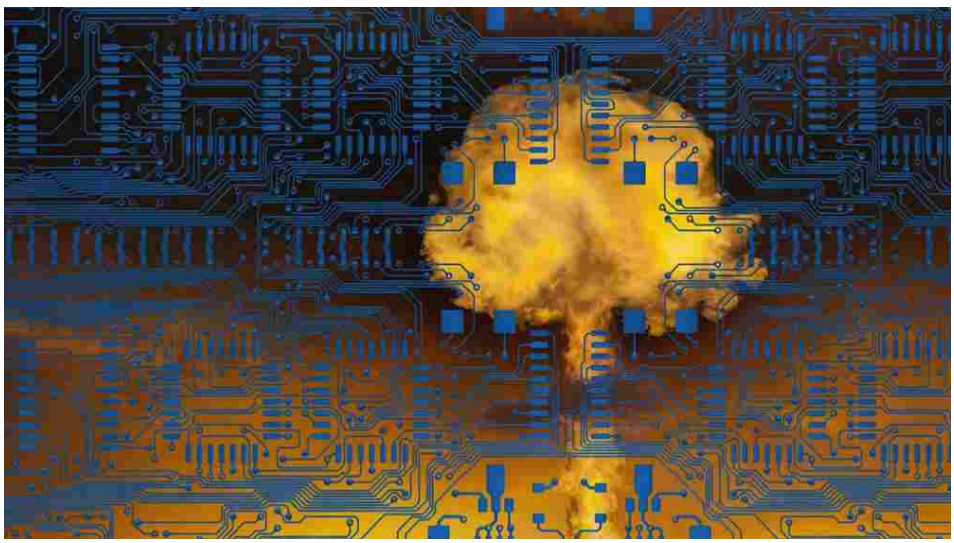
La quarta rivoluzione industriale mette al centro i dati
Il tocco che comanda: nei tatuaggi intelligenti la nuova frontiera dei ...
Ansip: contro le fake news in Europa serve più chiarezza
La luce perfetta in ufficio la regalerà un'app
DynamiTick: come riempire stadi e cinema con l'intelligenza artificiale

Quando l'hacker è uno Stato

Un estratto dal libro di Carola Frediani, "Guerre di rete", che spiega come virus e malware siano diventati parte fondamentale dell'arsenale militare dei governi di tutto il mondo



LEGGI ANCHE

ANSA
Molti siti hanno diffuso dati privati per errore, incluse le password
CAROLA FREDIANI

VIDEO CONSIGLIATI

È arrivata IperFibra. IperFibra senza costi d'attivazione e sconto canone 25€
Raccomandati da eDintorni

CAROLA FREDIANI
Pubblicato il 23/03/2017

Carola Frediani, esperta di nuove tecnologie, cultura digitale, privacy, hacking e altro, lavora per La Stampa. Ha scritto Dentro Anonymous. Viaggio nelle legioni dei cyberattivisti (Informant, 2012), Deep web. La rete oltre Google - personaggi, storie e luoghi dell'internet profonda (Quintadicopertina, 2014) ed è stata coautrice di Attacco ai pirati. L'affondamento di Hacking Team: tutti i segreti del datagate italiano (La Stampa - 40k, 2015). Il suo ultimo libro è Guerre di rete (Laterza, 2017), del quale pubblichiamo qui un estratto.

Stuxnet: la prima arma digitale

Il fenomeno dell'hacking statale o parastatale esisteva già da tempo, ovviamente, anche se più contenuto e sotto traccia. In un certo senso, l'anno zero – in cui si è strappato il cielo di carta – è stato il 2010, con la scoperta di Stuxnet. Questo malware ha alterato di nascosto la velocità delle centrifughe dell'impianto per l'arricchimento dell'uranio a Natanz, in Iran, portando alla sostituzione forzata di mille macchine. E questa è la prima novità: diversamente da altri virus o worm che puntavano a rubare informazioni o a violare e danneggiare sistemi informatici, Stuxnet realizzava, attraverso i computer, un'operazione di sabotaggio fisico. Il software malevolo era concepito in modo tale da modificare anche le informazioni che arrivavano ai tecnici, così che non si accorgessero della natura del malfunzionamento e la attribuissero ad altre cause.

