CF2R
Centre Français de Recherche sur le Renseignement

NOTA "CYBER RENS" N° 5

COMUNITÀ HACKER: UNA NUOVA POTENZA NEL CUORE DELLE SFIDE STRATEGICHE MONDIALI

Yves-Marie Peyry

Il termine hacker, molto usato dai mass media, contiene una diversità semantica difficilmente comprensibile per il neofita.

Parliamo volentieri di pirati informatici, di anarchici cibernetici o di ciberdissidenti. Certi hacker si sforzano di presentare una vocazione umanitaria[1], mentre altri si mettono in luce in azioni più imparentate con la cibercriminalità, il ciberterrorismo o addirittura il cibermercenarismo.

Gli Stati stessi, come per esempio l'Iran, la Cina o gli Stati Uniti, sollevano peraltro degli eserciti di hacker (chiamati il "quarto esercito" dopo quelli di terra, d'aria e di mare) per dei colpi informatici. Così, si stima che il "commando cibernetico" dell'esercito americano conti più di 100.000 uomini e donne, che lavorano, nell'ombra delle reti, per sferrare attacchi contro i server nemici.

Dinanzi a questa varietà di generi, un'analisi delle azioni recenti permette di delineare i contorni di numerosi movimenti che si distinguono, al contempo, per il loro modus operandi ma anche per l'ideologia che soggiace al loro comportamento.

Un attivismo al servizio della libertà d'espressione e della difesa delle libertà individuali

L'aiuto apportato da numerose comunità di hacker in difesa della libertà d'espressione durante le rivoluzioni arabe dimostra l'emergere di un hacking etico e militante a scopo umanitario. Il gruppo Télécomix ha dato così la sua assistenza ai ciberdissidenti arabi per aggirare la censura governativa. Attualmente, le comunità Télécomix e Anonymous sono impegnate in azioni volte a permettere il libero accesso a internet in Siria. Su quest'attivismo al servizio della libera espressione, ci dà la sua testimonianza un membro di Télécomix: "*noi non siamo un'organizzazione ufficiale o un'associazione. Noi cerchiamo unicamente di permettere a tutto il mondo di esprimersi. L'accesso a internet è un diritto per tutti, poco importa la sua localizzazione. Noi aiutiamo tutte le persone o i popoli che ne hanno bisogno e*

[1] Cfr. Note d'Actualité n° 249, http://www.cf2r.org/fr/notes-actualite/la-cyber-dissidence-au-coeur-des-revolutions-arabes.php.

che lo desiderano, blogger spagnoli, americani, iraniani. Forniamo dei mezzi di anonimizzazione gratuitamente, aiutiamo in progetti che rientrano nella nostra ottica (hosting, ecc…). Organizziamo seminari di sensibilizzazione (privacy, criptaggio, opendata, ecc.). Mettiamo in primo piano la neutralità della rete così come la libera circolazione dei dati. Internet è un vettore d'informazione e di libertà d'espressione, noi rimaniamo in guardia semplicemente perché resti tale, né più, né meno".

Questa nuova forma di attivismo hacker al servizio della libertà d'espressione si manifesta anche attraverso delle azioni volte a impedire il blocco da parte delle autorità di siti considerati sensibili. Così, quando il Ministero degli Interni francese ha annunciato la sua volontà di bloccare, mediante procedimento giudiziario, il sito internet *Copwatch*, che scheda poliziotti e gendarmi, i gruppi di hacker Anonymous e Télécomix hanno reagito immediatamente informando che avrebbero aiutato ad attivare siti specchio per aggirare qualsiasi tentativo di blocco.

La lotta contro la "schedatura informatica" è anche all'origine di numerose azioni rivendicate dagli hacker. Si può citare, all'inizio di novembre, la pirateria parziale del server del gruppo politico francese UMP. Il gruppo che ha rivendicato quest'intrusione si qualifica come gruppo di volontari "ciberidealisti" e intende dimostrare, mediante quest'attacco, i pericoli della schedatura di identità su server non abbastanza protetti.

