Contribution ID : **26** Type : **not specified**

dnstap-whoami: one-legged exfiltration of resolver queries

Sunday, 4 October 2015 17:00 (15)

A few existing “whoami” or “dnsecho” authoritative DNS services allow for limited extraction of information about the resolver to the original client that would normally be hidden. For example, querying an anycasted resolver like 8.8.8.8 with the command “dig @8.8.8.8 whoami.akamai.net” will return an address record revealing a unicast initiator address used by the anycast service. This is “one-legged”, because the original client only has visibility into the stub/recursive “leg” of the DNS interaction. The DNS-OARC porttest tool is another example of a “one-legged” service.

Similarly, many DNS research projects use special purpose zones with instrumented nameservers which capture incoming query packets for analysis. For example, scans for open recursive DNS servers typically control both the stub/recursive “leg” and the recursive/authoritative “leg” and are thus “two-legged”. This requires a more heavyweight investment but results in a richer set of data.

This talk will demonstrate an enhanced “whoami” authoritative DNS server that can exfiltrate more detailed information about the recursive/authoritative interaction to the original client, including the complete resolver query packet sent to the authoritative server, using the dnstap format to compactly tunnel structured information which can be decoded by the original client.

Summary

Please also consider this submission for the NANOG65 DNS track

Primary author(s) : EDMONDS, Robert (Farsight Security, Inc.)

Presenter(s) : EDMONDS, Robert (Farsight Security, Inc.)

Session Classification : Public Workshop: Resolvers Track

Track Classification : Lightning Presentations