Domain Abuse Activity Reporting (DAAR) System

Updated monthly report on data from November 2021

Office of the CTO Security, Stability and Resiliency team

November 2021

Contents

Preface

This report highlights activities reported in the Domain Abuse Activity Reporting (DAAR) System using monthly median values over the whole of November 2021. The DAAR system studies security threat concentrations across all top-level domain (TLD) registries for which required data is available. The report provides aggregated statistics and time series analysis about a specific set of security threats[1]. While no single snapshot can capture trends or anomalies, historical data collected over time will show trends and can be used to identify areas for further study. For more information regarding data used in the DAAR monthly report see *"Understanding the Domain Abuse Activity Reporting (DAAR) Monthly Report"* [1].

The overarching purpose of DAAR is to give the ICANN community reliable and persistent data as well as insights that help inform policy discussions around security threat concentration patterns utilizing an open and community vetted methodology. DAAR monthly reports do not measure security threat mitigations, i.e., how reliably or quickly security threats are mitigated by TLDs. DAAR only provides aggregated information related to trends in concentrations of security threats across TLDs based on threat data listed by the Reputation Block List (RBL) providers listed in the Appendix. The data from these third-party RBLs are collected using different methodologies such as honeypots, spam filters, and crowdsourcing, among others. As such, they are subject to limitations that correspond to their methodology. The DAAR system aims to use highly reputable data feeds and makes continuous attempts to evaluate and update DAAR RBL input lists accordingly. It is important to note that apart from a few feeds where the RBL itself contains tags, neither the DAAR system nor the other feeds make an explicit distinction between maliciously registered domains and those that have been compromised. To learn more about DAAR, visit the ICANN Domain Abuse Activity Reporting web page [2].

Up to June 2020, DAAR provided aggregated monthly gTLD registry reports only. From July 2020 onwards, ccTLDs could also volunteer to join the DAAR project by providing their zone files. Currently, ccTLD managers get their own individualized monthly report and their numbers are not included in this report. We intend on providing similar reports to gTLD managers in the future.

Finally, reporting about registrar portfolios requires domain name registration data to identify which domains are sponsored by which registrars. A system that can collect and analyze the necessary registrar data on a daily basis remains under development. We hope to add registrar reporting in future reports.

[1] The security threats of interest to DAAR for this report are: spam, phishing, malware distribution, and botnet command and control.

Executive Summary

The Domain Abuse Activity Reporting (DAAR) system provides data related to domain names and security threat concentrations within all generic Top-Level Domains (gTLDs) and other TLDs that have made their zone files available for analysis. This November 2021 report looked into 211,328,474 domain names from 1131 gTLDs in comparison to last month's 210,496,744 domains in 1116 gTLDs. Reputation feeds the DAAR system employs, reported at least one security threat in 437 of the 1131 gTLDs as of November 2021 in comparison to 457 of the 1116 gTLDs identified in October 2021. As a result, this report provides an analysis for only the 829,494 domains within the 437 gTLDs with at least one security threat.

Security threats are not uniformly distributed across legacy[2] and new gTLDs. While new gTLD domains seem to be more used in spam[3], domains in legacy gTLDs are distributed over botnet command and control (C&C) and malware with phishing being relatively equally distributed over both gTLD types.

Additionally, the report shows that while knowing where most security threat domains are concentrated is important, for a meaningful comparison between TLDs, the number of security threat domains needs to be normalized by the size of the TLDs.

[2] gTLDs launched before 2010, referred to hereafter as "Legacy gTLDs"

[3] when spam is used as a delivery mechanism for other types of threats such as a mean for malware distribution or provision of access to phishing links

1 General Trends in gTLDs

In November 2021, DAAR collected zone data for 1131 gTLDs. Table below summarizes the data captured in November 2021 and indicates the changes from the data reported for the previous month.

