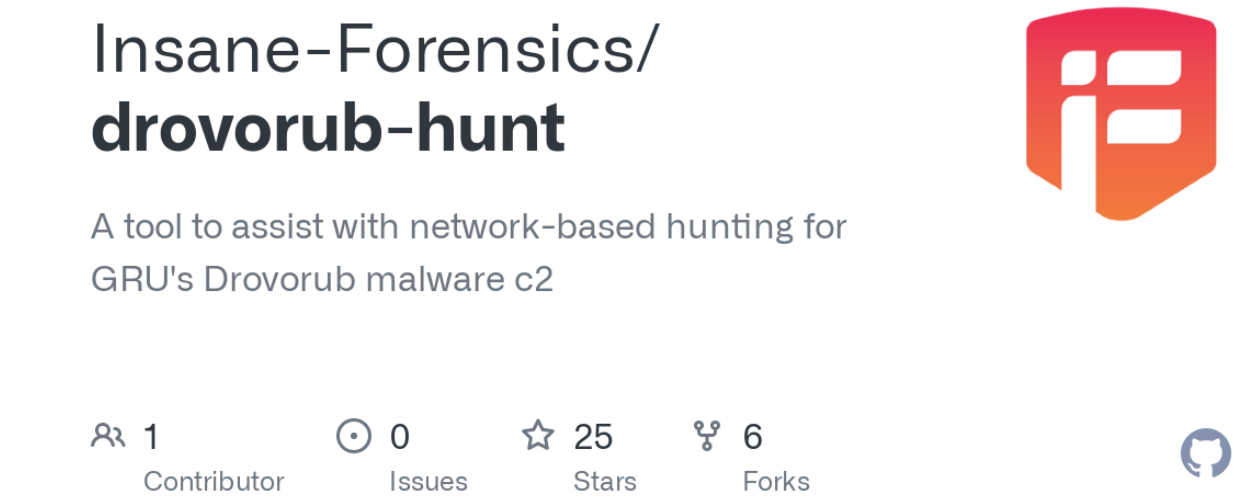
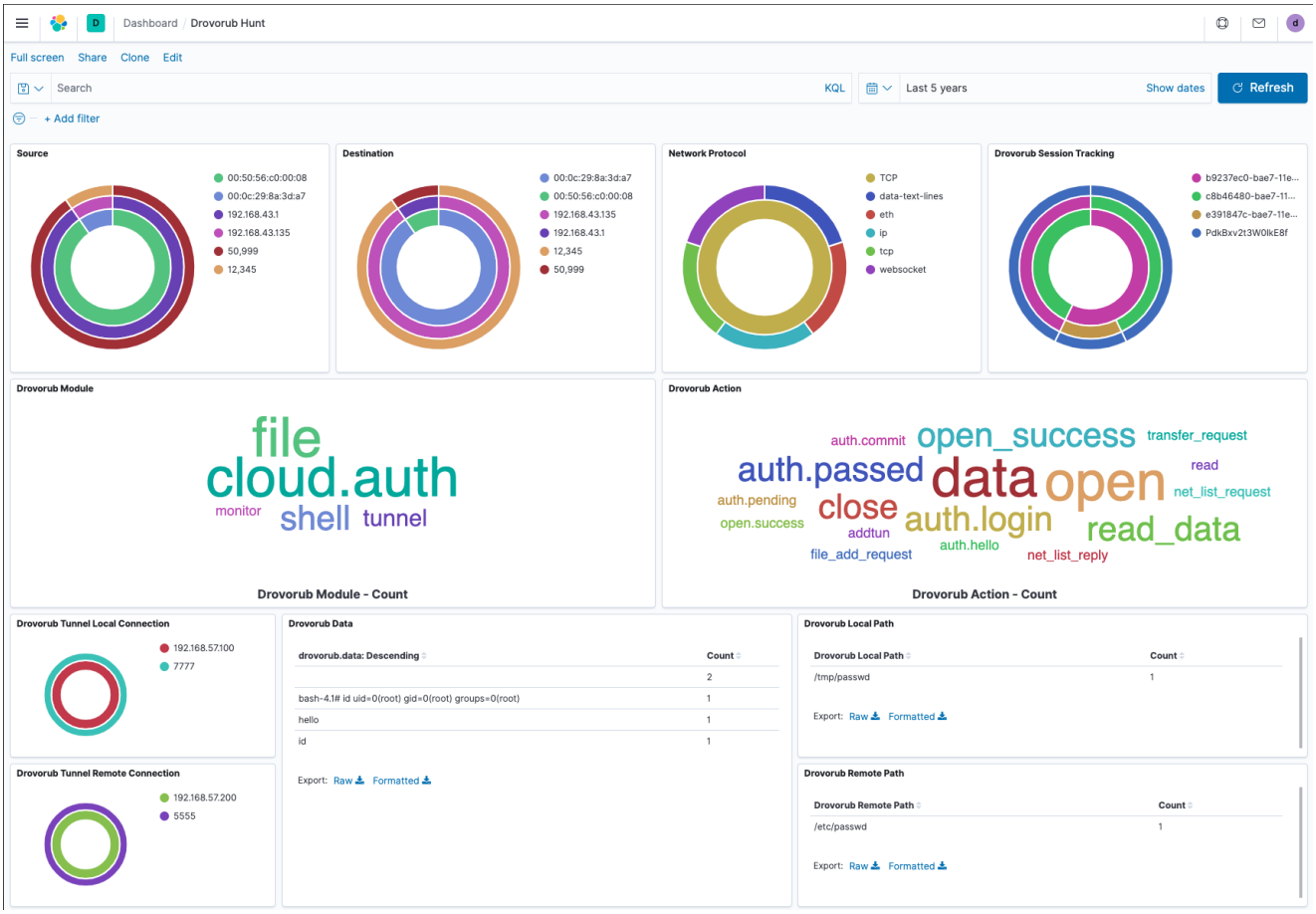
Dispatches from Drovorub: Network Threat Hunting for Russia GRU GTsSS' Malware at Scale

