White paper

Hacktivism

Internet, il nuovo mezzo di espessione politica

Di François Paget, McAfee Labs™

Sommario

Che cos'è l'hacktivism? Una combinazione di politica, Internet e altri elementi. Partiamo dalla politica. L'hacktivism è una derivazione dell'attivismo, un movimento politico che pone l'accento sull'azione diretta. Basti pensare agli attivisti di Greenpeace che solcano i mari per disturbare la caccia alle balene o alle migliaia di attivisti che nel luglio 2011 hanno risposto all'appello del periodico Adbusters per occupare pacificamente un parco di New York durante la campagna Occupy Wall Street.

Aggiungendo l'attività di pirateria online (con entrambe le connotazioni, buona e cattiva) all'attivismo politico abbiamo l'hacktivism. Secondo alcune fonti questo termine fu usato per la prima volta in un articolo riguardante il cineasta Shu Lea Cheang, a firma di Jason Sack e pubblicato su *InfoNation* nel 1995. Nel 1996 comparve online in un articolo firmato da un membro del gruppo americano Culto della Vacca Morta (Cult of the Dead Cow)[1]. Nel 2000 Oxblood Ruffin, un altro adepto del cDc, scrisse che gli attivisti informatici si avvalgono della tecnologia per difendere i diritti umani[2]. A volte molti di loro, citando ideali libertari (il desiderio di preservare la libera impresa, le libertà individuali, le libertà di parola e di circolazione delle informazioni), affermano inoltre che Internet dovrebbe essere gratuito. Il movimento Anonymous è la personificazione dell'hacktivism. Inizialmente si concentrava su azioni a sostegno della propria idea di Internet, poi ha espanso le proprie attività dalle azioni nel web a iniziative di lotta nelle strade.

L'hacktivism non è un fenomeno nuovo. Gli eventi di tre anni fa nelle ex repubbliche sovietiche dell'Estonia (nel 2007) e della Georgia (nel 2008) hanno portato l'hacktivism all'attenzione del mondo. Questi due attacchi informatici, che sembravano più l'inizio di una guerra cibernetica piuttosto di ciò che ora chiamiamo hacktivism, sono piuttosto diversi da quelli che presero di mira gli oppositori di WikiLeaks e aziende come la Monsanto.

Date importanti nelle origini dell'hacktivism

Data	Commento
12.09.81	Si forma a Berlino il Chaos Computer Club[3].
1984	Viene pubblicato il libro *Hackers. Heroes of the Computer Revolution* (Haker: gli eroi della rivoluzione informatica) di Steven Levy.
08.01.86	Pubblicato per la prima volta *The Hacker Manifesto* (Il Manifesto degli hacker), di Loyd Blankenship (alias The Mentor).
16.10.89	Usando il protocollo DECNET, un worm si diffonde nel Maryland attraverso una rete di computer NASA. Si chiama WANK (Worms Against Nuclear Killers, Worm contro gli assassini nucleari) e uno dei suoi obiettivi è quello di lanciare un messaggio di denuncia dei test nucleari[4].
05.11.94 (Guy Fawkes Day, Festa di Guy Fawkes)	Gli Zippies, un gruppo di San Francisco, lancia un attacco denial of service distribuito (DDoS) e una campagna di mail bombing contro i server del governo britannico per protestare contro una legge che proibisce i concerti all'aperto dal ritmo ripetitivo[5].
21.12.95	In Italia lo Strano Network decide di bloccare i siti web francesi per protesta contro i test nucleari a Mururoa[6].
09.02.96	John Perry Barlow pubblica *A Declaration of the Independence of Cyberspace* (Dichiarazione di Indipendenza di Internet).
30.06.97	Il gruppo di hacker portoghesi UrBan Ka0s attacca circa 30 siti governativi indonesiani per attirare l'attenzione sull'oppressione del popolo di Timor[7].
29.01.98	Manifestazione virtuale a supporto della guerriglia zapatista e in risposta a un massacro commesso dalle forze paramilitari in un villaggio del Chiapas, Messico[8].
Novembre 1999	Toywar: atto di resistenza contro il distributore di giocattoli eToys Inc., che aveva fatto causa a un gruppo di artisti con il pretesto che il loro nome di dominio era troppo simile al suo[9].
03.12.99, ore 16 GMT	Il collettivo Electrohippies organizza un sit-in virtuale, chiedendo a tutti i propri sostenitori di visitare le pagine web dell'Organizzazione Mondiale del Commercio al fine di bloccare l'uscita del comunicato finale della conferenza di Seattle, nello stato di Washington[10].
20.06.01	Contro l'uso di aeroplani Lufthansa per deportare i migranti privi di documenti al di fuori della Germania, due reti umanitarie tedesche organizzano una protesta virtuale bloccando il sito web della compagnia aerea con un bombardamento di e-mail[11].

Oggi nell'hacktivism si possono comprendere tre grandi gruppi:

1. **Anonymous**, il componente più pubblicizzato del movimento. I suoi membri sono noti per il sostegno alla libertà di Internet e per opporsi a chiunque sia ritenuto responsabile di impedire il flusso delle informazioni. I loro metodi spesso includono atti di pirateria informatica, fra cui attacchi DDoS, e la sottrazione e distribuzione di informazioni riservate e/o personali. Prediligono spesso scherzi di cattivo gusto e a volte sembrano allontanarsi dalle azioni politiche. Una gran parte di questo documento è dedicata a loro.
2. **Cyberoccupiers o occupanti informatici**, i veri attivisti. Usano principalmente Internet e i social network per instaurare relazioni e per diffondere propaganda e informazioni. Includono **dissidenti informatici** che, come le loro controparti nel mondo reale, non riconoscono più la legittimità del potere politico al quale dovrebbero obbedire. Tentando azioni ad alto profilo su Internet, sperano di sostenere la democrazia e di combattere la corruzione nelle loro nazioni.
3. **Cyberwarriors o combattenti informatici**, patrioti che si raggruppano in "eserciti informatici" e che prosperano in molte nazioni dalle tendenze totalitarie. Vero o no, questi gruppi affermano di agire per conto dei loro governi, supportando movimenti nazionalisti ed estremisti. La loro arma principale consiste nello sfigurare i siti web. Inoltre, usando strumenti DDoS, fanno tutto il possibile per mettere a tacere i dissidenti.

Il movimento Anonymous

Origini

Le origini di Anonymous risalgono al forum di immagini 4chan. Creato nel 2003 e inizialmente dedicato alla cultura manga, questo sito web è attualmente uno dei più frequentati in rete, con circa 9,5 milioni di visitatori unici al mese[12].

Anonymous è una propaggine della sua sezione più attiva, "/b/". Secondo il suo creatore, Christopher "moot" Poole, la bacheca di immagini /b/ ha ricevuto nel 2008 da 150.000 a 200.000 messaggi al giorno[13]. Un'assoluta libertà di parola e l'anonimato sono due dei suoi dogmi principali. Su questo sito, la risata fragorosa (lol) sta fianco a fianco con la sua controparte malvagia "lulz"[14]. Pornografia hard-core e immagini scatologiche, razziste o antisemitiche compaiono accanto a fotografie spiritose ad opera di ragazzi di "lolcats", fotomontaggi di gatti mostrati nelle circostanze più improbabili. A meno che siano notate o reintrodotte, la quasi totalità delle innumerevoli immagini inserite scivola nell'oblio. Il sito non ha un sistema di iscrizioni. Chiunque può scriverci e la maggior parte della gente posta senza un nome utente, ricevendo il nome predefinito: anonymous.

In quel periodo i membri di Anonymous frequentavano anche l'Encyclopedia Dramatica (ideata da Sherrod De Grippo nel dicembre 2004)[15]. Doppione di Wikipedia, documentava le notizie in modo ironico o addirittura scioccante.

Nel 2006 Anonymous fece il suo primo colpo grosso, noto come l'attacco ad Habbo. Coordinandosi con 4chan e usando degli avatar dall'aspetto di neri americani tutti con un vestito grigio, il gruppo impediva agli avatar adolescenti di entrare nella piscina del mondo virtuale di Habbo Hotel. Anche allora le loro motivazioni erano ambigue. Per alcuni costituiva solo un divertimento; per altri invece era un modo di evidenziare la mancanza di personaggi di colore nei social network.

Un altro dei primi bersagli di Anonymous furono i pedofili. Nel 2007 Anonymous identificò un pedofilo canadese che, grazie a questa ricerca, fu in seguito arrestato[16]. Di nuovo, la motivazione non era chiara. Immagini e barzellette collegati alla pedofilia sono circolate spesso su 4chan, che dispone di un'icona chiamata Pedobear. Frédéric Bardeau e Nicolas Danet, autori del libro *Anonymous*, scrivono: "Nella cultura di 4chan, la gente denuncia i pedofili e allo stesso tempo schernisce coloro che pubblicano su Internet immagini, non sempre in circostanze liete, dei propri bambini"[17].

Anonymous divenne veramente noto al pubblico nel 2008 tramite il progetto Chanology[18]. Tale progetto è tuttora in corso e i suoi obiettivi non sono cambiati. Il progetto contesta in modo non violento i miti alla base di Scientology, oltre che l'oscurantismo e i pericoli cui espone i suoi membri dal isolandoli dal resto del mondo.

Il 10 febbraio 2008 Anonymous scese in strada. Per evitare di essere identificati dagli adepti di Scientology, gli attivisti indossarono le maschere di Guy Fawkes, l'eroe dei fumetti protagonista del film *V per Vendetta*.

Locandina del film *V per Vendetta*

Guy Fawkes (1570-1606) era un cattolico inglese che aveva pianificato di assassinare il re Giacomo I il 5 novembre 1605, in risposta alla sua politica sulla religione, che riteneva non fosse sufficientemente tollerante.

La serie di fumetti del 1980 V for Vendetta, scritta da Alan Moore e illustrata da David Lloyd, che ha visto un adattamento cinematografico nel 2006 con un film dei fratelli Wachowski, tratta una storia completamente diversa. L'azione di svolge a Londra intorno al 2040, in una società dittatoriale dove un combattente per la libertà chiamato "V" cerca di instaurare un cambiamento politico e sociale, portando avanti una vendetta personale violenta contro i potenti. Il protagonista indossa una maschera con la faccia di Guy Fawkes, che desidera imitare incitando la gente a liberarsi dalla loro apatia. Dopo essere stata rielaborata per il film, la maschera è stata adottata dai membri di Anonymous per forgiare un'identità precisa.

Non entreremo nel dettaglio delle azioni che Anonymous portò avanti tra il 2006 e l'inizio dell'operazione WikiLeaks Cablegate. Un riepilogo è comunque fornito nella seguente tabella.

Date importanti nella storia di Anonymous

Data	Commento
12.07.06	Il grande attacco ad Habbo. Primo attacco al social network per adolescenti Habbo Hotel. Evidenzia la mancanza di personaggi di colore.
Dicembre 2006	Attacco al sito web del nazionalista americano Hal Turner.
Agosto 2007	Appoggio ai monaci birmani durante la Rivoluzione Zafferano.
05.12.07	Arresto del pedofilo Chris Forcand in Canada, al quale sembra abbiano contribuito i membri "vigilanti informatici" di 4chan[19].
14.01.08	Progetto Chanology. Caricamento su YouTube dei video di propaganda interni di Scientology. Nonostante la rapida rimozione dei video, la loro pubblicazione è il trampolino di lancio per la lotta di 4chan contro Scientology.
28.03.08	Informazione o mistificazione? I membri di Anonymous sono accusati di inserire animazioni e messaggi in JavaScript sul forum della Fondazione per l'Epilessia, al fine di causare emicranie e attacchi alle persone epilettiche.

Giugno 2008	I siti di musica hip-hop SOHH e AllHipHop vengono attaccati dopo aver pubblicato insulti ai sostenitori di 4chan.
Gennaio 2009	Un giovane californiano viene bersagliato per aver creato un sito web di protesta contro il turpiloquio (No Cussing Club).
Aprile 2009	Operazione MarbleCake. Manipolazione del sondaggio della rivista Time Magazine che elegge la persona più influente del mondo[20].
Aprile 2009	Operazione Baylout. Controversia riguardo il Pacchetto di Riforma delle Telecomunicazioni (un insieme di direttive europee per contrastare i download illegali). Attacco alla IFPI (l'associazione internazionale rappresentante l'industria discografica).
20.05.09	Giornata YouPorn. Distribuzione su YouTube di video apparentemente innocui, che però nascondono immagini pornografiche.
Giugno 2009	Appoggio ai dissidenti iraniani[21].
Settembre 2009	Operazione Didgeridie (Progetto Skynet). Prima fase aggressiva ("operazione distruttiva") per protestare contro una legge governativa mirante a filtrare i dati su Internet.
Ottobre 2009	Operazione CyberDyne Solutions (Progetto Skynet). Seconda fase informativa per insegnare alla gente come eludere i blocchi su Internet.
06.01.10	Giornata YouPorn (seconda edizione) per protesta contro la chiusura dell'account Lukeywes1234 (definito il re di /b/)[22].
10.02.10	Lancio dell'Operazione Titstorm. Protesta contro la decisione delle autorità australiane di bandire la pubblicazione di immagini pornografiche[23].
Settembre 2010	Operazione Payback. Inizia dopo che un'azienda indiana annuncia di aver condotto attacchi DoS ai siti di BitTorrent usati per scaricare gratuitamente musica e video normalmente protetti dai diritti d'autore. In risposta vengono attaccati molti siti associati ad artisti e all'industria cinematografica e musicale[24]. La cronologia di questa operazione è riportata sul sito myce.com[25].

