LE INSIDIE DELLA RETE

Dott. Marco Monoscalco

1. PREMESSA

Nello studio dell'informatica giuridica è dedicato spazio anche ai riflessi pratici legati all'uso delle nuove tecnologie. Ci si trova a studiare le caratteristiche proprie di un reato informatico, a volte senza riuscire a comprendere come questo possa effettivamente avvenire, o addirittura, si fa fatica a riconoscere un comportamento illecito semplicemente perché le cognizioni e la cultura informatica del lettore non superano il livello scolastico.
Ne è prova l'uso massivo dei software di scambio file, difatti, molti utenti non sono a conoscenza di essere a loro volta divulgatori del materiale che scaricano. La differenza di condotta è notevole, perché la sanzione relativa al procurarsi materiale coperto da diritto d'autore è di tipo amministrativo, mentre la divulgazione di tale materiale è punito da una sanzione penale.
Come si può facilmente intuire, non conoscere in modo approfondito il meccanismo ed il funzionamento di un sistema informatico può essere rischioso sotto molti punti di vista.
In questo capitolo, intitolato "le insidie della rete" cercheremo di fornire al lettore una visione ampia ma sufficientemente dettagliata di alcune delle più comuni vicende che riguardano il quotidiano vivere di ciascuno di noi, utilizzando un linguaggio quanto più possibile chiaro, inequivocabile, non ridondante: a prova di "non-informatico".
Quando si parla in modo generico di "insidie" della rete internet nella mente della maggior parte delle persone appare un'immagine di un vecchio ricurvo e bavoso davanti ad un computer: è un'immagine evocativa che ci riporta al problema della pedofilia.
Senza lasciarci distrarre dall'impulso che genera un senso di ripudio verso questo argomento, è bene precisare che su internet è più facile imbattersi in "materiale pedo pornografico" piuttosto che con pedofili veri e propri.
La differenza è ovvia, ma è bene chiarirla subito.
Non spenderemo molte parole su questo argomento, non ci addentreremo in aspetti psicologici delle parafilie e dei meccanismi compulsivi e ossessivi che le pervadono, ma parleremo della possibilità di imbattersi nella pedo pornografia che, seppur collegata, è cosa differente rispetto alla pedofilia vera e propria intesa come atti sessuali compiuti nei confronti di minori.
Ma non solo. Le insidie della rete sono molteplici e perciò in questo capitolo affronteremo i problemi e pericoli legati alla rete internet, cominciando dal *file sharing*, per passare ad una descrizione generalizzata delle varie truffe e dei raggiri in cui possiamo imbatterci nel *web*.
Non si tratta di un "manuale" contro le truffe web, ma la lettura di questa dispensa offre una visione globale di come il mezzo informatico sia usato anche da chi vuole approfittarsi della buona fede, dell'innocenza e dell'ingenuità degli utenti.

2. I PERICOLI DEL FILE SHARING

Lo sviluppo della rete abbinato al costante ed incessante aumento della dotazione tecnologica personale fa incrementare la quantità di dati scambiati e scambiabili tra gli utenti, e l'uso dei software di *file sharing* (eMule, Torrent, ecc...) sono per la loro stessa natura, una fonte di pericolo per gli stessi utilizzatori.
In questo paragrafo, per la trattazione dell'argomento, concentriamo la nostra attenzione verso i pericoli e le insidie dei software di tipo peer-to-peer diversi dalla violazione del diritto d'autore che in questa sede tralasciamo.
Per una più agevole comprensione da parte dei pochi che non conoscono la materia, possiamo spiegare che attraverso l'uso di questi programmi gli utenti di tutto il mondo

