[14] Get Rich or Keep Tryin' - Trajectories in dark net market vendor careers

Tim Booij (TNO), Thijmen Verburgh (TNO), Federico Falconieri (TNO) and Rolf van Wegberg (Delft University of Technology).

Reviews Phase 1

Review 1

Time: May 25, 12:30

Overall evaluation: 3 (strong accept)

The was a very good empirical paper looking at trajectories in Darknet Markets - well done. You make really interesting use of PGP keys to track providers across sites, and it was nice to see GBTM being used to such effect. Your overall findings are convincing and well-supported. I liked the separation of persistent but unsuccessful sellers from genuinely successful ones - this is a useful and novel finding, which you could even have made slightly more of by drawing from more criminological literature (as it nuances the idea of the 'concentration effect' and suggests that volume evolution over time isn't the only outcome factor). In places the paper was a bit under-referenced but overall acceptably situated in relevant literature. It could be improved by more engagement with the wider criminological literature, but I leave this to the judgement of the authors. The paper's self-evident excellent qualities aside, I now turn to a series of recommendations for improvement - I leave whether or not to incorporate these largely up to the authors.

A particular point - the 'age-crime curve' has a specific meaning and invokes a very large amount of criminological theory developed over decades - what you describe in your article is a much more micro-empirical look at behaviour. I would use 'vendor trajectory' (as they may have been involved in offending of other kinds both pre- and post- your sample) and recommend dropping the idea of the 'age crime curve' entirely from your article as I think it is theoretically unjustifiable. A focus on vendor trajectories is much more illuminating (and this is what you actually do in the empirical work).

Some more minor points - the paper could use a very brief (2 sentence) description of how PGP works in principle and why you can use it in this way. You have a welcome discussion of methods, but perhaps more on methodology - why this collection and analytical approach helps explore the concepts you're interested in and is appropriate. Use of GBTM seems to be fine, but it would be crucial to specify how these timestamps were aggregated - what level of resolution, hour, day, week, month? My own use of GBTM for similar research finds these aggregations are often crucial in determining how (and if!) the model actually converges. Would be good to see even a single sentence stating that you carried out the appropriate distribution testing and that your data meet the criteria for GBTM using the particular distribution model which you used (and some indication of your modelled distribution for each group).

There is a slightly uncritical discussion of 'criminals' and the idea of criminal careers. DNMs are used for a wide variety of products and services, and the different kinds of people selling will presumably have quite different motivations, life histories, etc. Aggregate analysis is justifiable (and well-justified in the piece) but some acknowledgement of the contested nature of the core concepts would be nice.

Discussion of nuances (e.g. ShinyFlakes) is good, but GBTM is quite a useful model as we can scan backwards and use it for prediction - so take the first chunk of a person's career and classify not including the post-intervention section, thus predicting which group they would have ended up in. This causes some problems for your model (i.e. you could have included intervention effects where someone's career terminates in this way due to outside action), but I think these are sufficiently explained for the purposes of the paper and the model retains clear utility.

Policy implications are welcome but slightly undercooked - surely targeting only the big fish would create openings for the small fry? If their exit from the market is due to being outcompeted then assuming that they would follow the same trajectory in the absence of bigger competitors is hard to support. One could equally argue that no arrests at all would be the best approach for ensuring that these smaller actors drop out of the market before they have a chance to progress on to more serious offending.

Overall, though, I leave the inclusion or incorporation of these points in the hands of the authors. This was an excellent paper and clearly one for inclusion in WACCO.

Reviewer's confidence: 5 (expert)

Review 2

Time: Jun 11, 02:28

Overall evaluation: 3 (strong accept)

This innovative and informative paper provides a methodology, a tool and descriptive statistics to analyze the career trajectories of darknet market vendors. It relies on the use of PGP keys by vendors to move seamlessly between markets to estimate the length of their careers, and the ratings received after each transaction to evaluate their criminal performance. For the first time, we are able to get a more precise idea of the size of the cybercrime ecosystem fuelled by 80 darknet markets and the profits generated by three types of offenders: established vendors, "challengers", and failed vendors. We discover the structure of this ecosystem and the small number of highly successful vendors (50 vendors or 2% of the population) who account for almost a third of revenues.