Secondo il già citato Ralph Langner, il 50 per cento dei costi di sviluppo di Stuxnet è probabilmente andato nel tentativo di nasconderlo. Il malware era estremamente sofisticato. Usava ben quattro "zero-day", ovvero vulnerabilità di un software che non sono ancora note a nessuno se non all'attaccante. Si chiamano così perché gli sviluppatori dei programmi vulnerabili, non avendo idea della loro esistenza, hanno avuto "zero" giorni a disposizione per metterle a posto. Inoltre Stuxnet ha dovuto anche aggirare il fatto che i computer di controllo del sistema da attaccare non fossero collegati a Internet. Per saltare questo "vuoto d'aria", il fatto cioè che i pc fossero separati dalla Rete, ha utilizzato come vettore d'attacco delle chiavette Usb. Gli attaccanti hanno prima infettato i computer di almeno quattro aziende esterne all'impianto di Natanz, che però erano connesse al programma nucleare iraniano o erano suoi fornitori, e da lì sono arrivati al loro target finale.

Ci sono state varie versioni di Stuxnet, in un crescendo di aggressività del malware. Tecnicamente era un worm, un virus che si sparge – oltre che per mezzo di Usb drive – attraverso la Rete. Pur potendo replicarsi e diffondersi su molti computer, rimaneva dormiente provocando solo misteriosi malfunzionamenti se non incontrava particolari condizioni, se non si trovava cioè su una macchina di un sistema di controllo industriale con specifiche configurazioni. Di fatto, però, Stuxnet col tempo si è diffuso in un centinaio di Paesi: qualcuno ha contato 300mila infezioni.

Altra novità di questo malware è che nasce apertamente da un progetto statale. Nel 2012 è arrivata la conferma di quello che molti sospettavano: e cioè che Stuxnet è il frutto di una collaborazione statunitense-israeliana. In particolare

faceva parte del piano americano "Olympic Games" – avviato sotto la presidenza di George W. Bush – che voleva sabotare il programma nucleare iraniano con un attacco informatico. Stuxnet è stata dunque la prima arma digitale sviluppata da uno Stato ed effettivamente usata a scopi offensivi. Secondo alcuni osservatori, l'impiego di questo malware avrebbe avuto il merito di impedire un intervento militare vero e proprio. Una "bomba digitale" avrebbe ottenuto effetti simili a quelli di un'incursione fisica ma in modo discreto e sotterraneo, danneggiando le centrifughe silenziosamente per mesi senza dare nell'occhio. Uno dei suoi vantaggi fondamentali era la possibilità di intervenire di nascosto e, qualora il malware fosse stato scoperto, di negare in modo plausibile di esserne i mandanti. C'è un'espressione tecnica, usata sia nello spionaggio sia nella sicurezza informatica, per indicare questa mossa: plausible deniability, appunto negazione (letteralmente, negabilità) plausibile.

Tuttavia, a medio e lungo termine, Stuxnet ha avuto anche alcune importanti ripercussioni negative. Proprio mentre gli Stati Uniti condannavano le incursioni di cyber-spionaggio cinese, aver rilasciato la prima arma digitale conosciuta li ha messi nella posizione di non poter più predicare astinenza agli altri, come ha notato Kim Zetter nel suo libro *Countdown to Zero Day* . "Il rilascio del malware ha lanciato una corsa alle armi digitali tra Paesi piccoli e grandi che altererà per sempre lo scenario dei cyber-attacchi", ha scritto la giornalista di "Wired". Peraltro – sostiene il documentario *Zero Days 4* di Alex Gibney, uscito nel 2016 – Stuxnet sarebbe stato solo un tassello di una campagna di hacking molto più vasta e articolata, nome in codice "Nitro Zeus", che aveva penetrato surrettiziamente una serie di infrastrutture critiche iraniane, cioè di quei sistemi vitali per il funzionamento di uno Stato, dall'energia ai trasporti alla difesa. E che avrebbe potuto innescare ulteriori scenari di cyber-guerra.

Ricordiamo che negli anni di maggior tensione sul programma nucleare di Teheran – tra il 2008 e il 2011 – si è svolta una guerra non detta fra le potenze in gioco, che non si è limitata all'hacking. Diversi scienziati e accademici iraniani collegati al programma sono stati assassinati in modo clamoroso. Il 29 novembre 2010, nello stesso periodo in cui Stuxnet veniva progressivamente svelato al mondo e il giorno esatto in cui Costin Raiu trovava il cubo con il suggerimento di prendersi un po' di relax, Majid Shahriari, professore quarantenne di fisica nucleare con un ruolo rilevante nei progetti atomici di Teheran, veniva ucciso dentro la sua auto in mezzo al traffico e in pieno giorno.