Anonymous è un meme di Internet, un fenomeno di massa propagato da diverse comunità costituite da utenti di Internet che agiscono in modo anonimo per un obiettivo specifico. Un meme di Internet fa riferimento al concetto sociologico di un meme, un elemento culturale riconoscibile che viene duplicato e trasmesso dal comportamento di un singolo imitato da altri singoli.

Con Distributed Denial of Service (DDoS) si intende un attacco informatico che utilizza computer distribuiti sulla rete, solitamente parte di una botnet (rete di robot). L'obiettivo è di rendere non disponibile un servizio Internet ai suoi utenti. Può essere utilizzato per bloccare un file server, rendere inaccessibile un server web, bloccare la distribuzione dell'e-mail in un'azienda o rendere non disponibile un sito web. Un attacco denial of service (DoS) proviene da un'unica fonte.

Definizione del movimento

Anche se i membri di Anonymous sono scesi in strada per contestare Scientology, il loro principale terreno di battaglia oggi è Internet e le loro azioni consistono nel reagire a qualsiasi tentativo di regolamentare questo mezzo. Per loro la libertà online consiste nel poter distribuire immagini "spazzatura" e nel combattere la censura iraniana. È la possibilità di scaricare gratuitamente musica e video senza preoccuparsi dei diritti d'autore e di promuovere la libertà completa nella circolazione di informazioni, anche se deriva da fonti che non dovrebbero diventare pubbliche. Pertanto era ovvio che Anonymous avrebbe appoggiato WikiLeaks non appena divenne chiaro che qualcuno voleva imbavagliarlo.

Più che un gruppo, Anonymous è un'idea. È un meme che i suoi singoli membri possono adottare per agire nell'anonimato[26].

Anonymous è un'etichetta che un individuo si assegna in un dato momento quando eseguono delle specifiche azioni, anche non molto sofisticate. Anche se non sembrano avere dei veri capi, questi individui si incontrano occasionalmente per portare avanti azioni coordinate - da scherzi (spesso di cattivo gusto) all'attivismo - per le quali trovano una motivazione comune. Qualsiasi utente di Internet può connettersi a una chat IRC, partecipare a discussioni e prendere parte o suggerire un'"operazione" su un argomento. Durante i livelli più alti di attività, particolarmente durante la Primavera Araba o l'Operazione Payback, pare che le reti di chat abbiano raggiunto un picco di presenze pari a 3.000 persone connesse simultaneamente.

La maggior parte delle volte un'operazione consiste nel rendere uno o più siti web inaccessibili. A tale scopo i membri di Anonymous usano vari tipi di software per attacchi; i più diffusi sono LOIC (Low Orbit Ion Canon, cannone ionico di orbita inferiore, uno strumento open-source per testare le reti e per creare attacchi DoS) e HOIC (il correlato High Orbit Ion Canon, cannone ionico di orbita superiore). Con tale software il sito da attaccare viene bersagliato di interrogazioni fino alla saturazione. Questo attacco si chiama denial of service distribuito (o DDoS), che è difficile da sopportare per qualsiasi sito.

Solitamente i membri di Anonymous postano dei video per annunciare e rivendicare la responsabilità delle operazioni. I video hanno spesso una voce fuori campo sintetizzata, che è diventata il marchio di Anonymous. Oltre a usare canali IRC e video, i membri di Anonymous comunicano tramite Twitter, Facebook e vari siti web. A prescindere dal mezzo, il messaggio termina sempre con le parole "We are Anonymous. We are Legion. We do not forgive. We do not forgive. Expect us." (Siamo Anonymous. Siamo una legione. Non perdoniamo. Non dimentichiamo. Aspettateci.)". La qualità dei video e delle immagini indica che la gamma delle loro capacità include le arti grafiche.

Il 28 novembre 2010 ebbe inizio l'Operazione Cablegate. Senza rivelare nessuna informazione cruciale, WikiLeaks aveva cominciato a pubblicare i telegrammi diplomatici statunitensi che davano un punto di vista inedito sul funzionamento interno del potere. Anonymous fu seccato nel vedere gli atti ostili che seguirono, miranti a imbavagliare WikiLeaks, così reagì e occupò il centro della scena.

WikiLeaks incontra Anonymous

WikiLeaks fu fondato nel 2006 dall'australiano Julian Assange, che ritiene fermamente che ci sia una forte disparità nell'accesso alle informazioni tra i governi e i relativi cittadini. Per rimediare a questa situazione, si propose come intermediario tra il pubblico e le talpe, che promise di proteggere. Per garantire l'anonimato di quest'ultime si rivolse a Jacob Appelbaum, un partecipante attivo del TOR (The Onion Router, software libero che consente la connessione a Internet senza rivelare il proprio indirizzo IP). Negli anni WikiLeaks ha reso noti documenti pubblici ma, spesso, anche segreti.

La tabella seguente elenca vari documenti pubblicati fra il 2006 e il novembre 2010, un mese memorabile nella storia di Anonymous e dell'hacktivism.

Date importanti nella vita di WikiLeaks

Data	Pubblicazioni di WikiLeaks
Dicembre 2006	Nota riguardante l'ordine di un assassinio politico in Somalia
Agosto 2007	Rapporto che accusa l'ex presidente del Kenya Daniel Arap Moi, e la sua famiglia, di corruzione[27]
Novembre 2007	Manuale dell'esercito statunitense risalente al 2003 sulla prigione della Baia di Guantanamo[28]
Marzo 2008	Documento interno dell'Ufficio Affari Speciali della setta di Scientology[29]
Maggio 2008	Documento di lavoro sull'Accordo Commerciale Anticontraffazione (ACTA)[30]
Aprile 2009	Riepilogo delle udienze del pedofilo belga Marc Dutroux[31]
Luglio 2009	Un documento interno appartenente alla banca islandese Kaupthing, elencante vari prestiti di bassa qualità approvati solo pochi giorni prima di essere nazionalizzata[32]
Novembre 2009	E-mail e file assegnati a funzionari del Climatic Research Unit (Unità di Ricerca sul Clima) dell'East Anglia (Regno Unito)
Aprile 2010	Omicidio collaterale: video dell'esercito statunitense mostrante l'uccisione di due fotografi della Reuters a Bagdad durante un attacco aereo il 12 luglio 2007, girato da un elicottero Apache. Soprannominato "Project B" da Assange, questa pubblicazione segna l'inizio della fama mondiale del sito web.
Luglio 2010	Diario della guerra afgana: 91.000 documenti militari segreti statunitensi sulla guerra in Afghanistan (in collaborazione con *The Guardian*, *The New York Times* e *Der Spiegel)*
Ottobre 2010	Diari della guerra irachena: 391.832 documenti segreti sull'Iraq che coprono il periodo dal 1° gennaio 2004 al 31 dicembre 2009
28.11.10	Cablegate: WikiLeaks inizia a divulgare i telegrammi diplomatici statunitensi e annuncia di possederne oltre 250.000

Come Jester, molti attivisti informatici e hacker scrivono utilizzando l'alfabeto "leet speak" (o "linguaggio elitario"), ovvero l'utilizzo di numeri o simboli che generalmente somigliano alla forma delle lettere per rendere il risultato meno comprensibile.

Per esempio, *leet speak* può essere scritto nel modo seguente:

- L33T 5P34K: codifica di base
- 1337 5p34k: codifica leggera
- £33‡ šp3@ķ: codifica di medio livello
- |_ 33¯|¯ _/¯|°3/-\|<: codifica complessa

(Fonte: Wikipedia. *http://fr.wikipedia.org/wiki/Leet_speak)*

Il 3 dicembre 2010 l'account PayPal di WikiLeaks fu sospeso e contemporaneamente aumentò il numero delle cause intentate contro di esso. L'hacker noto come Jester (th3j35t3r), autodefinitosi "attivista informatico a fin di bene", rivendicò di aver chiuso temporaneamente il sito di WikiLeaks. Per farlo aveva usato il tool DoS XerXes, che utilizzata regolarmente contro i siti web jihadisti[33].

In risposta alle preoccupazioni riguardanti la limitata accessibilità, WikiLeaks venne copiato su circa 20 siti "ufficiali", la maggior parte dei quali situata in nazioni con una legislazione digitale liberale. Il 4 dicembre, con la comunità Internet mobilitata per dare aiuto, in tutto il mondo si potevano trovare alcune centinaia di siti mirror. Uno di questi siti venne creato in Russia (mirror.wikileaks.info/IP: 92.241.190.202) da un fornitore di servizi Internet (Heihachi Ltd.) noto per la sua associazione con il crimine informatico. Il dominio wikileaks.org venne quindi puntato verso questo sito specifico. Spamhaus avvertì gli utenti Internet dei pericoli di tale mirror[34]. In risposta, l'organizzazione subì attacchi DDoS.

Dato che sanzioni finanziarie continuarono a essere imposte a Julian Assange nei giorni seguenti (da PostFinance, MasterCard, Visa International e Amazon), entrò in scena Anonymous. Il gruppo sferrò attacchi DDoS contro chiunque si opponesse a WikiLeaks. L'Operazione Payback, che originariamente prendeva di mira gli oppositori della pirateria Internet, si allargò a nuovi obiettivi. I volontari vennero invitati a scaricare LOIC, che usa la funzione "hive mind" (mente collettiva) per trasformare ogni computer in un bot volontario e consentire un attacco coordinato. All'apice degli attacchi c'erano 3.000 sostenitori connessi contemporaneamente.

Le strade di WikiLeaks e Anonymous si erano incrociate già diverse volte. Nel 2008 le rivelazioni relative a Scientology e all'ACTA ne avevano identificato gli interessi in comune. Alla fine di marzo 2010, prima del lancio del video Collateral Murder (Omicidio collaterale) (mostrante i fotografi della Reuters uccisi a Bagdad durante l'attacco aereo del 12 luglio 2007), Assange si trovava a Reykjavik con Raffi Khatchadourian, giornalista del *New Yorker*. Il periodico scrisse che, mentre lasciava la conferenza stampa di New York, il fondatore di WikiLeaks aveva pronunciato le parole "Ricordate, ricordate il 5 novembre [35]."Si trattava di un chiaro riferimento a Guy Fawkes, l'eroe anonimo che tentò di far saltare in aria il parlamento inglese nel 1605.

Intorno al 10 dicembre 2010 un gruppo di attivisti informatici che affermavano di far parte di Anonymous cambiò strategia. Questa decisione fu presa forse a causa dell'arresto di alcuni giovani utenti di LOIC. Gli attivisti informatici annunciarono l'Operazione Leakspin e si definirono "un collettivo spontaneo di persone con il comune obiettivo di proteggere il libero flusso di informazioni su Internet. ... Anonymous non è sempre lo stesso gruppo di persone: Anonymous è un'idea vivente [36]". Il collettivo chiese agli utenti di Internet di avviare un proprio lavoro investigativo sui telegrammi diplomatici pubblicati da WikiLeaks. L'obiettivo era di velocizzare il processo di scoperta per pubblicare fatti comunemente noti che però non erano ancora stati rivelati ai media. Anonymous lo chiamò crowd journalism o giornalismo di massa, una forma di giornalismo partecipativo che funziona in modo simile al modello di Wikipedia. Il gruppo suggerì inoltre un'altra iniziativa, l'Operazione Black Face, agli utenti che frequentano i social network. Il 18 dicembre chiese loro di sostituire la propria foto del profilo con uno sfondo nero, in segno di appoggio a WikiLeaks e Julian Assange. Senza molto successo, i membri di Anonymous scesero anche in strada a distribuire volantini (Operazione PaperStorm).

Operazione Payback: appello a sostegno di WikiLeaks

Tutti questi tipi di operazioni si propagarono durante il mese di dicembre e furono prevalentemente concentrati sulla difesa di WikiLeaks. Nonostante un calo di intensità dovuto ad appelli verso altri tipi di azioni, alla fine di dicembre si verificarono alcuni attacchi DDoS che videro Bank of America come vittima principale. Si formò una fazione di hacker anti-WikiLeaks, guidati da Jester, che tentarono di smascherare i membri di Anonymous partecipanti agli attacchi. Nel movimento, ulteriori divisioni portarono a conflitti fra quei membri accusati di essere semplici smanettoni degli script, vogliosi di colpire indiscriminatamente, e coloro che preferivano azioni più militanti contro i loro bersagli.

La fine del 2010 preannunciò un periodo di diffamazioni e diversificazioni. Lo Zimbabwe fu il primo Paese a subire la collera di Anonymous. Analizziamo questo esempio per capire come vengono prese le decisioni all'interno del gruppo.

A metà dicembre 2010, la moglie del presidente Robert Mugabe minacciò la redazione di un giornale locale che aveva usato informazioni, tratte da alcuni telegrammi diplomatici, per rivelare che la first lady si era arricchita con la vendita illegale di diamanti[37]. La decisione di attaccare il sito web del partito del presidente fu presa nella serata del 28 dicembre sul canale IRC #operationBOA.AnonOps. Nella stessa occasione alcuni membri avviarono una discussione in merito al prossimo bersaglio[38]. Il dibattito si concentrò sui siti governativi delle nazioni accusate di violare in qualche modo la libertà di parola su Internet. Furono citati Ungheria, Polonia e Iran, ma lo Zimbabwe si rivelò come l'obiettivo più attraente. Pochi minuti più tardi, l'istigatore del progetto creò il canale #OperationZimbabwe, contenente istruzioni per la configurazione del software LOIC. Un'ora dopo un sito governativo non era più disponibile mentre, durante la notte, fu defacciato il sito del Ministero delle Finanze. Parte del contenuto della home page fu sostituito dal messaggio "Siamo Anonymous. Siamo una legione. Non perdoniamo. Non dimentichiamo. Aspettateci.".

