CORRIERE DELLA SERA

01-AGO-2016
pagina 7
foglio 1 / 2

Corsari del web a caccia per Putin

Squadre di hacker ingaggiati per colpi clamorosi. Senza lasciare molte tracce. Come incastrarli?

Lo strumento
L'ex Armata Rossa ha utilizzato quest'arma in occasione di molte crisi internazionali

Il Partito democratico americano era stato messo sul chi vive dall'Fbi già mesi fa: attenti, cercheranno di penetrare nel vostro sistema. Un allarme unito ad altri sulle incursioni di hacker stranieri negli Usa, rapporti inviati al presidente Obama fin dal 2009. Eppure la breccia c'è stata comunque. Perché a scavarla — secondo le accuse statunitensi — sono stati i «migliori». Gli investigatori sono convinti che ci sia la mano dei pirati russi, non nuovi a questi assalti.

Mosca — come Washington, Pechino, Pyongyang e Gerusalemme — ha investito molto in questa arma, poco visibile ma in grado di fare danni. Come hanno sottolineato gli analisti, si tratta di una minaccia che dallo spazio «cyber» può passare a quello fisico in pochi attimi. Perché non solo è in grado di carpire segreti — da quelli finanziari ai dati personali — ma riesce a innescare reazioni a catena devastanti. Si paralizza una centrale, si manda in tilt un sistema di controllo.

I russi, maestri dello spionaggio e delle guerre delle ombre, hanno garantito risorse al famoso Politecnico di San Pietroburgo, dove nelle sue aule studierebbero degli esperti pronti poi a collaborare con il settore militare. Lo stesso vale per un centro all'interno dell'Università di Samara. Molto teoria e tanta pratica davanti ai computer. Lo Stato Maggiore dell'ex Armata Rossa si è esercitato ed ha poi utilizzato questa «freccia» in occasione di ogni crisi internazionale importante.

Nel 2007 contro gli estoni, nel 2008 durante il conflitto con i georgiani, nel 2014 nel mezzo del confronto sulla Crimea. Una copia di quanto fatto dagli Stati Uniti e da Israele contro gli apparati petroliferi iraniani con l'ormai famoso virus Stuxnet. Sabotaggio che ha spinto Teheran a dotarsi di unità speciali poi utilizzate nella prova di forza con l'avversario saudita.

Mosca, in caso di necessità, ha una doppia scelta. Affidare le missioni ai servizi segreti oppure ingaggiare team di hacker che si dedicano ad attività illegali. Di fatto ha trasferito metodi già visti sul terreno reale. Per eliminare i separatisti ceceni all'estero hanno chiesto la collaborazione di figure vicine al mondo del crimine. Personaggi che, se catturati, possono sostenere di aver agito per «altri motivi». Stessa cosa nel confronto via web. Sempre indiscrezioni americane chiamano in causa degli specialisti, noti come Apt28, Apt29, FancyBear, CozyDuke, CosmicDuke, MiniDuke. Sono come corsari, fanno la guerra per conto di un governo, in questo caso quello russo. Anche se non è sempre facile «tracciarli». Il rischio della «falsa bandiera» è sempre in agguato: chi colpisce cerca di nascondersi e fa ricadere la responsabilità su altri.

Quanti osservano questa battaglia aggiungono che gli 007 di Putin hanno molte carte in mano e sono in grado di ottenere dagli hacker ciò che vogliono. Un esempio pratico: sanno che mister X ha svaligiato conti in banche europee con una mossa cyber, allora lo contattano, lo mettono sotto pressione e in cambio dell'immunità lo convincono a «lavorare» per loro. Le inchieste internazionali hanno rivelato come le bande dell'Est abbiano messo a segno dei colpi clamorosi.

Ovviamente siamo sempre in un'area opaca. Hillary Clinton è certa dello zampino dello «zar». Il Cremlino respinge tutte le accuse. Le prove che stabiliscano un legame netto tra chi attacca e Mosca — riconoscono molti — sono complesse da raccogliere. La propaganda nei momenti di tensione pesa sugli scambi polemici. Inoltre il duello per la Casa Bianca è feroce, e la presunta intromissione straniera ne allarga le implicazioni. Detto questo, Washington aspetta l'appuntamento elettorale di novembre con grande apprensione.

Non sarebbe strano se i nemici invisibili — che sono tanti — tentassero di disturbare le elezioni presidenziali.

Guido Olimpio
@guidoolimpio

I precedenti

1 Corea del Nord
Il 24 novembre 2014 un gruppo di hacker «buca» i server della Sony. Dati i riferimenti al film «The Interview» sulla vita di Kim Jong-un, si sospetta che dietro l'attacco ci sia la Corea del Nord

2 Russia
Nell'ottobre 2014 hacker russi violarono la rete non classificata della Casa Bianca. L'intrusione informatica avrebbe riguardato anche l'agenda privata del presidente

3 Cina
Nel giugno 2011, in pieno scandalo Strauss-Khan, i server del Fondo monetario internazionale vengono attaccati. Secondo l'Fbi l'hackeraggio sarebbe opera di pirati informatici cinesi

La vicenda

- Il 23 luglio WikiLeaks, l'organizzazione guidata da Julian Assange, ha pubblicato 19.252 mail del Partito democratico
- Vertici del Partito democratico avevano denunciato l'hackeraggio in giugno e l'Fbi aveva avviato un'indagine
- Dopo l'hackeraggio si è parlato di un coinvolgimento russo: Assange alla tv russa ha manifestato la sua ostilità alla candidatura di Hillary alla Casa Bianca, indicandola come nemica
- Sia *il Guardian* che il *New York Times* indicano come possibile il coinvolgimento del gruppo hacker «Fancy Bear» che sarebbe legato all'intelligence russa. Anche l'hacker di origine rumena Guccifer è stato indicato come autore dell'attacco. Pure lui sarebbe legato a Mosca