Registration Authority Italiana

Editoriale:

Alcune considerazioni sul cybersquatting

Storie di cybersquatting

Nuove strategie e nuovi strumenti nella lotta al cybersquatting

La prima Convenzione europea sul cybercrime

eSafe: altri due anni di aiuti per un'Internet più sicura

Sempre più formazione mirata nei corsi della Registration Authority

Prevenire l'utilizzo abusivo dei futuri nomi a dominio sotto il country code ".eu"

I personaggi celebri e la registrazione abusiva di nomi a dominio: le nuove "guerre stellari"

N° 2
R.A. News
settembre 2002

Editorial

Considerations on cybersquatting

Stories of cybersquatting

New strategies and new tools in the fight against cybersquatting

Cybercrime in European black and white

eSafe: two more years of Safer Internet support

Increasingly targeted courses in the Registration Authority's future

Preventing the abusive use of future domain names under the country code ".eu"

Celebrities and abusive registration of domain name: the new "star wars"

Cybercrime: il lato oscuro della rete

Cybercrime: the dark side of the net

EDITORIALE

Il bello di Internet è di rendere incalcolabili quantità di informazioni accessibili a tutti, sempre, ovunque, comunque.
Attenzione: attraverso alcuni dei contributi di questo numero di RA news vi addentrerete in uno dei lati oscuri di Internet, di quell'enorme ragnatela dove i crimini stanno diventando rampanti, dove alcuni tipi di traffici o attività illecite hanno trovato un formidabile veicolo di diffusione e si stanno espandendo ad una velocità mai conosciuta prima d'ora.
Così, sempre più spesso si legge sui giornali della figlia di un noto corridore di auto, morto nel 1994 in un incidente sulla pista di Daytona negli Stati Uniti, che scopre che su un sito Web sono state pubblicate le foto, trafugate, dell'autopsia del corpo del padre; di 150 agenti del FBI quotidianamente impegnati nella lotta alla pornografia infantile su Internet che hanno arrestato 514 persone (nel 1996 erano "solo" 33 e avevano arrestato 68 persone); di un culturista morto per aver comprato ed assunto un certo tipo di droga, bandito dai governi mondiali per la sua pericolosità, ma reso disponibile agli acquirenti grazie ad un portale sulla rete; di un sito Web russo il cui nome, apparentemente innocente, poteva far pensare ad un negozio di fiori, ma che in realtà nascondeva centinaia di foto, filmati, video di bambini nudi in vendita (non esistendo specifiche leggi in materia in Russia, i due "impresari" artefici del tutto se la sono cavata con una condanna a sei mesi di detenzione).
Questo numero di RA news è dedicato al cybersquatting, ovvero al fenomeno dell'occupazione abusiva dei nomi a dominio, probabilmente il crimine più innocuo e nuovo legato al Web, considerando che gli altri sopra citati esistevano anche prima. Alcuni "luminari" della rete, interpellati sul cybersquatting, hanno dichiarato che non c'è rimedio a questo fenomeno se si vuol lasciare che la registrazione dei nomi a dominio prosegua sulla base della regola "first come, first serve". Ne hanno fatto e ne fanno tuttora le spese illustri politici ed attori, alcuni dei quali, grazie al Centro di Arbitrato sui nomi a dominio (soprattutto per i nomi a dominio registrati sotto i gTLD) dell'Organizzazione Mondiale per la Proprietà Intellettuale o tramite altri mezzi, si sono "riappropriati" del nome a dominio corrispondente al loro nome e cognome o al loro nome d'arte. Nel frattempo, però, sul sito Web che promanava dal nome a dominio erano state pubblicate informazioni di ogni genere e gusto.
Ci si può chiedere se, in alcuni casi, usando quella materia grigia che tutti - chi più, chi meno (così almeno si dice ed è stato provato da studi medici del settore) - dovremmo avere, non sia meglio "prevenire che curare". Con la speranza che il pensiero sia rivolto all'utente finale, al cittadino europeo, al consumatore sempre più tutelato da centinaia di regolamenti comunitari sulla materia, al bambino che, credendo di cliccare su un nome a dominio corrispondente ad un notissimo personaggio di Walt Disney, si trova di fronte due "siliconati gommoni" di qualche attrice del porno o ad esplicite proposte di estendere la sua non ancora sviluppata sessualità, lasciamo ai lettori l'ardua sentenza.

EDITORIAL

What is good about the Internet is that it supplies numberless pieces of information that are accessible to anyone, anytime, anywhere, anyway.
Warning: through some of the articles contained in this issue of RA news, you'll get into the meanders of one of the dark sides of the Internet, that huge spider web where crime is burgeoning, where some traffics or illegal activities have found an amazing means to spread everywhere and are growing at unparalleled speed.
Therefore, more and more often you read in the papers about the daughter of a famous motor racer, died in 1994 in an accident on Daytona's racing tracks in the United States, that discovered on a website the stolen pictures of the post-mortem made on her father's body; that 150 FBI agent, engaged every day in fighting child pornography on the Internet, have arrested 514 people (in 1996 they were "just" 33 and had arrested 68 people); that a body-builder died after buying and using a specific drug that had been banned by all the world's governments because it was too dangerous, but which could be bought on the web; that a Russian web site with an apparently innocent name, that apparently recalled a flower shop name, hid in fact hundreds of pictures, videos, films of naked children for sale (since there are no specific laws in Russia, the two "managers" who had organised it got off with a six-month sentence).
This issue of the RA news focuses on cybersquatting, the abusive registration of domain names, possibly the most harmless and newest crime related to the Internet, considering the others we mentioned already existed before.
Some "luminaries" of the web, asked what they thought of cybersquatting, said there is no way out of this phenomenon if we want to leave domain name registrations to continue to be supplied on a "first come, first served" basis.
This has cost and still costs a lot to some famous politicians and actors, some of whom, through the Domain Name Arbitration Centre (mainly for those domain names registered under gTLD) of the World Intellectual Property Organisation or other means, have "regained possession" of the domain names related to their family names or stage names.
But in the meantime details of all sorts and manners have appeared on the web sites linked to those domain names.
One might wonder if sometimes, using that grey matter that everyone should have - some more, some less (at least, so they say, and it has also been proved by some medical studies), "prevention wouldn't be better than cure".
But now, thinking about the end-users, about the European citizens, about the consumers more and more protected by hundreds of EU regulations, about those children who, believing they are clicking on the domain name of some well-known Walt Disney character, bump into two "huge silicon dinghies" of some porno actress or some explicit invitation to extend their still-underdeveloped sexuality, judge for yourselves.

Alcune considerazioni sul CYBERSQUATTING

di Ing. Stefano Trumpy

Come si identifica il cybersquatter? È una persona che registra nomi a dominio che sono identici o simili a nomi famosi, e/o che hanno un richiamo per il pubblico, con la intenzione di rivenderli, per trarne un profitto, oppure per attrarre un maggiore traffico sul proprio sito web o per danneggiare la reputazione del titolare del nome famoso (protetto da marchio o meno).

Per quanto riguarda la tipologia dello squatter, questo è in qualche caso un privato, in qualche caso un imprenditore che vende servizi a valore aggiunto o un accaparratore di nomi per rivendite future non meglio definite (wharehouser o meglio, immaganizzatore di nomi, come un noto personaggio italiano degli ultimi anni).

Ci si è domandati in passato se i nomi a dominio dovessero ritenersi legati alla proprietà intellettuale. La risposta dei tecnici è stata no, visto che questi sono stati concepiti come stringhe alfanumeriche in sostituzione di indirizzi numerici difficili da ricordare. Specie a seguito della affermazione dilagante dei servizi web e la progressiva espansione del commercio elettronico, la semantica delle stringhe alfanumeriche ha assunto importanza sempre maggiore e, sulla spinta dei legali chiamati a risolvere le dispute, anche i tecnici hanno dovuto accettare il fatto che la semantica conta. Resta il fatto che gli indirizzi in Internet devono preservare la loro unicità e pertanto il contenzioso deve risolvere anche casi di omonimie e di priorità sui diritti a detenere un determinato nome.

Sono sorte molteplici dispute con le prevalenti motivazioni che seguono:

- i nomi a dominio hanno acquisito un valore economico consistente in quanto spingono il pubblico ad accedere ad un sito web, qualora coincidano con un nome di richiamo od un marchio: ad esempio, il dominio "business.com" è stato venduto per 7.5 milioni di dollari;
- i nomi a dominio sono unici e per questo garantiscono una visibilità globale sulla rete; pertanto si possono creare conflitti tra marchi ed altre categorie di nomi protetti, qualora le stringhe alfanumeriche coincidano;
- i nomi a dominio sono normalmente concessi in uso dalle registration authority senza alcuna verifica preventiva del diritto al nome da parte del

Considerations on CYBERSQUATTING

by Eng. Stefano Trumpy

How do you identify a cyber-squatter? It's someone who registers domain names that are identical or similar to famous names and/or that are attractive to people, to the purpose of reselling them to make profit or to attract more traffic to one's own web site or to damage the reputation of the registrar of the famous name (whether protected by a trademark or not).

About the characteristics of squatters, they are sometimes private people, sometimes businessmen selling added-value services or hoarders of names for some vague future resale (warehousers, or better, name-storers, as a recent famous Italian character).

