Domain Abuse Activity Reporting (DAAR) System

Report on data from 31 March 2018

Office of the CTO Security, Stability and Resiliency team

March 2018

Contents

1 General Trends in New and Legacy TLDs **5**
1.1 Distribution of Domains Identified as Security Threats 6

2 Breakdown of Individual Security Threats **7**

3 Normalized Metric: Percentage of Abuse **8**

4 Percentage of Abuse: Breakdown of Individual Security Threats **9**

Executive Summary

This 31 March 2018 report from the Domain Abuse Activity Reporting (DAAR) system considers 186,550,656 resolving domain names from 1226 generic Top-Level Domains (gTLDs), in comparison to 185,550,909 domains in 1222 gTLDs reported on 28 February 2018. The reputation feeds the DAAR system employs reported at least one security threat in 414 of the 1226 gTLDs as of 31 March 2018 in comparison to 405 of the 1222 gTLDs identified on 28 February 2018. As a result, this report provides an analysis for only the 185,848,042 domains within the 414 gTLDs with at least one security threat.

Approximately 89 percent of the resolving domain names were in gTLDs launched before 2010 (referred to hereafter as "Legacy gTLDs"). Of the 1,908,923 domains identified as security threats, 934,220 or 48.94 percent were in legacy gTLDs. The other 974,703 or 51.06 percent were in the new gTLDs. In the February 2018 report, of 2,167,711 total domains identified as security threats 1,054,040 domains or 48.62 percent in legacy gTLDs and 1,113,671 domains or 51.38 percent in new gTLDs. This represents an approximate change of 0 percent in the number of security threat domains identified in legacy gTLDs.

Domains identified as security threats are not uniformly distributed across the gTLDs analyzed in this report. In the case of new gTLDs, 93 percent of the domains identified as security threats were in just 19 of those gTLDs. In the case of legacy gTLDs, 94 percent of the security threat domains were in just 4 of those gTLDs.

Preface

This monthly report to the ICANN Board of Directors highlights activities reported in the Domain Abuse Activity Reporting (DAAR) System, providing a snapshot as of 31 March 2018. The DAAR system studies domain name registration and security threat behavior across top-level domain (TLD) registries and ICANN-accredited registrars. This is a point-in-time report that includes data for all TLDs for which data was available. The report provides aggregated statistics and timeseries analysis about security threats of interest to DAAR[1] reported. In other words, this report provides analysis on domains that were identified as a security threat on 31 March 2018 only. While no single snapshot can capture trends or anomalies, historical data collected over time will show trends and can be used to identify anomalies for further study. For more information regarding data used in the DAAR monthly report check DAAR Context Document [1].

The overarching purpose of DAAR is to give the ICANN community reliable, persistent, and unbiased data using an open and community-vetted methodology that can be used to help inform policy discussions. To learn more about DAAR, visit the ICANN Domain Abuse Activity Reporting web page [2].

At this juncture, DAAR provides aggregated monthly gTLD registry reports only. Reporting about registrar portfolios requires domain name registration data to identify which domains are sponsored by which registrars. A collection system that will collect and analyze the necessary registrar data remains under development. We expect to add registrar reporting in future reports. Inclusion of country code TLD (ccTLD) registries, where the ccTLD registry information is voluntarily provided by the ccTLD administrator, is also planned for future releases.

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

1 General Trends in New and Legacy TLDs

On 31 March 2018, DAAR collected zone data for legacy and new generic top-level domains (gTLDs)[2]. The table below summarizes the data captured on 31 March 2018 and indicates the changes from the data reported for the previous month.

Table 1: Monthly snapshot comparison

	Domains for which DAAR is collecting data		**Domains for which one or more security threat incidents**	
	TLDs	Resolving domains in those gTLDs	TLDs	Resolving domains in those gTLDs
28 February 2018	1222	185,550,909	405	184,742,728
31 March 2018	1226	186,550,656	414	185,848,042
+/- changes from previous month	4	999,747	9	1,105,314

As Figure 1 displays, approximately 89 percent of gTLD domain names were registered in legacy gTLDs launched before 2010[3]. Figure 2 shows that the distribution stays more or less similar over time.

