DAAR and ITHI Data Collection

- Two primary sources:
  - Zone files from CZDS
  - Reputation data from DNS Reputation Providers
    - abuse.ch: malware
    - Anti-Phishing Working Group: phishing
    - Malware Patrol: botnet command and control, malware
    - PhishTank: phishing
    - Spamhaus: botnet command and control, malware, phishing, spam
    - SURBL: malware, phishing, spam
- DAAR reports (currently) are ”point in time” (last day of month)
- ITHI time series are monthly averages

DAAR Time Series (from https://www.icann.org/en/system/files/files/daar-monthly-report-31may20-en.pdf)

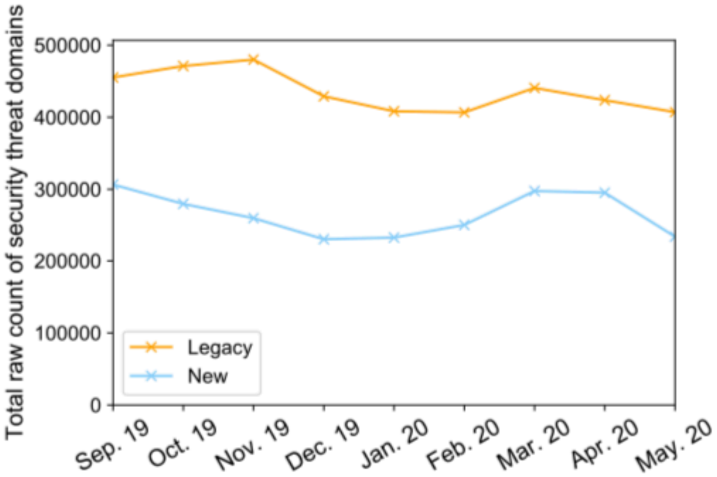


Figure 6: Total number of domains identified as security threats over time

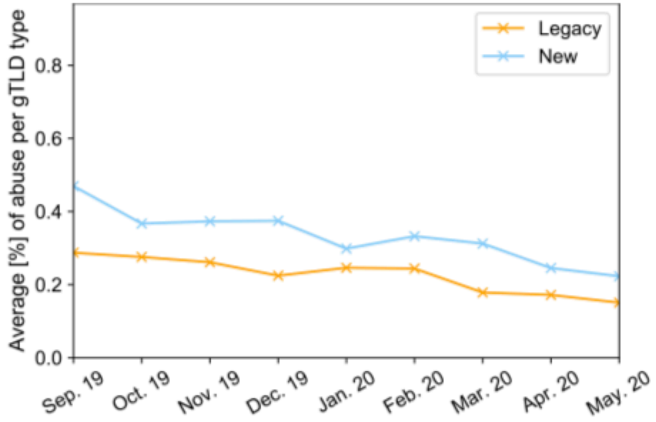
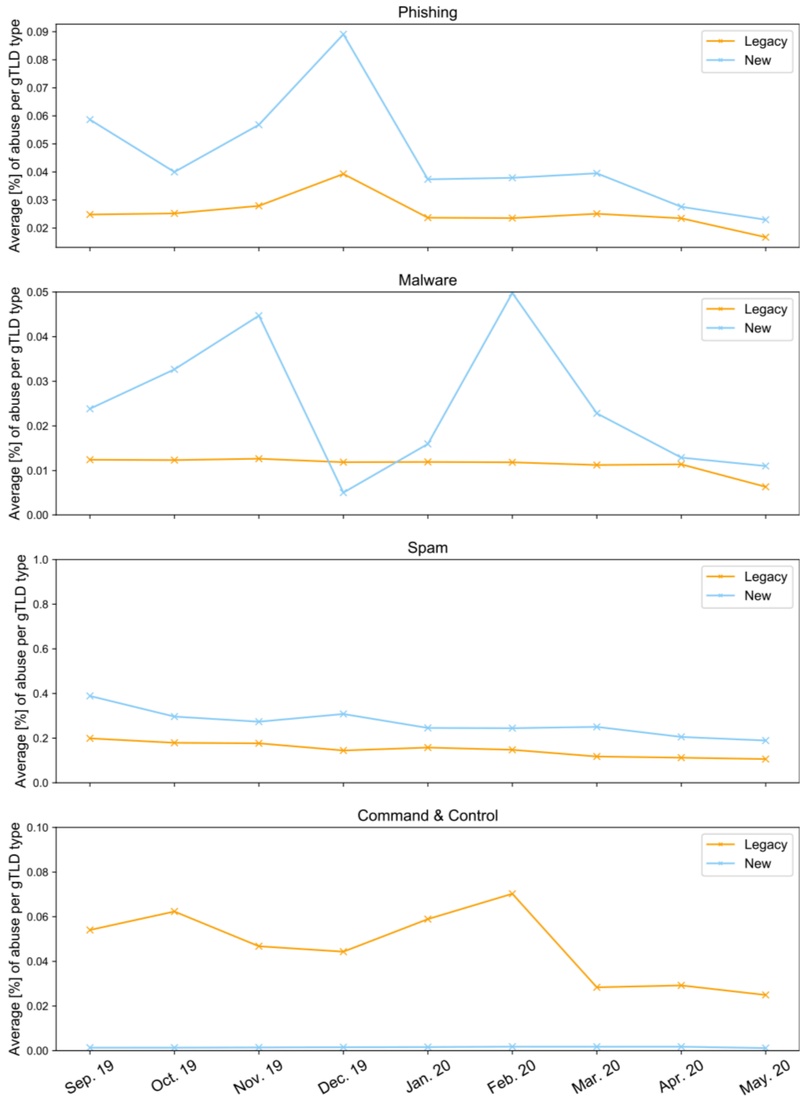


