Understanding the Domain Abuse Activity Reporting (DAAR) Monthly Report

DAAR identifies and tracks domain names identified as threats to the security of the domain name ecosystem, known as DNS Abuse. The DAAR report is automatically generated monthly from data collected on the last day of the month. This report is intended to give the ICANN community reliable, persistent, and unbiased data using an open and community-vetted methodology that can be used to facilitate policy discussions related to mitigating DNS Abuse.

General Overview of the DAAR Data

DAAR monthly report provides insight on security threat concentrations by collecting a large body of domain name data and complements this with a large set of reputation data feeds and aggregates this to Registries or Registrars.

Data used in the DAAR system is collected and reported by the iThreat Cyber Group (ICG). The system collects three sets of data: i) Top-Level Domain Zone Data, ii) Sponsoring Registrar Registration Data, and iii) Domain Reputation Data (Security Threat or Abuse Data).

The DAAR system relies on open or commercial blocklist data to identify and classify security threats. The Domain Reputation Data used are elected to be publicly or commercially available sourced so that the reports or findings from any studies that use the DAAR system would be reproducible or independently validated by any party who collects the same data sets and applies the same processing rules to those data.

At this juncture the statistics provided in the monthly reports are aggregated to gTLD registries. 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.

How Does DAAR Compile Security Threat Data?

In its aggregated statistics, DAAR only counts unique domain names identified as threats based on blocklist data. If a domain is listed for two or more types of security threats, that domain will be counted in each relevant security threat category. However, only unique domains are counted when calculating total security threat domains in the gTLD or registrar portfolio, and for computations of percentages of security threats relative to all resolving domains in a gTLD.

What Types of Security Threats Does DAAR Collect?

Academic and operational communities refer to phishing, scamming, malware, ransomware, spam, and botnet command-and-control domains as some of the most critical type of security threats [1, 2, 3, 4, 5, 6, 9]. Of these, the DAAR system tracks phishing, malware, and botnet command-and-control domains. These threats were explicitly identified by the ICANN Government Advisory Committee (GAC) Beijing Communiqué of 11 April 2013, which led to a requirement in the new generic top-level domain (gTLD) contracts to periodically conduct a technical analysis of security threat concentrations.

DAAR also includes spam as a fourth security threat type to track and report upon. Spam has been repeatedly identified as an important source of threat for the Domain Name System (DNS) and top-level domain (TLD) operators by the ICANN GAC and the academic community [1, 2, 8, 9,10, 21]. Spam is tracked by DAAR and is treated as an indicator of security threats.

Phishing domains — Domain names that identify web pages masquerading a trustworthy entity like a bank or online merchant. Phishing is often associated with financial fraud, but it is also used to steal identities, domain registration accounts, personal email, email contact lists, and more.

Malware domains — Domain names that used to host or spread hostile or intrusive software, typically installed without the knowledge of the user[1]. Statistics associated with malware infection often include Trojan software[2], rootkits[3], ransomware[4], and their variants.

Botnet Command-and-Control domains — Domain names that are used to identify hosts controlling communications between a set of compromised machines, known as botnets[5], and the controller of those machines. Botnets are frequently used in denial of service attacks, transmitting spam, and other attacks where a large number of clients are needed to effectively perpetrate the attack.

[1] AV-Test Institute claims to register 390,000 new malicious programs every day and publishes charts that illustrate total malware over time.

[2] https://www.kaspersky.com/resource-center/threats/trojans

[3] https://securingtomorrow.mcafee.com/consumer/identity-protection/what-is-rootkit/

[4] https://www.trendmicro.com/vinfo/us/security/definition/RANSOMWARE

[5] https://www.cs.ucsb.edu/~vigna/publications/2009_stone-gross_cova_cavallaro_gilbert_szydlowski_kemmerer_kruegel_vigna_Torpig.pdf

Spam domains — Domains used to support a spam delivery infrastructure for the distribution of other security threats such as malware and phishing pages[6]. Spam domains are primarily extracted from Universal Resource Identifiers (URIs) found in email message bodies or attachments (for example, in Adobe Portable Document Format (PDF) or Microsoft Office documents) to identify harmful or fraudulent sites or content. In cases where it is possible to determine that the sender domain in an email message is malicious, those domain names are counted as spam domains as well. Blocklist operators may also include domain names that are extracted from uniform resource locators (URLs) in text, SMS (cellular carrier text message submissions), comment, or other forms of messaging spam. Note that the DAAR system counts only spam domains, not spam messages.

