AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

Primo Piano - *Conflitto USA-Iran, David Stupples: "il rischio di cyber attacchi è reale"*

Roma - 07 gen 2020 (Prima Pagina News) **Dopo l'uccisione del generale Soleimani, le reti informatiche statunitensi rischiano di essere attaccate dagli hacker di Teheran. Il commento dell'esperto di spionaggio informatico militare, cyber sicurezza e docente alla City University of London David Stupples**

"Dopo l'attacco col virus Stuxnet alle centrali nucleari iraniane, probabilmente per mano di Israele, l'Iran ha investito massicciamente nella guerra cibernetica. Oggi, si ritiene che faccia parte della serie A del cyberterrorismo finanziato dal regime per sostenere l'attività terroristica della Forza Quds. È un'opinione largamente condivisa che l'Iran sia stato all'origine, negli ultimi cinque anni, di gravi cyber attacchi a numerosi Paesi del Golfo e stabilimenti petroliferi dell'Arabia Saudita. Inoltre, sia gli Stati Uniti che l'Unione europea hanno dichiarato di aver subito cyber attacchi, per lo più finalizzati alla raccolta d'informazioni, all'interno delle proprie frontiere. L'Iran ritiene che, grazie alla guerra cibernetica, sia possibile danneggiare gli interessi occidentali. La propria capacità di kinetic warfare (guerra con utilizzo di armi tradizionali, per opposizione a cyber warfare, ndr) è limitata alla regione del Medioriente mentre un'ondata di forti attacchi cibernetici potrebbe rappresentare la vendetta che sta cercando. Gli obiettivi che hanno più probabilità di essere attaccati sono quelli visibili alla popolazione nel suo insieme. Targets che potranno far paura alla popolazione mettendo in evidenza la vulnerabilità degli Stati Uniti agli attacchi informatici e compromettendo così l'autorità del proprio Presidente e del proprio governo centrale. Probabili attacchi potrebbero colpire gli impianti petrolchimici, le centrali nucleari, i trasporti (marittimo e aereo) e le case farmaceutiche. L'obiettivo è di attaccare i sistemi di controllo industriale o del traffico aereo per fare in modo che i dispositivi di sicurezza diventino instabili e/o poco sicuri. Come, per esempio, i sistemi informatici SCADA (Supervisory Control & Data Aquisition) sono indispensabili per garantire l'efficacia operativa e la sicurezza per praticamente ogni impianto industriale complesso. Nel centro dello SCADA c'è un software e un sistema informatico complesso. L'Iran è noto per avere la capacità di attaccare gli SCADA con risultati abbastanza sconcertanti - un esempio è l'attacco alle infrastrutture petrolifere saudite Aramco due o tre anni fa. Si dice che l'Iran stia affinando le proprie capacità di guerra cibernetica grazie alle collaborazioni con la Corea del Nord, la Cina e la Russia. Gli Stati Uniti, come il Regno Unito, hanno incentrato la propria cyber sicurezza sugli SCADA ma pare che siano rimasti indietro, almeno quando si tratta di cyberterrorismo di regime dove più soldi sono stati investiti nel cosiddetto "dark web". Basterà che l'Iran ottenga una vittoria decisiva per esercitare una minaccia costante." Così il commento dell'esperto di spionaggio informatico militare, cyber sicurezza e docente alla City University of London David Stupples

AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

(Prima Pagina News) Martedì 07 Gennaio 2020

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it