DomainTools

FARSIGHT SECURITY
A DOMAINTOOLS COMPANY

ThreatConnect, Inc. Case Study

Anthem Breach Investigation

ThreatConnect, Inc. is a leading provider of advanced threat intelligence products and services including ThreatConnect®, a comprehensive threat intelligence platform. Their customers include Fortune 100 companies and select accounts in the financial, energy, and biomedical markets.

The ThreatConnect® Approach

ThreatConnect® is a single threat intelligence platform built to bridgeincident response, defense, and threat analysis. Government agencies and Fortune 500 organizations worldwide leverage the power of ThreatConnect every day to aggregate, analyze, and act on their threat intelligence data. ThreatConnect collects and aggregates intelligence from multiple sources including open-source indicator and reputation feeds, as well as vendorprovided threat intelligence data such as Farsight's Passive DNS data.

"We use DNSDB every day. It's as important as email to the organization."

Farsight DNSDB Selection Process

ThreatConnect became familiar with the power of passive DNS several years ago. Through market research and the evaluation of open source and commercial passive DNS databases, ThreatConnect determined that "DNSDB is the industry's premier Passive DNS historical database."

Typical Farsight DNSDB Use Case

ThreatConnect uses the DNSDB dataset to enrich our own threat intelligence data: for example, a piece of malware may call out to a particular IP address so we want to find out other domains connected to that IP. In our team's investigations, we may use Farsight Security's Passive DNS data to confirm or reaffirm information found in our other threat feed sources.

Industry:
Network Security

Headquarters:
Arlington, VA

Objective:
Investigate Anthem Breach-Related Activity Farsight Security

Solution:
DNSDB™, the world's largest, most robust historical Passive DNS database available in the threat intelligence market today.

DNSDB Key Benefits:
DNSDB is a bridge to new data points in all of our investigations," said ThreatConnect Chief Intelligence Officer Rich Barger. "DNSDB fills some Threat Intelligence gaps. We always check DNSDB as one of our initial sources in any digital investigation.

Anthem Breach Investigation:

Connecting the Dots with Farsight DNSDB

In February 2015, it was revealed that Anthem Inc., the nation's second largest health insurer, suffered a significant data breach. Customer names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and other personal information were compromised.

ThreatConnect's independent investigation into the breach revealed threat activity which appeared to have begun long before December 2014, when WellPoint changed its corporate name to Anthem. Using Farsight's Passive DNS data, ThreatConnect was able to confirm:

- **The attackers' malicious infrastructure:** ThreatConnect used DNSDB to enrich and confirm their findings and malware analysis, indicating that fake domains such as we11point.com and www.we11point.com appeared to impersonate the legitimate WellPoint IT infrastructure.
- **Attack timeline:** Using DNSDB, ThreatConnect was able to determine that the attack started in April 2014 — much earlier than originally thought — by confirming when the fake domains were first created and later operationalized by the attackers.
- **New threat intelligence on the adversaries' objectives:** by analyzing different relationships with malware, IP addresses, and other data points in the investigation. ThreatConnect mapped malicious and benign infrastructure to help substantiate their analytic hypotheses.

"Farsight DNSDB was invaluable in our investigation of this activity,"

— Rich Barger

ThreatConnect Chief Intelligence Officer

About Domaintools

DomainTools is the global leader for Internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape

View our Farsight DNSDB page

DomainTools