La guerra "freddissima" tra Stati Uniti e Cina

Nelle complesse
e talvolta contraddittorie
relazioni internazionali
è emerso negli ultimi tempi
un caso singolare
che ha coinvolto il mondo
di Internet in inediti scenari.

Alessandro Ovi

L'Amministrazione americana già da qualche anno mantiene un atteggiamento "equilibrato" nei confronti della Cina. Da una parte riconosce a quella che è la seconda potenza economica mondiale, ma non solo, il ruolo che le compete nello scenario globale. Dall'altra, per vari motivi, ne contrasta alcuni comportamenti a cui la cultura del popolo americano è sempre sensibile, dal tema generale dei diritti umani a quello più specifico del "dumping sociale" che ha portato alla emigrazione di posti di lavoro dagli Stati Uniti alla Cina.

Questi temi hanno rappresentato un motivo ricorrente di qualunque incontro bilaterale, quasi che i rappresentanti del governo americano si sentissero in dovere di ricordarli, anche se sono sempre parsi ben consci della sterilità del loro messaggio. Lo hanno sempre fatto, certi che sul loro fronte interno il consenso popolare sarebbe comunque stato unanime.

Negli ultimi tempi è però avvenuto un caso singolare e a esserne coinvolto è il mondo di Internet che alla nostra rivista ha sempre interessato in modo particolare.

Abbiamo già parlato a lungo, ai tempi della Primavera Araba, del modo in cui in cui il governo cinese era riuscito a bloccare sul nascere la diffusione virale di messaggi antigovernativi e addirittura, con una tipica tecnica di marketing di origine americana, a girare a proprio favore la grande ondata di messaggi on-line scatenata dalla lettura degli interventi dei "ragazzi" di Tunisi o del Cairo. Ma tutto ciò rientrava in fondo nel solito discorso sulla limitazione della libertà d'informazione, che pare intrinseca, anche se non certo condivisibile dal punto di vista della democrazia, al modo di mantenere una certa stabilità politica, funzionale alla crescita di un enorme e complesso paese come la Cina.

Il caso singolare cui stiamo assistendo recentemente, si riferisce allo spionaggio industriale via Internet dove, a differenza del sia pure recente passato, la opinione pubblica americana si sta dividendo, così che anche la Casa Madre della nostra rivista si è trovata al centro di un dibattito forse inatteso.

In un recentissimo articolo da Cambridge si propone con ricchezza di particolari il Rapporto di 60 pagine di una società americana, Mandiant, specializzata in sicurezza informatica e *cyber crime*. Il rapporto spiega in che modo un Istituto cinese di Shangai**,** APT1, sia penetrato nelle comunicazioni riservate di importanti aziende per copiarne segreti industriali. Si tratterebbe di almeno 141 aziende dal 2006 a oggi, ivi inclusa Tencent, una società il cui software controlla infrastrutture energetiche (con un alto rischio di terrorismo informatico).

Il rapporto di Mandiant arriva una settimana dopo l'annuncio del presidente Obama di un nuovo impegno nazionale per difendere gli Stati Uniti dagli attacchi informatici usati per rubare segreti aziendali e anche per gettare le basi di un possibile sabotaggio delle infrastrutture energetiche.

Anche 'The Economist" ha parlato del rapporto Mandiant, traendone l'occasione per un severo richiamo alla Cina a comportamenti corretti. Già nell'articolo della edizione americana di MIT Technology Review, però, si faceva notare un dubbio che emerge dal Rapporto Mandiant, dove si giudica abbastanza strano che questi "furti" siano avvenuti senza nessuna attenzione a nascondere la provenienza dell'attacco informatico. Il Rapporto si domanda come sia possibile che gli autori di queste intrusioni, si siano dimostrati così poco "professionali". Mandiant, infatti, sostiene che APT1 fa parte dell'Unità 61398 dell'esercito cinese ed è impegnata in una campagna di spionaggio industriale per aiutare le imprese cinesi con informazioni riservate. Anche altre aziende in Canada, Regno Unito, Sud Africa e Israele sarebbero state presi di mira. Il fatto però che gli aggressori non si siano preoccupati di nascondere il loro indirizzo IP, fa dubitare che alle spalle di APT1 possa trovarsi realmente l'esercito cinese, la cui competenza informatica viene valutata di livello molto buono.

