# Click Trajectories: End-to-End Analysis of the Spam Value Chain

**Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Tristan Halvorson, Chris Kanich, He Liu, Damon McCoy, Geoffrey M. Voelker, Stefan Savage[1], Chris Grier, Christian Kreibich, Nicholas Weaver Vern Paxson[2], and Márk Félegyházi[3]**

[1]**Department of Computer Science and Engineering**
**University of California, San Diego**
[2]**Computer Science Division**
**University of California, Berkely**
[3]**Laboratory of Cryptography and System Security (CrySyS)**
**Budapest University of Technology and Economics**

**Review by: Jake Pitkin**

## SUMMARY

Spam-based advertising is a profitable enterprise operating on a global scale. Their products are made visible through the abrasive practice of e-mail spam. The approach is an aggressive and broad distribution of advertisements, with the goal of reaching vulnerable customers. The authors focus on three popular classes of goods: pharmaceuticals, replica luxury goods and counterfeit software. They execute a case study by meticulously examining every stage of the spam value chain and even purchase the advertised products to examine their authenticity.

The spam value chain can be viewed in three distinct stages: *advertising, click support,* and *realization*. Additional forms of advertising exist in the spam industry (sponsored advertising, social media spam and such) but the authors focus on e-mail spam. Click support encompasses the digital infrastructure needed to operate (domain registration, web hosting, name servers, and digital store front management). Finally, realization is the process of processing the customer's payment and fulfilling the order. With the ultimate goal of understanding at which stage intervention would be most successful at disrupting the spam business enterprise.

## IMPORTANCE

This work was the first of its kind to provide strong evidence that payment processing is a bottleneck in the spam value chain. That is, a small number of banks are used for payment processing and intervention at this stage would prove to be more fruitful than intervention elsewhere. If these banks refused to serve the spam business, it would be costly in both time and money for them to form a new merchant account with a new bank. As this operation is global, the authors propose a two-pronged solution to tackle this problem in other countries and in America.

A bulk of the previous literature focused primarily on the *advertising* stage of the spam value chain. By performing an extensive end-to-end study, the authors were able to identify the difficulty to replace each piece in the chain. They show that the affiliations needed for *advertising* or *click support* are cheap and easy to replace when compared to the cost of payment disruption. I find this to be an important advance as it gives direction for future action such as stronger regulation of the banking industry.

## CONTRIBUTION

I found this work to be novel as well as containing the technical depth to back the authors' claims. Their process is documented in great detail and I didn't find any gaps in the description of their processes. They provide the first empirical study to analyze each stage of the spam value chain in depth. An equal amount of attention was provided to each stage as to provide a fair assessment in determining a bottleneck.

## STRENGTHS OF THIS APPROACH

The authors provided the first strong evidence that the spam value chain should be disrupted at the payment level. The collaborative effort of 15 authors provided an impressively detailed and thoughtful approach to evaluating each stage of the spam value chain. I felt no corners were cut in the empirical study and the discovery of a bottleneck at the payment stage can be attributed to that. Additionally, the authors took time to reflect on the ethical elements of their project. This is an element that is often overlooked when conducting a research project.

## WEAKNESSES OF THIS APPROACH

I don't think there is a good reason to not accept this paper. One thing I think would of made the paper stronger would be to expand on the potential approaches for intervention at the payment level of the spam value chain. Exploring options of intervention could be a paper itself though and this is my guess for why this section was slim; the authors focus was on identifying where intervention would be the most effective.

## MOST VALUABLE ASSET IN THE SPAM ECOSYSTEM

The spam value chain can be viewed in three distinct stages: *advertising*, *click support*, and *realization*. Realization entails the process of using a *payment service* (a credit card transaction transferring money between the customer's bank and the merchant's bank) and *fulfillment* of the good. The authors identified that just three banks provided the payment servicing for 95% of the goods in their study. As such, the most valuable asset to control would be *payment services*. Removing these banks as a resource would impact a concentration of spammers and would be a costly hit to their operations.

## CLOSING THOUGHTS

I found this work to be exhaustive and a true end-to-end analysis of the spam value chain. The effort was validated as they found a bottleneck that a large number of spam merchants use for payment processing. I appreciated the level of detail in their data collection methodologies, it allowed me to accept their findings without hesitation.