Uno script kiddie (smanettone dello script) è un termine spregiativo che fa riferimento a qualcuno che è spesso giovane e cerca di farsi passare per un hacker, nonostante la conoscenza limitata o inesistente dei sistemi informatici. Spesso vengono accusati di utilizzare - senza saperli padroneggiare - script e programmi che scaricano da Internet, senza cercare di comprenderli.

Quindici mesi di attività

All'inizio del gennaio 2011 Anonymous decise di espandere il suo ambito d'azione, anche se l'affare WikiLeaks era ancora in discussione. Durante il primo trimestre dell'anno il gruppo incoraggiò la Primavera Araba. Tre mesi dopo, nonostante un po' di confusione, entrò in scena il gruppo Lulz Security. Il gruppo condusse attività di pirateria informatica a tutto campo che alla fine attirarono l'attenzione. Allo stesso tempo, altri attacchi ricordavano le prime attività di Anonymous, con un movente più goliardico che ideologico. A metà 2011 emersero dei centri di interesse distinti che dimostrarono il multiculturalismo di Anonymous.

La legge segnò qualche punto a suo favore aumentando il numero di arresti negli Stati Uniti, nel Regno Unito e in Olanda. La polizia fu oggetto di numerosi attacchi da parte di AntiSec e di chiunque la accusava di usare metodi brutali nei vari incontri organizzati dai movimenti Occupy e degli Indignati.

Alla fine del 2011 i media avevano fatto conoscenza con Anonymous, che è rimasto attivo anche se le sue divisioni - e persino manipolazioni - non hanno aiutato gli esterni a comprendere il movimento. Tentativi di azioni coordinate fra dimostranti e dimostranti informatici hanno avuto scarso impatto. Si è dovuto attendere fino all'inizio del 2012 per vedere la comparsa di numerose maschere di Guy Fawkes nelle strade.

Scorriamo i fatti più salienti.

Primavera Araba

Il 2 gennaio 2011 segnò l'inizio dell'Operazione Tunisia. All'inizio contestava il blocco del principale nodo di accesso al sito di WikiLeaks nel Paese. Gli attacchi colpivano solitamente un tunisino immaginario chiamato Ammar 404, nome ispirato al messaggio "Errore 404" mostrato dai browser web che tentavano di accedere a uno dei molti siti bloccati dal regime di Ben Ali. Molto rapidamente gli obiettivi si ampliarono a una protesta generale contro il regime, in connessione con le proteste in strada che lasciavano decine di morti.

AMMAR 404: la censura del web in Tunisia

Dopo la caduta del presidente Ben Ali il 15 gennaio, Anonymous sentì di aver dato un contributo sostanziale alla Rivoluzione del Gelsomino. Il gruppo affermò: "Siamo in guerra … una guerra che Anonymous sta vincendo [39]".

Questa affermazione era esagerata. La rivoluzione riuscì grazie ai manifestanti tunisini che non temevano di continuare a protestare nelle strade. La parte di Internet nel successo di questa rivoluzione, e in quelle che seguirono, sembra piuttosto limitata. Gli utenti di Internet che giocarono un ruolo, lo fecero soprattutto tramite i social network (Facebook e Twitter), mettendo in collegamento manifestanti locali e giornalisti stranieri e fornendo informazioni in tempo reale.

All'inizio del 2011 Anonymous chiamò alla mobilitazione per cause simili in Egitto (primo messaggio su AnonNews datato 23 gennaio), Arabia Saudita, Algeria (20 gennaio), Libia (18 febbraio), Iran (9 febbraio), Bahrein (17 febbraio), Siria, Giordania, Yemen e Marocco (15 febbraio).

Il gruppo informale di hacker RevoluSec, che ruota intorno ad Anonymous, portò avanti delle operazioni per deturpare diversi siti ufficiali appartenenti a città siriane. Il gruppo creò un monumento digitale per le vittime del conflitto, rappresentato da tante sagome umane di colore rosso. In questo esempio possiamo vedere il modo in cui Anonymous traduce in immagini la realtà dei conflitti locali in immagini[40]. Nel capitolo sui dissidenti informatici parleremo dell'hacktivism in Siria, in particolare delle azioni del gruppo Telecomix.

HBGary

Un altro fatto saliente del primo trimestre ci è offerto da *The Financial Times*. Il 5 febbraio 2011 il quotidiano annunciò che Aaron Barr, amministratore delegato di HBGary Federal, intendeva fornire all'FBI, l'Ufficio Investigativo Federale statunitense, le informazioni raccolte in merito ad Anonymous[41]. Il gruppo iniziò immediatamente ad attaccare i server dell'azienda. Tramite iniezione SQL, password non efficaci e social engineering, fu in grado di dirottare oltre 70.000 e-mail che furono rapidamente rese pubbliche. Il contenuto di alcune di esse era così distruttivo che Barr dovette dimettersi tre settimane dopo[42]. L'azienda fu anche pesantemente criticata dai media.

Anonymous pubblicò un file delle sue scoperte in HBGary. Conteneva oltre 130 fra nominativi e nomi utente, insieme a dati personali.

Lulz Security e delazioni

A partire dalla fine del primo trimestre 2011, una parte del movimento Anonymous privilegiò l'attivismo politico, criticando le azioni disordinate eseguite da un piccolo gruppo di hacker apparentemente vicini al gruppo Gn0sis. Nel dicembre 2010, il gruppo Gn0sis compromise Gawker Media, un gruppo multimediale online statunitense con una lunga storia di rapporti difficili con Anonymous e 4chan[43]. In quel periodo Gn0sis era molto attivo. Alcuni membri del gruppo furono sospettati di essere responsabili della violazione di HBGary.

All'attivismo, questo gruppo preferisce gli scherzi di cattivo gusto (lulz). I suoi membri si incontrano regolarmente sul popolare canale IRC #HQ. Quando interagiscono con Sabu, che a quanto pare è il loro capo, usano i nomi utente Topiary, Kayla, Tflow, m_nerva e Joepie91.

Il 7 maggio 2011, sotto il nome di Lulz Security (o LulzSec), il gruppo iniziò a rivendicare vari atti di pirateria. I suoi misfatti portavano di solito la firma "for the lulz". Due giorni dopo, con l'aumentare delle tensioni fra i due clan, il sito web anonops.net/ru, punto principale di inserimento per la comunità di Anonymous, fu compromesso da Ryan, un coamministratore vicino a Lulz. Nelle parole dei suoi oppositori, tentò di organizzare un golpe contro Anonops per assumere il controllo del sito.

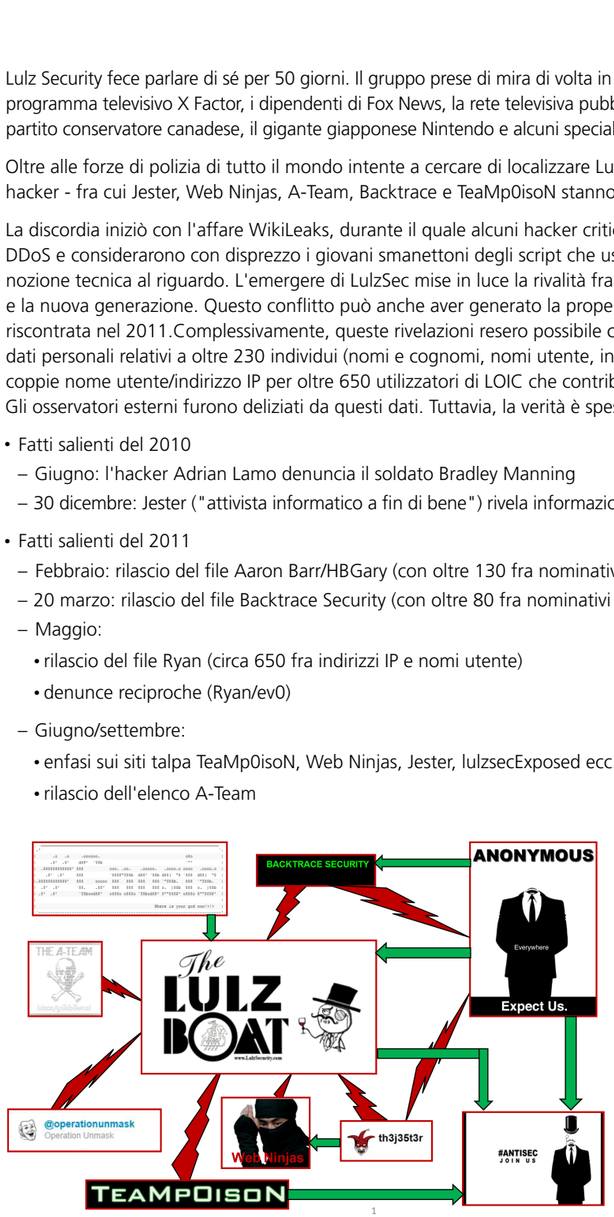
Il 18 maggio il giornalista Barrett Brown, portavoce ufficioso di Anonymous, rilasciò un'intervista a Computerworld nella quale denunciava il comportamento irresponsabile di Ryan[44].

Lulz Security fece parlare di sé per 50 giorni. Il gruppo prese di mira di volta in volta i concorrenti del programma televisivo X Factor, i dipendenti di Fox News, la rete televisiva pubblica statunitense PBS, il partito conservatore canadese, il gigante giapponese Nintendo e alcuni specialisti della sicurezza vicini all'FBI.

Oltre alle forze di polizia di tutto il mondo intente a cercare di localizzare LulzSec, anche diversi gruppi di hacker - fra cui Jester, Web Ninjas, A-Team, Backtrace e TeaMp0isoN stanno cercando di smascherarli.

La discordia iniziò con l'affare WikiLeaks, durante il quale alcuni hacker criticarono l'uso di attacchi DDoS e considerarono con disprezzo i giovani smanettoni degli script che usavano il LOIC senza alcuna nozione tecnica al riguardo. L'emergere di LulzSec mise in luce la rivalità fra gli hacker tradizionali e la nuova generazione. Questo conflitto può anche aver generato la propensione alla diffamazione riscontrata nel 2011.Complessivamente, queste rivelazioni resero possibile comporre un insieme di dati personali relativi a oltre 230 individui (nomi e cognomi, nomi utente, indirizzi ecc.) e un elenco di coppie nome utente/indirizzo IP per oltre 650 utilizzatori di LOIC che contribuirono agli attacchi DDoS. Gli osservatori esterni furono deliziati da questi dati. Tuttavia, la verità è spesso celata dalle bugie:

- Fatti salienti del 2010
  - Giugno: l'hacker Adrian Lamo denuncia il soldato Bradley Manning
  - 30 dicembre: Jester ("attivista informatico a fin di bene") rivela informazioni sugli aggressori di PayPal
- Fatti salienti del 2011
  - Febbraio: rilascio del file Aaron Barr/HBGary (con oltre 130 fra nominativi e nomi utente)
  - 20 marzo: rilascio del file Backtrace Security (con oltre 80 fra nominativi e nomi utente)
  - Maggio:
    - rilascio del file Ryan (circa 650 fra indirizzi IP e nomi utente)
    - denunce reciproche (Ryan/ev0)
  - Giugno/settembre:
    - enfasi sui siti talpa TeaMp0isoN, Web Ninjas, Jester, lulzsecExposed ecc.
    - rilascio dell'elenco A-Team



Relazioni tra LulzSec, Anonymous e altri movimenti

Il 17 giugno LulzSec celebrò il suo millesimo tweet e annunciò la fine della rivalità con Anonymous. Due giorni dopo, le due fazioni lanciarono l'operazione congiunta AntiSec. Accusarono i governi di voler limitare la libertà di parola su Internet tramite le policy di sicurezza e fecero appello a tutti i simpatizzanti per attaccare le agenzie e i governi responsabili.

Il 25 giugno LulzSec annunciò il termine delle sue operazioni. Come atto finale, pubblicò una serie di file su Pirate Bay, con il titolo 50 Days of Lulz. Le numerose attività di polizia in corso a quella data (specialmente negli Stati Uniti e nel Regno Unito) furono ampiamente responsabili di quest'uscita di scena. LulzSec continuò fino a settembre. Fino ad allora solo Sabu, il loro capo, sembrava essere sfuggito ai guai giudiziari. Benché il 22 settembre avesse confermato con un tweet che la maggior parte dei suoi amici era stata arrestata, solo nel febbraio 2012 siamo venuti a conoscenza del suo doppio gioco, ordito dopo il suo arresto del giugno 2011[45].

Sabu conferma in un tweet che la maggior parte dei suoi amici è stata arrestata.

Diritti verdi

Come abbiamo visto, i membri di Anonymous non si coalizzano su un singolo obiettivo. Hanno varie motivazioni e si aggregano, di volta in volta, con le persone che sono d'accordo con l'uno o con l'altro. Benché le prime azioni di AntiSec abbiano sollevato entusiasmi fra alcuni attivisti informatici, altri hanno voluto unirsi intorno a un'ideale ambientalista.

Alcuni giorni dopo il disastro sismico e nucleare di Fukushima, in Giappone, i membri di Anonymous lanciarono l'Operazione Green Rights. Lo scopo era quello di protestare contro le conseguenze ambientali e di denunciare sui social network la dipendenza dall'energia nucleare. La maggior parte dei sostenitori fu reclutata in Francia, Italia, Stati Uniti e America Latina. Ogni attacco fu preceduto da uno o più manifesti politici tradotti in più lingue. Quando giunse il momento dell'attacco, fu inviato un volantino con istruzioni specifiche sull'uso di LOIC.