In the past, one wondered if domain names had to be regarded as related to intellectual property. The experts said no, since they have been designed as alphanumeric strings in lieu of numeric addresses that would have been difficult to remember. Especially after the rampant diffusion of web services and the progressive expansion of e-commerce, the semantics of the alphanumeric strings has become more and more important and, pressed by lawyers called in to settle disputes, the experts had to accept that semantics matter. The fact is Internet addresses have to remain unique and so the disputes also involve the coincidence of names and the priority of rights to a given name.

Many disputes have arisen above all for the following reasons:

- domain names have acquired substantial economic value, since they urge the public to access a web site if it is has the same name as a popular name or trademark: for instance the "business.com" domain was sold for 7.5 million dollars;
- domain names are unique and this is why they guarantee global visibility on the Internet; conflicts can therefore arise between trademarks and other types of protected names, if the alphanumeric strings are identical;

richiedente o comunque si accetta la assunzione di responsabilità del richiedente; l'eventuale revoca del nome non può quindi avvenire se non attraverso un giudizio a posteriori sulla "mala fede" del registrante.

Casi di cybersquatting (ove si presume e poi si accerta la mala fede):

- uso fraudolento di un nome a dominio: "qualunque persona che deliberatamente registra un nome a dominio facendo conto sulla sua uguaglianza/somiglianza al nome di una marca o marchio registrato o al nome di una organizzazione commerciale, può aspettarsi di ricevere una ingiunzione di cessare l'utilizzo del nome scelto";
- conflitto tra marchi registrati (per l'Italia si cita l'esempio di Ferrari autovetture e Ferrari vini); si noti che esistono anche i marchi di fatto, non necessariamente registrati, che possono offrire argomenti per protezione giuridica; nel caso che il detentore del marchio faccia un uso del nome aderente alla "ragione sociale" del marchio, deve comunque continuare a valere il principio "first come first served";
- conflitto con nomi geografici;
- conflitto con nomi farmaceutici internazionali;
- conflitto con diritto al nome di persone.

ICANN ha considerato il problema sin dalla sua costituzione ed ha varato il sistema URDP (Uniform Domain Name Dispute Resolution Policy) per frenare il problema del cybersquatting. Questo sistema, definito da WIPO, si applica prevalentemente ai gTLD ed a taluni ccTLD che si comportano come gTLD. Nel nostro paese, è stato adottato per il ".it" un sistema analogo alle URDP, adattato alla nostra realtà normativa. In genere questi sistemi si occupano prevalentemente di proteggere i marchi registrati ed in secondo luogo alcune delle categorie sopra

- domain names are normally assigned by registries without checking to determine if the applicant has a right to the name, and in any case the applicant is considered as liable for that; so the name cannot be deleted unless the applicant's 'bad faith' is ascertained later on.

Examples of cybersquatting (in which bad faith is first assumed, then ascertained):

- fraudulent use of a domain name: "anyone who deliberately registers a domain name relying on its identity/similarity to a brand name or trademark or name of a commercial organisation can expect to receive injunction to stop using the chosen name";

- conflict between registered trademarks (an example in Italy is Ferrari cars and Ferrari wine makers); notice that there are also distinctive (unregistered) marks, which have grounds for legal protection; if the trademark holder uses the name consistently with the "business name" of the trademark, the "first come first served" principle shall still apply;
- conflict with geographical names;
- conflict with international drugs names;
- conflict with people's right to names.

ICANN has been investigating the issue since its foundation and has launched the URDP (Uniform Domain Name Dispute Resolution Policy) system to curb the problem of cybersquatting. This system, as defined by the WIPO, mainly applies to gTLDs and to a few ccTLDs that behave like gTLDs. Our country has adopted a system similar to the URDPs, but adjusted to our legal system. These systems generally protect firstly the registered trademarks and secondly some of the categories specified above, giving priority

menzionate, con una attenzione maggiore ai nomi di persona. Più difficile è difendere i nomi geografici, i nomi di genere o comuni, ed altre categorie che non hanno una protezione legale ben definita. Non è ancora stata stabilita una graduatoria di protezione (ad esempio, se una persona ha un cognome che coincide con un marchio o con un nome di città, quale categoria è prevalente, e quale conta di meno?) In genere, coloro che impegnano più energie e denaro alla fine prevalgono, magari perché si fanno cedere il nome a dominio dietro adeguato compenso da chi lo ha registrato per primo, con buona pace dei cosiddetti "cyberlibertarian" che stigmatizzano il fatto che il partito commerciale prevale quasi sempre.

Il primo ordinamento giuridico che si è occupato del problema del cybersquatting è stato quello degli USA che poi è stato seguito da altri. Tali ordinamenti si basano, per esprimere le sentenze, sulla evidenza che una registrazione è stata effettuata in cattiva fede e questo succede allorquando:

- la registrazione è finalizzata alla vendita od alla concessione in uso al possessore del marchio od ad un suo concorrente per trarne un profitto;
- la registrazione è fatta allo scopo di impedire al possessore del marchio di registrare il proprio nome;
- la registrazione è fatta allo scopo di danneggiare la attività di un competitore;
- la registrazione è fatta nell'intento di avere vantaggi commerciali dall'attrarre gli utenti di Internet ad un sito con un nome famoso (inganno nei confronti dell'utenza e conseguente danno per il possessore del marchio).

Nel mondo reale, i contendenti preferiscono trovare vie negoziali private prima di imbarcarsi in dispute giuridiche che sono lunghe e costose.

Il mio parere è che le vie giudiziali ed extragiudiziali funzionano come deterrenti per frenare il fenomeno del cybersquatting ma certamente non lo estinguono. D'altro canto non sarebbe percorribile la via di dover verificare la titolarità del nome per tutte le richieste di registrazione. Sulla titolarità poi esiste una questione di fondo: la libertà di espressione deve o meno essere ammessa? Inoltre, se ad esempio una persona ha inventato uno slogan ma non lo ha protetto con una forma legalmente riconosciuta, ha questa persona il diritto di rivendicare quel nome? La risposta dei "cyberlibertarian" è negativa e comunque gli appigli legali sono molto deboli.
Una forma di difesa preventiva dei nomi è stata istituita dai nuovi registri generali cosiddetti "sponsored". Ad

to people's names. Defending geographical names, general or common names and other categories that do not have a well-defined legal protection is more difficult. A protection list has not been drawn up yet (for instance if someone's surname is the same as a trademark or a city's name, which category comes first and which one is less important?) Generally speaking, those who invest more energy and money are the winners in the end, maybe because they buy their domain from those who registered it first, in spite of the so-called "cyber-libertarians" who denounce that in most cases the commercial party is the winner.

The first legal system to have dealt with the problem of cybersquatting was the US one which was then followed by others. To pass sentences, these legal systems are based on evidence that a registration has been made in bad faith and this happens when:

- the purpose of the registration is to sell or rent it to the trademark holder or to a competitor for profit;
- the purpose of the registration is to prevent the trademark holder from registering his/her name;
- the purpose of the registration is to damage a competitor's business;
- the purpose of the registration is to reap commercial benefits from attracting Internet users to a site through a famous name (deception of users and indirect damage to the trademark holder).

In the real world, litigants prefer to find some private settlement before embarking on time- and money-consuming legal proceedings.

My opinion is that trials and amicable settlements act as deterrents and certainly play a part in curbing cybersquatting but they certainly do not put paid to it. On the other hand, having to check the ownership of all names requested for registration would not be practicable.
Then there is a basic question underlying ownership: is freedom of expression to be admitted or not? In addition, if for instance someone invented a slogan but did not protect it in any legally recognised manner, would one be entitled to claim ownership of that name? The "cyber-libertarians" say no, and in

esempio, il ".coop" (http://www.nic.coop) è riservato alle cooperative riconosciute come tali.
I registranti devono essere in grado di mostrare la loro iscrizione ad albi appositamente costituiti ed ogni richiesta è verificata prima di assegnare il nome. Risultato non trascurabile di questa procedura è che il costo annuale di un nome a dominio è pari ad 80 dollari.
Gli altri registri "sponsored" sono il ".aero" (http://www.nic.aero) ed il ".museum" (http://www.nic.museum).
Anche in questi casi, il registrante deve mostrare evidenza di "appartenere alla categoria" secondo standard riconosciuti ma che dovranno essere ulteriormente sviluppati per adattarsi alle diverse realtà nazionali.
In una prima fase ci saranno pertanto casi dubbi che nel seguito dovranno essere chiariti.
È evidente che l'introduzione di sponsored TLD darà un impulso alla razionalizzazione dei nomi utilizzati da certe categorie di utenti della rete.
Tutto questo implica un costo aggiuntivo nella registrazione dei nomi, così come abbiamo visto per il ".coop". Per questo tipo di domini si presuppone pertanto che il fenomeno del cybersquatting sarà molto ridotto, anzi praticamente trascurabile.

any case the legal grounds are very lame.
A type of preventative name defence has been established by the new general registries, the so-called "sponsored" registries. For instance, the ".coop" (http://www.nic.coop) has been reserved to those co-operatives that have been recognised as such. Applicants must be able to produce proof of their registration in specific rolls and every application is checked before assigning the name. A non-negligible result of thus procedure is that the yearly fee for a domain name is 80 dollars.
The other "sponsored" registries are ".aero" (http://www.nic.aero) and ".museum" (http://www.nic.museum).
Once again, the applicant must produce proof of "belonging to the category" according to recognised standards that shall have in any case to be further developed and adapted to each country. At the onset, there will certainly be uncertain cases that shall have to be investigated with time.
Obviously, the introduction of sponsored TLDs will boost a more rational use of the names chosen by certain categories of Internet users. All this involves an extra cost for domain name registration as we have seen for the ".coop". This type of domains is expected therefore to keep cybersquatting at bay or even completely get rid of it.

