Dal computer crime al computer-related crime

Antonio Apruzzese[1]

Riassunto
Il "furto dell'identità digitale" è oggi divenuto uno dei più lucrosi affari criminali. Noto ai più come *phishing* consiste nella sottrazione dei riservati dati di accesso ai conti di utenti del servizio bancario on line. In un primo momento vittime dirette dei raggiri erano le persone, oggi lo sono diventati gli stessi computers. Pharming e keylogging sono solo alcune delle nuove sofisticatissime tecniche informatiche utilizzate dai criminali. Ultime arrivate le botnet, "mandrie" di computer infettate e gestite da unici centri di comando, che possono determinare gravissimi danni nel sistema della rete e favorire l'esecuzione di furti di identità digitale su larga scala. La criminalità organizzata è sempre più coinvolta in questo nuovo mondo criminale che assicura enormi guadagni. Per rispondere alla nuova difficile sfida epocale la Polizia di Stato italiana ha costituito nella Polizia Postale e delle Comunicazioni una agenzia di contrasto ad alta specializzazione.

Abstract
Nowadays, Digital Identity Theft has become one of the most lucrative illegitimate business. Also known as "phishing", it consists in unauthorized access to an individual's personal financial data aiming to capture information relative to on line banking and on line financial services. At the beginning people were the victims of such scams, currently the attention is directed to computer networks. "Pharming" and "keylogging" are some of the latest and utmost sophisticated data processing techniques used by computer crime fraudsters. Latest entries are the "botnets", herds of infected machines, usually managed by one sole command centre which can determine serious damages to network systems. Botnets have made large scale identity theft much simpler to realize. Organized crime is becoming more and more involved in this new crime world that can easily assure huge profits. The Italian State Police, in order to respond more effectively to this new rising challenge, has created, with the Postal and Communication Police, an agency highly specialized in combating such new phenomenon.

1. Introduzione.

[1] Primo Dirigente della Polizia di Stato, dirige il Compartimento della Polizia Postale e delle Comunicazioni dell'Emilia Romagna a Bologna. Con una decennale esperienza di Polizia Giudiziaria coordina le attività operative della Specialità della Polizia di Stato impegnata nel contrasto dei crimini informatici, della pedofilia on line e nella tutela delle comunicazioni.

La criminalità informatica ha evidenziato recentemente fenomeni evolutivi sino a poco tempo addietro assolutamente impensabili.

Le sempre più vaste e vantaggiose offerte di servizi on line interessanti oramai tutti gli aspetti della vita sociale (si pensi ad esempio all'*e-learning*, *all'e-governement* per finire all'*e-commerce*) sono diventate il terreno preferito di nuove scorribande criminali che vedono nel raffinato *know-how* tecnologico un dirompente cavallo di battaglia.

Il ben noto fenomeno del *phishing* ha portato recentemente all'attenzione dell'opinione pubblica nuove forme di criminalità informatica che hanno come comune obiettivo i sempre più diffusi servizi bancari on line e, più in generale, il così detto "furto di identità digitale".

La pervasività e la gravità del fenomeno appaiono tali da far temere l'insorgere di diffuse sensazioni di insicurezza nell'oramai foltissimo novero degli utenti.

Elemento caratterizzante di tali fenomenologie criminali è sostanzialmente il così detto "furto dell'identità" digitale (*identity theft*) delle vittime, vale a dire l'insieme dei dati riservati che consente l'accesso e la disponibilità dei conti bancari gestiti in forma telematica.

Da forme frodatorie in cui la evidente "leggerezza" della vittima giocava un ruolo cardine nell'agevolare la conclusione dell'iter truffaldino (*phishing* originario) si sta progressivamente passando a nuovi stadi (*pharming e key logging*) in cui il "furto" dell'identità digitale prescinde del tutto da atteggiamenti "colpevolmente negligenti"del derubato vedendo in sostanza vittima diretta dell'inganno la stessa macchina.

Si è in definitiva proiettati verso nuovi scenari in cui l'alta capacità tecnico-informatica appare sempre più un temibile strumento operativo di agguerrite organizzazioni criminali.

2. Phishing , Pharming , Key Logging e Botnet.

L'avvento del "nuovo evo " della criminalità informatica ha effettivamente avuto le sue prime concrete avvisaglie col diffondersi sempre più ampio dei fenomeni di *phishing*.

Il termine gergale, coniato dai praticoni dell'informatica e ricavato dall'inglese to fish – pescare, richiama con tutta evidenza il pesce che abbocca ad un'esca ben preparata.

Nella sua forma originaria si concretizzava nell'invio ai fruitori dei servizi bancari on line di e-mail trappola, apparentemente provenienti dagli istituti di credito, con l'invito, giustificato dalla necessità di procedere a verifiche della sicurezza dei sistemi, a digitare i riservati dati (*user name e password*) di accesso al conto telematico.

Gli inviti rinviavano a pagine web riproducenti con elevata verosimiglianza i reali siti delle banche interessate.