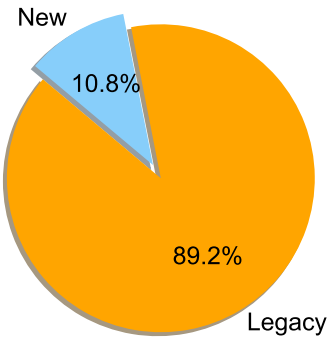


Figure 1: Distribution of resolving gTLD domains in zone files

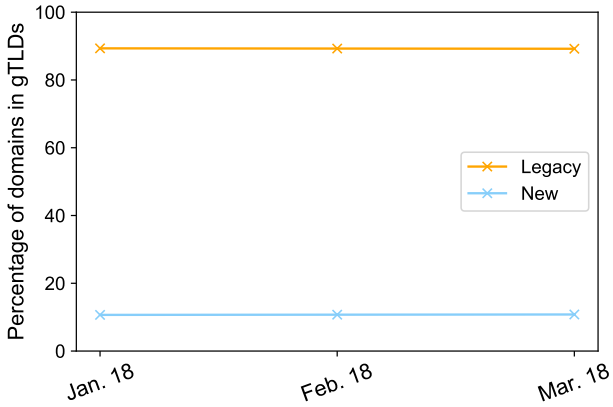


Figure 2: Distribution of resolving gTLD domains in zone files overtime

[2] While DAAR can support analysis on country code TLDs (ccTLDs), at this time, no ccTLDs are included in DAAR reports.

[3] Certain legacy TLDs – specifically INT, EDU, MIL, GOV, and ARPA – do not appear in DAAR because they are not under ICANN gTLD contract and as such, zone data from these TLDs has not been included.

1.1 Distribution of Domains Identified as Security Threats

Figure 3 illustrates the proportion of domains identified as security threats in percentages in legacy and new gTLDs. Of the 1,908,923 domains identified as security threats, 934,220 or 48 percent were in legacy gTLDs, and 974,703 or 51 percent were in the new gTLDs. Figure 4 displays this proportion overtime.

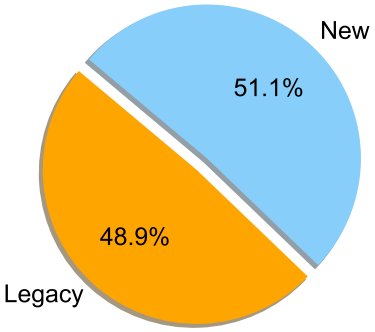


Figure 3: Distribution of domains identified as security threats

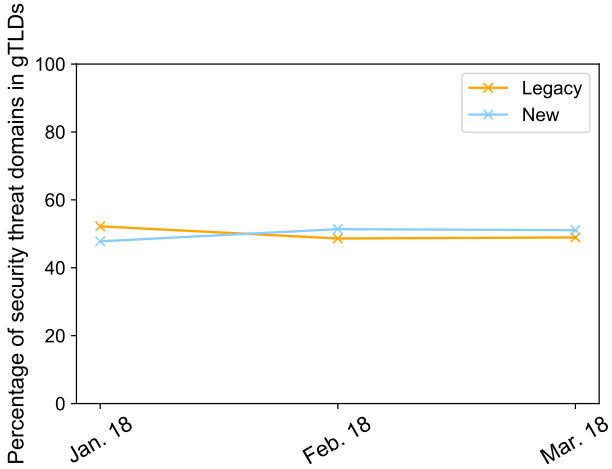
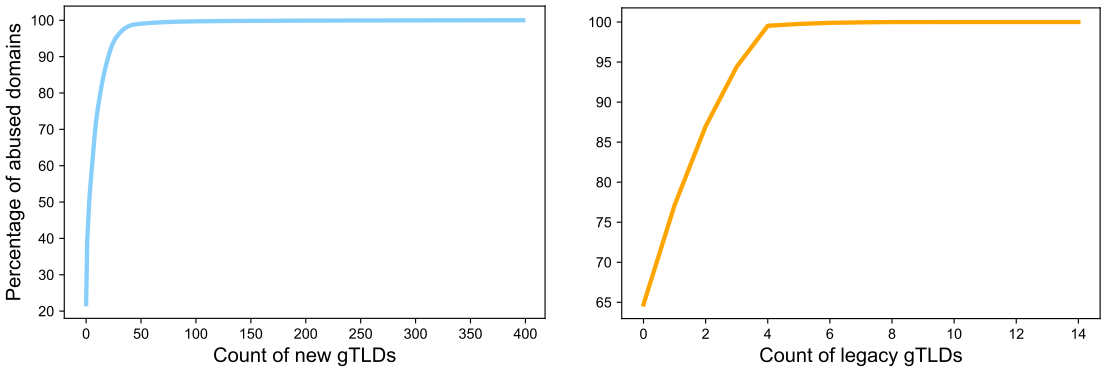