Storie di cybersquatting

di Avv. Patrizio Menchetti

Il cybersquatting ("to squat" in inglese significa occupare abusivamente) esiste da quando la registrazione di domini sulla rete è stata aperta anche ai privati. Come molte cose della rete, il fenomeno è iniziato negli Stati Uniti e si è gradualmente propagato nel resto del mondo. Inizialmente le aziende non si resero conto dell'importanza del nome a dominio come mezzo di valorizzazione dell'immagine o del prodotto aziendale. Si pensi che ancora nell'ottobre del 1994 circa i due terzi delle 500 maggiori società americane non aveva registrato un nome a dominio corrispondente ai propri marchi o alla propria ragione sociale. Infatti i primi casi storici non furono in realtà registrazioni a scopo speculativo, ma al contrario atti che volevano richiamare l'attenzione delle aziende sulla necessità di tutelare un cespite proprio registrando i domini corrispondenti ai marchi da queste detenuti.
Uno dei primi casi di questo tipo fu la registrazione del dominio "macdonalds.com" da parte di un giornalista americano, tale Quittner. La Mcdonalds aveva infatti

STORIES of cybersquatting

by Att. Patrizio Menchetti

Cybersquatting has existed since domain registration has been opened to private people as well. As many things in the web, the phenomenon started in the United States and gradually propagated to the rest of the world. At first, the business world did not realise how important domain names could be as a means to promote their products or reputation. Just think that, as late as October 1994, approximately two thirds of the 500 major US companies had not yet registered a domain name with their corporate name or brand. In fact, the first registrations were not for profit, but only aimed at recalling the companies' attention to the need to protect their assets by registering the domain names that coincided with their trademarks or brands.
One of the first examples was the registration of the "macdonalds.com" domain by a US journalist, a Mr. Quittner. Mcdonalds had only registered mcd.com, which in the US jargon means the famous hamburger. The journalist, after a good number of pieces asking his readers what he should do with the

registrato solo mcd.com, che in slang statunitense indica il celebre panino. Il giornalista, dopo una adeguata serie di articoli in cui chiedeva ai suoi lettori cosa dovesse fare del dominio "macdonalds.com", rinunciò al dominio in cambio di un finanziamento della Mcdonalds per l'accesso ad Internet in una scuola pubblica di New York. Il primo caso eclatante di cybersquatting tra concorrenti si verificò invece quando la società americana Princeton Review, che fornisce un servizio di preparazione agli esami, registrò il dominio "kaplan.com", corrispondente alla ragione sociale della Stanley Kaplan Educational Center, una azienda sua concorrente. Gli ignari utenti che digitavano "kaplan.com" convinti di finire sul sito della Kaplan si trovavano di fronte ad un sito web che, senza che vi fosse menzione che si trattasse di un sito della Princeton, presentava una tabella di comparazione tra i servizi offerti tra le due società, ed ovviamente qualificava come migliori i servizi offerti dalla Princeton. Alle richieste della Kaplan, la Princeton si offrì di trasferire il dominio in cambio di una cassa di birra, ma la Kaplan non la prese molto bene, e la questione finì di fronte ad un collegio arbitrale (che ovviamente si pronunciò in favore della Kaplan).

Anche gli enti pubblici sono stati parte in controversie relative a cybersquatting. Il comune di Saint Tropez a dovuto fare causa al web designer del suo sito che aveva registrato il dominio "saint-tropez.com". Il comune francese, in modo previdente, aveva anche registrato il marchio relativo ed il tribunale francese competente non faticò a dargli ragione.

Un altro intraprendente francese aveva invece registrato il dominio "interpole-info.com" dove, con il marchio Interpole informatique dalle sembianze grafiche pressoché identiche allo stemma di un'organizzazione di polizia, offriva in vendita una "carte interpole" dall'aspetto simile ai tesserini usati dalla polizia francese.

L'Interpol (titolare del dominio "interpol-pr.com") si è vista quindi costretta a far causa, ovviamente vincendola, al cybersquatter gallico.

Comunissimi sono poi i casi di chi ha registrato un ccTLD identico al gTLD di una delle più note dotcom per fornire identici servizi e trarre in inganno i consumatori. Ad esempio, in Grecia "amazon.com" ebbe ragione nella controversia che la contrappose ad una libreria greca che aveva registrato il dominio "amazon.com.gr" e che dichiarava di essere "la più grande libreria di tutta la Grecia".

Il tribunale di Syros stabilì che vi erano sufficienti motivi per indurre il consumatore a credere che la libreria greca fosse una filiale di "amazon.com".

"macdonalds.com" domain, gave up the domain in exchange for Mcdonalds' funding for the provision of Internet access to a New York public school.

The first glaring case of cybersquatting between competitors was when the US Princeton Review company, which offers exam training services, registered the "kaplan.com" domain which coincided with his competitor Stanley Kaplan Educational Center's corporate name. The unwary users who entered "kaplan.com" on their keyboards, sure they would get to Kaplan's web site, found a web site which, without mentioning it belonged to Princeton, showed a table of comparisons between the services supplied by the two companies where the services offered by Princeton obviously scored higher.

On Kaplan's request, Princeton volunteered to transfer the domain in exchange for a crate of beer, but Kaplan took it badly and the issue ended up before an arbitration panel (which obviously declared themselves in favour of Kaplan).

Public boards have also been involved in controversies on cybersquatting. The City Council of Saint Tropez had to sue the web designer of its web site who had registered the "saint-tropez.com" domain. The French City Council had been prudent enough as to register the attendant trademark as well and it didn't take long for the French court to prove them right. Another resourceful Frenchman had registered, instead, the "interpole-info.com" domain in which he offered for sale, under the Interpole informatique trademark whose graphics were essentially identical to the badge of a police organisation, a "carte interpole" which looked like the ID cards used by the French police. Interpol (the registrar of the "interpol-pr.com" domain) had therefore to sue the Gallic cyber-squatter and win of course the case.

In addition, there are plenty of cases of people registering a ccTLD identical to the gTLD of one of the best-known dot.coms to supply the same services and deceive the consumers. For instance, in Greece "amazon.com" won the case against a Greek bookshop, which had registered the "amazon.com.gr" domain stating they were "the largest bookshop in Greece". The Syros Court "saw sufficient grounds

La fantasia dei cybersquatters ha veramente pochi limiti, se si pensa che lo stesso dominio del registro TLD è stato oggetto di cybersquatting. I più "vecchi" della rete ricorderanno che la Network Solutions, ora controllata da Verisign, operava originariamente per conto della National Science Foundation sotto il dominio "internic.net", da cui cominciò ad offrire le prime registrazioni via Internet e carta di credito dei domini di secondo livello su gTLD ".com", ".net" e ".org". Una società australiana, la Internic Pty, pensò bene di registrare il dominio "internic.com" e poi di offrire, tramite un sito che ricordava nella grafica quello della Network Solutions, le stesse registrazioni, ma ad un prezzo quasi doppio, confidando nel fatto che gli utenti meno esperti sarebbero stati naturalmente portati a digitare "internic.com" piuttosto che "internic.net". Purtroppo per gli intraprendenti cybersquatters, in Australia opera una occhiutissima agenzia federale di protezione del consumatore, che, avvertita dalla Federal Trade Commission statunitense, trascinò prontamente la Internic Pty in tribunale per violazione delle norme sulla protezione del consumatore.
Come "ciliegina" finale, si può ricordare quell'americano che aveva registrato i domini "bbb.com" e "bbb.net" per offrirli in vendita al Better Business Bureau, una organizzazione statunitense di protezione del consumatore che opera attraverso il sito "bbb.org". e che ha tra le altre sue funzioni anche quella di segnalare offerte truffaldine.

to make consumers believe the Greek bookshop was a branch of "amazon.com". The cyber-squatters' imagination is really limitless if you just think that even the domain of the TLD registry fell prey to cybersquatting.
The "veterans" of the web will probably remember that in the past Network Solutions, now a subsidiary of Verisign, worked for the National Science Foundation under the "internic.net" domain, from where it began to offer the first second-level domain registrations under the ".com", ".net" and ".org" gTLDs, using the Internet and credit cards. An Australian company, Internic Pty, thought it better to register the "internic.com" domain, then to offer, through a site whose graphics recalled that of Network Solutions, the same registrations at almost twice the price, confiding that less experienced users would have naturally been led to enter "internic.com" rather than "internic.net".
Unfortunately Australia is watched over by an eagle-eyed Federal Consumer Protection Agency which, warned by the US Federal Trade Commission, promptly hauled Internic Pty to court on the grounds of breaching consumer protection regulations.
As the last straw, let's mention that American man who registered the "bbb.com" and "bbb.net" domains to sell them to the Better Business Bureau, a US Consumer Protection Organisation which operates through their "bbb.org" site and one of whose tasks is also to report on fraudulent activities.

