Falsari di tutto il mondo unitevi! Diffondi falsa informazione e abbindola i media nell'epoca del capitalismo immateriale

Falsi comunicati stampa, falsi siti, notizie bufala: tutto questo può fare molto male ai potenti di oggi, impariamo a utilizzare quest'arma affilata!

Tre Sezioni:

- Pizzardone teorico
- Alcune storielle interessanti che possono darci ispirazione
- Alcune idee pratiche approssimative su come inviare un falso comunicato/creare una falsa notizia

In questo testo troverai:

- Problemi nelle lotte sociali odierne, come sono connessi alla dimensione immateriale del capitalismo
- Comunicazione e hacking: sperimentare per evitare la repressione e trovare nuovi strumenti per le lotte sociali
- Perché queste tattiche potrebbero essere utili nella nostra lotta contro il capitalismo contemporaneo
- Alcune storielle interessanti di bufale che hanno ben funzionato nel passato
- Proposte per nuove sperimentazioni
- Una guida pratica con delle idee concrete, basate sulla spannometria, sull'arte di creare falsi

Pizzardone teorico (per chi si vuole male)

Introduzione: quale contesto ci ha fatto pensare alla strategia del falsario

Questo testo è stato scritto come risultato della riflessione di alcuni individui, ispirati da discussioni e processi collettivi, sulla trasformazione di società e potere. Vuole essere un piccolo contributo alle tante e molteplici sperimentazioni di nuove strategie di lotta. Discute tattiche finalizzate ad attaccare la dimensione immateriale del capitalismo, e quindi l'aspetto informativo del potere. Questo non vuole essere un testo coerente, ma una raccolta di spunti di riflessione presentati alla rinfusa. Questo perché pensiamo che le idee che presentiamo potrebbero essere utili strumenti per diverse tipologie di lotte sociali. E anche perché non ci veniva in mente ne un capo ne una coda. Non critichiamo tutti i mezzi tradizionali di lotta, ma pensiamo che spesso degli strumenti che hanno avuto un' importanza storica corrano il rischio di trasformarsi in rituali cristallizati. Talvolta la fedeltà a queste tradizioni tende a reprimere strumenti e strategie innovative. In questo testo troverete alcune idee sulle nuove tattiche che vogliamo discutere.

La storia insegna come l'umanità trovi sempre forme creative e innovative per resistere di fronte ai problemi che trova nella vita di tutti i giorni e nelle lotte. In questo momento, ci sono molti ostacoli rilevanti, e **riteniamo vitale evolvere i nostri strumenti di lotta e sperimentare diversi mezzi d'azione** per superare questi ostacoli. Il potere non si riposa mai, impara sempre dai nostri punti deboli e forti.

Ci sono diverse ragioni per cui pensiamo che sia molto importante sperimentare nuovi mezzi d'azione. Ne citeremo due.

- **Per chi partecipa a lotte sociali e movimenti, è un fatto – spesso amaro – che quando un movimento cresce la repressione diviene sempre più dura.** Sperimentare nuovi mezzi d'azione può permettere di spiazzare ed aggirare temporaneamente la repressione.

- **La nuova organizzazione della produzione e dello spazio rende alcune strategie di lotta del passato meno efficaci.** Se prendiamo come esempio il mondo del lavoro,la nuova organizzazione del lavoro è sempre più decentralizzata, flessibile e basata sull'outsourcing. La struttura gerarchica di imprese e istituzioni si sposta dall'internalizzazione all'outsourcing, ricorrendo a subappalti, controllo indiretto, sistemi flessibili di produzione e lavoro precario. In questo quadro, molte strategie di lotta del passato possono essere talvolta meno efficaci. Prendiamo ad esempio lo sciopero. Se un'impresa può reagire all'interruzione della produzione rivolgendosi a un appaltatore esterno o a un'agenzia interinale, l'efficacia di questa forma di lotta sarà molto ridotta. Inoltre, è più complicato organizzare uno sciopero in una struttura a rete con relazioni lavorative flessibili e asimmetriche che nella classica fabbrica fordista. **Alcune riflessioni simili e altrettanto importanti possono essere fatte sulle trasformazioni post-fordiste delle istituzioni e della struttura urbana (ma ci fiacca scriverle, é tardi, fa freddo e il caffè é finito, poi c é pure il gatto che ha deciso di giocare con il cavo di alimentazione, fatevele voi).**

Cos' é la strategia del falsario?

Negli ultimi anni molte azioni che coinvolgono comunicazione-guerriglia, hacking, la creazione di falsi, sono state effettuate. Alcune di queste pratiche sono state già largamente sperimentate, mentre altre cammini, secondo noi, potrebbero dare risultati molto interessanti ma non sono ancora sfruttati. Quello che ci interessa qui è **una forma di azione diretta mirata a diffondere false informazioni o a creare confusione, col fine di causare un danno economico o politico.** E' legata alla comunicazione-guerriglia o all'hacktivismo, ma ha delle caratteristiche peculiari che vale la pena di esplorare.
Pensiamo che una mistura di alcuni strumenti informatici di base, l'imitazione delle strategie comunicative del target e la raccolta di informazioni, possano produrre tattiche molto interessanti ed efficaci, che possono essere talvolta facili da sperimentare.