Figure 4: Distribution of domains identified as security threats over time

Domains identified as security threats in gTLDs are not uniformly distributed, either in the legacy or new gTLDs. The following graphs provide the cumulative distribution of domains reported as security threats for the legacy gTLDs and the new gTLDs respectively. Note that given the number of new gTLDs is many times larger than the legacy gTLDs, the X-axes of the two graphs are significantly different. As can be seen from Figure 5a, of the 974,703 domains identified as security threats reported in 399 new gTLDs:

- 55 percent were in the 5 most-exploited new gTLDs.
- 72 percent were in the 10 most-exploited new gTLDs.
- 93 percent were in the 25 most-exploited new gTLDs.
- 99 percent were in the 50 most-exploited new gTLDs.

For legacy gTLDs, Figure 5b displays the distribution of domains identified as security threats across legacy gTLDs. 1 legacy gTLD alone is responsible for 64 percent of domains identified as security threats and in total 4 legacy gTLDs bare more than 94 percent of all domains identified as security threats.



(a) new gTLDs (b) legacy gTLDs

Figure 5: Cumulative distribution of domains identified as security threats

Finally, the total amount of domains used for security threats is not the same over time. Figure 6 displays the total number of domains identified as security threats over time accross legacy and new gTLDs.

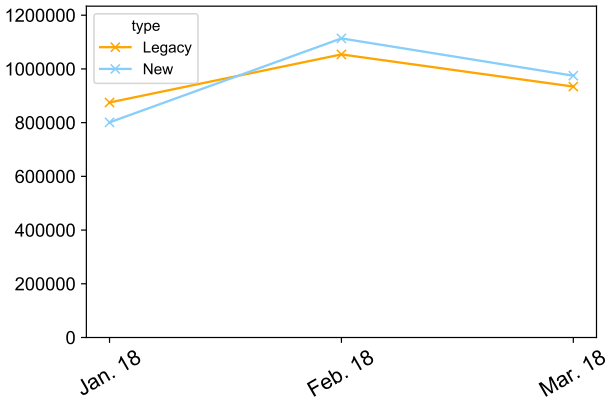


Figure 6: Total number of domains identified as security threats over time

2 Breakdown of Individual Security Threats

DAAR uses DNS Reputation Provider feeds to identify domain names reported to be associated with four kinds of security threats: phishing, malware distribution, botnet command-and-control, and spam. Figure 7 displays the breakdown of security threats from the DNS reputation data DAAR is utilizing[4].

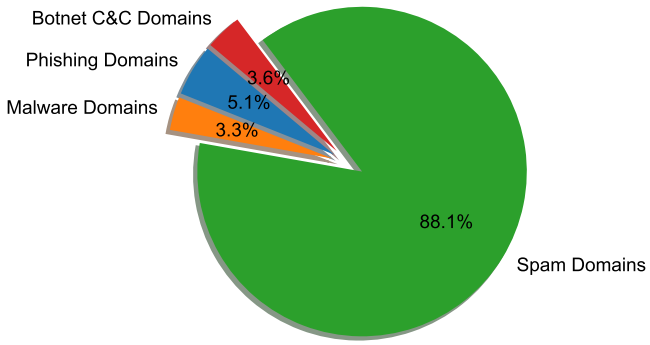


Figure 7: Breakdown of domains identified as security threats across all DAAR threat types

[4] The list of DNS Reputation Providers DAAR used for the generation of this report is included in the Appendix.

Figure 8 shows the distribution of security threats across new and legacy gTLDs for these four threat types and figure 9 captures that over time.