The security threat data DAAR uses meet several criteria: accuracy, coverage, industry adoption, and the feed's ability to classify events into the types of security threats that DAAR tracks. Below is a comprehensive list of blocklist feeds used in the DAAR system:

Reputation provider	Feed used	Threat type
SURBL [12]	JwSpamSpy + Prolocation Sa-blacklist SpamCop AbuseButler Phishing domains Malware domains	Spam Spam Spam Spam Phishing Malware
Spamhaus [13]	Domain Block List (DBL) [14]	Spam - Phishing - Malware - Botnet C&C
Anti-Phishing Working Group [15]	Phishing URLs	Phishing
PhishTank [16]	Phishing URLs	Phishing
Malware Patrol [17]	Malware URLs Ransomware URLs Botnet C&C URLs	Malware Malware Botnet C&C
Abuse.ch [18]	FeodoTracker [19] Ransomware Tracker [20]	Malware Malware

[6] https://www.cyberoam.com/downloads/ThreatReports/CyberoamCYRENInternetThreats2014April.pdf

References

1) Korczy'ski, M., Wullink, M., Tajalizadehkhoob, S., Moura, G. C., & Hesselman, C. (2017). *Statistical Analysis of DNS Abuse in gTLDs Final Report*. Technical Report. https://www. icann. org/en/system/files/files/sadag-final-09aug17-en. pdf.
2) Korczynski, M., Tajalizadehkhoob, S., Noroozian, A., Wullink, M., Hesselman, C., & van Eeten, M. (2017, April). Reputation metrics design to improve intermediary incentives for security of tlds. In *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on* (pp. 579-594). IEEE.
3) Stone-Gross, Brett, Thorsten Holz, Gianluca Stringhini, and Giovanni Vigna. "The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns." *LEET* 11 (2011): 4-4.
4) Levchenko, Kirill, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Márk Félegyházi, Chris Grier, Tristan Halvorson et al. "Click trajectories: End-to-end analysis of the spam value chain." In *2011 ieee symposium on security and privacy*, pp. 431-446. IEEE, 2011.
5) Szurdi, J. and Christin, N., Domain Registration Policy Strategies and the Fight against Online Crime.
6) Oprea, Alina, Zhou Li, Robin Norris, and Kevin Bowers. "MADE: Security Analytics for Enterprise Threat Detection." In *Proceedings of the 34th Annual Computer Security Applications Conference*, pp. 124-136. ACM, 2018.
7) Europol. “Avalanche Network Dismantled in International Cyber Operation”. [Online]. Available:https://www.europol.europa.eu/newsroom/news/‘avalanche’-network-dismantled-in-international-cyber-operation, Jan. 2019
8) ICANN Governmental Advisory Committee (GAC). "GAC Communiqué – Hyderabad, India”. [Online]. Available: https://www.icann.org/en/system/files/correspondence/gac-to-icann-08nov16-en.pdf, Jan. 2019
9) M3AAWG. “M3AAWG anti-abuse best common prac- tices for hosting and cloud service providers”. [Online]. Available: https://www.m3aawg.org/sites/maawg/files/news/M3AAWG Hosting Abuse BCPs- 2015- 03.pdf, Jan. 2019
10) Liu, He, Kirill Levchenko, Márk Félegyházi, Christian Kreibich, Gregor Maier, Geoffrey M. Voelker, and Stefan Savage. "On the Effects of Registrar-level Intervention." In *LEET*. 2011.
11) *ICANN Domain Abuse Activity Reporting*. https://www.icann.org/octo-ssr/daar. Jan. 2019.
12) *SURBL*. http://www.surbl.org/lists. Jan. 2019.
13) *Spamhaus*. https://www.spamhaus.org. Jan. 2019.
14) *Spamhaus Domain Block List (DBL)*. https://www . spamhaus . org / faq / section / Spamhaus%20DBL#291. Jan. 2019.
15) *Anti-Phishing Working Group (APWG)*. https://www.apwg.org. Jan. 2019.
16) *PhishTank*. https://www.phishtank.com. Jan. 2019.
17) *Malware Patrol*. https : / / www . malwarepatrol . net / enterprise-threat-data/. Jan. 2019.
18) *Abuse.ch*. https://abuse.ch. Jan. 2019.
19) *Abuse.ch Feodo Tracker*. https://feodotracker.abuse.ch. Jan. 2019.
20) *Abuse.ch Ransomware Tracker*. https://ransomwaretracker.abuse.ch. Dec. 2019.
21) Brian Krebs. 2019. “*Bomb Threat, Sextortion Spammers Abused Weakness at GoDaddy.com*”. [Online]. Available: https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com/