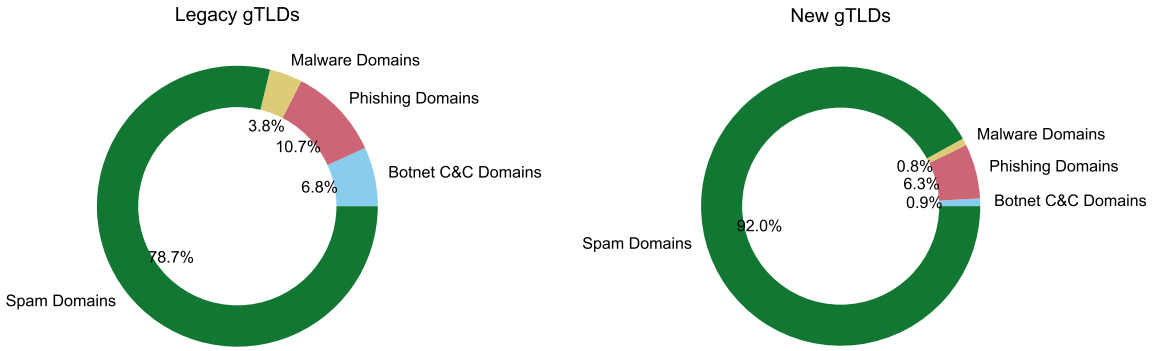
Table 1: Comparison of median counts over two consecutive months

	Total in DAAR		**Total listed as security threat**	
	TLDs	Domains	TLDs	Domains
31 October 2021	1116	210,496,744	457	890,529
30 November 2021	1131	211,328,474	437	829,494
+/- changes from previous month	15	831,730	-20	-61,034

The first column reports data on total domains and gTLDs for which DAAR collects data in two consecutive months. The second column reports numbers of domains and their corresponding gTLDs that are listed at least once in the RBLs that DAAR utilizes within the same time period.

2 Breakdown of Individual Security Threats

DAAR uses third-party reputation feeds to identify domain names that are associated with at least one of four kinds of security threats: phishing, malware distribution, botnet command-and-control, and spam. The rationale for tracking these specific security threats is documented in [3, 1]. Figures 1a and 1b display the breakdown of security threats out of the total number of threats identified this month in the reputation block list (RBL) data [4] that DAAR is utilizing for legacy gTLDs and new gTLDs respectively.



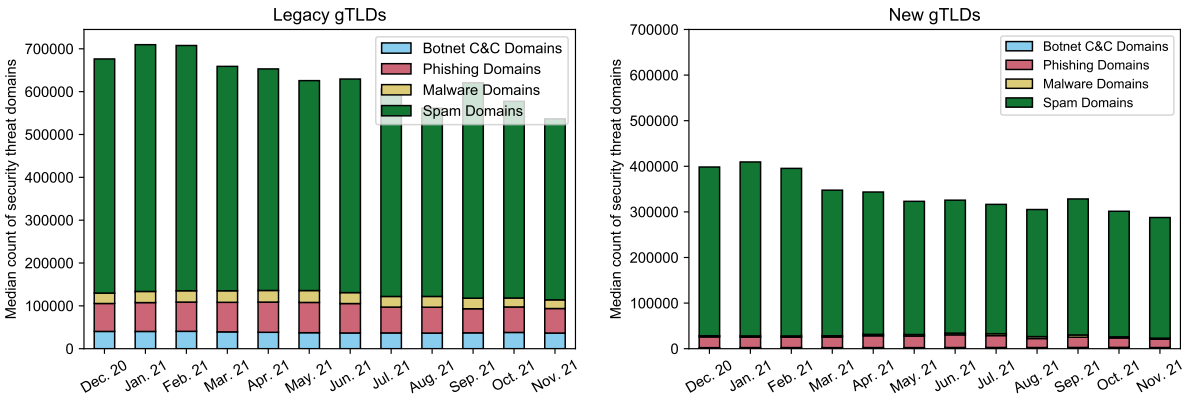
(a) (b)

Figure 1: Breakdown of domains identified as security threats across all DAAR threat types

Figures 2a and 2b display the breakdown of security threats in raw counts over time for legacy gTLDs and new gTLDs respectively.

