

TECNICHE di social engineering

Social engineering, ingegneria sociale. Il termine è quello che è, pomposo è il meno che si possa dire. Due cose però sono certe: la prima è che per carpire delle informazioni la tecnologia da sola non basta più; l'altra è che l'arte dell'inganno si sta diffondendo a macchia d'olio

Di Giuseppe Badalucco

Sembra preistoria ma sino a pochi anni fa i virus si trasmettevano da un Pc all'altro attraverso floppy disc infetti. Malware era un neologismo sconosciuto e comunque i danni che del codice dannoso poteva arrecare erano limitati; pochi i Pc connessi in rete, limitate le risorse e gli applicativi disponibili, inesistenti o quasi le difese. Oggi le co-

se sono cambiate. Siamo entrati in una fase in cui la pericolosità del malware è aumentata in maniera esponenziale; basta confrontare un attacco sferrato oggi con uno di qualche anno fa. Come numerosi indizi sembrerebbero confermare, la loro natura è cambiata; da una parte più potenze¹, precisione² e maggiore rapidità di diffusione³; dall'altra maggiore di-

sponibilità di mezzi e di strumenti evoluti da parte della criminalità organizzata⁴. «I laboratori TrendLabs hanno registrato un aumento del 2.000% delle minacce Web dall'inizio del 2005 alla fine del 2008; il 90% di tutte le minacce digitali, infatti, sfrutta il Web come veicolo di propagazione», afferma **Carla Targa**, marketing manager Trend Micro Italy

¹ Vedi in <http://www.nytimes.com/2008/11/10/technology/internet/10attacks.html> e <http://asert.arbournetworks.com/2008/11/2008-worldwide-infrastructure-security-report/>.

² Vedi in <http://www.securitywatch.co.uk/2008/04/18/browser-attacks-becoming-more-sophisticated-say-experts/> e in <http://www.securitywatch.co.uk/2008/10/08/poisoning-of-dns-caching-gets-worse/>.

³ Vedi per esempio in http://www.theregister.co.uk/2009/06/08/webhost_attack/.

⁴ Vedi in <http://www.e-commercalert.com/article907.shtml> e in <http://www.securitywatch.co.uk/2008/07/16/finjan-says-cybercrime-more-successful-and-profitable-than-ever/>.



(<http://it.trendmicro.com/it/home/>), secondo la quale insieme al volume è cresciuto anche il livello delle minacce. Sulla stessa lunghezza d'onda **Antonio Forzieri, principal consultant di Symantec** (www.symantec.com/it), che sottolinea come le ricerche e il monitoraggio di questi fenomeni «evidenziano un trend in costante crescita ed evoluzione: ogni giorno si assiste alla nascita di minacce sempre più invasive e sempre più complesse. Basti pensare che nel solo 2008 è stato individuato il 60% del codice malevolo esistente»; **Domenico Fusco, direttore vendite Panda Security** (www.panda-security.com/italy) rileva come «dal maggio del 2009 i database dei nostri laboratori contavano circa 26 milioni di esemplari di malware, ben 11 milioni in più di quelli rilevati l'anno scorso». Di diverso avviso **Marco Misitano, business development manager Ict & physical security di Cisco Italy** (www.cisco.com/it), secondo cui «i dati in nostro possesso ci suggeriscono che non c'è stato tanto un aumento esponenziale delle minacce quanto un aumento della loro sofisticazione unita a una maggiore precisione nel colpire i bersagli». Senza dubbio come nota **Fabrizio Cassoni, pre-sales engineer, Technological department di Symbolic** (www.symbolic.it), non esiste una correlazione diretta tra diffusione di una minaccia e livello tecnologico che essa incorpora; spesso si tratta solo di varianti dello stesso ceppo di malware; l'eccezione alla regola è stato Downadup (alias Conficker), un malware ben congegnato e diffusosi enormemente. «Probabilmente ognuno di noi valuterà in modo differente la qualità di un codice maligno - puntualizza Cassoni -: l'analista esaminerà con attenzione lo stile di programmazione del virus writer, l'amministratore di rete imparerà a temere i worm semplici, ma velocissimi a diffondersi, l'utente finale che è il



Carla Targa
marketing manager
di Trend Micro Italy



Antonio Forzieri
principal consultant
di Symantec

Ogni giorno nascono minacce più invasive. Nel solo 2008 è stato individuato il 60% del malware esistente

più esposto agli effetti di un malware, sarà portato a credere che il programma più maligno è quello che gli distrugge i dati o gli sottrae le informazioni confidenziali».

