Enriching TruSTAR Security Events with DNSDB
INTRODUCTION

RON BURNS, FARSIght SECURITY
  • VP SALES

ELVIS HOVOR, TRUSTAR
  • PM INTEGRATIONS
AGENDA

● INTRODUCTION TO PIVOTING WITH PASSIVEDNS & WHOIS

● TRUSTAR’S INTEGRATION

● USING THE FARSIGHT DNSDB INTEGRATION IN TRUSTAR TO ENHANCE INVESTIGATIONS TO MAP OUT AN ADVERSARY’S INFRASTRUCTURE
DNS RECURSION / PASSIVE DNS

Devices & Users → Recursive Server

Recursive Server → Farsight Security

Farsight Security

Root Servers

Registry Servers

DNS Servers

www.example.com → 93.184.216.34
DNS DATA WORLDWIDE - OUR SENSOR ARRAY

GLOBAL COVERAGE

DIVERSE SOURCES
• Consumer
• Government
• Education
• Enterprise
• ISPs & Mobile
• Social media

REAL-TIME & HISTORIC
• 200k+ Resolutions / sec
• 5+ TB / Day
• 100+ Billion DNS Resolutions
TWO WAYS TO EMPOWER SECURITY OPERATIONS

I. SECURITY INFORMATION EXCHANGE

• Proactively detect and block
• Empower your Firewall & Mail Servers
• 200,000+ observations/second
• Compliant with leading protocols for easy ingestion

II. DNS INTELLIGENCE DATABASE – DNSDB

• World’s largest historic database of DNS resolution and all records
• Empower your SIEM and Threat Platform
• Started 2007, rebuilt in 2010, updated in real-time, 100+ Billion resolutions recorded
• API and On-Prem Solution
THREATCONNECT AND DNSDB: DNS AS A MAP

- DNS IS USED EVERYWHERE
  - Desktop, Mobile, Laptops, Servers, Sites

- MAP EXISTING INFRASTRUCTURE BASED ON OBSERVATIONS
  - Naturally avoid private information (we avoid knowing who queried what)

- OBSERVATIONS & FACTS
  - CONTEXT FOR INVESTIGATIONS
  - ENHANCE THREAT INTELLIGENCE

- MISCREANTS NEED DNS FOR THEIR INFRASTRUCTURE, TOO
UNDERSTANDING PIVOTING WITH PASSIVE DNS AND WHOIS
PIVOTING: GUILT BY ASSOCIATION – PASSIVE DNS

KNOWN BAD HOSTNAME OR IP ADDRESS

WHAT OTHER HOST NAMES AT THE SAME ADDRESS AT THE SAME TIME?

WHAT OTHER INFRASTRUCTURE IS HOSTED IN THE SURROUNDING NETWORK BLOCK?

KNOWN BAD DOMAIN

WHAT OTHER HOSTS ARE IN THE DOMAIN?

WHAT OTHER DOMAINS ARE SERVED BY THE SAME NAMESERVER?
PIVOTING: GUILT BY ASSOCIATION – PASSIVE DNS

SIMILAR NAMING PATTERNS

FAST-FLUX BOTNET INFRASTRUCTURE

UNCOMMON NAMES USED IN MANY DOMAINS

DOMAIN GENERATION ALGORITHMS

SIMILAR LOOKING ANSWERS

SOA RECORDS?
TXT RECORDS?
SPF RECORDS?
PIVOTING PASSIVE DNS: REDUCING FALSE POSITIVES

INDICATOR FOR A HOSTNAME OR IP ADDRESS

- KNOWN REVERSE PROXY SERVICE?
- KNOWN SINKHOLE?
- HOSTING SERVICE?
- DOMAIN PARKING SERVICE?
- DYNAMIC DNS SERVICE?
- WIDELY USED CDN INFRASTRUCTURE?

Example: “ICE takedown mooo.com”
PIVOTING WHOIS: COMMON REGISTRATION FINGERPRINTS

KNOWN BAD DOMAIN

REGISTRATION EMAIL USED ELSEWHERE?
SAME OR SIMILAR REGISTRATION NAME USED ON OTHER DOMAINS?
SAME OR SIMILAR POSTAL OR PHONE INFORMATION USED ON OTHER DOMAINS?