NUOVE STRATEGIE e nuovi strumenti nella lotta al cybersquatting

di Andrew McLaughlin, Senior Adviser, ICANN

Negli ultimi mesi, ICANN ha approvato due importanti ed innovativi piani d'azione riguardanti lo spazio dei domini top-level generici globali (gTLD): (1) il Redemption Grace Period, e il Servizio (2) VeriSign Registry Waiting List. Questi due piani d'azione hanno obiettivi, portata e meccanica diversi, ma ognuno costituisce uno strumento nuovo, potente e utile per gli utenti di Internet nella continua lotta al fenomeno del cybersquatting.

1. Redemption Grace Period

A partire dall'inizio del 2001, ICANN ha notato una crescente ondata di problemi e di lamentele sulla cancellazione di registrazioni di nomi a

NEW strategies and new tools in the FIGHT against cybersquatting

by Andrew McLaughlin, Senior Adviser, ICANN

In recent months, ICANN has approved two innovative and important new policies for implementation in the global generic top-level domain (gTLD) space: (1) the Redemption Grace Period, and (2) the VeriSign Registry Waiting List Service. These two policies are different in their objectives, scope, and mechanics, but each will constitute a useful and powerful new tool for Internet users in the ongoing fight against cybersquatting.

1. Redemption Grace Period

Beginning in early 2001, ICANN observed a growing wave of problems and complaints in connection with the deletion of domain name registrations in the

dominio nei gTLD. Lo schema era evidente: una società o un'organizzazione o un privato perdevano involontariamente il diritto ad un nome a dominio; successivamente, quel nome a dominio veniva nuovamente registrato da qualcuno che in mala fede deviava il traffico verso i propri siti e/o chiedeva un profumato riscatto per la restituzione del nome a dominio. In alcuni casi, il pirata cercava di aumentare il prezzo del riscatto del nome a dominio indirizzandolo a contenuti mirati a far arrabbiare, infastidire o mettere in imbarazzo il titolare originario. Ad esempio, come è avvenuto in celebri casi, i nomi a dominio di alcuni gruppi ecclesiastici venivano cancellati, registrati da terzi e poi indirizzati verso materiale pornografico spinto.

I domini possono essere cancellati senza il consenso intenzionale del titolare per vari motivi:

- errori dei titolari dei nomi: si tratta probabilmente della causa più frequente di cancellazioni involontarie. I titolari del dominio talvolta lasciano involontariamente scadere le proprie registrazioni per errori d'ufficio o per la mancata ricezione dell'avviso di rinnovo (in genere perché il titolare del nome dimentica di tenere aggiornati i propri dati di contatto in caso di trasferimento o di cambio di Internet service provider). Può, inoltre, accadere che il titolare del nome a dominio non faccia accidentalmente caso all'avviso di rinnovo o lo scambi per un sollecito o per posta spamming.

- errori del registrar: possono verificarsi se il registro non informa il titolare del nome che il suo nome a dominio sta per scadere, magari a causa di un virus nel sistema automatico. Le procedure in atto per la gestione degli errori dei registrar chiedevano la volontaria collaborazione sia del registro in fallo che di quello a cui il titolare si rivolgeva successivamente – ma si dimostravano spesso inefficaci per la prevedibile riluttanza di questi ultimi a rinunciare alla registrazione per rimediare a un errore commesso da un altro registrar.

- frode e pirateria: si verificano quando, ad esempio, un aspirante cyber-squatter in mala fede si inserisce abusivamente nell'account del titolare del nome presso registrar, modifica i suoi dati di contatto, chiede la cessione della registrazione ad un altro registrar e poi fa domanda di cancellazione della registrazione al nuovo registrar. Il pirata registra poi immediatamente il dominio tramite un terzo registrar. "Riciclando" il dominio rubato

gTLDs. The pattern was easy to detect: A business, organization, or individual registrant would unwittingly lose its rights to its domain name; thereafter, the domain name would be re-registered by an unfriendly third party that would redirect traffic to its own sites, and/or demand a high ransom for the return of the domain name.

In some cases, the hijacker would seek to increase the ransom value of the domain name by pointing it to content intended to anger, irritate, or embarrass the original registrant. For example, in several well-known cases, domain names held by church groups were deleted, registered by third parties, and then aimed at hard-core pornographic material.

Deletions can occur without the intentional consent of the registrant for a number of reasons:

- registrant mistakes are probably the most common cause of unwanted deletions. Registrants sometimes inadvertently allow registrations to lapse due to a clerical mistake or failure to receive a renewal notice (usually as a result of the registrant's failure to keep his/her registration contact information up-to-date when moving or changing Internet service providers). Also, some registrants may accidentally overlook a renewal notice or mistake it for a solicitation or spam.
- registrar mistakes sometimes occur, when the registrar fails to notify the registrant about the pending expiration of his/her domain name, perhaps as a result of bugs in its automated systems.

Existing procedures for handling registrar mistakes required voluntary cooperation by both the losing and the gaining registrar – but often proved ineffective because of gaining registrars' predictable reluctance to lose the registration in order to correct another registrars mistake.

- fraud and hijacking would occur when, for example, a malicious would-be cybersquatter would hack into the registrant's account at the registrar, modify the registrant's contact information, request a transfer of the registration to another registrar, and then issue a request to the new registrar to delete the registration. The hijacker would then register the domain

attraverso due, tre o più registrar, il pirata può veramente impedire la correzione dell'errore originario e la restituzione della registrazione al legittimo titolare.

In tutti questi casi, le vittime erano titolari di nomi a dominio e i beneficiari erano i cyber-squatters – coloro che cercano di trarre vantaggio dalla violazione dei diritti legittimi e delle aspettative dei titolari di nomi a dominio.
Per risolvere questa serie di problemi, ICANN ha adottato il Redemption Grace Period per i gTLD non sponsorizzati (attualmente .biz, .com, .info, .name, .net e .org).
In breve, il Redemption Grace Period crea una nuova "rete di sicurezza" – un periodo di 30 giorni successivo alla cancellazione di qualsiasi nome a dominio durante il quale il titolare, l'registrar o l'operatore del registro possa rilevare e risolvere cancellazioni errate, involontarie o fraudolente.
Durante il periodo di grazia, il nome cancellato viene messo in status "registry-hold", cioè il nome non opera/non si annulla (il che tende ad attrarre immediatamente l'attenzione del titolare sull'imminente cancellazione), ma non è comunque disponibile ad essere registrato da terzi.
Riassumendo, il Redemption Grace Period è un meccanismo semplice ed efficace che minimizza le cancellazioni involontarie, che sono quelle che offrono ai cyber-squatters le maggiori opportunità di estorsione.

2. Servizio VeriSign Registry Waiting List

Nel marzo 2002, VeriSign (operatore del registro dei gTLD.com e .net) ha chiesto l'approvazione di un test di 12 mesi per il nuovo Waiting List Service (WLS). Dopo vari mesi di intense analisi e dibattiti all'interno della Domain Name Supporting Organization di ICANN, il consiglio di amministrazione di ICANN ha votato ad agosto l'approvazione di una prova di 12 mesi del WLS da varare non prima di sei mesi dall'attuazione del Redemption Grace Period.
Il Waiting List Service consente ai registrar di prenotare per conto dei clienti i nomi a dominio .com e .net già registrati. E' consentita un'unica prenotazione per ogni nome a dominio registrato, ogni registrazione vale un anno e le prenotazioni sono accettate in ordine cronologico di richiesta. I registrar devono pagare una normale quota al registro per la prenotazione, ed ogni registrar è libero di fissare il proprio prezzo di mercato per la rivendita ai clienti. Per rendere il servizio trasparente e proteggere nello stesso tempo la

immediately through a third registrar. By "laundering" the stolen domain through two, three, or more registrars, the hijacker could make it very difficult to correct the original error and get the registration restored to its legitimate registrant.

In all of these cases, the victims were domain name holders and the beneficiaries were the cybersquatters – those who seek to profit by violating the legitimate rights and expectations of domain name registrants.
As a solution to this set of problems, ICANN has adopted a Redemption Grace Period for the unsponsored gTLDs (currently .biz, .com, .info, .name, .net and .org).
In summary, the Redemption Grace Period creates a new "safety net" – a period of 30 days following any deletion of a domain name in which the domain name registrant, registrar, or registry operator can detect and correct any inadvertent, mistaken, or fraudulent deletions.
During the grace period, the deleted name is placed on "registry-hold" status, which means that the name does not function/resolve (which tends to bring immediate registrant attention to the impending deletion), but also that the name is not available for registration by third parties.
In short, the Redemption Grace Period is a simple, effective mechanism that minimizes the inadvertent deletions that give cybersquatters their greatest opportunities for extortion.

