The Last Four years in Retrospect: A Brief Review of DNS Abuse Trends

DNS Security Threat Mitigation Program

Samaneh Tajalizadehkhoob, Lead Security, Stability & Resiliency Specialist

Russ Weinstein, VP GDD Accounts and Services

22 March 2022

ICANN

TABLE OF CONTENTS

Introduction

Domain Name System (DNS) abuse is one of the most important ongoing discussions in the community and ICANN is the right place for these discussions. However, depending on what you mean by DNS abuse, some types of abuse perpetrated via the Internet may not fall within ICANN's remit and capabilities as the technical coordinator of the DNS. ICANN is not and was not designed to be the Internet's content police. Instead, ICANN org has a program focused on DNS security threats, which are within ICANN's technical remit and capabilities. To facilitate and inform the community's discussion, part of our role is to collect and provide high-quality data and reporting on trends related to DNS security threat concentrations.

Many of the existing industry white papers and general discussions around abuse incidents are based on data from Reputation Blocklists (RBLs). The results of such reports often indicate that domain name abuse is growing. However, these papers typically have used studies focused on a short time span such as half a year or less. Here, we study a longer time horizon, using the data from ICANN org's Domain Abuse Activity Reporting (DAAR) project.

The DAAR system collects DNS security threat data for phishing, malware, botnet command and control domains and spam as a delivery mechanism from Reputation Blocklist providers. Previous research shows that when the overlap between reputation feeds (RBLs) of different providers were studied, very little overlap has been found indicating that each list covers a different yet important part of this heterogeneous security threat landscape.[1] [2] This is why, for ICANN org's DAAR project, we use multiple well-reputed RBLs from a variety of providers, such as: SURBL, Spamhaus, Anti-Phishing Working Group, PhishTank, Malware Patrol, and Abuse.ch. For more detailed information about data sources please refer to the latest DAAR report.

General Statistics

In this report we demonstrate some of the general trends in security threat concentrations starting from when we began the DAAR project in October 2017 until January 2022. Figure 1 below shows changes in the total sum of domains in generic top-level domain (gTLD) zone files (new and legacy) that are included in DAAR over time. As both the blue line for legacy gTLDs and red line for new gTLDs indicate, the number of names have grown in the gTLD space in general.

[1] Kührer, Marc, Christian Rossow, and Thorsten Holz. "Paint it black: Evaluating the effectiveness of malware blacklists." International Workshop on Recent Advances in Intrusion Detection. Springer, Cham, 2014.
[2] Griffioen, Harm, Tim Booij, and Christian Doerr. "Quality evaluation of cyber threat intelligence feeds." International Conference on Applied Cryptography and Network Security. Springer, Cham, 2020.

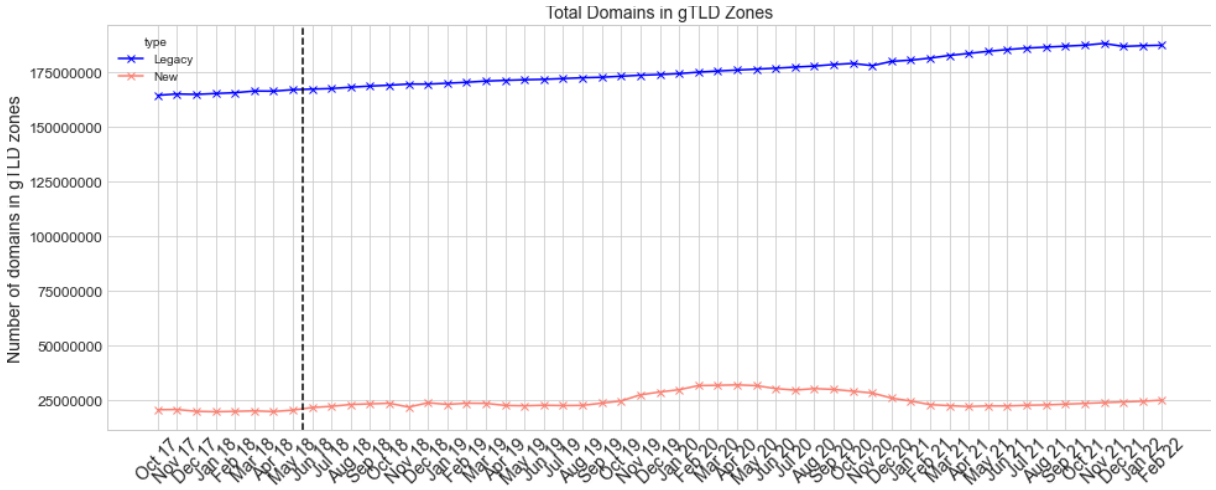

Figure 1 - Total number of domain names in gTLD zones over time

While Figure 1 demonstrates growth in the total number of registered domains in zone files, Figure 2 shows that the total number (absolute count) of security threat domains, according to the RBLs we use for DAAR, declined over the same period. What we do know from a closer look at the source data is that the spam data from Spamhaus is a significant contributor to the decline. Future research by ICANN's Security, Stability and Resiliency (SSR) group will take a deeper dive into the underlying reasons for the decline as well as the periodic spikes in the data.