Volantino di preparazione dell'attacco a Monsanto

Dopo l'attacco del maggio 2011, Anonymous ha affrontato altre problematiche ambientali colpendo a turno i siti web delle varie società elettriche ENEL, General Electric, EDF ed ENDESA[46]. Questi attacchi includevano:

- Giugno: protesta contro i produttori di organismi geneticamente modificati (Monsanto, Bayer)
- Luglio: gli eccessi dei giganti del petrolio (Exxon Mobil, ConocoPhillips, Canadian Oil Sands Ltd., Imperial Oil, The Royal Bank of Scotland, The Canadian Association of Petroleum Producers)
- Dicembre: violazioni da parte dei progetti ferroviari nelle aree naturali protette (treno ad alta velocità tra Francia e Svizzera, tratta ferroviaria Lione-Torino)
- Dicembre: il comportamento delle compagnie minerarie nei riguardi dei residenti nelle future aree operative (Guatemala e Perù)
- Dicembre 2011 – gennaio 2012: difesa delle popolazioni amazzoniche minacciate dalla costruzione della diga sul fiume Xingu

Altre operazioni

Nel secondo trimestre 2011, Anonymous condusse altre due operazioni. A maggio, l'Operazione Blitzkrieg prese di mira i siti web di estrema destra e neonazisti[47]. L'Operazione SaveKids cercò di identificare e denunciare le persone coinvolte nella pornografia infantile[48].

AntiSec, doxing e copwatching

Anche se Lulz Security sembra essere sparito, il collettivo AntiSec ne ha raccolto l'eredità. AntiSec, che si dice sia parte integrante di Anonymous, riunisce tutti coloro che desiderano sfidare le leggi, i governi e le società che direttamente o indirettamente infrangono le libertà individuali. Per maggiori informazioni sulle azioni eseguite sotto il nome di AntiSec, visitare la pagina di Wikipedia ad esse dedicata[49].

Il doxing è la pratica di pubblicare foto, informazioni di contatto, informazioni personali e informazioni relative alla famiglia per un'azione compiuta da una o più persone. Il copwatching prevede la pubblicazione di dati identificativi e indagini relative a personale delle forze dell'ordine su siti web dedicati.

Illustrazione tratta da un articolo apparso nel dicembre 2011[50]

L'arma preferita da AntiSec nel 2011 fu il doxing. Con nomi in codice tratti dagli insulti gridati alla polizia, il collettivo divulgò a ondate i dati sottratti ai server dei corpi di polizia o alle aziende che collaborano direttamente con essi.

Principali attacchi di doxing

Ch** la Migra (F****** la polizia frontaliera)**

Data	Obiettivi
24.06.11	Dipartimento di Pubblica Sicurezza dell'Arizona
29.06.11	Dipartimento di Pubblica Sicurezza dell'Arizona
01.07.11	Confraternita della Polizia dell'Arizona
02.09.11	Associazione dei capi della polizia del Texas

F* FBI Friday (Venerdì del F****** all'FBI)**

Data	Obiettivi
05.06.11	InfraGard
08.07.11	IRC Federal
29.07.11	ManTech
19.08.11	Vanguard Defense Industries
18.11.11	Fred Baclagan, investigatore nel settore del crimine informatico
03.02.12	Polizia di Boston

Le vittime del doxing sono stati singoli individui (spesso poliziotti). Il 24 settembre 2011 un poliziotto di New York spruzzò del gas lacrimogeno contro due donne che manifestavano. Due giorni dopo, una significativa quantità di dati relativa a lui e alla sua famiglia fu diffusa su Internet. Il 18 novembre, al campus Davis dell'Università della California, un poliziotto spruzzò del gas sui manifestanti impegnati in un sit-in. Il suo nome e le informazioni private furono immediatamente pubblicati.

Il doxing non si limita agli Stati Uniti. Il 26 settembre AnonAustria pubblicò le informazioni personali di 25.000 poliziotti austriaci[51]. Due giorni dopo in Francia, il Ministero dell'Interno denunciò per diffamazione un sito web (CopwatchNord-idf.org) che metteva in cattiva luce la polizia mostrando immagini e testimonianze relativi a sospetti abusi, insieme a commenti offensivi[52].

Il 6 agosto Anonymous annunciò due fughe di dati in Sud America. Uno riguardava la polizia federale brasiliana (8 GB di dati rilasciati), mentre l'altro conteneva le informazioni personali di 45.000 poliziotti ecuadoriani[53].

La risposta dei corpi di polizia

Dopo gli attacchi DDoS sferrati durante l'Operazione Payback alla fine del 2010, le forze di polizia hanno tentato di spazzare via i membri di Anonymous contravvenenti alla legge. Indagini, perquisizioni e arresti furono frequenti fra il luglio 2011 e il febbraio 2012.

La tabella seguente mostra i dati della recente attività di applicazione della legge e si basa su articoli apparsi tra il dicembre 2010 e l'aprile 2012.

Numero approssimativo di indagini, perquisizioni e arresti negli ultimi 15 mesi

Nazione	Totale	Minori di 18 anni	Da 18 a 28 anni	Maggiori di 28 anni	Età sconosciuta
Stati Uniti	107	5	24	8	70
Turchia	32	8			24
Italia	15	5	10		
Regno Unito	16	6	9	1	
Argentina	10				10
Spagna	7	1			6
Cile	6	2	4		
Olanda	6	1	1		4
Colombia	5				5
Francia	3	1		1	1
Grecia	3	2	1		
Polonia	1		1		

Nei tribunali degli Stati Uniti sono in corso molti più processi che altrove, ma questo non significa necessariamente che gli Stati Uniti abbiano una percentuale maggiore di attivisti informatici in rapporto alla popolazione. L'applicazione della legge negli Stati Uniti ha affrontato il problema a partire dai computer con LOIC, anziché dai server di comando di IRC. Gli utenti di LOIC sono stati arrestati e denunciati ma in altre nazioni, come in Francia, sono stati indagati solo i botmaster di LOIC.

In Gran Bretagna sono stati individuati alcuni membri di spicco associati a LulzSec (ColdBlood, Peter, Ryan, tFlow, Topiary, Nerdo, NikonElite, Kayla ecc.).

Da parte della polizia italiana è nota una sola operazione, che ha identificato il membro dal nome utente di Phre.

In Turchia sono stati effettuati 32 arresti. Pare che gli arrestati avessero partecipato a un'operazione il 10 giugno 2011 contro vari siti governativi turchi[54]. Si opponevano alla creazione di un grande filtro censorio, presentato dal governo come un modo per "proteggere" i giovani del Paese.

Nel febbraio 2012 l'Interpol ha lanciato l'Operazione Unmask che ha portato a una serie di arresti in Spagna e America Latina. Gli arrestati sono sospettati di aver sferrato attacchi contro gli account Facebook e Twitter di personaggi famosi colombiani, contro i siti del governo colombiano (luglio 2011) e la società elettrica cilena Endesa (maggio 2011).

OpCartel

In un video caricato il 6 ottobre 2011, una fazione messicana di Anonymous chiese il rilascio di un suo membro rapito da Los Zetas, un'organizzazione criminale. Il rapimento avrebbe avuto luogo fra il 20 e il 29 agosto, mentre l'attivista stava distribuendo volantini per l'Operazione PaperStorm a Veracruz. A supporto della loro richiesta, i membri di Anonymous annunciarono che, se entro il 5 novembre il loro amico non fosse stato rilasciato, avrebbero rivelato l'identità di giornalisti, poliziotti e tassisti collegati al cartello[55].

I Los Zetas sono notoriamente violenti, non esitano a uccidere chiunque ostacoli loro la strada, compresi poliziotti e giornalisti. In quel periodo, tentarono anche di ridurre al silenzio quegli utenti di Internet che usavano i social network per combatterli. Il 13 settembre i corpi di due di essi furono ritrovati sotto un ponte a Nuevo Laredo, vicino al confine con gli Stati Uniti[56]. Il 24 settembre, nelle vicinanze, fu rinvenuto il corpo mutilato del redattore di uno dei quotidiani cittadini, con un messaggio indicante che l'omicidio era connesso alla sua denuncia del crimine organizzato tramite i social network[57]. Un quarto omicidio fu commesso il 9 novembre.

Dopo l'ultimatum, su Internet circolarono messaggi contraddittori. Alcuni invitavano alla cautela, mentre altri affermavano che l'operazione era stata annullata per paura di rappresaglie. I Los Zetas minacciarono di uccidere 10 persone per ogni nome rivelato. Tuttavia, nonostante la reputazione del cartello, Anonymous annunciò il 3 novembre che la persona rapita era stata rilasciata[58]. Nonostante il progetto di divulgazione fosse stato annullato[59], il portavoce Barrett Brown, uno dei pochi membri a non indossare la maschera, minacciò su YouTube che l'operazione sarebbe continuata[60].

Si trattava di un'edulcorazione oppure Anonymous era riuscito davvero a piegare quei pericolosi criminali? Non è dato sapere.

Anonymous nelle strade

L'attuale simbolo di Anonymous (e di alcuni movimenti Occupy), la maschera di Guy Fawkes, fu visto nelle strade per la prima volta nel 2008 durante una manifestazione contro Scientology. I manifestanti si nascosero il viso per evitare rappresaglie.

Alcuni membri di Anonymous vogliono portare le loro proteste digitali nel mondo reale. Alcune proteste di strada di inizio 2011 erano estensioni di azioni partite online (pro WikiLeaks, per esempio). Tuttavia, questi tentativi hanno ispirato pochissimi dimostranti.

Altri hanno lanciato le operazioni PaperStorm, che consistevano nel distribuire volantini per strada nell'intento di attirare l'attenzione del pubblico. Ma questi appelli alla mobilitazione hanno finora ricevuto poche risposte. Nel febbraio 2012 PaperStorm ha avuto luogo in diversi Paesi (Germania, Spagna e Canada) ma in giornate distinte per mancanza di coordinamento.

Un'altra fazione ha tentato di unirsi agli Indignati e ai membri del movimento Occupy.

L'Operazione BART, che prende il nome dalla ferrovia dei pendolari della Baia di San Francisco, è un buon esempio di questi movimenti congiunti. Nacque dalla decisione dell'azienda di creare interferenze nelle comunicazioni wireless, al fine di disturbare l'organizzazione di manifestazioni da parte di utenti insoddisfatti o di altri. Mentre su Internet avevano luogo i consueti attacchi, 200 persone con la maschera di Guy Fawkes manifestavano in strada.

Il movimento internazionale degli Indignati ha avuto inizio in Spagna nel maggio 2011 e riunisce persone che periodicamente riempiono le strade per protestare pacificamente contro il sistema economico e finanziario delle nazioni industrializzate. Negli Stati Uniti, questo movimento è noto come Movimento Occupy, o The 99%. Come Anonymous, questi movimenti non hanno leader. Desiderano rimanere egualitari e rifiutano qualsiasi tipo di autorità tra le loro file.

Anonymous scende nelle strade

	Strada	Internet
18.12.10	Operazione PaperStorm (sostegno a WikiLeaks)	
20.03.11	Giornata Internazionale di Appoggio a Bradley Manning	Operazione Bradical, DDoS a Quantico
13.08.11	Revival dell'Operazione PaperStorm. La motivazione della protesta (WikiLeaks, arresti di Anonymous ecc.) viene lasciata ai distributori.	
13-15.08.11	Sit-in presso la stazione San Francisco Civic Center della linea ferroviaria Bay Area Rapid Transit (BART)	Operazione BART
17-24.09.11	Day of Rage (Giornata della Collera) (17 settembre)	Day of Vengeance (Giornata della Vendetta) (24 settembre)
2.10.11	Occupy Wall Street	Invadere Wall Street
15.10.11	Protesta globale - Occupare il Mondo	
26.10.11	Occupy Oakland	OpUprise

Negli Stati Uniti, Occupy Wall Street è stato avviato da Adbusters, una rete di attivisti anticapitalisti con lo slogan "L'unica cosa che abbiamo in comune è che Siamo il 99% che non tollererà più a lungo l'avidità e la corruzione dell'1%".

Fonte: occupywallst.org

Il 15 ottobre 2011 ebbe luogo il primo raduno di Anonymous e del gruppo The 99%. Diversamente dalla fazione AntiSec, responsabile spesso di azioni controverse, questi attivisti volevano unirsi a chiunque fosse spinto da motivazioni politiche. Volevano inoltre scrollarsi di dosso l'immagine di pirati o disturbatori informatici, che secondo loro poteva metterli in cattiva luce con i media.

Alla luce delle leggi rafforzanti la lotta contro la pirateria (SINDE in Spagna, ACTA, SOPA e PIPA negli Stati Uniti, HADOPI e LOPPSI in Francia, C-30 in Canada ecc.), Anonymous ha fatto diverse volte appello ai suoi sostenitori per mettersi in marcia. L'11 e il 25 febbraio 2012, hanno riempito le strade in molte delle principali città europee.

Luoghi delle proteste tenutesi l'11 febbraio 2012

Manipolazione e pluralismo

Dato che Anonymous non dispone di un leader o di una qualsiasi fonte ufficiale di comunicazioni, chiunque può proporre un'operazione come proposta di gruppo. Diverse volte sono state annunciate azioni, solo per essere rapidamente smentite come autentiche. A seconda delle circostanze, alcuni hanno etichettato questi appelli all'azione come pessimi scherzi, manipolazioni, disinformazioni o divergenze interne. Tali ostacoli sono stati seguiti da informazioni contraddittorie nei media. Alcuni avrebbero poi rimproverato ad Anonymous la scelta indiscriminata di azioni, mentre altri avrebbero pubblicato una negazione non verificata.

Un esempio classico è quanto iniziò con un video pubblicato su YouTube il 9 agosto 2011, annunciante la fine di Facebook per il 5 novembre (anniversario della sconfitta di Guy Fawkes). Il social network era accusato di non rispettare la riservatezza degli utenti. Nonostante la rapidità con cui il video fu negato da altri membri di Anonymous, la voce non smise di circolare fino al 6 novembre, quando fu chiaro che tale evento non si sarebbe mai verificato.

