Top Abused Top-Level Domains
• .gq
• .cf
• .ml
• .men.tk
• .top
• .work
• .click
• .loan
 	
Malware Hunting Display Filters
• http.request
• http.response
• ssl.handshake.type==1
• dns.qry.name == "*.cn"
• ssl.handshake.type==11
• dns
• tcp.flag eq 0x0002
• tcp.port==3389
	Ports to Watch
	• HTTP = 80
	• HTTPs = 443
	• DNS = 53
	• RDP = 3389
	• FTP = 21
	• Telnet = 23
	• TFTP = 49
	
	Identifying Hostnames
	• udp.port==67 or udp.port==68
	  ○ Option: (12) Host Name
	• bootp
	• Windows: nbns
	• MAC: ip contains MacBook
	• MS ADDS:
	  ○ Kerberos.CNameString
	  ○ !(Kerberos.CNameString contains $)

Blasater Worm:

dst port 135 and tcp port 135 and ip[2:2]==48

Welchia Worm:

icmp[icmptype]==icmp-echo and ip[2:2]==92 and icmp[8:4]==0xAAAAAAAA

Looking for worms calling C2s:

dst port 135 or dst port 445 or dst port 1433 and tcp[tcpflags] & (tcp-syn) != 0 and tcp[tcpflags] & (tcp-ack) = 0 and src net 192.168.0.0/24

Heartbleed Exploit:

tcp src port 443 and (tcp[((tcp[12] & 0xF0) >> 4) * 4] = 0x18) and (tcp[((tcp[12] & 0xF0) >> 4) * 4 + 1] = 0x03) and (tcp[((tcp[12] & 0xF0) >> 4) * 4 + 2] < 0x04) and ((ip[2:2] - 4 * (ip[0] & 0x0F) - 4 * ((tcp[12] & 0xF0) >> 4) > 69))