Figura 1. fonte: Internet Software Consortium (<www.isc.org>).

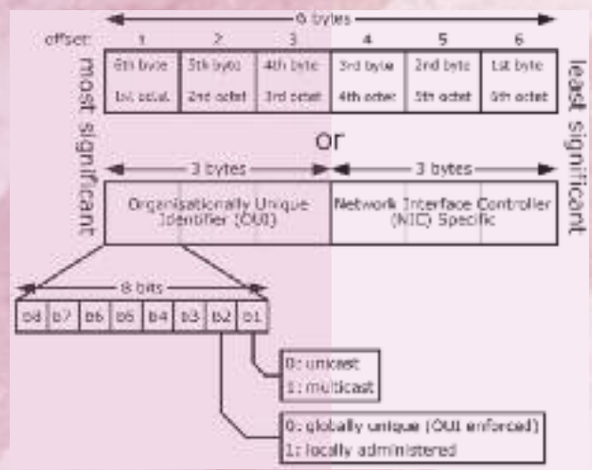
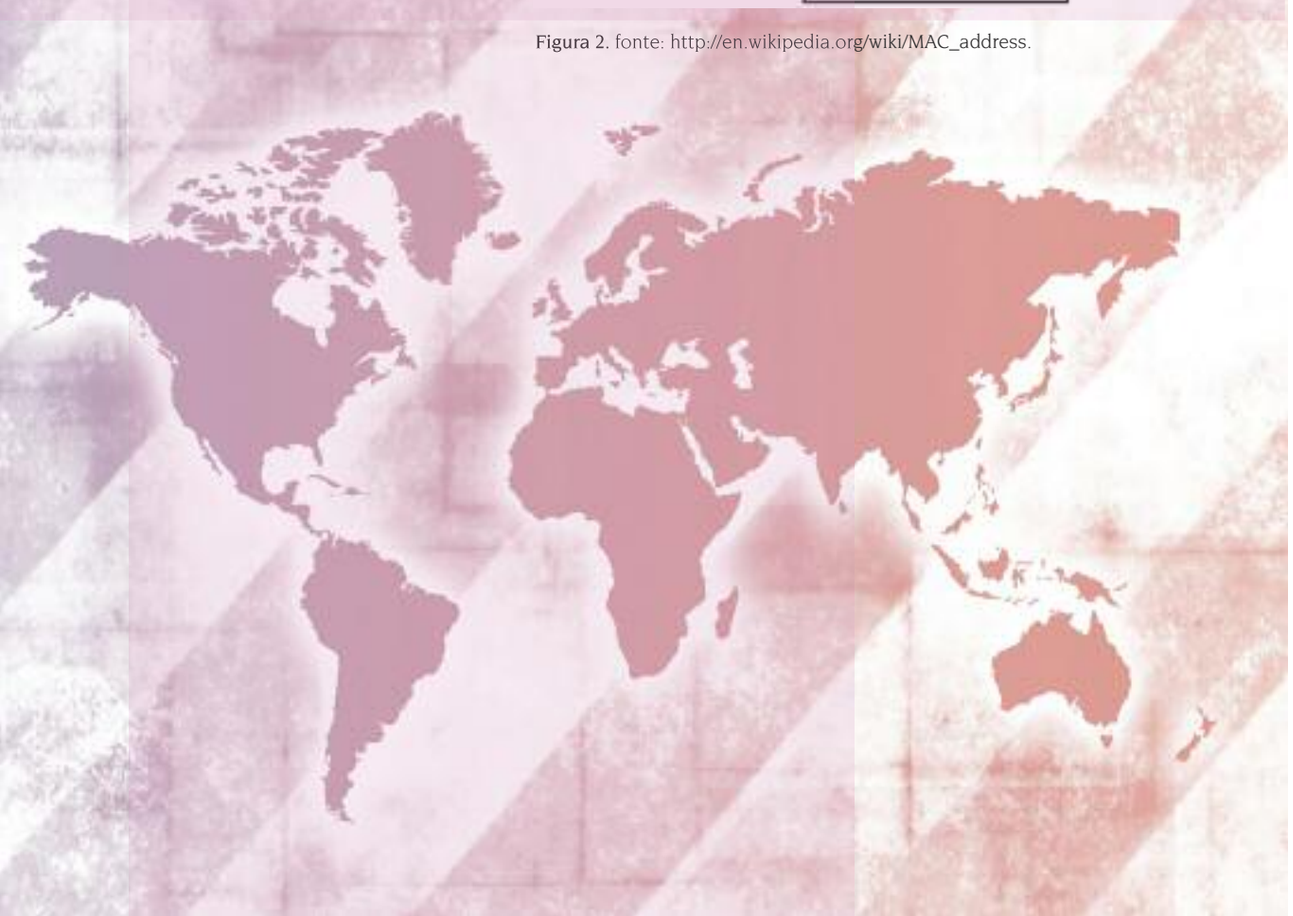


