IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

TYPOSQUATTING – A NEW MENACE TO SOCIETY

Ms. Palak Sharma
Research Scholar, Banasthali University
District-Tonk, Rajasthan, 304022 India

ABSTRACT

People are generally well aware of how cybercrime is carried out and the hefty profits made by the attackers, but the harms incurred by victims are less well known. We're even less aware of trifling cybercrimes like typosquatting. This study presents a comprehensive analysis of the losses incurred by internet users who have received less attention from both the government and the general public around the world. While there are provisions related to the remedies provided to domain name owners but unfortunately persons who have been affected by typo squatting in general goes unanswered. Ignorance about this is very widespread among the general populace, who become easy targets for such menace and, due to the veniality of the crimes; state does not give it much thought. While the effectiveness of cyber attackers continues to rise at a constant pace, Legislations are constantly falling behind, particularly in India.

Keywords: *Typosquatting, Cybersquatting, Cyberspace, Intellectual Property Rights, Cyber Crime, Cyber Laws*

INTRODUCTION

Today, the internet is becoming one of the most significant components of an individual's existence. It caters to almost all elements of life, including communication, data processing, machine control, typing, editing, selling, and purchasing. The expansion of cyberspace has spawned a new kind of criminal activity, the reasons and repercussions of which are still enigmatic and unknown. It's no secret that, after years of work, legislators, jurists, and organisations are still looking for answers to the complicated legal concerns produced by the World Wide Web, a technical arena that allows billions of people to connect pretty much instantly. [1]

It is necessary that we comprehend the technical aspects of the issues discussed in this paper. Each website on the internet has an IP address associated with it. A domain name system is required by each web server to translate the domain name to an IP address, which is a string of digits. [2] A website's domain name is unique. It's a unique identifier for that website. Creating websites with unique domain names has become a standard practice in recent years, allowing businesses to be easily identifiable by their trademarks. A single firm can have a big number of customers, yet neither the company nor the customers can physically connect with each other. Domain names give the company with a foundation from which they may easily communicate with their customers, both of whom are inhabitants of cyberspace.

Pay-per-click (PPC) advertising on a website is how domain name owners generate money. Money is made for the domain owner every time a user clicks on the advertising that appears on the website.

The original domain name, symbolics.com, was registered in March 1985, about 31 years ago. Domain name registration grew as the World Wide Web became more contemporary. There are millions of domain names that are being used today. Domain names allow companies to communicate with their customers. However, unlike trademarks, domain names are often registered on a first-come, first-served basis. This technique has allowed tech-savvy criminals to benefit from others' marks and goodwill through "cybersquatting," or the "registration as domain names of well-known trademarks by non-trademark holders who then attempt to sell the domains back to the trademark owners." [3]

TYPOSQUATTING

Typosquatting is a form of cybersquatting. While several legislations and judgements have offered definitions for cybersquatting, typosquatting has yet to be given a legal term. Nonetheless, several authors have attempted to define typosquatting in the following way:

Typosquatting is the practice of registering internet domain names that seem to be similar to those of well-known websites in the hopes that a user types the website's name incorrectly would land on the typo domain rather than the intended destination. [4]

Typosquatters are aware that the user intended to visit another site, and instead of visiting theirs, which is a misspelled version of the intended site, they bombard the user with advertisements and, sometimes in malware cases. Typosquatting hasn't been demonstrated to be very dangerous in terms of malware infection, as the number of typo sites visited is still lower than the number of valid sites. [5] Despite the fact that the damage produced by typosquatting is minor, it pushes users to spend in defensive registration.

Despite the fact that typosquatting is not a serious cybercrime, some characteristics may be identified:

- It can even be seen at the network level;
- Typosquatting sites exist only to target unwary customers of a similarly spelt site; they rely on the fact that internet users will make typographical errors when typing domain names into their browsers. The following are some examples of typosquatting:
- The domain name wwwflipkart.com is missing the "dot";
- *flpkart.com* is a typical misspelling of the intended website.
- *flipkarts.com* is a domain name that is worded differently.
- *flikart.org* is a separate top-level domain. [6]

EFFECT OF TYPOSQUATTING

The confusion generated by misspellings of website names not only results in a loss of prospective visits for website owners, but it also annoys customers, who lose not only money, but also efforts and time. Each time a customer visits a typo site, it represents the amount of time, money, and effort he has wasted. While these are the obvious damages that typosquatting causes consumers, he also suffers other losses, which are outlined below:

The most prevalent and well-known loss sustained by any citizen of cyberspace as a result of any sort of cybercrime is monetary loss. Cybercrime is on the rise, and the major goal of all types of cybercriminals is to make money, whether it's through credit card theft or by people accidentally clicking on adverts on websites. In the event of typosquatting, when internet users mistakenly access lexically identical sites that are infected with malware and adware, financial loss is rather prevalent.

