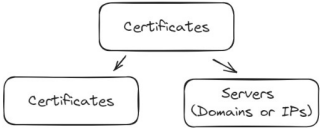


?	🔗	What to look for?	
Dedicated	Whois	Top 1M	Search engine
Dedicated IP	Passive DNS	Few domains registered on the same IP or many with similar patterns (DGA, similarity, TLD..)	
Free hosting	Search Engines	Subdomains of known dynamic DNS, blogpost, free hosting providers	
Compromised	Web Archive	Old capture Existing path, pages vulnerable CMS or CMS plugins	
Pattern	Whois	Registrar information	
	Passive DNS	Patterns: simple DGA, same TLD, same period...	
Deanonimization	IP Scanner	Search Engines	Passive DNS
Certificates	Crt.sh	Same spoofed values	Subdomains
Used as a C2	Virus Total	Samples communicating with this domain	Search Engines
	URL scanner	the payloads	URL pattern associated with

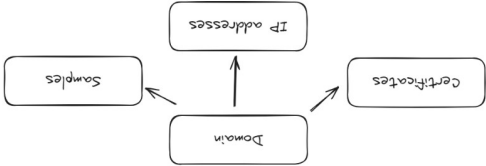
Certificates



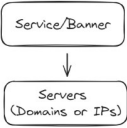
- Are other servers using the same certificates?
 - Uniqueness? Associated with a legitimate service?
 - Self-signed certificates? If so, search for similar Subject and Organization
 - Other domains listed as Common Name

?	🔗	What to look for?	
Self-signed	IP Scanner	Certificates with the same value in the Organization or Subject Name fields	
Common Name	IP Scanner Crt.sh	Domains listed as Common Name IP hosting the same certificate	

Domain		
		<ul style="list-style-type: none"> Is the domain controlled by the threat actor? <ul style="list-style-type: none"> Dedicated? Hosted on a dedicated IP? Hosted on free hosting, tunnels, dynamic DNS? Is it possible to fingerprint it to find other similar domains? <ul style="list-style-type: none"> Compromised? (WordPress) Registration pattern? (Registrar, uptime) Hosting? Certificates? Content (Analytics, HTML) Deanonimization? (Cloudflare) Used as C2? Is any other sample refers to this domain?



Service/Banner

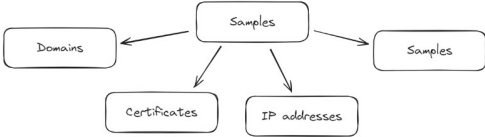


- Does the same banner/content is seen on another IP or Domain?
 - Uniqueness? Correspond to a default configuration?
 - TLS Fingerprint: JA3, JA4, JARM
 - Content: Banner hashes, HTML, Analytics ID

?	🔗	What to look for?	
Uniqueness	IP Scanner	Differences from the default configuration, servers that share them.	
JA3, JA4, JARM	IP Scanner JA3 Databases JA4 Databases	Related to known software Specific or not	
Analytics ID	Search Engines PublicWWW IP Scanner	Domains associated with the Analytics ID	

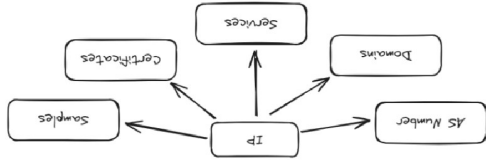
?	🔗	What to look for?	
Dedicated	Reverse DNS	<ip-like>.registrardomain.com	without patterns
Compromised	IP Scanner	Port/Protocols related to IoT	Vulnerable appliance
Existing	IP Scanner	Opened port and default services	IP Scanner
Services	IP Scanner	Banner, banner hash, JA3, JA4, JARM	IP Scanner
Services	IP Scanner	HTTP patterns, analytics IDs	Search Engines
uniqueness	Search Engines		
Certificates	IP Scanner	Self-signed certificate	Pattern between certificates
Used as a C2	Virus Total	Samples communicating with this IP or IP within the same range	Sandboxes
	URL scanner	URL pattern associated with the payloads	Search Engines

Samples



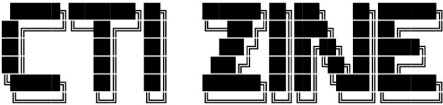
- Does some samples share the same C2? (IP, Domain)?
- Does some samples are similarly written, packed or obfuscated?
- Does some samples are signed with the same certificate?

?	🔗	What to look for?	
Same C2	VirusTotal Sandboxes Intel feeds	Samples related to the same IP or domains or to similar ones Refers to IP and domains pivot	
Similar content or features	VirusTotal	A good reverser! (YARA) Content search	
Certificates	VirusTotal	Samples associated to the same certificate or similar ones Refers to certificates pivots	



- Is the IP address is controlled by the threat actor?
 - Dedicated? (VPS)
 - Compromised? (Botnet, ORB)
 - Other? (Commercial VPN, proxy, Tor)
 - Is it possible to fingerprint it to find other similar IPs?
 - Existing services? (Web, administration, database)
 - Services configuration? (widespread, unique)
 - Certificates?
 - Autonomous System?
- Is this IP used as C2? Does any other sample refer to this IP?

IP address



PIVOT EDITION