



Vertex

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

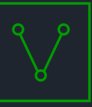
Data	Form
FQDN	<code>inet:fqdn</code>
IP address	<code>inet:ipv4, inet:ipv6</code>
CIDR range	<code>inet:cidr4, inet:cidr6</code>
AS number	<code>inet:asn</code>
AS range	<code>inet:asn4, inet:asn6</code>
Server	<code>inet:server</code>
Client	<code>inet:client</code>
Host	<code>it:host</code>
Network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



Network Registration Data

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

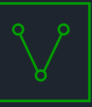
The **synapse-nettools** Power-Up can perform a **live** lookup to query current whois data.



Protocol Data - DNS

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

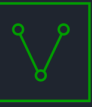
Synapse can record both "**fused**" and "**instance**" data related to DNS.



Protocol Data - HTTP

Protocol	Data	Form
HTTP (<code>inet:http:*</code>)	HTTP request	<code>inet:http:request</code>
	HTTP response	<code>inet:http:response</code>
	HTTP header	<code>inet:http:request:header</code> <code>inet:http:response:header</code>
	HTTP cookie	<code>inet:http:cookie</code>
	HTTP session	<code>inet:http:session</code>

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



Network Communications

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



Common Enrichment Tasks

Question	Workflow
What can I learn about this FQDN?	Use Power-ups to ingest: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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	<code>#cno.mal</code>	<code>#cno.mal</code>	<code>#rep.eset.mal</code>
Associated with a malware family	<code>#cno.mal.<family></code>	<code>#cno.mal.industroyer</code>	<code>#rep.eset.industroyer</code>
Associated with a threat group	<code>#cno.threat.<group>.own</code> (or <code>.tc</code>) <code>#cno.threat.<group>.use</code>	<code>#cno.threat.nickel</code> <code>#cno.threat.nickel.own</code> <code>#cno.threat.nickel.use</code>	<code>#rep.microsoft.nickel</code>
Has certain capabilities or demonstrates use of certain TTPs	<code>#cno.ttp.<category>.<sub></code>	<code>#cno.ttp.se.hijacked</code> <code>#cno.ttp.t1584.001</code>	

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

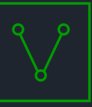


Infrastructure Tag Examples

Assessment	Tag
Infrastructure - DDNS (for FQDNs)	<code>#cno.infra.ddns</code>
Infrastructure - anonymous	<code>#cno.infra.anon.tor</code> <code>#cno.infra.anon.vpn</code> <code>#cno.infra.anon.proxy</code>
Infrastructure - other	<code>#cno.infra.dns.sink.*</code> <code>#cno.infra.dns.parking</code> <code>#cno.infra.dns.redirect</code>



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