Abusive Domain Names by Internet Entities

Subjects: Computer Science, Information Systems

Contributor: Yanan Cheng, Zhaoxin Zhang, Tingting Chai

A large number of domains are abused every day for cybercrime. At the same time, the fight against abusive domains is not the fight of one person or organization but a battle that requires the cooperation of the entire community. A large number of domain names on the Internet are misused daily for cybercriminal activities, ranging from spoofing victims' private information (phishing), to maliciously installing software onto end-users' devices (malware attacks), to distributing illegal obscene videos. Internet abuse continues to victimize millions of people each year, reducing trust in the Internet as a place to conduct business and non-business activities. This decline in confidence has a detrimental effect on all stakeholders in the Internet ecosystem, from end-users to infrastructure service providers.

Keywords: abuse reporting ; abusive domain names ; Internet entities ; Internet ecosystem

1. Introduction

Internet abuse continues to victimize millions of people each year, reducing trust in the Internet as a place to conduct business and non-business activities [1][2]. This decline in confidence has a detrimental effect on all stakeholders in the Internet ecosystem, from end-users to infrastructure service providers.

A lot of resources are devoted to how to identify or detect these abusive domains early and accurately [3][4][5][6][7][8]. However, the issues of determining which Internet entities are responsible and what methods are used to handle discovered abusive domains are worthy of in-depth one [9]. An abusive domain name involves many Internet entities (for example, registrars and web hosting providers), from registration to the commission of cybercrime, as shown in **Figure 1**. As a result, the fight against domain name abuse is not the fight of one person or organization but a battle requiring the entire community's participation [10]. The Internet Corporation for Assigned Names and Numbers (ICANN) states that the best strategy to combat domain name abuse is to join many entities and choose the best approach, such as governments, operators, institutions, and Internet communities.

