

## C'è una spia nel computer

**Con una semplice chiavetta Usb, untori elettronici possono infettare intere reti informatiche. E accecare così aziende o avversari politici. Lo rivelano i nuovi Spy Files di Assange**

Di Stefania Maurizi

Laptop che possono essere infettati da chiavette Usb apparentemente innocue e che non richiedono alcuna conoscenza informatica. Programmi che possono essere integrati nella rete di un Internet service provider in modo «da infettare i computer in massa». Sono questi gli "untori" di dati che possono devastare i computer di un'azienda, un partito o un movimento politico. Nei nuovi "Spy Files" dedicati all'industria della sorveglianza elettronica, 23 dossier e video divulgati per la seconda settimana da WikiLeaks e pubblicati in esclusiva da "l'Espresso", c'è un asso pigliatutto: si chiama FinFisher ed è un prodotto commercializzato da due giganti del settore che hanno stabilito una stretta collaborazione: l'inglese Gamma e la tedesca Elaman. Niente sembra poter sfuggire a FinFisher: è una tecnologia capace di agire su computer e telefonini, che penetra gli scudi di firewall e antivirus, ed è capace di rubare qualsiasi informazione: dalle conversazioni via Skype alle chat, dai file stampati a quelli cancellati. Può essere installata direttamente nei computer attraverso dispositivi fisici, come le chiavette Usb, ma anche a distanza, attraverso file che infilano il micidiale cavallo di Troia "FinSpy", «un Trojan professionale che è completamente invisibile e tutte le sue comunicazioni sono totalmente coperte». Uno strumento per monitorare mafiosi, terroristi e criminali, certo. Ma che potrebbe finire nelle mani di chiunque. E i documenti diffusi da WikiLeaks fanno capire che la tecnologia FinFisher non è pensata solo per colpire obiettivi specifici, ma anche per la sorveglianza di massa. Leggendo la brochure del "FinSpyISP", per esempio, viene fuori che questo prodotto «può essere integrato nella rete di un service provider per infettare i computer in massa o quelli di singoli target». E non c'è modo di impedire che questi spioni informatici non vadano a finire nelle mani di dittature spietate: nei mesi scorsi, la Bbc ha ricostruito i contatti tra la Gamma e l'apparato di regime del presidente egiziano Mubarak, per vendere il software FinFisher. Sarebbe dovuto servire per monitorare attivisti e dissidenti, una circostanza prontamente smentita dalla Gamma. Come ha smentito qualsiasi affare diretto con le dittature africane e del Medio Oriente, l'azienda italiana Hacking Team, che commercializza un Trojan analogo al FinSpy: il Remote Control System (Rcs), anch'esso capace di infettare computer e telefonini. Finita sotto i riflettori internazionali, anche grazie agli "Spy Files" di

WikiLeaks, la milanese Hacking Team ha dichiarato di non accettare contratti con Paesi sotto embargo. Una scelta eticamente irreprensibile, della quale bisogna fidarsi alla cieca. Non esistono infatti controlli internazionali sull'esportazione di queste tecnologie, potenti come armi perché capaci di accecare e spiare reti di computer e telefoni.

Le aziende, quindi, possono dire tutto e il contrario di tutto: nessuno potrà smentirle. Ci sono, però, eccezioni. Come quella capitata all'americana Blue Coat, anch'essa censita nei database di WikiLeaks, le cui tecnologie per la sorveglianza sono finite in mano a tua dittatura spietata come quella di Bashar al-Assad in Siria, che sta sterminando migliaia di oppositori. Il caso è emerso grazie alla denuncia di un gruppo hacker: Telecomix. Okhin è un membro di Telecomix, che parlando sotto pseudonimo racconta a "l'Espresso" come molte delle aziende che fanno questo business sanno benissimo dove finiscono le loro creature: «Per funzionare, questi software devono per forza essere aggiornati», racconta Okhin, «e, ogni volta che parte l'aggiornamento, il congegno "telefona a casa" per verificare se la licenza del software è legittima». Membri di Telecomix - che hanno chiesto l'anonimato vista la delicatezza del loro impegno contro i regimi - raccontano di non aver rintracciato tecnologie di Hacking Team in Libia, mentre il lavoro di "monitoraggio" della Siria sta andando avanti: se qualche azienda occidentale e, in particolare, italiana ha venduto al regime software o hardware per la sorveglianza contro la popolazione e i dissidenti, prima o poi emergerà.

I file su FinFisher, però, sono solo una goccia nel mare scuro della sorveglianza. Tra i documenti più interessanti rilasciati da WikiLeaks c'è il campionario completo della tedesca Elaman: un documento riservato ("confidential") di centinaia di pagine, simile al catalogo Postalmarket che permette di scoprire lo strumento ad hoc per spiare qualunque forma di comunicazione in qualunque situazione. Nel catalogo, oltre al capitolo sui Troian "FinSpy", Elaman presenta ai potenziali clienti sistemi jammer per confondere le onde elettromagnetiche emesse dagli schermi dei computer. Oppure microfoni sofisticatissimi, capaci di carpire conversazioni nei posti più rumorosi, come i bar e ristoranti. Trapani a bassissimo rumore (silent drilling) per poter installare di nascosto microfoni negli uffici da controllare. E ogni sorta di veicolo per la sorveglianza: dai furgoni alle macchine fino alle moto imbottite di telecamere nascoste. Ci sono scooter trasformati in centrali d'ascolto. Infine apparecchi da 007, come «tecniche di camuffamento non convenzionale altamente sofisticato» per inserire microspie ovunque: dai timbri dell'ufficio, ai fiori, fino ai telefonini. Non è folklore, ma una potenziale minaccia alla libertà di comunicazione.