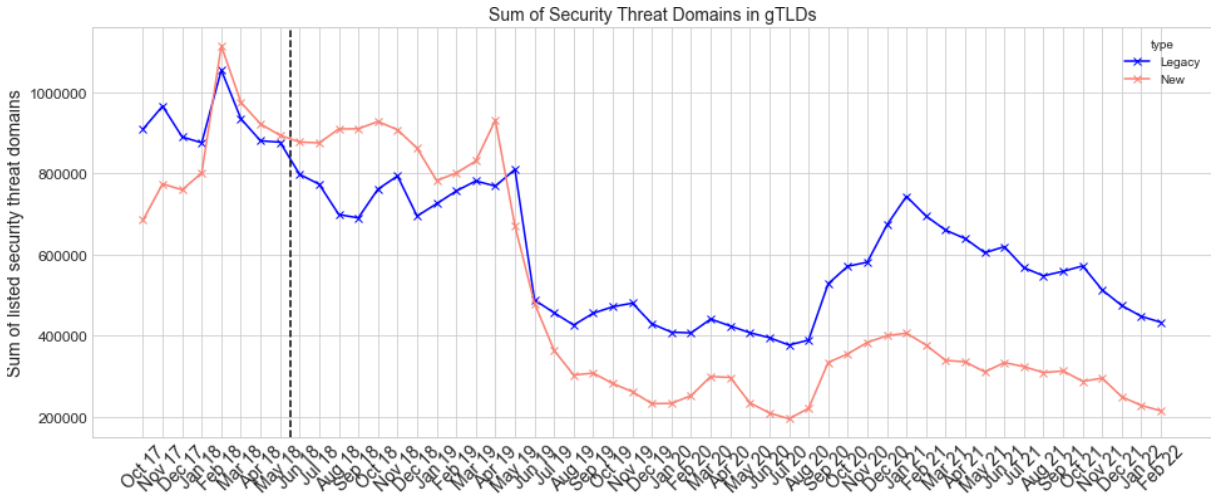

Figure 2 - Sum of absolute counts of security threat domains across threat gTLD types over time

While absolute counts are important to understand the scale of the security threat concentrations across gTLDs, relative normalized counts, which take the size of gTLDs into account, are essential to put these counts and trends into perspective of how gTLDs are performing in comparison to their sizes and market shares.

Figure 3 shows the changes in the normalized sum (percentage) of security threat domains in gTLDs over time. This is calculated by taking the sum of security threat domains in each type of gTLD and dividing it over the sum of each gTLD size, and then taking the percentage of this for any given month.[3] See Figure 3 for more details. As the trend shows, in February 2022, security threat domains are less than 1% of all domain names in new gTLDs and closer to 0.5% in legacy gTLDs.

[3] Normalized [%] of security threat = (Sum of absolute counts of security threat domains per gTLD type/Sum of gTLD sizes per gTLD type) * 100