Per contro, comunicazioni contraddittorie a dicembre affermavano tutto e il contrario di tutto relativamente al caso della compromissione di Stratfor, nella quale i dati di migliaia di account (compreso quello dell'ex segretario di stato americano Henry Kissinger) furono sottratti per eseguire bonifici a favore di organizzazioni no profit[61]. Nel febbraio 2012, mentre WikiLeaks cominciava a pubblicare la corrispondenza rubata in quell'occasione, divenne chiaro che Anonymous era coinvolto in questo atto di pirateria. L'operazione potrebbe addirittura essere stata manipolata dall'FBI[62].

Questa storia suggerisce di rimanere scettici di fronte alle minacce di azioni online, come quelle nei confronti della rete elettrica statunitense[63] o dei root server DNS (febbraio 2012). Nel secondo caso, l'idea di fermare temporaneamente il web fu proposta in connessione con l'Operazione Global Blackout, avviata nel novembre 2011 come massiccia campagna di protesta contro la legge SOPA. Annunciato per il 31 marzo e consistente in un attacco DDoS con amplificazione riflettente dei DNS, l'attacco fu zeppo di ordini e contrordini.

Negazione dell'Operazione Global Blackout da parte di due canali informativi di Anonymous

Operazione Megaupload

Il 19 gennaio 2012 durante la discussione sull'Accordo Commerciale Anticontraffazione (ACTA), la chiusura di Megaupload (sito sospettato di ospitare software piratato), provocò "il più grande attacco DDoS nella storia di Internet" secondo Anonymous[64]. Molti siti web caddero vittime degli attacchi DDoS. L'operazione, alla quale pare abbiano preso parte 5.000 persone, prese di mira molti siti web: U.S. Department of Justice (doj.gov), Universal Music (universalmusic.com), Motion Picture Association of America (mpaa.org), Recording Industry Association of America (riaa.com), U.S. Copyright Office (copyright.gov), Broadcast Music Incorporated (bmi.com) e HADOPI (hadopi.fr).

Ad alcuni sostenitori del movimento Anonymous fu chiesto perché appoggiavano il capo di Megaupload Kim Dotcom, considerato da molti più come un avido criminale cibernetico che come un fautore di un Internet aperto e libero. Intervistato dal quotidiano francese *Le Nouvel Observateur*, Vador-M, un membro francese di Anonymous, riassunse così il pensiero dei suoi colleghi: "Con la chiusura di Megaupload siamo stati privati di una libertà. Dovevamo agire. La motivazione principale non è la difesa di Megaupload, ma la lotta contro la censura. Non stiamo cercando di difendere Kim Dotcom, che è sospettato di aver messo in piedi una mafia, ma Megaupload era più di un'azienda, era una vera e propria istituzione".

Comunicazioni

Social network e siti web

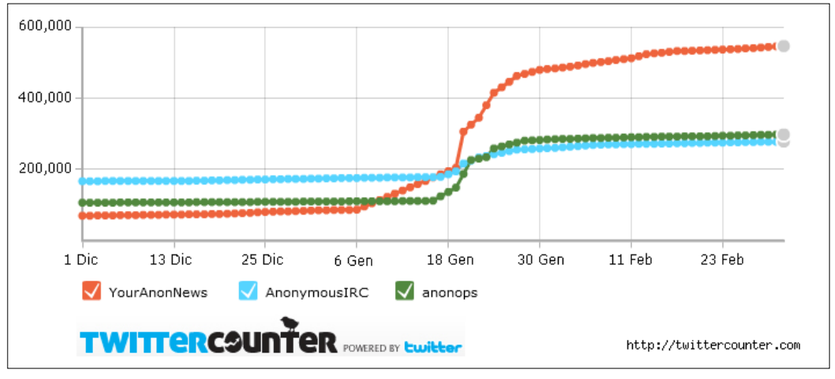
Molti siti web e account di social networking che affermano di parlare per conto di Anonymous sembrano interferire con il movimento e sicuramente creano confusione. Come specificato sopra, alcuni inviti ad agire vengono immediatamente contraddetti da altri.

In particolare, gli account Twitter di Anonymous attraggono molti follower curiosi, specialisti della sicurezza e, senza dubbio, investigatori pubblici o privati. Nel corso dell'estate del 2011, l'account Twitter di LulzSec (The Lulz Boat) contava oltre 350.000 follower. Quando è stato disattivato nel luglio 2011, è subentrato l'account appartenente al suo ex leader, Sabu, (@anonymouSabu, 43.000 follower all'1 marzo 2012). Eppure, l'account di Sabu rappresenta solo una fazione del gruppo.

Cinque account Twitter principali offrono molte delle novità di Anonymous:

- @AnonOps: Combattiamo per la libertà di Internet
- @AnonymousIRC: Siamo l'ambasciata di #AntiSec
- @YourAnonNews
- @AnonymousPress
- @Anon_Central: Operazioni di Anonymous

Questi account popolari hanno ricevuto un afflusso di follower quando Megaupload è stato chiuso.



Statistiche di Twitter nel 2011–2012 per alcuni account Anonymous

I principali siti web per le notizie di Anonymous:

- anonops.blogspot.com
- youranonnews.tumblr.com
- anoncentral.tumblr.com
- anonnews.org

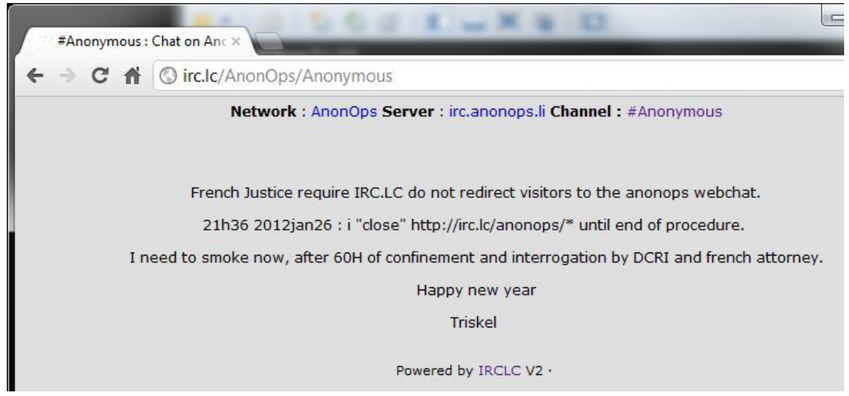
IRC

Internet Relay Chat (IRC) è il mezzo di comunicazione principale tra i sostenitori e i membri più attivi del gruppo. IRC è un protocollo per le chat di testo che utilizza canali dedicati per discussioni di gruppo. Il protocollo IRC autorizza il rilevamento del software LOIC per gli attacchi DDoS.

La rete più attiva è AnonOps. Il collegamento può essere effettuato da una chat web o in modo più sicuro da un client IRC (come XChat o mIRC).

Una chat web è un'applicazione web (che utilizza HTTP) che permette a un utente di parlare su canali IRC senza un software client. Il browser web visualizza messaggi di testo su una pagina web che deve essere periodicamente ricaricata.

Un giudice francese ha ordinato a un sostenitore di Anonymous di smettere di offrire funzionalità di chat web a utenti Internet che cercavano di raggiungere i canali di AnonOps. Quel sito è ora chiuso ma ne sono disponibili molti altri. Per esempio, webchat.anonops.com, webchat.power2all.com e search.mibbit.com permettono a molti simpatizzanti di chattare con AnonOps tramite IRC.



L'annuncio della fine di un sito reindirizza al server IRC di AnonOps

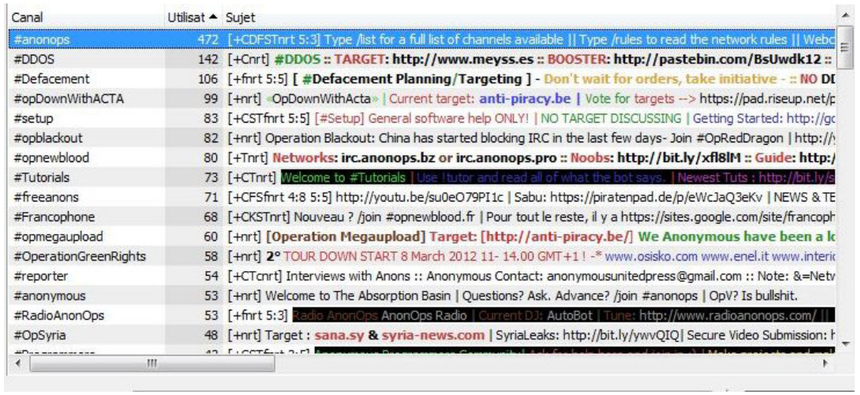
Quando si utilizza un client IRC, AnonOps è accessibile attraverso i seguenti indirizzi:

- irc.anonops.li (ora inaccessibile)
- irc.anonops.bz
- irc.anonops.pro
- irc.anonops.su

Sui forum di discussione, l'URL di collegamento è spesso accompagnato da un numero di porta (per esempio irc.anonops.li/6697) che è diverso dalla porta IRC di default (6667). Quest'opzione invita gli utenti a utilizzare una porta SSL[65] per proteggere il collegamento con funzioni di cifratura (purché il client supporti il protocollo SSL).

All'interno della rete AnonOps, ci sono molti canali dedicati alle attività, discussioni e informazioni tecniche attuali. Alcuni partecipanti ricoprono un ruolo fondamentale in diversi canali, mentre altri sono coinvolti in solo uno o due chat IRC alla volta. Gli operatori ("ops") detengono una semi-posizione di autorità. Sono responsabili di mantenere l'ordine. Possono respingere o interdire persone indesiderate. Nel caso di AnonOps, è proibito collegarsi e scollegarsi continuamente, per prendere di mira i media o esaltare la violenza[66].

Alcuni operatori sono presenti solo per interagire sull'infrastruttura, mentre altri partecipano nella maggior parte delle operazioni politiche condotte da Anonymous. Anche se non sono gli unici a stabilire attivamente piani o operazioni, l'opinione degli operatori viene sempre ascoltata.



I principali canali e argomenti di AnonOps (acquisiti l'8 marzo 2012)

Anonimato

Per non essere identificati, molti sostenitori di Anonymous utilizzano strumenti dedicati. Uno è TOR (The Onion Router). Questo software di routing utilizza un proxy per far passare il traffico Internet attraverso diversi nodi, rendendo difficile identificare l'utente e recuperare il suo indirizzo IP. Ricordiamo che lo scopo di TOR è fornire anonimato al traffico, non cifratura end-to-end.

Tuttavia, TOR non è facilmente compatibile con la rete IRC di AnonOps. Chiunque desideri utilizzarlo per collegarsi deve prima impostare una password e fornire un hash di tale password a un operatore di canale #help[67]. Quindi, è possibile collegarsi utilizzando un URL (con il dominio che termina in .onion) specifico per la rete TOR[68]. Altri server erano collegati a Anonymous e volti a far sì che altri canali accettino collegamenti TOR. Questo è il caso di AnonNews (irc.cryto.net), per esempio.

Considerato da Anonymous come un "Internet all'interno di Internet"[69], I2P (Invisible Internet Project) è famoso tra gli attivisti informatici. Questo strumento è un protocollo di scambio anonimo con cifratura end-to-end che può essere utilizzato da molte applicazioni trovate su Internet "normale". I2P supporta, tra le altre cose, il browsing web su siti specifici (domini con .i2p), scambi di file tra utenti di I2P e chat IRC anonime. Poiché non possono rimanere anonimi sul resto di Internet (utilizzando HTTP o HTTPS), molti utenti che desiderano rimanere sconosciuti installano I2P e TOR sui loro computer creando profili multipli per il browser Firefox.

Esistono altre soluzioni per gli scambi anonimi e, come prima, il loro uso non è limitato a Anonymous. Con Commotion Wireless, qualsiasi semplice computer con una scheda WiFi può essere parte della rete e accedere a Internet tramite una terza parte. Questi nodi possono anche diventare un collegamento per un altro computer per accedere a Internet[70]. Con Freenet[71], una rete anonima che è distribuita, cifrata e (semi) privata, gli utenti possono collegarsi a Freesites, discutere all'interno di newsgroup, scambiare messaggi utilizzando Thunderbird e scambiare e condividere file. Freenet si comporta come una "Darknet", una rete in cui gli utenti possono limitare l'accesso ad amici noti.

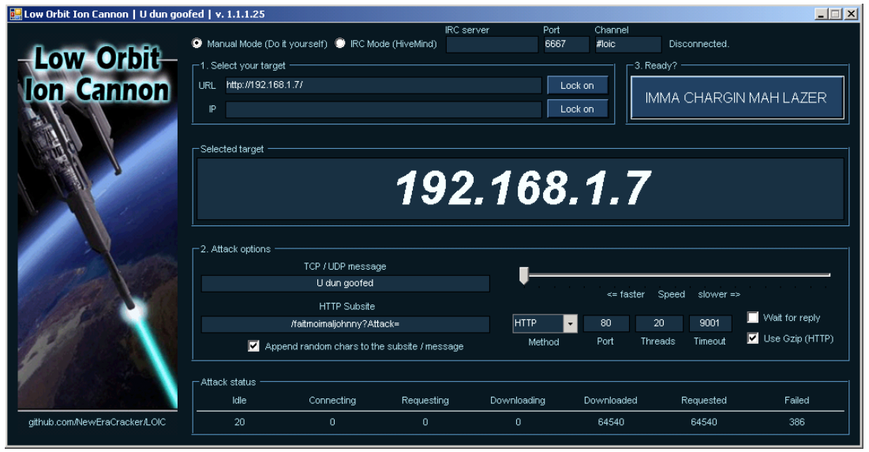
Strumenti DDoS

Per perpetrare attacchi DDoS, i membri di Anonymous utilizzano vari strumenti Internet. Il più noto è LOIC, che è stato sviluppato per testare le reti. Semplice da utilizzare, permette a persone non tecniche di partecipare agli attacchi dai loro computer.

