NEXSEN | PRUET

Using the UDRP to Combat Unauthorized Access to Computer Systems and Online Fraud

Related Professionals

Seth L. Hudson
704.338.5307
SHudson@nexsenpruet.com

Practices

Intellectual Property Law

Intellectual Property Litigation

Article
05.14.2021

Scams involving domain names, resulting in unauthorized access to a company's computer network and online fraud, have increased during the pandemic. These scams involve an entity registering a domain name identical or confusingly similar to a domain name of a legitimate company to defraud an unsuspecting individual or company of their money or data or gain unauthorized access to the company's computer systems. Registering a visually similar domain name to a legitimate domain name that contains one or more typographical errors is referred to as typosquatting. Variations of typosquatting include registering a domain name that omits a character, adds a character, transposes characters, or substitutes characters in a legitimate domain name to deceive.

Many times, the legitimate company's website is cloned. The HTML from a legitimate website is scrapped and replicated on the fraudulent domain, making the scam challenging to ascertain by the unsuspecting victim. These cloned websites have a home page with a login feature, similar to the login feature of the legitimate website, inviting an unsuspecting individual to input login credentials, such as a username and password, inadvertently exposing this information. The login credentials are used to access the company's computer system for nefarious purposes.

Emails incorporating the fraudulent domain name ("email domain") and purportedly sent from an actual person at the company are increasingly used in various scams to gain unauthorized computer system access or other fraudulent purposes. In these instances, the unsuspecting recipient does not recognize the variation in the email domain. These emails direct the recipient to access a provided link for a cloned website to enter data, such as login credentials, account numbers, or even make a payment on an account. In a fairly common example, an employee of a legitimate company or one of the company's clients or customers receives an email, or even a phone call, directing the individual to use a new website tied to the fraudulent domain to access the company's computer systems or make future payments, allowing the perpetrators to gain access to login

credentials or obtain a payment intended for the legitimate company. These scams are becoming increasingly complex, and employees should be vigilant in their daily activities, including email usage.

An effective avenue available to any company that learns a domain name is registered that is identical or confusingly similar to one of its trademarks is to file a complaint under the Uniform Domain Name Dispute Resolution Policy ("UDRP complaint"). In a UDRP complaint, the legitimate company, referred to as a Complainant, must prove:

1. The domain name is identical or confusingly similar to a trademark in which the Complainant has rights;
2. The opposing party has no rights or legitimate interests in respect of the domain name; and
3. The domain name has been registered and is being used in bad faith.

The UDRP complaint should be carefully drafted to comply with ICANN requirements and include evidentiary support to back up the assertions. A UDRP complaint is decided solely on its merits without the ability to provide further testimony, additional evidence, or a hearing. Failure to comply with ICANN requirements or provide the requisite proof may result in an adverse ruling, even if the respondent fails to reply. The more evidence provided in the complaint, the greater chance of success. Therefore, it is extremely important to front-load your UDRP complaint with the requisite evidence based upon the facts of the case. A successful UDRP complaint results in the transfer of the domain name to the Complainant.

Once a company learns a fraudulent domain name is registered, it is crucial to immediately begin accumulating evidence and contact a knowledgeable attorney. As websites can be removed within seconds, it is vitally important to begin gathering as much evidence as possible immediately upon learning of the fraudulent domain name. This evidence will likely consist of:

1. Screenshots of all webpages associated with the fraudulent domain:
2. Screenshots of webpages with pay-per-click links to various third-party websites, as this is further evidence of bad faith;
3. Emails received from the fraudulent domain, including emails a third-party, such as a customer, client, or service provider, may have received; and
4. A log of any phone calls received directing an individual to a website associated with the fraudulent domain, if possible. Pertinent information to include in the log would be the date, the person receiving the call, the purported name of the individual making the call, the telephone number of the caller, and a detailed description of the contents of the call.

Since time is essential, it is important to expeditiously gather evidence while simultaneously consulting a knowledgeable attorney to file a UDRP complaint to obtain ownership of the domain name.

If you have any questions about the UDRP or other intellectual property issues, please contact the Nexsen Pruet Intellectual Property team.