DNS Security Investigation Cheat Sheet

DNS Record Types

Record	Purpose	Investigation Use
A	IPv4 address	Identify hosting / CDN
AAAA	IPv6 address	Often overlooked attack surface
MX	Mail servers	Phishing config check
NS	Name servers	DNS provider / DDNS flags
TXT	SPF / DKIM / DMARC	Email security posture
CNAME	Alias / redirect	Third-party service exposure
SOA	Zone authority	Admin email, serial, TTL
PTR	Reverse DNS	Validate IP ownership

Email Security Records

Check	Good	Red Flag
SPF	v=spf1 ... -all	+all (anyone can send)
DMARC	p=reject or quarantine	Missing entirely
DKIM	Selector record present	No DKIM configured
MX	Known provider	Unexpected config / investigate

5-Step Investigation Workflow

Step	Action
1 Run DNS Lookup	Query A, AAAA, MX, NS, TXT, CNAME
2 ID Infrastructure	Hosting, CDN, cloud platform, geo
3 Check Email Sec	SPF, DKIM, DMARC, MX provider
4 Evaluate Risk	DDNS usage, fast-flux, missing controls
5 Continue Intel	RDAP, Phishing Scanner, Safe Link Decoder

Fast-Flux Indicators

Indicator	Why It Matters
Many A records	Botnet / distributed infra
Low TTL + frequent IP changes	Warrants investigation
Constant DNS changes	Evasion technique
Global IP spread	C2 / phishing resilience

Common Cloud / CDN IP Ranges

Cloudflare	104.16.x.x – 104.20.x.x 172.64.x.x – 172.66.x.x 188.114.x.x → *Verify ownership via ASN / RDAP*
Amazon AWS	3.x.x.x 13.x.x.x 18.x.x.x 34.x.x.x 44.x.x.x 52.x.x.x amazonaws.com cloudfront.net → *Representative ranges only*
Microsoft Azure	20.x.x.x 40.x.x.x 52.x.x.x azurewebsites.net cloudapp.azure.com → *Representative ranges only*
Google Cloud	34.x.x.x 35.x.x.x 104.x.x.x run.app appspot.com → *Representative ranges only*
DigitalOcean	134.122.x.x 157.230.x.x 159.65.x.x 167.71.x.x → *Common in phishing infrastructure*

Suspicious DDNS Providers

Provider	Common In
duckdns.org	Home labs / malware investigations
ddns.net	Legitimate DDNS / observed in C2
no-ip.com	Legitimate DDNS / seen in malware
hopto.org	no-ip subdomain / remote access tools
zapto.org	no-ip subdomain / phishing chains

Quick Questions to Ask

Question
Who owns the IP address?
Is the domain behind a CDN?
Does the domain receive email?
Is SPF configured correctly?
Is DMARC present and enforced?
Is IPv6 enabled — and monitored?
Is Dynamic DNS being used?
Does infrastructure match the org?

ITKB Investigation Tools

Tool	itknowledgebases.com + path
DNS Lookup	/dns-lookup/
Phishing Scanner	/phishing-check/
Safe Link Decoder	/safe-link-decoder/
RDAP Lookup	/rdap/
IP Geolocation	/ip-geolocation/
CVE Advisory Feed	/advisory/