Contestazioni in materia di phishing nelle procedure di riassegnazione UDRP

Il contrasto ai crescenti fenomeni di cybercrime

#GLPoint

Davide L. PETRAZ
Co-Managing Partner

Tommaso LA SCALA
Trademark Attorney

Il *Domain Name System* (DNS) e l'UDRP si trovano a fronteggiare oggi un contesto digitale ben diverso da quello esistente alla fine degli anni '90 (quando la Policy è entrata in vigore).

Ora che ogni genere di interazione e transazione commerciale è passata dalla "carta" al mondo digitale – e dopo che gli strumenti software di progettazione, *editing* e *layout* sono diventati disponibili al grande pubblico e *mainstream* – la criminalità informatica è cresciuta enormemente, causando danni considerevoli ai titolari di diritti di privativa. Frodi finanziarie, furti di identità e di informazioni commerciali sono solo alcuni degli esempi di condotte indebite che influenzano in modo sostanziale i procedimenti UDRP.

È noto che il *phishing* è un tipo di truffa effettuata su Internet, attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente e/o una società affidabile tramite una comunicazione digitale.

Negli ultimi anni, le tecniche di *phishing* si sono rapidamente evolute dalla classica e pedissequa "riproduzione" di siti web aziendali ufficiali, email, fatture ecc. verso modalità molto più raffinate, tra le quali lo *"spear phishing"*, meritevole di un'attenzione particolare.

Lo *"spear phishing"* è un attacco informatico mirato che prevede contenuti-esca altamente personalizzati. Il malintenzionato svolge in genere un approfondito lavoro di ricognizione, sondando *social media* ed altre fonti di informazione dell'obiettivo che intende colpire. Questa pratica consiste nell'ingannare un utente di Internet che si collega inavvertitamente a siti internet falsi (credendo di trovarsi in aree web ufficiali) divulgando così le proprie informazioni personali. Tale condotta può anche indurre gli utenti ad aprire documenti salvati online, cliccando su link che installa automaticamente un *malware* nel computer del malcapitato.

Una volta installato tale *malware*, il malintenzionato può manipolare da remoto i computer infetti. In base al *Data Breach Investigation Report (DBIR) 2021* pubblicato da Verizon, il 74% delle società negli Stati Uniti ha subìto un attacco di *phishing* concluso con successo. Di questo ammontare, il 96% è stato sferrato tramite e-mail. I settori finanziari, dell'e-commerce e della vendita al dettaglio sono per ovvie ragioni gli ambiti imprenditoriali più colpiti.

Considerato che, nella maggior parte dei casi, è un messaggio e-mail ad essere il vettore principale di questi attacchi di *phishing*, è confortante sapere che l'UDRP è perlomeno un'arma utile a combattere le frodi online. Invero, gli indirizzi e-mail rientrano nell'ambito di applicazione della *Policy*, in quanto trattasi di caselle di posta create a partire da un nome a dominio ed il paragrafo 4(b)(iv) dell'UDRP include proprio la generica definizione di *"other on-line location"* come destinazione alternativa del dirottamento di un utente internet. Il medesimo paragrafo copre anche l'ipotesi di un nome di dominio simile a quello del marchio registrato per stabilire una falsa affiliazione tra il titolare del marchio e il mittente dell'e-mail alla base del *phishing*. L'ambito non esaustivo del paragrafo 4(b) comprende chiaramente l'uso di domini di posta elettronica ingannevoli per perpetrare (o tentare di perpetrare) una frode. A questo proposito, la detenzione passiva di un nome di dominio (cioè registrato ma non utilizzato in relazione a un sito web attivo) non cambia la sostanza, giacché i criteri e i fattori utilizzati dagli arbitri per determinare la mancanza di interesse legittimo sono ancora quelli indicati nella *WIPO Overview 3.0(3)*, ovvero (i) il grado di distintività o di notorietà del marchio del ricorrente, (ii) la mancata presentazione di una risposta da parte del resistente o l'assenza di prove che attestino un uso effettivamente in buona fede, (iii) l'occultamento dell'identità del resistente o l'uso di credenziali false (in palese violazione del contratto di registrazione con il Registrar) e (iv) il fatto che risulti non plausibile un qualsiasi uso in buona fede del nome a dominio registrato ed oggetto di contestazione.

Il *case-law* sviluppato dagli arbitri della WIPO sembra confermare che i casi in cui il registrante del nome di dominio ha utilizzato un dominio di posta elettronica ingannevole per perpetrare una frode (ad esempio, la fatturazione fittizia di un fornitore) sono decisamente semplici da dirimere: a ben vedere, le sfumature e le differenze tra i tipi di possibili frodi non influiscono generalmente sull'esito della decisione.

Tenuto conto di quanto sopra, sebbene i singoli procedimenti UDRP non avranno un impatto significativo sul volume delle attività illegali di registrazione di nomi a dominio, non c'è dubbio che gli stessi rappresentino uno strumento rapido ed economico per i titolari di marchi al fine di bloccare la condotta dannosa posta in essere online dai truffatori.

Via L. Manara 13
20122 MILANO
Tel: +39 02 54120878
Email: glp.mi@glp.eu

Viale Europa Unita 171
33100 UDINE
Tel: +39 0432 506388
Email: glp@glp.eu

Via di Corticella 181/4
40128 BOLOGNA
Tel: +39 051 328365
Email: glp.bo@glp.eu

glp.eu

Other offices:
PERUGIA · ZÜRICH
SAN MARINO