Derek Smythe

This response is firstly to thank the originators and folks who worked on the DAAR concept for this attempt at putting something long overdue on the table.

Secondly this response would like to make some comments believed to be in line with the project and also a suggestion that Advance Fee Fraud (AFF) data should be considered as relevant to this project. Understanding the argument of such inclusion leads to constructively commenting in a realistic fashion on the attempted outcomes of DAAR.

For the sake of definition, Advance Fee Fraud (AFF) in this context is meant as the requirement for a consumer to pay for a service or item that does not exist, whereby the consumer becomes the victim to fraud. This fee can be direct such as paying for an item at a fake online store, or indirect where an online presence is abused as a prop to confuse and deceive a consumer into believing a linked related part of the fraud is real. Such may be a fake United Nations, Interpol, FBI or like impersonation. Yet it may equally be more subtle such as a fake business with a fictitious director or staff member as is used in Romance Scams. The fraud is illegal in every country and we find alerts and arrests reports on a regular basis. AFF relies massively on domain based abuse to succeed and businesses models exist to facilitate this fraud, sometimes even forming part of larger organized crime such as narcotics trafficking, grand theft, money laundering and other human rights abuses. It is also a precursor to BEC. Not many in depth studies have been done into this issue, although some do exist from varied points of view, yet reaching the same conclusion:
https://www.agari.com/wp-content/uploads/2018/05/Behind-the-from-lines-Agari-Whitepaper.pdf [agari.com]
https://www.crowdstrike.com/wp-content/brochures/reports/NigerianReport.pdf [crowdstrike.com]
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/unit42-silverterrier-rise-of-nigerian-business-email-compromise [paloaltonetworks.com]

It's only with an understanding of the underlying AFF mechanisms that one is able to fully appreciate the roles domains play in this ever growing threat to consumers. More to the point, most malware vendors do not block these domains, nor do mail filtering system cater for this abuse - unless by accident. In turn the non-recognition of the underlying threat value leads to this part of domain abuse also featuring in UDRP decisions as "phishing" and also the basis for such decisions being in favor of brand owners, a case of the correct result for the wrong reasons. Yet this approach disavows the greater reality that many banks spoofs are not phishing, nor does it explain why a bank may be spoofed with a domain similar to the real bank's domain name, but the online content not matching the real bank's content, nor why totally fake banks exist. In these the user is not asked for credentials as mentioned, rather the user is given credentials. This opens a Pandora's box for many researchers where they rather choose to close the door. The phishing classification also does not fit the common job scam or mule scam, where a company is spoofed and jobs offered as being that company. We sometimes find *fantasy* descriptions of the fraud with no connection as to how the actual fraud plays out, affecting different consumers as a target group than believed. This mis-identification has led to the rights of consumers being missed out in many negotiations and policy discussions, leaving vast areas of domain abuse not described, also as such not recognized. In turn this leads to alerts such as those of the FDA, DEA about extortion by parties spoofing them. We see similar alerts from the likes of the US Better Business Bureau; Pet Scams, Vehicle Escrow Scams etc. Domain registration abuse is systematic and growing in AFF. It's not uncommon to find a 100 or 200, even more, domains linked to a single facilitator hiding in plain sight. With a bit of historic data, that abuse can easily be linked to over a 1000 domains! This nefarious usage is by parties well versed in domain abuse and methods to ensure the longevity of such abusive domains. Some even infiltrate the domain reseller channel. This issue is not merely a content issue, the fraud may rely on sub-domains to hide, or are only used for email abuse. Some of these domains are even sometimes re-purposed for BEC or phishing attacks. The simple fact is many purely consumer facing threats are hardly recognized at registrar, registry or ICANN level. In turn law enforcement is left to mitigate as a best effort basis with little to no real consumer protection.

In line with the above, comments are made regarding the DAAR system where certain pertinent issues are pointed out.

ICANN org's DAAR methodology paper

> DAAR does not attempt to measure mitigation activity, i.e. it is not intended to measure how various parties (including registries and registrars) respond to abuse activity.

This is a pity. However we understand why this is extremely complex, encountering some of the obstacles ourselves. aa419 attempts to monitor malicious domains checking statuses at least once per week. Registry rate limiting and count blocking frustrates such attempts to a degree, especially where a registry or registrar has allowed an inordinate number of malicious domains into a registry, typically after a discounted domain price sale. The effect of such processing is felt for quite a while. Yet even so, such a full domain life cycle study does yield interesting results such as UDRP transfers and secondary abuse cropping up from time to time in the domain resales market. Domain transfers between registrars also shows where malicious actors feel safe. As such, even if only weekly or monthly, such mitigation monitoring should be attempted if it does not undermine other efforts. The inability to mitigate abuse led to the concept of "abuse days" at aa419. Many registrars and registries desire reports of fraudulent domains they sponsor, while others discourage such reporting. In the AFF field fake registration details abound and it's only in hindsight that many malicious domains can be identified. Yet even so, enough data exists to proactively flag and block many new registrations before they become a consumer threat. Our own records also led to the discovery that certain domain names are continuously registered by the same parties as they already have the matching content for the matching domain name. We also noticed registrar shifts by some malicious actors to registrars where they are tolerated.

> As part of this project, we have encountered Whois rate limiting by some registries. Rate limiting sometimes makes gathering the data very difficult. It impedes our ability to keep up with daily changes to some zone files aa419 also encounters this problem. More to the point, it appears that at least one registry operator also operating a ccTLD where they allowed much abuse into the system, counts queries against this one ccTLD and in a total rate limiting count across all registries where they manage ccTLDs and gTLDS. This has contractual implications and may be a point of failure recording in itself. While rate limiting and blocking is appropriate to protect against the harvesting of registrant details, the thick registry structure does not allow only status and date selection.

