Spamcraft: An Inside Look At Spam Campaign Orchestration

C. Kreibach, C. Kanich, K. Levchenko, B. Enright, G. Voelker, V. Paxon, S. Savage

Published for the Second USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)

Presented by Mark David Spadafora

Summary

- The paper presents a study of spam campaign orchestration. The study was conducted through continuous infiltration of the 'Storm' botnet, this involved collecting data both unobtrusively as well as active injection of data into the Botnet's Command and Control traffic.

Appreciative Comment

- Well conceived 'Two Pronged' data collection.

- The study takes into account several different aspects of spam campaign orchestration, email to/from, templates, dictionaries for generating unique spam, etcetera – a broad and unspecific focus.

- However, as the Data collection is structured into two 'platforms', the '**Command and Control Crawler**' and the **'Command and Control Rewriting Engine**', the two systems can be used together to narrow down on specific aspects of the spam campaign.

- For example, the Crawler works continuously, collecting all campaign data it forwards. For short periods of time the Rewriter injects email addresses which are then in turn picked up by the crawler when they are used in a spam campaign, from this a processing time from harvest to distribution can be deduced.

Critical Comment

- The paper appears to operate under the assumption that the spammers are oblivious to the fact that people may try to infiltrate their network.
- This is a serious shortcoming as without planning an experiment with this in mind, it may become obvious to the target that people are trying to infiltrate, and as such the target may be supplying bogus data.

More on Critical Comment

- For example, consider that all the injected email addresses are distributed by the same array of proxies, which are all on the same network.

- Additionally, consider that the email addresses are of a consistent format:

  'harvest.worker@random.domain'

  all of which are hosted by the same Domain Name Servers and routed to the same mail endpoint sink – this means that any emails that are sent out by the spammers to these injected emails all end up being delivered to the same mail server.

More on Critical Comment

- The previous slide touches on the immediately visible aspects of the described experimental design, and it is seen that there is possibly a signature inherent in the setup that the researchers are using.

- As the researchers show no consideration for possible detection of their experiment, it is likely that there are other issues beneath the surface in their experiment which can also lead to detection that have been overlooked by the researchers. So we cannot really know how reliable the data collected is.

Question

- Given what the article has presented about the architecture of the storm botnet infiltration engine the researchers use, from a bot master's point of view, what methods can you think of to detect the infiltration? Do we even need to?

- (thinking as a spam master allows us to consider how we can improve the research method to avoid detection)