Figure 12: Percentage of abuse for different gTLD types over time



Phishing

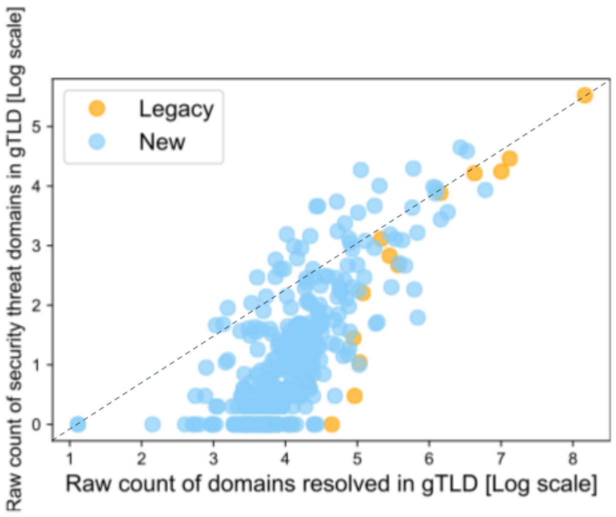
Malware

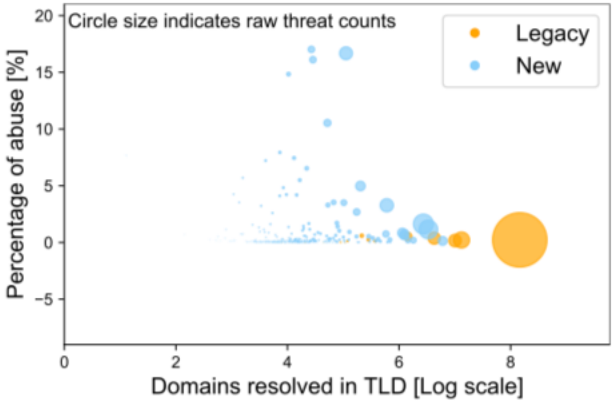
Spam

Command & Control

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

DAAR Scatter Plots (from https://www.icann.org/en/system/files/files/daar-monthly-report-31may20-en.pdf)





