Il Messaggero

17-NOV-2016
pagina 9
foglio 1 / 2

L'allarme degli 007 sul referendum: «Hacker all'attacco»

▶Contromisure dell'intelligence per fermare i pirati informatici: vogliono orientare il voto

ROMA Allarme dell'intelligence dopo quello lanciato dalla Ue sulla possibilità di nuovi attacchi degli hacker russi alle urne, anche a quelle italiane del prossimo appuntamento referendario. Gli 007 hanno rilevato anomalie sulla rete, un'attività irregolare che ha reso necessari maggiori controlli investigativi. L'assalto sembra aver puntato in particolare sul Comitato per il Sì.

Mangani a pag. 9

L'intelligence: gli hacker vogliono orientare il voto

▶Comitato per il Sì sotto attacco da giorni
Chi si collega si ritrova sul sito del No

▶Per i Servizi un'azione coordinata on line
L'allarme già nel colloquio Renzi-Obama

OGGI LA DENUNCIA FORMALE ALLA POLIZIA POSTALE I DATI: SU FACEBOOK 81MILIONI DI PROFILI FALSI 20MILIONI SU TWITTER

IL RETROSCENA

ROMA I social network come strumenti di contropotere. La Rete come veicolo per orientare e fare propaganda. E se finora eravamo abituati a fare i conti con Anonymus e gli attacchi contro siti istituzionali e di servizio, ora il fronte della "controinformazione" sembra puntare alle elezioni politiche, e in particolare a quella che ci riguarda, del 4 dicembre prossimo, quando gli italiani saranno chiamati a esprimersi sulla riforma Renzi-Boschi.

Strane cose stanno accadendo in questi giorni sul web, tanto da richiedere una presenza e un controllo più massicci da parte dei nostri servizi di intelligence e degli esperti della polizia postale e delle telecomunicazioni. Non sembra infatti così fantasioso l'allarme lanciato dalla Ue, che teme nuovi attacchi degli hacker russi sulle urne, e non esclude l'Italia con il suo appuntamento referendario. Ne sanno qualcosa gli americani, dove il gruppo The Dukes, noto anche come Apt29 e Cozy Bear, ha iniziato a infiltrarsi già durante l'estate nei registri elettorali della Democratic National Committee. E poi ha continuato a colpire diverse organizzazioni residenti a Washington con email di phishing che promettevano documenti scottanti sul tema elettorale e sulla possibilità di contestare la vittoria di Donald Trump.

L'ATTACCO

Nel nostro Paese, i "banditi" dell'online sembrano aver preso di mira il Comitato del Sì, che è vittima da più giorni di un massiccio attacco informatico. Se digiti www.bastaunsi.it ti ritrovi su siti dedicati al No. «Inoltre - spiegano - non possiamo pubblicare contenuti e gli utenti non possono più accedere al sito. Stiamo lavorando con l'aiuto di esperti per accertare la responsabilità di questi attacchi. Presenteremo una denuncia all'autorità di pubblica sicurezza».

Le manovre messe in atto dai pirati del web in Italia seguono diversi percorsi. E un sito messo fuori uso per qualche ora, preoccupa meno di un'operazione mirata a orientare e "indottrinare". Ne sanno qualcosa i nostri 007 che già devono fronteggiare le minacce terroristiche e che stanno notando un aumento di "bot", i profili fasulli, che rilanciano messaggi contro la riforma e


L'intelligence: gli hacker vogliono orientare il voto
VIA MARGUTTA TI ASPETTA!

chiedono di schierarsi per il No al referendum. Twitter, Facebook, Instagram, sono presi d'assalto. Naturalmente gli hacker non potranno modificare il dato finale dei voti. Il segno sulla scheda è a matita e i conteggi vengono fatti a mano. Ma è sul fronte propaganda che c'è grandissimo fermento.

FAKE E TROLL

E l'aspetto preoccupa parecchio lo stesso premier Matteo Renzi che, durante l'incontro di qualche mese fa con Obama, ha dichiarato: «I social network non sono attendibili come unico riferimento, in politica sono spesso infestati da fake, troll, che sono parte di strategie politiche. C'è una strategia di creare finti profili, che rilanciano messaggi o siti civetta e che lasciano pensare che quella informazione siccome è virale diventi vera. Non è così. Non è detto che ciò che è virale sia anche vero». Le piattaforme sociali, dunque, come "generatori di odio automatici". Con un fenomeno, quello dei falsi profili generati da robot, che fa registrare cifre enormi.

LE BOT FARM

Secondo alcune fonti, i "fake" su Facebook sarebbero circa 81 milioni, ma c'è chi parla anche di 170. Su Twitter, invece, circa 20 milioni, anche se del pacchetto fanno parte tante utenze silenti e in generale gli strumenti che permettono questi check-up non funzionano poi così bene. Inoltre esistono società specializzate di social media marketing - vere e proprie "bot farm" come la misteriosa Rantic che sforna fino a 50mila fake al giorno, anche se la maggior parte ha sede in India, Bangladesh e Filippine - che, utilizzando numerosissimi intermediari, fanno da anni ricchi affari. Gli scopi della creazione di queste false utenze sono vari. E se prima si parlava di "social doping", cioè di un aumento dei follower e del seguito, oggi si spazia dalle recensioni finte alla lotta e alla propaganda politica.

Cristiana Mangani