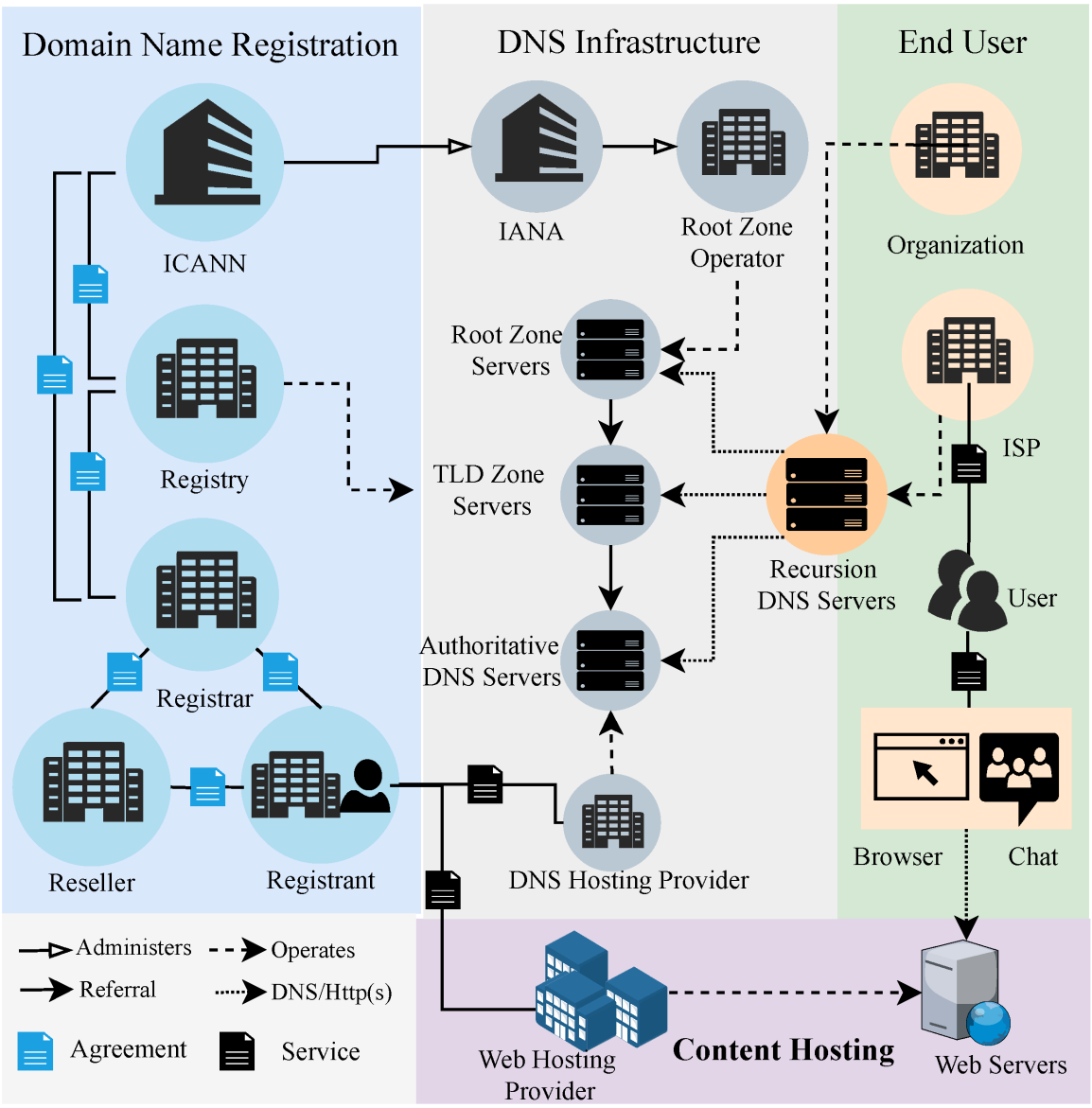

Figure 1. Conceptual diagram of the Internet ecosystem portion contractually.

In China, pornography and gambling domains are not only defined as abusive but are also against the law. At the same time, China has one-fifth of the world's Internet users. Therefore, the government, the security community, and academia need to learn more mechanisms to deal with abusive domains quickly and effectively.

2. Definition of Abusive Domain Name

The report of the ICANN Security and Stability Advisory Committee (SSAC) [10] defines five types of harmful activities as DNS abuse, namely malware, botnets, phishing, pharming, and spam, all of which are domain name related. On the other hand, SSAC considers some of the specific definitions to be limited, and the above does not provide a general definition of abuse that can accommodate the evolving nature of abuse and cybercrime across the country and over time. The definition of domain name abuse also needs to consider each country's culture and legal requirements. For example, in some countries [11][12][13][14], the use of domain names for pornography (especially child pornography) and gambling is not only abusive but also illegal.

Chinese law strictly prohibits individuals or organizations from establishing and accessing pornographic or gambling websites. At the same time, China has one-fifth of the world's Internet users. Thus, the abusive domain names surviving on the Internet affect a wide range of users. This indicates the importance of how quickly and effectively entities can deal with abusive domains, which is also the goal of this paper. Moreover, while it uses pornography and gambling domain names, the methods and response time of Internet entities to deal with different types of abusive domain names are the same.

3. Internet Entities Involved in Domain Names

The Internet is a worldwide distributed network comprised of numerous autonomous networks connected voluntarily. It is governed by a decentralized and international multistakeholder network of interconnected autonomous groups comprised of civil society, business, government, academia, research, and national and international organizations. They work together across their different jobs to develop policies and standards that keep the Internet working worldwide for the public good. As a result, this architecture leads to many infrastructures and entities involved in the Internet for end-users to access the services (e.g., websites and email) provided by domain names, as illustrated in **Figure 1**.

Abusive domain names to victimize or attack end-users involve four main categories of Internet infrastructure or entities:

- Domain name registration. At this stage, the abuser selects the appropriate registrar to register the domain name for user access to the abusive content. According to the data published by ICANN, there are presently 2543 ICANN-accredited [15] registrars worldwide. Generally, abusers choose registrars that are inefficient at handling abusive domains or charge lower fees for domain names.

- Renting web servers. A web hosting provider provides the services required for the abuser to create and maintain websites and make them available on the World Wide Web. When choosing a provider, abusers consider the price and the provider's authority to fight against abusive domain names. For example, most owners of pornographic websites do not choose a provider in China. This is because the Chinese providers require the site owner to authenticate with their real name. This dramatically increases the risk of legal sanctions against abusers.

- Configuring DNS records for the domain name. Similarly, the abuser chooses a DNS hosting provider and uses the resolution services it provides to configure the correct DNS records for the domain name.

- Accessing abusive domain names. An end-user accesses abusive domain names using the browser of a device (PC or cell phone) based on the network service provided by the Internet Service Providers (ISPs). In resolving the domain name to an IP, the DNS recursive server used by the user may be the ISP's default configuration or another organization's DNS (for example, Google 8.8.8.8) configured by the user.

