ICANN Submission to ITU Council Working Group on the Internet

14 September 2021

Submission Summary

This is the Internet Corporation for Assigned Names and Numbers' (ICANN) contribution in response to the ITU Council Working Group on International Internet-Related Public Policy Issues Call for Comments[1] on the topic "The role of the Internet and international Internet-related public policy in mitigating the impact of COVID-19 and possible future pandemics".

Introduction

The Internet is an important tool for mitigating the impact of the COVID-19 pandemic and possible future pandemics. Preserving the security, safety, stability, and resiliency of the global network is vital to sustaining and fortifying the overall trust that users around the world have in Internet services. Many technical organizations around the world work together to ensure this trust remains, especially with the growing reliance on the Domain Name System (DNS) as a trustworthy underlying infrastructure.

ICANN, whose mission is to coordinate the stable operation of the Internet's unique identifier systems (including the DNS), dedicates an important part of its work to ensuring a strong foundation for this activity globally. It does so, in cooperation with other relevant stakeholders, by monitoring security trends and potential threats to the stability of the DNS and keeping the global community informed about the latest developments touching on ICANN's mission. This allows for a cooperative and multistakeholder approach in identifying and mitigating risks. The DNS is a centerpiece of the Internet infrastructure, providing the ability for anyone globally to access services and applications online by name instead of by numbers. The continued resilience and security of the DNS is critical regardless of the situation, location, and contingencies.

Several factors imposed by the pandemic have forced people around the world to work and live differently: lockdowns have increased remote working and boosted online shopping habits of consumers in countries with the existing infrastructure, moreover, decreased travel has transferred many face-to-face interactions and events to online video calls. Inevitably, all these changes created additional demand on the DNS.

In addition to the resilience of the DNS, there is also the question of the malicious use of domains, often referred to as domain abuse. These are domains created with the aim of

[1] Published here: https://www.itu.int/en/council/cwg-internet/Pages/consultation-feb2021.aspx

harming innocent Internet users. Various forms of abuse exist including attempting to steal login credentials (phishing), installing malicious software (malware) and sending unwanted email (spam, often used to facilitate other forms of abuse).[2]

Background Summary

To assess the impact of the pandemic on the DNS, the ICANN organization (ICANN org) conducted tests and analyzed traffic data to measure and test the resilience built into the DNS. These measurements and studies demonstrated that the DNS has handled the increase in traffic and proved its resiliency by responding to the new challenges.[3]

Suspicious vs Malicious

Major events, such as the COVID-19 pandemic, attract unscrupulous actors to create phishing/malware sites. The proportion of new pandemic-related domains seen to be involved with phishing or malware distribution (malicious domains) is around 2% or as high as 6% with a lower evidentiary bar. To put this in another way, 94% to 98% of new registrations which contained COVID-19 related terms showed no evidence of malicious use.

Accordingly, any effort to label suspicious domains as malicious should be conducted carefully to avoid including benign domains. ICANN org ensures making this distinction when looking at the potentially pandemic-related domains by filtering lists of new registrations against a set of key-words. To categorize and separate newly registered malicious domains from the merely “suspicious” or “potentially malicious”, ICANN org looks for third-party evidence for each domain’s status. The details of this work are presented elsewhere.[4]

It is also worth noting, that while ICANN org included translations of terms allowing filters to pick up non-English language and non-Latin characters via Internationalized Domain Names (IDNs) for identification of the malicious sites, country code top-level domains (ccTLDs) were not analyzed, as ICANN org does not have access to ccTLD data.

---

[2] See: ICANN, DNS Security Threat Mitigation Program, https://www.icann.org/dnsabuse

[3] Roy Arends, ICANN Office of the Chief Technology Officer, Analysis of the Effects of COVID-19-Related Lockdowns on IMRS Traffic, OCTO-008, 15 April 2020, https://www.icann.org/en/system/files/files/octo-008-15apr20-en.pdf

[4] Siôn Lloyd, Reporting Potential Pandemic-Related Domains, 1 May 2020, https://www.icann.org/en/blogs/details/reporting-potential-pandemic-related-domains-1-5-2020-en
Siôn Lloyd, An 18 Month Summary of ICANN’s Domain Name Security Threat Information Collection and Reporting (DNSTICR) Project, 2 September 2021, https://www.icann.org/en/blogs/details/an-18-month-summary-of-icanns-dnsticr-project-2-9-2021-en
A more detailed report will be issued in the near future.