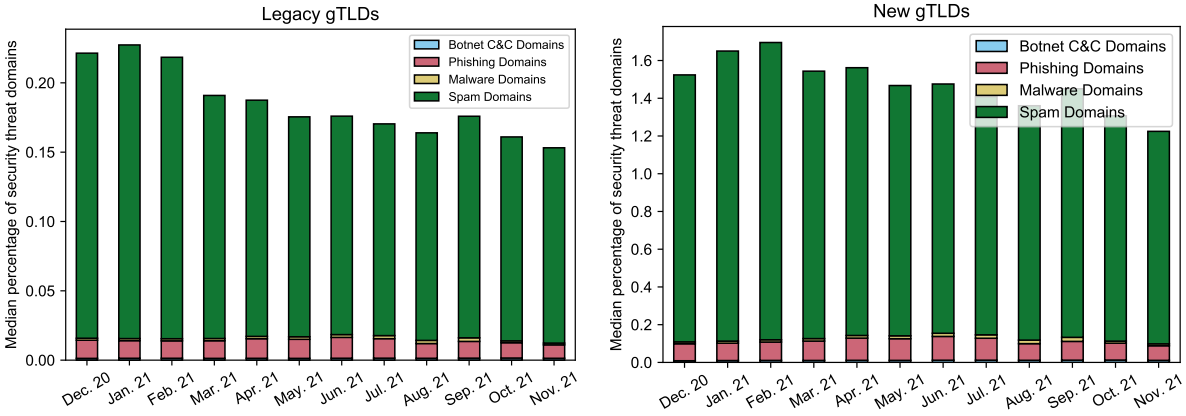
Figures 3a and 3b display the breakdown of security threat percentage in proportion to total domains over time for legacy gTLDs and new gTLDs respectively.

[4] The list of Security Threat Reputation Providers DAAR uses for the generation of this report is included in the Appendix.



(a) (b)

Figure 2: Breakdown of domains identified as security threats across all DAAR threat types over time



(a) (b)

Figure 3: Breakdown of percentage of domains identified as security threats in proportion to all domains in zone files across all DAAR threat types over time [note:y-axis scales differ across graphs]

3 Normalized Metric: Percentage of Security Threats

Raw counts of domains identified as security threats do not necessarily reflect the extent to which a TLD is the focus of exploitation by security threat actors, since each TLD has a different number of domains registered. For this reason, we calculate a normalized value, a percentage of security threat (P_{st}). P_{st} represents the percentage of domains that are listed for being a security threat in at least one of the reputation blocklist feeds DAAR utilizes, normalized by the amount of resolving domains within a given TLD. That is, P_{st} is determined as follows:Figure 4 demonstrates the median raw counts of domains identified as security threats (y-axis) versus domains in TLD zone files (x-axis) over this month. A logarithmic scale is used for the x-axis and y-axis to assist in visualizing the diverse counts of these two variables.

$$P_{st} = (\frac{\text{Median of domains identified as security threats in TLD}}{\text{Median number of domains within TLD zone}}) \times 100$$

P_{st} can be used to provide “apples to apples” comparisons for the number of resolving domains that are identified as security threats over time or between TLDs. This information could help the TLD operators determine whether their anti-abuse measures are effective as well as help the ICANN community in making informed policy decisions regarding security threat mitigation.

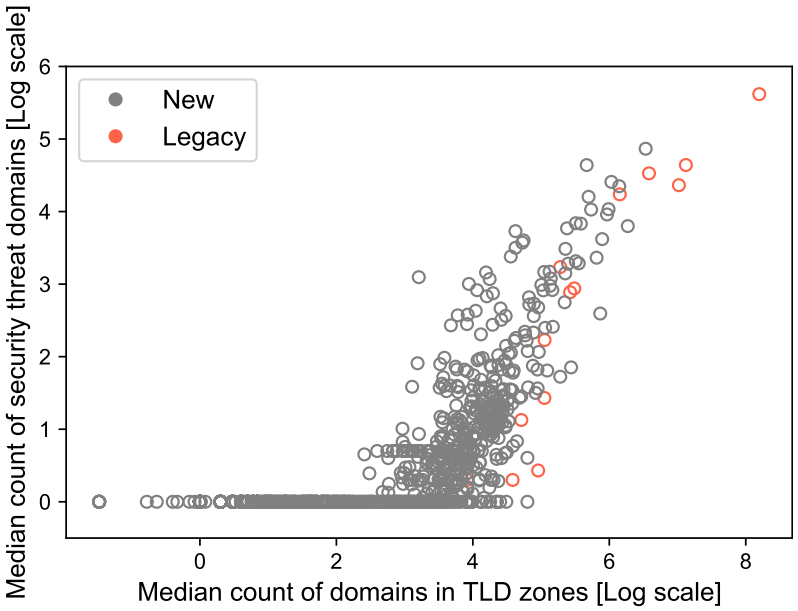


Figure 4: Raw counts of domains identified as security threat vs. median count of domains in TLD zones