Dalle sue prime versioni, LOIC offriva tre tipologie di attacchi: HTTP flood, TCP flood e UDP flood. Questi possono essere lanciati dalla stazione di lavoro dell'utente semplicemente entrando nel sito da attaccare, selezionando la forza dell'attacco (bassa, media e elevata) e facendo clic su "Fuoco!".

Durante Operazione Payback (Operazione Resa dei Conti, Dicembre 2010), sono apparse versioni modificate di LOIC (Versione 1.1.1.3, autore NewEraCracker) con il supporto per IRC. Questi rilasci possono associare LOIC a un canale, impostarlo per farlo funzionare automaticamente e aspettare istruzioni. In effetti, queste sono le prime botnet volontarie. Il programma potrebbe essere lanciato in modalità stealth, senza una finestra visibile e senza apparire nella barra dei task. Ciò rende possibile lanciare segretamente istanze da computer pubblici con accesso aperto.

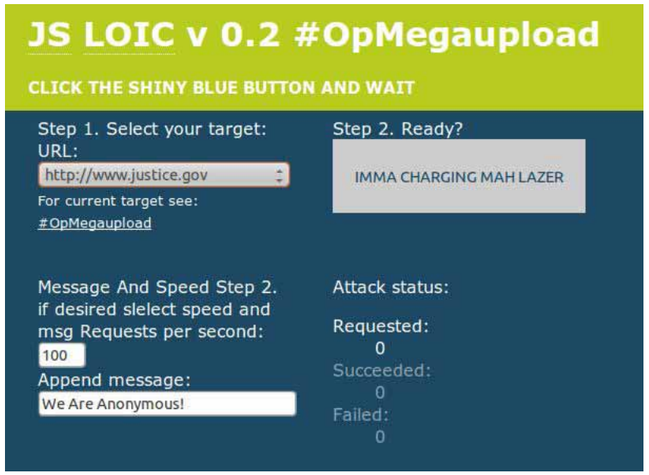
Un flood è un'azione, solitamente dolosa, che consiste nell'invio di una grande quantità di dati non necessari a una rete per renderla inutilizzabile. Con il software LOIC, gli hacker possono attaccare "inondando" un server di pacchetti TCP, pacchetti UDP o richieste HTTP.



LOIC - Versione 1.1.1.25[72]

Altre versioni di LOIC sono apparse a partire da Operazione Payback. JS LOIC, o LOIC Mobile, permette ai principianti di partecipare a un attacco semplicemente collegandosi a una pagina web dal loro browser, che lasciano aperto nel momento designato per l'attacco. Il codice JavaScript quindi apre pagine web e lancia una serie di richieste HTTP per saturare le risorse del server. È così che i membri di Anonymous hanno attaccato il sito web del Vaticano nell'agosto 2011 durante la Giornata Mondiale della Gioventù (Operazione Pharisee)[73].

Codice simile che chiedeva ai partecipanti di selezionare un obiettivo da un elenco predefinito apparve a seguito della chiusura di Megaupload.



L'interfaccia di JS LOIC[74]

Una versione di LOIC è stata recentemente sviluppata per Android. LOIC para Android by Alfred viene attualmente utilizzato in America Latina[75].

HOIC è un altro strumento utilizzato per creare attacchi DDoS che può eseguire solo un attacco HTTP flood, ma dispone di Booster Scripts[76], ovvero file di configurazione che possono aggiungere più richieste e nasconderle meglio all'interno del traffico regolare.

Anonymous qualche volta viene sospettato di utilizzare altri strumenti di attacco, come Apache Killer (scritto da Kingcope), Slowloris (scritto da RSnake), r-u-dead-yet e ZapAttack (su MacOS X). LOIC e i suoi discendenti (JS LOIC, WEBLOIC) sembrano essere i più utilizzati. Alcuni rapporti dei media citavano il progetto RefRef[77], ma questo sembra essere stato solo una truffa.

Dissidenti informatici

Il secondo ramo dell'hacktivism include dissidenti informatici o occupanti informatici. Sebbene Anonymous protegga strenuamente la libertà di parola e il libero scambio su Internet, gli occupanti informatici, che sono ancorati al mondo reale, vedono Internet come uno strumento per aiutarli nella loro lotta per ottenere una società più libera. Nelle nazioni democratiche, le loro azioni sono sottovalutate perché sono spesso al limite della legalità. Questa lotta è generalmente bonaria ed è spesso confinata ad un uso attivista del social networking, che diventa un mezzo di comunicazione e propaganda. Quando questa lotta politica è rivolta contro un regime totalitarista o estremista, definiamo spesso questi attivisti come dissidenti informatici. Quando agiscono, non nascondono la loro identità per divertimento o motivi ideologici, piuttosto per evitare una reazione violenta che potrebbe essere utilizzata contro di loro qualora venissero riconosciuti. Sebbene separiamo dissidenti e occupanti informatici dal movimento di Anonymous, il confine tra questi due gruppi è alcune volte poco chiaro. Alcuni dissidenti informatici firmano le loro azioni prendendosi la responsabilità come Anonymous, mentre i membri di Anonymous spesso lanciano operazioni uniche per supportare i movimenti Occupy.

Telecomix

L'attenzione posta all'insurrezione araba ha creato una coscienza politica più forte in alcuni attivisti informatici, come per esempio il gruppo Telecomix, creato nell'aprile del 2009 in Svezia. I suoi membri operano senza un leader o una gerarchia. Si dice operino in base al concetto di "do-ocracy" ovvero una struttura organizzativa in cui ciascuno si sceglie il proprio ruolo e i propri compiti e li esegue. "È sufficiente avere delle idee; poi gli altri possono unirsi e aiutare. Nessuno ha una visione globale di tutti i progetti", spiegano fo0 e Menwe[78]. Secondo Okhin, un "critto-anarchico" e uno dei rappresentanti di Telecomix, il gruppo conta dalle 250 alle 300 persone. "Viviamo nella rete. Viviamo in base e per la rete. Se viene attaccata, la difenderemo"[79].

Do-ocracy, una contrazione di "to do" (fare) e "democracy" (democrazia), può tradursi in democrazia attraverso l'azione. Si tratta di una struttura flessibile in cui i singoli si auto-assegnano dei compiti e li portano a termine, assumendosene la piena responsabilità.

Nel gennaio 2011, Telecomix ha ripristinato parzialmente l'accesso al web in Egitto, dopo che il governo di Hosni Mubarak aveva bloccato i collegamenti a Internet ai suoi 20 milioni di utenti. Si dice che Telecomix abbia impostato linee telefoniche collegandole a modem a 56K e poi abbia trasmesso le informazioni su Facebook e Twitter[80]. Il gruppo ha replicato l'operazione in Libia nel febbraio 2011.


TELECOMIX INTERNATIONAL

للتوزيع فوراً
FOR IMMEDIATE DISTRIBUTION

نحن تيليكوميكي نأتيكم بسلام. نحن نحاول مساعدتكم بتقديم أي من وسائل الاتصال المتوفرة. يرجى توزيع هذه المعلومات لكل الراغبين بالحصول على امكانية اتصال مجاني.
This is Telecomix. We come in peace. We are trying to help with providing every means of communications available. Please distribute this information to all those who are in need of free communication.

معلومات للوصول إلى الإنترنت
INTERNET DIAL-IN INFORMATION

استخدم المعلومات الموجودة أدناه مع مودم 56 كيلوبايت

Un estratto del messaggio che Telecomix ha inviato al popolo egiziano

Quando la guerra civile si è intensificata in Siria, gli attivisti di Telecomix hanno cercato di supportare anche questi ribelli, a costo di ricevere minacce. L'operazione ha avuto inizio nell'agosto 2011 con un messaggio di massa inviato agli utenti Internet siriani che spiegava come scavalcare il controllo online nel paese. Nella notte tra il 4 e il 5 settembre, un'ampia porzione di Internet in Siria fu scavalcata da un attacco di pirateria informatica simultaneo da parte di tutti i router TPLink[81]. Gli utenti di Internet potevano accedere solo a una pagina, che forniva un kit di sopravvivenza per l'utilizzo da parte degli avversari di Bashar al-Assad. "La tua attività Internet è sotto controllo. Ecco gli strumenti per evitare tale controllo", veniva spiegato in una parte della pagina, in Inglese e Arabo. Il kit conteneva estensioni di sicurezza (plug-in) per Firefox, TOR, software sicuro per la messaggistica immediata (hushmail), un servizio VOIP in concorrenza con Skype (Mumble), un sistema di cifratura delle conversazioni (Pidgin con il plug-in Off-The-Record), un client IRC (Xchat) e un link alla chatroom Telecomix[82]. Questo pacchetto da 60 MB includeva anche linee guida di sicurezza di base per evitare di rivelare informazioni personali su Internet. Nel marzo 2012, le operazioni di supporto continuavano.

Messaggio alla popolazione siriana (5 settembre 2011)

Telecomix opera come se fornisse assistenza web internazionale alle persone, agendo di sua propria iniziativa, nel caso Internet venga oscurato o ne venga limitato l'accesso. Gli estimatori di Telecomix fanno notare che "non agiscono tramite attacchi DDoS e non effettuano atti di pirateria informatica"[83]. A Ginevra, volontari di Telecomix offrono corsi di formazione sulla crittografia all'organizzazione no-profit Reporter senza frontiere. In una nazione democratica come la Francia, le azioni di Telecomix possono in alcuni casi essere considerate oltre i limiti della legalità, come nel caso in cui avevano effettuato il mirroring del sito "Copwatch" che le autorità francesi avevano deciso di chiudere.

Altri successi

Sebbene Anonymous sia apparso solo nell'ultimo trimestre del 2010, le proteste virtuali e gli attacchi con motivazioni politiche sono moltiplicati con l'inizio di quest'anno. Alcuni di questi atti possono essere paragonati alle azioni di organizzazioni come Greenpeace, che spesso sfida le leggi nazionali e internazionali per sensibilizzare l'opinione pubblica. Nel mondo Internet, i seguenti esempi, sebbene illegali, hanno attirato simpatie e sono stati ritenuti giustificati da alcune persone.

- Gennaio 2010. Un hacker in Turchia ha modificato il sistema informatico utilizzato per richiamare i fedeli alla preghiera. I messaggi sono stati trasmessi a 170 moschee nella nazione. I messaggi originali sono stati sostituiti da canzoni di un artista morto nel 1996 noto per il suo ruolo pioneristico per il riconoscimento dell'omosessualità in Turchia.
- Febbraio: In Lettonia, il gruppo 4ATA (Fourth Awakening People's Army) ha annunciato di essersi impossessato di milioni di dichiarazioni dei redditi e ha poi divulgato alcune delle informazioni per far luce sulla corruzione nel paese. Il principale sospettato, un ricercatore nel settore dell'intelligenza artificiale dell'Università di Riga, è stato identificato a maggio.
- In aprile, un professore dell'Università della California di San Diego ha lanciato una protesta virtuale (un appello a partecipare a un attacco DDoS) contro il sito web della sua università per contribuire a creare più opportunità per un numero maggiore di studenti svantaggiati[84].
- Il 14 luglio, un gruppo di attivisti in Francia ha falsificato il sito web del Ministero degli Affari Esteri per mostrare un portavoce fasullo che annunciava sostegno per aiutare Haiti.
- Durante l'azione "Climategate II", il 24 novembre 2011 gli hacker hanno mostrato oltre 5.000 email che sembravano confermare che alcuni scienziati avevano una missione politica - non per la ricerca della verità - in tema di riscaldamento globale[85].
- Il 1° dicembre, WikiLeaks rivelò gli Spy Files, circa 1.100 documenti di produttori sul controllo e l'intercettazione di telecomunicazioni[86]. Queste rivelazioni dimostrarono che esisteva un mercato redditizio per lo spionaggio e il controllo cibernetico a livello nazionale. Gli avversari di tali pratiche sostenevano che i prodotti, principalmente sviluppati nelle democrazie occidentali, erano venduti ovunque, inclusi dittature ancora esistenti o minate dalla Primavera Araba.

L'home page di Spy Files, che evidenzia la Francia

- Mentre le manifestazioni contro l'aumento dei prezzi del petrolio scuotevano la Nigeria, un sito web appartenente all'esercito nazionale ha subito un attacco di defacing il 16 gennaio 2012 da parte di attivisti informatici. Il messaggio lasciato sul sito era il seguente "Lasciate IN PACE i contestatori innocenti"[87].