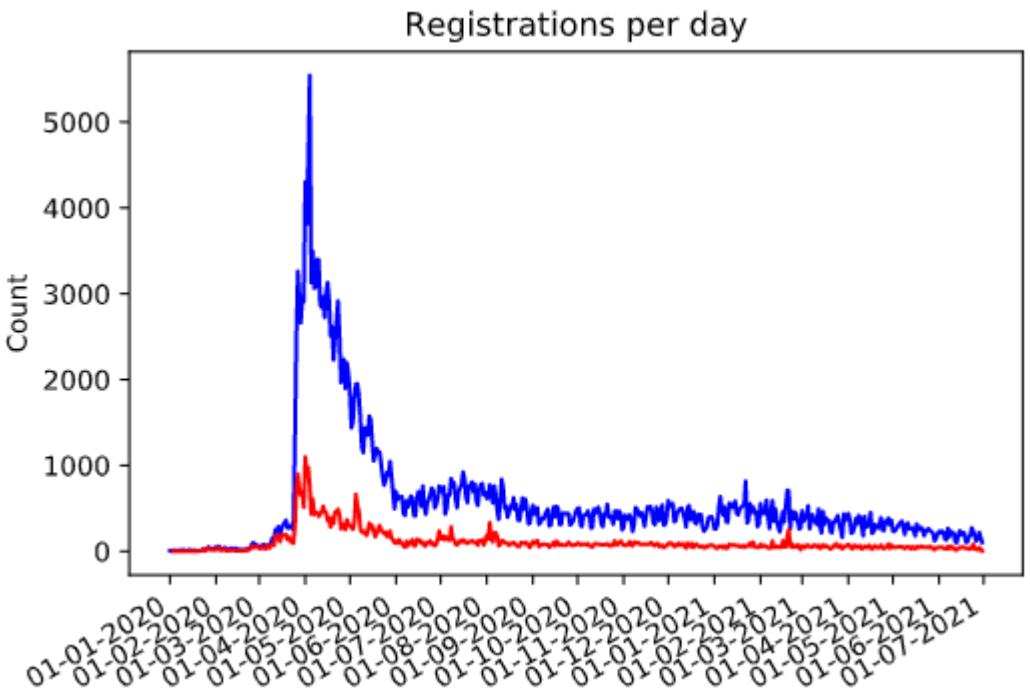

Figure1. --- Registrations per day matching one or more of our keywords
--- Registrations having one or more third-party reports

For example, the blue line in figure 1 above, shows new, pandemic-related domain registration volumes. Specifically, the volume of new registrations that match one or more terms from the list of pandemic-related key-words that ICANN org used within the study. The red line shows the number of those domains where any evidence of malicious behavior was found, representing the 6% figure above. Noticeably, there is a spike in pandemic-related registrations, which is accompanied by a matching growth of possible malicious content, lasting for a period of approximately two months. Yet, the majority of domains looked at display no evidence of phishing or malware distribution.

Understanding Context

The pattern above depicts pandemic-related new registrations only and should be seen in the wider context of malicious domain use that is not specifically pandemic related. To that end, ICANN org has a long-running project known as Domain Abuse Activity Reporting (DAAR)[5] which is a system for studying and reporting on malicious domain use across top-level domain (TLD) registries.

[5] See: the ICANN Domain Abuse Activity Reporting (DAAR) website: https://www.icann.org/octo-ssr/daar

By using a consistent methodology over time and observing data from before and during the pandemic, ICANN org noticed that the total number of malicious domains actually fell in the early stages of the pandemic. Figure 2 below shows the counts of domains seen on Reputation Block Lists (RBLs)[6] illustrating this drop, before levels pick up again in the second half of the year.

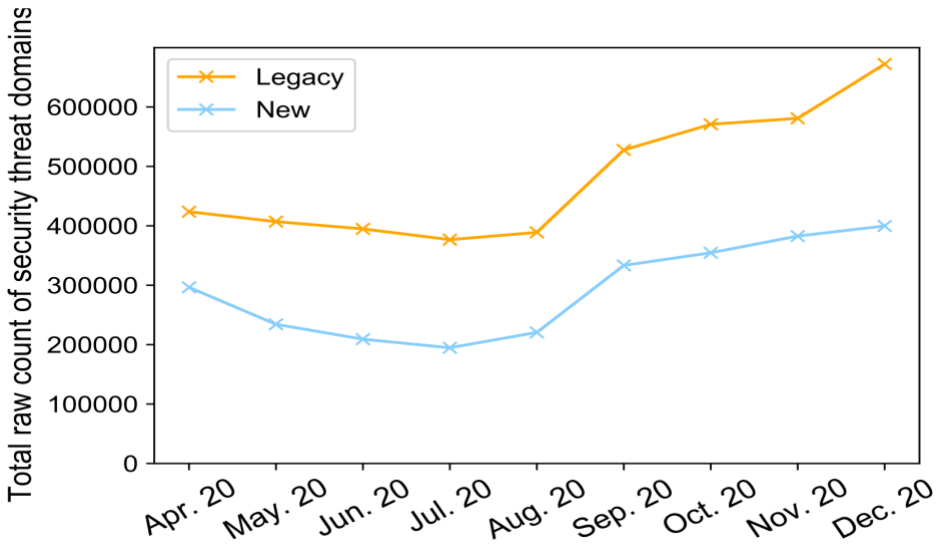

Figure 2. Total counts of abusive domains seen in a set of RBLs across TLDs. “legacy” indicates TLDs created before 2010 and “new” indicates those created later.

