Synapse Bootcamp

Module 17

Network Infrastructure Analysis

v0.4 - May 2024

Objectives

- Define network infrastructure analysis
- Identify key data model elements related to network infrastructure
- Understand common pivots and queries to use
- Understand how to use relevant Power-Ups to obtain and enrich data

What is Infrastructure Analysis?

- Examine network communications and / or network-based indicators
  - Identify, characterize, track, and correlate threat activity
- Can be viewed very broadly
  - No 'CNO' without networks!
- Characteristics of networks
  - Location, ownership, size…
- Characteristics of network traffic / communications
  - Protocols, patterns…
- Characteristics of network hosts
  - Type of host / device, ports / services…

Threat Intelligence and Infrastructure

- **Location** of network resources
  - Geolocation, Autonomous System…
- **Ownership** of network resources
  - Domain whois, netblock registration
- **Use** of network resources
  - Malware communication, source / destination of activity, anonymization services…
- **Characteristics** of resources
  - Hosts: Certificates, ports, services, vulnerabilities
  - Protocols: How used, unique identifiers…
- **Patterns** among resources
  - Which resources are communicating with other resources?
  - What other resources share these characteristics?

Basic Network Components

Data	Form
FQDN	`inet:fqdn`
IP address	`inet:ipv4, inet:ipv6`
CIDR range	`inet:cidr4, inet:cidr6`
AS number	`inet:asn`
AS range	`inet:asn4, inet:asn6`
Server	`inet:server`
Client	`inet:client`
Host	`it:host`
Network interface	`inet:iface`
MAC address	`inet:mac`

Network Registration Data

Data	FQDN Form	IP / Netblock Form
Whois record	`inet:whois:rec`	`inet:whois:iprec`
Whois contact data	`inet:whois:contact`	`inet:whois:ipcontact` `ps:contact`
Whois domain registrar	`inet:whois:rar`	`ps:contact`
Whois domain registrant	`inet:whois:reg`	`ps:contact`
Whois email address	`inet:whois:email`	
Whois name server	`inet:whois:recns`	

The **synapse-nettools** Power-Up can perform a **live** lookup to query current whois data.

Protocol Data - DNS

Protocol	Data	Form
DNS (`inet:dns:*`)	DNS record	`inet:dns:* (inet:dns:a, inet:dns:ns, etc.)`
	DNS PTR record	`inet:dns:rev, inet:dns:rev6`
	DNS query	`inet:dns:query` `inet:dns:request, inet:dns:answer`

Synapse can record both **"fused"** and **"instance"** data related to DNS.

Protocol Data - HTTP

Protocol	Data	Form
HTTP (`inet:http:*`)	HTTP request	`inet:http:request`
	HTTP response	`inet:http:response`
	HTTP header	`inet:http:request:header` `inet:http:response:header`
	HTTP cookie	`inet:http:cookie`
	HTTP session	`inet:http:session`

A subset of SMTP-related data is represented using `inet:email:header` nodes.

Network Communications

Data	Form
Server hosting SSL/TLS certificate	`inet:tls:servercert` / `inet:tls:clientcert` (new) `inet:ssl:cert` (old)
JARM hashes / data	`inet:ssl:jarmhash`, `inet:ssl:jarmsample`
JA3 hashes / data	`inet:tls:handshake` `inet:tls:ja3:sample` / `inet:tls:ja3s:sample`
Server service banner	`inet:banner`
Network connection / flow	`inet:flow`
URL hosting a file	`inet:urlfile`
Server hosting a file	`inet:servfile`
File downloaded from server	`inet:download`

Common Enrichment Tasks

Question	Workflow
What can I learn about this FQDN?	Use Power-ups to ingest: - Whois data (current / historical) - DNS data (A, AAAA, CNAME...) - Passive DNS data - Communicating malware - Tags
What can I learn about this IPv4 / IPv6?	Use Power-ups to ingest: - DNS PTR data - Passive DNS data - AS and geolocation data - Whois / netblock registration data - Open ports / banners (current/historical) - SSL/TLS certificates (current/historical) - Services / versions - JARM signatures - Communicating malware - Tags

Additional Common Analysis Tasks

Question	Object	Workflow
Where has <thing> been seen?	File (`file:bytes`)	Pivot to `inet:urlfile`, `inet:servfile`, `inet:download`
	SSL/TLS certificate	Pivot to `inet:tls:servercert` / `inet:ssl:cert`
	Any property of interest	Pivot from properties to find similar objects (server port, email header, HTTP header, banner content…)

Common Tag Examples

Assessment	Tag Format	Example	Third-Party
Is malicious	`#cno.mal`	`#cno.mal`	`#rep.eset.mal`
Associated with a malware family	`#cno.mal.<family>`	`#cno.mal.industroyer`	`#rep.eset.industroyer`

Associated with a threat group	`#cno.threat.<group>.own` (or `.tc`)
	`#cno.threat.<group>.use`
		`#cno.threat.nickel`
		`#cno.threat.nickel.own`
		`#cno.threat.nickel.use`
			`#rep.microsoft.nickel`

Has certain capabilities or demonstrates use of certain TTPs	`#cno.ttp.<category>.<sub>`	`#cno.ttp.se.hijacked` `#cno.ttp.t1584.001`	

You can use **triggers** in Synapse to automatically apply tags when certain conditions are met!

Infrastructure Tag Examples

Assessment	Tag
Infrastructure - DDNS (for FQDNs)	`#cno.infra.ddns`

Infrastructure - anonymous	`#cno.infra.anon.tor`
	`#cno.infra.anon.vpn`
	`#cno.infra.anon.proxy`

Infrastructure - other	`#cno.infra.dns.sink.*`
	`#cno.infra.dns.parking`
	`#cno.infra.dns.redirect`

Network Analysis - Demo

Summary

- **Network infrastructure analysis** involves a broad range of data
  - Objects, hosts, servers, SSL/TLS certificates
  - Registration / whois data
  - Network communications (including malware communications
  - Network protocols
- Power-Ups such as **NetTools** and **Maxmind** provide whois, DNS, AS and geolocation data
- Various third-party Power-Ups may provide:
  - Passive DNS data
  - SSL/TLS certificate download, history, or validity checks
  - Data on network flows, connection activity, or scanning activity
  - Servers / ports / services