Loss of effort: while we are all aware of users' financial losses, the annoyance of visitors' time and effort as a result of stumbling across such typosquatted sites is rarely discussed. Adware and spyware are frequently found on typosquatted sites. A user's credit card may be lost, however this is only a temporary setback. As a result, the user will need to get a new card and block the old one, as well as update his security and fix any holes in the system that the virus may have introduced.

Loss of time: Cybercrime's negative externality has hardly been dealt with. Time lost by visitors and time lost by site operators are still unaccounted for. Time that a user must spend after being harmed by malware installed on a typosquatting site. Renewal of the card, as well as cleanup of the system follows the attack. Even if the virus does not do any damage to the system, the customer must ultimately update their protection to avoid future problems caused by uncontrolled malware.

Apart from direct harm to consumers, indirect harms that have seldom been considered should also be taken into account. It cannot be argued that cybercrime such as typosquatting has a psychological impact on consumers. According to the most recent statistical research and publications, there is a possibility of a decrease in online transactions and other internet services owing to a loss of trust in cyberspace security. [7]

GLOBAL REGULATORY AUTHOROTIES

U.S - The Anti-Cyber-Squatting Consumer Protection Act (ACPA) of 1999 was passed in the United States. [9] The act provides protection against cybersquatting for Individuals and proprietors of distinctive trademarked names. A victim in the United States has two options: sue under the Anti-Cybersquatting Consumer Protection Act (ACPA) or use the Internet Corporation for Assigned Names and Numbers' international arbitration system (ICANN). However, due to jurisdictional issues in the courts, the WIPO (World Intellectual Property Organization) Arbitration and Mediation Center has developed an online Internet-based mechanism for resolving commercial intellectual property disputes. It offers a remedy in 45 days. [10]

India - A cybersquatting victim in India has three alternatives (I). Victims can sue in court under the Trademark Act of 1999 for different injunctions preventing cyber squatters from exploiting domains. There are two types of reliefs possible under the Trademarks Act of 1999, as in previous cases: [8]

1. Infringement remedy

2. Passing off remedy [11]

Infringement Remedy: Only after a trade mark is registered may the owner of the mark seek infringement relief under the Trade Mark Act.

Passing off Remedy: If the owner wishes to use the passing off remedy, no registration of the trade mark is necessary.

Uniform Domain Name Dispute Resolution Policy (UDRP) - ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) is primarily used to address disputes concerning bad faith registrations. WIPO is the premier ICANN authorised domain name dispute resolution service provider under the UDRP, which was created to promote the global protection, dissemination, and use of intellectual property. India is one of the 171 countries that make up the World Intellectual Property Organization (WIPO).

CASES OF TYPOSQUATTING

Joseph Shields, a cartoonist, registered the domain name joecartoon.com in 1997 to display his work and sell Joe Cartoon merchandise. After winning the Macromedia Shock site of the day award in April 1998, the site grew in popularity, and it now receives over 700,000 monthly views. John Zuccarini registered five

misspellings of the domain name and used them to display adverts for other websites and credit card businesses. Fans of the Joe Cartoon characters who visited one of Zuccarini's sites unwittingly found themselves mousetrapped and unable to leave the maze of web pages and pop-up adverts. [12]

Advertisers paid Zuccarini between ten and twenty-five cents for each hit, which included both the first unintended visit and all pop-up advertising activated by the unintentional visitor.

Shields retaliated by sending Zuccarini cease-and-desist letters, but no answer was returned. Zuccarini quickly modified the fake web sites' content to a "political protest" page. Despite the fact that Zuccarini removed the advertisements from his website, Shields was unable to prevent confusion and direct potential viewers to the correct web page.

