RISCHI GLOBALI Il fronte digitale

Armiamoci di bit

di **Corrado Accaputo**

Aziende, governi, media, privati: la guerra on line è scoppiata per tutti. Ecco come viene combattuta

Dalle segrete stanze della Casa Bianca e del Pentagono filtra un po' di nervosismo. I rapporti consegnati dagli analisti sono allarmanti: il 2017 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce cyber. Un fenomeno «fuori controllo». La stima dei danni globali è di circa 500 miliardi di dollari. Non solo malware e attacchi su scala planetaria contro target multipli: a preoccupare è soprattutto la definitiva discesa in campo degli Stati come attori principali di una guerra informatica. Ma anche il tentativo di interferire nella vita dei cittadini e sul piano finanziario e geopolitico. Studi di settore lo hanno certificato anche in Italia: secondo Clusit, l'Associazione italiana per la sicurezza informatica, 1.127 attacchi «gravi» sono stati registrati nel mondo lo scorso anno. Una media di 94 al mese. Quasi un miliardo di persone ha subito estorsioni, truffe, furti di denaro e dati: per i privati cittadini si tratta di una perdita stimata in 180 miliardi di dollari.

Una minaccia che secondo le analisi degli esperti Usa crescerà ancora, in vista delle elezioni di medio termine a novembre negli Stati Uniti, e nel 2019 quando il dominio della cyber security dovrà essere per Washington la principale tra le priorità. Ne è convinto Dan Coats, il capo dell'Intelligence nazionale americana, che in una sua recente relazione non ha nascosto il timore di un futuro conflitto tra Stati, anche sul terreno della sicurezza informatica. Una vera e propria guerra senza esclusione di colpi, strumenti e target. Con l'obiettivo finale di plasmare società, mercati, accordi, regole, istituzioni nazionali e transnazionali a uso e consumo di un'incontrastata supremazia mondiale. Quella a cui aspirano, secondo gli esperti di Washington, nemici di vecchia e nuova generazione: la Russia, con cui i rapporti sono tornati ai tempi della guerra fredda, la Cina, la Corea del Nord e l'Iran.

Negli ultimi mesi l'attività di alcuni di questi Paesi è stata fervida. Pesantissime interferenze di natura cyber sono state segnalate durante le presidenziali negli Stati Uniti e in Francia. Nel mirino sono finiti gli esperti di Mosca, additati come i principali responsabili. Persino la tregua olimpica è stata violata all'inizio dei Giochi invernali di PyeogChang. Società di servizi pubblici, produttori di schermi video, media, compagnie di telecomunicazione, aziende edili sono stati oggetto di attività di pirateria. Per le agenzie di sicurezza americane il momentaneo blackout sarebbe stato provocato dall'Olympic Destroyer, un malware di origine russa apparentemente veicolato dall'intelligence militare di Mosca (Gru) sotto «falsa bandiera». Chi ha gestito l'operazione avrebbe però utilizzato provider nordcoreani con il chiaro intento di chiamare in causa il regime di Pyongyang. Che da parte sua in questi mesi non è rimasto certo a guardare. Il leader Kim Jong Un ha chiesto la creazione di una nuova unità di cyber spie di Stato (Apt37 Reaper), recentemente individuata dai ricercatori della società di sicurezza informatica Fire Eye, e il suo governo sta espandendo le proprie capacità cyber con l'obiettivo di colpire in via prioritaria Corea del Sud, Giappone, Vietnam e parte del Medio Oriente. Per poi magari spingersi un po' più in là e provare a penetrare i sistemi americani.

Per farlo serve un livello di sofisticazione assai elevato e quello raggiunto dagli esperti nordcoreani, sebbene in costante evoluzione, non sarebbe ancora tale. Sono altri i Paesi attualmente in grado di paralizzare o distruggere sistemi e infrastrutture essenziali, persino vitali. Almeno in sette nel mondo hanno questa capacità: oltre a Stati Uniti, Russia e Cina, anche Regno Unito, Canada, Australia e Nuova Zelanda. È il livello massimo di insicurezza cibernetica: «catastrofico». A questo stadio, obiettivi civili e militari, reti energetiche e di telecomunicazione, interi settori della società - Sanità, Giustizia, Sicurezza, Difesa, Finanza, Commercio - possono subire danni irreparabili. Informazioni, dati e funzioni di primaria importanza verrebbero compromessi per un tempo prolungato o in via definitiva. Una minaccia tanto più pericolosa dopo le ultime informazioni ottenute dagli esperti americani. Pechino e Mosca lavorano da tempo all'acquisizione di tecnologia di intelligenza artificiale allo scopo di coordinare attacchi informatici di massa a basso costo. E sarebbero pure parecchio avanti. Molti vantaggi e pochi rischi: scarsa manodopera, massima efficacia. Rapidità di apprendimento, riproduzione e diffusio-

