BLOG GENERAL/DEFENSE

How Domain Intelligence and Passive DNS Create A Fuller Domain Profile

12/10/2024

Kali Fencl

Introduction

We often hear of folks using our tools that they may have a preference for one over another. I think that's just human nature – we tend to stick with what we know because it's been working for us – if it ain't broke why fix it?

While it may be true that your queries are working, are they working as hard as they could be? Could they be even more impactful? Once you grasp the why and how, your investigations will be better targeted, giving you and your team more detailed information to better understand if that rabbit hole you're going down is truly worth following.

This article aims to demonstrate how our integrated domain intelligence tool, Iris Investigate, and our passive DNS tool, Farsight DNSDB (DNSDB), complement each other and how the two used together can create a fuller investigation.

What is DomainTools Iris Investigate and Farsight DNSDB?

Before we get too ahead of ourselves, newer visitors to our website may be asking: "What is Iris Investigate and Farsight DNSDB?

DomainTools Iris Investigate

Iris Investigate provides rich context for indicators. Think of it as an atlas for threat actor infrastructure. It provides the most comprehensive DNS data and domain intelligence along with risk scoring to support deep dive investigations. You can predict the risk of indicators and associate clear identification of infrastructure connections, guide investigations, and track threat actors.

Farsight DNSDB

For those who may not know, DomainTools acquired Farsight Security in 2021, and Farsight DNSDB is now part of the DomainTools suite of products. This is our passive DNS (pDNS) tool, meaning it's a historical database providing a fact-based view of internet infrastructure for investigations, and leveraging Farsight's Security Information Exchange (SIE) data-sharing platform for real-time proactive applications. Here are some quick stats on Farsight DNSDB:

- 2TB DNS data collected daily
- 100+ billion DNS records
- 200k+ observations per second
- 1Gb/sec real-time streaming data

Why Use Both Iris Investigate and Farsight DNSDB?

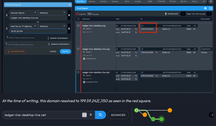
Iris Investigate is a great tool to provide starting metrics on domain name attributes including risk score, DNS, Whois, SSL, and more to expose connections between infrastructure and help get ahead of and learn more about who is behind threats. Using DNSDB builds on discoveries made in Iris Investigate, as it's DNS-centric. Pulling information from DNSDB will not only lead to new discoveries, but show how the existing threats emerge and evolve over time.

Sample Investigation

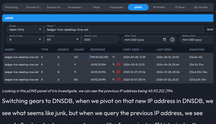
In this example, I'll use ledger-live-desktop-live[.]net, a domain we've been monitoring, likely tied to a fake cryptocurrency wallet.

When I input that domain into Iris Investigate, and with one IP pivot, I can see 127 records (as shown in the screenshot below)

At the time of writing, the domain actively resolved to 199.59.242[.]350, but records also show previous resolutions elsewhere, including 45.93.201[.]194.

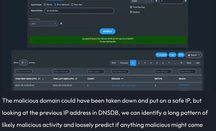


At the time of writing, this domain resolved to 199.59.242[.]350 as seen in the red square.



Looking at the pDNS panel of Iris Investigate, we can see the previous IP address being 45.93.201.194.

Switching gears to DNSDB, when we pivot on that new IP address in DNSDB, we see what seems like junk, but when we query the previous IP address, we see nearly five hundred new records, a wealth of new pivots off historical rather than current DNS records. Sometimes you might find an indicator of compromise (IOC) where the current IP doesn't give you a lot to go off of, but when looking at the historical IP address, we can see much more.



The malicious domain could have been taken down and put on a safe IP, but looking at the previous IP address in DNSDB, we can identify a long pattern of likely malicious activity and loosely predict if anything malicious might come from it in the future.

Conclusion

While a domain may look inactive today, historical data can provide a more accurate picture of its use in past contexts, better informing what we can expect from it going forward. Using both Iris Investigate and Farsight DNSDB can paint a fuller picture of a domain profile, showing that when you use the two tools in tandem, you can make better decisions regarding preventative actions.

Frequently Asked Questions

How do I know if I have Farsight DNSDB?

If you are a Tier 1 customer, you automatically have access to DNSDB with 100 queries per day. The key only goes to one person at an organization though, so you may need to contact your team to verify who has access.

I don't have Farsight DNSDB and I'd like it

Please discuss with your Account Executive or reach out to enterprisesupport1@domaintools.com regarding access.

Why would we go to Farsight DNSDB if passive DNS is in Investigate

Iris Investigate has the ability to cross-reference multiple data points across DNS, Whois, SSL, and more, but if research is a specific IP. Additionally, if the goal is to resolve to a specific IP address, that can be done in the pDNS panel in Iris. DNSDB allows for a more granular search around phishing patterns detectable in DNS records.

Each tool has its own strengths, but depending on your query complexity, you may find more granular results with DNSDB.

Related Content

BREAKING BARRIERS

[Special Report] Father Phishmas, Give Us The Money

Listen Now

BLOG

Return to Sender - A Brief Analysis of a US Postal Service Smishing Campaign

Read more

Related Content

BLOG

Phishmas Comes Early: New Developments in USPS Smishing Attacks

Read more

BLOG

Post Quantum Cryptography (PQC): You May Already Be Using It!

Read more

BLOG

A Website Attacked

Read more