Il Rapporto è certamente interessante, ma ancora più interessante è che non tutti i commenti dei lettori sono stati negativi nei confronti dei cinesi. Anzi, ci sono state anche critiche nei confronti del Rapporto. Si va dalla analisi dei suoi errori fino a deprecare che la rivista del MIT lo abbia comunque pubblicato.

Ancora più interessante, è che pochi giorni dopo, una fonte autorevole come Bloomberg Business Week Technology Insider abbia smentito la provenienza cinese di queste attività di *cyber crime*, scrivendo che all'origine vi sarebbero operatori dell'Est Europa (si era già constatato un legame della Bielorussia con gli attacchi informatici alle centrifughe iraniane per l'arricchimento dell'uranio). Il racconto di Bloomberg parte dalla recente Conferenza di Barcellona dove i più grandi operatori Internet del mondo (Microsoft, Apple, Facebook, Twitter...) hanno condiviso le loro esperienze di vittime di *cyber crime*.

È stato identificato il metodo usato per gli attacchi, il cosiddetto *waterhole attack,* e quindi dall'ipotesi che all'origine ci fosse la Cina l'attenzione si è spostata sull'Est Europa e sulla mafia russa come operatore principale. L'obiettivo sarebbe puramente commerciale: quello di rubare i segreti industriali non per favorire lo sviluppo di aziende nazionali, ma per venderli al miglior offerente in qualunque parte del mondo.

Cosa sta succedendo? I grandi americani di Internet vedono la Cina con occhi diversi dal più recente passato in cui Google si era duramente scontrato con il governo di Pechino, oppure dobbiamo dare una lettura dei fatti diversa da quella più semplicistica che i Cinesi rubano tecnologie via Internet nell'interesse nazionale? Forse la Cina non c'entra affatto, o forse anche APT1 opera per fini commerciali e non di "politica industriale nazionale". Si tratta di ipotesi che per ora fanno parte della fantapolitica. Serve però ricordare e confrontarle per avviare una riflessione che ci può portare lontano.■

Alessandro Ovi è direttore della edizione italiana di MIT Technology Review.

Virus e antivirus: una battaglia infinita

I tradizionali software per la sicurezza sono disarmati di fronte agli attacchi informatici sempre più sofisticati. Ma altre risorse sono pronte a scendere in campo.

Tom Simonite

Questa estate i laboratori che si occupano di sicurezza informatica in Iran, Russia e Ungheria hanno annunciato la scoperta di Flame, che il centro di ricerca ungherese CrySyS ha definito «il più complesso malware mai incontrato».

Per almeno due anni, Flame ha copiato documenti, ha "catturato" schermate di file, registrazioni audio, sequenze di battute di tasti e chiamate telefoniche su Skype da computer infettati. Tutti questi dati sono stati trasmessi ai server controllati dagli hacker. Fino a oggi, nessun software per la sicurezza aveva lanciato l'allarme.

La scoperta di Flame è solo l'ultima che indica come il tradizionale software antivirale sia un sistema ormai superato per proteggere i computer dai malware. «Flame è stata la Caporetto dell'industria degli antivirus», ha scritto Mikko Hypponen, il fondatore dell'azienda di antivirus F-Secure. «Avremmo dovuto fare molto di più, ma non ne siamo stati capaci. Siamo chiusi nell'angolo».

I programmi per la sicurezza dei computer di aziende, governi e consumatori funzionano allo stesso modo: le minacce vengono rilevate confrontando i codici dei programmi e le loro attività con una banca dati di malware conosciuti. Le aziende per la sicurezza come F-Secure e McAfee sono alla ricerca costante di nuovi malware per aggiornare la loro lista. L'obiettivo è di creare un muro invalicabile per i malintenzionati.

In realtà, negli ultimi anni gli attacchi a governi e aziende hanno utilizzato software che, sia pure non sofisticati come Flame, hanno aggirato il sistema di difesa basato sul riconoscimento delle tracce. Alcuni esperti e aziende sostengono che sia giunto il momento di modificare questa forma di protezione. «Gli antivirus tradizionali rimangono una componente importante della difesa dai malware, ma devono venire affiancati da altri rimedi», afferma Nicolas Christin, ricercatore della Carnegie Mellon University. «Dobbiamo cambiare logica e non intestardirci a costruire una specie di linea Maginot, che viene regolarmente elusa dagli hacker».