Doesn’t matter if registration is real or faked – just similar.

One known bad domain could lead to more.

Similar registration information (and hosting patterns) helps confirm two domains could be managed by same actor.

Check out https://www.domaintools.com/partners/integrations/threatconnect/
HOW FARSIGHT DATA IS USED

FARSIGHT SECURITY

- Threat Platforms
- Firewalls
- Mail Servers
- Orchestration / Automation
- Bulk Queries
- Machine Learning
- SIEMs
HOW TO USE IT

- Indicator of Compromise correlation
- Historical resolution lookups
- Time-based analysis
- Fully qualified domain name lookups
- SIEM event enrichment
- Domain or IP enrichment to proactively hunt for threats
We power threat intelligence ecosystems for both enterprise teams and exchange groups

1. Leverage Internal Intelligence
   - All internal security tools and teams have visibility across historical events and analysis.
   - Sample Enterprise Customers

2. Operationalize External Intelligence
   - All-source intelligence enrichment from external CTI sources and email listservs.

3. Scale Intelligence Exchange
   - Orchestrate high-signal intel exchange across peers, partners and supply chain as a security force-multiplier.
   - Sample Hosted Exchange Groups
FIRST, IT’S ALL ABOUT THE ENCLAVE...

With intelligence and collaboration, there are critical and inevitable challenges with:

- Access Control
- Normalization
- Customization
- Integration

TruSTAR’s Enclave Architecture
BALANCING AUTOMATION, ACCESS CONTROL AND HUMAN ANALYSIS TO LEVERAGE ALL-SOURCE INTEL
HOW OUR USERS TALK ABOUT THE BENEFITS...

Automate the mundane and time-consuming components of enterprise security knowledge management.

Augment human analysts through targeted, integrated use of graph-based UI made by analysts for analysts.

Leverage historical knowledge of indicators, events, intelligence reports, and analysis to speed investigation across event lifecycle.

Validate, operationalize and intelligently manage external data sources (and spend $$!) and control noise as you grow.

Facilitate secure intelligence exchange across teams, business units, partners, sharing groups and the broader TS Community.
User activates Farsight DNSDB integration from the TruSTAR marketplace using API Key.

Every 15 mins newly extracted indicators from reports are queried against DNSDB and the response submitted to customers enclave in TruSTAR.
DS INTEGRATION IN TRUSTAR

Farsight DNSDB node inside a customer’s enclave
QUERIES AND INDICATOR ENRICHMENT...

Domain,
Request Example :
Response:
JSON (Full Body)

IP,
Request Example :
https://api.dnsdb.info/lookup/rdata/ip/104.244.13.104?limit=100
Response:
JSON (Full Body)

Returned data on queried indicators is submitted into customers Digital Shadows enclave in TruSTAR
LEVERAGE AND OPERATIONALIZE INTEL...

Ticket is auto-updated back into Private Enclave for searchable, visual log and can be easily auto-redacted and shared with w/ other groups on/off TS.

L2 Analyst enriches initial ticket using data from across their intelligence network and visual link-analysis shares all to CIRT for final mitigation action.

CIRT operator examines viz analysis and takes mitigation action and closes ticket.

Alert from SIEM / IDS causes L1 Analyst to create ticket which is auto-ingested into Private Enclave via API.

Automated ingest of intel from paid CTI feeds into Private Enclave.

Outcomes

- Intel from sharing relationships enriches analysis and helps drive mitigation.
- Demonstrates active participation in sharing network and advances FFIEC cyber maturity from Domain 2 -> 3.
- Save time previously spent copy-pasting and maintaining other custom tools.

Based on case-study: <Fortune 500 Financial>
HOW WE SET OURSELVES APART FROM THE COMPETITION...

- Tailored Partner Integrations
  - Indicator Query
  - Feed Ingest

- Detailed Enrichment Report
  - What you have is what you see

- Flexible Data Mapping
  - Few unique mappings (External ID, Title, Tags)

- Automated Indicator Extraction

- Graph Visualization and Correlation Engine
THANK YOU FOR YOUR ATTENTION.

QUESTIONS?

Trustar.com
Farsightsecurity.com
DNSRPZ.INFO
Enriching TruSTAR Security Events with DNSDB