Phishing claims in UDRP domain name disputes

Responding to the wave of cybercrime

#GLPoint

Davide L. PETRAZ
Co-Managing Partner

Tommaso LA SCALA
Trademark Attorney

The DNS and UDRP are currently confronting a digital environment that did not exist in the late 90's.

Once commercial interaction and transaction have transitioned from paper to the digital world – and after software design tools became available and mainstream for the large public – cybercrime hugely growth, thus causing considerable damages to IP owners. Financial frauds, theft of identities and valuable commercial information are only a few samples of the exploitative behavior that now affect UDRP proceedings substantially.

It is well-known that phishing is a type of social engineering attack used to steal user data, including login credentials and credit card numbers.

In the past years, phishing techniques quickly evolved from the classic "mimic" of official corporate websites/emails/invoices etc. to much more refined methods, among which *"spear phishing"* deserves a separate dissertation.

Spear phishing is a targeted phishing attack that involves highly customized lure content. Attacker will typically do reconnaissance work by surveying social media and other information sources about their intended target. Such practice may involve tricking an internet user into logging into fake sites and divulging credentials. It may also lure users into opening documents by clicking on links that automatically install malware. With this malware in place, attackers can remotely manipulate the infected computers.

According to *Verizon's 2021 Data Breach Investigation Report* (DBIR), 74% of organizations in the United States experienced a successful phishing attack. Of them, 96% were delivered by email. Financial, e-commerce and retail industries are the more targeted in this regard.

Provided that – in most cases – an email is the primary vector of these phishing attacks, it is at least comforting to know that UDRP is a useful weapon to fight back online frauds. As a matter of fact, email addresses are within the scope of UDRP, since they are "domain names" and, *inter alia*, paragraph 4(b)(iv) on the Policy includes *"other on-line location"* as a destination of diversion.

The very same paragraph also covers use of confusingly similar domain name to establish false affiliation between trademark owner and email sender located at online location. Non-exhaustive scope of 4(b) clearly encompasses use of deceptive email domains to perpetrate (or attempt to perpetrate) fraud. In this regard, passive holding of a domain name (meaning registered but not actively used in relation with an active website) does not change the equation, as the criteria and factors used by panelists in order to determine lack of legitimate interest still are the ones indicated in WIPO Overview 3.0(3), namely (i) the degree of distinctiveness or reputation of the complainant's mark, (ii) the failure of the respondent to submit a response or to provide any evidence of actual or contemplated good-faith use, (iii) the respondent's concealing its identity or use of false contact details (noted to be in breach of its registration agreement), and (iv) the implausibility of any good faith use to which the domain name may be put.

The case-law built by WIPO panelist seems to confirm that cases in which domain name registrant has used deceptive email domain to perpetrate fraud (e.g. fictious vendor invoicing) are typically "straightforward": indeed, differences in types of fraud do not generally affect the decision outcome.

Taking into account all the above, although single UDRP proceedings are not going to significantly impact on volume of unlawful registration activity, there is no doubt they represent a quick and cost-efficient tool for brand owners in order to shut down the incredibly damaging conduct carried out online by fraudsters.

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