github.com/Insane-Forensics/drovorub-hunt

Insane-Forensics



Recently, the National Security Agency and Federal Bureau of Investigation released a report outlining command and control capabilities leveraged by the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26265 to interfere with the 2016 U.S. Presidential election. While this report contained technical details outlining the malware technologies, the report did not provide a network-scale tool ready for network-based threat hunting. Today, Insane Forensics makes public a free, open source tool to assist with scaled network detection and response for GRUs Drovorub malware using Elasticsearch and Kibana. The provided tool works on existing network captures (pcap files) and also supports live capture mode.



Disclaimer: We built this tool entirely with the NSA/FBI report data. We did not have actual malware samples or packet captures. If you have samples/network captures or can validate this tool with real data, please get in touch.

Included in this Toolkit

- A python script to load previously collected pcap data or listen live on an interface
- Elasticsearch index mapping
- Kibana dashboards for analyst

Requirements

- TShark in environment path
- Elasticsearch and Kibana
- Python3

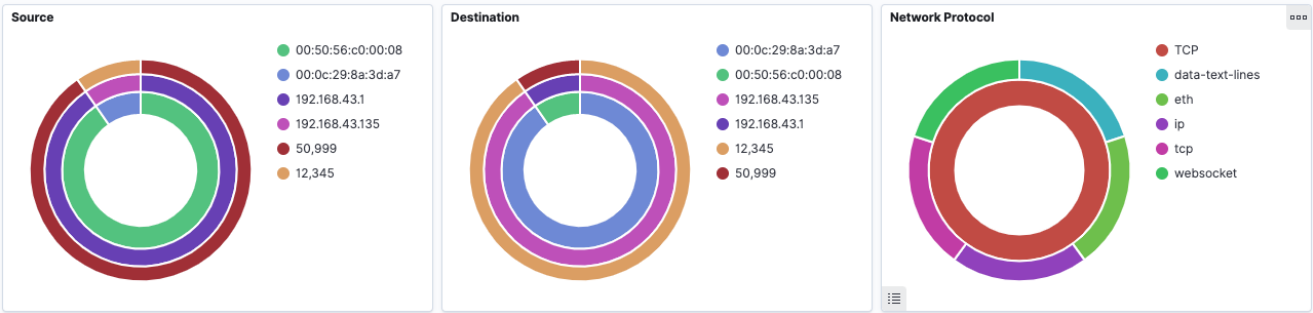
Usage

These instructions are for informational purposes only. Understand variations required for your environment before proceeding