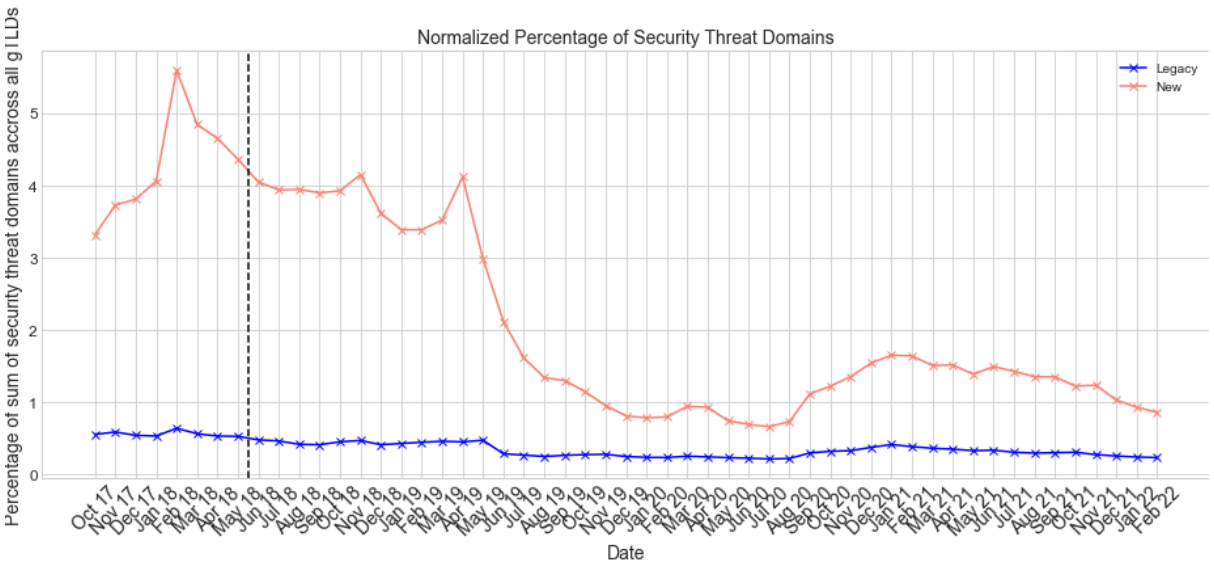

Figure 3 - Normalized [percentage] of security threat domains across gTLD types over time

Please note that our calculations of a normalized percentage of security threat domains in gTLDs over time is different from the calculations used in the DAAR monthly report. We focus on the “sum of security threat domains over a month” whereas DAAR reports look at “average number of security threat domains over a month.

Last but not least, we look at how the proportion of different threat types changed over the years. As the bar plot in Figure 4 shows, the proportions remain quite constant over time, with spam being the most prominent type, for which we collect data, followed by phishing.

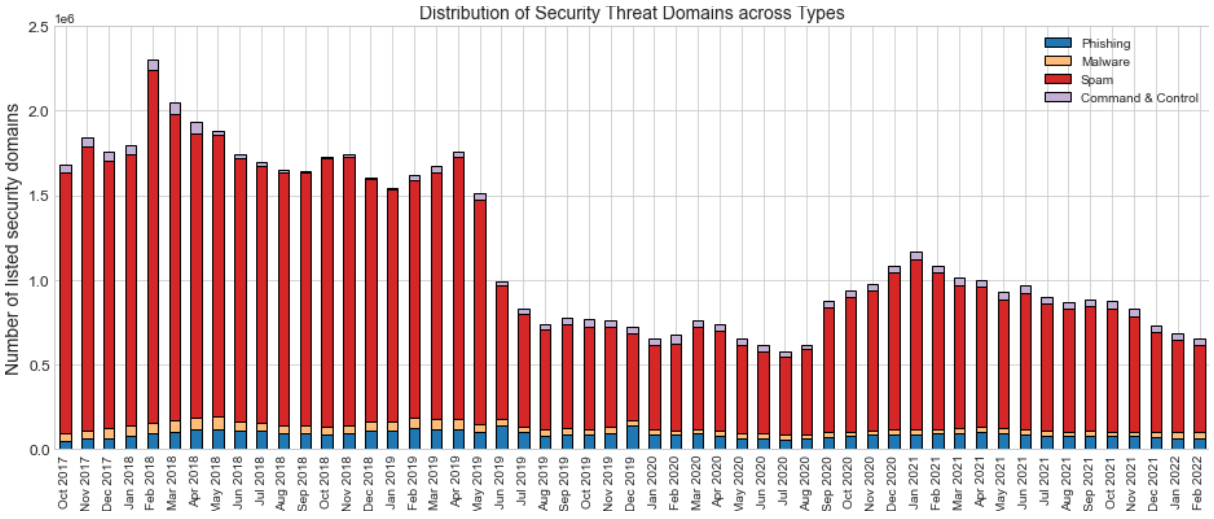

Figure 4 - Distribution of security threat domains across threat types over time

Conclusion

When trying to spot trends it is important to ensure an understanding of the timeframe and perspective of the data set being analyzed, i.e., the question that is answered using the data. While looking at recent data is interesting, it is important to zoom out to assess the context of the trend. As the data shows here, once we zoom out, we see DNS security threats trending down both in absolute terms and normalized rates. This does not mean the work is any less important and certainly not done when it comes to combating DNS security threats. ICANN org encourages the community to continue the important discussions about what additional measures can and should be done to further combat DNS abuse. In parallel, ICANN org continues to focus efforts on supporting the mitigation of DNS security threats, with projects like DNSTICR, increasing data sets in DAAR, and enhanced reporting by Contractual Compliance to name a few. For more information, please visit: https://www.icann.org/dns-security-threat.

One World, One Internet

Visit us at **icann.org**


@icann


facebook.com/icannorg

youtube.com/icannnews


flickr.com/icann


linkedin/company/icann


soundcloud/icann


instagram.com/icannorg