DOMAINTOOLS®

Passive DNS Data in Iris

Gain Critical Insights Into Potentially Malicious Infrastructure

Add Passive DNS to Iris for Next-Level Investigations

DomainTools has partnered with DNS data pioneer Farsight Security and several other top-tier providers to integrate passive DNS ("pDNS") data into Iris. Complementing the active DNS resolutions performed by DomainTools, passive DNS providers capture domain-to-IP mappings observed "in the wild" across the globe. Many of the world's most advanced security teams rely daily on passive DNS to support their threat hunting, incident response, and adversary analysis activities. The aggregation of data from multiple sources, some of which have specific strengths unique to them, builds a more complete picture of infrastructure and traffic patterns.

Query	Type	Source	Count	Response	First Seen ▾	Last Seen
webmail.groupweblogs-gsm1900.com	A	A	1	165.22.196.7	2019-07-17, 19:52	2019-07-18, 02:15
cpanel.groupweblogs-gsm1900.com	A	D	2	165.22.196.7	2019-07-17, 15:56	2019-07-17, 15:56
mail.groupweblogs-gsm1900.com	A	A	1	165.22.196.7	2019-07-17, 15:54	2019-07-17, 15:54
mail.groupweblogs-gsm1900.com	NAME	A	1	groupweblogs-gsm1900.com.	2019-07-17, 15:54	2019-07-17, 15:54
mail.groupweblogs-gsm1900.com	CNAME	A	1	groupweblogs-gsm1900.com.	2019-07-17, 15:53	2019-07-17, 20:11
groupweblogs-gsm1900.com	A	B	3	165.22.196.7	2019-07-14, 19:49	2019-07-16, 19:31
groupweblogs-gsm1900.com	NS	B	3	rreui10.traeumtgerade.de	2019-07-14, 19:49	2019-07-16, 19:31
groupweblogs-gsm1900.com	NS	B	3	rreui11.traeumtgerade.de	2019-07-14, 19:49	2019-07-16, 19:31
groupweblogs-gsm1900.com	DOMAIN	A	1	groupweblogs-gsm1900.com.	2019-07-14, 10:04	2019-07-20, 10:17
groupweblogs-gsm1900.com	A	A	1	165.22.196.7	2019-07-14, 10:04	2019-07-20, 10:17
groupweblogs-gsm1900.com	MX	D	6	groupweblogs-gsm1900.com	2019-07-12, 16:42	2019-07-17, 15:56
www.groupweblogs-gsm1900.com	CNAME	D	2	groupweblogs-gsm1900.com.	2019-07-12, 16:42	2019-07-12, 16:42

What is Passive DNS?

The Domain Name System is designed to provide IP address mappings of domain names, as well as related data such as mail server (MX) records, contact information in the form of Start of Authority (SOA) records, mail disposition rules (Sender Protection Framework or SPF), and more. Each of the record types in DNS can be valuable for forensics, in threat hunting, or incident response operations.

Providers of passive DNS use sensors located around the world to capture DNS replies from authoritative name servers as they answer resolution requests from end-user systems. The records are then added to a database which cross-indexes them for searching and filtering. Certain kinds of information, such as subdomains, can only be accessed at scale through passive DNS.

Passive DNS can help investigators:

- ✓ Discover evidence of DNS tunneling for malware command and control or data exfiltration
- ✓ Identify domains involved in credential harvesting or phishing campaigns
- ✓ Temporally correlate domain hosting with intrusions or other events

Armed with reliable passive DNS data, analysts can learn many valuable things:

- What are all of the domains observed on a given IP address, and when were they hosted there?
- What are the IP addresses that a given domain uses, or has used?
- When did DNS requests for a given domain first appear?
- What are the subdomains tied to a given domain, or observed on a given IP address?

In a threat hunt or incident response investigation, passive DNS data:

- Provides fine-grained correlation of the timing of events such as attacks or breaches with domain and hostname resolutions for malicious infrastructure.
- Produces evidence of unusual DNS behavior such as fast-flux configurations.
- Yields comprehensive context on IP addresses by showing what domains are currently, or were previously, hosted on them. This can help an analyst determine whether an IP is part of a given adversary's infrastructure.
- Can help the analyst decide whether a domain or IP warrants blocking.
- Gives the analyst insight into the nature of a domain by exposing subdomains. For example, domains used as part of credential-harvesting or phishing schemes often use subdomains such as "login," "download," or the name of a legitimate service or company.

Passive DNS in Iris

Iris incorporates passive DNS data as an investigation component, allowing for fast and easy lookups on domains or IP addresses. When an IP address has one or more domains tied to it in passive DNS, those domains can be further explored in Iris to gain insights into threat campaigns and the actors controlling them. Passive DNS is an optional upgrade to the Iris investigation platform.

DOMAINTOOLS®

Test the power of the world's Largest DNS Forensics Database Today.

WWW.DOMAINTOOLS.COM | SALES@DOMAINTOOLS.COM | 206.838.9020