Questa difesa della libertà d'espressione sulla rete è inoltre all'origine di lotte intestine all'interno della comunità hacker. In effetti, il 14 novembre scorso, un gruppo denominato *Voxel Project* ha attaccato il sito internet di BFM-TV per dichiararvi la sua ostilità al gruppo internazionale di hacker Anonymous e minacciare di divulgare, per il 25 dicembre, i nomi di molti dirigenti a capo degli Anonymous. *Voxel Project* precisa: "*non possiamo sopportare l'idea che un gruppo, Anonymous, imponga, senza alcun dibattito, il suo modo di pensare e blocchi questo o quel sito (…). Nessuno ha il diritto di imporre una maniera di pensare e di bloccare milioni di persone*".

Come si vede, la comunità hacker non è solidale. Al suo interno si oppongono alcune correnti ideologiche. Se alcuni si attribuiscono la missione di "guardiano" delle libertà individuali e della libera espressione sulla rete, altri vedono nella propria azione un mezzo di contestazione e di comparsa di un contropotere.

Un attivismo impegnato al servizio della comparsa di un contropotere

Dopo alcuni mesi, si osserva una netta radicalizzazione di certe comunità hacker. Così, si assiste alla moltiplicazione di azioni di "ciber-ribellione" caratterizzate dalla volontà di esercitare un contropotere in cui l'hacker non esita a utilizzare la minaccia informatica o addirittura a distruggere o trafugare dati sensibili per la sicurezza degli Stati.

I metodi impiegati per questi attacchi – dove prevalgono l'attacco per negazione di servizio e il defacing – differiscono dai mezzi utilizzati da altre comunità di hacker, come Télécomix, che, dal canto suo, mostra la volontà di non deteriorare le reti informatiche e, soprattutto, di non distruggere i dati che vi sono immagazzinati.

L'attacco per negazione di servizio, ben noto agli ambienti hacker, utilizza software semplici. Uno dei più conosciuti si chiama LOIC (*Low Orbit Ion Cannot*). Questo programma

permette di stabilire un gran numero di connessioni simultanee al fine di provocare una saturazione del server attaccato e, così, bloccarne l'accesso. Contrariamente a quanto si pensa, un membro di una comunità hacker conferma la facilità di compiere un tale attacco: "*i due unici prerequisiti sono avere il programma LOIC, che è facilmente scaricabile, e comunicare ai membri l'indirizzo del sito che si desidera attaccare. Contemporaneamente, dai quattro angoli del pianeta e con qualche click di mouse, sarà sferrato l'attacco*".

Questo tipo di attacco rivela l'impiego di un vero e proprio "esercito di hacker" pronto a far tremare le maggiori istituzioni civili e militari. La cosa più pericolosa è che un computer può essere utilizzato a distanza, a insaputa del suo utente, per partecipare a un attacco. Così, certi gruppi hacker rivendicano il controllo di molte migliaia di computer, detti "macchine zombi". Questa potenza di calcolo fenomenale permette di aumentare l'impatto di un attacco per negazione di servizio o di decifrare un codice in un tempo notevolmente inferiore che con una sola macchina. Una rapidità d'azione che riduce i rischi di una localizzazione dell'attacco. Su scala planetaria, si stima che oggi giorno ci siano 250 milioni di computer "zombi". Una forza d'urto cinquanta volte più potente della rete di computer utilizzata per il programma SETI per la ricerca di segnali extraterrestri. Secondo alcuni esperti, questo "esercito virtuale" potrebbe infliggere dei danni superiori a un attacco militare convenzionale e annientare, in poche ore, l'insieme delle reti di comunicazione di un Paese, o di vari Stati. Nessun server sembra poter sfuggire a tale minaccia. Per gli hacker "qualsiasi oggetto connesso alla rete è vulnerabile".