The contribution of this paper is significant and justifies my strong accept decision. The comments below are merely questions or suggestions to clarify the paper:

1. What were the patterns of activity across markets for each category of vendors? Did vendors succeed more by being active across a large number of markets, or on the contrary by focusing on niche segments where they could establish their business? 2. How do the authors explain the overlap across categories in terms of revenues at the extreme ends of the range of profits? For example, the highest-grossing "challenger" earned more than the highest-grossing established vendor. The most successful "failed vendors" also generated a significant amount of revenue. It would be helpful if the authors could reflect on those zones of overlap between the three categories. 3. Have the authors considered that some vendors operate on a full-time basis while others might be part-timers who have a limited interest in moving to a full-time commitment? Might this explain the longevity of challengers who might be just where they want to be and may feel their minimize the risk exposure to police arrest? 4. Why have the revenues not been used to build the model? I am not sure I understand, and it would be helpful to justify this decision. 5. Is there a correlation between the diversity of products offered by vendors (or certain categories of products offered) and the criminal performance of vendors? This would be interesting and may seem possible based on my understanding of the data. 6. The policy implications are stimulating, but I would also have been interested to read about future research opportunities: what other research questions may this dataset and data collection tool help us answer? Could this research be conducted in the current darknet environment? What may have changed since 2015?

Some additional typos picked-up along the way: p. 3, title III: Measurement Methodology (instead of Ethodology) p. 8, 3rd paragraph, "who publish not their own..." (instead of there) p. 9, 3rd paragraph, "from burglars to homicides." (instead of homocides)

Reviewer's confidence: 5 (expert)

Rebuttal Letter

Dear chairs, reviewers,

We would like to thank the reviewers for their positive feedback, thoughtful comments, and efforts towards improving our paper. In the following, we highlight our thoughts on the comments and additions proposed by the reviewers.

Both reviewers suggest similar additions to distinct parts of the paper. A basic description of how PGP keys work, an explication of the distribution testing of our GBTM model, an explanation on the profit ranges, and a short elaboration on the possibility of 'part-time' criminals. Likewise, we will explicitly elaborate on our choice not to use revenue for the creation of the different vendor groups, and sharpen the policy takeaways on the point raised by Reviewer 1.

Besides this, Reviewer 1 raises the interesting point of evaluating interventions employing the GBTM model. We feel a lot of interesting additional questions can be answered by such an analysis. However, we think that such an approach would require a lot of additional research and would be a different paper altogether. Yet, we will touch upon this in the future work section.

Reviewer 2 raises the question if there is any diversification in activity on other markets between the vendor groups. We agree this is indeed very interesting, and we will add an additional analysis to answer this question. Furthermore, Reviewer 2 asks if there is diversity amongst products offered by the vendors. We have performed an analysis to look into this question. We did not incorporate this in the initial version of our paper, but we will add a subsection on this point in the final version of our work.

Again, we would like to thank our reviewers for their positive feedback and thoughtful comments. We are looking forward to presenting our final work on the 3rd Workshop on Attackers and Cyber-Crime Operations.

Reviews Phase 2

Review 3

Time: Jun 29, 14:49

Overall evaluation: 3 (strong accept)

This paper combines known individual techniques in a new way to piece together more of the cybercriminal careers. The authors then continue to analyse the possible careers and explain how these different groups develop throughout the years in the dataset.

This seems a well-written paper, with a strong contribution to the field.

spelling comments: * section III should be called Measurement Methodology * page 8: should be "_their_ own public PGP-keys"

Reviewer's confidence: 4 (high)

Review 4

Time: Jun 30, 21:16

Overall evaluation: 3 (strong accept)

I read the paper with interest and I think it is well written and interesting. It addresses a challenging problem of evolution of dark markets actors (most studies are spot in time). I did not review the initial submission but I saw the rebuttal document and I think the paper is of sufficient quality for the conference.

Reviewer's confidence: 5 (expert)