**DNS TXT Resource Records for Command-and-Control Covert Channel**

This document describes the contents of the DNS TXT resource records for command-and-control covert channel and the conditions under which the packets were collected. This dataset was assembled in 2025.

Both text and pcap (pcapng) file types can be opened with Wireshark.

Contact Info: Gavin Hunsinger [gavinhunsinger11@gmail.com](mailto:gavinhunsinger11@gmail.com)

Bruce Hartpence [bhhics@rit.edu](mailto:bhhics@rit.edu)

Daryl Johnson [dgjics@rit.edu](mailto:dgjics@rit.edu)

Bill Stackpole [wrsics@rit.edu](mailto:wrsics@rit.edu)

**DNS Datasets**

The dns\_covert\_chan\_client.pcap and dns\_covert\_chan\_serv.pcap datasets capture DNS traffic from a covert channel that exploits the DNS TXT resource records. The covert channel is established using a Python script running on the client machine, which listens for base64-encoded commands embedded in DNS TXT records sent from the server. The client script decodes and executes these commands, essentially making the client system a remote execution agent controlled via DNS queries.

To maintain continuous operation, a system service is deployed on the Linux DNS client. This service ensures the Python script is always running and ready to process incoming commands from the server, allowing it to act as a persistent agent. As a result, the DNS server effectively becomes a command-and-control (C2) server, distributing commands via the DNS TXT records. The DNS protocol, which is typically used for legitimate domain resolution, is misused for covert data exfiltration and command execution.

To simulate a high volume of DNS traffic in this dataset, the BIND9 server actively instructs the client to perform repeated nslookup queries across various resource records. This is accomplished dynamically on the server by updating the covermessage2.research.net resource record using a Python script. This helps distribute the traffic more evenly and increases the frequency of DNS requests, potentially masking the covert channel's true nature amidst legitimate DNS traffic. By querying different DNS resource records in a balanced manner, the traffic pattern becomes more complex, making detection by simple traffic analysis tools more challenging. Additionally, the command output on the client is sent back to the server via a dynamic update for the response2 TXT resource record.

**Current Capture Files**

dns\_covert\_chan\_client.pcap

dns\_covert\_chan\_serv.pcap

dns\_covert\_chan\_client.txt

dns\_covert\_chan\_serv.txt

**Topology**

The following topology depicts the DNS server that doubles as a command-and-control server and the target device being controlled. The domain that these devices operate on is called “research.net” and TXT resource records within this domain, mainly covertmessage1 and covertmessage2, are used to specify commands that are executed on the dns-client device.