Molte azioni sono già state effettuate diffondendo falsi comunicati stampa, ma solitamente avevano come principale fine la creazione di consapevolezza su una questione, denunciando la politica di una specifica impresa/istituzione, smascherando il discorso dominante e portando alla luce scomode verità (anche se sicuramente alcune di queste azioni hanno avuto un indubbio impatto economico).
Altre azioni hanno bloccato server e siti, effettuato il defacing di siti web, etc., causando seri danni.
Tuttavia, **raramente i militanti hanno cercato di causare un danno economico diffondendo false informazioni su un impresa;** far questo può richiedere strumenti informatici molto semplici, uno studio meticoloso del target, un po' di conoscenza del settore e, se possibile, l'aiuto di un “insider” volenteroso a smazzare informazioni, modelli, etc...

Consideriamo la strategia del falsario efficace ed interessante per diverse ragioni:
- Informazione è profitto.

Una crescente quota di profitto è basata sull'informazione. La dimensione immateriale del capitalismo prende un ruolo centrale nel processo di valorizzazione. Ogni aspetto della vita è sempre più mercificato. Le relazioni sociali, i valori, gli immaginari, la conoscenza, sono divenuti una fonte centrale di profitto. L'immagine di un'azienda (verso clienti, distributori, azionisti) e la sua capacità di generare valore immateriale sono spesso più importanti dell'efficienza nella produzione fisica dei beni. L'informazione è una risorsa importante per le imprese per poter controllare clienti, anticipare le strategie delle altre imprese, evolvere in un mercato sempre più globale e complesso, prevedere uno scenario sull'evoluzione dei mercati finanziari. Inoltre, il successo di un'istituzione finanziaria è basato sulla capacità d'influenzare i flussi d'informazione dei mercati finanziari e accedere alle informazioni in tempo reale.

Nell'economia post-fordista, l'adozione di strategie flessibili di marketing mirate allo specifico consumatore è fondamentale, questa è una ragione per cui il costante controllo dei comportamenti individuali ha tanto valore. Per esempio, Google consegue i suoi enormi profitti spiando le abitudini degli utilizzatori di internet, vendendo questi dati e fornendo pubblicità mirate. Dato che la complessità e l'incertezza del sistema economico mondiale stanno crescendo, l'accesso all'informazione allo scopo di fare buone previsioni del futuro ha un immenso valore economico. Specialmente nei mercati finanziari - dove il processo di valorizzazione è basato sulle aspettative degli attori finanziari e le strategie sono basate sulla razionalità comportamentale - la raccolta di informazioni e la rapida produzione di scenari gioca un ruolo cruciale. Le attese che riguardano una società e il suo corso azionario, la sua reputazione e le informazioni che circolano sulla società influenzano l'attitudine dei mercati verso le sue azioni e di conseguenza le plusvalenze legate alla valorizzazione finanziaria.

Dato che il profitto si basa sempre di più sulla produzione immateriale, **le tattiche che mirano a colpire l'aspetto immateriale del profitto diventeranno sempre più potenti.** Se un'impresa spende milioni per costruire la sua reputazione, costruendo una buona strategia di marketing e un efficace sistema di gestione delle informazioni, questo è un buon punto dove attaccare.
Inoltre, questo tipo di azioni può portare aziende o istituzioni a riorganizzare le loro procedure operative/sistemi di comunicazione/ambienti di lavoro, portando a costi più alti. Persino sabotaggi e danni materiali spesso causano più danni indiretti (perdita di reputazione, necessità di modificare le procedure operative, rallentamenti) che danni diretti (spesso le aziende sono assicurate, e i danni materiali sono spesso trascurabili in relazione al grande fatturato aziendale). In un capitalismo post-fordista, delle tattiche post-fordiste di lotta ci possono dare nuovi modi per contrattaccare efficacemente.

- Il capitalismo sfrutta il nostro cervello ma ci dà anche nuove armi per contrattaccare

Il capitalismo sfrutta il nostro cervello – la nostra razionalità, le nostre capacità sociali e le nostre emozioni – tutti gli aspetti della nostra vita – come fonte di profitto. Sfrutta le nostre funzioni cognitive durante tutta la giornata. Le nostre azioni quotidiane, la nostra immaginazione, le nostre creazioni intellettuali, sono facilmente – direttamente e indirettamente – espropriate. Dato che usano i nostri cervelli nella loro produzione immateriale, spesso acquisiamo informazioni e competenze (per esempio chi lavora per una ditta conosce il funzionamento ed il linguaggio della stessa e possiede certe competenze per utilizzare la sua tecnologia ed i suoi sistemi). **Perché non condividiamo queste informazioni e competenze per contrattaccare?**

-Permette di cospirare senza esporsi

Inoltre, molte persone trovano difficile essere coinvolte apertamente nelle lotte sociali. Anche se non vogliono esporsi, alcuni hanno informazioni rilevanti. In una condizione precaria (in senso lato) e isolata, e in una società atomizzata, non tutti vogliono iniziare una lotta aperta. Ma la lotta può anche consistere nella condivisione di informazioni da usare per cospirare contro le imprese e le istituzioni. La fedeltà è una strategia crescente del potere aziendale e istituzionale per controllare, e rifiutarla può essere una forma di resistenza. E poi c é sempre chi parla troppo, impariamo dagli sbirri che ci spionano tutto il tempo, per una volta tendiamo noi le orecchie aperte e offriamo una birra in più al chiacchierone di turno.