ATTACCHI DAI SITI DI SOCIAL NETWORK

Gli attacchi riflettono tendenze, livello di conoscenze, entità dei mezzi a disposizione e così via; dalla loro intensità e quantità si possono trarre considerazioni molto interessanti. Come abbiamo visto possono esserci differenze anche sostanziali di interpretazione circa la loro diffusione e efficacia. Ora non si tratta di stabilire se, come sostengono alcuni recenti rapporti, spam e spyware sarebbero ormai minacce superate sia dall'affermarsi di nuove tecnologie sia soprattutto dalla diffusione e dall'affinamento delle tecniche di social engineering. Piuttosto è sotto gli occhi di tutti come il boom dei siti di social network abbia avuto conseguenze importanti sulle tecniche di attacco. Non si tratta

di un fenomeno isolato. In generale per carpire informazioni e infettare i computer si tende a utilizzare quali vettori di propagazione siti molto visitati e/o affidabili, fenomeno questo, come nota **Massimiliano Graziani, security manager di Visiant Security** (www.visiantsecurity.it), agevolato dal fatto che «oggi chi attacca non modifica l'aspetto della pagina; inserisce semplicemente del codice capace di carpire informazioni o infettare gli utenti che hanno un sistema vulnerabile». La natura interattiva dei siti più diffusi di social network è resa possibile dall'impiego di tecnologie e applicativi di cui possono servirsi anche i malintenzionati. Se non tutti concordano nel dire che il volume delle minacce Web è aumentato, tutti riconoscono che è cresciuto il loro livello di sofisticatezza. «Oggi gli attacchi contengono diverse tipologie di malware, un cocktail virtuale delle migliori tecniche e di social engineering il cui scopo è colpire gli utenti su diversi fronti», ci dice **Carla Targa** di Trend Micro Italy. Per apprezzarne l'evoluzione basta leggere come uno dei pionieri del social engineering sfruttava le debolezze umane non più tardi di quindici/venti anni fa⁵. Cresce il numero di dati che gli utenti decidono di metter online; così come l'utilizzo di applicativi che accrescono l'esperienza di network condiviso da parte degli utenti. Grazie alla disponibilità di una mole senza precedenti di informazioni gli attacchi sono sempre più mirati e personalizzati e si prestano a incorporare la componente social engineering, ormai diventata irrinunciabile nella progettazione di tool e tecniche di intrusione⁶. Prendiamo per esempio lo spam. Secondo alcuni esperti questo metodo d'attacco diventa ogni giorno di più "socialmente ingegnerizzato". Le mail fasulle sono sempre più simili alle mail che la banca o il provider pre-

⁵ K. D. Mitnick, L'arte dell'inganno, Feltrinelli, 2003.

⁶ Come dimostra questo articolo su Conficker in <http://isc.sans.org/diary.html?storyid=5695>

so di mira potrebbe davvero inviare al malcapitato cliente. Mail scambiate per genuine perché contenenti informazioni ritenute credibili dalla vittima, come per esempio la nostra vera data di nascita oppure il numero di conto corrente. La diffusione dei social network alimenta la popolarità delle tecniche di social engineering; il loro utilizzo, consentendo di ottenere guadagni sempre più elevati, è garanzia di diffusione. Secondo alcuni esperti questi attacchi, se già non lo sono, diverranno presto virtualmente impossibili da identificare da parte degli utenti: «Le truffe di phishing, gli attacchi mossi via email, trojan horse e altri attacchi arrivano a essere così personalizzati che persino l'occhio più attento potrebbe cadere nella trappola ben orchestrata del social engineering», questo, per esempio, sostiene **Jeff Green, senior vice president, McAfee Avert Labs.**

IL PROBLEMA SOCIAL ENGINEERING PER AZIENDE E ISTITUZIONI

Il social engineering è un attacco portato contro le persone che fanno parte di un'organizzazione, non contro la tecnologia che la stessa impiega. Il malintenzionato fa leva sulle emozioni, paura, avidità, compassione, curiosità. Si serve dell'inganno per adescare le vittime e carpire informazioni personali. Il raggio d'azione delle tecniche di social engineering è ampio: dipendenti e dirigenti; partner dell'azienda e clienti. Il social engineering trae enormi vantaggi da eventi come le Olimpiadi, le calamità naturali, le elezioni politiche. Le tecniche sono in continua evoluzione. L'obiettivo invece non cambia. Come sappiamo le e-mail di phishing sono uno degli strumenti più utilizzati per applicare le tecniche di social engineering. Per esempio un malintenzionato genera un account su un mail server anonimo dal quale invia un messaggio praticamente identico a quello che potrebbe provenire dal si-