1. Install needed python dependencies using the provided requirements.txt file.
    1. `pip install -r requirements.txt`
2. Create the Elasticsearch index mapping.
    1. We've provided a helper script to assist with this. For our authenticated ELK stack, we used `python3 create_elk_index.py https://<elk ip>:9200 drovorub_test -elk_un <elk username> -elk_pw <elk password>`
3. Add the kibana saved objects (visualizations, dashboards, index pattern)
    1. In Kibana: Management -> Stack Management -> Saved Objects -> Import
    2. Use the provided drovorub_hunt.ndjson
4. Load data to analyze using one of the following options. The elk_un and elk_pw fields should only be used if your elk node uses authentication.
    1. **Packet Capture Mode:** `python3 drovorubhunt.py <elk ip> drovorub_test -elk_un <username> -elk_pw <password> -pcap <pcap file>`
    2. **Live Capture Mode:** `python3 drovorubhunt.py <elk ip> drovorub_test -elk_un <username> -elk_pw <password> -live <interface>`
    3. **Test Data Mode:** `python3 drovorubhunt.py <elk ip> drovorub_test -elk_un <username> -elk_pw <password> -test`. If you use test data, make sure to set the time window back to 2016 as the sample data is from that timestamp. The test data payload comes from the NSA/FBI report screenshots.

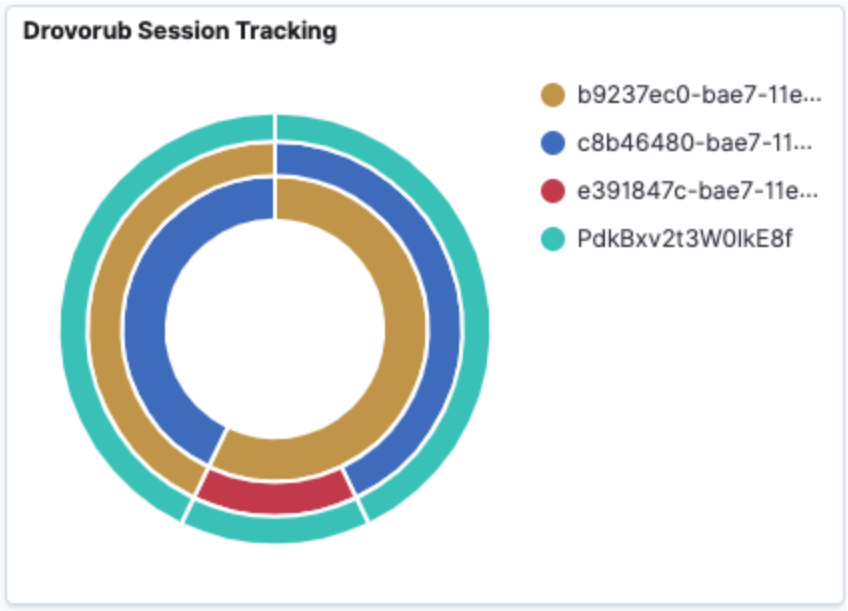
Data Analysis Techniques

The provided dashboard allows for primary hunting and response techniques covering Drovorub's command and control (c2). Drovorub C2 uses the WebSockets protocol outlined in RFC 6455. All WebSocket communications will appear in the source, destination, and network protocol panels of the provided dashboard. We came to this design decision in wanting to allow a wider aperture on potential unknown or undecoded WebSocket communications beyond known communication formats outlined in the report.



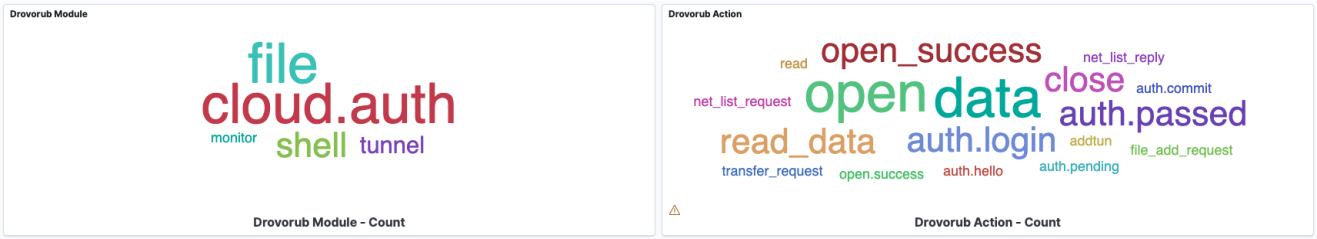
As a network analyst, you should try to understand the difference between healthy and abnormal WebSocket communications in your environment. The innermost ring of the source and destination panes shows the mac addresses of communicating assets. The middle circle shows IP addresses, and the outer ring shows the port. For the network protocol pane, the inner ring shows the transport protocol while the outer ring shows the application-level protocols. You can pivot by clicking on any ring value or the values on the right.

