CORRIERE DELLA SERA.it

FOCUS CRIMINALITÀ INFORMATICA

Internet, l'assalto dei virus

Italia, in sei mesi ne sono stati «censiti» 1,2 milioni «Ora sono intelligenti, ingannano il pc e non l'uomo»

Arrivano dalla Russia, dalla Romania e, da poco, anche dalla Bulgaria. Entrano nelle nostre case. Rubano, copiano ed escono senza lasciare tracce (o quasi). Per poi vendere la «refurtiva » su un web-mercato nero il cui giro di affari potenziale è stimato, a livello internazionale, più grande di quello della droga. Un dollaro per una «dose», cioè per un'identità digitale. Costa così poco avere i nostri dati, nome, cognome, codice fiscale e password e numeri del conto corrente, per prelevare denaro dai conti o per perpetrare truffe a nostre spese. Sono questi i nuovi criminali inseguiti da polizie e servizi segreti. Si muovono come l'eroina larssoniana della trilogia letteraria «Millenium», Lisbeth Salander: senza farsi notare entrano nei nostri computer di lavoro o personali tramite Internet e se ne impossessano grazie ai virus digitali che hanno fatto registrare un vero boom in Italia. Secondo i numeri inediti del Security Intelligence Report 5 della Microsoft sono stati 1.274.325 nel primo semestre dell'anno con una crescita del 20% sul secondo semestre del 2007 e del 110% se si risale al primo.

Il dato è preoccupante, anche se va sottolineato che la maggior parte di questi virus sono solo «trojan horse», cioè cavalli di Troia, programmi con la «sorpresa» dentro, o dei semplici file eseguibili che non veicolano furti ma fanno solo danni al notebook. In ogni caso i due dati sono strettamente correlati: boom di virus vuol dire anche maggiore rischio di furti digitali. Il bello (o brutto) è che il nuovo business della criminalità non richiede l'uso delle armi. Una volta dentro i pc si impossessano dei dischi rigidi, li copiano o, nei casi peggiori, li monopolizzano spiando i nostri movimenti e carpendo informazioni personali. Solo che a differenza di Lisbeth questi non si fermano di fronte a nulla come dimostrano anche i recenti furti di piccole somme dal conto dello stesso presidente francese, Nicolas Sarkozy. La parte più interessante del caso «politico»? È che nonostante i dispiegamenti degli esperti della polizia informatica e della brigata della finanza sguinzagliati da Sarkozy i colpevoli sono ancora ignoti. Segno che non si trattava di avventurieri. «Qui non si tratta più di inseguire dei giovani hacker come nei film — spiega al Corriere Antonio Abruzzese, dirigente del centro della Polizia Postale di Bologna, diventata in questi anni la "Scotland Yard italiana" delle frodi e della criminalità informatica — ma di un problema molto serio: oramai il volume globale dell'home banking e dell'e-commerce su cui vengono attuate le truffe della monetica è più ampio del traffico del mercato della droga. E di questo se n'è accorta anche la grande criminalità organizzata».

Alla fine le bande dell'Europa dell'Est e i professori universitari russi fanno solo il lavoro sporco. Sono loro ad inviare quelle email dove tra refusi ed errori grammaticali elementari ci chiedono di confermare i nostri dati con l'intestazione di qualche banca (phishing). Quando qualcuno abbocca finisce in un archivio che viene venduto. Il problema, come spiega Abruzzese, è che «il phishing è solo la tecnica più semplice per venire in possesso dei nostri dati». Ed era anche la più facile da cui difendersi: basta non

fare nulla. Coadiuvati dai «geni» matematici russi, le bande stanno mandando in cantina quelle tecniche di prima generazione che erano state usate anche nel caso degli spionaggi illegali partiti dall'ufficio sicurezza Telecom su cui sta indagando la magistratura italiana. «Ultimamente si sono molto evoluti. Ora siamo al phishing tecnologico. Si tratta di veri e propri malware (neologismo inglese che sta per software malvagio, ndr) che ingannano il pc. Una volta il sistema più comune era la deviazione degli accessi. Il cosiddetto farming... cioè la gestione della fattoria dove vanno le pecore: creo un sito, come per esempio www.bancadiroma.it, apparentemente uguale a quello vero dove però il controllo è dei criminali». L'attenzione e la conoscenza geografica del web poteva aiutare a subodorare la truffa. La differenza è che adesso nemmeno un esperto si rende conto di cosa sta succedendo perché «si è passati dall'inganno dell'uomo all'inganno della macchina con infezioni che colpiscono i siti veri di grande accesso. In sostanza ora è sufficiente guardare il video, anche se non si clicca su nulla».

Potrebbe succedere su YouTube, su Facebook, come sul sito di un giornale online. Si tratta di virus intelligenti che si attivano solo con alcune parole chiave. Il meccanismo è lo stesso delle intercettazioni internazionali solo che qui dall'altra parte non ci sono agenti della sicurezza ma si finisce dritti dritti dentro la tana dei cattivi. «Il web è come un terreno enorme sul quale sono state disseminate mine e bombe». Potrebbe sembrare un'esagerazione, ma bastano un paio di esempi storici per capire: quando nel maggio del 2007 è partito da Mosca un attacco informatico all'Estonia con un sabotaggio dei siti del governo, dei media e delle banche si è discusso se far scattare l'articolo cinque della Nato che preve de la difesa collettiva dello Stato aggredito. Altro esempio: i dieci peggiori virus della storia fino al 2004, tra computer da buttare e servizi bloccati, hanno causato danni stimati tra i 25 e i 30 miliardi di dollari. Un altro termometro arriva d a l l a p i ù grande azienda di software al mondo, la Microsoft. Come spiega il vice president mondiale, Umberto Paolucci, «noi spendiamo in sicurezza circa 2,6 miliardi all'anno, un terzo degli investimenti totali in ricerca e sviluppo». Ma perché queste informazioni vengono cedute invece di essere usate direttamente? Gli esperti della Polizia Postale guidati da Domenico Vulpiani, ex capo Digos ed ex responsabile della sicurezza dei servizi di scorta del capo dello Stato, stanno ricostruendo tutto il puzzle grazie agli ultimi casi risolti, come quello dello scorso luglio.

Intercettando un invio di materiale digitale partito dal computer di un camionista romeno che vive a Verona e arrivato in un account di Craiova la polizia ha seguito il viaggio di migliaia di codici Postepay scoprendo il trucco. «Quando ho i numeri di identità — spiega Abruzzese—posso potenzialmente accedere ma rimane la parte più difficile: la monetizzazione. Non posso lasciare tracce. Qui le tecniche sono diverse. I russi che non hanno una grossa distribuzione in Italia reclutano i soldatini anche attraverso il social networking e poi rimpatriano i soldi con le reti come Western Union. Per i rumeni è diverso: in Italia sono tanti e hanno un servizio di riciclaggio interno gestito grazie alle carte anonime come le revolving». Insomma, nel secondo passaggio serve una rete più complessa. Ed è per questo che la «dose» costa così poco e che in questo passaggio entra in gioco la grande criminalità anche con l'obiettivo di creare una database di informazioni con cui controllare un futuro sempre più digitale. «Ormai — conclude Abruzzese — c'è un commercio mondiale sulle banche date di identità. E a gestire tutto è una holding criminale per la quale servirebbe più collaborazione internazionale».

Massimo Sideri
msideri@corriere.it
stampa | chiudi