-Permette d'invertire la relazione tra movimenti radicali e media

I movimenti sociali spesso si trovano di fronte a un dilemma sul come relazionarsi con i media mainstream:
Rifiutare di comunicare con loro comporta il rischio di vedere le nostre azioni deformate e meno visibili. Comunicare con

loro invece comporta il rischio di essere manipolati e vedere il nostro messaggio deformato. Alla fin dei conti, scriveranno in ogni caso quello che vogliono.

Perché non contrattaccare e non cercare d'invertire la relazione tra movimenti radicali e media, cercando di ritorcere la loro costante disinformazione contro di loro? Perché non cercare per una volta di usare i media come un vettore per diffondere false informazioni? I media riscrivono la realtà ogni giorno, sono sottomessi ai poteri politici ed economici e hanno una fede intaccabile nelle grandi agenzie di stampa. Molti giornalisti credono e riproducono tutte le informazioni che arrivano da certe fonti.
Perché non avvantaggiarsi da queste debolezze per un uso sovversivo, e usare i media senza essere manipolati? Perché non prendere per il culo i media e prendere in prestito la loro macchina di propaganda?

Alcune idee e spunti d'azione:

- Far pubblicare dai media false informazioni per danneggiare la reputazione di un'azienda o un'istituzione e disturbare la sua strategia di comunicazione
- Un falsa mail inviata a nome di un capo, di un burocrate, può creare conflitti o evidenziare dei comportamenti nascosti. Può essere una potente arma di rappresaglia
-Un falso comunicato stampa di un'azienda che include false informazioni economiche per danneggiarla sui mercati finanziari
-Etc,etc,etc!

Questi esempi possono potenzialmente servire per svariati tipi di lotta sociale, problemi quotidiani...

Sfruttano il nostro cervello – la nostra razionalità, le nostre capacità sociali e le nostre emozioni – tutti gli aspetti della nostra vita come fonte di profitto. Giocano con le nostre vite ogni giorno attraverso i mercati finanziari, i media che diffondono paure irrazionali e ideali marci, la burocrazia kafkiana. Perché non contrattaccare a quel livello e scombussolare i loro bei modelli e le loro magnifiche procedure?

Organizziamoci!
Condividiamo le informazioni e le competenze che abbiamo per cospirare insieme e contrattaccare!
Possiamo trasformare i loro processi immateriali nel loro incubo immateriale!

AZIONE DIRETTA ORA!

Alcune storielle che possono darci ispirazione

Yes Man vs Dow Chemical

Dow ha acquistato nel 2001 Union Carbide, impresa responsabile della catastrofe di Bhopal (per la quale ci furono decine di migliaia di vittime a causa di una fuoriuscita di sostanze tossiche da un impianto). Dow rivendica che l'impresa non eredita responsabilità per il disastro di Bhopal, ma le vittime non si sono rassegnate e hanno continuato a lottare contro Dow per avere un risarcimento. Gli Yes Men hanno deciso, nel 2002, di “aiutare” Dow Chemical a spiegare meglio perché non poteva fare nulla per gli abitanti di Bophal: loro non sono azionari. Gli Yes Man hanno creato a questo fine un falso sito che imitava lo stile di Dow Chemical, DowEthics.com.

Due anni dopo, a fine novembre 2004, un invito è arrivato a questo sito, precedentemente restato inosservato. Bbc voleva un rappresentante di Dow per discutere la posizione dell'impresa sulla tragedia di Bhopal in occasione del ventesimo anniversario del disastro. Jude Finisterre, presunto portavoce del colosso della chimica mondiale Dow Chemical (in realtà uno Yes Men), fece dagli schermi della Bbc un clamoroso annuncio: la multinazionale aveva deciso di riconoscere in pieno le proprie responsabilità per la catastrofe e di risarcire quindi in solido i 120.000 indiani colpiti più o meno gravemente dalla nube tossica.

Dow Chemical smentì la falsa intervista due ore dopo, nel frattemento l'intervista fu trasmessa integralmente 2 volte, e la notizia restò al top di news.google.com per due ore. La novità clamorosa provocò un finimondo a Wall Street, costando alla Dow quasi due miliardi di dollari di capitalizzazione. La smentita di Dow Chemical chiarisce che Dow non risarcirà nessuno e non rimedierà a nulla, visto che la sua unica responsabilità è verso gli azionisti. La notizia e la smentita resteranno top story su news.google.com per tutta la giornata.

http://theyesmen.org/hijinks/bbcbhopal

Burla contro Whitehaven Coal

Il 7 Gennaio 2013, un falso comunicato stampa ha costretto Whitehaven Coal a una sospensione temporanea delle sue azioni dopo aver perso 314 milioni di dollari di valore azionario.

Il falso comunicato, prodotto dal gruppo di attivisti Font Line Action on Coal, dichiarava di venire da ANZ e sosteneva che questa banca avesse ritirato il recente prestito di 1.2 miliardi di dollari concesso a Whitehaven per sviluppare il progetto di miniera a Maules Creek. La notizia ha rapidamente causato una svendita delle azioni di Whitehaven, con il valore azionario che ha perso sino al 9% a mezzogiorno. Quando la smentita è circolata le azioni hanno cominciato lentamente a riprendere valore, ma comunque la loro vendita è stata sospesa.

Il falso comunicato suggeriva che ANZ avesse ritirato il prestito per l' “instabilità del mercato globale del carbone, l'attesa dell'aumento dei costi e il codice di responsabilità aziendale di ANZ”. Il codice di ANZ dice che i fondi non devono essere prestati per progetti che avranno un impatto negativo a livello sociale e ambientale.”Vogliamo che i nostri clienti siano tranquillizzati sul fatto che non investiremo in progetti che causano significanti espulsioni di contadini, danni inaccettabili all'ambiente, o conflitti sociali”, diceva il falso comunicato.

Front Line Action on Coal ha rivendicato l'azione e ha affermato che il comunicato è stato inviato per protestare contro il progetto di miniera a Maules Creek.

http://www.miningaustralia.com.au/news/fake-press-release-wipes-$314-million-off-whitehav.html

I No Tav attaccano Banca Intesa

Sul mercato azionario era un tranquillo venerdì pomeriggio di primavera, con le banche che recuperavano terreno dopo lo storno dei giorni precedenti. Tra queste, Intesa Sanpaolo, che, intorno alle 15.30, faceva segnare un progresso dell'1,6 per cento. Poi, intorno alle 15.40, succede l'inaspettato: le principali testate finanziarie ricevono un falso comunicato dall'indirizzo email group@intesasanpaolo.com che riferisce delle dimissioni dell'amministratore delegato della banca, Carlo Messina.
"Intesa Sanpaolo - vi si legge - conferma di aver ricevuto oggi una lettera dal suo consigliere delegato e CEO, Carlo Messina. La lettera, datata 24 Aprile 2015, è circolata a tutti i membri del Board ed è stata inviata alla CONSOB. Carlo Messina ha ammesso di aver falsato la contabilità, esagerando il risultato netto di 1.920 milioni di euro nel 2014. Considerando queste nuove informazioni, Intesa Sanpaolo riporterebbe un bilancio in perdita per il 2014". La nota riportava, inoltre, il link a un sito apparentemente del gruppo Intesa ma in realtà esterno dove era possibile leggere il comunicato.

Sta di fatto che, dopo l'uscita della finta nota stampa sulle dimissioni di Messina, il titolo a Piazza Affari cambia direzione e arriva a perdere l'1% circa intorno alle 16.05, dopo che soltanto alle 15.57, quando ancora probabilmente non si era propagato l'effetto della finta nota, guadagnava oltre il 2 per cento. Il falso comunicato ha generato una caduta verticale del titolo, durata lo spazio di pochi minuti: a cavallo delle 16:00 è passato da 3,1 a 2,99 euro.

Sempre in serata, i "No tav" hanno rivendicato il gesto, in una mail, diffusa dallo stesso indirizzo da cui era giunta la falsa nota, dal titolo: "Rivendicazione Falso comunicato che ha fatto precipitare le azioni di Intesa Sanpaolo - No Tav". Il testo della mail definisce una "buona notizia" l'accaduto e indica che Intesa è la principale banca che finanzia la Tav", ossia la linea ad alta velocità tra Torino e Lione.

http://www.repubblica.it/economia/finanza/2015/04/24/news/intesa_sanpaolo_falso_comunicato-112751049/?refresh_ce

Alcune idee pratiche approssimative su come inviare un falso comunicato/creare una falsa notizia

Questo non é ne un manuale ne una guida, la teoria sul soggetto non é certo a punto, questo é piuttosto un confuso brainstorming e una collezione di trucchi...

UNA BREVE INTRODUZIONE: COME FUNZIONA LA COMUNICAZIONE

Di solito imprese e istituzioni hanno una lista di contatti e-mail alla quale inviano regolarmente comunicati e newsletters. Normalmente è facile essere aggiunti alla loro newsletter, basta inviare una mail o utilizzare la procedura automatica spesso presente sul loro sito. I loro comunicati hanno quasi sempre lo stesso formato, riportano gli stessi loghi e la stessa struttura e sono inviati dallo stesso indirizzo mail.

Le agenzie di stampa distribuiscono notizie a tutti i media della loro zona. Qualsiasi cosa arrivi da loro è considerata come oro colato dai giornalisti. Se riesci a ingannare una di loro, probabilmente tutti i giornali saranno ingannati di conseguenza.

La psicologia del giornalista (e dell' umano) è un aspetto importante al quale pensare. Spesso non controllano cosi' tanto l'informazione se hanno fiducia nella loro fonte. Se ricevono un comunicato potrebbero guardare il sito il cui link è riportato nella mail, chiamare il numero del contatto, contattare altre fonti che possono avere informazioni aggiuntive.

RACCOMANDAZIONI GENERALI: IMPARA COME PROTEGGERTI PRIMA DI AGIRE

Non affrettarti, dovresti seguire delle buone misure di sicurezza per proteggere te stesso e le tue investigazioni.