Figura 2. fonte: http://en.wikipedia.org/wiki/MAC_address.



Ixp e privacy delle telecomunicazioni

Giuseppe Arcangeli

La minaccia alla privacy delle telecomunicazioni è un tema sempre molto dibattuto e seguìto con attenzione dall'opinione pubblica, anche per la vasta eco mediatica riservata al caso Snowden-datagate e, più recentemente, al rapporto del Garante per la privacy sulle vulnerabilità degli snodi di rete, i cosiddetti Internet Exchange Point (Ixp). L'articolo, allo scopo di inquadrare con concretezza e verosimiglianza le possibili tipologie di minaccia alla privacy delle telecomunicazioni, è redatto nell'ottica di un ipotetico agente che intenda acquisire clandestinamente i dati circolanti negli Ixp. I temi trattati in tale prospettiva sono 'internet' (ambiente in cui si sviluppa la minaccia alla privacy) e 'intelligence tecnologica' (la minaccia più subdola poiché difficilmente rilevabile dalla 'vittima'), concludendo con alcune considerazioni sulla regolamentazione della privacy delle telecomunicazioni.

Internet: ambiente in cui si sviluppa la minaccia alla privacy

È noto che i sistemi informativi sono fortemente integrati nella vita quotidiana. Le tecnologie relative alle informazioni concentrano i dati (spesso sensibili) e ne incrementano la velocità di elaborazione e trasmissione, legando i risultati praticamente a ogni aspetto della vita sia del singolo che di organizzazioni sociali.
Internet può essere considerato il sistema di telecomunicazioni più globalizzato esistente. Il grafico riporta in modo inequivocabile il gigantesco trend di crescita della rete nel primo decennio d'utilizzo, di tale evidenza che non ha più senso analizzarne l'andamento negli anni successivi [figura 1].
Si ha così piena contezza di trovarsi in un mare magnum di dati informativi che, evidentemente, attira un numero altissimo di 'pescatori' alla ricerca di informazioni, disposti a tutto pur di ottenerle. Questa considerazione induce alla ragionevole certezza che è in atto una vera e propria guerra in direzione delle reti di comunicazione e dei sistemi informativi, la cosiddetta 'guerra cibernetica', riguardante sia la comunicazione globale che l'informatizzazione del lavoro e dei servizi, dei trasporti e dell'energia elettrica.
È interessante rilevare il rapporto che lega le competenze tecniche degli aggressori alla complessità dei cyber-attacchi. Risulta, infatti, che quest'ultima sia crescente a causa

delle tecnologie sempre più sofisticate dei sistemi-vittima e dei loro mezzi di difesa. La preparazione tecnica degli hacker segue, invece, un trend decrescente e ciò verosimilmente perché le tecnologie di attacco (in particolare i software) sono sempre più 'user-friendly'. Esistono in commercio, infatti, autentici 'kit' per compiere attacchi informatici e realizzare siti malevoli. Di solito tali kit sono usati contro le piccole imprese (in genere le più indifese, in quanto non dispongono di adeguati sistemi di sicurezza) al fine di 'rubare', ad esempio, le credenziali d'accesso agli account bancari[1].