L'incauto correntista on line che abboccava all'esca veniva così derubato della sua "identità digitale" bancaria e i suoi conti poco dopo consistentemente alleggeriti.

Quale leggerezza o negligenza imputare però all'ignaro correntista on line che nel tentativo di connettersi al sito della sua banca viene automaticamente dirottato verso i siti esca allestiti dai criminali?

E' la ricorrente ipotesi del temibile *pharming* incentrato sulla alterazione delle procedure di risoluzione dei così detti nomi a dominio (*domain names*) che associano agli effettivi indirizzi digitali dei siti i loro nomi di uso corrente, di più agevole memorizzazione ed utilizzabilità (così ed esempio il reale IP *address* del sito www.poliziadistato.it risulta 195.120.182.169).

In sostanza, se ci si vuol connettere al sito www.poliziadistato.it il computer si dirige automaticamente verso apposite banche dati che risolvono quel dato nominale individuando il suo reale indirizzo digitale 195.120.182.169, da raggiungere per realizzare la connessione.

Alterata la procedura automatica di risoluzione dei nomi a dominio, si viene così inconsapevolmente dirottati verso siti diversi da quelli desiderati ma a questi assai simili.

Convinti di connettersi alla banca di fiducia si viene in realtà deviati verso siti gestiti dalle organizzazioni criminali che carpiscono così i riservati dati di accesso ai conti bancari.

La più recente esperienza investigativa fa peraltro rilevare anche altri fraudolenti tipi di re-indirizzamento informatico realizzati attraverso la propagazione di specifici virus.

Altrettanto arduo appare difendersi dalle insidie del così detto *key logging*.

Il termine richiama oramai diffusissimi programmi informatici "dannosi" (*malware*) che installano sui computer codici spia che consentono ai criminali del web di "vedere" i tasti premuti dall'utente e risalire quindi, tra l'altro, ai dati riservati di accesso al suo conto bancario.

Creati originariamente "a fin di bene", per controllare ad esempio l'uso dei computer da parte dei minori, sono stati sempre più raffinati sino ad essere congegnati per attivarsi solo nei momenti in cui un utente si connette al sito di una determinata banca.

Non deve sorprendere d'altro canto che tali temibilissimi "*malware*" siano facilmente ricavabili da Internet e quindi di agevole fruibilità.

Una delle ultime gravi minacce in campo informatico è rappresentata dalle così dette "*botnet*".

Il termine, acronimo dei due vocaboli inglesi robot e network (reti di robot), indica un insieme di programmi informatici (software robotizzati) che eseguono in maniera automatica e ripetitiva operazioni che altrimenti richiederebbero l'intervento di un operatore "umano" alla tastiera.

Nati nel mondo dei canali di *chat* (IRC), tali programmi possono essere utilizzati per acquisire il controllo remoto di interi gruppi di computer e per far compiere a tali macchine, ormai fuori dal controllo degli effettivi titolari, operazioni indesiderate, prevalentemente con fini illeciti, quali ad esempio la disattivazione di servizi offerti dai siti web, gli attacchi a interi sistemi informatici, lo *spamming* e i furti di dati identificativi personali e di codici di carte di credito.

In Italia le *botnet* si stanno evidenziando proprio nell'ambito del *phishing*.

Si è rilevato, ad esempio, che le migliaia di e-mail trappola inviate per carpire ingannevolmente i riservati codici di accesso ai conti bancari on line risultano inoltrate automaticamente da computer

"violati" e utilizzati da remoto all'insaputa degli effettivi titolari.

Non solo. Gli stessi successivi accessi truffaldini ai conti, realizzati utilizzando i dati "rubati", sono effettuati mediante macchine violate di cui i criminali sono entrati in disponibilità.

Il tutto ovviamente per disperdere le tracce, dissimulare l'origine delle azioni criminose e assicurare l'impunità agli autori.

Il fenomeno *botnet*, di rapida diffusione, ha recentemente cominciato a destare serie preoccupazioni.

Le "mandrie" di macchine violate e "asservite", gestite abilmente da unici centri di comando e controllo, possono essere utilizzate per sferrare multiformi attacchi illeciti a sistemi informatici.

Tra i più frequenti quelli destinati a realizzare la disattivazione su larga scala di servizi offerti da siti web (fenomeno tecnicamente indicato come *denial of service*, negazione di servizio).

Alle *botnet* si fa ancora ricorso per propagare virus informatici, particolarmente devastanti, se introdotti nelle reti aziendali o nella virtuale spina dorsale automatizzata degli enti governativi.

Frequente utilizzo di *botnet* è stato peraltro rilevato anche per gestire il noto fenomeno dello *spamming*.

Nel mondo anglosassone, solito anticipare in positivo e negativo le applicazioni dell'innovazione tecnologica, sono già state registrate nuove fenomenologie estorsive concretizzatesi in richieste di denaro per evitare intrusioni ad opera di *botnet*.