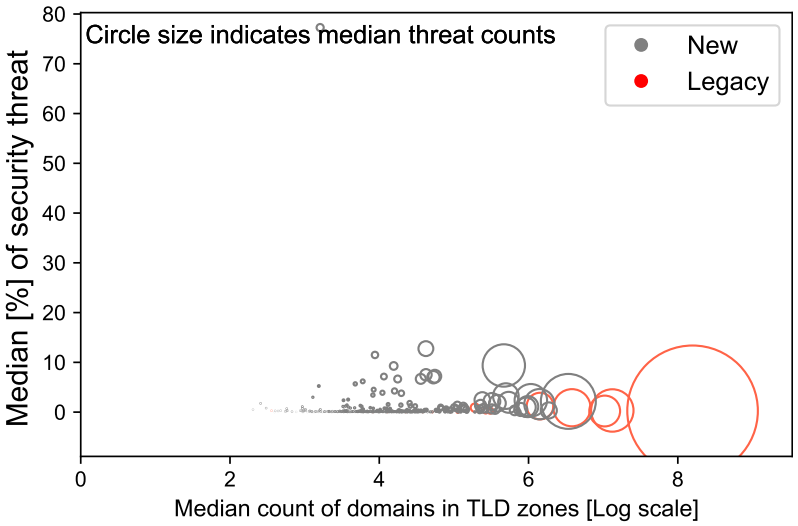


Figure 5: Percentage of domain names identified as security threats vs. median count of domains in TLD zones

The average P_{st} for all 1131 gTLDs in DAAR for November 2021 is approximately 0.28%. Figure 5 illustrates the P_{st} in these TLDs. Circle size indicates the median non-normalized raw counts of domains identified as security threats in November 2021. Additionally, Figure 6 displays the trends of the average P_{st} across different TLD types over time.

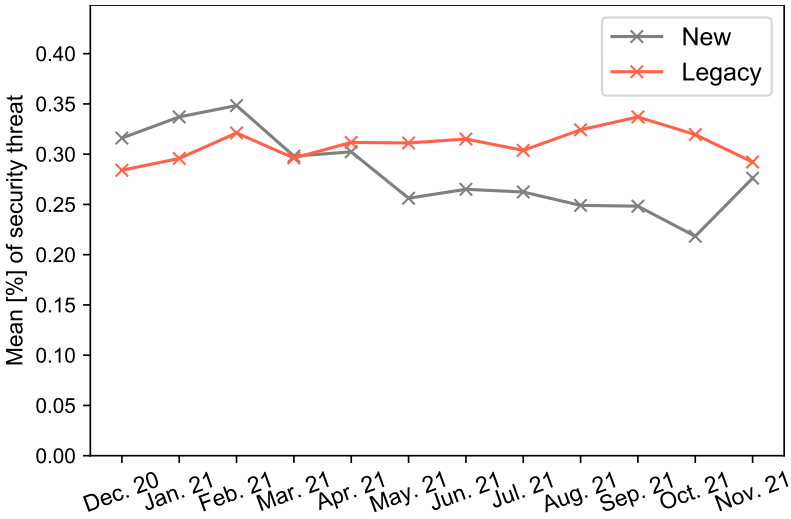


Figure 6: Percentage of domain names identified as security threats over time

4 Percentage of Security Threats: Breakdown of Individual Threats

Figure 7 displays the percentage of security threat for domains identified as security threats versus domains resolved in new and legacy gTLDs for each of the security threats of interest to DAAR. Each dot represents a TLD. The larger the dot, the higher the raw non-normalized count of domains identified as security threats.