scambiano quantità impressionanti di dati, e ognuno diventa allo stesso tempo fruitore e divulgatore del medesimo materiale.
Un toccasana per la cultura e l'etica hacker, una catastrofe per chi vive dei proventi del copyright.
Il software eMule (lo citiamo non in quanto unico software di questo tipo, ma perché è il più famoso e diffuso) consente di scaricare filmati, musica, testi, archivi ecc... prelevando tali dati non da un server centrale che detiene tutte le informazioni, ma direttamente dai computer di tutti coloro i quali, in quel medesimo momento, sono collegati alla rete e usano lo stesso software.
Lo scambio avviene in modo automatico e, normalmente, l'utente non si preoccupa di conoscere direttamente o indirettamente le persone e i computer dai quali preleva il materiale, né quelle ai quali quello stesso materiale viene reso disponibile.
La diffusione di questi software è inarrestabile, ma come ogni strumento tecnologico può nascondere delle insidie.
I pericoli più frequenti sono caratterizzati dall'esistenza di software malevoli quali *virus*, *cavalli di troia*, *malware*, ecc... che vengono abilmente celati all'interno di programmi disponibili per il *download*.
Normalmente, tali programmi sono nascosti all'interno dei c.d. *crack* o *keygenerator* che permettono la rimozione delle protezioni software dei programmi.
Chi scarica ed installa software che contengono tali insidie offre il fianco a innumerevoli attacchi, il più pericoloso dei quali è quello relativo al c.d. "ponte", cioè la possibilità per un terzo di utilizzare il computer dell'utente come base per altri attacchi informatici o per l'invio massivo di messaggi di posta elettronica indesiderati.
Ma l'insidia maggiore è caratterizzata dal c.d. "*FAKE*" termine anglosassone che tradotto significa "falso", o "fregatura", ed è generalmente riferito a quei file che hanno un contenuto differente dal loro titolo. Un esempio classico è quello della ricerca di un film di prima visione (ricordo che non ci occupiamo in questo paragrafo di tutela del diritto d'autore) che una volta scaricato si rivela essere un filmato pornografico.
Ma come può un *fake* essere un pericolo per un utente?
Diventa un pericolo quando il contenuto del file è un software malevolo o peggio ancora, quando è relativo a materiale pedopornografico.
Il *fake* è un pericolo a causa della natura stessa di eMule e degli altri software dello stesso tipo, infatti, il download di un file può richiedere molto tempo, a volte anche alcuni giorni, durante i quali le parti del file che si sta scaricando sono già disponibili per l'*upload* verso altri utenti.
Chiariamo il concetto con un esempio: può accadere che un utente stia scaricando un file denominato "partita di calcio Italia–Francia.avi", ma in realtà il file ha contenuto pedopornografico.
Durante il *download*, che come detto può durare molto tempo, le parti già acquisite sono rese automaticamente disponibili come fonte per la divulgazione del file, ed in quello stesso momento molti altri utenti ne stanno prelevando le porzioni già scaricate.
Dunque, capita che un utente scarichi e divulghi inconsapevolmente materiale pedo-pornografico, incrementandone la diffusione. Ma a volte il *fake* viene scoperto con molto ritardo, a causa dell'insana abitudine di molti utenti di lasciare lavorare il computer "da solo", lasciando attivo il *download* per giorni e giorni, e verificando di tanto in tanto il materiale scaricato.
E' praticamente impossibile sapere a priori se un file ricercato con eMule sia o meno un *fake*, e cosa in realtà sia contenuto all'interno del file stesso. Questa considerazione è utile per tenere presente che nessuno può ritenersi immune da questo problema, anche gli utilizzatori più smaliziati ed esperti.

L'attività di contrasto alla pedopornografia è svolta in Italia dalla Specialità della Polizia di Stato chiamata Polizia Postale e delle Comunicazioni, che ogni anno pubblica statistiche confortanti circa il numero di siti illegali oscurati e di pedofili individuati grazie alla rete internet.
Attraverso il monitoraggio costante della rete, è possibile individuare coloro i quali divulgano materiale pedopornografico anche tramite i software di *file sharing.*
Data la diffusione mondiale della rete, anche gli organi di polizia stranieri possono rilevare violazioni avvenute da computer situati nel nostro Paese, e quando accade trasmettono le risultanze dei loro accertamenti all'Autorità Giudiziaria italiana, che provvede ad approfondire le indagini.