Questo "potere nocivo" manifesta inoltre la sua forza attraverso l'anonimato. Un anonimato che è diventato il simbolo del gruppo internazionale di hacker Anonymous creato nel 2003. Il suo motto riflette, senza ambiguità, la sua volontà di esercitare un contropotere: "*Noi siamo Anonymous/Anonimi. Noi siamo Legione. Noi non perdoniamo. Noi non dimentichiamo. Preparatevi*".

Utilizzando come simbolo la maschera di Guy Fawkes – l'istigatore della Congiura delle polveri che mirava ad assassinare il re inglese protestante Giacomo I[2] – Anonymous rivendica numerose operazioni mondiali di hacking. Uno dei suoi membri descrive il gruppo come "*una comunità planetaria, socialmente, ideologicamente e culturalmente eteroclita*". E aggiunge: "*non si può tracciare un profilo tipo. Quello che ci unisce è l'idea che la comunità cibernetica possa sfuggire ai controlli dello Stato ed esprimere la sua dissidenza aldilà delle frontiere. È un contropotere che, secondo noi, restaura l'equilibrio tra il debole e il forte. La rete è incontrollabile e deve rimanere tale*".

Anonymous si è messo in luce attraverso degli attacchi che hanno avuto grande eco per quanto i suoi bersagli potevano essere sensibili. Si può citare, nel mese di luglio del 2011, l'attacco della società Booz Allen Hamilton, un'impresa di consulenza che lavora in particolare per il Pentagono. Anonymous afferma di aver cancellato più di 4GB di dati e scoperto informazioni che permettono futuri attacchi contro strutture governative. Ma il gruppo non si presenta come una minaccia rivolta unicamente agli Stati. La comunità hacker Anonymous si è fatta conoscere anche per la sua lotta contro la Chiesa di Scientology, le reti di pedofili o addirittura un cartello della droga, Los Zetas, in Messico.

[2] http://it.wikipedia.org/wiki/Guy_Fakes.

Tuttavia, le azioni di Anonymous non raccolgono l'adesione dell'insieme della comunità hacker. Alcuni vi vedono "*degli pseudohacker che non sanno fare altro che servirsi di software fabbricati da altri*". Un hacker testimonia: "*alcuni si credono dei re della pirateria informatica mentre non sono capaci di scrivere una sola riga di programmazione. Sono pericolosi quanto dei conducenti che guidano senza patente e non sanno nemmeno dove si trovi il pedale del freno*". Anonymous riconosce d'altra parte degli sbandamenti: "*la nostra struttura è aperta, il suo principio è la garanzia dell'anonimato e ciascuno può effettuare un attacco rivendicandolo in nome di Anonymous, anche se la regola da noi non è di tirare l'acqua al proprio mulino. Abbiamo addirittura visto dei servizi ufficiali farsi passare per noi per screditare la nostra immagine*".

Se alcuni consacrano il proprio talento informatico all'affermazione di un contropotere, di una ribellione cibernetica, altri vi trovano l'opportunità di un'arma temibile per portare a termine i piani di imprese criminali.

Un attivismo lucrativo impegnato in una nuova forma di criminalità

Questa forma di hacking è in continua progressione. Essa risponde ai bisogni lucrativi di un individuo o di un'organizzazione criminale. Qui, lungi dal difendere la libera espressione o di cercare di far emergere un contropotere, l'hacker diventa un "cibermercenario" pronto, dietro remunerazione, a compiere delle missioni di ciberspionaggio, di cibercriminalità o perfino di ciberterrorismo.