> Individual measures of the number of abuse domains that have been classified as phishing, botnet command and control (C&C), malware, and spam domains, using the reputation data feeds that the DAAR system employs (per registry, registrar), see the section entitled Security Threats observed by the DAAR System.

and

> Phishing domains – Domain names that support web pages that masquerade as a trustworthy entity such as a bank or online merchant. Phishing is often associated with financial fraud but is also used to steal identities, domain registration accounts, personal email or email contact lists, and more.

and

> A domain name that we extract from any reputation data list will cause the domain name to be counted once as an abuse domain when we calculate unique abuse totals14. If a domain is listed for two or more types of abuse, that domain will be counted (again, once) in each relevant abuse category.

There be dragons here. Many AFF domains such as spoofs are inadvertently listed as phishing (and mitigated as such using incorrect methods).

> The article, Reputation Block Lists: Protecting Users Everywhere, describes the many adoptions and application of RBLs that make this security service arguably ubiquitous.

Caution: Some registrars use these mechanisms on their ICANN mandated abuse email addresses. This sometimes leads to the perverse effect that they cannot receive abuse reports on domains they are sponsoring.

> For these reasons, the statistics the DAAR system reports should be considered as a subset of the abuse problem in a given gTLD, or in the gTLD portfolio of a given registrar.

It is our opinion that AFF should be considered as an additional category as the existing categories does not reflect the real consumer threat landscape. It's not uncommon, upon comparing notes with other parties to identify recurring areas of concern, but then notably areas where different operator at various levels appear based upon the type of abuse and the operator's recognition of such abuse.

> Investigative reports. Compliance, GDD, or OCTO SSR could initiate a report when, for example, those departments become aware of extraordinary security threat activity. Such reports could be presented to an identified registry or registrar operator for compliance action or a cooperative abuse investigation with affected parties.

This is particularly true in the AFF arena. The US BBB did such an international study on an issue in our arena and found one registrar cropping up continuously during their study. Their results also confirmed our results and fraud reports.

> The most commonly used and effective way to identify spam messages is to collect email messages at mail user accounts that are intentionally created to capture unsolicited email (spam). These accounts are called spam traps.

This is a proven technique, also used in the anti-AFF arena. The anti-AFF implementation is somewhat more complex and intensive called baiting. While certain communities engage in this activity for other reasons, ethical baiting is done in such a manner as to glean information that can be used to the detriment of the AFF actors. While the initial spam email will be sent via a free disposable email address, interacting with the sender leads to the malicious sender passing what he believes to be a victim up the chain of command to parties in the AFF syndicate who disclose the malicious domains in either fraudulent emails or URLs for fake and fraudulent online presences. Other information also simultaneously obtained is fed to the authorities and like. This sometimes leads to the uncovering of money laundering operations.

Recommendations:

Artists Against 419 (aa419) records domain based abuse in a ring-fenced set of AFF circumstances, where such a domain has no legitimate purpose and is registered for nefarious usage (not hacked/hijacked), capturing evidence and with an appropriate data feed mechanism. Entries are manually verified as to make sense from the noise and madness that is consumer information. Such noise may be consumer reports by victims of AFF, where details on the incident are analyzed as consumers are not generally technical, or spam leading to baiting exercises. In turn this leads to research using DNS identifiers, online content and known past usage patterns. Only 100% confidence entries are entered. Getting it wrong and listing a legitimate business may destroy such a business, causing as much harm as fraud could and does. Even now again a reseller with ~250 domains and only three *potentially* legitimate domains is being escalated to the upstream registrar based upon a single fake bank being reported. This case illustrates tracking at all these levels to ensure a reliable result. Additional similar complaints led to ICANN Compliance complaints. In a recent escalation, Mr Marby was also asked to please consider making AFF a study subject for ICANN SSAC, as domain abuse is extremely pervasive in this arena.

Single digit annual fake positives is testimony to accuracy of our findings. Some registrars and registries use our data either proactively or requests listings from us. We offer access to our feed to the DAAR project for free as an unique set of data reflecting consumer threats that has overlapping interest with commercial/government interests in some cases, while representing other areas not even recognized, yet equally illegally used internationally. Some of this may be intuitive like fake currency being offered for sale yet never appearing on a blacklist outside aa419. The data will show the reason for Romance Scam fraud and associated threats being at an all time highest as published by the authorities. Historical data will also show UDRPs and the issues described earlier:
https://db.aa419.org/fakebankslist.php?cmd=ADV&x_PublicComments=UDRP [db.aa419.org]

The correctness of our data can easily be measured since we record all attributes of our listings. Further we apply a life cycle management system to each entry, with each change leading to an updated timestamp. Changes can also be tracked all the way to expiration of each entry as to reduce the active data set. The goal is to create a dataset easy to use and that can be found by the common user as to protect himself, while retaining other elements not commonly visible like automated snapshots with embedded metadata and tracking information. The data is also linked to other sources and from such sources where users can identify the fraud targeting them, obtain a better understanding and ask for assistance.

Artists Against 419 is open to sharing this data freely and does. Artists Against 419 is also willing to provide training and advice to any serious player in the AFF field in methods of detection, tracking and mitigation.
It needs to be stated clearly that this is not a commercial proposal, rather an altruistic attempt at addressing a problem long since outstanding and being done with no hidden motives other than to protect ordinary innocent consumers.

We trust this offer meets your consideration as a method to measure AFF in the domain name system.

Thank you.