Considerando quanto detto finora, ipotizziamo (ma non è infrequente) che durante lo scaricamento di un file *fake* dal contenuto pedopornografico uno o più investigatori italiani o stranieri prelevino quel file o parte di esso, tracciando l'indirizzo IP del divulgatore.
Inizia così una indagine che porterà all'individuazione della linea telefonica e/o telematica usata dall'utilizzatore di eMule che stava divulgando il file.
Conseguenza inevitabile è l'accertamento diretto, eseguito con una perquisizione informatica che tenderà a rintracciare il file oggetto di indagine o altri della stessa natura.
Qualora il file fosse stato scaricato inconsapevolmente, gli accertamenti peritali probabilmente consentiranno di dimostrare l'involontarietà dell'azione e quindi l'assenza dell'elemento soggettivo necessario per la configurazione del reato, ma questo accertamento viene svolto durante il dibattimento, quando cioè il procedimento penale a carico dell'utilizzatore di eMule si trova allo stadio avanzato. Ma l'essere stati anche solo indagati per questo tipo di reato lascerà per sempre un velo di diffidenza e una pessima reputazione nei confronti delle persone coinvolte, che porteranno addosso il peso di un "sospetto" che può diventare insostenibile al pari di una sentenza di condanna.

3. IL FURTO DELLE PASSWORD

I servizi informatici di tutti i tipi sono essenzialmente diretti a persone che dispongono di un "*account*" al quale è inevitabilmente legata una "*password*" di accesso.
Tutti gli esperti informatici consigliano di mantenere una password diversa per ogni servizio, e cambiarla spesso. La password deve essere lunga, deve contenere caratteri speciali, numeri, lettere maiuscole e minuscole.
Queste accortezze, condivisibili in linea teorica, sono però disattese nella vita reale a causa dell'eccessivo numero dei servizi on-line come la posta elettronica personale, quella dell'ufficio, del servizio di consultazione dello statino paga, del sito di *e-commerce*, dell'*home banking*, del forum di discussione, del *social network*, ecc...
Succede così che la maggior parte delle persone scelga una password sola che usa per tutti i servizi e c'è anche chi attiva la funzione di memorizzazione della password all'interno del pc.
I più saggi scelgono password diverse per ogni sito o servizio, ma inevitabilmente devono poi scrivere queste password in una agenda perché in pochi riescono a ricordarle tutte.
Ma a che cosa servono tutte queste accortezze per le password? La risposta è ovvia, per impedire ad altre persone di accedere all'account.
Prima di procedere ad esaminare i pericoli e le insidie che possono capitare agli sfortunati utenti a i quali viene carpita la password di accesso, analizziamo sinteticamente le modalità e le tecniche usate da chi vuole impossessarsi delle password altrui.

Il primo e più semplice di tutti è quella di leggerla dal post-it attaccato sullo schermo del computer o scritta a matita dietro la tastiera. Sembra paradossale, ma il modo più diffuso è proprio questo, che sfrutta l'inadeguatezza e la superficialità di molte persone che non comprendono l'importanza e il valore della segretezza della chiave di sicurezza.
Molto diffuso è anche il metodo che consiste nel chiederla direttamente all'interessato con metodi ingannevoli. Certamente, per essere credibile il malfattore cercherà di celarsi in vari modi, ed il metodo più usato è definito "*phishing*" che consiste nell'inviare un messaggio che replica fedelmente le caratteristiche grafiche del gestore di un servizio, comunicando all'utente un improvviso guasto o l'accreditamento di un bonus, e invita ad effettuare l'accesso al servizio utilizzando il collegamento presente nel messaggio stesso.
Il collegamento in realtà non porta alla pagina d'accesso originale, ma ad una identica gestita dal malfattore, che carpirà nome utente e password per poi accedere all'account vero e proprio e operarvi all'interno.
Il *phishing*, quando è applicato all'*home banking*, produce risultati economicamente disastrosi per le vittime.
Altro metodo diffuso è quello di catturare le informazioni direttamente dalla tastiera dell'utente, utilizzano software malevoli chiamati "***keylogger"*** in grado di memorizzare ogni tasto premuto sulla tastiera, inviando poi i dati tramite posta elettronica al malfattore.
A titolo didattico segnaliamo anche l'esistenza di *keylogger* di tipo *hardware*, cioè piccoli dispositivi che si attaccano fisicamente al computer, tra lo spinotto della tastiera e il computer stesso, capace di immagazzinare le stesse informazioni del *keylogger software* ma che deve poi essere recuperato fisicamente.
La scelta dell'uno o dell'altro metodo dipende da quale e quanta libertà d'azione ha il reo, preferendo sempre il *keylogger hardware* perché non viene rilevato dai *software* di controllo, però non può essere installato sui computer portatili.
Ulteriore e più complesso è il metodo dello *sniffing*, cioè l'acquisizione di tutto il traffico telematico passante allo scopo di reperire, una volta decodificato, le informazioni d'accesso.
Questo metodo è assiduamente usato da coloro i quali accedono abusivamente alle reti WiFi protette delle abitazioni private. Appositi software liberamente reperibili *on-line* permettono di memorizzare il flusso dati e analizzare le chiavi d'accesso, scorporando i dati utili per l'accesso abusivo.
I tre metodi appena accennati non esauriscono la disamina delle possibilità d'azione, ma possono dare una prima visione globale del fenomeno.
Tutti i comportamenti accennati configurano il reato previsto dall'***art. 615 quater*** del codice penale.

