Victim Infected Machine **C&C** Server (Bot) ReportServer.UploadDeviceCharacteristics ListeningSocket.Port23+101.Create Socket.EstablishConnection InitialHandler.Check.CNCRegisteredUser == TRUE Else If InitialHandler.Check.NewBotRegistration == TRUE ClientList.AddBot APIHandler.Check.APIKeyValid APIHandler.Check.BotCount < MaxBotCount (\*) UserCommand.PlainText.Receive UserCommand.Parse Bot Command. Byte Array. GenerateIf Targets Not In WhiteList, Attack.Queue Worker().UpdateBotList (RS) **←** Worker().DistributeAttackCommand DDoS.Execute(PacketFlood) **→** (\*\*\*)

(\*) := Sent from Attacker
(RS) := Report Server
(\*\*) := Other Infected Machines (Bot) included
(\*\*\*) := Targeted victim of DoS attack. Can be TCP, SYN, ACK,
HTTP, Valve Source Engine query floods or slow drip DDoS attack
on DNS server, or generated GRE encapsulated Ethernet and IP
packets

Note: C&C communication is NOT encrypted, unlike APTs