Domenico Fusco
direttore vendite
di Panda Security



Marco Misitano
business development
manager Ict & physical
security di Cisco Italy

Il boom dei siti di social networking ha avuto conseguenze ampie e importanti sulle tecniche di attacco

to preso di mira, riproducendone fedelmente lo stile, il layout, la firma di un responsabile, richiedendo al malcapitato di digitare una coppia di credenziali per autenticarlo prima di farlo accedere al proprio conto, fasullo. Altre volte l'informazione non viene neppure richiesta; si preferisce cercare di convincere l'utente a scaricare ed eseguire un programma capace di sottrarre un certo dato direttamente dal computer. Anche il vecchio telefono continua a essere uno strumento molto utilizzato. Per esempio si viene contattati da un falso tecnico che con la scusa di dover effettuare una manutenzione cerca di impadronirsi, se non proprio delle credenziali di accesso al conto in banca, almeno di qualche informazione preziosa per arrivare a obiettivi altrettanto remunerativi. Ma anche il semplice gironzolare all'interno di un ufficio può essere sufficiente a un occhio allenato per impossessarsi di informazioni preziose, magari appuntate sul monitor di un'impiegata smemorata. Per sferrare un attacco di successo occorre disporre delle informazioni giuste. Spesso anche un semplice dipenden-

te può essere a conoscenza di informazioni preziose: password, numeri di telefono, indirizzi e-mail, locazione degli allarmi e così via. Tuttavia come rileva **Filippo Silvestri, sales account Intergraph Italia LLC** (www.intergraph.it), «è in contesti complessi, dove l'operatore o il team oggetto di aggressione è mediamente un soggetto preparato, professionalmente e culturalmente, che il social engineering raggiunge livelli di raffinatezza davvero notevoli. E più tale contesto è elevato ed esclusivo, più la minaccia diviene pericolosa». Non c'è limite alla mole di informazioni che un malintenzionato dotato di una qualche conoscenza e faccia tosta può ottenere. Certo per fare bingo occorre essere in grado di instaurare un rapporto amichevole, conquistare quel minimo di fiducia e familiarità che consentiranno presto o tardi di carpire le informazioni giuste. Non si deve credere che si tratti di doti di cui sono pochi a disporre. D'altra parte non occorrono le stesse qualità per trovare un impiego o conoscere una ragazza?

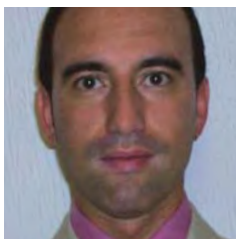
DIFESE INCENTRATE SU PERSONE E TECNOLOGIE

Come abbiamo visto le tecnologie e i metodi utilizzati per gli attacchi sono sempre più sofisticati, evolvono rapidamente e costringono a mantenere elevata la soglia di attenzione. Perciò i crimini informatici riconducibili ad attacchi "socialmente ingegnerizzati" devono essere fronteggiati a diversi livelli; in primo luogo per poter rispondere all'evoluzione delle minacce è necessario adattare dinamicamente le proprie politiche di sicurezza e aggiornare periodicamente le proprie tecnologie di sicurezza. «L'impiego di strumenti che rendono più semplice l'amministrazione dei sistemi permette di liberare risorse che potranno più utilmente essere impiegate in attività di gestione e controllo della sicurezza minimizzando così il rischio di

