+++ BSL UMF – //TS//NOPORN//NONSA +++

Good Evening, Agent. Interpol have asked for our help to investigate and shutdown a notorious botnet controlling many computers around the globe. They have supplied us with a copy of the bot executable which was found on an infected computer.

Your mission, should you choose to accept it, is to investigate the executable and discover the bot's command and control (C&C) infrastructure. Using the information you find, gain control of the botnet and shut it down.

Submission requirements: Submit a write-up to challenges@bsideslondon.org.uk which includes a full description of your investigation and shutdown, including any passwords and server IPs/hostnames. If you use a username of your choice to connect to any servers, then you must include this so that we can verify your submission.

Safety: The bot can be killed from the task manager and then deleted if you no longer wish to continue your investigation. Whilst we have taken reasonable care to eliminate any risk to you from fellow participants, we cannot give an absolute guarantee therefore we recommend that you only run it in a Virtual Machine.

Foul play: The use of port and vulnerability scanning, brute forcing or server 'exploitation' is unnecessary and will result in you being automatically firewalled from the C&C servers.

We have set up a covert back channel to communicate with a deep-cover UMF agent embedded in the crime syndicate we believe is responsible for the botnet. The agent can be contacted, if necessary, via @malforchallenge

As always, should you or any of your U.M. Force be caught or killed, the Director will disavow any knowledge of your actions. This document will self-destruct in five seconds. You *did* disable macros before you opened it, didn't you?