¤ ATTUALITÀ

Internet contro sicurezza: chi vincerà?

Forze dell'Ordine coalizzate per garantire la riservatezza sul web. A colloquio con il capitano Francesco Mandalari, tra i più esperti collaboratori del Gat, per capire di più

di ALESSANDRO NANNI
alessandro.nanni@carabinieriditalia.it

Internet è entrato prepotentemente nella vita di tutti i giorni, parole come web, link, chat, e-mail, fanno parte ormai del linguaggio comune, senza contare poi il boom di connessioni in rete testimoniato dalle percentuali da capogiro delle transazioni economiche effettuate annualmente sul web, che hanno raggiunto numeri a due cifre; in tutto il mondo quasi un terzo delle persone si collega giornalmente sul web. Ci sono quelli che consultano il valore dei propri investimenti (Azioni, titoli di stato, ecc.), coloro che si collegano per sapere cosa accade nel mondo, e chi invece si connette semplicemente per controllare i messaggi sul proprio account di posta elettronica.

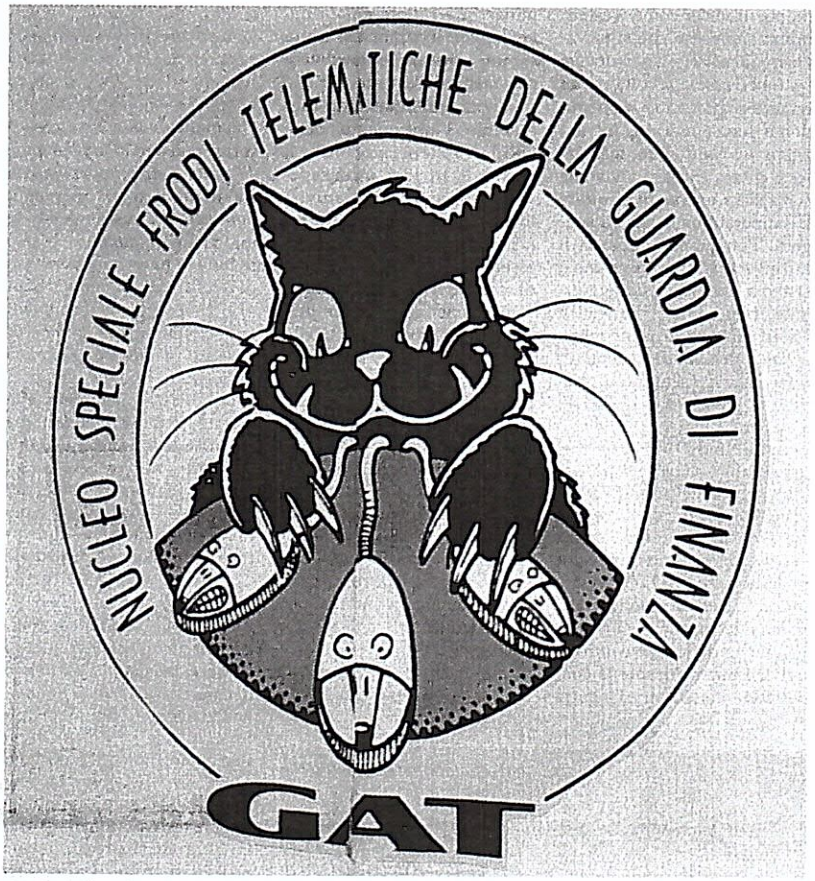
Il popolo degli internauti appare quindi molto variegato e non potrebbe essere altrimenti, visto che il web è una fonte inesauribile di dati e informazioni. Tuttavia il fenomeno internet sembra accrescere le sue dimensioni in maniera esponenziale, lo sviluppo della telefonia VOIP, con l'operatore Skype in testa, è riuscito a soppiantare l'utilizzo dei mezzi di comunicazione tradizionali poichè viene offerta la possibilità all'utente di chiamare a condizioni estremamente vantaggiose qualsiasi persona, anche se quest'ultima si trovi nel posto più sperduto del Globo; un discorso a parte meritano invece le piattaforme P2P (sistema utilizzato per lo scambio di files), che consentono la diffusione indiscriminata dei contenuti protetti da copyright, alimentando la cosiddetta "pirateria" informatica, un fenomeno irrefrenabile; chiunque infatti può scaricare abusivamente files audio e video in modo indisturbato per poi commerciarne i contenuti (film, canzoni, ecc.), contravvenendo sistematicamente alle normative vigenti in materia fiscale.

Il punto debole del web rimane la mancanza di rispetto del diritto alla riservatezza on-line; ci sentiamo un po' tutti spiati, quando ci connettiamo in rete, soprattutto a causa della diffusione degli spyware (programmi che raccolgono senza il consenso dell'utente una serie di dati personali); spiati dicevamo, anche per aver navigato molte volte senza possedere un buon programma antivirus e senza porre la giusta attenzione all'attacco dei famosi malware che costituiscono una seria minaccia sia per la sicurezza del proprio computer, sia per i numerosi dati sensibili memorizzati nel disco fisso del proprio PC, immagazzinati in seguito alle numerose "richieste invasive" alle quali siamo sottoposti.

Per la semplice iscrizione a una newsletter oppure a un forum, vengono richieste quasi sempre le nostre credenziali, indirizzo, nome e cognome, casella di posta elettronica ed una password di fantasia che quasi sempre è la stessa per non correre il rischio di dimenticarla; a volte vengono richieste informazioni differenti come la professione esercitata, in quale settore lavoriamo, numero di cellulare e telefono di casa. In quest'ultimo caso però l'utente è chiamato ad accettare l'informativa ai sensi del regolamento in materia di protezione dei dati personali (Decreto Legislativo n. 196 del 2003) autorizzandone il trattamento da parte di determinati soggetti legittimati a farlo; nel caso in cui non si accetti tale informativa, l'iscrizione a un servizio viene spesso negata.

Tutti questi dati potrebbero essere "rubati" dagli abilissimi hackers (specialisti che si infiltrano nella rete superando limitazioni di ogni tipo), soprattutto quando riguardano l'accesso ad un conto corrente on-line; sono infatti aumentati i casi di phishing e di reati informatici.
Contro lo scorretto utilizzo di tutte queste informazioni operano gli encomiabili investigatori delle Forze dell'Ordine, i quali, adottando tecnologie informatiche sofisticate ed avvalendosi dei loro "geni" della rete, riescono molte volte a smascherare vere e proprie organizzazioni criminali dedite ad attività illecite sul web. Anche se i risultati ottenuti potrebbero sembrare clamorosi, rimangono alquanto esigui se paragonati alla vastità di internet, per questo motivo una normativa più efficace per regolamentare la rete risulterebbe più che mai necessaria; nel frattempo, all'ignaro utente, non rimane altro che navigare con accortezza tra gli innumerevoli siti internet, divulgando il meno possibile i propri dati.

Tuttavia l'incommensurabile grandezza di internet è confermata dalla costante nascita di nuovi fenomeni sociali, come ad esempio **le "cyberdroghe", un nuovo business che rientra nelle attività illecite monitorate dalle Forze dell'Ordine; si tratta in sostanza di vere e proprie I-dosi costituite da files audio, scaricabili a pagamento da alcuni siti come i-Doser.com, oppure da altri portali che li inseriscono come risorsa gratuita.** Queste sequenze sonore includerebbero degli infrasuoni, che sarebbero in grado di provocare reazioni cerebrali molto simili a quelle scatenate dalle sostanze stupefacenti; tutto questo avverrebbe per la presenza di



particolari onde aventi frequenze che vanno dai 3 ai 30 hertz, le stesse su cui lavora il cervello umano, la durata delle I-dosi è variabile, tuttavia non supera i trenta minuti. Gli esperti non si sono ancora pronunciati ufficialmente sui rischi di questa nuova neurodipendenza, eppure si parla già di allarme sociale, anche se molti s'interrogano: esistono davvero degli effetti collaterali oppure è tutta una frode architettata ad arte per sfruttare la suggestione della psiche umana? La risposta a questa domanda sta iniziando ad arrivare dai vari gruppi investigativi del settore.

Tra questi, i più agguerriti sono la Polizia Postale e delle Comunicazioni e il GAT della Guardia di Finanza (Nucleo Speciale Frodi Telematiche); quest'ultimo annovera tra le sue fila lo Sceriffo del Web, il Colonnello Umberto Rapetto, uno specialista dell'informatica che oltre ad essere un abile investigatore, insegna Sicurezza sul Web agli studenti dell'Università di Malta Link Campus a Roma. Molte sono le tecnologie a disposizione delle forze di Polizia nel settore delle frodi telematiche, fra queste ci sono sofisticatissimi strumenti di intercettazione, complicati software e l'utilizzo di enormi banche dati in grado di fornire preziose informazioni in un lasso di tempo molto breve.

È opportuno evidenziare però che le tecnologie investigative più efficaci sono quelle tradizionali, utilizzate ad esempio nelle indagini contro la pedofilia on-line; in questo caso gli encomiabili "investigatori del web" hanno utilizzato un programma particolare che funziona come una sorta di "rilevatore" a 360°.

Una volta inserito nella rete sospetta, questo software intelligente può riconoscere e individuare video e immagini a carattere "pedopornografico" tracciando il percorso di questi files e segnalare tutti gli utenti che li condividono. La procedura degli accertamenti viene effettuata dagli investigatori rispettando la privacy e i diritti degli utenti.

Gli "addetti ai lavori" suggeriscono, per connettersi sul web in modo sicuro, di non aprire e-mail sospette inviate fraudolentemente a nome di grosse aziende (poste, banche, assicurazioni, ecc.) il cui oggetto potrebbe sembrare serio; queste di solito presentano evidenti errori di ortografia poiché i loro autori sono, molte volte, specialisti stranieri che non conoscono perfettamente la lingua italiana.

L'ultimo consiglio, ma non per questo meno importante, consiste nel verificare, quando si inseriscono dei dati riservati su una pagina web, di assicurarsi che la stessa sia protetta.

Le pagine protette sono riconoscibili poiché l'indirizzo che appare nella specifica barra di navigazione (browser) inizia con https:// e non con http://; inoltre deve comparire un lucchetto nella sezione situata in basso a destra, cliccando due volte su di esso si può verificare l'esistenza di un certificato che rappresenta la garanzia sull'autenticità del sito.

E' fondamentale controllare a chi (e da chi è stato rilasciato il certificato). Tuttavia, ogni volta che un utente accerta una anomalia di qualsiasi genere sul proprio PC, è possibile informare gli organismi investigativi attraverso denunce, querele e segnalazioni presso l'Ufficio della Polizia Giudiziaria più vicino alla propria residenza (Carabinieri, Guardia di Finanza, Polizia di Stato), il quale successivamente informerà gli "sceriffi del web", pronti a scovare ogni possibile internauta criminale. Per approfondire l'argomento abbiamo formulato alcune domande al Capitano Francesco Mandalari, uno dei più esperti collaboratori del GAT.

Il settore dell'informatica e internet sono in continua evoluzione: quali sono le nuove tecnologie utilizzate dalla criminalità informatica? Quali invece quelle messe a disposizione degli investigatori per contrastare il fenomeno?

"La criminalità si sta adeguando all'uso di tutte le tecnologie disponibili, ultimamente viene sfruttata la trasmissione dei dati attraverso le reti peer 2 peer, sistemi di trasmissione poco visibili, attraverso i quali viene scambiato tantissimo materiale pedopornografico; bisogna menzionare inoltre il VOIP, voice over IP, come sistema criptato di comunicazione difficilmente intercettabile. Il cyber crimine inoltre utilizza lo scambio di emails per finalizzare varie operazioni illecite, dal momento che tanti operatori offrono la possibilità di accedere a caselle di posta elettronica provenienti da providers stranieri; vi è poi il meccanismo del Proxy che consiste nell'uso di server attraverso indirizzi IP gestiti da fornitori di servizi di connettività esteri.

Questo comporta molte difficoltà per le Forze dell'Ordine perché bisogna instaurare dei rapporti di collaborazione internazionale con gli organi di Polizia omologhi dei paesi dove si trova materialmente il server utilizzato dai malviventi. Le tecniche criminali informatiche si basano quasi sempre sulle stesse procedure; il primo passo è quello del furto di identità per diventare invisibili. Recentemente è diventato famoso il fenomeno del BOTNET, che significa Robot Network, un sistema di reti costituito da diversi computer controllati dai criminali; a tal proposito c'è un dato statistico significativo, nel 2007 è stato calcolato, che su circa 600 milioni di computer collegati a internet nel mondo, l'11% era sotto il controllo di criminali che li utilizzavano come botnet, quindi persone che non erano i reali utenti; questo dato è attendibile, infatti lo troviamo sui bollettini del ced della Difesa. Attraverso la BOTNET, un criminale con buone conoscenze informatiche sfrutta i virus oppure le tecniche di port scanning, che consistono nell'invio di messaggi con lo scopo di capire quali sono le porte del computer aperte, dalle quali è possibile entrare; si tratta di porte virtuali predisposte per il trasferimento di dati anche all'interno del PC fra una pe-

riferica e l'altra. Sono più di 65000 le porte che sono predisposte dal computer, bisogna solo impostarle.

Il port scanning quindi va a sondare quali porte sono aperte per prendere il controllo del computer, che, una volta attivato, permette di costituire una rete di computers gestiti illecitamente.
Immaginiamo di controllare 1000 computers, se invio un'email al minuto con ognuno di essi, ci possiamo rendere conto di quante emails possiamo spedire con l'intento di frodare l'utente finale, magari attraverso il phishing.
Con la botnet si possono causare danni attraverso l'allagamento degli account di posta elettronica in modo tale da non consentire più il funzionamento del computer oppure impedire il ricevimento delle emails; il sistema è semplice, consideriamo che un server sia predisposto per la ricezione di un dato numero di emails, nel caso in cui lo stesso sia "obbligato" a rispondere a una quantità di richieste maggiore si trova a non poter gestire più la memoria e quindi va in crash, in questo modo il malvivente renderà indisponibile il servizio da parte di quel server.

Le tecnologie utilizzabili dagli investigatori invece dipendono dalle risorse economiche a disposizione. Tuttavia la migliore tecnica è quella derivante dalle qualità personale: l'acume investigativo. E' possibile individuare quali sono le caratteristiche di un fenomeno malavitoso, o una nuova tecnica di frode, attraverso dei segnali che derivano dalla navigazione individuati mediante il monitoraggio dei siti. Dal punto di vista pratico invece, oltre ai classici metodi d'intercettazione telematica, vengono utilizzati software che analizzano i comportamenti dei computers, come i programmi di datameaning usati per la ricerca di contenuti attraverso chiavi specifiche".

