Valuable Datasets to Analyze Network Infrastructure

Cheat Sheet

Dataset	Record Type	Observation	Potential Indication
 *DNS*	IP Address	Frequently changing IP addresses associated with a domain name	Fast flux
	IP Address	Low number of domains hosted on a single IP address with consistent naming	Can give high confidence that infrastructure is controlled by a single actor
	Nameserver	Cryptocurrency-themed hosters	Suspicious infrastructure
	Nameserver	Low number of domains with consistent naming pointing to a nameserver or nameserver IP	Infrastructure was stood up by an individual, so connected domains and infrastructure may act as valuable artifacts
	Nameserver	Domain's NS record points to a nameserver owned by those operating a sinkhole	Shadowserver and Microsoft do a lot of sinkholing, as do many independent security researchers
	Nameserver	Single nameserver for a domain	Suspicious infrastructure
	Nameserver	Nameservers hosted on multiple IP addresses	Suspicious infrastructure
	Nameserver	Change in nameserver from default hosting to owned infrastructure	Suspicious infrastructure
	SOA	Unique RNAME emails associated with known bad domain names	The email address can cluster domains, which may represent malicious campaign infrastructure

	SOA	Short TTL	May indicate a fast-flux network, especially if other red flags exist
	MX	MX record for a mail server on the same domain	Owner-managed setup. In the case that this is coupled with mail server validation like SPF records it can be a sign that an attacker is trying to make their mail look legitimate to pass through mail servers while phishing
	MX	MX server host information doesn't match host for IP address or nameserver	Actor could be operating their own email server locally, making it easier to monitor their activity and profile their behaviors
	MX	Few or one MX servers on a single domain	Unusual activity that isn't typical for legitimate organizations
	MX	Mismatch of MX and other infrastructure hosting (IP/Nameserver)	Someone is running their own MX server
	MX	High entropy in the MX record name	Malicious intent
	MX	Typosquatting	Malicious intent
	TLD	Uncommon or inexpensive TLD	Threat actor acquiring inexpensive domains in TLDs where realistic spoof names are sometimes more available

 *Whois*	Domain Name	Typosquatting or non-typo spoofing (e.g. affixes/prefixes)	Suspicious infrastructure
	Domain Name	High entropy strings or a combination of random words	Potential use of DGA technique
	Domain Name	Young, culturally-relevant themed domain names with close proximity to blocklisted infrastructure	Suspicious infrastructure
	Registrant Email	Unique emails associated with other malicious domains, SOA records, or SSL records	Suspicious infrastructure
	Registrant Email	Unique free email domains with a higher concentration of badness in combination with close proximity to known bad infrastructure	Suspicious infrastructure
	Registrant Address	Elements of a unique address shared between a small number of domain names (especially if the domain names share a collective theme)	Shared domain ownership
	Registrant Address	Inconsistent or inaccurate address information that isn't associated with a legitimate entity	Suspicious infrastructure
	Registrant Phone Number	Inconsistent or inaccurate phone information that isn't associated with a legitimate entity	Suspicious infrastructure
	Registrar Name	Registrars operating out of countries who aren't likely to respond to legal actions by the US and EU	Suspicious infrastructure
	Create Date	Domain age is less than 30 days	Suspicious infrastructure
	Expiration Date	Recently expired domain with changed registration information from previous ownership	Potential BEC or phishing infrastructure

 *Passive DNS*	Subdomain	Typosquatting or non-typo spoofing (e.g. affixes/prefixes)	Suspicious infrastructure
	Hostname	Hostname with high entropy	Potential DNS tunneling infrastructure
	Hostname	Hostname with 27+ unique characters	High likelihood of DNS tunneling infrastructure
	AAAA	Queries with odd A or AAAA responses	Potential C2 infrastructure
	IP	A single IP cycling quickly through queries or domains	Fast flux
	Nameserver	Nameserver response associated with known badness associated with a dynamic DNS provider	Attacker is likely running their own infrastructure
	CNAME	Typosquatting	Potential phishing infrastructure
	CNAME	CNAME connected to other known-bad infrastructure (e.g hostnames, domains, etc)	Suspicious infrastructure
	TXT	Large TXT records	Potential DNS Tunneling infrastructure
	TXT	Large TXT records	Potential DDoS infrastructure
	TXT	TXT responses with SPF or DKIM records associated with typosquatting domains/CNAMEs/Subdomains/ Nameservers	Potential BEC or phishing infrastructure