Pivoting by Drovorub Communication Session

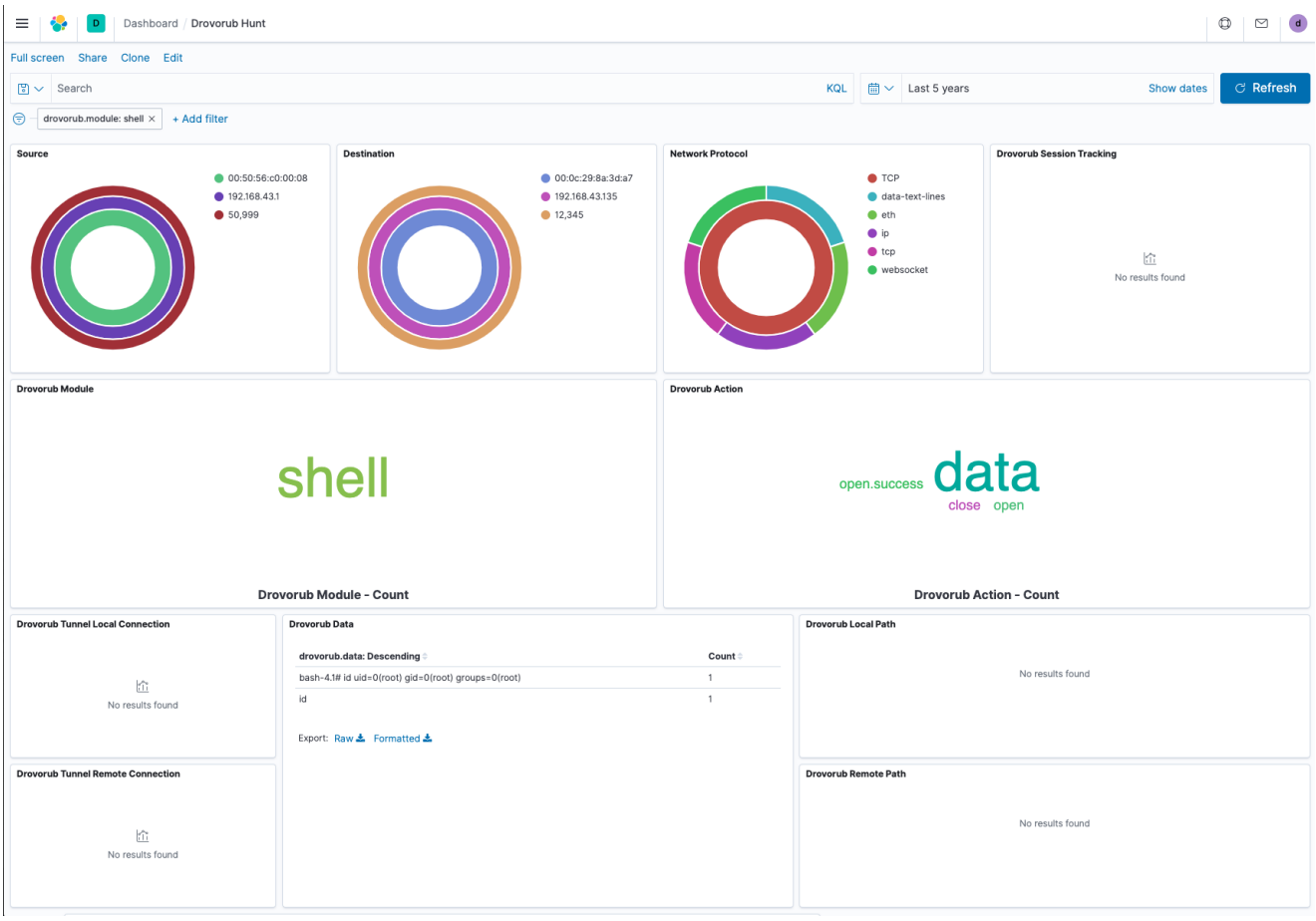


The pane titled Drovorub Session Tracking allows you to pivot between session IDs present in Drovorub C2 sessions. This pane can also show how many sessions are active across your environment and to a single host. The inner ring represents the destination ID, the middle ring represents the source ID, and the outer ring represents the session ID. In the dashboard shown, we see one session between two Drovorub communicating assets.

