



Hacking Team. Dove sono (se ci sono) le responsabilità?

L'uso di spyware da parte dello Stato ha suscitato prese di distanza da una tecnologia che è impossibile vietare.



Il 6 luglio 2015 Hacking Team, una società italiana che si occupa di sicurezza informatica ha subito il furto di 400 gigabyte di dati, una parte rilevante dei quali (email, nello specifico) è stata pubblicata su Wikileaks. Non è certo la prima volta che un'azienda subisce un massiccio furto di dati (basti pensare ai 3 milioni di account Adobe compromessi nel 2013, ai dati sottratti nel 2014 a Sony Pictures Entertainment e al network di Sony Playstation, o agli account Dropbox finiti in mani ignote). Ma la particolarità di questo caso è che la "vittima" produce trojan e spyware a uso di servizi segreti e strutture investigative di mezzo mondo e che i file sottratti, oltre a rivelare i dettagli degli accordi commerciali e l'identità dei clienti istituzionali, contengono anche il codice di queste applicazioni. Benché la notizia sia estremamente seria, i vari talk-show televisivi di solito molto attenti all'attualità sono rimasti in silenzio, e la stampa non è andata oltre i soliti articoli pieni di luoghi comuni del tipo "siamo tutti controllati" da una "sostanziosissima tecnologia" venduta anche a "paesi che violano i diritti umani". Non poteva mancare il Garante per la protezione dei dati personali che esprime una "preoccupazione" sull'uso di questi software perché - si legge su Repubblica.it del 15 luglio - "in un colpo solo, può entrare nei telefoni e nei pc, copiare tutto e creare nuovi file, attivare una telecamera e un microfono per spiare la vita della "vittima". E registrare tutto, anche dentro casa."

In realtà, per quanto paradossale sia questa affermazione, sulla vicenda Hacking Team si sta facendo molto rumore per (quasi) nulla. Vediamo perché. Sorvolo,

innanzi tutto, sulla questione "software venduto ai paesi che violano i diritti umani". Se una nazione siede nell'ONU e la vendita è conforme ai trattati internazionali (come fanno i venditori di armi) la transazione sarà anche "sgradevole" ma non è illegale. L'etica è un fatto individuale, separato dal rispetto della legge. Ai tanti "attivisti da tastiera" si dovrebbe chiedere, semmai, perché non si sono occupati degli accordi internazionali che consentono simili accordi commerciali.

Spyware e trojan sono in giro da tantissimo tempo, e la rete è piena di programmatori votati al "lato oscuro della forza" in grado di scrivere malware estremamente efficienti (Cryptolocker, citandone uno per tutti). Dunque, per quanto Hacking Team abbia sicuramente realizzato un prodotto di alto livello, non è né il primo né il solo in grado di consentire il controllo remoto di un computer e la sottrazione a distanza di file.

È illegale utilizzare software di questo genere?

Il codice di procedura penale, recependo la Convenzione europea sul crimine informatico del 2008 ha previsto che la polizia giudiziaria possa perquisire a

distanza un computer, anche forzando l'accesso cioè: bucare una risorsa di rete e analizzarne il contenuto. A maggior ragione, dunque, se la polizia giudiziaria può perquisire a distanza, può anche sequestrare a distanza quanto rinvenuto dopo la perquisizione. La risposta alla domanda, pertanto, è no, non è illegale da parte degli investigatori usare trojan e spyware. Analoga risposta vale per i servizi segreti che, di fatto, hanno molti meno vincoli operativi e che non devono raccogliere "prove giudiziarie" ma

elementi informativi non destinati a essere valutati da un giudice. E a proposito di servizi segreti, vanno anche demistificate le affermazioni che si leggono in giro sulla compromissione di attività di intelligence in corso e sull'importanza della fuga di informazioni provocata dalla diffusione di email e documenti. Innanzi tutto la storia dell'intelligence è piena di "defector" (disertori) o di "mole" (talpe) che nel corso degli anni hanno provocato la fuoriuscita di grandi quantità di informazioni veramente pericolose (per l'altra parte), mentre quelle detenute da Hacking Team non sono certo paragonabili all'archivio Mitrokhin o agli exploit di Kim Philby. In secondo luogo, e cominciamo a parlare di informatica, anche se effettivamente delle operazioni segrete fossero state compromesse, la responsabilità prima sarebbe di chi, nelle istituzioni, ha scelto di rivolgersi a un'azienda privata invece di sviluppare in casa determinati strumenti di intelligence.

In terzo luogo, ed è inutile nascondersi dietro una foglia di fico, Hacking Team, ma prima ancora, i vari criminali informatici che scorrazzano per Internet, hanno fatto quello che hanno fatto grazie alla spregiudicatezza delle politiche di marketing delle software house che, al di là delle dichiarazioni pubbliche, non hanno mai praticato seriamente il "security by design". Sotto accusa, nel caso specifico, è Flash, ma non è la sola né l'unica tecnologia a essere (rimasta) vulnerabile da troppo tempo.

Sarebbe un bene per tutti che software house e responsabili IT delle aziende imparassero qualcosa dalla vicenda di Hacking Team, ma probabilmente, come si dice dalle mie parti, "passata la festa, gabbato lo santo" e fra un po' di tempo faremo nuovamente tutti la fila per scaricare l'ennesimo "security update".

Security by design

Diverse tecnologie ampiamente diffuse sono rimaste vulnerabili a lungo nonostante i proclami marketing