Il forte aumento del numero di scambi commerciali su internet ha attirato le brame della pirateria informatica. Un hacker confida nel fatto che la vendita di dati confidenziali rubati mediante intrusione informatica nei server di siti di vendita online gli permetta di "arrotondare" lo stipendio di qualche centinaia o qualche migliaia di euro. L'individuo non è assolutamente un asso della pirateria informatica, lo riconosce lui stesso: "*non faccio altro che sfruttare le falle di sicurezza ormai ben note. Ci sono dei software molto accessibili che circolano sulla rete per effettuare questo tipo di intrusione in un server. La remunerazione varia in proporzione all'importanza dei dati rubati*".

Altri attaccano i server di grandi società per rivendere i file trafugati a dei concorrenti. Lo spionaggio industriale o economico mediante intrusione informatica permette di penetrare nel cuore stesso delle imprese per sottrarre rapidamente e senza il bisogno di compromissioni interne, spesso lunghe e fastidiose, i dati confidenziali ambiti. Inoltre, questi attacchi rimangono perlopiù "silenziosi". In effetti, si stima che l'80% delle imprese vittime di spionaggio informatico non sa di esserlo.

Aldilà del furto di informazioni confidenziali, i pirati informatici fanno gravare altre minacce sulle imprese. L'estate scorsa degli hacker sono riusciti a falsificare gli indirizzi di grandi direttori francesi e a inviare delle mail ai servizi di contabilità di grandi imprese con delle richieste di bonifico che andavano dai 90.000 agli 800.000 euro.

Alcune società sono anche vittime di estorsione di carattere informatico. Con la minaccia di attaccare i suoi server, l'hacker chiede all'impresa un riscatto. In generale, la minaccia di hacking si accompagna a un "defacing" (modifica non richiesta della homepage di un sito) come avvertimento. Quest'estorsione informatica può anche prendere la forma del *Ransomware*. In questo caso, l'hacker introduce nel PC o nella rete della sua vittima un virus

informatico che chiede del denaro per non mettere in esecuzione le proprie minacce. Molti internauti giapponesi ne sono stati vittime all'inizio del 2011. Infatti, degli amanti di manga a sfondo pornografico sono stati minacciati da un virus informatico che pretendeva il versamento di una somma di 1.500 yen (pari a circa 12 euro) per non rendere pubblico sulla rete il nome dell'internauta con le schermate dei siti pornografici visitati. Un importo volutamente basso per aumentare le probabilità di percepire la somma richiesta. Questo è anche uno dei vantaggi offerti all'hacker dalla criminalità cibernetica. L'immensità della rete offre una moltitudine di "prede" potenziali. Può accontentarsi, per ogni vittima, di piccole cifre e, così, limitare i rischi di denunce, aumentando le sue possibilità di ricevere il frutto del suo ricatto.

L'attrattiva del guadagno è una delle principali motivazioni della cibercriminalità. Tuttavia, per certi Stati e gruppi radicali, il "terrore informatico" è anche una nuova "arma operativa".

La minaccia ciberterroristica

Il terrorismo, tematica prioritaria nell'ambito della sicurezza in questo inizio di XXI secolo, ha trovato nelle reti informatiche un nuovo mezzo di espressione, affrancandosi dalle costrizioni frontaliere.

Di fronte a questa minaccia, dopo molti anni, gli Stati si esercitano nei ciberattacchi per premunirsi contro un possibile "attentato informatico". Si considerano molteplici scenari: attacchi alle reti telefoniche, ai centri di approvvigionamento dell'acqua o dell'elettricità, alle reti dei trasporti, dei circuiti finanziari, ecc.

Questo terrorismo informatico non ha nulla dello scenario fantascientifico. Recentemente, un'infrastruttura di gestione dell'acqua dello Stato dell'Illinois è stata vittima di un ciberattacco proveniente dalla Russia. Se quest'attacco non ha avuto gravi conseguenze sul funzionamento dell'impianto (sebbene si sia registrato un arresto temporaneo), esso può essere considerato un avvertimento, poiché il pirata è riuscito a penetrare nel cuore stesso del sistema di gestione della sua vittima. Inoltre, un altro impianto americano di trattamento dell'acqua sarebbe stato attaccato nello stesso modo.