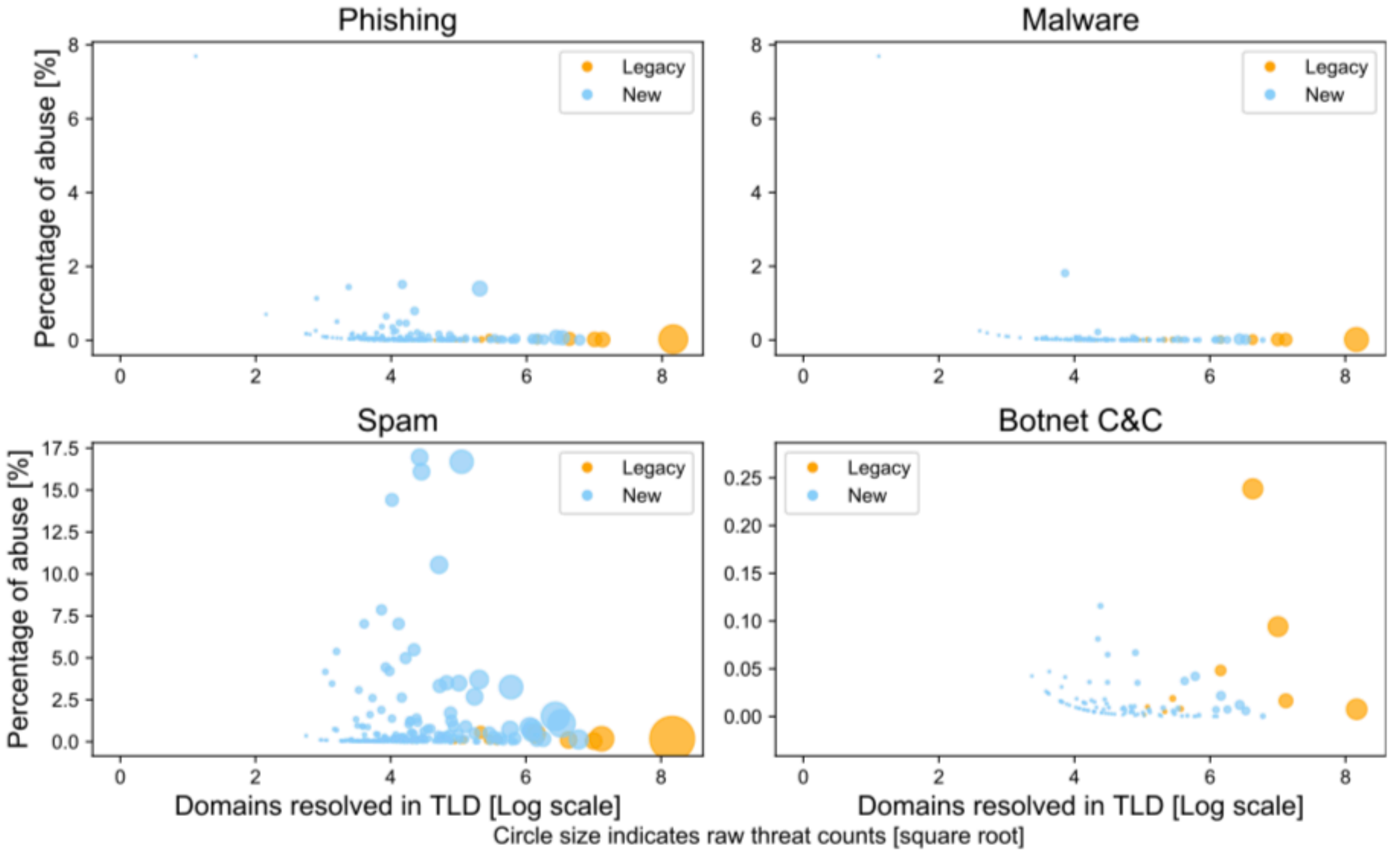


Figure 13: Percentage of abuse for domains identified as security threats vs. counts of resolved domains in gTLDs across different threat types

ITHI DNS Abuse (M2) Statistics (https://ithi.research.icann.org/graph-m2.html)

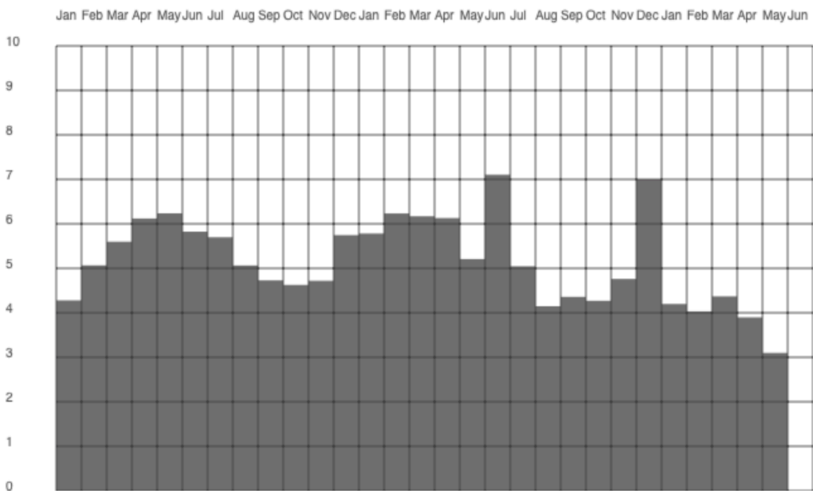
gTLD Abuse Rates	May 2020	High	3 Mo Avg	Low	TLDs accounting for 90% abuse
Phishing	0.031%	0.071%	0.041%	0.031%	7
Malware	0.013%	0.041%	0.014%	0.013%	4
Botnet	0.017%	0.040%	0.021%	0.004%	4
Spam	0.252%	1.127%	0.274%	0.243%	17