Navigare sulla rete è come parlare dal balcone: molti possono sentirti...
Quando ti connetti a un sito o a un motore di ricerca, di solito il tuo indirizzo IP verrà registrato.
L'indirizzo IP è l'identificante della tua connessione Internet e ti può tracciare. Meglio quindi connettersi da un wireless pubblico che non ha legami con te! Persino se ti connetti da un wireless pubblico, puoi essere identificato per il tuo indirizzo MAC. L'indirizzo MAC è un codice unico associato alla tua scheda di rete (quindi con il tuo laptop). Ma niente paura, puoi facilmente modificarlo (in Linux con il comando Macchanger). Inoltre il tuo computer conserva nella sua memoria le tracce delle tue attività, anche se pensi di aver cancellato le informazioni compromettenti.

Ecco alcuni strumenti che possono esserti utili:

***Tor*:** Tor è una rete di tunnel virtuali che permette di migliorare la propria privacy e sicurezza su Internet, navigando in modo relativamente anonimo. Tor non può risolvere tutti i problemi di anonimato, ma aiuta molto.

https://www.torproject.org/

Crittografia del disco: tecnologia che protegge i tuoi dati trasformandoli in un codice illeggibile che non può essere decriptato da persone non autorizzate. Puoi crittare il tuo hard disk o una chiavetta USB per rendere l'informazione inagibile a chi non conosce la password. Il meglio é usare LUKS su Linux, altrimenti Truecrypt su Windows o Mac.

Tails: un sistema operativo live, che puoi avviare in quasi ogni computer da una chiavetta USB, un DVD, o una carta SD. Protegge la tua privacy e il tuo anonimato, e ti aiuta a: navigare anonimamente in Internet e aggirare la censura (tutte le connessioni passano per Tor); non lasciare traccie sul computer che stai usando; usare i più aggiornati strumenti di crittografia per criptare i tuoi file, le tue mail e le tue chat.

https://tails.boum.org/

La sicurezza informatica e l'anonimato sono questioni importanti che ti permetteranno di proteggerti, puoi trovare un sacco di guide interessanti sulla rete, per esempio:

(Italiano) https://we.riseup.net/assets/144942/crypt%20or%20die.pdf
(Inglese) http://zinelibrary.info/files/FINAL.pdf

Fai i test necessari prima di agire!

CREARE UNA FALSA NOTIZIA

Assumiamo che tu voglia attaccare un'impresa chiamata “Spazzatura Costosa”.

Devi pensare come vuoi diffondere la tua falsa informazione: via mail? Via Twitter? Attraverso un falso sito sperando di essere contattato? A nome dell'impresa? A nome di un'altra fonte?

L'imitazione richiede un'analisi accurata. Studiare il comportamento del target ed il suo stile di comunicazione è vitale per portare avanti un azione di successo. Puoi fare tante cose: iscriverti alla newsletter del target, guardare il materiale che mette in linea, fare altre ricerche...

Se vuoi inviare un falso comunicato via mail, puoi adottare due strategie: creare un nuovo indirizzo e-mail allo scopo (dovrai quindi registrare il dominio del tuo indirizzo – con un falso nome logicamente!), oppure falsificare l'indirizzo mail dal quale l' impresa invia i suoi comunicati. Quindi, se il tuo target invia i suoi comunicati da info@spazzaturacostosa.com , puoi registrare un dominio leggermente diverso (ad esempio spazzatura-costosa.com) e creare un indirizzo mail ad hoc da cui inviare il falso comunicato (info@spazzatura-costosa.com)..
Un altro metodo puo' essere usare Telnet, in modo da poter utilizzare l'indirizzo originale (info@spazzaturacostosa.com), o un altro indirizzo, a partire dallo stesso dominio, che ritieni più convincente (comunicazione@spazzaturacostosa.com , salastampa@spazzaturacostosa.com , spazzaturacostosa@spazzaturacostosa.com, etc.).

Se il tuo target non comunica molto, probabilmente non tanti giornalisti ricevono le sue newsletter e quelli che le ricevono presumibilmente non ricorderanno il loro format e il loro mittente. Se il tuo target è un'impresa/istituzione importante con una strategia di comunicazione pro-attiva, è cruciale fare un'imitazione convincente dell'originale.

Un trucco facile per formattare correttamente una mail con un falso comunicato per imitare il formato originale è salvare il codice di un comunicato ufficiale e modificarlo inserendo il testo falso. Una base di conoscenza di HTML può facilitare questa operazione (a meno che il messaggio sia inviato in mero plain text)

Se vuoi inviare una mail da un indirizzo falsificato, devi sicuramente imparare a usare Telnet. Se hai creato un'email ad-hoc, puoi inviarlo dal tuo dominio. Ma controlla i limiti posti dal fornitore di servizio (massimo numero di mail per ora, etc.): per un invio massivo, Telnet potrebbe essere in ogni caso la soluzione più facile ed efficace. Parleremo di Telnet più tardi.

Sul contenuto del tuo comunicato: pensa anche ai link e ai numeri di telefono che sono riportati. I giornalisti spesso cercano di avere delle informazioni aggiuntive per le loro notizie, e controllano il sito dell'azienda o chiamano il responsabile stampa. Un'idea intelligente è fare un falso sito del target e inserire un link nel comunicato: alcuni giornalisti apriranno il link e saranno più convinti dell'autenticità della notizia!
Sui numeri di telefono: è importante evitare che i giornalisti chiamino il numero del corretto responsabile stampa, perché smentirebbe il falso. Meglio inserire un numero di telefono al quale risponderà un complice che si spacci per il portavoce di Spazzatura Costosa. O un numero che è sempre occupato o non risponde mai il giorno scelto. Ma fai una chiamata di prova prima: una segreteria telefonica smentirebbe l'identità del numero!