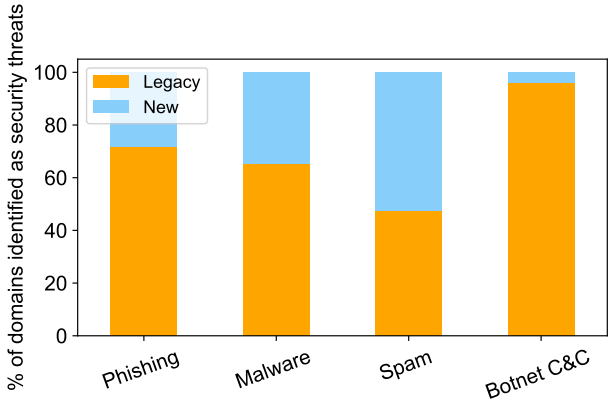


Figure 8: Proportion of domains identified as security threats within gTLD types

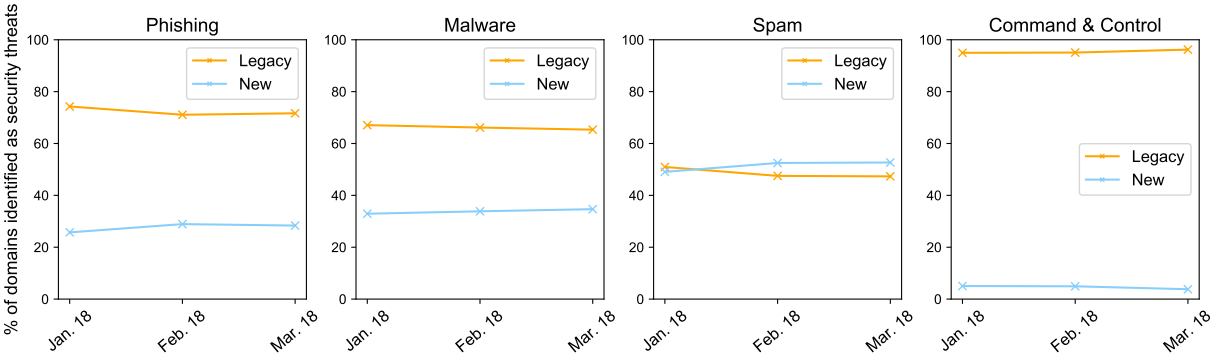


Figure 9: Proportion of domains identified as security threats within gTLD types over time

3 Normalized Metric: Percentage of Abuse

Figure 10 demonstrates the raw counts of domains identified as security threats (y-axis) versus domains resolved in gTLD zone files (x-axis). We use a logarithmic scale for the x-axis and y-axis to assist in visualizing the diverse counts of these two variables.

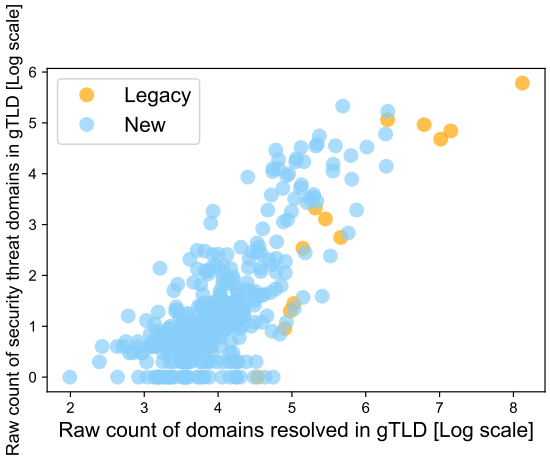


Figure 10: Raw counts of domains identified as security threat versus counts of resolved domains in gTLDs

Raw counts of domains identified as security threats do not necessarily reflect the extent to which a gTLD is the focus of exploitation by security threat actors, since each gTLD has different number of domains registered. For this reason, we calculate a normalized value, a percentage of abuse (P_{ab}). P_{ab} represents the percentage of domains that are listed for being a security threat in at least one of the DNS Reputation feeds DAAR utilizes, normalized by the amount of resolving domains within a given gTLD. For gTLDs, P_{ab} is determined as follows:

$$P_{ab} = \left(\frac{\text{Number of domains identified as security threats in TLD}}{\text{Number of resolving domains within TLD zone}}\right) \times 100$$

P_{ab} 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 gTLDs. 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.

The average P_{ab} for all 1226 gTLDs in DAAR for March 2018 is approximately 0.51 percent. Figure 11 illustrates the P_{ab} in these gTLDs. Circle size indicates the non-normalized (raw) count of domains identified as security threats.

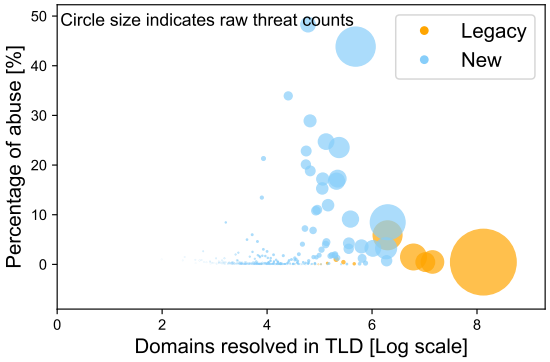


Figure 11: Percentage of abuse for domains identified as security threats vs. counts of domains resolved in gTLDs

Additionally, Figure 12 displays the average P_{ab} across different gTLD types over time.