Una sorta di vero e proprio "pizzo informatico"che non sembra peraltro troppo distante dalla nostra realtà.

3. Considerazioni generali e strategie di difesa.

Dal quadro sopra tracciato nelle sue linee di estrema sintesi emerge che il così detto *computer crime* va oggi considerato in una accezione assai più ampia di quella originaria.

Non più circoscritto a comportamenti delittuosi in danno della rete tout court (*computer crime* classico per cui si richiamano le più comuni figure di reato dell'accesso abusivo ad un sistema informatico o telematico ex. art.. 615-*ter* c.p., della detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici ex art . 615-*quater* c.p. o della diffusione di programmi diretti a danneggiare od interrompere un sistema informatico ex . art. 615-*quinquies* c.p.), il *computer related crime* vede la utilizzazione strumentale, ad opera di composite organizzazioni criminali, delle abilità tecnico-informatiche di *hacker* o "smanettoni" di vario genere.

Il caso del phishing è in tal senso emblematico.

Abili tecnici informatici sono "arruolati" per allestire siti civetta e realizzare furti di identità digitale su vasta scala.

Affiorano d'altro canto nuovi schemi di riciclaggio incentrati sul reclutamento di centinaia di "soldatini" che si prendono carico di ricevere le somme truffate e di "rigirarle " ad altri sconosciuti "commilitoni" avviando un tortuoso iter di "lavaggio" del denaro sporco che rende pressoché impossibile risalire ai reali beneficiari.

Le raffinate menti criminali che tirano le fila del gioco si assicurano così guadagni al momento inestimabili ove si pensi ad esempio che le razzie informatiche dei conti bancari on line avvengono in

danno di clienti di centinaia di istituti bancari disseminati nei più vari paesi del mondo.

In sostanza il profilo "classico" d'autore del delinquente informatico sembra oramai discostarsi decisamente dalle figure dei così detti *hacker*, *cracker* e *phreaker* tipiche del primo evo della criminalità informatica.

Ci si sta in definitiva accostando a figure criminologiche classiche in senso proprio da collocare e analizzare in più ampi contesti di associazionismo criminale.

Il ruolo preponderante giocato dallo strumento informatico, sempre più diretto obiettivo dell'azione criminale mediante utilizzo di sofisticate tecnologie informatiche, sprona peraltro a ripensare decisamente ai classici schemi vittimologici.

Quale infatti l'attendibile profilo criminologico della vittima nei sofisticati raggiri informatici?

Di innovata attualità balza ancora il delicato contesto della formazione degli operatori di Polizia nel settore specifico.

L'individuazione del più equilibrato punto di fusione tra competenze tecnico informatiche e capacità investigative classiche appare argomento oggi sempre più complesso imponendo profonde riflessioni sul come far correttamente formazione.

4. Strategie di contrasto.

Le strategie di contrasto di forme di criminalità così pervasive ed articolate rendono indispensabili nuovi approcci sia in termini investigativo-repressivi sia in termini di adeguate misure preventive.

Si palesa sempre più imprescindibile una risposta investigativa su ampia scala orchestrata tra forze di polizia specializzate, ben collegate e coordinate in ambito internazionale.

Ogni concetto di territorialità geografica si è, infatti, dissolto sia in ragione della dimensione mondiale del fenomeno sia in ragione della natura stessa del mezzo (internet e le reti telematiche in generale) utilizzato per attuare gli attacchi criminosi.

Sul fronte della prevenzione appare assolutamente indispensabile una capillare e continua azione di sensibilizzazione degli utenti dei servizi telematici verso nuove forme di cultura di sicurezza informatica.

La Polizia di Stato italiana ha da pochi anni allestito e attivato nella Polizia delle Comunicazioni un'agile e specifica agenzia di contrasto di tali nuove minacce.

Alla creazione di unità investigative ad alta specializzazione, capillarmente distribuite sul territorio nazionale, tale struttura associa l'attivazione di collegamenti internazionali con analoghe agenzie operanti quasi in tutti i paesi del mondo. Un continuo monitoraggio delle reti informatiche è finalizzato a rilevare e prevenire ogni nuovo tipo di insidia.

Particolarmente indicativo risulta in tal senso la costituzione, presso il Servizio Centrale della Polizia Postale e delle Comunicazioni, del C.N.A.I.P.I.C. – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche. Il Centro è volto a realizzare efficaci forme di contrasto di attacchi informatici con matrice criminale terroristica dirette verso le così dette infrastrutture critiche quali ad esempio quelle del settore dell'energia, dei trasporti, delle comunicazioni e dell'*e-government*.

Bibliografia

AA.VV., *Internet e diritto*, Gedit, Bologna, 2001.

AA.VV., *Internet. Nuovi problemi e questioni controverse*, Giuffrè, Milano, 2001.

De Grazia L. M., *Il giurista ed Internet*, Simone, Napoli, 1999.

Pomante G., *Internet e criminalità*, Giappichelli, Torino, 1999.