Fatta questa breve panoramica, appare opportuno fissare l'attenzione su ciò che si intende per privacy delle telecomunicazioni: «Assicurare la privacy significa essenzialmente adottare tutte quelle misure idonee a proteggere la rete dalla divulgazione non autorizzata dei dati informativi (sia accidentale che intenzionale), dalla modifica o distruzione degli stessi dati o della rete stessa, dalla distruzione delle risorse di elaborazione della stessa rete (specialmente i software), dall'impossibilità per chi ne ha titolo ad accedere alla rete e ai suoi servizi».

L'esperienza ha dimostrato che le effettive minacce alla rete si manifestano essenzialmente in tre modi:

– minaccia umana non intenzionale: avarie accidentali all'alimentazione elettrica per mancanza-inadeguatezza-inefficienza di batterie tampone o gruppi elettrogeni; videoterminali lasciati accesi e senza sorveglianza; condivisione di una stessa password tra più soggetti (credenziali condivise);
– minaccia naturale: episodi meteorologici di particolare intensità, quali incendi, alluvioni o terremoti;
– minaccia umana intenzionale: spionaggio classico (portato essenzialmente verso il personale tecnico e/o amministrativo che opera ai vari livelli della rete), virus e vermi informatici, backup non autorizzati di dati (spesso operazioni non rilevabili a posteriori), Sigint (Signals Intelligence).

Privacy delle telecomunicazioni non significa, quindi, garantire esclusivamente la riservatezza dei dati, ma anche la continuità del funzionamento fisico delle reti e la possibilità di accedere regolarmente a esse da parte di chi ne abbia titolo.

La minaccia tecnologica, la più subdola: cosa è, come funziona e da chi proviene

La minaccia tecnologica necessita di notevoli risorse economiche, in quanto non può prescindere dal possesso di sofisticati sistemi elettronici, capaci di operare su un'ampia gamma di obiettivi. Il concetto può essere spiegato meglio con un esempio: i normali apparati di telecomunicazione massiva (ponti radio, satelliti ecc.) sono dispositivi molto

1. Alcuni esempi: 'Zeus Malware Kit' (Demo, in <www.youtube.com/watch?v=E0TQW82o8cc>). 'Search Engine Optimisation kits' <www.sophos.com/en-us/why-sophos/our-people/technical-papers/sophos-seo-insights.aspx?cmp=70130000001xGqlAAE> e 'Blackhole exploit kit' <www.nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-2/>.

complessi e con alti costi di realizzazione; pertanto, chi volesse dotarsi di un sistema per potervi accedere clandestinamente dovrebbe acquisire sistemi tecnologici molto più cari e sofisticati, in grado di operare su segnali spesso appena percettibili, filtrarli dal rumore elettronico e amplificarli, quindi, registrarne campioni significativi da memorizzare in una banca dati per successive analisi o riscontri.

Una volta individuati i segnali di potenziale interesse informativo, si procede all'acquisizione sistematica dei relativi flussi di trasmissione e alla loro successiva demodulazione e decodifica. In caso di contenuti cifrati (evidentemente i più appetibili dal punto di vista informativo), i dati vengono smistati a complessi sistemi di criptoanalisi per l'eventuale decrittazione. Acquisito il contenuto informativo dei dati (voce, e-mail, telefax, immagini, social network ecc.), un composito sottosistema di selezione automatica preleva le parti tematiche di maggiore interesse e le smista agli analisti, i quali 'lavorano' gli argomenti nelle diverse lingue in funzione della tipologia (militare, economica, criminale ecc.) e provvedono a valorizzarne i profili informativi redigendo rapporti per le strutture interessate, non senza averli prima archiviati in banche dati da consultare per successive analisi.

Affinché l'intero sistema tecnologico sia affidabile ed efficace nel tempo, bisogna poi procedere sia a un'oculata (quanto costosa) manutenzione, sia a un aggiornamento tecnologico-funzionale che deve seguire 'in tempo reale' gli sviluppi, oggigiorno sempre più frequenti, dei sistemi di telecomunicazione. Non sono, inoltre, trascurabili i costi per la formazione del personale tecnico e operativo, costi talvolta vicini a quelli degli stessi apparati tecnologici.

