Introduction to Malware Network Traffic

Malware (malicious software) like users, can generate network traffic. Some types of malware, like worms, are self replicating over network devices. Malware network traffic can create suspicious network traffic that can be detected by network analysts.

Step By Step Guides

How to Detect Malicious HTTP POST Requests (http && frame contains “POST”)

1. Open Wireshark
2. In the search bar type “ http && frame contains “POST””
3. You could also use http.request.method == “POST”
4. Look at the POST Request frames for malicious traffic
5. Look for sql, javascript, file uploads, etc which could indicate possible malicious content.

How to Analyze Suspicious DNS Behaviour (dns.qry.name contains “suspiciousdomain.com)

1. Open Wireshark
2. In the search bar typ “dns.qry.name contains “x”
3. Replace x with a suspicious domain name that has been connected to in the capture.
4. Look at the frames and determine if there are any suspicious downloads from the domain or any possible c2 connections.

How to Identify Beaconing Behaviour (ip.dst == x.x.x.x && tcp.flags == 0x02)

1. Open Wireshark
2. In the search bar type “ip.dst == x.x.x.x && tcp.flags == 0x02”
3. Replace the x’s in with the destination ip address you would like to filter
4. The “tcp.flags == 0x02” portion of the filter filters tcp syn packets.
5. If there are many tcp syn requests within a short period of time or in a consistent interval this may be an indication of beaconing.

Screenshots