2. VeriSign Registry Waiting List Service

In March 2002, VeriSign (the registry operator for the .com and .net gTLDs) requested approval to initiate a 12-month test of a new Waiting List Service (WLS). After several months of intensive analysis and debate within ICANN's Domain Name Supporting Organization, the ICANN Board voted in August to approve a 12-month trial of the WLS, to be launched no earlier than six months after the implementation of the Redemption Grace Period.
The Waiting List Service allows registrars, acting on behalf customers, to place reservations for currently-registered .com and .net domain names. Only one reservation is allowed for each registered domain name; each reservation is for a one-year period; and reservations are accepted on a first-come/first-served basis. Registrars must pay a common registry fee for reservations, and each registrar is free to set its retail market price for customers. In order to provide some transparency to the service, while protecting

privacy, il registrar ha l'obbligo di informare il titolare del nome a dominio di eventuali prenotazioni fatte su quel nome, ma senza rivelare l'identità del titolare della prenotazione. (inoltre, mantenendo riservata l'identità del titolare della prenotazione WLS, i titolari correnti del nome a dominio sono meno incentivati a diventare essi stessi dei cyber-squatters rinnovando le registrazioni unicamente allo scopo di estorcere denaro all'abbonato WLS in lista d'attesa. In pratica, ecco come funziona la WLS: quando viene cancellato dal registro un nome a dominio .com o .net (alla scadenza del Redemption Grace Period), il VeriSign Registry verifica se tale nome sia già stato prenotato. In caso affermativo, il nome viene assegnato a quel registrar; il registrar registra il nome a favore del cliente e vengono effettuati i pagamenti del caso (la quota di registro da parte del registrar, e il prezzo al pubblico da parte del richiedente al registrar). In mancanza di prenotazioni, il VeriSign Registry cancella il nome dal registro e lo rimette tra i nomi registrabili da qualsiasi utente Internet con assegnazione in ordine cronologico di richiesta.
La speranza è che, fornendo un meccanismo prevedibile, equilibrato e trasparente per la prenotazione dei singoli nomi a dominio, la WLS riduca notevolmente le opportunità di arricchimento disonesto, abusivo e speculativo sui nomi a dominio che alimenta l'industria del cybersquatting. Anche se la WLS vale soltanto per i domini .com e .net, altri registri gTLD e country-code TLD seguiranno da vicino i 12 mesi di prova per verificarne la percorribilità e il valore per gli utenti di Internet.

privacy, there is a requirement that the registry must notify the current domain-name registrant whenever a reservation has been placed on the name, but without revealing the identity of the party holding the reservation. (Also, keeping confidential the identity of the WLS reservation holder gives current domain name holders less of an incentive to become cybersquatters themselves by renewing registrations solely to extort money from the waiting WLS subscriber).In practical terms, here's how the WLS works: When a registered .com or .net domain name is deleted from the registry (after the expiration of the Redemption Grace Period), VeriSign Registry checks to determine whether a reservation for that name is in effect. If so, the name is assigned to that registrar; the registrar registers the name to the customer; and the usual payments are made (the registry fee by the registrar, and the registrar's retail price by the registrant). If there is no reservation, VeriSign Registry deletes the name from the registry, returning it to the pool of names that are openly available for registration by any Internet user on a first-come/first-serve basis.The hope is that by providing a predictable, balanced, and transparent mechanism for individual domain name reservations, the WLS will massively reduce the opportunities for the kind of abusive and speculative domain name profiteering that fuels the cybersquatters. Though the WLS applies only to the .com and .net domains, other gTLD and country-code TLD registries will be watching the 12-month trial closely to assess its workability and value to Internet users.

La PRIMA Convenzione europea sul cybercrime

di Peter Csonka, Vicedirettore divisione crimini economici, Consiglio d'Europa

Le società moderne dipendono fortemente dall'uso di computer collegati in rete, offrendo così molti target in tutti i settori della società. Se non affrontato, il cybercrime rappresenta una grave minaccia per la salute e la sicurezza dei cittadini e può invalidare le potenzialità di Internet come strumento di comunicazione, di commercio e di espansione delle opportunità formative di tutti i popoli del mondo.
In risposta, il Consiglio d'Europa ha creato nel 1997 un Comitato di Esperti sul Crimine nel cyber-spazio (il Comitato "PC-CY") per affrontare le questioni del cyber-crime (o computer crime) e della procedura penale nel settore dell'informatica.

CYBERCRIME in European black and white

by Peter Csonka, Deputy Head of Division, Division of Economic Crime, Council of Europe

Modern societies are heavily dependent on computers that are networked, and thus offer many targets across every sector of society. Left unchallenged, computer crime poses a serious threat to the health and safety of citizens and may stifle the Internet's power as a tool to communicate, engage in commerce, and expand people's educational opportunities around the globe.
In response, the Council of Europe set up in 1997 the Committee of Experts on Crime in Cyberspace (Committee "PC-CY") to deal with cybercrime (computer crime) and criminal procedure problems linked with information technology. It was given the task of preparing a legally binding instrument.

Il Comitato è stato incaricato di preparare uno strumento legalmente vincolante. Il comitato ha ultimato i lavori alla fine del 2000 e ha collaborato strettamente con il G-8 e altri enti internazionali alla redazione di una Convenzione sul cybercrime.
Il Comitato europeo sulla criminalità informatica ha approvato la versione finale della Convenzione nel giugno 2001.
Il Comitato dei Ministri ha adottato la Convenzione sul cybercrime l'8 novembre 2001, presentandola alla firma il 23 novembre 2001 a Budapest, in occasione della conferenza internazionale tenuta a Budapest il 22 e il 23 novembre 2001. La Convenzione (Convenzione di "Budapest") è stata firmata da 30 stati, tra cui 26 stati membri del Consiglio d'Europa e 4 stati non membri che avevano partecipato alla sua redazione.
La Convenzione sul cybercrime è assolutamente innovativa essendo il primo accordo multilaterale ad affrontare specificamente i problemi posti dall'internazionalità del cybercrime.
Questo strumento multilaterale elimina o minimizza i vari ostacoli procedurali e giurisdizionali che possono ritardare o compromettere le indagini e i procedimenti giudiziari internazionali sui crimini collegati all'informatica.
La Convenzione è innovativa soprattutto in quest'area (1) imponendo ai paesi firmatari di stabilire alcuni reati sostanziali nel settore del cybercrime, (2) imponendo alle parti di adottare norme procedurali interne per l'indagine del cybercrime e (3) fornendo una solida base per la collaborazione all'attuazione di leggi internazionali contro i reati commessi tramite sistemi informatici.

I futuri firmatari di questa Convenzione ne trarranno diretto vantaggio, avendo a disposizione metodi migliori per ottenere aiuti internazionali dalle altre parti in caso di reati informatici, in particolare perché gli altri firmatari della Convenzione avranno più o meno le stesse definizioni minime di cybercrime e gli strumenti procedurali interni necessari ad indagare tali reati.
La Convenzione e il relativo rapporto esplicativo sono disponibili sul sito web del Consiglio d'Europa: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/

The Committee has completed its work at the end of the year 2000 and worked in close co-ordination with the G-8 and other international bodies on a the draft Convention on Cybercrime.
The European Committee on Crime Problems approved the final draft of the Convention on cyber-crime in June 2001.
The Committee of Ministers adopted the Convention on Cybercrime on 8 November 2001, which was then opened for signature on 23 November 2001 in Budapest, on the occasion of an international conference organised in Budapest on 22 and 23 November 2001. 30 states signed the Convention (the "Budapest" Convention), among which 26 Council of Europe member States and 4 non-member States which had participated in the drafting.
The Convention on Cybercrime breaks new ground by being the first multilateral agreement drafted specifically to address the problems posed by the international nature of computer crime.
This multilateral instrument removes or minimizes the many procedural and jurisdictional obstacles that can delay or endanger international investigations and prosecutions of computer-related crimes.
The Convention makes particularly progress in this area by (1) requiring signatory countries to establish certain substantive offenses in the area of computer crime, (2) requiring parties to adopt domestic procedural laws to investigate computer crimes, and (3) providing a solid basis for international law enforcement cooperation in combating crime committed through computer systems.

Future parties to this Convention will directly benefit from it by having better methods of obtaining international assistance from other parties in computer-related crime cases, particularly because the other parties to the Convention will have similar minimum definitions of computer crimes and the domestic procedural tools needed to investigate those crimes.
The Convention and its Explanatory Report can be found at the Council of Europe's website: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/

eSafe: altri due anni di aiuti per un'Internet più sicura

di Richard Swetenham, Safer Internet Action Plan, Commissione europea

I contenuti illegali e dannosi su Internet, di qualsiasi forma o aspetto essi siano, continuano a preoccupare i legislatori, l'industria e le famiglie. Per i bambini o le famiglie che sentono parlare solo dei lati positivi di Internet, la navigazione in rete è un territorio inesplorato. Le nuove tecnologie stanno, inoltre, dando vita a nuove minacce, mentre le minacce già esistenti cominciano appena ed essere universalmente riconosciute.L'Unione europea è all'avanguardia nella lotta contro i contenuti illeciti e dannosi dal 1996. Una delle sue armi principali è stato il Safer Internet Action Plan (IAP) di durata quadriennale, dal 1999 al 2002. Il Piano è un'iniziativa dell'Unione europea per affrontare più efficacemente il problema dei contenuti illegali e dannosi, tra cui la pornografia infantile, i contenuti violenti/razzisti e i siti fautori del terrorismo. L'approccio si basa sull'offerta all'utente di informazioni e strumenti che lo rendano più responsabile. Il Piano si sviluppa su tre versanti: la creazione di un ambiente più sicuro tramite una rete europea di hotline e l'incentivazione dell'auto-normativa e di codici comportamentali; la messa a punto di sistemi di filtraggio e valutazione; e la promozione di azioni di sensibilizzazione.