FATTI UNO SCENARIO

Ti consigliamo di predisporre uno scenario, di pensare quando e come agire a seconda dei tuoi fini e di come reagirà chi

leggerà la notizia.

Dovresti chiederti alcune questioni: i tuoi destinatari sono giornali, agenzie di stampa, persone specifiche o un pubblico specifico? Vorresti che la notizia si diffondesse il più rapidamente possibile nella rete? O preferiresti farla passare silenziosamente durante il giorno stesso per essere pubblicata l'indomani nei quotidiani cartacei?

Le risposte ti aiuteranno a decidere la tempistica. Considera che passerà un po' di tempo prima che il tuo messaggio sia letto e pubblicato/ritrasmesso. E tanto più larga è la tua lista stampa, più probabilità hai di avere una reazione rapida. Prima e più largamente il tuo falso sarà diffuso, prima il target scoprirà il falso e in poco tempo potrà smentirlo.
Se invii il tuo comunicato troppo presto, la smentita potrebbe arrivare troppo presto per i tuoi obiettivi.
Se vuoi vedere la tua notizia pubblicata nei giornali del giorno dopo, inviarla più tardi è una buona idea, per evitare una smentita prima che le redazioni chiudano.
Se vuoi influenzare il corso azionario il giorno medesimo, dovresti inviare il tuo falso almeno un'ora o più in anticipo rispetto alla chiusura della borsa.

GIUSTO EQUILIBRIO TRA REALISMO, INTERESSE MEDIATICO E DANNOSITA'.

Se crei una falsa notizia dovresti considerare questi tre assi e trovare il giusto equilibrio.

Se crei una falsa notizia troppo esagerata e grottesca i giornalisti potrebbero avere alcuni dubbi e verificare prima di diffondere la notizia (anche se non si sa mai: è già successo che i media diffondessero bufale clamorosamente irrealistiche)

Se la tua falsa notizia è realistica ma troppo irrilevante, non abbastanza “succosa” per i media, i giornalisti potrebbero crederci ma non pubblicarla.

E anche se la tua falsa notizia è pubblicata, potrebbe non dare un gran fastidio al target se non contiene nessuna informazione che può suggerire un serio rischio per la sua solidità economica o per la sua immagine.

Dovresti creare un falso realistico, allo stesso tempo abbastanza sensazionale per essere pubblicato e abbastanza dannoso per il target. Ti puoi ispirare alle migliaia di notizie e comunicati che si trovano sulla rete. E non essere troppo timida/o: anche se un falso è un po troppo esagerato, i giornalisti non sono poi sempre cosi scrupolosi! Meglio rischiare di diffondere un falso troppo esagerato che causerà il dubbio della maggior parte dei giornalisti che non lo pubblicheranno, meglio rischiare una rapida smentita del target, che diffondere un falso troppo insipido che nessuno pubblicherà. Se solo un paio di giornalisti crederanno al tuo falso e lo pubblicheranno in tempi rapidi, il gioco è fatto!

SCEGLI LA TUA PRESS LIST

Un buon falso dovrebbe essere inviato a destinatari appropriati, che non trovino strano il fatto di ricevere questo comunicato. Il meglio sarebbe poter contare sulla lista stampa del tuo target, o su una buona approssimazione, ma questo può essere difficile. In ogni caso, i giornalisti ricevono tante di quelle notizie ogni giorno che non saranno probabilmente sorpresi di ricevere un comunicato da una nuova fonte.

Pensa anche al pubblico dei destinatari, e a come ridistribuiranno il falso. Se i tuoi destinatari sono prevalentemente giornali, siti e agenzie, faranno da ripetitore, diffondendo esponenzialmente la notizia. Anche 2 o 3 a pubblicare sono sufficienti e permetteranno di raggiungere un pubblico vasto! In questo caso non hai bisogno di un' enorme lista (qualche centinaio di contatti può essere sufficiente) – ma di una lista ben selezionata!
Se vuoi inviare la notizia ai destinatari finali, fingendoti media (per esempio se fingi di essere un giornale, un sito d'informazione, una newsletter), la diffusione dipenderà principalmente da quanto ampia è la tua lista.

Costruire la lista non è sempre facile, richiede della creatività e dell'ingegneria sociale. I modi in cui trovare degli indirizzi mail rilevanti sono molteplici, qua ti daremo qualche suggerimento:

- domanda a qualcuno che potrebbe avere accesso direttamente o attraverso un collega alla press list dell'organizzazione per il quale lavora! Molte imprese, istituzioni, associazioni comunicano con i media ed hanno un ufficio stampa che può avere

una buona lista di contatti.

- cerca su Internet! Molti giornalisti, blogger, testate lasciano il loro contatto sul loro sito

- esistono siti web commerciali che vendono press list, puoi chiedere una demo!

- puoi estrarre contatti dai network sociali, e con un po di creatività puoi trovare gli indirizzi mail a partire da questi contatti

- puoi usare degli harvesting bots per trovare tutti gli indirizzi mail presenti su dei siti...