Quali misure di sicurezza consiglia di adottare per gli internauti che navigano sul web? E quest'ultimi quali rischi corrono?
"Il primo rischio è quello di subire il furto d'identità o dei dati personali; troppo spesso chi naviga non si rende conto della delicatezza delle informazioni che immette durante la connessione, pensiamo per esempio a un Curriculum Vitae dettagliato, dove è presente il nome, cognome e gli altri dati personali, resta solo da specificare quali siano le credenziali di accesso del proprio conto corrente bancario. Ci vuole quindi prudenza nell'immissione delle informazioni personali. Il sistema del cosiddetto web 2.0 poi, è quello che evidenzia le opportunità date dai social network con le comunicazioni attraverso le chat, con la possibilità di essere conosciuti nel mondo.
Tuttavia bisogna fare attenzione nella frequentazione dei siti, i cyber criminali infatti, cercano di sfruttare i punti di vulnerabilità delle persone; ci sono delle proposte di lavoro ad esempio, che arrivano via email, come collaboratore finanziario, il cui obiettivo è quello di ottenere la disponibilità di conti correnti "puliti" sui quali trasferire le somme precedentemente rubate da altri conti oppure attraverso carte di credito. Queste somme dovrebbero essere trasferite dal titolare del conto corrente mediante sistemi di money transfer come western union a soggetti che si trovano in altri Paesi. La proposta potrebbe essere accolta da un qualsiasi precario, uno studente senza reddito, un anziano in condizioni disagiate, è chiaro che il malvivente cerca sicuramente di sfruttare la vulnerabilità di questi soggetti. Per quanto riguarda il PC invece, è importante che il sistema operativo sia aggiornato, così come il firewall e l'antivirus che lo proteggono e sono dei validi sistemi di difesa che consentono di rilevare la presenza di spyware, **e trojan.**
Quest'ultimo è un virus che, grazie alla sua azione trasparente, consente di prendere il controllo e fare delle operazioni su un computer, senza che il suo legittimo utilizzatore se ne accorga. Lo spyware invece cattura le immagini dal video e le trasmette al malvivente che detiene il controllo del computer durante la connessione internet. Un'altra minaccia è rappresentata dal keylogger, in pratica si tratta di un software o hardware che memorizza tutto ciò che si digita sulla tastiera (per esempio l'inserimento della URL). A volte si corre anche il rischio di trovarsi inconsapevolmente coinvolti in attività illecite. I propri dati anagrafici per esempio, potrebbero essere riportati su una carta di credito ricaricabile utilizzata poi per commettere delle truffe; altro caso è quello dei portali di aste, dove può partecipare qualcuno che ha rubato i dati di un account associati ad un'altra persona, poi vende un oggetto che non sarà mai consegnato e offre come possibilità di pagamento, l'accredito su una carta ricaricabile accesa con i dati identificativi di un terzo, che ignaro e inconsapevole si troverà ad essere incriminato per quella truffa".

Le numerose operazioni investigative portate a termine si sono concretizzate con numerosi arresti? Quali tipi di misure cautelari sono state adottate dalla Magistratura per i cyber-crimini?
"In molti casi sì. Una cosa è certa, non credo che si possa parlare di proporzionalità fra il numero di interventi, denunce e arresti; spesso le informative devono essere redatte in un primo momento nei confronti di ignoti, proprio perché gli accertamenti che ci consentiranno poi di arrivare a identificare una persona o quanto meno il computer che fisicamente è servito per commettere una frode avverranno successivamente. Nei casi in cui il reato lo consente, come per esempio il riciclaggio o la pedopornografia, viene contemplato l'arresto in flagranza.

Tuttavia già per il possesso d'immagini pedopornografiche, in alcuni casi sono stati disposti la custodia cautelare in carcere o gli arresti domiciliari da parte della magistratura.
Personalmente sono stato coinvolto in diverse operazioni che sono terminate con 18 arresti; c'è stata poi un'altra brillante indagine relativa a truffe e altri reati legati alla tutela della privacy riguardanti i dati sensibili personali, la sostituzione di persona, il furto d'identità, l'intrusione abusiva in sistemi informatici, in una di queste operazioni abbiamo arrestato 5 persone. La natura e la gravità del reato quindi deve essere tale da consentire l'arresto in fragranza oppure la disposizione da parte del magistrato di misure cautelari, del resto la flagranza di reato è difficile da contestualizzare. Pertanto ci sono state una vasta gamma di operazioni, proprio perché il mondo del crimine informatico è sempre in continua evoluzione. Quella che ci ha fatto più inorgoglire riguarda la cattura di sei hackers che nel 2005 sono entrati perfino nel sistema informatico del Pentagono, avevano violato anche i siti istituzionali del Senato e dell'aeronautica, nonché vari siti istituzionali; erano sei ragazzi, uno maggiorenne mentre gli altri dai 14 ai 16 anni.
Siamo riusciti a prenderli proprio attraverso quel sistema combinato d'intuizioni investigative, esperienza tecnica e specializzazione, aggiungendo inoltre lo studio di determinati elementi, tipo l'indirizzo IP dal quale era partita una determinata connessione; abbiamo poi ricercato in rete ulteriori indizi scaturiti

da sfumature, che hanno consentito di individuare alcuni di questi cyber criminali che formavano il gruppo Hitech Hate (odio ad alta tecnologia), fino al momento in cui, quasi in diretta, è stato fatto l'intervento mentre si apprestavano a lanciare un attacco al sistema informatico di una azienda di rilevanti dimensioni".

Può tracciare un profilo dei criminali individuati? Sono tutti Hackers specializzati nelle violazioni di sicurezza?

"Sicuramente no; comunque dipende dal tipo di violazione commessa, possiamo dire che c'è anche qualcuno di loro che lo fa per divertimento. Generalmente il cyber criminale ha delle competenze tecniche, ed in base a queste compie reati più o meno gravi; come nel caso del Botnet per esempio, dove c'è bisogno di assumere il controllo di numerosi computers.

Sono invece sufficienti delle cognizioni di media rilevanza per potersi sostituire al mittente di un'email; a molti è capitato di ricevere un'email dal proprio indirizzo di posta elettronica.

E' un sistema attraverso il quale si riesce a manipolare l'intestazione della mail che è stata spedita inserendo il nome del destinatario come se fosse partita dalla propria casella di posta elettronica.

Pertanto i diversi gradi di conoscenza tecnica consentono di tracciare vari profili dei criminali informatici, possiamo menzionare i cosiddetti script kitties che hanno un livello di conoscenza minimo, sono perlopiù ragazzini che utilizzano gli script, cioè stringhe di comando reperibili su internet, attraverso i quali si possono fare dei tentativi di accesso sui sistemi informatici.

Può comunque verificarsi il caso in cui coloro che scaricano il virus per usarlo a terzi possano averlo in qualche format sul proprio computer e quindi da carnefici diventano vittime.

Poi c'è che confeziona dei malware (malicious software) che sono dei programmini usati per controllare un computer o eseguire su di esso delle attività, il più pericoloso di questi è il warm ovvero un virus che si replica nel computer fino a occupare tutta la memoria in modo da renderlo inservibile".

Oltre agli Hackers sono attivi sul web anche i crackers, quale differenza esiste tra queste due figure?

"L'hacker possiede un notevole livello di conoscenze informatiche e vuole dimostrare di poter violare determinati sistemi di sicurezza.

In sostanza la sua attività finisce qui, si può quindi considerare un puro, poiché si limita a lasciare un messaggio sulla home page del sito violato nel quale scrive: ecco, ho superato i vostri controlli!

Il cracker invece, ha un livello di conoscenze tale da consentirgli di entrare all'interno del computer, sebbene le sue azioni siano mirate alla distruzione di un sito, di un sistema oppure di dati; compie delle attività criminali che si verificano dopo l'intrusione abusiva nel sistema informatico.

Il cracker ad esempio potrebbe entrare in un database di una banca e prendere tutti i codici e le credenziali di accesso dei conti correnti al fine di usarle in seguito per ricaricare carte di credito e prelevare denaro agli sportelli ATM, oppure portare a termine delle estorsioni tramite l'invio di un'email, con la quale si chiede una determinata somma da accreditare su un conto oppure una carta di credito, altrimenti viene distrutto il sito oppure il server della vittima".

Quale misure di prevenzione sta adottando il vostro Nucleo Speciale per contrastare il fenomeno?

"La nostra opera si concretizza soprattutto con la prevenzione e la ricerca di nuovi sistemi di frode o violazione nei confronti degli utenti. Abbiamo anche intrapreso delle campagne di comunicazione attraverso conferenze e comunicati stampa per divulgare informazioni su fenomeni come il parcelling, una tecnica simile al phishing, con la quale alcune organizzazioni criminali reclutano degli internauti volontari.

Questi ultimi dovrebbero prestare la loro opera mettendo a disposizione per esempio la propria abitazione, oppure il proprio garage, per ricevere beni acquistati con denaro proveniente da carte di credito clonate oppure C/C il cui accesso è avvenuto illecitamente.

Questi beni, generalmente materiale Hi-Tech (Computers, TV al plasma, ecc.) dovrebbero essere teoricamente inviati ad altri destinatari come ospedali o orfanotrofi in costruzione nei Paesi del Terzo Mondo.

Il volontario ritiene di aver fatto qualcosa di buono, purtroppo si è prestato inconsapevolmente ad una attività di ricettazione o riciclaggio. Pertanto la campagna informativa ha come oggetto la sensibilizzazione della collettività verso fenomeni illeciti di questo tipo". ●