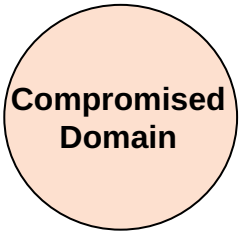
Malicious vs Compromised Domains

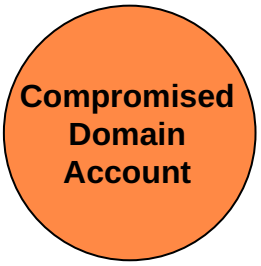
Definitions

“Malicious Domain” means a domain name that is registered or used with the intent to facilitate DNS Abuse.



“Compromised Domain” means a domain name that was registered for legitimate purposes but is subsequently exploited, or controlled by an unauthorized party to conduct DNS Abuse without the knowledge, authorization, or participation of the registrant.

“Misused Service” means a service associated with a domain name that was created for legitimate purposes but is subsequently exploited, misused, or controlled by an unauthorized party to conduct DNS Abuse without the knowledge, authorization, or participation of the registrant. This could include the misuse of user-generated content, subdomain or link-shortening functionality, or abuse of third-party services such as advertising or traffic distribution.



“Compromised Domain Account” means a domain name account (for example at a registrar, reseller, or hosting company) that was created for legitimate purposes but is subsequently exploited, misused, or controlled by an unauthorized party to conduct DNS Abuse without the knowledge, authorization, or participation of the registrant, including by registering new, malicious, domain names.

Malicious vs Compromised Domain Examples

A domain name is registered and immediately used for DNS Abuse.	**Malicious domain**
A domain name is registered and, 3 years later, used for DNS Abuse.	May be a **malicious domain**, may be a **compromised domain**
A domain name is registered and used for legitimate purposes; 2 years later, it is used for DNS Abuse.	Likely a **compromised domain**
The domain is used to offer subdomain or URL hosting services.	Legitimate service, may be a **misused service**
The domain is used to provide link shortening services.	Legitimate service, may be a **misused service**
The domain is used to host user-generated content.	Legitimate service, may be a **misused service**
A vulnerability in the CRM of the website under the domain is exploited by threat actor to display abusive content.	Legitimate service, may be a **misused service**
A domain name is parked with a traffic arbitrage system; one of the advertisers of the parking provider resells the traffic to a threat actor.	Legitimate service, may be a **misused service**
A domain name is registered and ADC reveals four legitimate domains, each older than 4 years.	Likely a **compromised domain account**
A domain name is registered and, after briefly displaying a personal blog, is misused for DNS Abuse.	Likely a **compromised domain account** (hosting)

Links to relevant information:

CPH Definition of DNS Abuse (PDF)

RAA §3.18.1 defines DNS Abuse