CREARE UN FALSO SITO

Può essere utile creare un falso sito che imiti quello originale dell'impresa/istituzione che vuoi attaccare. Se invii un falso comunicato via mail, dovrebbe ridirigere verso l'indirizzo del falso sito. Per esempio, se il sito del target è www.spazzaturacostosa.com, potresti registrare un dominio con un nome molto simile, come www.spazaturacostosa.com o www.spazzatura-costosa.com. Il più facile da fare sarebbe copiare il codice HTML del sito originale e caricarlo sul tuo sito fuffa. Dovrai semplicemente modificare qualche piccola parte del codice in modo da inserire il tuo falso, cambiare le date... Se il sito originale contiene una lista di comunicati, dovrai semplicemente aggiungere il tuo alla lista!

Registrare un dominio fuffa ti permette anche di creare indirizzi mail che sono molto simili agli indirizzi originali del tuo target. Se il responsabile stampa del tuo target ha come indirizzo mail pinco.palla@spazzaturacostosa.com, puoi creare un indirizzo mail pinco.palla@spazzatura-costosa.com.
Ancora una volta, sii sicuro/a e registra il dominio anonimamente! E' facile registrare un sito con un falso nome, ma più difficile pagare senza essere tracciati: Paysafecard o Ukash sono buone soluzioni, ma non tutti i rivenditori di domini accettano questi mezzi di pagamento.

INVIARE MAIL DA UN INDIZZO FALSIFICATO CON TELNET

Telnet

Grazie a un fortuito dono della storia di internet, il protocollo SMTP (utilizzato per inviare e-mail) normalmente non ha bisogno di autenticazione. Questo significa che se vuoi inviare una mail dal mittente info@spazzaturacostosa.com, devi solamente dichiarare che il mittente è info@spazzaturacostosa.com. Più facile di cosi'! Un programma facilissimo che permette di utilizzare SMTP è Telnet – puoi inviare una mail falsa in pochi secondi ! Ma ricorda: **falsificare una mail non è anonimo!** Le mail che mandi mostreranno il tuo indirizzo IP... quindi scegli un buon wireless aperto che non può essere associato a te.

Puoi trovare un sacco di tutorial sulla rete che ti spiegano come inviare una mail falsificata (ad esempio http://vitedigitali.blogspot.it/2007/10/come-inviare-mail-con-telnet.html)

Qui mettiamo un piccolo box che spiega sinteticamente come utilizzare Telnet

Telnet è un protocollo di rete utilizzato su Internet. È solitamente utilizzato per fornire all'utente sessioni di login remoto di tipo linea di comando tra host su internet

Per lanciare Telnet, non dobbiamo fare altro che entrare nel terminale (il Prompt per Windows) e digitare **telnet**. Ora che sappiamo come entrare in Telnet, dobbiamo collegarci al server SMTP del nostro provider. Per fare questo dobbiamo conoscere l' indirizzo di questo server. Il server di tin per esempio è **smtp.tin.it**

Quindi apro il terminale, scrivo telnet e poi scrivo open smtp.tin.it 25 per potermi connettere al server di Tin. Il server mi risponde con un messaggio che cambia da provider a provider, ma dovrà contenere 220 in caso di connessione positiva.
Ora che siamo connessi al server, dobbiamo identificarci scrivendo **HELO tin.it**. In tutti i server SMTP dobbiamo identificarci scrivendo **HELO nomedominio** dove nomedominio è il dominio del nostro provider ma in linea generale possiamo scrivere anche un nostro nickname.
Dopo essermi identificato, il server risponde con una riga che include **250,** che indica la corretta identificazione.
A questo punto indichiamo l' indirizzo del mittente della mail che vogliamo inviare scrivendo **MAIL FROM:** seguito dall' indirizzo del mittente posto tra i segni <>.
Ora dobbiamo indicare l' indirizzo del destinatario scrivendo **RCPT TO:** seguito dall' indirizzo del destinatario posto tra i segni <>.
Dopo aver scritto l' indirizzo del destinatario, dobbiamo scrivere il messaggio della mail. Scriviamo quindi il comando **DATA** e premiamo invio: qui possiamo inviare il contenuto della mail correttamente formattato e con tutti i campi necessari (Subject: , To: , Content-Type: , etc.). E' importante imparare come formattare correttamente il contenuto di una mail, oppure possiamo copiare il codice originale di un'altra mail e modificarlo.
Quando abbiamo finito dobbiamo premere il tasto Invio, premere il tasto del punto e ripremere il tasto Invio. Se tutto va bene il server ci risponderà con un messaggio del tipo **250 <******> Mail accepted** oppure **250 <******> Queued mail for delivery**. Per uscire definitivamente scriviamo **quit**.

La nostra mail contraffatta é stata inviata!

Trovare un buon server smtp per la tua azione

Non tutti i server SMTP sono appropriati. Ogni ISP configura il suo server SMTP in modo differente e può essere complicato trovare le singole politiche di ogni ISP. Queste politiche restrittive sono in luogo soprattutto per limitare lo spam. Quindi, per esempio, molti server SMTP limiteranno il numero di destinatari, il numero di connessioni in un periodo di tempo, alcuni server persino non ti lasceranno inviare nessuna mail... La rete che tu usi, inoltre, potrebbe essere blacklisted se è già stata usata da spammer. E' una buona idea fare dei test approfonditi, e provare diverse connessioni con differenti ISP. **Dovresti controllare se il server è un buon relay e ti lascia inviare un e-mail al numero desiderato di destinatari, e se il messaggio arriva correttamente.** Ma stai attento a non abusare del server SMTP per testarlo: se invii troppe comunicazioni spammose attraverso il server, potrebbero pensare che degli spammer hanno usato il loro server e adottare restrizioni più severe...
Impara dagli spammer!

