Crawl/Walk/Run

Introduction to DNSDB®

Part 1: Crawl - Advancing your threat intelligence and navigating possible roadblocks when using DNS in investigations
Learn from Farsight Security CEO Dr. Paul Vixie, as he teaches the fundamental investigative techniques and methodologies of how to use DNSDB to combat common cyberattacks. Starting with a single IOC (indicator of compromise), Dr. Vixie will guide us on how to pivot through domain infrastructure to build intelligence of associated malicious activity.

Summary

Goal: Given a starting “clue,” we will work on enriching the clue and finding others related to uncover what the bad guys did and seek recourse.

Starting with a Spam Sample

Redirection

Farsight Security’s DNSDB Passive DNS

Using DNSDB: Starting “Clue”

Checking Whois

Using DNSDB: Associated Domains

Using DNSDB: Associated IPs

Resources
Summary

- You’ll walk through a series of “pivots,” going from an initial clue domain to an IP to an encompassing netblock to new domains.

- You’ll see what’s possible without passive DNS and how passive DNS can enable you to broaden a single specific clue into a broad and more encompassing dragnet.

- This process of finding related domains with passive DNS is critical to ensuring that you don’t end up playing “whack a mole,” taking down just a single domain at a time when a given abuser might have hundred or even thousands.

Goal: Given a starting “clue,” we will work on enriching the clue and finding others related to uncover what the bad guys did and seek recourse.

In this example, let’s say our clue is a domain name.

Traditionally, we rely on the DNS to map domain names to IP addresses and vice versa. While we still do that, the DNS is a 30-year-old system today with a lot of other things in it. Starting here will reveal a lot more than an IP address. We can also look for:

- Is this a brand new domain or has it been around for a long time?
- Is the domain on the same IP as it has always used or has it been hopping from one IP to another?
- Is it the only domain on the IP or is it sharing that IP with a bunch of other domains?
  - If there are many domains on that IP, are they thematically related?
- Are there other suspicious domains in the same network neighborhood?
- Can we find related domains by looking at shared resources the domain name uses?

Starting with a Spam Sample

Our real-life spam sample comes from http://untroubled.org/spam/2020-04.7z

Looking at an email header, we see a spamvertised host www.sonicbook[dot]icu. This URL is not accessible directly. It first lands on offerhub[dot]buzz. Why is there a redirection page? The page serves several important purposes:

- Affiliate attribution tracking
- Interfering with automated page crawlers
- Decoupling the spamvertised page from the ultimate page displayed to the user
- Where the page sends us depends in part on where we came from
Using Whois, we learn that offerhub[dot]buzz is hosted through Cloudflare.

With the help of Dr. Nicole Apelian, I finally gathered all the remedies and medicinal plants of North America and included them in one book:
http://www.sonicbook.icu/i/1t9Gc47950W124UF/1b12P9i13V3203NI108IT193991220M2905379929
The most powerful remedies growing in your state

Redirection

Back to the offerhub[dot]buzz—the interstitial site takes us to “Discover The Forgotten Power of Plants with Nicole Apelian” at lostbookofremedies[dot]com.
Again using Whois, we learn that lostbookofremedies.com is also hosted via Cloudflare.

We also learn that there is an association with ClickBank, thanks to a logo appearance on the lostbookofremedies website.

On the ClickBank site, we find an affiliate page that mentions the book offer. This does not give us another lead.
Back to the lostbookofremedies website, we see that the “Contact” link points users to askaprepper.com.

On askaprepper[dot]com, we find they are advertising *The Lost Book of Remedies* book.
Farsight Security’s DNSDB Passive DNS

Let’s try investigating with DNSDB Scout, a GUI for the DNSDB API. DNSDB is a passive DNS historical database that provides a unique, fact-based, multifaceted view of the configuration of the global Internet infrastructure.

Using DNSDB: Starting “Clue”

Let’s start with our original spamvertised domain.

Using Whois, let’s check if we can find anything for the IP address 172[dot]245.173.132. We find a range of IP addresses, a street address, and an organization name.
We go back to scout with the IP address to see if there are other suspicious domains on the same IP, and there are a lot. Most of them have been created a while ago but used recently and the names are typically “spammy.”

Because some of these domains are .us, we can find more valuable information from Whois. A search reveals a name, address, and phone number.
Checking the USPS site, we can verify that the address is invalid.

Whois is required to be correct. Because this point of contact information is invalid, we could file a complaint to get the domain corrected or torn down. Unfortunately, the domain is only a $1.47 investment, and the abuser has plenty of others.

Using DNSDB: Associated IPs

Recall the handoff IP from the beginning. Through Whois, we find another address which is a mail forwarding service.
Through ARIN, we can look up information about this particular point of contact. This reveals that this POC has not responded to their attempts to validate the address.

From a different perspective, let’s find the reputation of 173.44.148.89 using valli.org’s multi-RBL lookup. We find that it’s heavily RBL’ed.
173[.dot]44.148.64 was part of a netblock /27, which means there 32 adjacent addresses. Badness often clumps together. What will we find if we check the rest of that /27 with DNSDB Scout?

We find another batch of domains to investigate further.
Resources

Want more?
Check out the complete webinar
Crawl/Walk/Run Introduction to DNSDB

View more Webinars

Learn more about DNSDB

About Farsight Security, Inc.

Farsight Security®, Inc. is the world’s largest provider of historical and realtime DNS intelligence solutions. We enable security teams to qualify, enrich and correlate all sources of threat data and ultimately save time when it is most critical - during an attack or investigation. Our solutions provide enterprise, government and security industry personnel and platforms with unmatched global visibility, context and response. Farsight Security is headquartered in San Mateo, California, USA.

Learn more about how we can empower your threat platform and security team with Farsight Security passive DNS solutions at www.farsightsecurity.com or follow us on Twitter: @FarsightSecInc

+1-650-489-7919