The following pcaps, when replayed with tcpreplay will trigger rules in the current IDS ruleset run by the sensor. These pcaps were provided by ActiveCounterMeasures which reference here: as a source of lab generated malware samples.

The pcaps can be download at the end of each malware page outlining the details of the specific malware:

Signature ID: 2027793, Rule Name: ET MALWARE Covenant Framework HTTP Beacon
PCAP:
https://www.activecountermeasures.com/malware-of-the-day-indicators-of-compromise-lateral-movement-and-backup-c2/

Signature ID: 2009125, Rule Name: ET MALWARE Comfoo Outbound Communication
PCAP: https://www.activecountermeasures.com/malware-of-the-day-comfoo/

Signature ID: 2029741, Rule Name: ET MALWARE Cobalt Strike Malleable C2 (Magnitude EK)
PCAP: https://www.activecountermeasures.com/malware-of-the-day-magnitude/

To use these pcaps to trigger a rule, *tcpreplay* is required. tcpreplay is a tool which will replay the traffic in a pcap onto a specified NIC as if the traffic was live. The easiest way to use tcpreplay to trigger a rule is to run it from the sensor host, it will need to be installed if not already available on the host. tcpreplay should be run as follows:
sudo tcpreplay -i {sniffing interface name} /path/to/pcap

After 5-10 minutes, a new investigation should be visible on the investigations page with the details of the alert.