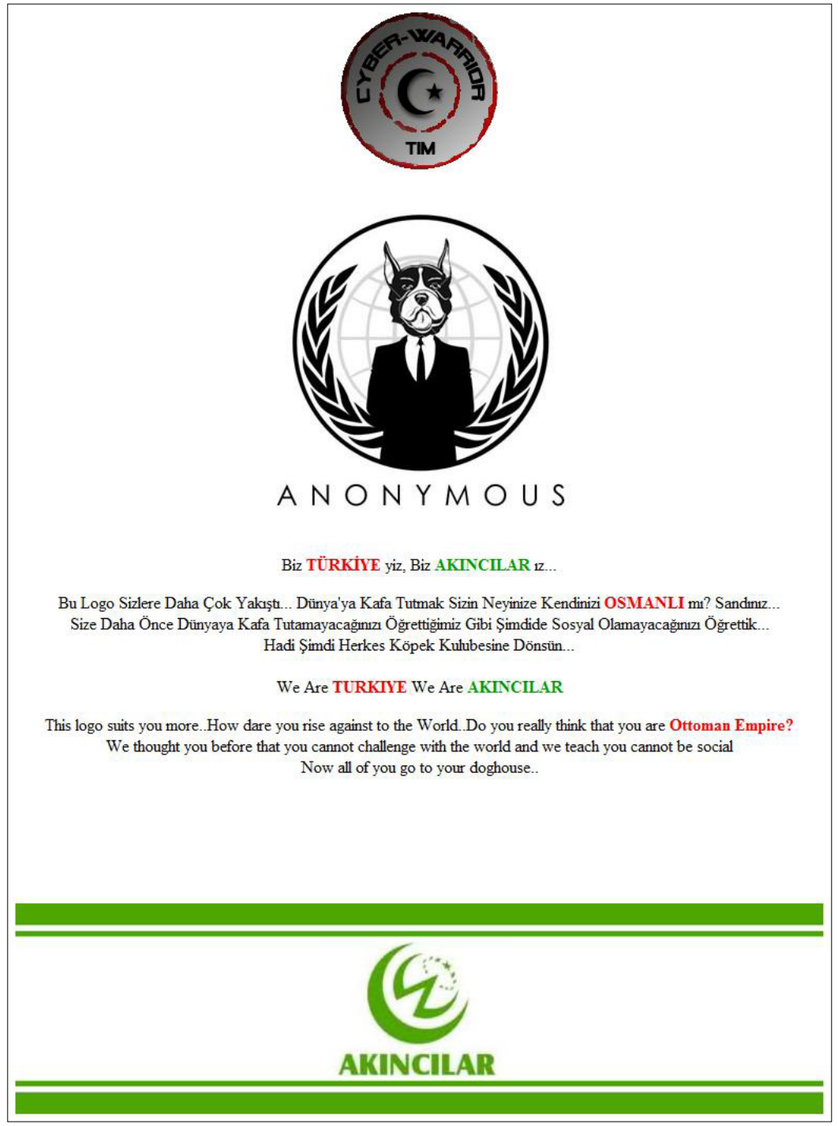
Patrioti e combattenti informatici

Mentre occupanti e dissidenti cibernetici legati a Anonymous difendono la libertà di parola e scendono in campo per difendere le minoranze e coloro che vogliono ottenere la propria libertà, altri gruppi - spesso dittatoriali e religiosi - che sembrano vicini ai loro governi reagiscono a ciò che considerano un'interferenza. A differenza di Anonymous, questi "patrioti" spesso operano come fondamentalisti mentre anche loro si comportano come attivisti informatici.

Che si auto-definiscano nazionalisti russi, patrioti cinesi, indiani o pakistani o difensori di Israele e della Palestina, tutti questi piccoli gruppi eseguono azioni di guerriglia online contro chiunque considerano essere il nemico. Raggruppati in (pseudo) eserciti informatici, creano botnet volontarie o effettuano il defacing e distruggono i messaggi o le azioni di dissidenti e avversari.

Reazione violenta contro Anonymous

Nel giugno 2011, Anonymous ha lanciato Operazione Turkey per supportare i giovani che protestavano contro la censura di Internet. Per alcuni giorni, non è stato possibile accedere ai siti del governo a seguito di attacchi DDoS tramite botnet LOIC lanciati al di fuori del paese. Il 16 luglio, il gruppo Akincilar ha risposto effettuando il defacing dell'home page di AnonPlus, un nuovo sito che alcuni membri di Anonymous avevano dovuto creare dopo essere stati banditi da Google+.



Il gruppo Akincilar attacca Anonymous

I sostenitori di Bashar al-Assad si sono irritati per le azioni a sostegno della popolazione siriana. Il 9 agosto, come ritorsione per il defacing da parte di Anonymous del sito web del Ministero della Difesa della Siria, il "Syrian Cyber-Army" ha violato il sito AnonPlus tramite un attacco di avvelenamento cache DNS. Al posto della pagina consueta, gli utenti di Internet hanno visualizzato immagini di soldati morti con un messaggio che implicava che sostenendo gli oppositori del regime di Bashar al-Assad, Anonymous sosteneva la Fratellanza Musulmana[88].

TeaMp0isoN

TeaMp0isoN è divenuto noto inizialmente come nemico spietato di LulzSec e Anonymous, ma il gruppo ha in seguito annunciato l'unione con AntiSec. Dal 2010, i tre membri principali del gruppo, incluso il suo leader TriCk, hanno chiarito le loro opinioni politiche e religiose. Hanno spesso firmato i loro attacchi congiuntamente con la Mujahideen Hacking Unit quando difendevano la causa palestinese. Durante gli attacchi contro siti indiani, si dichiaravano membri dell'Esercito Informatico Pakistano o di ZCompany Hacking Crew. Sulla base dei messaggi rilasciati durante questi attacchi, li classifichiamo come esercitici informatici.

I successi del gruppo:

- Giugno 2011: In segno di rappresaglia contro l'intervento militare in Iraq, TeaMp0isoN ha pubblicato la rubrica e alcune informazioni private relative all'ex primo ministro inglese Tony Blair.
- Agosto: Quando Research in Motion (RIM), produttore dei dispositivi BlackBerry, ha annunciato la sua collaborazione con la polizia per arginare i disordini che scuotevano la Gran Bretagna, TeaMp0ison ha effettuato il defacing del blog dell'azienda e minacciato di pubblicare dati riservati dei dipendenti se l'azienda avesse insistito a rivelare informazioni sugli utenti dei suoi telefoni. TriCk ha scritto, "Siamo tutti dalla parte dei rivoltosi coinvolti negli attacchi contro la polizia e il governo"[89].
- Agosto: Il gruppo ha violato un forum di discussione della NASA rivelando dettagli dell'account dell'amministratore.
- Novembre: TeaMp0isoN pubblica informazioni per l'accesso a migliaia di account personali come parte del Programma di Sviluppo delle Nazioni Unite.

Nel Novembre 2011, TeaMp0isoN annunciò un'alleanza con Anonymous e di aver creato p0isAnon, che lancio l'Operazione Robin Hood in segno di solidarietà con Occupy Wall Street[90]. In un video, un portavoce affermò che "Operazione Robin Hood si impossesserà delle carte di credito e effettuerà donazioni al restante 99% (ovvero i poveri) e a vari enti di beneficenza in tutto il mondo". Vennero diffuse su Internet schermate dei pagamenti a organizzazioni come CARE, la Croce Rossa Americana e Save the Children dai conti bancari di varie personalità. L'informazione presumibilmente derivava dalla violazione del sito web Stratfor.

Quest'operazione ha danneggiato l'immagine di Anonymous ed è stata anche un duro colpo per le organizzazioni non governative. Sostanzialmente, i pagamenti fraudolenti dovevano essere rimborsati per evitare di dover pagare spese ulteriori.

TriCk è stato arrestato nel Regno Unito nell'aprile 2012. Questo diciassettenne musulmano rivendicava di essere il fautore della divulgazione di conversazioni telefoniche estremamente sensibili dalla linea diretta antiterrorismo di Scotland Yard[91].

Altri successi

Nonostante siano numerose, le azioni da parte degli eserciti informatici hanno un impatto relativamente contenuto. I media le segnalano solo quando qualcuno attacca un sito istituzionale o un sito che appartiene a un partito politico o a un politico.

L'arma preferita dagli eserciti informatici è la tecnica del defacing. Ogni giorno, gli hacker la utilizzano su migliaia (o più) di siti. In circa il 10% dei casi, è opera di attivisti informatici che apparentemente sono legati all'ideologia dei combattenti informatici.

Statische sui siti colpiti da defacing, da zone-h

Motivo dell'attacco	Numero di siti
Beh…solo per divertimento!	829.975
Voglio essere il miglior "deturpatore"	289.630
Non disponibile	94.017
Patriottismo	58.970
Motivazioni politiche	57.083
Vendetta contro quel sito web	45.093
Come sfida	44.457

I dati di zone-h citano i motivi principali rivendicati dagli hacker per gli attacchi contro siti web nel 2010. Oltre 800.000 azioni sono state eseguite "solo per divertimento"[92].

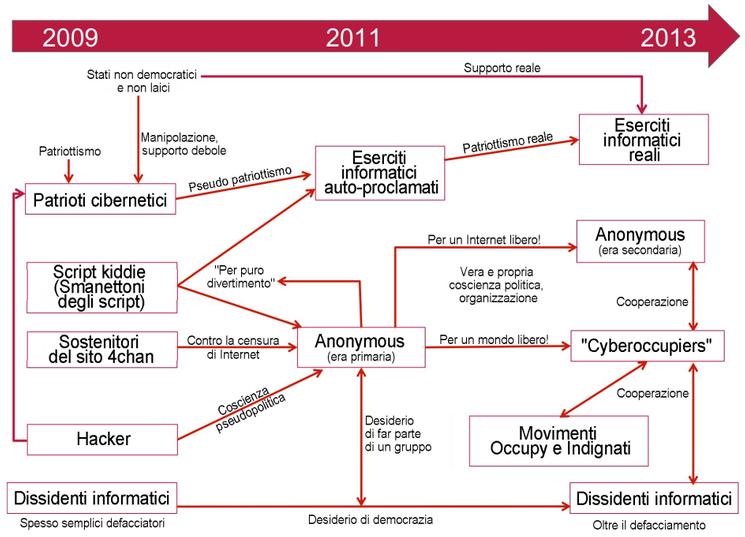
Esempi di eserciti informatici in azione:

- Nel corso del 2010, hacker indiani e pakistani si sono colpiti l'uno con l'altro con numerosi attacchi informatici. L'Esercito informatico Indiano e l'Esercito Informatico Pakistano hanno rivendicato gli attacchi.
- Nell'aprile del 2010, diversi hacker rumeni hanno effettuato il defacing di siti web francesi e inglesi. Protestavano contro il fatto che alcuni membri dei media non fanno distinzione tra rumeni e zingari. In Francia, uno sketch di Jonathan Lambert ha particolarmente irritato i contestatori.
- Nel 2010, sostenitori del gruppo palestinese Hamas hanno distribuito un video animato con il padre del soldato israeliano Gilad Shalit. Immediatamente dopo, è stato effettuato il defacing di siti che supportavano la causa palestinese. A maggio, gli account Facebook di molti israeliani sono stati violati in risposta al blocco della flottiglia della pace in viaggio verso Gaza.
- Nelle Filippine, siti web hanno subito attacchi di defacing il 27 agosto. Gli esecutori hanno richiesto un'indagine per gli otto turisti di Hong Kong uccisi (il 23 agosto) durante un assalto a Manila su un bus che ha portato al rapimento di 15 ostaggi.
- A novembre, per ritorsione contro la distribuzione di video che mostravano la tortura di papuani attribuita all'esercito indonesiano, molti siti web non governativi, incluso quello di Survival International, sono stati colpiti dagli attacchi informatici.
- Nel febbraio 2011, patrioti turchi hanno lanciato una campagna per protestare contro il processo di riconoscimento del genocidio armeno, per un totale di 6.000 siti colpiti. A dicembre, in Francia la mossa del governo per dichiarare illegale il ripudio dei genogidi ha suscitato la collera degli attivisti informatici turchi. Tra i siti colpiti quello di Valérie Boyer, membro del parlamento che aveva dato avvio al testo, e Patrick Devedjian, un membro armeno del parlamento.
- Durante il primo fine settimana di marzo, circa 40 siti web del governo coreano sono stati colpiti con attacchi DDoS.
- In marzo, si affermò che un sito informativo che sosteneva l'opposizione Thai era stato infiltrato. L'autore dell'attacco presumibilmente aveva presentato articoli fasulli volti a screditare i media.

Conclusioni

Fare ordine tra Anonymous, occupanti ed eserciti informatici può rendere complicato comprendere i protagonisti e le loro motivazioni. Come alcuni attivisti entrano illegalmente in impianti nucleari e altre proprietà private, gli attivisti informatici entrano in aree digitali private. Bloccate dalla loro mancanza di struttura, le operazioni di alcuni attivisti rimangono confinate a scherzi di cattivo gusto (lulz), mentre altre possono essere collegate a attività simili alla mafia (come il furto di dati bancari). Il valore di queste violazioni è spesso discutibile e difficile da comprendere. Quest'apparente casualità di intenti suggerisce che alcune persone stiano forse facendo il doppio gioco, nascondendo attività illegali sotto la copertura dell'attivismo informatico politico. Gli hacker etici fanno notare che la mancanza di etica in molte operazioni suggerisce che alcuni attivisti informatici possono essere controllati dai servizi segreti governativi.

L'hacktivism, legato o meno a Anonymous, è oggigiorno un fenomeno di rilievo. Come i criminali dieci anni fa hanno compreso che Internet poteva diventare uno dei loro campi d'azione preferiti, molti utenti Internet hanno scoperto nel 2010 che il web potrebbe diventare una piattaforma di protesta collettiva. Incoraggiati da Anonymous, che ha afferrato questo concetto qualche tempo fa, gli attivisti informatici sono stati molto attivi tra il 2010 e il 2011. Ora diamo un'occhiata alle loro possibili organizzazioni nei prossimi due anni.



