Table 1: Signatures for Detecting Botnet Attacks

Attack	Type	Signature
5*Flooding	TCP Syn Flooding	alert tcp any any ->any any (flags: S; msg flow: stateless; detection_filter: track by_d
	Smurf Attack	alert icmp any any ->any any (msg: ”ICM ;detection_filter: track by_src, count 1000,
	Large ICMP Packet Size	alert icmp any any ->any any (msg:”MISC classtype:bad-unknown;sid:1000000003; re
	UDP Flooding	alert udp any any ->any any (msg: ”Susp detection_filter:track by_dst,count 1000,sec
	Malicious C&C on Port 80	alert tcp any any ->any 80 (flow:not_estab ”Malicious - C&C on port 80”; sid:100000
2*Downloading	Identifying HTTP Get Method	alert tcp any any ->any any (msg:”GET r content:”GET”;nocase;content:”HTML”;n 1000000009; rev:1;)
	Executable Download	alert tcp any any ->any any (msg:”WGET ”Wget”;nocase;content:”HTTP”;nocase;co nocase;sid:1000000010;rev:1;)
! 5*C&C Communication	IRC	alert tcp any any ->any any (msg:”IRC ch content:”irc”;nocase;sid:1000000011; rev:1
	IRC over HTML	alert tcp any any ->any any (msg:” IRC o nocase;content:”HTML”;nocase;content:”N
	Contineously Sending TCP packets without any payload & bad checksum	alert tcp any any ->any any (flags:0;msg:”
	Detecting Malicious C&C connections on tcp port 6667 with 1) Multiple connection attempts 2) terminated or aborted (i.e proper connection not established at each timestamp	alert tcp any any ->any 6667 (flow:not_est ”Malicious- C&C (at each timestamp)”; si
	W.r.t Source	alert tcp any any ->any 6667 (flow:not_est ”Malicious-C&C w.r.t Source”;detection_fi sid:1000000007;rev:1;)
Brute Force	Multiple Password Attempts	alert tcp any any ->any 22 (msg:”Possible threshold: type both, track by_src, count