A tutto ciò si aggiunga che il mercato delle telecomunicazioni generalmente non offre sistemi di intelligence tecnologica, oppure, se ve ne siano, si tratta di sistemi tattici ovvero apparati finalizzati a soddisfare puntuali esigenze di polizia. È pertanto ineludibile ricorrere ai pochi Paesi che promuovono e finanziano ricerche nel settore, permettendo così a industrie specializzate (altamente sensibili, quindi controllate dai governi) di produrre idonei sistemi di intelligence tecnologica. È evidente che il loro approvvigionamento comporta che l'acquirente, oltre a un'adeguata disponibilità finanziaria, debba stipulare accordi bilaterali i quali, vista la delicatezza della materia, tendono spesso a realizzarsi a livello governativo. È bene tener conto del fatto che, di norma, i sistemi così ceduti sono quasi sempre 'degradati tecnologicamente' rispetto agli originali, e ciò – come è comprensibile – per evitare di devolvere integralmente a Paesi terzi le proprie capacità tecnico-operative e il relativo know-how.

Si riscontra, dunque, questa duplice esigenza per acquisire efficaci apparati d'intelligence tecnologica: ingenti finanziamenti e accordi bilaterali che richiedono, di frequente, interventi governativi.
Tutto ciò evidenzia come la minaccia tecnologica alla privacy delle comunicazioni globali sia normalmente demandabile a organizzazioni d'intelligence a livello di nazione[2]. È poi ragionevole ritenere che gli Ixp, data l'enorme quantità di traffico comunicativo gestito, rappresentino verosimilmente un obiettivo proficuo dal punto di vista costo-efficacia.
La disamina si sofferma, poi, sulla minaccia tecnologica dal punto di vista di chi è intenzionato a portarla contro un nodo di interscambio internet (Ixp). L'ipotetico aggressore, per avere possibilità di riuscita, opererà prevedibilmente per ottenere:

– accesso, fisico o virtuale (via rete), all'Ixp;
– conoscenza dell'Ixp, per individuarne 'punti deboli' mediante i quali accedere fisicamente o tramite rete e, quindi, acquisire il traffico informativo.

L'accesso fisico, posto che l'ubicazione degli Ixp italiani è pubblicata in internet, comporta solo che l'aggressore si adoperi per individuare il sito che, contraddistinto da palesi vulnerabilità, garantisca maggiori possibilità di successo nell'azione fraudolenta. Si può scegliere di avvalersi della collaborazione di operatori Humint, i quali, grazie alla rete informativa locale, possono venire a conoscenza di eventuali falle nel sistema di controllo degli ingressi e, in qualche caso, riescono persino a creare false credenziali di accesso. La stessa componente Humint, inoltre, potrebbe fornire informazioni sul tipo di apparati utilizzati[3], favorendo l'hacker nell'individuazione delle utenze idonee a inserirsi nella rete dell'Ixp, oppure nel predisporre adeguati pacchetti dati di manipolazione che, integrati illegalmente nei sistemi di trasmissione, possano essere gestiti da remoto con applicativi software. L'intruso, più semplicemente, una volta entrato nell'Ixp, potrebbe danneggiare o distruggere gli apparati cibernetici.
La difesa minima per ridurre l'entità di una simile minaccia è un buon sistema di controllo fisico degli accessi h24, ivi compresi sistemi anti-intrusione e telecamere di sorveglianza.

2. Gli Usa (Nsa) e la Gran Bretagna (Gchq), ad esempio, si sono dotati di Servizi quasi esclusivamente dedicati ad attività di intelligence tecnologica difensiva e offensiva.
3. Le principali ditte fornitrici non sono di difficile individuazione, in quanto operano in pochi Paesi a tecnologia avanzata. Talvolta la Humint riesce a ottenere anche i manuali tecnici degli apparati.