errori umani», afferma **Emilio Turani**, country manager di Stone-soft Italia, Grecia, Svizzera Italiana e Turchia (www.stonesoft.com/it). Un unico investimento su una sola tecnologia non è più sufficiente: «Il fronte della difesa deve ampliarsi con differenti sistemi di controllo che possano monitorare e, se necessario, reagire alle nuove minacce», ci dice **Massimiliano Graziani** (Visiant Security). **Marco Misitano** (Cisco) invece sottolinea che, sebbene le minacce sono diventate più sofisticate, «è possibile contrapporre tecnologie di prevenzione e protezione sempre più raffinate e alla portata anche delle aziende di medie e piccole dimensioni». La capacità di andare oltre il semplice monitoraggio e di visualizzare lo stato dell'infrastruttura è l'approccio che, come sottolinea **Turani** (Stonesoft), meglio si adatta a questi scenari mutevoli, «dove anche le attività di social engineering si concretizzano in atti e minacce rilevabili da strumenti di intrusion prevention e detection, capaci di cogliere l'anomalia o di offrire all'intelligenza umana gli elementi per identificarla con successo e prontezza». Naturalmente anche il singolo utente può e deve collaborare attivamente. In primo luogo occorre prestare la necessaria attenzione nell'utilizzo del computer e nella navigazione su Internet; «adottare le tecnologie di protezione più avanzate non basta: è necessario, infatti, che siano affiancate da una maggiore consapevolezza dei rischi a cui si è esposti, prevenire comportamenti scorretti causati da utenti malintenzionati o semplicemente distratti», sostiene **Antonio Forzieri** di Symantec. Occorre altresì fare attenzione a offerte, inviti e quant'altro ricevuti via e-mail o tramite reti di social networking, che suonino troppo allettanti o vantaggiosi. Inoltre è necessario fare propri alcuni comportamenti di prudenza, soprattutto sul luogo di lavoro. Pur tenendo sempre in considerazione che la sicu-



Emilio Turani
country manager
di Stonesoft Italia, Grecia,
Svizzera Italiana e Turchia



Rossano Ferraris
research engineer
della divisione Internet
Security Intelligence di CA

Persino l'occhio più attento e vigile potrebbe cadere nella trappola ben orchestrata del social engineering

rezza totale è irraggiungibile, si possono applicare contromisure al fine di ridurre i rischi. «Gli utenti devono considerare approcci multivalenti per combattere il malware e dotarsi di software anti malware che comprenda diverse componenti come antivirus, anti spam, anti spyware, intrusion prevention e Web filtering», ci dice **Rossano Ferraris**, research engineer della divisione Internet Security Intelligence di CA (www.ca.com/it).

L'ANELLO DEBOLE

Contrariamente a quanto si crede è difficile tenere il passo con l'evoluzione della tecnologia. Solo apparentemente ci si abitua ai cambiamenti che introduce; ed è una pia illusione credere che le innovazioni siano velocemente metabolizzate nel quotidiano. Se vogliamo ciò è ancor più evidente nel settore della sicurezza, in cui a fronte di un'escalation continua di minacce sempre più sofisticate sembrerebbero contrapporsi risposte efficaci e tempestive in grado di contrastarle. In effetti, qualunque sistema, e ancor più quelli che sovrintendono alla sicurezza fisica e logica, sono pensati per evitare

quanto più possibile errori o omissioni. Ma tale limite non può essere spinto all'eccesso, pena la decadenza dell'attività dell'anello debole del sistema, l'uomo. È in contesti complessi dove l'operatore è mediamente più preparato, professionalmente e culturalmente che si insinua il social engineering. E' in questa faglia che le conseguenze possono essere particolarmente gravi. Tuttavia la maggiore conoscenza del fenomeno permette notevoli progressi nell'individuazione delle tecniche di difesa; e non v'è dubbio che questa conoscenza lungi dall'essere patrimonio dei soli analisti o dei vertici aziendali, vada condivisa a tutti i livelli dell'organizzazione attraverso interventi formativi mirati. Ora tutti a parole concordano nel dire che la formazione del personale è importante per contrastare il social engineering. Ma in quante aziende la formazione è più un dovere da espletare spendendo il minimo possibile e la prima voce di spesa a essere tagliata appena compaiono le prime nuvole nere? La formazione quale progetto da seguire con attenzione è una mera chimera in tante realtà aziendali. In qualunque processo e dunque anche in quelli legati all'implementazione della sicurezza It le persone intervengono in modo significativo. L'efficacia dei sistemi di sicurezza è strettamente correlata alla linearità dei processi produttivi, alla corretta identificazione di ruoli e responsabilità, all'entità degli investimenti messi a budget. Nella realtà però le cose vanno diversamente. Per esempio la mera formalizzazione delle procedure non è di per sé garanzia di efficacia. Il mondo è pieno di aziende certificate strutturate su procedure tanto belle quanto disapplicate. Disattendere una procedura può essere più pericoloso che non averla proprio. Il rischio si ingigantisce, perché si danno per scontati comportamenti senza che nessuno li verifichi. Non ci sono patch per l'uomo. Ma non ci sono neppure scorciatoie per le aziende. **DM**