Tip: in Italia Libero/Infostrada e Tim non sono provider adatti, mentre Tiscali si... inoltre puoi sperimentare i server di università e istituzioni...

Scrivere un piccolo script

Se la tua mail deve raggiungere una lista di destinatari consistente, meglio utilizzare uno script per automatizzare l'uso di Telnet. Expect (Tcl) è un buon linguaggio per questo scopo, disponibile per Linux, Mac e Windows (ma se vuoi veramente essere sicura/o e anonima/o, meglio passare a Linux). Puoi trovare un esempio alla fine del testo.

Capire come funziona l'antispam

Uno dei più grandi rischi è che la tua falsa mail finisca nella cartella dello spam, o forse non arrivi neanche. Meglio fare un test prima di agire.

Se invii la tua mail ad un piccolo numero di destinatari.

Se la tua mail raggiunge la cartella dello spam significa probabilmente che il campo DATA (il codice della mail) è formattato male, o che hai scelto male l' HELO. *Ricontrolla il codice.*

Se invii la tua mail a un gran numero di destinatari.

Molti provider commerciali hanno criteri restrittivi che possono segnalare un messaggio come spam se inviato a un largo numero di destinatari in tempo breve. Questo problema riguarda soprattutto domini commerciali (Yahoo, Gmail, Hotmail), non tanto domini istituzionali o aziendali, che hanno spesso filtri antispam più lassi. Se la maggioranza dei tuoi destinatari hanno mail aziendali o di redazione, non preoccuparti troppo, questo rischio non dovrebbe interessarti.

Puoi solitamente trovare sulla rete la politica antispam di ogni e-mail provider.

Alcune consigli per ridurre il rischio di essere bloccati dai filtri antispam:
- non usare un server SMTP/un indirizzo IP che è blacklisted per questioni di spam
- invia ogni mail una per una e includi il destinatario nel campo DATA (evita gli invii multipli, preferisci gli invii seriali)
- cerca di evitare i messaggi di errore del server SMTP, per esempio effettuando troppe connessioni contemporaneamente
- scegli un buon HELO, di solito la miglior soluzione è usare il nome del server SMTP al quale sei connesso

#Appendice per i più smanettoni: esempio di uno script in Expect (brutto ma funzionale)

Questo script aprirà una sessione Telnet che si connetterà al server SMTP, per poi inviare la tua mail sequenzialmente (lo script invia una mail separata per ogni destinatario: il miglior modo per evitare noie dall'antispam)

```
#!/usr/bin/expect -f

#The first argument is a text file with all the recipient e-mail addresses
#The second argument is the smtp server to which you want to connect, usually the
local ISP provider of the network you are using
#The third one is the HELO you give to the server. The more anti-spam friendly
solution is to put the very same name of the smtp server
#The forth one is the sender e-mail
#The fifth one is the first part of the data field, till the “To:” field (this can
be empty if the data field start with the recipient mail)
#The sixth one is the second part of the data field, after the “To:” field

set timeout 20
set server [lindex $argv 1]
set myhelo [lindex $argv 2]
set sender [lindex $argv 3]
set recipients [lindex $argv 0]
set data_file1 [lindex $argv 4]
set data_file2 [lindex $argv 5]
set rcpt_id [open $recipients r]
set data1_id [open $data_file r]
set data2_id [open $data_file1 r]
set data1 [read $data1_id]
set data2 [read $data2_id]
spawn telnet $server 25
expect {
     "220"   {puts "ok"}
     timeout { send "QUIT\n" ; puts "Smtp server not answering"; exit}
}
send "HELO $myhelo\n"
expect {
     "250"   {puts "ok"}
     timeout { send "QUIT\n" ; puts "Not answering to HELO" ; exit}
}
set line [gets $rcpt_id]
while { $line >= 0 } {
   send "MAIL from: $sender\n"
   expect {
     "250"    {puts "ok"}
     timeout { send "QUIT\n" ; puts "Connection lost: connectivity problem or smtp
server? Last recipient:", puts $line; exit}
}
   send "RCPT to: $line\n"
   expect {
     "250"    {puts "ok"}
     timeout { send "QUIT\n" ; puts "Connection lost: connectivity problem or smtp
server? Last recipient:",puts $line; exit}
}
   send "DATA\n"
  expect {
     "354"   {puts "ok"}
     timeout { send "QUIT\n" ; puts "Connection lost: connectivity problem or smtp
server? Last recipient:", puts $line; exit}
}
   send $data1
   send "To: <$line>\n"
   send $data2
   send "\n.\n"
   expect {
     "250"   {puts "E-mail successfully delivered"}
     timeout { send "QUIT\n" ; puts "Connection lost: connectivity problem or smtp
```

```
server? Last recipient:", puts $line; exit}
}
   puts $line
   set line [gets $rcpt_id]
}
send "QUIT\n"
expect "221"
exit
```