Information Sharing

ICANN org also detects and analyzes sites which assume fraudulent identities that may well mirror a legitimate government site or appear to link to a government scheme. These sites are tailored to specific countries or regions. For example, figure 3 depicts two versions of the same template being used to target two different countries (other countries were also seen being targeted with this template).

[6] RBLs report domains that are seen to present a security threat of some kind, be that phishing, malware, botnet activity or spam. More details on how this data is collected and used can be found on the DAAR web page: ICANN, Domain Abuse Activity Reporting, https://www.icann.org/octo-ssr/daar

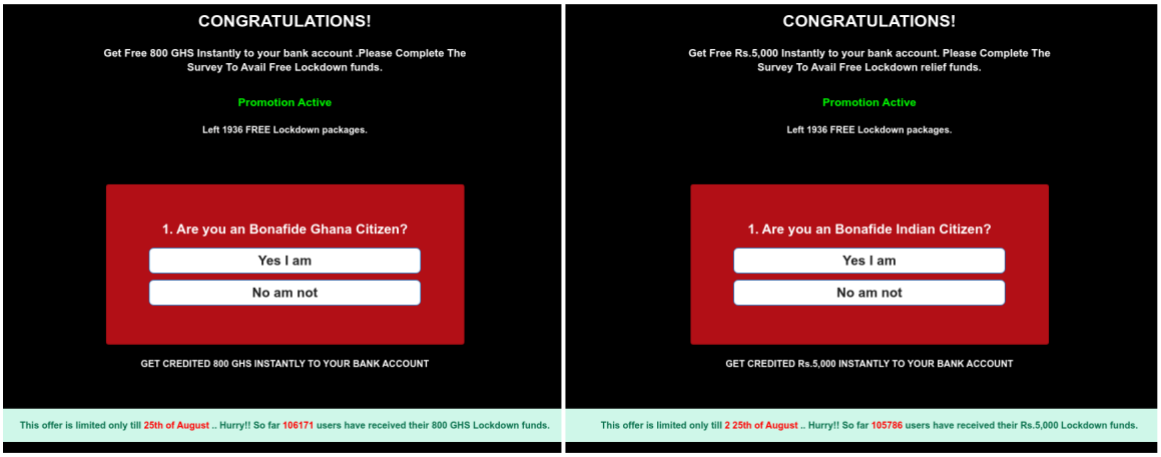

Figure 3. Phishing template customized to two different countries.

Having a “bigger picture” of suspicious or malicious domain names can show patterns which may make spotting other abusive domains possible. Therefore, information sharing can amplify the effectiveness of efforts to remove malicious domains. This could be paramount in times of crisis, when the demand for specific new domain names increases, consequently leading to a growth in specific domain name misuse. In mid-March 2020, it was relatively early in the unfolding situation that collaborative groups started being created to enable the sharing of threat intelligence, for example the COVID-19 Cyber Threat Coalition (CTC) or the COVID-19 Cyber Threat Intelligence (CTI) League.

Knowledge Sharing

There is benefit to be gained from knowledge sharing around general best practices for DNS security. ICANN’s new program KINDNS[7] (Knowledge-Sharing and Instantiating Norms for DNS and Naming Security) was created to develop a framework that focuses on the most important operational best practices or concrete instances of DNS security best practices. With KINDNS, ICANN will work with the DNS technical community to identify and document (in the form of guidelines) a set of mutually agreed norms that support a secure DNS ecosystem that both small and big operators can easily implement. The goal of the program is to provide an additional layer of guarantees against the possible misuse of domain name registrations during the time of crises, such as the COVID-19 pandemic.

Conclusion

The research findings described above demonstrate the resilience of the DNS. Moreover, they highlight the importance of data collection and analysis, as well as collaboration in

[7] ICANN Community, Knowledge-sharing and Instantiating Norms for DNS and Naming Security (KINDNS), https://community.icann.org/display/KINDNS

sharing the findings to mitigate the impact of pandemics or other threats to the system. ICANN org concludes that there continues to be a need for accumulation and analysis of the data for research into the specific pandemic-related circumstances of DNS registration and DNS abuse.

ICANN org will continue to encourage and work with all relevant stakeholders around the world, who are actively engaged in mitigating the impact of COVID-19 and possible future pandemics, to preserve and further develop a strong and resilient Internet infrastructure.