Abusive domain names require many Internet resources if they are to function correctly. If an abuser acquires a resource directly (through purchase or provisioning), the related service provider would be the most effective party to handle the issue. Likewise, when a service is compromised, its owner and provider might play a critical role in fixing the compromise and misuse. In general, these entities are not just accountable for the proper operation of the Internet ecosystem, such as Internet users accessing websites via their browsers. Additionally, these entities are responsible for fighting against abusive domain names.

4. Abusive Domain Names by Internet Entities

Identifying and detecting abusive domain names, their reporting, and how they should be addressed are hot topics in the Internet enterprise and the academic fields.

- Detection of abusive domain names. Many [4][5][6][7][8][16][17][18] have focused on detecting abusive domains; that is, how to quickly detect different types of abusive domains, such as phishing and malware, from a large number of domains on the Internet. The methods or systems proposed in these works are divided into two categories: Blacklists and proactive detection. So far, blacklists have been the most popular solution that prevents users from accessing malicious domains. A blacklist is a list of identifiers of malicious communication objects. Some utilize techniques such as machine learning or deep learning to detect malicious domains proactively. These methods are primarily based on various types of information present in domains, such as WHOIS, web content, and DNS records.

- Abusive domain name notifications/reporting. Numerous [9][19][20][21][22] have been conducted to determine whether and how abuse notifications can help speed the cleanup of compromised websites. Notifications can be issued to the affected owners of the site or their hosting providers. Cetin et al. [19] conducted the first empirical one of a real-world 'walled garden' system for notifying and quarantining end-users with malware-infected computers—a well-recognized ISP security best practice. Vasek et al. [22] found that more detailed abuse notifications to hosting providers resulted in a greater cleanup rate than notifications with less information. Jhaveri et al. [9] developed a model of the abuse reporting infrastructure to explain how volunteer action against cybercrime operates today, to increase understanding of what works and how to improve remediation effectiveness in the future.

- Handling abusive domain names. As it is known, Domain name system security is a joint task for the Internet industry. Meanwhile, the ongoing security community works to mitigate security threats to the DNS. ICANN and its multistakeholder community have engaged in an extended dialogue on DNS abuse and the need to define, measure, and mitigate DNS-related security threats [23]. Domain blocking should never be taken lightly and should always be considered a last resort in the fight against unlawful content. Not only is deleting such content more effective in the long term, but it also mitigates the possibility of collateral damage associated with domain blocking [24]. Hu et al. [25] conducted empirical research of browser Internationalized Domain Names (IDN) policies and a user to ascertain how users perceive homograph IDNs. They also evaluated the browser's protection against homograph IDNs systematically. Liu et al. [26] characterized the impact that registrar-level interventions have had on scammers' use of domain names, how and why scammers have adapted in response, and ultimately how to reason about the use of this approach as a general anti-abuse tool. Mohammadreza et al. [27] carried out to assess the effectiveness of known solutions to prevent DNS rebinding attacks. Moreover, they proposed a defensive measure, a browser plug-in, that can detect, inform, and protect users in the event of an attack.

References

1. 2019 Internet Crime Report Released. Available online: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (accessed on 25 February 2022).
2. Internet Organised Crime Threat Assessment (IOCTA). 2019. Available online: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (accessed on 25 February 2022).
3. M3AAWG Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers. Available online: https://www.m3aawg.org/sites/default/files/document/M3AAWG_Hosting_Abuse_BCPs-2015-03.pdf (accessed on 25 February 2022).
4. Szurdi, J.; Kocso, B.; Cseh, G.; Spring, J.; Felegyhazi, M.; Kanich, C. The long "taile" of typosquatting domain names. In Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, USA, 20–22 August 2014; pp. 191–206.
5. Antonakakis, M.; Perdisci, R.; Dagon, D.; Lee, W.; Feamster, N. Building a dynamic reputation system for DNS. In Proceedings of the 19th USENIX Security Symposium (USENIX Security 10), Washington, DC, USA, 11–13 August 2010.
6. Plohmann, D.; Yakdan, K.; Klatt, M.; Bader, J.; Gerhards-Padilla, E. A comprehensive measurement study of domain generating malware. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016; pp. 263–278.
7. Liu, D.; Li, Z.; Du, K.; Wang, H.; Liu, B.; Duan, H. Don't let one rotten apple spoil the whole barrel: Towards automated detection of shadowed domains. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 30 October–3 November 2017; pp. 537–552.
8. Tian, K.; Jan, S.T.K.; Hu, H.; Yao, D.; Wang, G. Needle in a haystack: Tracking down elite phishing domains in the wild. In Proceedings of the Internet Measurement Conference 2018, New York, NY, USA, 31 October–2 November 2018; pp. 429–442.
9. Jhaveri, M.H.; Cetin, O.; Gañán, C.; Moore, T.; Eeten, M.V. Abuse reporting and the fight against cybercrime. ACM Comput. Surv. 2017, 49, 1–27.
10. SAC115 SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS. Available online: https://www.icann.org/en/system/files/files/sac-115-en.pdf (accessed on 25 February 2022).
11. Public Security Administration Punishment Law of the People's Republic of China. Available online: http://www.law-lib.com/law/law_view.asp?id=403793 (accessed on 25 February 2022).
12. Standing Committee of the National People's Congress. Criminal Law of the People's Republic of China. Available online: https://www.gzzx.gov.cn/rdzt/kjyqgzzxzxd_1/fyygflfg/202106/P020210615548394847969.pdf (accessed on 25 February 2022).
13. The Central People's Government of the People's Republic of China. Decision of the Standing Committee of the National People's Congress on Maintaining Internet Security. Available online: http://www.gov.cn/gongbao/content/2001/content_61258.htm (accessed on 25 February 2022).
14. The State Council Information Office of the People's Republic of China. Indonesia Will Block 90% of Pornographic Websites. Available online: http://www.scio.gov.cn/wlcb/blxxjbygl/Document/732654/732654.htm (accessed on 25 February 2022).