Nel 2007, l'Estonia è stata sottoposta a un ciberattacco massiccio in seguito alla rimozione di un monumento commemorativo della Seconda Guerra mondiale nel centro di Tallinn. Questi attacchi, realizzati mediante negazione di servizio, hanno provocato la disconnessione di numerosi siti governativi e dimostrato la fragilità delle strutture statali rispetto alla minaccia informatica.

Secondo un rapporto dei servizi segreti canadesi reso di dominio pubblico, il grande blackout del 2003, che ha privato dell'elettricità decine di milioni di utenti nell'America del Nord e causato dei danni che ammontavano a sei miliardi di dollari, illustra le conseguenze che potrebbe avere un attacco informatico massiccio contro uno Stato.

Su questa minaccia di terrorismo informatico, Nigel Inkster, ricercatore presso l'Istituto Internazionale di Studi Strategici (IISS) di Londra ed ex membro dell'MI 6, il servizio d'intelligence estera britannica, confessa la sua preoccupazione di vedere degli hacker prestare i loro servizi o il loro esercito di computer "zombi" a imprese terroristiche.

Inoltre, se certi attacchi recenti sono stati perpetrati da gruppi che non proclamano un'appartenenza a un movimento terroristico, l'ipotesi di un'infiltrazione di numerose comunità di hacker da parte di gruppi radicali non deve essere scartata. Dopo che il gruppo Anonymous ha rivendicato, lo scorso luglio, di aver sottratto a un'impresa che lavorava per il Pentagono delle informazioni che avrebbero permesso futuri attacchi contro strutture governative, c'è grande timore di vedere questi dati cadere nelle mani di un gruppo terroristico.

L'attualità recente mostra anche che questo tipo d'attacco non è solo appannaggio di gruppi radicali o fondamentalisti. In effetti, numerosi Stati lavorano, nell'ombra delle reti, per costituire il loro "quarto esercito" ed elaborare attacchi informatici contro delle strutture nemiche. Paesi come la Cina, gli Stati Uniti, l'India, l'Iran, Israele, la Corea del Sud e la Corea del Nord sono regolarmente sospettati di essere all'origine di attacchi informatici ai server di Paesi ritenuti ostili. Nel luglio del 2009, vari ciberattacchi sono stati lanciati contro i siti web del governo americano quali il Pentagono e la Casa Bianca, come pure agenzie governative nella Corea del Sud. Questi due governi accusano la Corea del Nord di aver lanciato questi attacchi. Nel 2010, il virus *stuxnet*, che ha infettato 30.000 sistemi informatici in Iran – tra cui dei PC utilizzati dalla centrale nucleare iraniana di Bouchehr – è stato identificato come una ciberarma volta a colpire un bersaglio preciso, un'"infrastruttura di grande valore situata in Iran" e verosimilmente legata al programma di ricerca nucleare. Molti esperti in sicurezza informatica sospettano che l'*Unité 8200*, un'unità d'intelligence elettronica dell'esercito israeliano, specializzata nell'intrusione elettromagnetica e nella decifrazione di codici, sia all'origine del *malware stuxnet*. Questa stessa unità è stata recentemente sospettata di aver attaccato i server palestinesi nel mondo all'indomani dell'ingresso della Palestina nell'UNESCO.

*

Lo spazio cibernetico oggi è diventato indispensabile per i nostri scambi commerciali, politici, sociali o culturali. Quest'universo virtuale ha profondamente sconvolto i nostri comportamenti e modificato la nostra visione del mondo. Mediante le sue azioni e il suo potere d'influenza, la comunità hacker ne è diventata un attore di primo piano il cui impatto sociale e a livello di sicurezza pubblica è da prendere in considerazione nell'analisi delle principali sfide strategiche della nostra epoca.

Yves-Marie Peyry
Membro del comitato di redazione di *RENSEIGNOR*
Dicembre 2011