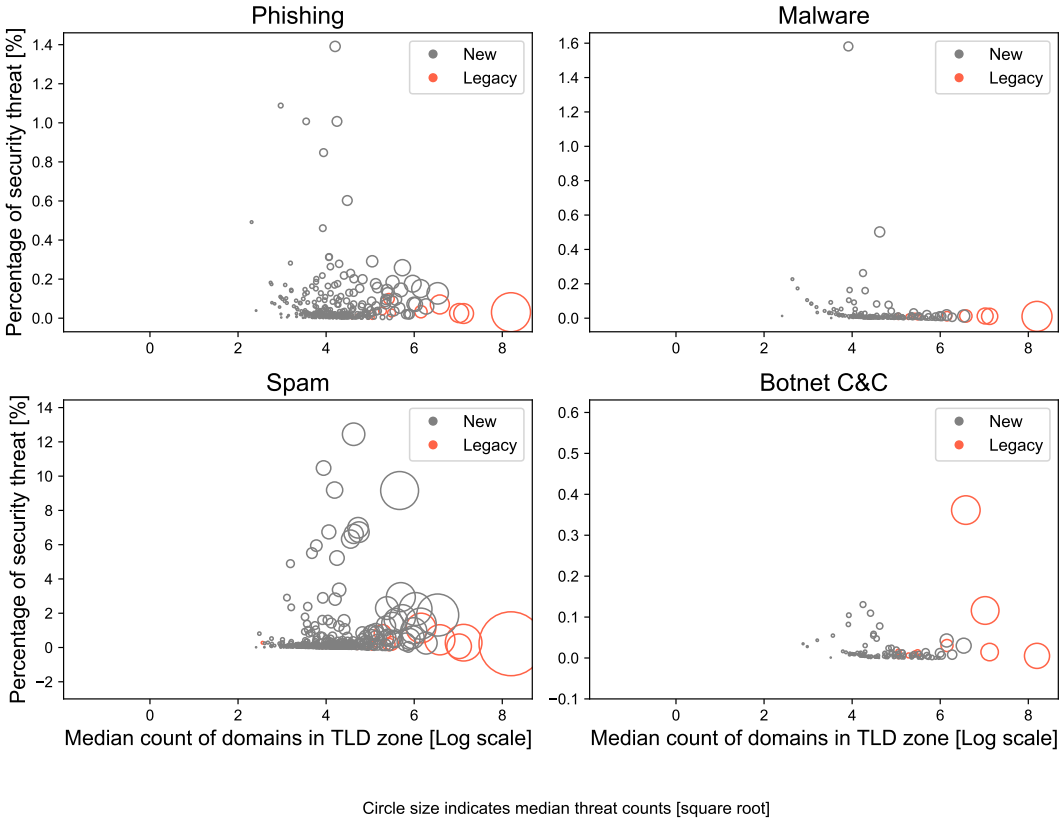


Figure 7: Percentage of domain names identified as security threats vs. counts of domains in TLD zones across different threat types

Finally, Figure 8 shows the trends in changes in the average percentage of security threat in legacy and new gTLDs over time for each security threat of interest to DAAR.

