



CYBERWAR

SABOTAGGIO, SPIONAGGIO, VIRUS INFORMATICI E AZIONI DEGLI HACKER: È LA GUERRA CIBERNETICA. PERCHÉ IL PERICOLO, OGGI, CORRE (ANCHE) SUL WEB
DI GABRIELE ROSANA ILLUSTRAZIONE DI LORENZO FROSI

0 1 0 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 1 0 0 0 0 1 1 1 1
 1 SCENARI 1 0 0 0 0 1 1 1 1 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1
 0 0 1 1 0 1 0 0 0 1 1 1 1 1 0 0 1 1 0 1 0 0 1 0 0 0 1 1 0 0 0 1
 0 0 1 0 1 1 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1
 0 0 0 1 1 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 1 1 1 0 1 0 0 1 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 1 1 0 1 0 0 0 1 1 1 1 1 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0
 0 0 1 1 ANONYMOUS 0 1 1
 0 1 1 0 0 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 1 1 0 0 0 1 0 0 0 1 1 0 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1
 1 1 0 0 1 0 0 0 0 0 0 0 0 1 1 0 1

0 0 1 0 1 0 0 1 0 0 1 1 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 1
 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
 0 0 0 1 0 1 1 1 1 1 0 0 1 1 1 1 0 0 0 1 0 0 0 1 0 1 1 1 1
 0 0 0 0 0 0 0 1 1 W O R M 1
 1 0 1 1 1 0 1 0 1 0 0 1 0
 1 0 0 0 1 0 1 1 0 1 1 1 0
 0 1 0 0 0 0 0 0 0 0 0 0 1
 0 0 1 1 0 1 1 0 1 0 0 0 0
 0 0 1 1 1 1 0 1 0 1 0 0 1
 0 1 0 0 1 0 1 0 1 0 0 0 0
 1 B O T N E T 1 0 1 1 1 0
 1 0 0 0 1 1 0 0 0 0 1 1 0

IN NUMERI

6mila

gli hacker al servizio del regime nordcoreano

30

le nazioni a oggi in grado di costituire una minaccia cyber, secondo l'intelligence americana

750mila

le identità digitali a rischio hacking in Estonia, mentre 230mila sono stati i cittadini ucraini costretti al buio dopo il sabotaggio delle infrastrutture elettriche

18

gli Stati che avrebbero condotto a oggi operazioni di attacco cyber

20mila

gli account del Parlamento tedesco "bucati" da sospetti hacker russi

registrati nel palmarès dei nerd nordcoreani, due obiettivi di tutto rispetto: la Federal Reserve di New York e la Sony Pictures.

Gli hacker di Kim si sono invece fermati sulla soglia delle Olimpiadi di Pyeongchang in Corea del Sud, durante le quali non risultano tentativi di sabotaggio da parte dei cugini del nord, impegnati com'erano a usare l'evento come vetrina per sponsorizzare il disgelo tra i due Paesi all'altezza del 38° parallelo. In compenso, ci hanno pensato i russi (o almeno, così si dice; non solo è complesso attribuire un attacco cyber, ma l'ambito è a forte tasso di segretezza e gli Stati tendono a non scoprirsi più di tanto, con informazioni segretate): un'operazione ha oscurato per mezza giornata la pagina web ufficiale dei Giochi e turbato il funzionamento del wi-fi e dei televisori dello stadio olimpico.

La tensione cyber, insomma, non sembra curarsi della pax olimpica. Ne sanno qualcosa i brasiliani, che durante un'altra edizione dei Giochi (quelli del 2016 a Rio de Janeiro) hanno ottenuto la medaglia d'oro per la mole di attacchi di phishing, aventi come obiettivo le caselle di posta elettronica dei tantissimi appassionati presenti, a conferma della varietà di impieghi dell'arma cyber e dei profili degli hacker: non sono solo Stati, ma anche organizzazioni criminali più o meno complesse, attivisti politici, autonomi, persino terroristi. L'Isis di tanto in tanto rivendica aggressioni

informatiche (come quando si "impossessò" della home page e dei social media della francese TV5 Monde), ma impiega l'ambiente digitale principalmente come veicolo di propaganda. Al pari dei vettori di fake news, che sfruttano la Rete per influenzare l'andamento degli appuntamenti elettorali. Tutto questo a conferma della tesi per cui «l'ambiente digitale altro non è che la prosecuzione di quello fisico, la continuazione di uno

spazio civile e politico unico», aggiunge Darnis.

Dall'intrusione nei server del Partito democratico statunitense nel 2016 al furto delle informazioni su 20mila account attivi nella rete informatica della Camera bassa del Parlamento tedesco: neppure le arene del gioco democratico riescono a difendersi dalle operazioni cibernetiche. Ma la verità è che forse, in questa guerra, siamo davvero soltanto alle prime battute. «Nessun attacco cyber finora ha avuto un effetto tale da poter essere considerato al pari di un'aggressione militare». Un buon motivo per tenere alto il livello di guardia, suggerisce Tommaso De Zan, «tenendo presente che una continua espansione dell'Internet of things aumenta esponenzialmente la superficie di attacco per gli hacker. Non possiamo insomma escludere che un'intrusione informatica possa avvenire sfruttando la connessione Bluetooth di dispositivi smart come Fitbit, che utilizziamo quotidianamente per tener traccia della nostra attività fisica. Ecco perché sarà indispensabile puntare non solo sull'educazione e la consapevolezza digitale di tutti, ma anche sulla sensibilità al tema della classe politica e dei vertici militari». Una situazione magmatica, che porta Darnis a presagire la necessità di un'alleanza tra l'Occidente e le grandi aziende del mondo digitale: «La posta in gioco è la tutela dei diritti individuali e la sopravvivenza delle democrazie moderne».

PRIMAVERA 2016

USA, hacker entrano nei server del Democratic National Committee durante le presidenziali, rubando materiale informativo.

LUGLIO 2016

FILIPPINE, nel giorno della sentenza favorevole all'Aja sulla sovranità nel Mar Cinese meridionale, attacchi a 68 siti del governo.

MAGGIO 2017

FRANCIA, migliaia di email e altri documenti della campagna elettorale di Macron vengono pubblicati appena prima del voto.

GIUGNO 2017

VARI STATI, il ransomware WannaCry è usato per cifrare dati: per la decrittazione viene richiesto un riscatto.

LUGLIO 2017

ITALIA, attacco informatico contro il gruppo bancario UniCredit, acquisito l'accesso ai dati di 400mila correntisti.

FEBBRAIO 2018

COREA DEL SUD, un attacco attribuito alla Russia oscura per 12 ore il sito ufficiale delle Olimpiadi invernali di Pyeongchang.