Christin e diverse startup che si occupano di sicurezza, sono impegnati nella creazione di nuove strategie difensive per rendere gli attacchi più difficili e aiutare chi li subisce.

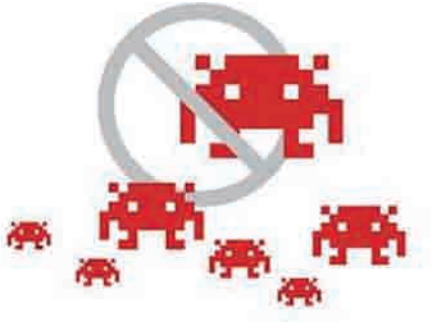
Un ottimo esempio della nuova linea di azione è costituito da CrowdStrike, un'azienda fondata da esperti del settore antivirus, che ha raccolto 26 milioni di dollari di fondi d'investimento. Dmitri Alperovitch, responsabile tecnologico e cofondatore di CrowdStrike, sostiene che l'azienda ha intenzione di presentare un sistema intelligente di allarme per segnalare qualsiasi tipo di attacco e la sua provenienza.

Questo sistema è realizzabile, dice Alperovitch, perché l'hacker, oltre a modificare facilmente il codice di un virus come Flame per sfuggire agli scanner dell'antivirus, dovrebbe avere un obiettivo primario: accedere ed estrarre dati di valore. Comprensibilmente, CrowdStrike non vuole rivelare dettagli della sua tecnologia, ma è verosimile che prenda in considerazione le attività del sistema dell'utente per individuare una eventuale infiltrazione.

Le nuove strategie del chi e non del come

La strategia è quella di ostacolare le tattiche più diffuse e di rendere la vita più dura ai malintenzionati, invece di concentrarsi sugli strumenti, in continua evoluzione, impiegati dagli hacker. «Dobbiamo guardare a chi spara, non alla pistola», come sostiene Alperovitch.

Altre aziende la pensano nello stesso modo. «È necessario convincersi che, come direbbe un tutore dell'ordine, "il crimine non paga"», afferma Sumit Agarwal, cofondatore della startup Shape Security. L'azienda ha raccolto 6 milioni di dollari dagli investitori, tra cui Eric Schmidt, presidente di Google. Anche Shape Security mantiene uno stretto riserbo sulla sua tecnologia, ma Agarwall dice che l'obiettivo è quello di alzare il costo dell'attacco informatico rispetto al ritorno economico, vanificandolo.



Alperovitch dice che la sua azienda collaborerà con le vittime, nei limiti delle leggi, per identificare chi si trova dietro gli attacchi. «Azioni di "difesa attiva" possono sconfinare nell'illegalità, ma non è illegale intraprendere iniziative nei confronti delle persone che traggono vantaggi dai dati "rubati", alzando in tal modo i costi commerciali di chi attacca un sistema», spiega Alperovitch. Si può, per esempio, chiedere al governo di sottoporre il caso alla Organizzazione Mondiale per il Commercio e rendere di dominio pubblico quanto è successo, per denunciare chi ha condotto l'operazione di spionaggio industriale.

Christin e i suoi colleghi universitari hanno evidenziato come si possano intraprendere azioni legali relativamente semplici per neutralizzare le operazioni di crimine informatico. La loro ricerca ha preso in considerazione le tecniche di manipolazione dei risultati della ricerca, volte a promuovere prodotti farmaceutici illeciti, arrivando a concludere che l'inganno si sarebbe potuto bloccare operando su un esiguo numero di servizi che reindirizzano i visitatori da una pagina Web a un'altra. Lo scorso anno, alcuni ricercatori dell'Università della California, a San Diego, hanno dimostrato che una larga parte dello spam passa attraverso tre sole banche dati.

Comunque Agarwal mette in guardia sui "pericoli" della denuncia legale. «Immaginate di essere una grande azienda e di entrare accidentalmente in rotta di collisione con la mafia russa. Potreste mettere in moto un meccanismo incontrollabile». ■

Tom Simonite lavora nella redazione di San Francisco come responsabile dell'area software e hardware della edizione americana di MIT Technology Review.