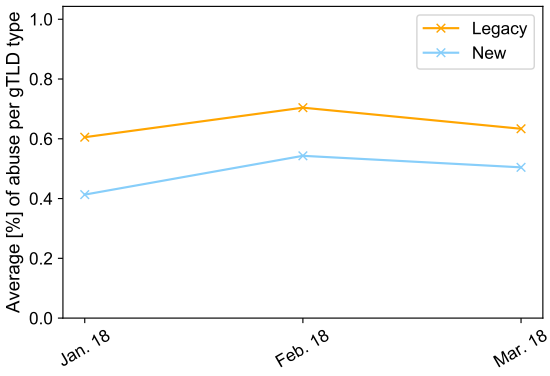


Figure 12: Percentage of abuse for different gTLD types over time

4 Percentage of Abuse: Breakdown of Individual Security Threats

Figure 13 displays Percentage of abuse 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 dots represents a gTLD provider. The bigger the size of the circle the higher the absolute count of domains identified as security threats.

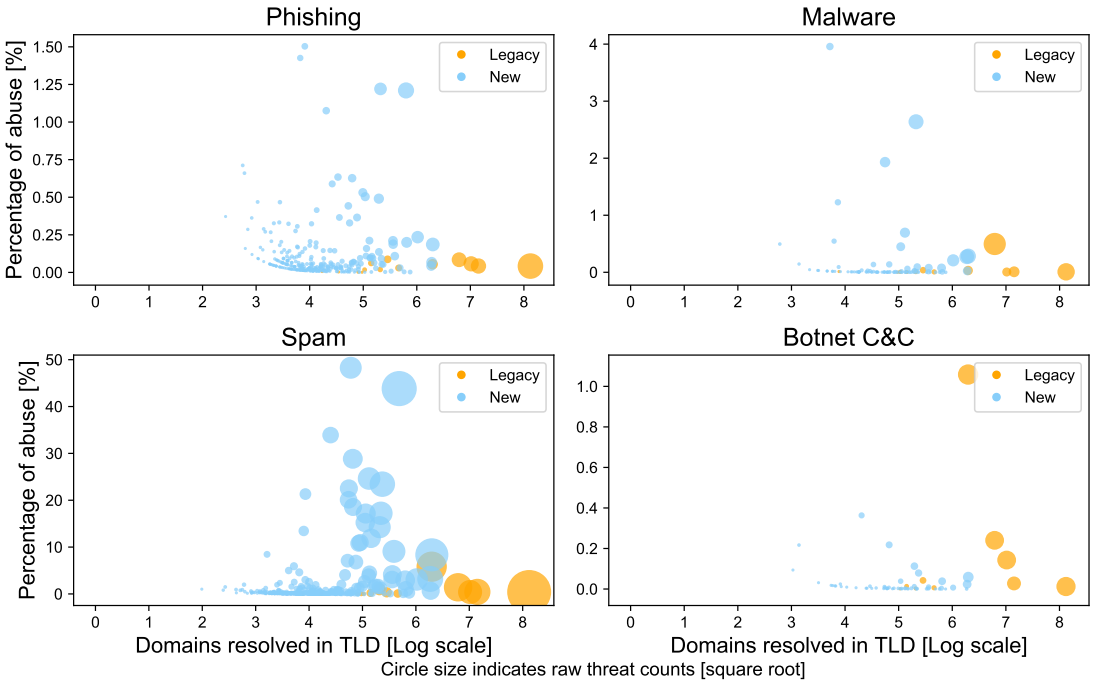


Figure 13: Percentage of abuse for domains identified as security threats vs. counts of resolved domains in gTLDs across different threat types

Finally, Figure 14 shows changes in the average percentage of abuse in legacy and new gTLDs for each security threat of interest to DAAR.

