2. Furto d'identità nuova frontiera del crimine organizzato

Il danno causato dai nuovi troiani è maggiore del phishing: si parla di **"furto d'identità"** come nuova frontiera della delinquenza informatica. È possibile, quindi, non solo perdere il denaro sul conto corrente online, ma diventare vittime di truffe gravi: organizzazioni criminali clonano carte, chiedono mutui e prestiti, fanno acquisti usando identità false. Il malcapitato può essere coinvolto, a sua insaputa, in crimini come la pedofilia e la pornografia. È capitato anche personaggi molto noti tra cui il presidente della repubblica francese, Nicolas Sarkozy e giornalisti famosi come Vittorio Zucconi. Non è un caso se come primo atto di sicurezza per il nuovo Presidente USA, gli è stato proibito l'uso di Internet e del suo fedele Blackberry.

Secondo il centro anticrimine di **Poste Italiane**, oggi le organizzazioni criminali riescono a rubare denaro in meno di 1 minuto grazie alle sinergie tra conto online, carte prepagate bancarie e carte prepagate telefoniche. Ma per il furto d'identità i tempi si accorciano ancora di più: **secondo i tecnici RSA** oggi il mercato dell'identità rubata è fiorente e utilizza forum, chat e community spesso insospettabili per vendere e acquistare identità, software maligno (Scam), numeri di carte di credito e così via. Un mercato, quello delle identità rubate, che si avvale della complicità di una fitta rete di persone che lavorano come addetti alle pulizie per grandi società, banche, istituzioni pubbliche, anche e soprattutto di origine straniera, e con scarso o nessun controllo da parte degli organi di sicurezza privati o della polizia. Per **Symantec,** nel suo ***Report on the Underground Economy***, i primi dieci operatori del cyber crimine hanno guadagnato nel 2007 circa 276 milioni di dollari a testa, per un giro d'affari complessivo che sfiora i 7 miliardi di dollari. Mentre il **Security Report di Cisco**, grazie alle informazioni dalle Cisco Security Intelligence Operations, ha evidenziato a fine 2008 che il numero totale delle vulnerabilità scoperte è cresciuto dell'11,5% rispetto al 2007, mentre le vulnerabilità nelle tecnologie di virtualizzazione, che sono quelle che maggiormente impattano sul pubblico domestico, sono quasi triplicate passando da 35 a 103 anno su anno. Gli attacchi stanno diventando sempre più misti, multi-vettore e mirati. In compenso, il volume di malware propagato con successo tramite allegati alle e-mail, il phishng,

sarebbe in calo: negli ultimi due anni (2007-2008), il numero di attacchi inviati in allegato è sceso del 50% rispetto al biennio precedente (2005-2006)[24].

Le community del crimine

Gli strumenti in mano alla polizia, inoltre, sono scarsi, sia in tecnologia che in persone addette, mentre il fenomeno del crimware è in crescita esponenziale, spinto anche dal basso costo dell'investimento necessario ad operare come criminale informatico: bastano, a volte, un computer di un Internet cafè in Nigeria o in Russia, 25 dollari per acquistare un virus, altri 30 per un elenco di identità rubate, meno per un elenco di email e numero di carte di credito clonate. Il ricavo in tempi rapidissimi, meno di un minuto, varia dai 1000 ai 3000 dollari che soprattutto per chi abita in Africa o negli ex paesi del blocco sovietico rappresentano una vera fortuna. I derubati spesso non si accorgono di nulla, perché le cifre sottratte sono molto piccole, anche di qualche decina di dollari ed euro a testa. Se per **Poste Italiane** solo il 63% di frodi online viene individuato e bloccato, per ABI la percentuale relativa a tutto il comparto bancario scende al 39%. Nel 2008, la Polizia postale ha effettuato 7 arresti, l'anno precedente 4 mentre nel 2006, primo anno di effettiva attività investigativa a livello nazionale, gli arresti erano stati nulli. Tutto questo mentre sale del 100% il numero di denunce e di segnalazioni. La legislazione nazionale è carente: chi viene arrestato subisce condanne pari a un massimo di 5 anni e viene quindi arrestato "a piede libero", in pratica è libero di perpetuare la frode, grazie anche a una versa e propria