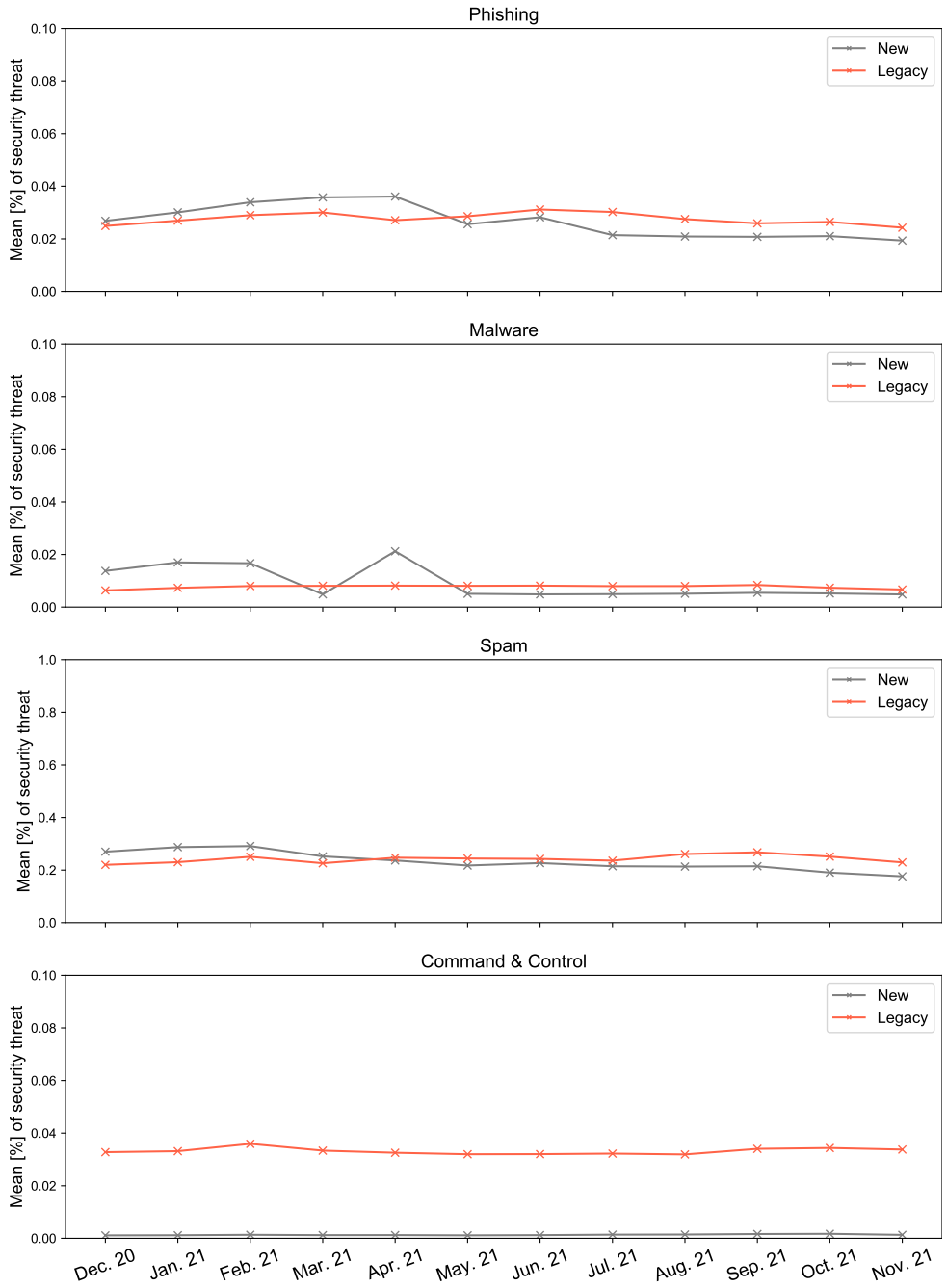


Figure 8: Average percentage of security threat in TLDs across different threat types over time

References

[1] *Understanding the Domain Abuse Activity Reporting (DAAR) Monthly Report*. https://www.icann.org/en/system/files/files/daar-monthly-report-04feb19-en.pdf. Jan. 2019.

[2] *ICANN Domain Abuse Activity Reporting*. https://www.icann.org/octo-ssr/daar. Dec. 2018.

[3] *The Domain Abuse Activity Reporting (DAAR) System Methodology Document*. https://www.icann.org/en/system/files/files/daar-methodology-paper-30nov17-en.pdf. Nov. 2017.

[4] *SURBL*. http://www.surbl.org/lists. Dec. 2018.

[5] *Spamhaus*. https://www.spamhaus.org. Dec. 2018.

[6] *Spamhaus Domain Block List (DBL)*. https://www.spamhaus.org/faq/section/Spamhaus%20DBL#291. Dec. 2018.

[7] *Anti-Phishing Working Group (APWG)*. https://www.apwg.org. Dec. 2018.

[8] *PhishTank*. https://www.phishtank.com. Dec. 2018.

[9] *Malware Patrol*. https://www.malwarepatrol.net/enterprise-threat-data/. Dec. 2018.

[10] *Abuse.ch*. https://abuse.ch. Dec. 2018.

[11] *Abuse.ch Feodo Tracker*. https://feodotracker.abuse.ch. Dec. 2018.

Appendix

The table below provides a listing of the reputation providers and feeds used in the DAAR system along with their corresponding threat types.

Reputation provider	Feed used	Threat type
SURBL [4]	JwSpamSpy + Prolocation	Spam
	Sa-blacklist	Spam
	SpamCop	Spam
	AbuseButler	Spam
	Phishing domains	Phishing
	Malware domains	Malware
Spamhaus [5]	Domain Block List (DBL) [6]	Spam - Phishing - Malware - Botnet C&C
Anti-Phishing Working Group [7]	Phishing URLs	Phishing
PhishTank [8]	Phishing URLs	Phishing
Malware Patrol [9]	Malware URLs	Malware
	Ransomware URLs	Malware
	Botnet C&C URLs	Botnet C&C
Abuse.ch [10]	FeodoTracker [11]	Malware