M³AAWG | Messaging Malware Mobile Anti-Abuse Working Group

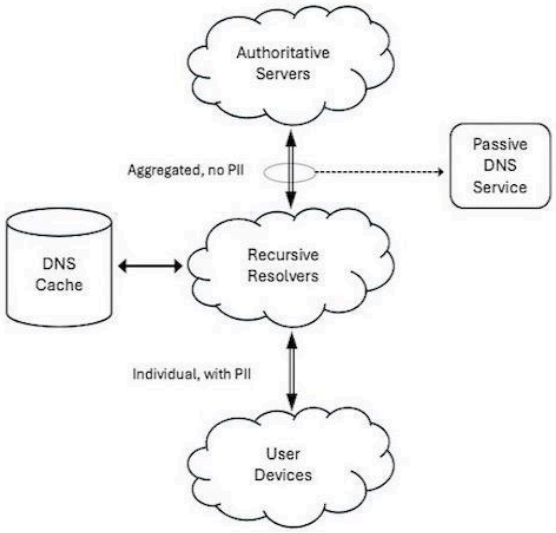
Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Technology Summaries

Passive DNS

What is DNS? The Domain Name System is the internet's phonebook. It's a distributed database that makes it possible for people to use symbolic names (such as "example.org") rather than having to cope with raw numeric IP addresses (such as 203.0.113.220).

What is passive DNS? The term "passive DNS" refers to the process of passively collecting successful DNS lookups and responses. It is called passive because it doesn't involve actively probing the DNS, just logging queries and responses that are organically happening.



What about the user's privacy? Privacy-respectful passive DNS service providers aggregate queries between many large shared recursive DNS servers and authoritative DNS servers (see diagram, right). These aggregated queries are not directly associated with individual users.

Wouldn't encrypted DNS prevent passive DNS traffic collection? No. DNS over HTTPS (DoH) and DNS over TLS (DoT) encrypt the traffic between the recursive resolver and the end-user device. Privacy-respectful passive DNS services collect only the traffic shown above the recursive resolver in the diagram. Privacy concerns are also mitigated due to the aggregation of multiple query sources and other DNS privacy technologies and standards.

Will a passive DNS service really see enough traffic to have complete DNS data? Yes. Passive DNS services will normally arrange to receive query traffic from multiple partner locations worldwide. While some obscure or little-used domains may escape detection, global sensor deployment ensures that most domains that are in active use worldwide will be seen. Some passive DNS services may augment passive collection with active probing or registry zone file data.

How does passive DNS help cybersecurity? Domain name relationships and history can be a rich source of cybersecurity insights. Passive DNS makes it possible to answer questions such as these:

- What domain names share a specific IP address (or address range)? Checking this before seizing a server or blocking a network can help prevent unintentional collateral damage. Conversely, finding domains pointing to the same malicious IP address can uncover larger networks.
- What domain names use the same authoritative name server or mail server? Shared resources may lead to additional related (but previously unknown) abusive domains.
- Where has a domain name been hosted over time? Has a given domain moved around a lot? Domain hosting instability is often a sign that malicious activity may be taking place.
- What DNS entries were modified during a cyber intrusion, potentially by an intruder?
- What domain names have published an SPF record or DKIM keys?
- What domains appear to be targeting banks for phishing or brands in an attempt to sell knock-off products? What domains have been hijacked?