# Guerra informatica

9 Ottobre 2018

Da Rassegna di Arianna del 7-10-2018 (N.d.d.)

A quanto pare, la storia è così: in aprile, grazie alle indagini congiunte del controspionaggio di Olanda, Usa, Svizzera e Canada, quattro agenti russi specializzati nello spionaggio informatico sono stati fermati a l’Aja e poi, essendo dotati di passaporto diplomatico, espulsi verso la madre patria. I quattro, secondo le cronache, stavano cercando di hackerare le comunicazioni dell’Opac (Organizzazione per la proibizione delle armi chimiche, già premio Nobel per la pace nel 2013), presumibilmente per scoprire qualcosa sulle indagini che l’Organizzazione sta svolgendo sugli attacchi chimici che l’esercito siriano avrebbe condotto nella città di Douma. La questione è seria, anche se ovviamente per ragioni tutte diverse da quelle raccontate in questi casi. Le cronache dell’arresto dei quattro sono piene di sciocchezze. Per hackerare i computer dell’Opac, gli agenti russi (gli agenti di qualunque servizio segreto) non avrebbero certo avuto bisogno di piazzarsi nel parcheggio dell’hotel dove ha sede l’Opac stessa. Così come fa ridere la considerazione, esposta con grande solennità come se fosse una prova, che uno stesso computer portatile avrebbe “lavorato” in Brasile (per infiltrarsi nei laboratori dove si conducono indagini sul doping degli atleti, questione scottante per la Russia), in Svizzera (altro laboratorio dell’Opac, che si occupa del caso Skripal) e in Malaysia (abbattimento del volo Amsterdam-Kuala Lumpur sui cieli dell’Ucraina, nel 2014). Da quando per hackerare qualcosa o qualcuno è necessario avvicinarsi? Quando mandiamo una mail spostiamo il computer vicino a chi deve riceverla? Altro elemento da oggi le comiche. Uno degli agenti russi avrebbe commesso una distrazione fatale, tenendosi in tasca una ricevuta del taxi che, dalla sede del Gru (il servizio segreto militare), posta in pieno centro di Mosca, l’avrebbe portato in aeroporto. È da escludere che un agente esperto possa fare un errore di questo genere, ma siamo abituati a sentirci raccontare anche di peggio. Per esempio che l’agente, anche lui del Gru, che avrebbe violato i server del Partito democratico americano nel 2016 era stato scoperto dall’Fbi perché, dopo aver completato con successo l’intrusione (da Mosca, peraltro, senza andare col computer fino in America), con lo stesso computer, con lo stesso indirizzo Ip e senza usare programmi di schermatura si era messo a navigare su Twitter.