[24] Le minacce più diffuse per Cisco sarebbero, al primo posto lo Spam. Per il team di Cisco si contano circa 200 miliardi di messaggi di spam ogni giorno, circa il 90% delle email inviate a livello globale. Gli Stati Uniti ne sono la fonte maggiore, con il 17,2%. Tra le altre Nazioni che contribuiscono allo spam vi sono Turchia (9,2 %), Russia (8 %), Canada (4,7 %), Brasile (4,1 %), India (3,5 %), Polonia (3,4 %), Corea del Sud (3,3 %), Germania e Regno Unito (2,9% ciascuna). Al secondo posto, c'è il Phishing, mentre gli attacchi mirati di spear-phishing rappresentano circa l'1% di tutti gli attacchi di phishing, Cisco prevede che questo dato sia destinato a crescere in quanto i criminali personalizzano lo spam e creano messaggi che appaiono sempre più credibili. Le botnet, al terzo posto, sono diventate un insieme di attività criminali su Internet. Nel 2008, svariati siti Web legittimi sono stati infettati con IFrames, un codice dannoso iniettato da botnet che reindirizzavano i visitatori verso siti da cui scaricare malware. L'uso del social engineering è il quarto trend della sicurezza: le community sono utili per spingere vittime ad aprire file o cliccare su link specifici continua a crescere. Cisco prevede che nel 2009, le tecniche di ingegneria sociale aumenteranno in termini di numero, vettori, e sofisticatezza. Inoltre, sempre più spesso i criminali informatici ricorrono a veri account e-mail con grandi fornitori di servizi di posta elettronica legittimi per inviare spam (Reputation hijacking). Questo "dirottamento della reputazione" offre una maggiore garanzia di ricezione dello spam perché lo rende più difficile da rilevare e bloccare. Secondo Cisco, nel 2008 lo spam risultante da questo "dirottamento di reputazione" delle e-mail dai maggiori fornitori di posta elettronica ha rappresentato meno dell'1% di tutto lo spam a livello globale, ma al tempo stesso il 7,6% del traffico dei provider di e-mail.

"community" del crimine fatta di "amici" o per meglio dire di "complici" che utilizzando strumenti del Web 2.0., si scambiano informazioni, dati, nuove idee per perpetuare i loro crimini.

Per l'Home Banking, la nuova crisi legata al furto d'identità con troiani, che Of-Osservatorio finanziario aveva già annunciato nel precedente Rapporto Banca Più sicura (aprile 2007- Leggi qui), ha prodotto una perdita economica cospicua, non solo a causa di truffe riuscite, ma soprattutto a causa del timore da parte di utenti poco esperti. Si parla di un **raffreddamento dell'entusiasmo** e interesse verso un servizio che è, al contrario, ormai maturo e ricco di opportunità. Chi usa l'online, rimane sul web per pochi minuti, necessari a svolgere quell'operazione e non "naviga" in giro per provare nuovi servizi o raccogliere altre informazioni. Il numero di utenti è cresciuto - sono circa due milioni e mezzo di utenti che usano il conto almeno una volta la settimana, per poco più di 13 milioni di conti online "puri" (che sono circa 1,7 milioni a fine 2008) sommati ai conti correnti tradizionali abilitati al servizio e-banking - ma a scapito del tempo di accesso ai servizi che è, in proporzione, calato del 33%. Mentre sono aumentati del 141% le interrogazioni al cellulare nelle due tiplogie, quella pull, per ricevere avvisi in modo automatico e quella pull, per richiedere il saldo oppure per effettuare ricariche o in alcuni casi anche pagamenti e bonifici.

I clienti vogliono sentirsi sempre più sicuri e vogliono essere rassicurati. Come ammette anche l'esperto internazionale di sicurezza **Bruce Schneier**, la sicurezza è molto spesso più un problema di percezione (*feeling*), che di realtà (*reality*). La paura nasce da una scarsa conoscenza del mezzo: il **digital divide** in Italia è ancora molto elevato e, sorprendentemente, cresce soprattutto tra i più giovani, grandi utilizzatori di cellulari e videogiochi, ma molto meno di computer e Internet.

Il dipendente bancario prima cavia anti-crimine

C'è poi anche il problema legato al cosiddetto **"ventre molle" delle banche** che sono i dipendenti**: l'intranet bancario** si è rivelato un "Giano bi-fronte". Da un lato costringe il dipendente ad utilizzare Internet come primo canale informativo relativo alla propria attività, e questo fa crescere la conoscenza nel nuovo media; ma dall'altra parte offre a un vasto uditorio ancora poco preparato la possibilità, purtroppo non remota, di essere complice di truffe phishing. Of non ha studiato la sicurezza legata ai servizi **Intranet bancario**, ma segnala che in quest' ambito le banche hanno fatto massicci investimenti in sicurezza proprio a causa di alcune falle

che, sembra, per fortuna, non abbiano creato seri problemi. Al contrario sono serviti per provare (*testing*) i sistemi di sicurezza della banca.