Uno sguardo su eSafe

La Commissione europea ha proposto di prorogare l'attuale piano d'azione per altri due anni col nome di eSafe. Nella preparazione del programma successivo, la Commissione ha consultato i relativi attori. Il supporto al coordinamento è stato travolgente nel settore del miglioramento della sicurezza di Internet, sia a livello nazionale che europeo. Secondo l'opinione comune, la Commissione deve agire per facilitare e sostenere la collaborazione europea e mondiale ed è in un'ottima posizione per raggiungere una "massa critica" veramente europea. Sarebbe utile un decentramento tramite reti di partecipanti nazionali per soddisfare le necessità locali in questo ambito paneuropeo.
Occorre lavorare ancora per sensibilizzare il pubblico ad un uso più sicuro di Internet, in particolar modo per le applicazioni personalizzate, interattive e portatili.
Nella fattispecie, lo scopo di eSafe è quello di:

- stimolare lo scambio di informazioni e il

eSafe: two more years of Safer Internet support

by Richard Swetenham, Safer Internet Action Plan, European Commission

Illegal and harmful content on the Internet in whatever shape or form continues to be a concern for lawmakers, industry and parents.
For the unwary, such as children or parents who only hear of the benefits, navigating the Web is uncharted territory. In addition new technologies are breeding new threats while even existing threats are just becoming fully recognised.
The European Union has been at the forefront in the fight against illegal and harmful content since 1996. One of its major weapons has been the Safer Internet Action Plan (IAP) spanning a four-year period from 1999-2002.
The Plan is a European Union initiative to help tackle the controversial issue of illegal and harmful content including child pornography, hate/racist content and sites encouraging terrorism.
The approach taken centres on user empowerment through information and the provision of tools.
The three main strands of the Plan have been to create a safer environment through a European network of hotlines and encouraging self-regulation and codes of conduct; to develop filtering and rating systems; and to encourage awareness actions.

Introducing eSafe

The European Commission proposes extending the current Action Plan for another two years under the name of eSafe. In preparing the follow-up programme, the Commission consulted the relevant actors.
The support was overwhelming for co-ordination within the safer Internet field, both nationally and across Europe.
It was felt that the Commission should act as a facilitator for and contributor to European and global co-operation and is well placed to reach a truly European "critical mass".
Decentralisation using networks of national players would help meet local needs within this pan-European framework.
Additional work on raising awareness of safer Internet use is still needed, particularly for personalised, interactive and mobile applications.
Specifically eSafe intends to:

- encourage information exchange and co-ordination

coordinamento con gli attori a livello nazionale, con particolare riferimento ai paesi candidati;

- riunire tutti gli attori dell'auto-normazione in un forum costruito sul modello dell'ottimo forum sul cybercrime;
- affrontare vari tipi di contenuti o comportamenti illegali, compresi i materiali razzisti e violenti;
- cercare metodi per proteggere i bambini dai contatti dei pedofili on line.

Il programma operativo di eSafe sarà adottato ed implementato una volta ricevuta l'approvazione del Parlamento europeo e del Consiglio dell'Unione europea sui due anni di proroga. Per saperne di più sugli sviluppi di eSafe, visitare il sito ufficiale della Commissione:
http://europa.eu.int/information_society/programmes/iap/index_en.htm o abbonarsi alla newsletter Safer Internet all'indirizzo:
http://www.saferinternet.org.

with actors at national level with special reference to candidate countries;

- bring together all self regulation actors in a forum modelled on the successful cybercrime forum;
- cover different types of illegal content or conduct, including racist and violent material;
- seek ways to protect children from being contacted by paedophiles online.

The work programme of eSafe will set out the details for implementation and will be adopted once the European Parliament and the Council have given their agreement t the two years' extension.
To find out how eSafe takes shape, visit either the official Commission site at:
http://europa.eu.int/information_society/programmes/iap/index_en.htm or subscribe to the Safer Internet newsletter at
http://www.saferinternet.org.

NEWSFLASH

Sempre più formazione mirata nei corsi della Registration Authority

Con un totale di circa cinquecento partecipanti ed un loro giudizio più che positivo su relatori e contenuti (elaborando i questionari distribuiti durante i corsi emerge che il 72% degli intervenuti è rimasto più che positivamente soddisfatto per i corsi Base, DNS e su Aspetti Legali e Giuridici; il dato sale al 91% per i corsi sul sistema operativo Linux), i corsi della Registration Authority chiuderanno il 2002 (prima della fine dell'anno sono ancora in programma un corso PKI, seguito dal corso Linux a Venezia, un corso PKI a Napoli ed un altro corso PKI seguito dal corso standard a Milano) dimostrando ancora una volta di essere una vera e propria pietra miliare delle attività condotte dalla RA.

Con riferimento ai corsi sulla PKI, la PKI-RA sta progressivamente distribuendo i certificati agli oltre 2400 provider/maintainer che hanno sottoscritto un contratto per la registrazione ed il mantenimento dei nomi a dominio sotto il ccTLD ".it": la tecnologia dei certificati digitali, ormai consolidata, consente di garantire riservatezza, integrità e autenticità delle informazioni che vengono scambiate sulla rete.
La RA sta utilizzando questa tecnologia all'interno del progetto "Posta certificata per la RA", che è rivolto agli ISP.
Abbiamo installato e gestiamo la Certification Authority della Public Key Infrastructure della RA (PKI-RA) dal 2000.
I certificati rilasciati durante gli appositi seminari sono conformi alla direttiva quadro europea 1999/93/CE.

NEWSFLASH

Increasingly targeted courses in the Registration Authority's future

With a total number of approximately five hundred participants and their more than positive opinion on the lecturers and contents (the questionnaires handed out at the courses showed that 72% of the participants felt absolutely satisfied with the Basic, DNS and Legal/Juridical courses, a figure which rises to 91% for the Linux courses), the Registration Authority's courses will close the year 2002 (one PKI course followed by a Linux course in Venice, one PKI course in Naples and one in Milan followed by a standard three-day course will be held before the end of the year) by proving once again they are a real milestone in RA's activities.
With reference to PKI courses, the PKI-RA is progressively delivering digital certificates to all the providers/maintainers that have entered into contract to register and maintain domain names under ccTLD ".it" (more than 2400): digital certificates represent a well known technology that can ensure the confidentiality, integrity and authenticity the information exchanged over the net.
The RA is exploiting this technology within the "Certified e-mail project", which is addressed to the ISPs.
We have installed and are managing the Certification Authority of the Public Key Infratructure of the Italian RA (PKI-RA) since 2000.
The issued certificates are in compliance with the European framework directive 1999/93/CE.

Il programma dei corsi 2003 sarà on-line all'interno del sito Web della RA riservato ai provider-maintainer a fine gennaio 2003.
Il grande successo dei corsi su Aspetti Legali e Giuridici e sul sistema operativo Linux (per il primo corso Linux tenutosi a Torino a novembre 2001 i 30 posti disponibili si sono esauriti in 45 minuti), così come per i corsi sulla PKI, ci spinge a confrontarci per il 2003 con nuove ipotesi di formazione che alcuni di Voi hanno suggerito, sempre attraverso i questionari di valutazione, con la ferma convinzione che i corsi continueranno a rappresentare un momento di reciproco arricchimento di cui tutti dobbiamo far tesoro.

The 2003 course schedule will be online in the RA's web site reserved for providers-maintainers by late January 2003.
The success obtained by the Legal/Juridical and Linux courses (the 30 places available at the first Linux course held in Turin in November 2000 sold out in 45 minutes), as well as for the PKI courses, encourages us to set ourselves new challenges for 2003, by developing new training courses that some of you have suggested in the questionnaires, convinced as we are that these courses will continue to be a time of mutual enrichment we all have to treasure.

