How is Cybercrime Evolving?

Journal of Strategic Threat Intelligence

Abstract

Firms spend enormous resources on digital advertising and promoting their brand online. In the meantime, ad-fraud undertaken by cybercriminals cost $42 billion in 2019 and could reach $100 billion by 2023. However, while digital advertisers continue to wrestle with how to effectively counteract ad-fraud, the topic of advertising fraud itself has received little academic attention. Here, we investigate this gap between practice and research through an exploration of ad-fraud communities. Our research implemented a multimethod approach for data collection in a longitudinal (18 months, October 2017 to April 2019) online investigation of this phenomenon. Integrating qualitative and quantitative analysis, we examined (1) internal interactions within ad-fraud communities and (2) ad-fraud communities' performance and growth. Our online investigation extends our conceptual understanding of ad-fraud and explains how ad-fraud communities innovate. Our findings indicate that capabilities enacted by some communities foster requisite variety and enable the coordination of complex, iterative, and incremental dynamics (cocreation of artificial intelligence-based bots, customer involvement, and reinforcing capabilities). This research has both theoretical and practical implications for innovation in cybercriminal communities. Furthermore, we provide practical guidance for policy-makers and advertisers regarding how to improve their response to business threats. Indeed, a better understanding of how ad-fraud communities innovate enables organizations to develop countermeasures and intelligence capabilities.

Highlights

- This is one of the first studies documenting the way ad-fraud communities innovate and create value for their criminal customers.
- A multimethod approach was applied for data collection, integrating qualitative and quantitative assessment of six cybercriminal communities.
- Specialized ad-fraud communities provided a wealth of knowledge and incremental innovations in ad-frauds.
- General and customer-oriented ad-fraud communities showcased the most internal interactions, as well as exhibiting better performance and growth.
- General and customer-oriented ad-fraud communities have developed specific capabilities, focusing on innovation through artificial intelligence, which fuels customer engagement and fosters (criminal) attractiveness.

Reference

Richet, J.-L. 2022. “How Cybercriminal Communities Grow and Change: An Investigation of Ad-Fraud Communities,” *Technological Forecasting and Social Change* (174), p. 121282. (https://doi.org/10.1016/j.techfore.2021.121282)