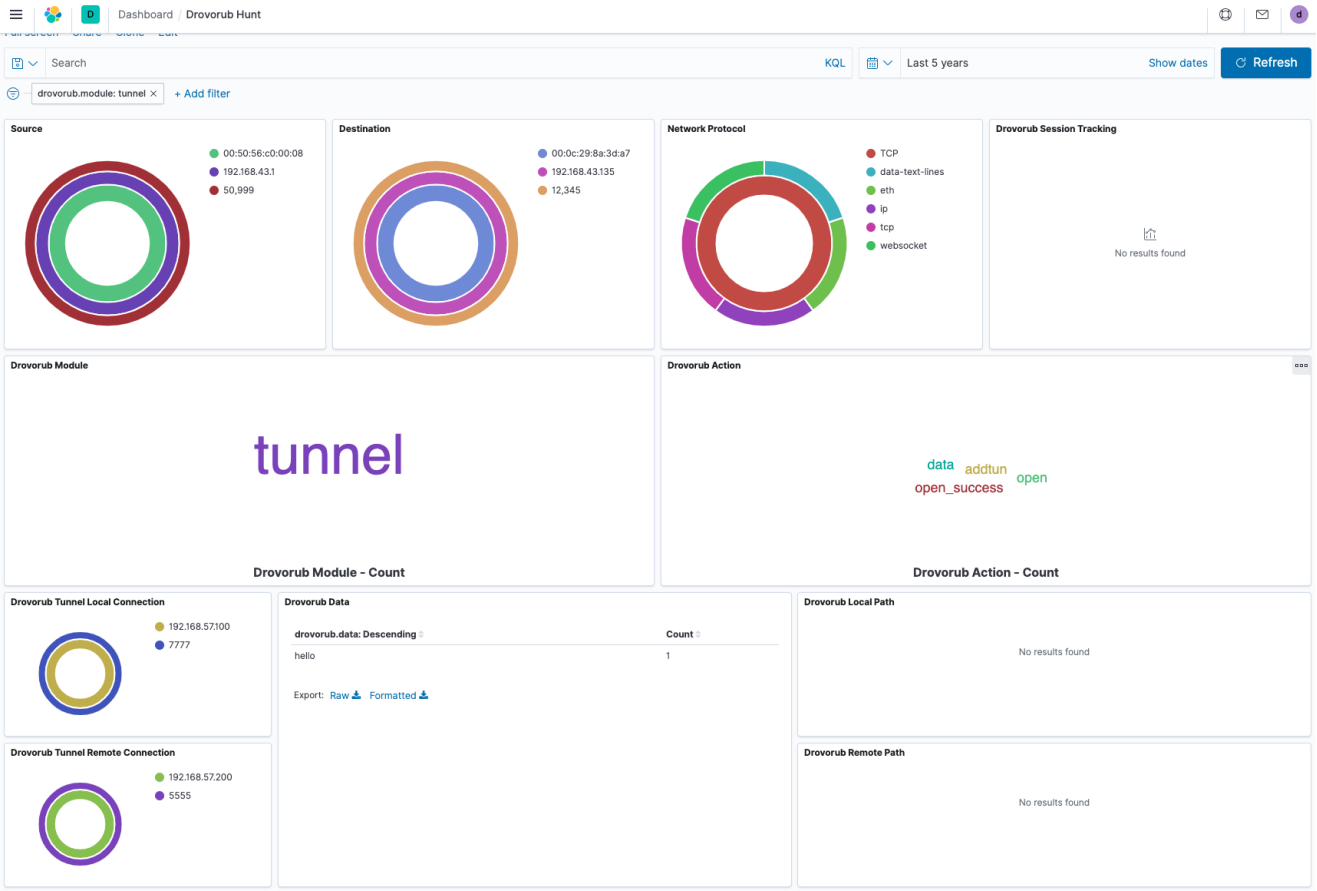
Pivoting by Drovorub Module and Action



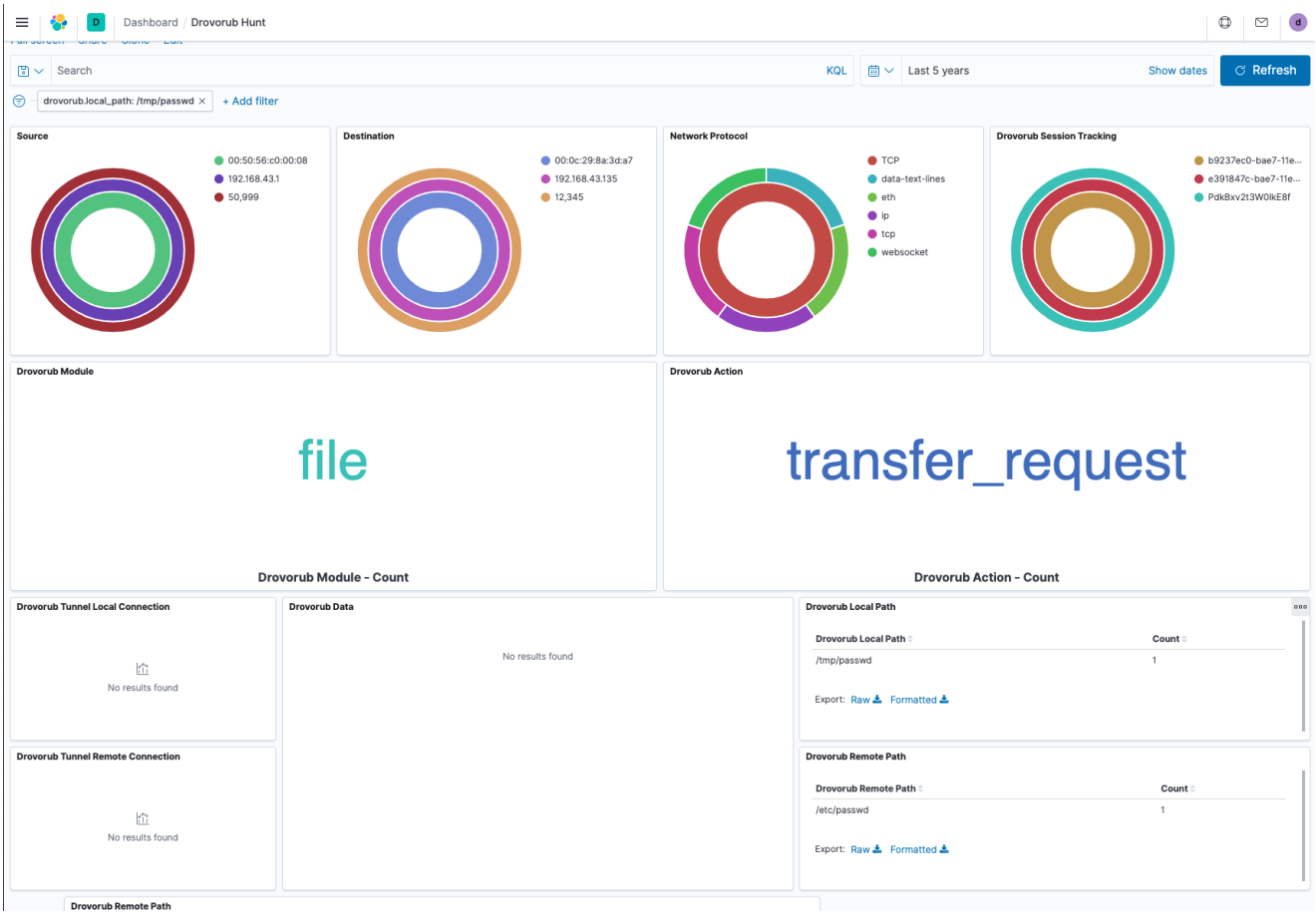
The module and action panes allow you to pivot by the Drovorub module or actions observed. Each panel represents a word cloud of the weighted count of each module or action seen. You can pivot on a particular module by merely clicking on it. Clicking applies a Kibana filter to the entire dashboard. In the image below, the active filter displays Drovorub shell module communication traffic. We can see quickly see shell module traffic between two hosts with a root level command prompt returned in the data field.



Viewing Parameter Data



The rest of the dashboard displays a few parameters for various modules and actions. The tunnel local connection and tunnel remote connection panes above show tunnel information used by Drovorub's tunnel module.



The local and remote path fields show information on what files were requested and where the files moved. In this case, the /etc/passwd file moved to /tmp/passwd.

We Want To Hear From You

If you find this tool useful, need help or want to contribute, please let us know! You can reach us on our website or LinkedIn.