4. VIOLAZIONE DEGLI ACCOUNT

Dopo aver accennato ai modi (solo alcuni) per entrare in possesso delle password di accesso, vediamo cosa accade frequentemente agli account.
La violazione degli account, pur se vietata, è una pratica diffusissima e pochi riescono a rendersi conto d'averla subìta.
Chi viene a conoscenza della password d'accesso ad un servizio, come ad esempio la posta elettronica, può facilmente prendere cognizione del contenuto o usarla a piacimento.
Se lo scopo è danneggiare, alterare o sopprimere dati, l'azione di disturbo avviene una sola volta, ma se lo scopo è legato allo spionaggio, l'abusivo intrusore può controllare il contenuto anche più volte, senza che titolare dell'account se ne accorga.
I più interessati a questa illecita pratica sono i concorrenti di mercato, gli investigatori privati, coniugi gelosi (o in fase di separazione), ma anche semplici "curiosi" che non resistono all'impulso di farsi i fatti degli altri.

Ma c'è chi cerca di accedere ad account altrui anche per commettere reati utilizzando le informazioni e/o le peculiarità dell'account stesso. Possiamo citare, ad esempio, la violazione degli account del sito di commercio elettronico eBay allo scopo di pubblicare aste o mettere in vendita oggetti inesistenti sfruttando la reputazione (chiamata *feedback*) dell'account violato.
Ma per meglio comprendere questo concetto prendiamo in esame il più famoso *social network Facebook.* Ricordandoci sempre che il lettore può non conoscere questo sistema, ci preoccupiamo di chiarire che chi lo usa dispone di un *account* collegato al proprio indirizzo di posta elettronica con il quale comunica ed interagisce con le persone inserite nella propria "lista amici".
Uno strumento semplice, efficace, utilissimo e gratuito che ha consentito e consente di ritessere amicizie perdute o riavvicinare persone lontane.
E' pur vero che la frenesia per questo strumento ha portato tanti utilizzatori a definire "amici" anche persone conosciute per caso ad un evento o alla fermata dell'autobus, di cui magari si conosce solo il nome e null'altro, ma tant'è, e ci sono utenti che superano abbondantemente la quota dei 500 amici, pur frequentandone abitualmente molti meno.
Ultimamente è stata importata su questo sistema una truffa rapida e fastidiosamente ingegnosa che inizia con la violazione di un account. In questo caso, dopo la violazione, il malfattore si preoccupa di modificare la password di accesso in modo da impedire al legittimo utilizzatore di limitarne gli effetti e le conseguenze ulteriori.
Il meccanismo è semplice: inviare un messaggio di posta privato a tutti i contatti presenti nella lista amici (e i truffatori scelgono sempre le persone che hanno una lista molto corposa) con un testo breve ma efficace "*Ti prego aiutami, sono appena arrivato in Inghilterra e mi hanno rubato tutti i bagagli compreso il portafoglio e il cellulare. Sono rimasto senza un soldo, ho bisogno di acquistare i biglietti per rientrare a casa e mangiare qualcosa. Ora mi trovo in una stazione di polizia e mi stanno facendo usare il loro computer per chiedere aiuto. Ricaricami almeno 200 € sulla carta di credito XXXXXXXX te li restituirò appena rientro. Grazie tante, fai presto*". E chi non correrebbe in aiuto di un amico in difficoltà?