Possibile evoluzione del movimento degli attivisti informatici

Dopo aver giocato a fare i vandali e i contestatori chiassosi, gli attivisti informatici con una reale coscienza politica hanno collaborato per evolvere e organizzarsi. Generati dal movimento Anonymous che conosciamo oggi, i primi attivisti informatici sembravano trasformarsi lentamente, nel momento in cui si aggiungevano reclute con nuove capacità:

- Artisti grafici per comunicazioni migliori
- Giornalisti volontari per iniziative di giornalismo partecipativo simile a Wikipedia (giornalismo collaborativo)
- Scienziati informatici esperti per eseguire operazioni più sofisticate e danneggiare maggiormente le vittime predestinate
- Strateghi esperti per trovare altri modi di agire e riunire attivisti e attivisti informatici
- Avvocati per istituire il diritto di manifestare online (come la legalizzazione di alcune forme di attacchi DDoS)

Per noi del settore della sicurezza online, quest'ultimo punto può essere sorprendente. Alcuni sostenitori dell'hacktivism possono essere gli avversari della globalizzazione digitale di domani; in realtà argomentano in favore della legalizzazione di un attacco DDoS ispirato all'attivismo. Nel diagramma precedente, queste persone rappresentano la seconda era di Anonymous. Una fonte loro vicina ha confermato a McAfee Labs che ritengono il defacing di un sito web analogo al mostrare una bandiera e che considerano il lancio di un attacco DDoS simile a un sit-in che blocca l'ingresso a un edificio. Come alcune persone richiedono un permesso per marciare e protestare, la seconda generazione di Anonymous immagina di specificare le date, gli obiettivi e la durata di un blocco DDoS.

Se gli attivisti informatici restano defocalizzati e continuano ad accettare chiunque dia il consenso per agire per loro conto, potremmo trovarci sull'orlo di una guerra civile digitale. L'intero movimento di attivisti informatici può cadere vittima di un aumento della criminalizzazione, oltre che di governi che temono che le loro attività economiche e infrastrutture critiche possano essere indebolite dal momento che dipendono sempre più dalle tecnologie informatiche. Tuttavia, se gli attivisti informatici del 2012 riescono a maturare, organizzarsi e mobilitarsi al di fuori del web, potremmo pensare a Anonymous come a una Versione 2.0 delle organizzazioni non governative, ideologicamente discutibile, forse, ma rispettata all'interno delle nostre democrazie. Legami con nuovi tipi di organizzazioni politiche, come il movimento politico internazionale Partito Pirata, potrebbero essere un primo passo in questa direzione[93].

Informazioni sull'autore

François Paget è un ingegnere ricercatore senior presso McAfee Labs in Francia. Si occupa di ricerche in ambito malware fin dal 1990 ed è stato uno dei fondatori di Avert (ora McAfee) Labs nel 1995. Paget tiene spesso presentazioni ad eventi di sicurezza in Francia e internazionali, è autore di un libro e di numerosi articoli ed è segretario generale del CLUSIF (French Information Security Club, il corrispettivo francese del CLUSIT italiano).

Informazioni su McAfee Labs

McAfee Labs è il gruppo di ricerca globale di McAfee. Con l'unica organizzazione di ricerca focalizzata su tutti i vettori di minaccia, ovvero malware, web, e-mail, rete e vulnerabilità, McAfee Labs raccoglie l'intelligence dai propri milioni di sensori e dal suo servizio McAfee Global Threat Intelligence™ basato su cloud. I 350 ricercatori pluridisciplinari di McAfee Labs in 30 nazioni seguono la gamma completa di minacce in tempo reale, identificando le vulnerabilità delle applicazioni, analizzando e correlando i rischi e attivando rimedi immediati per proteggere aziende e consumatori.

A proposito di McAfee

McAfee, società interamente controllata da Intel Corporation (NASDAQ:INTC), è la principale azienda focalizzata sulle tecnologie di sicurezza L'azienda offre prodotti e servizi di sicurezza riconosciuti e proattivi che proteggono sistemi e reti in tutto il mondo, consentendo agli utenti di collegarsi a Internet, navigare ed effettuare acquisti sul web in modo sicuro. Supportata dal suo ineguagliato servizio di Global Threat intelligence, McAfee crea prodotti innovativi destinati a utenti consumer, aziende, pubblica amministrazione e service provider che necessitano di conformarsi alle normative, proteggere i dati, prevenire le interruzioni dell'attività, individuare le vulnerabilità e monitorare e migliorare costantemente la propria sicurezza. McAfee è impegnata senza sosta a ricercare nuovi modi per mantenere protetti i propri clienti. www.mcafee.com/it

[1] "Hacktivism, From Here to There." Attivismo informatico, da qui a lì. Cult of the Dead Cow. Pubblicato online. McAfee Labs sconsiglia di visitare questo sito, indicato come "rosso" da McAfee SiteAdvisor.
[2] Cult of the Dead Cow. Pubblicato online.
[3] http://www.bris2600.com/hall_of_fame/ccc.php
[4] http://www.cert.org/advisories/CA-1989-04.html
[5] http://en.wikipedia.org/wiki/Intervasion_of_the_UK
[6] http://www.tommasotozzi.it/index.php?title=Netstrike_(1995)
[7] http://www.2600.com/hackedphiles/east_timor/
[8] http://findarticles.com/p/articles/mi_6914/is_2_22/ai_n28817798/pg_4/
[9] http://www.etoy.com/projects/toywar/
[10] http://www.fraw.org.uk/projects/electrohippies/archive/wto_prelease.pdf
[11] http://www.libertad.de/inhalt/projekte/depclass/spiegel/fr/info/review.html
[12] http://digital-stats.blogspot.com/2010/08/forum-4chan-receives-approximately-95.html
[13] http://techland.time.com/2008/07/10/now_in_papervision_the_4chan_g/
[14] Lulz è il plurale di lol, e significa anche risata sgradevole, malvagia o sardonica.
[15] http://encyclopediadramatica.se/Main_Page. Una nuova forma del sito, apparentemente più politicamente corretta, è disponibile all'indirizzo http://ohinternet.com/Main_Page.
[16] http://cnews.canoe.ca/CNEWS/Crime/2007/12/07/4712680-sun.html
[17] ISBN 978-2-916571-60-7
[18] "Chanology" è una fusione di Chan (dal forum 4chan) e Scientology.
[19] http://cnews.canoe.ca/CNEWS/Crime/2007/12/07/4712680-sun.html
[20] http://musicmachinery.com/2009/04/15/inside-the-precision-hack/
[21] http://www.businesspundit.com/anonymous-joins-fight-against-tyranny-in-iran/
[22] http://www.guardian.co.uk/media/pda/2010/jan/06/youtube-porn-attack-4chan-lukeywes1234
[23] http://delimiter.com.au/2010/02/10/anonymous-attacks-govt-websites-again/
[24] http://knowyourmeme.com/memes/events/operation-payback
[25] http://www.myce.com/news/anonymous-operation-payback-timeline-infographic-36481/
[26] http://www.zonebourse.com/barons-bourse/Mark-Zuckerberg-171/actualites/Anonymous-prevoit-de-detruire-Facebook-le-5-novembre-prochain--13753673/
[27] http://www.guardian.co.uk/world/2007/aug/31/kenya.topstories3
[28] http://www.reuters.com/article/2007/11/14/us-guantanamo-manual-idUSN14242070200711l4?pageNumber=1
[29] http://www.theregister.co.uk/2008/04/08/church_of_scientology_contacts_wikileaks/
[30] https://www.eff.org/files/filenode/EFF_PK_v_USTR/USTRcomplaint.pdf
[31] http://mybroadband.co.za/news/internet/14702-outcry-in-belgium-over-wikileaks-publications-of-dutroux-dossier.html
[32] http://icelandweatherreport.com/2009/08/kaupthings-loan-book-exposed-and-an-injunction-ordered-against-ruv.html
[33] http://fr.wikipedia.org/wiki/Leet_speak
[34] http://www.spamhaus.org/news/article/665
[35] http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian
[36] http://www.youtube.com/watch?v=_4LU7piK9X4
[37] http://www.thestandard.co.zw/local/27601-first-lady-gono-in-diamond-scandal-wikileaks.html
[38] http://cert.lexsi.com/weblog/index.php/2011/01/07/398-operation-zimbabwe-chronique-dune-cyber-attaque-contre-les-sites-gouvernementaux-zimbabweens-par-le-groupe-hacktiviste-anonymous
[39] http://temporaryartist.wordpress.com/2011/01/17/we-are-winning-the-thoughts-of-a-single-humble-anon/
[40] *Anonymous*, pagina 235, di Frédéric Bardeau e Nicolas Danet (ISBN 978-2-916571-60-7)
[41] http://www.ft.com/intl/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html
[42] http://www.guardian.co.uk/commentisfree/cifamerica/2011/jun/22/hacking-anonymous
[43] http://www.mediaite.com/online/exclusive-gawker-hacker-gnosis-explains-method-and-reasoning-behind-his-actions/
[44] http://blogs.computerworld.com/18307/face_of_anonymous_quits_exclusive_interview_with_barrett_brown
[45] http://www.foxnews.com/scitech/2012/03/06/hacking-group-lulzsec-swept-up-by-law-enforcement/
[46] ENEL: Ente Nazionale per l'Energia Elettrica, Italia; EDF: Electricité de France; ENDESA: Empresa Nacional de Electricidad, SA, Spagna e America Latina
[47] http://www.tgdaily.com/security-features/55690-anonymous-launches-operation-blitzkrieg
[48] http://e-worldwar.com/~/index.php?option=com_content&view=article&id=86&Itemid=494
[49] http://en.wikipedia.org/wiki/Operation_AntiSec
[50] http://www.thetechherald.com/articles/The-FBIs-warning-about-doxing-was-too-little-too-late
[51] http://www.rtbf.be/info/medias/detail_le-groupe-de-pirates-anonymous-a-publie-les-coordonnees-de-25-000-policiers-autrichiens?id=6816493
[52] http://www.ladepeche.fr/article/2011/09/29/1179489-copwatch-gueant-porte-plainte-contre-le-site-anti-flic.html
[53] http://archives-lepost.huffingtonpost.fr/article/2011/08/08/2564639_anonymous-les-donnees-personnelles-de-la-police-americaine-sur-internet.html
[54] http://www.ft.com/intl/cms/s/0/e8a6694c-95bb-11e0-8f82-00144feab49a.html#axzz1nDE7Z4df
[55] http://globalvoicesonline.org/2011/10/31/mexico-fear-uncertainty-and-doubt-over-anonymous-opcartel/
[56] http://www.lanacion.com.ar/1406114-mexico-asesinados-y-colgados-por-denunciar-en-twitter-asuntos-narcos
[57] http://www.tadla-azilal.com/technologies/mexique-les-menaces-sur-la-presse-setendent-aux-reseaux-sociaux/
[58] http://www.pcmag.com/article2/0,2817,2395863,00.asp#fbid=EBREppl_iKE
[59] http://www.bbec.lautre.net/www/spip_truks-en-vrak/spip.php?article2121
[60] http://www.youtube.com/user/BarrettBrown
[61] http://www.f-secure.com/weblog/archives/00002290.html
[62] http://www.guardian.co.uk/technology/2012/mar/06/lulzsec-court-papers-sabu-anonymous?intcmp=239
[63] http://www.v3.co.uk/v3-uk/news/2154453/anonymous-laughs-nsa-claims-hacking-power-grid
[64] http://obsession.nouvelobs.com/la-fermeture-de-megaupload/20120123.OBS9528/anonymous-en-fermant-megaupload-ils-nous-ont-prive-d-une-liberte.html
[65] SSL o Secure Sockets Layer, è un protocollo per proteggere gli scambi su Internet, in origine sviluppato da Netscape e ora spesso denominato TLS (Transport Layer Security).
[66] http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action
[67] Questa procedura viene spiegata in diversi forum, tra cui il seguente: http://pastebin.com/hR9FakGs
[68] 2mjtgjozdqg2aumu.onion
[69] http://pastehtml.com/view/1e8t85a.html
[70] https://code.commotionwireless.net/projects/commotion/wiki/Newbie_How_it_Works
[71] http://freenetproject.org/whatis.html
[72] http://thanatos.trollprod.org/sousites/hoic/
[73] http://www.nytimes.com/2012/02/27/technology/attack-on-vatican-web-site-offers-view-of-hacker-groups-tactics.html?_r=1&pagewanted=all
[74] http://www.nbs-system.com/blog/analyse-de-loutil-de-ddos-loic.html
[75] http://blogs.mcafee.com/mcafee-labs/android-diy-dos-app-boosts-hacktivism-in-south-america
[76] http://blog.spiderlabs.com/2012/01/hoic-ddos-analysis-and-detection.html
[77] http://thehackernews.com/2011/07/refref-denial-of-service-ddos-tool.html
[78] http://www.rezocitoyen.fr/telecomix-hacker-pour-la-liberte.html?artpage=2-3
[79] http://www.siliconmaniacs.org/telecomix-on-ne-casse-rien-on-repare-on-ameliore-on-reconstruit/
[80] http://www.rue89.com/2011/08/18/hackers-libertaires-notre-but-cest-partager-la-connaissance-218241
[81] http://owni.fr/2011/09/14/opsyria-syrie-telecomix/
[82] Questo kit è ancora disponibile: https://telecomix.ceops.eu/tcxnetpack.tgz
[83] http://reflets.info/internet-coupe-en-egypte-enfin-presque/
[84] http://www.theregister.co.uk/2010/04/09/virtual_protest_as_ddos/
[85] http://www.contrepoints.org/2011/11/24/57189-climategate-2-0-de-nouveaux-mails-entachent-la-science-climatique
[86] http://wikileaks.org/the-spyfiles.html
[87] http://observers.france24.com/fr/content/20120116-site-armee-nigeriane-hacker-activistes-mobilisation-internet-prix-essence
[88] http://www.branchez-vous.com/techno/actualite/2011/08/anonplus_anonymous_defacage_cyber_armee_syrie.html
[89] http://www.bbc.co.uk/news/technology-14476620
[90] http://www.theinquirer.net/inquirer/news/2128175/anonymous-team-poison-start-op-robin-hood
[91] http://www.huffingtonpost.co.uk/2012/04/12/mi6-phone-hack-attack-was-easy-trick-mi6_n_1420308.html
[92] http://www.zone-h.org/news/id/4737
[93] http://www.pp-international.net/

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it