Prevenire l'utilizzo abusivo dei futuri nomi a dominio sotto il country code ".eu"

Chi sarà l'organismo che gestirà i nomi a dominio sotto il ccTLD ".eu"? Nel frattempo, la Commissione europea ha invitato l'opinione pubblica a esprimere il proprio parere sulle misure da intraprendere per contrastare la registrazione abusiva o speculativa dei nomi di dominio nel futuro dominio di primo livello ".eu".
In occasione del lancio, il 30 luglio 2002, della consultazione online, i rappresentanti della Commissione hanno distinto due diversi tipi di controversie sui domini,.Da un lato, vi sono situazioni in cui due parti intendono, in buona fede, utilizzare lo stesso nome per promuovere se stessi o le proprie attività su Internet.
Dall'altro, tuttavia, vi sono i cosiddetti "cybersquatter", ovvero individui che, pur non avendo alcun legame con un nome, né tanto meno un interesse legittimo, registrano nomi a dominio in malafede, nella speranza di ricavare cospicui profitti rivendendoli a prezzi esorbitanti a privati, imprese o organizzazioni che hanno un legame con il nome in questione.Il Commissario per le Imprese e la Società dell'informazione, Erkki Liikanen, ha ammonito che "il fenomeno del "cybersquatting" potrebbe pregiudicare gli sforzi volti a fare del dominio ".eu" uno degli elementi di slancio per l'utilizzo di Internet e del commercio elettronico in Europa".
Gli ha fatto eco il Commissario per il Mercato interno Frits Bolkestein, il quale ha tuttavia aggiunto che la Commissione non "ostacolerà gli utenti legittimi di Internet.
Per inviare le proprie osservazioni sul "cybersquatting" (entro il 31 ottobre 2002), consultare il questionario online all'indirizzo Web: http://europa.eu.int/yourvoice/cybersquatting_it.htm

Preventing the abusive use of future domain names under the country code ".eu"

Who will be the agency in charge of managing domain names under the ccTLD ".eu"? In the meantime, the European Commission has invited the public to express their opinions on the measures that should be taken to fight abusive or speculative domain name registrations in the future first-level ".eu" domain.
On the occasion of the launch of the online poll, on July 30th 2002, the members of the Commission distinguished two types of domain litigation.
One is the situation in which two parties intend to use one name in good faith to promote themselves or their activities on the Internet.
The other concerns "cyber-squatters", i.e. people who, although having no relations to, even less any legitimate interest, in a name, register domain names in bad faith, hoping to reap substantial profit by reselling them at extortionate prices to people, companies or organisations that have some relation with that name.
Erkki Liikanen, Commissioner for the Enterprise and Information Society sectors, warned that "the so-called "cybersquatting" could endanger the efforts made to turn the ".eu" domain into one of the propellers for the use of the Internet and e-commerce in Europe".
Frits Bolkestein, member of the Domestic Trade Committee, agreed with him, adding also that the Committee will not "get in the way of legitimate Internet users".
To send comments on "cybersquatting" (by October 31st, 2002), fill in the online questionnaire at:
http://europa.eu.int/yourvoice/cybersquatting_it.htm

I personaggi CELEBRI e la registrazione ABUSIVA di nomi a dominio: le nuove "guerre stellari"

di Avv. Luca Barbero

La procedura arbitrale ai sensi della Uniform Domain-Name Dispute-Resolution Policy dell'ICANN (UDRP), come descritta dettagliatamente nell'articolo pubblicato ne "R.A. News n.1", consente la riassegnazione di un nome a dominio contestato a chiunque sia in grado di provare che 1) un nome a dominio sia identico o confondibile con un marchio registrato dal ricorrente; 2) l'attuale titolare del nome a dominio non abbia alcun diritto né legittimo interesse sul nome a dominio; 3) il nome a dominio sia stato registrato e venga utilizzato in malafede.

La prima ed essenziale condizione per poter ricorrere a questa procedura arbitrale è pertanto la titolarità di diritti di marchio e, ovviamente a condizione che anche gli altri due requisiti sussistano, tale procedura si è rivelata, per i titolari di marchi, relativamente semplice, rapida ed efficace.

I cybersquatters, tuttavia, non sono attratti unicamente da nomi a dominio corrispondenti a marchi di terzi, ma hanno anche registrato numerosi nomi di personaggi celebri. A titolo di esempio, sono stati oggetto della procedura arbitrale sopra citata, tra altri, i seguenti nomi a dominio: jimihendrix.com, jethrotull.com, mickjagger.com, celinedion.com, backstreeboys.com, giancarlofisichella.com, valeriamazza.com, mikahakkinen.net, francescototti.com, peterframpton.com, robbiewilliams.info, tutti riassegnati ai sensi di procedure arbitrali UDRP al legittimo proprietario in quanto titolare di marchio anteriore.

Ma cosa succede se il nome di un cantante famoso o di un noto attore non sono stati registrati a titolo di marchio? Uno dei primi casi di questo tipo è stata la controversia sul nome a dominio "juliaroberts.com" nel quale la ricorrente era la famosa attrice contro Russell

Celebrities and ABUSIVE registration of domain names: the new "STAR WARS"

by Att. Luca Barbero

The arbitration procedure according to the ICANN'S Uniform Domain-Name Dispute-Resolution Policy (UDRP), as detailed in the article published in R.A. News n.1, allows the transfers of a contested domain name to anyone who successfully proves that it is 1) confusingly similar or identical to the complainant's own trademark; 2) that the current domain holder has no right to or legitimate interest in the domain name; and 3) that the name was registered and is being used in "bad faith."

The first and essential condition to adopt the above arbitration procedure is therefore to have rights in a trademark and for trademark owners, provided that also the other two conditions are met, the procedure has proven to be relatively straightforward, quick and effective.

Nevertheless, Cybersquatters are not only attracted by domain names identical to third parties trademarks but also the have been largely registering the names of celebrities. As an example were object of an UDRP arbitration procedure, inter alia, the following domain names jimihendrix.com, jethrotull.com, mickjagger.com,celinedion.com, backstreeboys.com, giancarlofisichella.com, valeriamazza.com, mikahakkinen.net, francescototti.com, peterframpton.com, robbiewilliams.info, all of them were transferred back to the legitimate owner in light of their prior trademark registrations.

But what happens if the name of the name of a famous singers and/or renown actors were not registered as a trademark? One of the first cases of this kind was a matter involving "juliaroberts.com." where the complainant was the famous actress against Russell Boyd.

Boyd created a web site filled with cartoons, poems and message boards, all making fun of the star. It is relevant to point out that the domain owner at the time was also the registered owner of over fifty other domains using the names of celebrities and that he had put the domain name "juliaroberts.com", up for auction on eBay web site

The real issue in the present and in the other similar cases is to ascertain whether the actress had sufficient rights in her name to successfully opt for the UDRP procedure. Ms. Roberts did not have a registered trademark but alleged instead that she had "common law trademark rights" because her name had acquired

Boyd. Boyd aveva attivato un sito contenente caricature, poesie e una bacheca di messaggi che dileggiavano l'attrice. E' importante sottolineare che, a quel tempo, il titolare del dominio aveva registrato anche più di cinquanta altri nomi a dominio corrispondenti a nomi di personaggi celebri e che lo stesso nome a dominio "juliaroberts.com" era stato messo all'asta sul sito eBay.

La questione principale in questo e negli altri casi simili è accertare quindi se l'attrice potesse vantare diritti sul proprio nome sufficienti per poter adire alla procedura UDRP. La Signorina Roberts non aveva un marchio registrato, ma rivendicava diritti di marchio cosiddetto "di fatto" in virtù del "secondary meaning" acquisito dal proprio nome. Un marchio di fatto che abbia acquisito "secondary meaning" significa, in breve, che – benché un nome (sia di persona, come nel caso di specie, o di prodotto o servizio) non sia stato registrato a titolo di marchio – il pubblico associ immediatamente quel nome ad una particolare persona o società come conseguenza di un uso particolarmente consolidato nel commercio. Questo concetto si applica comunemente alle situazioni in cui il marchio o il titolo equivalente sia stato utilizzato per un certo periodo di tempo ed venga stato utilizzato in modo tale da "condizionare" la memoria del pubblico.

Gli arbitri concordarono che nella memoria del pubblico era avvenuta l'identificazione tra il nome e la persona dell'attrice e conclusero pertanto che quest'ultima possedeva "diritti di marchio", benché non avesse alcun marchio registrato.

Gli altri aspetti del caso in esame erano analoghi a tutte le procedure ai sensi della UDRP (assenza di legittimo interesse e malafede). Il collegio arbitrale aveva infatti dichiarato che il nome era stato registrato in mala fede unicamente allo scopo di rivenderlo all'attrice o a terzi e che il resistente aveva attuato con la propria condotta un "pattern" registrando molti altri nomi dello stesso genere. Il collegio decideva quindi che il nome a dominio venisse riassegnato a Julia Roberts.

Anche Helen Folsade Adu, la famosa cantante nota con il nome d'arte Sade, aveva intentato un'azione ai sensi dell' UDRP contro una società produttrice di software della Louisiana che aveva registrato il nome a dominio sade.com. Il nome a dominio appariva come "disponibile" su una pagina del sito della resistente nella quale venivano "casualmente" offerti in vendita numerosi altri nomi corrispondenti a noti gruppi o cantanti. La resistente rispose che c'erano molti usi e significati possibili per la parola SADE e che molti navigatori ne sarebbero stati attratti con a "secondary meaning". A common law trademark which has acquired "secondary meaning" means that - although a name (whether a personal name as in this instance or a product or service name) is not a registered mark - the public has come to associate that name with a particular person or company in light of the intensive use in commerce.

This term is usually applied in situations where the mark or claimed rights have been in use for a period of time and have been used in such a way so as to create this reference in the minds of the public.

The panel members found that there was an identification in the minds of the public between the actual name and the person of the actress. Thus, they concluded, she possessed "trademark rights" even if she had no actual registered mark.

The other issues of the case are analogous to all the procedures according to the UDRP (lack of legitimate rights and bad faith). The panel found that the domain name was established in bad faith solely for the purpose of selling it to the actress or others and that the respondent had established a "pattern of conduct" by registering many other such domains. The panel therefore decided that the domain name had to be transferred to Julia Roberts.