Nel caso italiano, tale minaccia appare particolarmente concreta, considerato che anche il Garante per la privacy ha evidenziato proprio un'insufficiente sicurezza fisica negli Ixp italiani[4]. La stessa Authority ha rappresentato anche l'inadeguatezza delle 'procedure di gestione'[5]: ciò potrebbe consentire all'ipotetico intruso di sfruttare eventuali credenziali condivise per attivare, ad esempio, le potenzialità di 'port mirroring'[6] e duplicare il traffico dati, per poi deviare altrove[7] la copia ottenuta. Tra l'altro, ove la segnalata inadeguatezza delle procedure riguardasse anche il monitoraggio di hardware/software, siffatte operazioni sarebbero difficilmente rilevabili; pertanto né l'Ixp, né tantomeno gli utenti 'vittima' avrebbero contezza immediata della minaccia portata alla privacy. L'accesso da remoto agli Ixp è ipotizzabile mediante particolari hardware e software in grado di inserirsi nella rete di trasmissione dati senza accedere fisicamente all'Ixp, in modo da 'forare' i firewall o altre eventuali difese Infosec[8]. È inoltre necessario considerare che i gestori connessi agli Ixp italiani sono anche stranieri (ad es.: At&T, Amazon, Facebook, Google, Microsoft, Verizon e altri), di talché gli eventuali accessi da remoto potrebbero teoricamente avvenire da una qualunque parte del globo.
La minaccia dell'intercettazione elettronica via etere (Sigint) sembrerebbe esclusa, poiché il traffico viene generalmente smistato dagli Ixp mediante cablaggi[9]. Sarebbe opportuno, tuttavia, verificare se a monte e/o a valle degli Ixp, il traffico (o parte di esso) segua delle tratte via etere, nel qual caso si aprirebbe anche la criticità Sigint.
Un'ultima considerazione riguarda il fatto che gli apparati dell'Ixp, essendo preposti allo smistamento dei dati, non esaminano i contenuti informativi, ma processano essenzialmente gli header dei singoli pacchetti. Ciò sembrerebbe ridimensionare la minaccia ma, a ben vedere, le cose non stanno proprio così. Negli header, infatti, si trovano i 'Media Access Control-Mac' (detti anche 'indirizzo fisico' o 'indirizzo Ethernet/Lan'), ciascuno dei quali è un vero e proprio indirizzo composto da un codice univoco esadecimale di 12 caratteri, necessario a identificare ogni scheda di rete (Ethernet o wireless) presente nel pc. Il 'Mac address', quindi, identifica univocamente un particolare apparato dotato di connettività internet (un router Wi-Fi, la scheda Ethernet di un computer, una stampante di rete, un Nas[10] ecc.) nel mare magnum dei dispositivi analoghi connessi on-line.

4. C. Bonini, «la Repubblica» (18 luglio 2014), p. 16.
5. *Ibidem*.
6. Il *Port Mirroring*, noto anche come *Switched Port Analyzer* (Span), è una funzionalità standard di duplicazione del traffico dati.
7. 'Altrove' può significare entità d'intelligence di Paesi ostili o, talvolta, concorrenti sul piano economico-industriale.
8. La storia recente offre esempi di organizzazioni d'intelligence (ma anche di singoli hacker) che sono riusciti a forare e/o eludere le difese Infosec di potenti organizzazioni governative, come il Pentagono e la Cia.
9. Il presente articolo non esamina tematiche Tempest.
10. Il *Network Attached Storage* (Nas) è un dispositivo collegato a una rete di computer ed è preposto alla condivisione di una memoria di massa (in genere hard disk) tra gli utenti della rete.

È interessante notare che le dodici cifre esadecimali del Mac address sono divise in sei coppie (o 'ottetti'). I primi tre ottetti (ovvero le prime sei cifre) identificano il produttore del dispositivo di rete e sono conosciuti come Organizationally Unique Identifier (Oui). Gli altri tre ottetti, detti Network Interface Controller (Nic), identificano serialmente il device e possono essere assegnati liberamente dal produttore. Si noti che il Mac address assegnato dal produttore viene definito a livello hardware, quindi non cambia nel tempo (a meno di interventi da parte dell'amministratore di rete) mentre, ad esempio, l'indirizzo Ip viene stabilito a livello software e può mutare anche a ogni nuova connessione alla rete [figura 2].

Alla luce di tale considerazione, il Mac address, più che un indirizzo, può essere considerato l'etichetta identificativa del device usato da uno specifico utente connesso alla rete e, come tale, rappresenta un dato oggettivamente sensibile.