All’arresto dei russi a L’Aja è seguita, com’è ovvio, la solita raffica di dichiarazioni. James Mattis, ministro della Difesa Usa, ha detto che “la Russia dovrà render conto di questi attacchi”. Il governo olandese ha convocato l’ambasciatore russo. Donald Tusk, il polacco che preside il Consiglio europeo, ha deciso di inserire il tema del cyber spionaggio russo all’ordine del giorno del Consiglio del 18/19 ottobre, preludio forse ad altre sanzioni contro la Russia. E Jens Stoltenberg, segretario generale della Nato, ha detto che “la Russia deve cessare il suo comportamento sconsiderato”, ottima scusa per ulteriori dispiegamenti delle truppe Nato nell’Europa dell’Est. Folklore e veline a parte, però, la situazione si sta facendo davvero seria. Perché ciò a cui stiamo assistendo sono i prodromi e i test per una guerra informatica su scale globale, in cui tutti i paesi sono coinvolti. Che a noi la raccontino come una campagna della Russia contro il resto del mondo fa parte del gioco e nulla più. Lo dimostra la vicenda di NotPetya, il virus informatico più “cattivo” della storia che nel 2017 è stato immesso nelle reti dell’Ucraina e da lì, grazie all’interconnessione ormai quasi globale, ha infettato mezzo mondo, mandando in bomba milioni di computer, colpendo uffici e aziende grandi e piccole, infliggendo un totale di 10 miliardi di dollari di danni ( il colosso farmaceutico Merck, secondo le valutazioni di Wired, avrebbe perso 870 mila dollari, Federal Express 400 mila, l’impresa di costruzioni francese Saint Gobain 384 mila, la compagnia danese di spedizioni marittime Maersk 300 mila e così via). I servizi segreti Usa accusarono subito il solito Gru, anche se NotPetya colpì duramente anche la Russia, sabotando per esempio le operazioni del colosso statale RosNeft, terza compagnia petrolifera del Paese. Gli esperti si divisero sul senso dell’attacco: secondo alcuni, l’obiettivo era “solo” fare il massimo del danno; secondo altri, l’intento era anche di cancellare memorie e programmi e condurre una specie di prova generale di ciò che si potrebbe fare, domani, per paralizzare e mettere in ginocchio un Paese considerato ostile. Tanto più che, stando alle successive indagini, gli hacker erano rimasti annidati per mesi nel sistema di comunicazioni ucraino, prima di colpire. Quello che non è mai arrivato al grande pubblico è questo. NotPetya non era un programma originale. La sua devastante peculiarità era di combinare Eternal Blue e Mimikatz, due programmi usati per penetrare i computer ed estrarre le password. E chi aveva sviluppato quei due programmi? EternalBlue è una creatura della National Security Agency (Nsa) americana, mentre Mimikatz fu sviluppato nel 2011 da Benjamin Delpy, un esperto di informatica dei servizi segreti di Francia. E secondo voi, Stati Uniti e Francia certi giocattoli li inventano per poi tenerli nel cassetto? Queste cose le sappiamo grazie… agli hacker. In particolare grazie a Shadow Broker, che tra 2016 e 2017 ha infiltrato i computer della Nsa e rivelato un po’ dei suoi segreti, compresi quelli relativi a certi attrezzi del mestiere come EternalBlue. L’attacco fu prima attribuito a un tecnico di un’azienda informatica che collaborava con la Nsa, tale Harold Martin, poi finito in galera, quindi ai soliti russi. Comunque sia, abbiamo appreso che all’interno della Nsa c’è una speciale unità, all’epoca chiamata Tailored Access Operations (Tao) e poi ribattezzata Computer Network Operations (Cno) in cui lavorano più di mille tra hacker, ingegneri elettronici e analisti, sia militari sia civili. E che la Tao/Cno, oltre a sviluppare micidiali armi elettroniche, è abituata a pratiche come: intercettare i computer acquistati online, inserire in essi sistemi di spionaggio e poi farli

arrivare agli acquirenti; intercettare le comunicazioni dell’Opec, l’organizzazione dei produttori di petrolio; intercettare le comunicazioni dai cavi sottomarini a fibre ottiche che collegano decine di Paesi, tra cui l’Italia; hackerare i ministeri del Messico, in particolare quelli della pubblica sicurezza; passare tecnologie ai servizi segreti inglesi che, con quelle, hanno intercettato il traffico di diversi provider europei tra cui Belgacom, che garantisce le comunicazioni al Parlamento europeo e alla Commissione europea; più una serie di altre prodezze simili. Coloro che attribuivano l’attacco di Shadow Broker ai soliti hacker del Cremlino, davano del gesto questa interpretazione: la Russia sta ammonendo gli Usa ad andarci piano con le loro campagne, perché in ogni momento potrebbe svelare certi segreti che agli americani non piace render pubblici. A noi la propaganda non interessa. Ciò che conta è capire che siamo nel bel mezzo di una potenziale guerra informatica virtuale, proprio come Siria, Ucraina, Iran, Palestina e altri fronti sono gli scenari materiali della stessa guerra. Le fake news su un solo Paese “cattivo” che terrorizza il mondo mentre i Paesi “buoni” subiscono o al massimo cercano di difendersi, sono quello che sono. Fake news, appunto.

Fulvio Scaglione