MAC Flooding Attack - MACOF:

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - High Volume of Unique MAC Addresses"; detection_filter: track by_src, count 500, seconds 10; sid:3000001;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Rapid MAC Table Exhaustion"; detection_filter: track by_src, count 1000, seconds 30; sid:3000002;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Suspicious Burst of New MAC Addresses"; detection_filter: track by_src, count 300, seconds 5; sid:3000003;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Excessive ARP Traffic"; content:"\x08\x06"; offset:12; detection_filter: track by_src, count 200, seconds 10; sid:3000004;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Broadcast MAC Spoofing"; content:"\xff\xff\xff\xff\xff\xff"; offset:0; depth:6; sid:3000005;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - High Rate of New MAC Registrations"; detection_filter: track by_src, count 400, seconds 10; sid:3000006;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Network Instability Due to Flooding"; detection_filter: track by_src, count 600, seconds 15; sid:3000007;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Excessive Ethernet Frames Per Second"; detection_filter: track by_src, count 1000, seconds 5; sid:3000008;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Unexpected MAC Learning Events"; detection_filter: track by_src, count 500, seconds 20; sid:3000009;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Frequent MAC Table Flushes"; detection_filter: track by_src, count 300, seconds 10; sid:3000010;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Overwhelming Number of MAC Changes"; detection_filter: track by_src, count 800, seconds 10; sid:3000011;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Unusual Increase in Ethernet Traffic"; detection_filter: track by_src, count 900, seconds 15; sid:3000012;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Sudden MAC Address Surge"; detection_filter: track by_src, count 700, seconds 10; sid:3000013;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - ARP Storm"; content:"\x08\x06"; offset:12; detection_filter: track by_src, count 500, seconds 10; sid:3000014;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Unusual Source MAC Randomization"; detection_filter: track by_src, count 750, seconds 10; sid:3000015;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Repetitive Source MAC Usage"; detection_filter: track by_src, count 1000, seconds 10; sid:3000016;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Layer 2 Traffic Saturation"; detection_filter: track by_src, count 1200, seconds 10; sid:3000017;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Massive Number of MAC Frames"; detection_filter: track by_src, count 1300, seconds 10; sid:3000018;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Overflowing Network Switch"; detection_filter: track by_src, count 1400, seconds 10; sid:3000019;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Attack Targeting CAM Table"; detection_filter: track by_src, count 1500, seconds 10; sid:3000020;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Excessive DHCP Requests"; content:"\x35\x01"; offset:240; depth:2; detection_filter: track by_src, count 500, seconds 10; sid:3000021;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Bogus IPv6 Neighbor Discovery Packets"; content:"\x86\xdd"; offset:12; detection_filter: track by_src, count 600, seconds 10; sid:3000022;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Overflowing VLAN MAC Tables"; detection_filter: track by_src, count 700, seconds 10; sid:3000023;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Unusual Spanning Tree Protocol (STP) Traffic"; content:"\x00\x26\x98"; offset:0; depth:3; sid:3000024;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Rapid IGMP Membership Reports"; content:"\x22\x14"; offset:0; depth:2; detection_filter: track by_src, count 400, seconds 10; sid:3000025;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Suspicious BPDU Flooding"; content:"\x00\x00\x0c\x07\xac"; offset:0; depth:5; detection_filter: track by_src, count 300, seconds 10; sid:3000026;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Excessive Gratuitous ARP Packets"; content:"\x08\x06"; offset:12; detection_filter: track by_src, count 800, seconds 10; sid:3000027;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Frequent Layer 2 Readdressing"; detection_filter: track by_src, count 900, seconds 15; sid:3000028;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Anomalous MAC Activity"; detection_filter: track by_src, count 1000, seconds 20; sid:3000029;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - VLAN Hopping Attempts"; content:"\x81\x00"; offset:12; depth:2; sid:3000030;)

alert ether any any -> any any (msg:"MAC Flooding Attack Detected - Unusual MAC Spoofing Behavior"; detection_filter: track by_src, count 1100, seconds 10; sid:3000031;)