C'è quindi un nuovo aspetto da tenere in considerazione quando si tratta di sicurezza: **l'irrazionalità**. L'Home banking è un servizio sempre più apprezzato quando la banca che lo offre è anche capace di coinvolgere il cliente rassicurandolo sulle proprie capacità di gestione del servizio. La facilità d'uso, la **protezione del brand**, cioè l'accuratezza con cui una banca protegge il nome del proprio servizio acquistando tutti i possibili suffissi (non solo .it, ma soprattutto .com, .org, .net, .eu e così via) e disegna le proprie pagine web certificandole secondo standard internazionali, la buona comunicazione in tema di sicurezza fino allo sviluppo di vere e proprie community dove trovare "amici di banca" che aiutino ad usare meglio il proprio conto online in modo rilassato e, appunto, "amichevole", sono punti d'osservazione aggiuntivi che riguardano il **modello sicurezza bancario**, oltre, ovviamente, alla tecnologia.

Il **phishing è, d'altra parte, non proprio dietro le spalle**, anzi. Le organizzazioni internazionali di truffatori informatici utilizzano il sistema delle e-mail false in modo industriale: è, infatti, un metodo sicuro per "pescare" anche piccoli importi su un numero molto vasto di utenti in modo semplice, veloce e soprattutto poco costoso. Uno dei problemi riguarda la velocità: il criminale è tanto più veloce, quanto sono lenti i sistemi di rilevazione della truffa e, soprattutto, la macchina giudiziaria in grado di scovare e punire i colpevoli. L'Italia è il terzo paese al mondo più bersagliato dal phishing, con 9 istituti finanziari colpiti da 296 attacchi nel solo mese di ottobre 2008 provenienti da Stati Uniti, Cina e Russia. L'Anti-Fraud Command Center (AFCC) **di RSA** segnala anche che ad infettare maggiormente sono codici maligni, chiamati botnet, iniettati con il code injection verso data base Microsoft MSQL server 2000 e 2005. In pratica, questi botnet si installano nei Pc di utenti ignari che diventano a loro volta centri di infezione per altri computer. Sempre gli esperti di RSA rilevano che più di 100 mila istituti finanziari globalmente sono stati colpiti dal fenomeno dei virus troiani dal marzo 2008, con una vera e propria impennata del numero degli attacchi proprio nei primi mesi di quest'anno. [25]

La sicurezza bancaria oggi deve essere necessariamente multicanale: solo un sistema che autentichi su due canali, web e filiale, web e telefono o cellulare, è in grado di essere chiamato

[25] Il troiano peggiore si chiama Sinowal Trojan che dal 2006 al 2008 è riuscito a rubare oltre 250 mila carte di credito e di debito e più di 300 mila dati di accesso ad altrettanti conti correnti e di deposito e trading.

sicuro. Non lo è nemmeno il sistema adottato da banche molto importanti, cioé la autenticazione doppia con password mono uso con token, perché già oggi si sono registrate le prime truffe capaci di dirottare il cliente su siti clone e di carpire anche le password temporanee. Si tratta, per fortuna, di casi isolati e che non hanno colpito nessuna banca nazionale.

D'altra parte, l'Home Banking in Italia è ancora un fenomeno marginale, se pure in rapida crescita: banche online storiche come **Fineco** e **We@bank**, oggi diventata banca a tutti gli effetti, non raggiungono i 100 mila utenti, mentre **UniCredit Banca** e **Intesa Sanpaolo**, pur offrendo servizi Home Banking sempre più ricchi di servizi, hanno affrontato spese elevate per mettere a disposizione sistemi ATM intelligenti e desk con terminali all'interno delle loro filiali, ben sapendo che Internet è considerato quasi un "gadget" dai loro clienti. **Unicredit Banca** ha anche attivato filiali di nuovo tipo, **AgenziaTu**, una specie di **banca nella banca**, dove il canale web è unito in modo completo al canale fisico, adattandolo ad un pubblico di giovani e immigrati molto interessati alla banca low cost e soprattutto sempre disponibile 24 ore al giorno. Una evoluzione di ciò che è stato già sviluppato tre anni fa dal gruppo **Monte Paschi di Siena** in alcune filiali. E che sta interessando numerose banche territoriali tra cui la **Friuli Adria e alcune BCC.**