Strategie di difesa prima di un attacco informatico

ne di metodi e tecniche di intrusione su scala finora impensabile. Milioni di virus inviati contemporaneamente a personal computer e smartphone con un allegato infetto, che renderanno gli attacchi di phishing più potenti, auto-diffondenti, multi-target. Una campagna sofisticata e automatizzata, simultanea e coordinata, per rubare informazioni e distruggere sistemi, senza un coinvolgimento diretto di hacker.

Un rischio che richiede un'attenzione degli Stati molto alta. E che introduce un nuovo elemento di preoccupazione. «Le tecnologie di intelligenza artificiale se da una parte permettono una difesa migliore dall'altra consentono di poter attaccare in modo più efficace», commenta Alessandro Piva, dell'Osservatorio Information Security and Privacy del Politecnico di Milano. L'Italia in questo campo è rimasta indietro. «La situazione nel nostro Paese è un po' preoccupante perché non sembra esserci la percezione di questi temi nel dibattito politico quotidiano». Solo a settembre dello scorso anno, ad esempio, è stato costituito ufficialmente il Cioc, il Comando interforze per le operazioni cibernetiche. Protegge reti e informazioni militari. Ma in generale resta evidente un quadro di colpevole ritardo nella conoscenza di questi strumenti e di scarsa dimestichezza con le tecnologie digitali. Una condizione che «ci colloca sicuramente tra i Paesi più a rischio di attacchi, tra quelli avanzati», sottolinea l'esperto. E il generale di brigata aerea Francesco Vestito, che guida il Cioc, conferma: «Il cyber crime è attualmente il rischio più elevato», mentre «la cyber warfare ha fatto registrare una tendenza a crescere da tenere sotto controllo».

Certo non aiuta la cronica insufficienza di investimenti in cyber security nel nostro Paese, che ci pone all'ultimo posto tra quelli sviluppati. Il mercato delle soluzioni di information security in Italia nel 2017 ha raggiunto un valore di poco superiore a un miliardo di euro, i danni complessivi ammontano invece a circa 10 miliardi. «C'è stato un incremento della spesa del 12 per cento sul 2016», ma nonostante il trend positivo resta l'evidenza di un dato «molto piccolo» che conferma un problema strutturale: «gli investimenti da parte delle nostre aziende rappresentano solo una frazione minima rispetto ai danni che possono derivare da attacchi cyber», precisa Piva. In questo modo, le difese del Paese contro Cyber crime, Information warfare e Cyber espionage - fenomeni in forte crescita a livello mondiale - restano piuttosto basse; mentre i tempi medi tra un attacco, la sua individuazione e l'attuazione di attività di contrasto permangono molto lunghi.

Insomma, il problema è stato «sottovalutato per anni» e ancora oggi scarseggiano le competenze all'interno delle imprese. Anche in questo campo le grandi società italiane «sono rimaste indietro»: «solo poco più del 50 per cento di queste ha in organico una figura di riferimento che si occupa di information security. E anche quando sono presenti, queste figure non hanno una funzione gerarchica tale da poter esercitare un ruolo importante nelle scelte societarie».

Resta dunque l'urgenza di mettere in atto forme di gestione della sicurezza basate sul rischio, a fronte di una crescente disponibilità di tecnologie che consente la dotazione di armi sempre più sofisticate. Secondo Alon Arvatz, cofondatore di IntSights, siamo in un momento in cui «le nazioni stanno testando i loro limiti e valutando le reazioni». Una fase «prebellica» in cui la guerra globale è stata già dichiarata. Difficile capire chi ha sparato il primo colpo. Ancora di più sapere chi esploderà l'ultimo. ■