Example

(Underground Ecosystems.) Several ecosystems and market places of a malicious nature have been studied in the literature via captured datasets. Stone-Gross et al. analyzed credential stealing malware [29] and spam botnets [14] by taking over part of the botnet infrastructure to understand their inner workings. Wang et al. studied SEO campaigns to sell counterfeit luxury goods and the effectiveness of various interventions to combat such activities [30]. Alrwais et al.[34] investigate illicit activities in the domain parking industry by interacting with the services to collect ground truth data. Christin [31] analyzed the Silk Road marketplace by running daily crawls of its webservices for 6 months to understand merchants, customers, and what was being sold. A followup study by Soska and Christin [32] examined 16 anonymous market places also by periodically crawling their webservices and found that marketplace takedowns may be less effective than pursuing key merchants that may migrate to others. Another followup study by Wegberg et al. [33] augments previous studies by examining evidence for commoditization of entire cybercrime value-chains in underground marketplacesand finds that only niche value-chain components are on offer.

Datasets on the underground can also be leaked by criminal competitors. McCoy et al. used leaked databases of three affiliate programs to study pharmaceutical affiliate programs[15]. More recently, Brunt et al.[35] analyzed data from aDDoS-for-hire service and found that disrupting their reg-ulated payment channel reduced their profitability but thatthey were still profitable by switching to unregulated cryp-tocurrency payments. Hao et al. [16] analyzed a combinationof leaked and legally seized data to understand the ecosys-tem for monetizing stolen credit cards. Our dataset resulted from the aftermath of the legal takedown of the BPH provider MaxiDed. To the best of our knowledge, there has been no prior academic work on BPH using such ground-truth data. Our study uniquely provides a comprehensive picture of thesupply, demand and finances of the entire BPH operation.

(Bulletproof hosting.)Earlier efforts on detecting BPH have relied heavily on identifying autonomous systems.Fire [9] was one of the first systems for detecting BP ASes by temporally and spatially aggregating information from multiple blacklists in order to detect elevated concentrations of persistent abuse within an AS’s IP blocks. Shue et al. [36]noted that BP ASes often fast-flux their BGP routing informa-tion to evade detection. ASwatch [11] leveraged fast-fluxing BGP routing as strong indicator of a BP AS to build a clas-sifier and detect BP ASes before they appear on blacklists. Others have developed security metrics to compare concen-trations of abuse on various hosting networks and to identify negligent providers that may be suspected of operating BPHservices [37, 38], while Tajalizadehkhoob et al. developedtechniques to analyze abuse concentration on the hosting mar-ket as a whole by identifying providers from their WHOISinformation rather than BGP data [39]. BPH however, has evolved over time. Alrwais, et al.[5] studied a recent approach of BPH abusing legitimate hosting providers through resellerpackages to provide a more agile BP infrastructure. Our work complements this work by providing a unique perspectiveinto to the the ecosystem of BPH. Based on our analysis, wecan better reason about which mitigation techniques might be effective and which are likely ineffective for underminingmodern agile BPH marketplaces