15. List of Accredited Registrars. Available online: https://www.icann.org/en/accredited-registrars?sort-direction=asc&sort-param=name&page=1&view-all=true (accessed on 25 February 2022).
16. Cheng, Y.; Chai, T.; Zhang, Z.; Lu, K.; Du, Y. Detecting malicious domain names with abnormal whois records using feature-based rules. Comput. J. 2021.
17. Shin, S.; Gu, G. Conficker and beyond: A large-scale empirical study. In Proceedings of the 26th Annual Computer Security Applications Conference, New York, NY, USA, 6–10 December 2010; pp. 151–160.
18. Xia, P.; Nabeel, M.; Khalil, I.; Wang, H.; Yu, T. Identifying and characterizing COVID-19 themed malicious domain campaigns. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, Virtual Event, USA, 26–28 April 2021; pp. 209–220.
19. Cetin, O.; Ganán, C.; Altena, L.; Tajalizadehkhoob, S.; van Eeten, M. Let me out! Evaluating the effectiveness of quarantining compromised users in walled gardens. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, MD, USA, 12–14 August 2018; pp. 251–263.
20. Çetin, O.; Gañán, C.; Altena, L.; Tajalizadehkhoob, S.; Van Eeten, M. Tell me you fixed it: Evaluating vulnerability notifications via quarantine networks. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 326–339.
21. Maass, M.; Stver, A.; Pridhl, H.; Bretthauer, S.; Herrmann, D.; Hollick, M.; Spiecker, I. Effective notification campaigns on the web: A matter of trust, framing, and support. In Proceedings of the 30th USENIX Security Symposium, Virtual Event, 11–13 August 2021; pp. 2489–2506.
22. Vasek, M.; Moore, T. Do Malware reports expedite cleanup? An experimental study. In Proceedings of the CSET'12, Bellevue, WA, USA, 6 August 2012.
23. Ongoing Community Work to Mitigate Domain Name System Security Threats. Available online: https://blog.verisign.com/domain-names/ongoing-community-work-to-mitigate-domain-name-system-security-threats/ (accessed on 25 February 2022).
24. Eco topDNS Initiative Fights DNS Abuse. Available online: https://circleid.com/posts/20220208-eco-topdns-initiative-fights-dns-abuse (accessed on 25 February 2022).
25. Hu, H.; Jan, S.T.K.; Wang, Y.; Wang, G. Assessing Browser-level defense against IDN-based phishing. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), Anaheim, CA, USA, 11–13 August 2021; pp. 3739–3756.
26. Liu, H.L.; Levchenko, K.; Félegyházi, M.; Kreibich, C.; Maier, G.; Voelker, G.M. On the effects of registrar-level intervention. In Proceedings of the 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 11), Berkeley, CA, USA, 29 March 2011.
27. Hazhirpasand, M.; Ebrahim, A.A.; Nierstrasz, O. Stopping DNS rebinding attacks in the browser. In Proceedings of the ICISSP, Online Streaming, 11–13 February 2021; pp. 596–603.