Helen Folsade Adu the famous singer known with the stage-name of Sade, brought an action under the UDRP against a software company based in Louisiana which had registered sade.com.

The domain name was simply listed as an "available" domain name on the Respondent's sign-up page where a number of other domains corresponding to well known groups and singers were offered for sale. The Respondent submitted that there were many possible uses and meanings of the word "SADE" as well as many users could have been attracted to it in the context of the "Marquis de Sade".

However the Respondent did not provide any proof of such an use nor has given any explanation

riferimento al Marchese de Sade (!).
La resistente non fornì, tuttavia, alcuna prova di tale uso, né alcuna spiegazione ragionevole su come era avvenuta la scelta del nome a dominio sade.com. La ricorrente, d'altro canto, utilizzava il nome d'arte Sade dal 1983. L'arbitro ritenne che in quel periodo di tempo la ricorrente avesse affermato una sostanziale connessione tra quel marchio e la vendita di dischi, compact disc, video, cd-rom, biglietti per concerti, pubblicità e promozioni, abbigliamento e altro materiale in tutto il mondo.
La ricorrente, benché non avesse registrato la parola SADE a titolo di marchio in nessun Paese, utilizzava tale segno come nome d'arte e l'arbitro concluse che la ricorrente aveva dimostrato di poter vantare sufficienti diritti di marchio di fatto.
Nel caso dei nomi a dominio nicholekidman.com e nicholekidmannude.com, (nonostante l"h" in più) l'arbitro decise analogamente che la Kidman aveva dimostrato di poter vantare diritti di marchio di fatto sul proprio nome in virtù dei propri film di successo e della notorietà ottenuta e che pertanto il proprio nome in relazione a servizi di intrattenimento costituiva una inequivocabile indicazione di provenienza, riassegnando i nomi a dominio all'attrice.
Anche nella procedura UDRP sul nome a dominio venusandserenawilliams.com, le famose sorelle Williams congiuntamente sono riuscite ad ottenere la riassegnazione del nome in quanto l'arbitro ha stabilito espressamente che – ai fini della procedura in questione – il marchio del ricorrente non deve essere necessariamente registrato e che sono sufficienti diritti di marchio di fatto.
Si deve tener presente, tuttavia, che – benché i personaggi celebri abbiano spesso ottenuto ragione, anche quando non avevano marchi registrati – non è sempre stato possibile ottenere la rassegnazione dei domini.
Il cantante Bruce Springsteen iniziò una procedura arbitrale ai sensi della UDRP contro il titolare del nome a dominio brucespringsteen.com, un fan che gestiva un club attraverso il sito. Nel caso Springsteen il collegio arbitrale sostenne che non era stata fornita alcuna prova che il nome "Bruce Springsteen" avesse acquistato un "secondary meaning".
Alla luce anche le altre condizioni per la decisione, il collegio decise comunque che i diritti di marchio di fatto sul nome Bruce Springsteen potevano essere riconosciuti ai sensi della UDRP ma che, in considerazione della mancanza della dimostrazione della malafede, il nome a dominio non poteva essere riassegnato al Signor Springsteen (anche se, a nostro avviso, l'interpretazione più corretta del

whatsoever as to how it came to choose the domain name "sade.com".
The Complainant on the other hand, had since 1983 used the stage-name SADE. The panel held that in that time the Complainant has established a substantial goodwill in that mark and service mark in connection with sales of records, compact discs, videos, CD-ROMs, tickets for live performances, advertising and promotion, clothing and other merchandising in many jurisdictions throughout the world.
Although the Complainant has not registered the word " SADE " either as a trademark or as a service mark in any jurisdiction, the Complainant has adapted the word "SADE" as her stage-name the Administrative Panel is further satisfied that the Complainant has established that she has common law rights in the said mark.
In the case of the domain names nicholekidman.com and nicholekidmannude.com, the panel (regardless of the additional "h") stated that Kidman has also established common law trademark rights in her name by virtue of her successful films, she has achieved renown, and the use of her name in connection with entertainment services provides a strong indication of source, transferring the domains to the actress.
Also in the UDRP procedure on venusandserenaw illiams.com, the famous Williams sisters managed jointly to have the domain name transferred as the Panel stated that for the purposes of the UDRP relevant trade mark rights of the Complainant do not have to be registered rights and common law rights will suffice.
It has to be noted that although celebrities were often victorious even if they did not register the trademarks it was not always possible to secure the transfer of the domain names.
The singer Bruce Springsteen started an UDRP arbitration procedure against the owner of brucespringsteen.com, a fan who was running a club on the site.

The arbitration panel in the Springsteen case stated no evidence has been given of the name "Bruce Springsteen" having acquired a secondary meaning. As it was possible to possible to decide the case on other grounds, however, the Panel proceeded

caso di specie è quella espressa nella dissenting opinion in calce alla decisione della maggioranza del collegio arbitrale).

Nel caso del musicista Sting (al secolo Gordon Sumner) contro Michael Urvan, titolare del nome a dominio sting.com, gli arbitri hanno indicato che "sting" era una parola di uso comune (al contrario dei nomi di persona) che non poteva pertanto probabilmente essere rivendicata in modo esclusivo in assenza di una registrazione di marchio.

Il caso fu deciso a favore di Urvan, anch'egli conosciuto con il soprannome "Sting," ma solo in considerazione della mancata prova della malafede e lasciando formalmente aperta la questione dei marchi di fatto. Urvan ha comunque poi ceduto il nome a dominio a Sting e www.sting.com è attualmente il sito ufficiale del cantante.

Alla luce di quanto precede, si può concludere che la giurisprudenza ai sensi della UDRP ha sostanzialmente ampliato tale tutela anche ai nomi di personaggi famosi non registrati come marchio (concedendo quindi nuove "armi" per le loro "guerre stellari"), sebbene sia comunque sempre opportuno provvedere ad ottenere una adeguata protezione dei propri segni distintivi attraverso la preventiva registrazione sia come marchio che come nome a dominio.

E' inoltre opportuno condurre un'attenta attività di sorveglianza sull'uso dei propri marchi da parte di terzi, sia nel "mondo reale" che su Internet, in quanto nessuna strategia è completamente "a prova" di pirata.

Ad esempio, la società Verizon Wireless, che - oltre al marchio - aveva registrato centinaia di registrazioni "difensive" (compreso il nome a dominio verizonsucks.com) si è vista registrare da un cybersquatter verizonreallysucks.com.

A seguito della minacciosa lettera di diffida e prima che Verizon procedesse con le altre relative azioni legali, per tutta risposta, il titolare aveva registrato anche VerizonShouldSpendMoreTimeFixingItsNetworkAndLessMoneyOnLawyers.com (!).

on the assumption that the name Bruce Springsteen was protected under the policy but in view of the lack of bad faith, the domain name was not transferred to Mr Springsteen (even though we are convinced that the opinion expressed in the dissenting opinion is preferable).

In the case of the recording artist Sting (real name: Gordon Sumner) against Michael Urvan, owner of sting.com, the arbitrators indicated that "sting" was a common word (as opposed to personal names) which could not be successfully claimed without a trademark registration.

The case was decided for Urvan who also just happens to go by the nickname "Sting," but only on the issues of lack of bad faith leaving therefore again the matter of the common law rights somewhat open.

Urvan has since agreed to transfer the name to Sting and Sting.com is now the singer's official site.

In light of the above, we may conclude that the decisions according to the UDRP have extended the protection of such a procedure also to the names of the celebrities not registered as trademark (allowing new "weapons" for their "star wars"). But it is also anyway preferable to secure adequate prior protection of its distinctive signs both via trademark and domain name registrations.

Furthermore, it is advisable an attentive monitoring activity of third party uses of trademarks both in the "real world" and on Internet since no strategy is fully pirate safe.

For instance, Verizon Wireless which have registered – beside the trademark - hundreds of defensive registrations, including verizonsucks.com had verizonreallysucks.com registered by a cybersquatter. Verizon then sent a nasty letter to said registrant but, even before Verizon was starting the other legal actions, as only reply, the cybersquatter registered also VerizonShouldSpendMoreTimeFixingItsNetworkAndLessMoneyOnLawyers.com (!).

R.A. News N°2
settembre 2002

Redazione/Central office:
Registration Authority Italiana
Istituto di Informatica e Telematica - CNR
Via G. Moruzzi, 1
I-56124 Pisa
Tel.+39-050-3139811
Fax +39-050-3152713
e-mail: newsletter@nic.it

Direttore responsabile/Director in charge:
Prof. Franco Denoth

Responsabile di redazione/Editing:
Giovanni Seppia

Collaboratori in redazione:
Stefania Fabbri, Daniela Medda, Ilaria Mazzoni, Sonia Sbrana

Progetto grafico e impaginazione/Graphics and paging:
Francesco Gianetti

Stampa/Printed by:
Tipografia Graphicarts Snc

Si ringrazia per la preziosa collaborazione a questo numero/Special thanks for the publication of this issue: Ms. Theresa Swinehart, Safer Internet Action Plan Unit of the European Commission, Council of Europe Press Office

Autorizzazione n.297/2002 rilasciata dal Tribunale di Pisa

Stampato su carta ecologica/Printed on ecologic paper

Registration Authority Italiana