usa" e lanciare tali virus significa "sollevare un coperchio che poi può ritorcere contro chi l'ha creato". WannaCry sarebbe strato sottratto l’anno scorso, insieme ad altrui virus informatici, dagli “arsenali elettronici” della National Security Agency (NSA) dagli hacker del gruppo Shadow Brokers, che a quanto pare cercò di rivenderli sul Darkweb per poi distribuirli almeno in parte gratuitamente allo scopo di fare danni. Polemiche anche a Londra dove il virus ha colpito soprattutto il Ministero della Sanità e gli ospedali: dopo che il ministro degli Interni Rudd aveva ammesso sabato di non riuscire a risalire all’origine degli attacchi, il *Times* ha raccontato che l’allarme per un simile attacco era stato lanciato già da mesi accusando il governo di non aver preso nessuna misura cautelare.

Del resto il virus continua a colpire in queste ore dopo essere stato rallentato da un giovane hacker (così si racconta) che he aveva individuato una vulnerabilità: segno che gli Shadow Brokers o chi per loro hanno fatto evolvere il virus modificandolo e rendendolo meno attaccabile. Come per i veri virus sviluppati nei laboratori di guerra batteriologica durante la Guerra Fredda, anche per quelli informatici l’incubo peggiore è che vengano sottratti dalla banche dati del servizi di sicurezza come la NSA che nel 2010 impiegò il virus Stuxnet per danneggiare, ritardandolo di alcuni anni, il programma nucleare iraniano. Il caso WannaCry, ancora irrisolto, conferma la vulnerabilità di tutte le società avanzate che hanno affidato all’informatica la gestione degli apparati strategici, militari e civili e di tutti i servizi alla collettività.

Il “virus globale” ribadisce inoltre la furtività della minaccia cyber e la difficoltà a risalire al responsabile dell’attacco. Per questo appare stringente anche per l’Italia dotarsi di strumenti difensivi (ma anche offensivi per scoraggiare attacchi da altri Paesi)a livello nazionale e non solo nell’ambito di alleanze politico-militari come UnioneEuropea e NATO. A tal proposito il governo ha stanziato con l’ultima Legge di Stabilità150 milioni per la cyber defense ma non è ancora chiaro quali programmi verrannofinanziati.

La minaccia portata da organizzazioni criminali è oggi globale come quella rappresentata dai singoli Stati che spesso si celano affidando gli attacchi a gruppi privati di hacker per attaccare avversari ma anche amici e alleati che sono però al tempo stesso competitor economici.

WannaCry ha dimostrato la concretezza del rischio di un attacco cyber su scala globale ma si tratta probabilmente solo di avvisaglia di quello che potrebbe accadere se un virus paralizzasse anche solo per poche settimane la distribuzione di servizi essenziali come quelli sanitari, ferroviari o la rete elettrica.