

Cosa sono le catene di Sant'Antonio e come imparare ad evitarle



Scritto da Alessandro Sigismondi

lunedì 24 dicembre 2007

Sentiamo ultimamente parlare delle catene di Sant'Antonio, ma effettivamente da che cosa sono e da dove viene originato il nome nessuno sa dare una spiegazione. Facendo una ricerca ho visionato uno dei più autorevoli siti (<http://leggende.clab.it/>) dedicati alle leggende metropolitane, il Centro per la Raccolta delle Voci e delle Leggende Contemporanee, il termine deriva da una tradizione molto diffusa a partire dagli anni Cinquanta del secolo scorso (il 1900): si riceveva una lettera che iniziava con "Recita tre Ave Maria a Sant'Antonio" e proseguiva descrivendo le fortune capitate a chi l'aveva ricopiata e distribuita a parenti e amici e le disgrazie che avevano colpito chi invece ne aveva interrotto la diffusione.

Ai giorni d'oggi invece delle lettere recapitate si utilizzano l'email che è considerato il mezzo più veloce ed economico e devo aggiungere anonimo per inviare messaggi. La catena di sant'Antonio" è un mezzo per diffondere un messaggio inducendo il destinatario a produrne delle copie da spedire, a nuovi destinatari di sua conoscenza.

Tra i gli argomenti più comunemente sfruttati da queste vi sono storie che manipolano le emozioni, sistemi piramidali che promettono un veloce arricchimento e l'uso della superstizione per minacciare il destinatario con sfortuna, malocchio o anche violenza fisica o morte se "rompe la catena" e rifiuta di aderire alle condizioni poste dal messaggio email.

Tra i metodi comunemente sfruttati dalle catene di sant'Antonio vi sono storie che manipolano le emozioni, sistemi piramidali che promettono un veloce arricchimento e l'uso della superstizione per minacciare il destinatario con sfortuna, malocchio o anche violenza fisica o morte se "rompe la catena" e rifiuta di aderire alle condizioni poste dal messaggio.

Le catene di Sant'Antonio che arrivano per e-mail spesso sono fatte partire proprio dagli spammers, (Lo spammers è colui che invia grandi quantità di messaggi indesiderati, generalmente commerciali), con lo scopo di accumulare un gran numero di indirizzi. Infatti, quando si inoltra un messaggio a tutta la rubrica, gli indirizzi vengono elencati in chiaro ed in modo totalmente visibile, e se il messaggio capita tra le mani di uno spammer questi (inclusa l'e-mail del mittente) finiscono nel suo database.

A quel punto tutte le caselle associate a quegli indirizzi vengono tempestate di e-mail indesiderate, con relativo rischio virus. Questi messaggi puntano al lato emotivo del destinatario e sono storie completamente false, inventate o riadattate e la loro diffusione è basata sulla disattenzione dei destinatari, che non verificano con cura le informazioni riportate e, basandosi solo sul fatto che conoscono la persona da cui hanno ricevuto il messaggio, lo girano immediatamente ai loro contatti nella rubrica.

Faccio un appunto su come funziona l'invio dell'email: Quando si spedisce una e-mail da un computer ad un altro attraverso la rete, ciò che succede non è la semplice copia di un file di testo da un disco fisso ad un altro. La principale differenza è che, oltre ai due computer mittente e destinatario, ne sono coinvolti anche altri. Un primo computer che non si vede è quello ove risiede la casella del destinatario.

Questo computer, che deve essere per quanto possibile sempre attivo e accessibile in rete, ha il compito di ricevere tutte le e-mail dirette agli utenti che hanno la casella su di esso e conservarle finché ciascun destinatario, con suo comodo, non avrà provveduto a scaricarle. Spesso ci si riferisce a tale computer come POP server. Il mittente, così come il destinatario, sul proprio computer dispone solamente di un client di posta elettronica, ossia un programma in grado di gestire un archivio di e-mail (in arrivo e in partenza), di scaricare la posta in arrivo da un POP server e spedire posta tramite protocollo denominato SMTP. Le catene di Sant'Antonio sono legate a filo doppio ad altri fenomeni tristemente noti di internet, come lo spam, le "bufale" (hoax), virus o i cosiddetti "sistemi piramidali". Questi messaggi sono anche chiamati "chain letter" tradotta significa "lettera a catena" (una lettera inviata a un certo numero persone con la richiesta che ciascun destinatario la invii a sua volta a un uguale numero di persone) che è un concetto molto evoluto della classica "catena di Sant'Antonio". Come riconosce i messaggi: l'esca serve a catturare l'attenzione del lettore, che viene così indotto a proseguire fino alla fine del messaggio. Le trappole possono essere richiami come "Make Money Fast" ("Come fare soldi in poco tempo") oppure "Get Rich" ("Come arricchirsi") o altre frasi legate all'idea di fare soldi in fretta e senza troppo lavoro. Altre trappole molto sfruttate sono frasi del tipo "Danger!" ("Pericolo!") e "Virus Alert" ("Allarme Virus") oppure "A Little Girl Is Dying" (una bambina che sta morendo). Queste trappole fanno appello al nostro timore di avere problemi al computer e al nostro buon cuore verso chi soffre. Si tratta ormai di un fenomeno ricorrente: avvisi di presunti virus che arrivano a priorità alta e pre-annunciano la totale distruzione di un sistema infettato. Il messaggio di solito è una e-mail inoltrata decine di volte, e vi viene spedita da un conoscente, acquistando così maggiore credibilità. Altro tipo di truffa. Riporto i temi più ricorrenti utilizzati per generare questo tipo di email

1) la classica "lettera portafortuna", spesso corredata da un breve testo educativo e buonista

2) la richiesta di aiuto per bambini gravemente malati

3) cuccioli da salvare

4) notizie sconvolgenti provenienti da un'altra nazione da diffondere al più presto

5) la promessa di un facile e rapido arricchimento

6) la minaccia di sfortuna o di morte

7) l'eredità che aspetta di essere condivisa proprio con te

8) un file nascosto sul tuo PC assolutamente da cancellare perché è un virus a tempo 9) appelli umanitari o allarmi per ipotetiche emergenze sanitarie. Di sicuro ne ho dimenticata qualcuna, ma penso vi siate fatti un'idea di massima... Quali sono gli avvertimenti da utilizzare quando riceviamo questo tipo di email nella nostra casella:

- per prima cosa non dobbiamo mai rispondere alle email poiché se si risponde, oltre ad installare nel nostro pc un eventuale e certo virus, facciamo esattamente il gioco di chi le ha mandate

- Non eseguire MAI alcuna istruzione data nel messaggio (es. Reply REMOVE)

- Utilizzare sempre antivirus e antispam aggiornati. Se qualche lettore vuole chiarimenti o proporre argomenti mi può scrivere all'indirizzo email a.sigismo@gmail.com