Mapping the Maze

A peek into a real-time ransomware investigation with HYAS Insight and Farsight DNSDB®
Ready to learn how to leverage DNSDB in a ransomware investigation, but not quite ready for the full feature?

Here's an abbreviated version with just the highlights.

Key Take Aways

- Correlating Indicators of Compromise (IOC) across multiple datasets accelerates investigations and increases efficacy and helps pivot to additional infrastructure to proactively block in your environment.
- Adversarial infrastructure is constantly changing—real-time situational awareness is critical.

Contents

Farsight Security Overview
HYAS
Deep Dive Into a MAZE Ransomware Investigation
Start with One Indicator
Pivot to Uncover Additional Domain Infrastructure Associated with the Adversary
Integrating OSINT and Other Source of Intel
Using proprietary HYAS data sets, we can often get down to their doorstep

Farsight Security Overview

Founded in 2013, Farsight observes and records DNS resolutions worldwide as they happen. There are two kinds of passive DNS, below the recursive and above the recursive. Farsight observes information above the recursive, between the recursive resolver and the authority server. We do not have information as to who made the query.

DNSDB enables users to pivot data, review historical data, and conduct wildcard searches—all of which are not possible with the current domain name system alone.

HYAS

Founded in 2015, HYAS Insight lets users connect specific attack instances and campaigns to billions of historical and current indicators of compromise faster than ever before.
Deep Dive into a MAZE Ransomware Investigation

The MAZE ransomware group are among the most active and aggressive in targeting and extorting victims.

Start With One Indicator: A C2 Domain

Here are helpful pivots to correlate additional infrastructure:

- Domain
- Email
- Phone Number
- Registration Alias
- A Record
- Passive DNS

We find that the associated cell phone numbers originate from Russia. We also find three additional email addresses associated with the initial phone number.

Pivot to Uncover Additional Domain Infrastructure Associated with the Adversary

Route 1: Starting with a registration alias

- Live phone numbers with devices associated with them have a much higher recidivism rate for domain registration.
- They also tend to have multiple addresses associated with them.
While some hosting providers may make name server associations useless, users can still review the history of a record—activity that may not have always been hidden behind services like Cloudflare.

Using a wildcard search, users can uncover more potentially valuable information like names and locations.

**Route 2: Starting with a wildcard lookup**
Users can start with a wildcard lookup and still drill down to records that may link seemingly unrelated entities.
Integrating OSINT and Other Source of Intel

- Other sources of OSINT and Intel can help expose opsec failures of the actor.
- Password reuse and naming conventions can lead to other email addresses and data that tie back to the actor seen initially.

Using Proprietary HYAS Data Sets, We Can Often Get Down to Their Doorstep

Based on the actor’s IP addresses, the investigator can pivot into the address infrastructure and better understand the adversary.

Closing Notes

Farsight and our premier partners, like Hyas, can help investigative teams navigate the complexities of combating ransomware groups. Starting with a single indicator of compromise, security professionals can leverage the world’s most comprehensive passive DNS database and our partner tools to track and expose ransomware groups in real-time and prevent future attacks.

Learn how Farsight can work seamlessly with your existing security solutions.
Resources

Want more?
Check out the complete webinar Mapping the Maze: A peek into a real-time ransomware investigation with HYAS Insight and Farsight 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