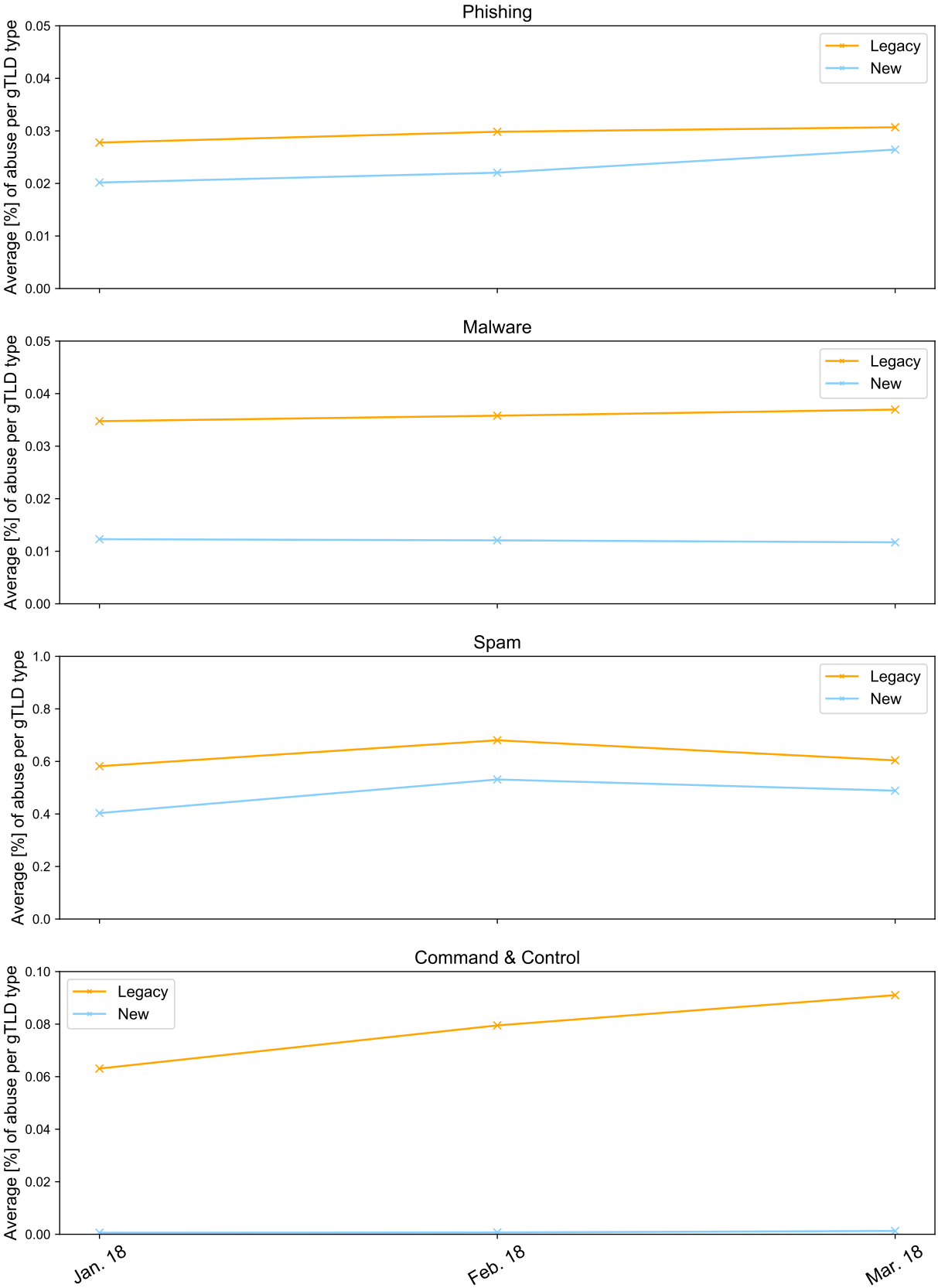


Figure 14: Average percentage of abuse in gTLDs across different threat types over time

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

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

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

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

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

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

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

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

[11] *Abuse.ch Ransomware Tracker*. https://ransomwaretracker.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 [3]	JwSpamSpy + Prolocation	Spam
	Sa-blacklist	Spam
	SpamCop	Spam
	AbuseButler	Spam
	Phishing domains	Phishing
	Malware domains	Malware
Spamhaus [4]	Domain Block List (DBL) [5]	Spam - Phishing - Malware - Botnet C&C
Anti-Phishing Working Group [6]	Phishing URLs	Phishing
PhishTank [7]	Phishing URLs	Phishing
Malware Patrol [8]	Malware URLs	Malware
	Ransomware URLs	Malware
	Botnet C&C URLs	Botnet C&C
Abuse.ch [9]	FeodoTracker [10]	Malware
	Ransomware Tracker [11]	Malware