GIORNALE DI BRESCIA
Quotidiano
Editori Laterza
Data 19-03-2017
Pagina 37
Foglio 1 / 2

La Grande Rete > Potenzialità e pericoli in Internet

# Tutte le guerre del Selvaggio web tra spie e governi guardie e ladri

## Il saggio di Carola Frediani Nove storie, altrettanti fronti: dal nucleare in Iran ai ricatti personali

**Claudio Baroni**
c.baroni@giornaledibrescia.it

■ Nove storie e altrettanti campi di battaglia, nel Selvaggio web. Le racconta Carola Frediani, giornalista tra i pochi specializzati sul mondo digitale, nel suo «Guerre di rete». Un libro imperdibile: lo stile è quello della spy story, i dati sono il frutto di una ricerca accurata, il tentativo è di fare il punto di una realtà in costante mutazione. Il risultato sono 170 pagine illuminanti su quel che ci sta accadendo attorno e in casa, senza che ce ne rendiamo neppure conto. La parola chiave è «malware», crasi di «malicious software», ovvero un programma maligno che si annida in pc, smartphone, tablet, o in un sistema informatico, e li rende preda di operazioni che vanno dal più raffinato spionaggio alla criminalità più sfacciata. Spesso cybercriminali e gruppi parastatali sono mescolati in modo indistricabile. In queste guerre c'è chi usa missili planetari, come Stuxnet, un «worm» (virus che si sparge in un sistema) ideato da americani e israeliani, che ha messo in crisi il programma nucleare iraniano. Obiettivi sensibili di questi attacchi sono i servizi pubblici: centrali elettriche o telefoniche, aeroporti e reti di trasporti. Ma per entrare in azione hanno bisogno di un intervento diretto, anche se basta una chiavetta usb. Ci sono poi in campo forze parastatali costantemente all'attacco, sono le Apt, sigla che sta per «Advanced persistent threat», minaccia persistente avanzata. E anche questo fronte è ampio e variegato: si va dai criminali russi specializzati in frodi bancarie ai «latinos» che mescolano spionaggio e droga, ai mediorientali emergenti in cyber-intelligence. Società nate dal nulla, pagate da non si sa chi, fuori dalla portata della legge, con la complicità di Stati: è il sistema che non solo Putin potrebbe (dovrebbe) spiegarci come funziona.

**Attacchi.** Impressionante però è anche la galassia degli attacchi quotidiani ai dati degli utenti. A cominciare dai «ramsonweare», le intrusioni nei «device» di virus che li bloccano se la vittima non paga un «ramson», un riscatto al ricattatore. C'è spazio per ogni sorpresa: società israeliane fornirebbero agli Emirati Arabi i sistemi più efficaci per controllare, censurare e perseguitare cittadini non allineati. In crescita le bande dell'Est Europa, che attraverso mail camuffate - finte fatture Enel o Telecom, ad esempio - si fanno aprire l'accesso ai pc, vi si annidano e raccolgono ogni tipo di informazione. La preda preferita sono le password da impiegare poi per truffe e raggiri. Per difendere i propri utenti e la loro privacy, le company del web hanno fatto ricorso massiccio alla crittografia. Sono arrivati persino a mettere premi da un milione di dollari a chi scoprisse le falle dei loro sistemi. E sono spesso andate in rotta di collisione con i governi e le polizie, quando questi hanno domandato di poter accedere ai dati, in nome della lotta alla criminalità e al terrorismo. Fbi, Cia e loro consimili hanno chiesto di poter avere «golden key», che permettessero ai servizi di sicurezza di decifrare i dispositivi. Le company hanno sempre fatto resistenza: niente «backdoor» - porta di servizio - per polizia e servizi, ne va della libertà.

**Trappole.** Quando vogliono, i servizi di intelligence, aggirano tranquillamente i vincoli. Basta pensare agli «Stingray» che le polizie usano in occasione di raduni o manifestazioni: sistemi integrati in grado di intercettare comunicazioni voce, telefono o sms, fino a diecimila "target" per ogni area controllata. Oppure sapere che esistono scatolette collocabili in stazioni, aeroporti, centri commerciali, che si allineano al wi-fi libero e entrano nei dispositivi quando si agganciano, praticamente in tutti, visto che ognuno di noi lascia sempre attiva l'opzione «cerca rete». A difesa della riservatezza sono stati elaborati anche software che permettono di navigare e comunicare in modo anonimo. Il più celebre è Tor. Ma molti lo guardano con sospetto, essendo nato dalle parti del Pentagono e per l'80% è ancora finanziato dal governo Usa.

Conclusione: la rete è pervasiva e planetaria, ha potenzialità immense, nel bene e nel male. Scrive Carola Frediani: «Dobbiamo essere consapevoli delle nostre abitudini, di come usiamo la Rete e di come attori malevoli potrebbero approfittarsene». //

**Diventare consapevoli di come usiamo la Rete e di come attori malevoli potrebbero approfittarsene**

GIORNALE DI BRESCIA

Quotidiano

Editori Laterza

Data 19-03-2017
Pagina 37
Foglio 2 / 2

# Appuntamento al Festival del giornalismo di Perugia

«Guerre di rete» (Laterza, 170 pagine, 15 euro) è l'ultimo saggio di Carola Frediani, giornalista specializzata in nuove tecnologie, privacy e hacking. Il saggio sarà presentato al Festival internazionale del giornalismo dal 5 al 9 aprile a Perugia, dove la Frediani interverrà ai dibattiti su guerra dell'informazione, malware, hacking di stato e hacking democracy.

**Privacy e sicurezza.** Dalle password alla crittografia, difendersi nel web è una sfida aperta


CULTURA&SPETTACOLI

Tutte le guerre del Selvaggio web tra spie e governi guardie e ladri