CONCLUSION

The ultimate purpose of this study is to analyse and categorise the losses sustained by users as a result of typosquatting. Typosquatting is a very minor cybercrime that goes virtually unreported. The purpose of this article was to demonstrate the lack of public knowledge of this crime, as well as the lack of effort on the part of state governments to address the problem. Edmund Burke once stated, that “We must all obey the law of change”. And change is constant in nature because law is a mirror of society, it must adapt to changes as they occur. As the number of people using the internet grows, so does the number of cybercriminals.

The solutions for the menace of typosquatting in 21st centuary are:

Typosquatting is a lucrative business, with some typosquatters making millions of dollars annually. In view of the enormous advertising income generated by typosquatting, existing legal damages may be inadequate. For example, Joseph Shields only received $50,000 in damages after successfully suing John Zuccarini for registering misspelling variants of the domain name joecartoon.com. $50,000 in civil damages is minimal when compared to Zuccarini's annual income of almost $1 million. [13] In summary, civil litigation fails to dissuade typosquatters and prospective typosquatters since a single court loss does not render the typosquatters bankrupt, either by deleting all violating domain names or incurring substantial monetary damages.While major organisations may be able to tolerate the expense of long-running litigation, criminal sanctions are required to deter any typosquatting.

Finally, making typosquatters pay with their freedom rather than their money helps innocent Internet users. Under the ACPA, those who have been mouse trapped in a maze of flashing advertising or who have had unsolicited pornographic pictures pouring across their computer displays have no recourse. Although the ACPA gives some relief to successful litigants, it does not provide any legal protection to the affected Internet user. Criminalizing typosquatting, on the other hand, protects Internet users by allowing public

prosecutors to prosecute typosquatters in the public interest rather than depending on private claimants who are likely motivated by profit.

Further, to prevent typosquatters from getting deceptive domain names in the first place, the domain name registration procedure should be revised to demand an independent investigation before handing the applicant a domain name. Applicants currently simply need to give a credit card number and tick a box indicating that they accept the registration terms. While upfront investigations are expected to lengthen the registration process and increase fees and administrative costs, fewer claimants will pursue ICANN arbitration because the organisation exclusively handles disputes involving bad-faith domain name registration.

REFERENCES

1. Carl C. Butzer And Jason P. Reinsch , Cybersquatting, Typosquatting, And Domaining: Ten Years Under The Anti-Cybersquatting Consumer Protection Act .
2. P. Charan, Z. H. Khan, M. A. Ansari, "A Survey of a Prominent Effects of Cybersquatting In India," International Journal of Scientific & Engineering Research, Volume 6, Issue 2, February-2015, ISSN 2229- 5518
3. Sporty's Farm L.L.C. v. Sportsman's Market, H.R. Rep. No. 106-412, at 5-7 (1999).
4. Mohammed Taha Khan, Xiang Huo, Zhou Li &Chris Kanich, Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosquatting.
5. J. Szurdi, B. Kocso, G. Cseh, M. Felegyhazi, and C. Kanich, "The Long "Taile" of Typosquatting Domain Names," in Proceedings of the 23rd USENIX Security Symposium, 2014.
6. Sanchit Mehta, Cyber Squatting And Its Legal Positions, Manupatrafast.Com (Apr. 30, 2022, 10.00AM), www.manupatrafast.com/articles/PopOpenArticle.
7. 7 Ross Anderson, Chris Barton , Rainer B¨Ohme , Richard Clayton , Michel J.G. Van Eeten , Michael Levi , Tyler Moore & Stefan Savage, Measuring The Cost Of Cybercrime .
8. Trademark Act, 1999.
9. Anti Cyber Squatting Consumer Protection Act, 1999.
10. Anti-cyber squatting Consumer Protection Act (ACPA), 1999.
11. Singh & Associates,India: Cyber Squatting Laws In India, (Apr. 30, 2022, 10.00AM), mondaq,www.mondaq.com/india/x/208840/.../CYBER+SQUATTI+NG+LAWS+IN+INDIA
12. Shields v. Zuccarini, 89 F. Supp. 2d 634 (E.D. Penn. 2000). 1999 II AD (Delhi) 229.
13. NS. Srinivasulu, Intellectual Property Law (Dynamic Interfaces), Lexis Nexis, 2017.