5. LE FRODI E LE TRUFFE TELEMATICHE

Dopo aver illustrato brevemente quali tipi di insidie possono nascondersi dietro l'uso abusivo degli account, vediamo in quali altre insidie potremmo imbatterci sulla rete.
Come si è visto la rete è usata da tutti, anche da chi vuole approfittare della buona fede, dell'innocenza e della ingenuità degli utenti per arricchirsi ingiustamente.
Per trattare questo tema servirebbe più di un capitolo, ma ci limiteremo ad elencare alcuni dei sistemi ingannevoli più comuni, con la speranza che queste indicazioni siano utili ad impedirne almeno una.
La parola SCAM è usata in gergo informatico per indicare tutti quei messaggi di posta elettronica di tipo ingannevole.
Non parliamo di messaggi pubblicitari o indesiderati per altra natura (c.d. SPAM), parliamo dei messaggi che vengono usati come mezzo per compiere truffe o raggiri.
Il più frequente è quello già descritto nei paragrafi precedenti quando abbiamo parlato del *phishing,* ma non è l'unico.
Caratteristica comune a tutti i messaggi di questo tipo è la genericità e l'indeterminatezza del destinatario, cioè l'invio massivo e non selettivo dei messaggi ad una quantità indefinita di destinatari e con questo metodo, analogamente al metodo della "pesca a strascico in mare", i truffatori sperano in una quantità anche minima di successo. Supponiamo l'invio di 20 milioni di email (da un pc usato come "ponte" - v. primo

paragrafo) ad altrettanti destinatari casuali, e di questi lo 0,6% cada nella trappola: significa 120 mila persone truffate.
Questi numeri, a dire la verità ipotetici perché nella realtà sono sicuramente maggiori, lasciano capire la dimensione del fenomeno. Ma analizziamone alcuni.
Lo SCAM sentimentale è sempre più frequente. Consiste nell'inviare un messaggio, normalmente scritto in inglese, al quale è allegata una fotografia di una ragazza o di una donna di bella presenza non in atteggiamenti erotici o seducenti, ma in posa semplice, spesso a mezzo busto.
Nel messaggio è scritto che la ragazza ha letto il "profilo" corrispondente all'indirizzo email del destinatario e che è "interessata". Così facendo, simula di aver frequentato un sito specializzato in incontri e, qualora il destinatario casuale li frequentasse davvero, il messaggio sembrerebbe credibile.
La persona che cade nel tranello inizia un rapporto epistolare che può durare anche diversi mesi, nel quale la ragazza (o presunta tale) si confida, si rende disponibile all'ascolto.
L'obiettivo è subdolo, circuire la vittima. Molti finiscono per innamorarsi dell'interlocutrice, anche se non si sono mai incontrati, e la truffa vera e propria si consuma quando la ragazza chiederà denaro per affrontare gravi situazioni personali come uno sfratto imminente o malattie di familiari, con richieste sempre più pressanti abbinate alla promessa di incontrare personalmente il suo nuovo amore.

Un ulteriore recente fenomeno estorsivo sta prepotentemente emergendo, si tratta di un sistema che utilizza le minacce per ottenere denaro da parte degli utenti dei siti di incontri e di webcam-chat.
La vittima viene invitata ad eseguire una videochat erotica di fronte ad una webcam e successivamente viene minacciata di pubblicazione del video se non corrisponderà una certa cifra all'estorsore.
Si tratta di una estorsione particolarmente subdola, poiché si approfitta del pudore e della reputazione delle vittime le quali, per non vederla danneggiata, spesso aderiscono al pagamento senza denunciare l'accaduto alla magistratura, rendendo difficoltoso l'accertamento dei fatti.

