Leveraging DNS to Help Counter DDoS, Malware, Phishing, Spam, and Other Attacks
Coordinating Attack Response at Internet Scale (CARIS) Workshop, Berlin, June 19th, 2015
Merike Kaeo, Farsight Security, Inc.

I. Introduction
Because virtually everything that occurs on the Internet begins with a DNS lookup, DNS traffic from instrumented name server infrastructure can provide useful insights, both with respect to normal Internet usage and Internet attacks.

Farsight Security, Inc. (FSI), works extensively with DNS traffic, among other types of Internet data. FSI routinely collects cache-miss DNS traffic from a network of over 450 sensors located above recursive resolvers running on partner network sites worldwide.[1] FSI re-shares that passive DNS data with its customers via the Security Information Exchange (SIE)[2] and DNSDB.[3] Although Farsight Security is a for-profit company and finances its operations through subscription fees, we are also committed to supporting law enforcement agents, academic researchers, and non-profit organizations with full or partial grants of FSI's services.

There are many valuable insights that can be shared with CARIS participants based on Farsight's experiences with passive DNS, and based on our experience sharing information via SIE

II. "You Can Observe A Lot By Just Watching" (Yogi Berra – American Baseball Player)
Many Internet attacks can be easily identified -- and effectively worked -- as a result of data obtained from watching DNS traffic. For example:

1. Many spammers attempt to avoid notoriety by using a large number of unique domain names during the course of a single spam run. By doing so, they avoid potential operational single points of failure, and no single web site will show up too-often in any summary roll-up of the top spamvertised domain names. (This is the same reason why a given spammer may employ multiple store front "brands" for their consumer websites.)

Passive DNS can help investigators overcome spammer attempts at operational persistence and obfuscation by identifying common underlying infrastructure linking all the spamvertised domains. For instance, perhaps:

-- all the spamvertised domains share the same set of *name servers*, or
-- all the spamvertised domains share the same *name server IP addresses*, or
-- all the spamvertised domain names are *hosted on the same IP addresses*.

Having started with one spamvertised domain as a "loose thread," passive DNS allows an investigator to find a larger set of associated domains and IP, and by pivoting and iterating, it is often possible to enumerate a spammer's entire network, even if that includes thousands or more unique base domain names.

Being able to use passive DNS to identify latent infrastructural relationships makes it far harder for major spammers to successfully "fly under the radar," avoid official investigative attention, and stay in operation.
2. Because blocklists and domain reputation systems quickly and routinely list domains associated with spam, phishing, malware, and other abuse, it has become routine for *attackers* to create, abuse, and then quickly abandon a steady stream of brand new domains.

---

[1] That data is intentionally collected solely from sensors running above recursive resolvers to ensure that individual DNS queries cannot be directly associated with any specific individual.
[2] https://www.farsightsecurity.com/Services/SIE/
[3] https://www.farsightsecurity.com/Services/DNSDB/

Of course, this easily-identified behavior also makes it easy for *defenders* to focus on those **Newly Observed Domains**,[4] perhaps temporarily blocking access to *all* newly observed domains for a matter of minutes or hours until blocklists and domain reputation systems have had a chance to take a look and render an opinion. Because virtually no legitimate site requires users to access new domains mere minutes or hours after that domain has come up, briefly blocking brand new domains provides a virtually collateral-damage-free approach to protecting users from hit-and-run-based malware and phishing attacks.

3. A third example of an Internet attack that can easily be identified when DNS is well-instrumented would be **DNS-focused denial of service attacks**,[5] particularly randomized-subdomain attacks. Randomized-subdomain attacks require us to do something a bit unusual, and turn our attention from domains that *successfully* resolve to all the unique FQDN domains that *do not* resolve.

There are just a few of many other examples of how DNS traffic data can be used to counter routinely seen attacks -- *IF these techniques are broadly shared and their use is institutionalized by practitioners.*

III. "I'd Like To Teach The World To Sing" (lyric from a popular Summer 1971 commercial for Coca-Cola)
While passive DNS is a generally straight-forward tool to use, there are still some generalizable challenges that are worth explicitly noting and tackling:

1. Training: At least some investigators may still not be familiar with DNS-based investigative approaches. If investigators haven't been exposed to the power of DNS-based approaches, they won't use them in their daily work. Additional awareness/training/education outreach effort is needed. If you're an experienced and DNS-focused person, it is easy to assume that everyone else is too, but, in reality, many security practitioners may lack even introductory-level exposure to DNS concepts and architectures. We neglect the importance of training at our peril when it comes to empowering investigators with new tools.

2. Sensor Coverage (Particularly in the Southern Hemisphere): The power of any data-driven approach is a function of the data that's been collected. We don't discuss the specifics of who does and doesn't operate sensors and contribute data,[6] but like most data-driven security companies, Farsight's sensor coverage is particularly strong in North America, Europe, and Asia. We also have sensor nodes in the Southern Hemisphere, but we're continually seeking to expand our sensor coverage, particularly there in that part of the world. We believe Southern Hemisphere networks are a very important part of the Internet and we'd like to ensure that cyber criminals don't inadvertently have a haven from which they can hide and commit cybercrime. We welcome discussions with anyone who'd like to contribute data, regardless of your location. Please see the referenced blog article for more information.

3. Moving From Retrospective Use of Passive DNS to Real-Time Stream Cyber Security: We also need to help users move from a retrospective/historical perspective (e.g., use of DNSDB for incident response) to a real-time/forward-looking perspective (e.g., processing real-time DNS telemetry directly from live SIE broadcast channels. By analogy, many analysts are spending far too much time looking in the rear-view mirror, and not nearly enough time looking through the windshield at what's coming at them now/next. This is a critical approach to security that needs to get fixed.

---

[4] https://www.farsightsecurityces/NOD/
[5] Renuka Nadkarni, "DNS-based DDoS Attacks - What's In A Name?", https://community.infoblox.com/blogs/2014/10/02/dns-based-ddos-attacks-what%E2%80%99s-name
[6] See the discussion in https://www.farsightsecurity.com/Blog/20150304-stsauver-dnsdbsensor/