Si è detto in precedenza che nel settore dell'intelligence tecnologica, dopo l'accesso ai dati, il più grande problema è la selezione, ossia la necessità di individuare, nella mole di dati, quelli di potenziale interesse. È di tutta evidenza che, vista l'enorme quantità di dati 'grezzi', le operazioni di selezione automatica mirano ad accertare se il traffico acquisito contenga determinati indicatori, tra i quali il Mac address.

Se si pensa che gli utenti dei device interessati sono (oltre che, naturalmente, i privati) organizzazioni governative, imprese, industrie, società e simili, appare chiaro che i Mac possono essere, da soli, oggetto di analisi per mezzo di software dedicati[11], in grado di ricostruire, ad esempio, la rete di contatti del Mac d'interesse. Insomma, per chiarire, con gli indirizzi Mac si potrebbe stabilire chi contatta chi, le quantità di comunicazioni dirette/originate ai/dai singoli utenti in rete e così via. Sulla base di tale analisi, l'intelligence è in grado di ottenere informazioni operative ed elementi utili per decidere su quali utenti attivarsi al fine di acquisire il contenuto informativo dei dati.

Assetto normativo sulla privacy delle telecomunicazioni

La sicurezza informatica, a mente della normativa vigente, è demandata al Presidente del Consiglio dei Ministri[12]. Sotto il profilo della sicurezza, però, la stessa normativa prevede che le reti di comunicazione elettronica rientrino nell'ambito delle attribuzioni di altre due pubbliche Istituzioni, ossia il Garante per le comunicazioni[13] e il ministero per lo Sviluppo economico[14].

11. Un tipico esempio di tali Sw è 'i2 analyst's notebook', in <www-03.ibm.com/software/products/it/analysts-notebook>.
12. D.lgs. 11.4.2011, n. 61 (G.U. n. 102 del 4.5.2011): 'Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione'.
13. Legge 31 luglio 1997, n. 249: 'Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo' (G.U. n. 177 del 31.7.1997 - Suppl. Ordinario n. 154).
14. Codice delle comunicazioni elettroniche (G.U. n. 214 del 15.9.2003 - Suppl. Ordinario n. 150).

Il Dpcm del 24.01.2013[15] apre la strada al coordinamento della sicurezza informatica, prevedendo l'adozione, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica (Cisr), di un P*iano nazionale per la protezione cibernetica e la sicurezza informatica nazionali*. Tuttavia, l'architettura definita sarà efficace solo se identificheranno inequivocabilmente le competenze di ciascun Ente[16], per evitare rischi del tipo 'rimbalzo di responsabilità', visto che i problemi di sicurezza degli Ixp, oltre a minacciare la privacy, incidono sulla sicurezza nazionale[17].

Ciò consente di sostenere che, nel terzo millennio, uno dei compiti principali degli Stati consisterà nel fronteggiare le minacce portate alle infrastrutture critiche (di una nazione e/o di un gruppo di nazioni alleate) tramite lo spazio cibernetico.

Alcuni Paesi e organizzazioni, sulla scorta dell'aggravarsi della minaccia, hanno già dato vita a strutture con competenza esclusiva in materia di guerra cibernetica, come il Cyber Command negli Usa (31.10.2010) e il Cooperative Cyber Defence Centre of Excellence della Nato (maggio 2008).

È quindi benvenuto il Piano italiano sulla sicurezza informatica[18] (Gazzetta Ufficiale n. 41 del 19 02.2014) che, inevitabilmente, dovrà interfacciarsi con le strategie degli alleati. Solo una strategia complessiva, infatti, potrà contrastare efficacemente una minaccia globale, coniugando il fine condiviso della sicurezza con i mezzi resi disponibili dai singoli paesi

G

15. Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, adottata con Decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, G.U. n. 66, del 19 marzo 2013.
16. Art. 1, comma 2: «I soggetti compresi nell'architettura istituzionale di cui al comma 1 operano nel rispetto delle competenze già attribuite dalla legge a ciascuno di essi».
17. C. Bonini 2014, p. 16.
18. <http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/piano-nazionale-cyber_0.pdf>.