Altro tipo di insidia è caratterizzata dallo SCAM lavorativo. Chi non ha mai ricevuto allettanti proposte di lavoro via posta elettronica? Questi messaggi sono sempre scarni, ed inviati allo scopo di catturare l'attenzione di chi vuole cambiare lavoro, di chi lo cerca, e di chi è interessato ad un guadagno supplementare.
Ad una prima risposta di interesse, il mittente del messaggio SCAM invierà via posta elettronica una corposa documentazione corredata da carte intestate, schemi, moduli di contratto, ecc... riferibili ad una società multinazionale che non ha ancora attivato sedi o filiali in Italia e che per far questo, sta cercando un "responsabile" o "dirigente".
Il lavoro proposto sembra anche semplice, gestione dei pagamenti relativi ai contratti che gli agenti sul territorio riusciranno a stipulare.
Per questo lavoro è sufficiente un conto corrente on-line gestibile dal nuovo "responsabile", il quale comincerà a ricevere bonifici relativi ai pagamenti che dovrà registrare sul sito della società e subito dopo trasferirli ad altri conti correnti trattenendo la percentuale pattuita all'atto della stipula del contratto (di solito l'8 %).
Il problema è che quel denaro, transitato sul conto corrente della persona, non è affatto proveniente da contratti stipulati da inesistenti agenti di una inesistente società

multinazionale, ma è denaro trafugato dai conti correnti on-line ai quali è stata carpita la password d'accesso con i metodi visti nei paragrafi precedenti.
A seguito dei vari passaggi, il denaro ripulito transita all'estero, e il malcapitato si troverà a rispondere penalmente per il concorso nella truffa e nel riciclaggio.

Il "nigerian SCAM" è il raggiro più conosciuto e più vecchio del web.
Sono anni che un gruppo di persone di nazionalità nigeriana gira il mondo inanellando truffe con una frequenza impressionante. E' un metodo che abbina l'ingegno truffaldino alla malizia e la disonestà della vittima stessa, che ha oggettive e soggettive difficoltà a denunciare d'esser stato truffato.
Come per gli altri raggiri, inizia con un messaggio di posta elettronica scritto in lingua inglese nel quale un finto funzionario di una banca africana propone ("a seguito di segnalazione di persona di fiducia") di falsificare dei documenti relativi ad un conto corrente contenente una somma ingente, più 20 milioni di dollari, appartenuto ad una persona deceduta da poco tempo che non ha eredi.
Poiché secondo le leggi di quel Paese i beni non ereditabili finiscono nelle casse dello Stato, la proposta di falsificazione consisterebbe nel far risultare come unico erede proprio il destinatario del messaggio, e dopo l'operazione il funzionario richiede il pagamento del 30% della somma.
Le persone che aderiscono alla proposta saranno convocate in un lussuoso albergo, verranno presentati di persona tutti i dettagli dell'operazione.
L'unica raccomandazione è il silenzio più assoluto, perché si tratta di una operazione illecita. A quel punto la vittima si pervade d'uno stato d'euforia derivante dall'aspettativa di una vita agiata, fino a quando dopo qualche giorno i suoi sogni vengono infranti da una telefonata o da un nuovo messaggio che invita nuovamente ad incontrarsi in un albergo.
Il motivo della nuova convocazione è semplice: un altro funzionario della banca si è accorto dell'operazione e per consentire che tutto si svolga come pattuito, richiede una tangente di 10.000 dollari che nessuno vuole sborsare.
I più si affannano per pagare la tangente, con l'aspettativa di riceverne molti di più, ma poi si rendono conto di aver perso quei soldi proprio perché non esiste nessuna banca con quel nome.
In pochi trovano il coraggio di sporgere denuncia all'autorità giudiziaria, e questa truffa continua e continuerà probabilmente per molto tempo.