Notes:

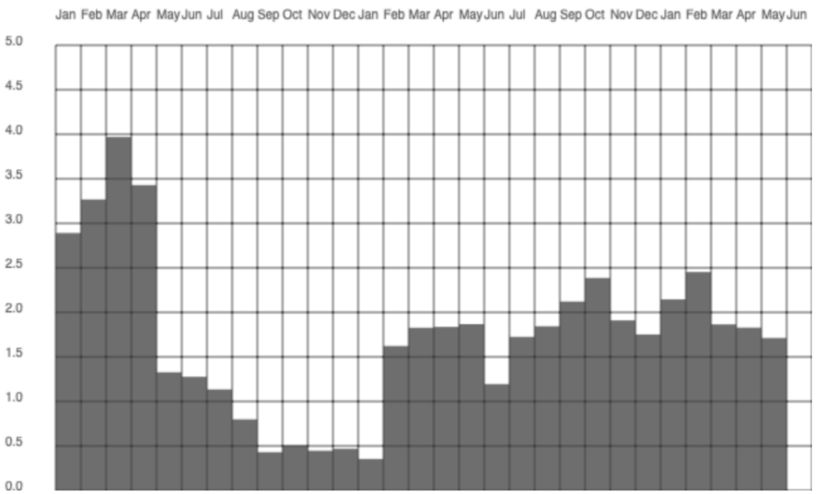
- Total across all gTLDs
- "*TLDs accounting for 90% abuse*" correlates strongly with size of gTLD

ITHI gTLD Abuse Time Series (from https://ithi.research.icann.org/graph-m2.html)

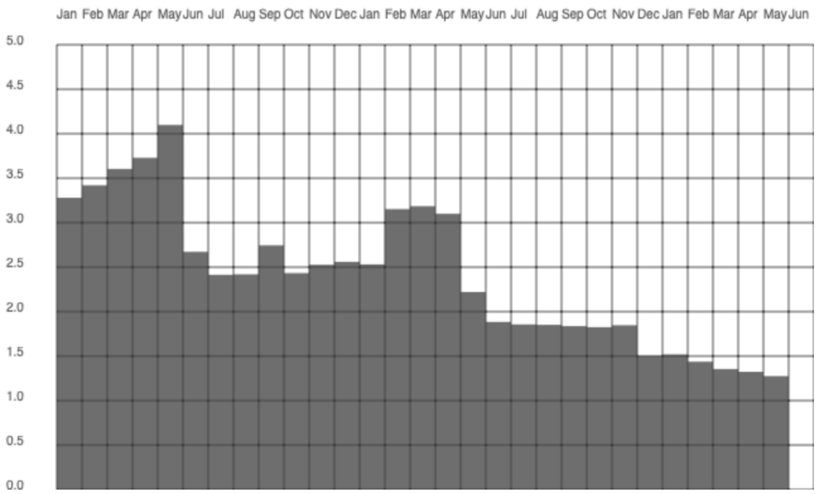
Phishing Domains per 10000



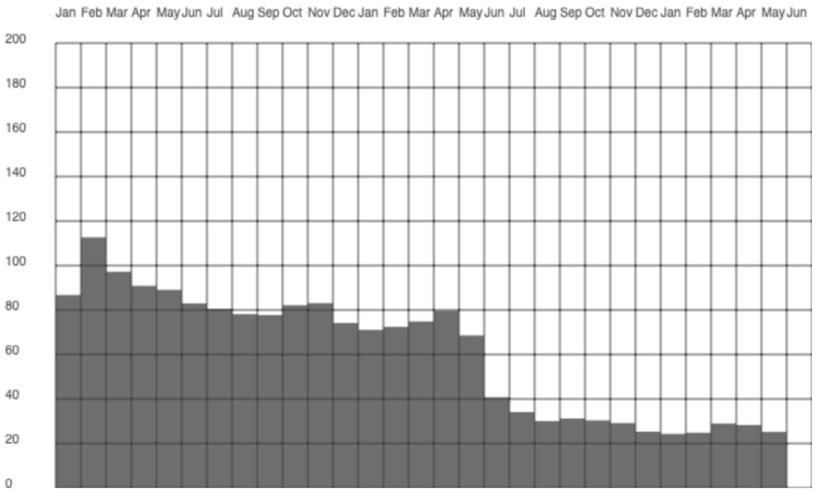
Botnet Domains per 10000



Malware Domains per 10000



Spam Domains per 10000


Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun