Botnet business models, takedown attempts, and the darkweb market: a survey

DIMITRIOS GEORGOULIAS, Aalborg University, Denmark
JENS MYRUP PEDERSEN, Aalborg University, Denmark
MORTEN FALCH, Aalborg University, Denmark
EMMANOUIL VASILOMANOLAKIS, Technical University of Denmark, Denmark

Botnets account for a substantial portion of cybercrime. Botmasters utilize darkweb marketplaces to promote and provide their services, which can vary from renting or buying a botnet (or parts of it), to hiring services (e.g. distributed denial of service attacks). At the same time, botnet takedown attempts have proven to be challenging, demanding a combination of technical and legal methods, and often requiring the collaboration of a plethora of entities with varying jurisdictions. In this article, we map the elements associated with the business aspect of botnets, and utilize them to develop adaptations of two widely used business models. Furthermore, we analyze the 28 most notable botnet takedown operations carried out over from 2008 to 2021, in regard to the methods employed, and illustrate the correlation between these methods and the segments of our adapted business models. Our analysis suggests that the botnet takedown methods have been mainly focused on the technical side, but not on the botnet economic components. We aim to shed light on new takedown vectors and incentivize takedown actors to expand their efforts to methods oriented more towards the business side of botnets, which could contribute towards eliminating some of the challenges that surround takedown operations.

CCS Concepts: • **Security and privacy** → **Economics of security and privacy**.

Additional Key Words and Phrases: cybercrime, botnets, economics, business models, attacks, takedowns, marketplace, forum, darkweb

ACM Reference Format:
Dimitrios Georgoulias, Jens Myrup Pedersen, Morten Falch, and Emmanouil Vasilomanolakis. 2022. Botnet business models, takedown attempts, and the darkweb market: a survey. 1, 1 (December 2022), 37 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Cybercrime is a constantly increasing threat to the digital world [38, 125]. Attackers are evolving their methods of operation and defenders are trying to adapt to these methods, to effectively counter them. It is a never ending cycle, a cat-and-mouse game [39, 103], with data suggesting that the defenders are on the losing side, always being a step behind [12, 20, 93]. One of the main reasons behind cybercrime' s constant evolution, is the economic incentive. Cyber criminals are motivated by profit to keep coming up with new ways to carry out their operations and evade the authorities' detection, defense and disruption attempts. The revenue of each cybercrime enterprise is proportionally linked to its ability to conduct its business uninterrupted and to the maximum potency possible. The smoother and more impactful the operations are, the more profit the organisation will eventually produce.

Authors' addresses: Dimitrios Georgoulias, Aalborg University, Copenhagen, Denmark; Jens Myrup Pedersen, Aalborg University, Copenhagen, Denmark; Morten Falch, Aalborg University, Copenhagen, Denmark; Emmanouil Vasilomanolakis, Technical University of Denmark, Kongens Lyngby, Denmark.

Manuscript submitted to ACM

Cybercrime actors have the option of utilising their resources privately or providing them as a product/service for a fee to potential clients, known as Cybercrime-as-a-Service (CaaS). These clients can simply go online, access marketplaces both in the clearweb and the darkweb, and choose from a large variety of services. This leads to cybercriminals operating under an "as-a-service" model [62, 127] and essentially turning their collective operations into a business industry. An individual or organisation can build their business around a wide range of services that, depending on their nature, can be provided through various pricing models.

1.1 Botnet Background

The Internet Chat Relay (IRC) protocol is considered as the origin of botnets. Bots were initially benign and used by the protocol to provide services and support. The first IRC bot was created in 1993, under the name Eggdrop [26, 106, 124]. Eggdrop was then further developed, and soon malicious bots made their appearance. These bots' purpose was to attack other IRC users or even whole servers, which in time resulted in these bots being engineered to be able to carry out Distributed Denial of Service (DDoS) [72] attacks. Nevertheless, the first botnet that managed to gain public attention was the *Earthlink Spammer* [35], which surfaced in 2000 and had been created by Khan K. Smith. The botnet managed to send over 1.25 million malicious emails in one year's span, with the purpose of collecting sensitive information from users, such as credit card credentials. The number of botnets has increased to a significant degree since then, leading to various types of botnets, categorized based on certain characteristics.

In essence, botnets are devices infected by malware which allows them to be controlled by an individual other than the legitimate owner, called the botmaster. They can be used for a variety of purposes [71], the main ones being *information gathering* [25], *distributed computing* [129], *cyber fraud* [29], *spreading malware*, *cyberwarfare* [22, 140], *unsolicited marketing* [130], *network service disruption* [72], and *cryptojacking* [37, 96].

In addition to purpose, another point of differentiation amongst botnets is their architecture, which varies depending on the mechanism used to disseminate the botmaster commands throughout the botnet. There are three basic architectures: *centralised*, *decentralised* and *hybrid* [124] (see Figure 1). In a *centralised* architecture the bots receive the botmaster commands through one or more Command and Control (C&C) servers. In this scenario the C&C servers are the backbone of the infrastructure, providing coordination to the bot army, and the main protocols used are IRC and HTTP. In a *decentralised* architecture this task is carried out using a Peer-to-Peer (P2P) protocol, with all of the bots contributing to the coordination of the bot network by disseminating commands[1] to their peers [56, 143]. Lastly, in a *hybrid* architecture, the dissemination mechanism is a combination of the two aforementioned architectures. An example would be a botnet using multiple C&C servers, tasked with handling a specific number of bots, which are communicating though P2P. Each architecture presents its own pros and cons. The fundamental advantages of the centralized architecture, are its speed and simplicity; however, it lacks in resilience due to the fact that the C&C servers are potential points of failure. The decentralized and hybrid architectures are more complex to implement but provide a higher level of resilience against takedown attempts.

Maintaining a healthy bot supply is a priority for botmasters. This is where the propagation mechanism comes into play. There are two major families of mechanisms tasked with the propagation of the bot malware: *active* and *passive* [71]. Active propagation is achieved mainly through scanning, where the infected devices search for new potential hosts, without the need of human interaction. Passive propagation on the other hand, requires a certain level of human interaction, with *Drive-by Download*, *Infected Media*, and *Social Engineering* as the main mechanisms utilized [71].

[1]In this case, due to the lack of C&C servers, the botmaster can instead connect to one of the bots to issue the commands, which will gradually spread via P2P to the rest of the botnet.

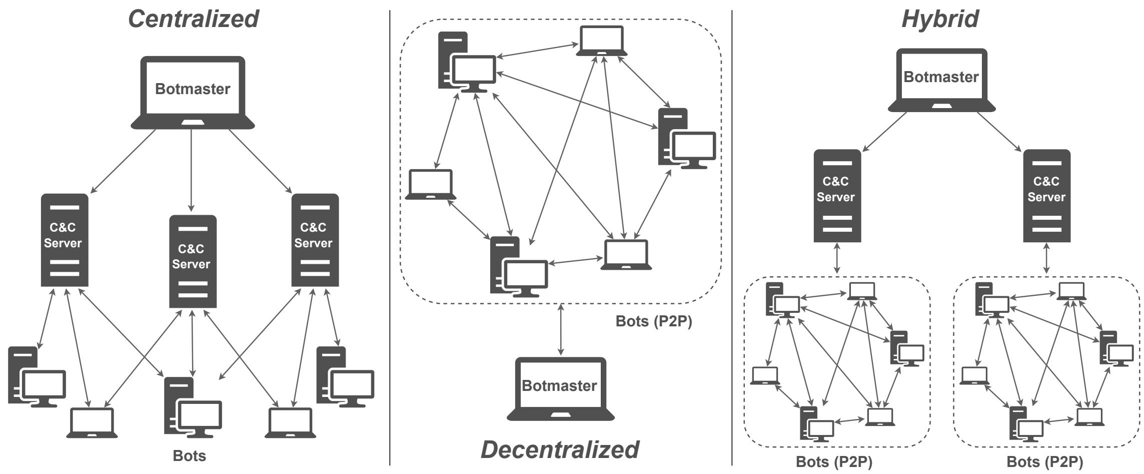

Fig. 1. Examples of the *Centralized*, *Decentralized*, and *Hybrid* botnet architectures.

Stealth is always critical when running any illegal enterprise. Botmasters are using a variety of methods, like Bulletproof Hosting Services (BPHS) [6, 54] (see Section 3.2.1) and fluxing techniques [7, 71], that aim to obfuscate the C&C server(s). These methods provide takedown resilience to botnets, since they make locating the C&C server a challenging task for takedown actors. Furthermore, many botmasters, have started utilising the darkweb, and specifically the Tor network [7], aiming to provide increased stealth to their operations. The way they achieve this is by using a Tor *Hidden Service (HS)* [139] as the C&C server, a service which can only be found inside the Tor network and only if someone possesses the unique address of the service, known as the *Onion Address*. This infrastructure provides even greater resilience to the C&C server. However, the darkweb is not only being used for C&C obfuscation purposes. It also serves as the most popular marketplace for botmasters to advertise and provide their services through HSs, and that is mainly thanks to the anonymity that it provides to potential users – clients. The combination of cost effectiveness and resilience, has led to botnets turning into a very successful market, where someone can buy a whole botnet infrastructure, rent one (or even parts of it) or acquire the services of one (e.g. attacks) [62, 113].

The reason why botnets are so widely used by cybercriminals is because they can be inexpensive to deploy while being effective, turning them into one of the most common threats on the Internet for many years [35, 38]. In the hands of a malicious user, they can be a source of significant financial harm, contributing to cybercrime amounting to billions of dollars in damages annually and specifically closing in on $1 trillion in 2020 [125]. Additionally, in recent years, Internet of Things (IoT) botnets have been on the rise, with *Mirai* [8, 72] being a prime example, making matters even worse by providing new bot supply sources for botmasters. These types of botnets are networks of devices like smart watches, cameras, medical sensors and smart refrigerators, adding to the recruitment potential of botmasters.

With so many options being available to botmasters in regard to bot assimilation and coordination, obfuscation of their operations, as well as selling platforms, takedown operations are bound to face many challenges (see Section 4.3). These challenges can be technical, legal [32, 146], or related to jurisdiction, since in most cases botnet architectures tend to be spread over different countries. To counter the elusiveness and resilience of botnet operations, in many occasions several organisations (e.g. law enforcement agencies, large corporations, legal authorities) will pool their resources together, to increase the effectiveness of takedown attempts. This approach has proven fruitful over the years, but demands careful coordination.

1.2 Article contributions

The topic of botnets is widely popular among researchers, a fact that has lead to notable work on several of their aspects, namely their use purposes, architectures, defence, detection, evasion/obfuscation, as well as research focusing on their economic elements (see Section 5.) We argue that due to the state of the botnet ecosystem there is promise in further researching the economic infrastructure of botnets. Their operation, which resembles that of a legitimate online business, follows certain business models. Researching those models provides insight on how the botnet economy operates internally. In this article, we explore the financial ecosystem of a botnet business, map its components by developing two adaptations of the *Value Chain Model* and the *Business Model Canvas*, and analyse how this ecosystem can be correlated to takedown attempts performed against 28 botnets from the year 2008 and onward. To the best of our knowledge, this is the first work following such an approach. The ultimate goal we aim to contribute towards are economic disruption methods, which can be a valuable addition to the arsenal of botnet takedown operations. Such methods would eliminate various challenges these operations often face, such as legal issues, technical issues (e.g. reverse engineering of the botnet malware), or issues related to the jurisdiction of the entities involved [32, 146] (see Section 4.3). Hence, the identification of weak points in the botnet business models that are directly related to revenue generation, and their exploitation, can prove to be a very efficient tool in the fight against botnet cybercrime, by striking at the heart of the botnet cybercrime, namely the generation of profit. Hindering the mechanisms that operate under the revenue making umbrella, would gradually take away the botmasters' incentives, by making their efforts not worth the risks that accompany running a cybercrime enterprise.

The contribution of this work can be summarized in the following points. In this paper we:

- illustrate how the *Value Chain Model* and the *Business Model Canvas* can be used to map out the elements of a botnet infrastructure operating as a profitable business, leading to the development of two adapted models,
- analyze takedown attempts against 28 botnets from 2008 until 2021, in terms of takedown methods utilized, and illustrate the correlation between these methods and our adapted models,
- explore the technical, legal, and jurisdictional challenges that surround botnet takedown operations,
- provide insight on potential directions for future botnet takedown operations.

1.3 Methodology

The first step in our process for this work was gathering scientific research papers suitable to provide background information on botnets, covering several of their aspects (e.g. architectures and detection methods) (see Sections 1 and 5). Surveys and taxonomies on botnets, with a high scientific contribution, were a valuable source for this information.

Secondly, after choosing to utilize Michael Porter's *Value Chain Model* [108] and Alexander Osterwalder's *Business Model Canvas* [102] because of their popularity and wide application, with the goal of mapping out the elements of a botnet as a business, we explored the authors' original work, as well as available online resources, such as articles on economics which elaborated on the two models' implementation.

The next phase was dedicated to research on the specific topic of botnet economics (see Section 5.2), which also included work gravitating towards the development of disruption methods, with elements related to economics as their foundation. In order to create an archive of papers to review on this subject, we carried out a literature review on the basis of keywords and phrases such as *"botnet economics"*, *"botnet disruption"*, and *" botnet takedown"*.

The fourth step incorporated analyzing past botnet takedowns since 2008, in terms of the methods used, the entities involved, as well as the characteristics of each botnet (e.g. size and impact) (see Section 4), which was achieved though scientific papers and online articles available on the websites of organisations participating in the takedown operations, such as law enforcement agencies (e.g. Europol), large enterprises (e.g. Microsoft), and non-profit cyber security organisations (e.g. The Shadowserver Foundation). Articles on widely popular websites related to cyber security (e.g. Krebs on Security), worldwide news agencies (e.g. BBC) and newspapers (e.g. The Guardian), also contributed to completing this task.

Last but not least, these same resources were also utilized to examine the difficulties that surround botnet takedown operations, which can be of legal, ethical, or technical nature, as well as related to the jurisdiction of the takedown actors (see Section 4.3). Analysing past botnet takedowns along with the accompanying challenges of these operations, provided the necessary insight needed to create the link between takedown efforts and the business models applied by botnets, but also led to observations regarding the potential course of action in future takedown operations.

1.4 Outline

The remainder of this article is as follows. At the end of this section, we present the methodology used to carry out this survey. In Section 2, we give an overview of cybercrime's evolution, darkweb marketplaces and forums, and two economic models that can be applied to cybercrime operations. In Section 3, we present our implementations of the *Value Chain Model* and the *Business Model Canvas*. Section 4 is dedicated to botnet takedown efforts, how they can be correlated to economic models, the challenges that surround takedown operations, as well as potential future steps. In Section 5, we report notable existing research on botnets, as well as on the specific topic of botnet economics. Lastly, in Section 6, we summarize this survey and discuss the main takeaway points.

2 CYBERCRIME AS A BUSINESS

In this section, we are discussing the phenomenon of cybercrime over the years, darkweb marketplace and forum utilisation by cybercrime actors, their impact, as well as efforts made towards taking down these platforms.

In the earlier days of cybercrime, the communication between cybercriminals and potential clients, was mainly carried out using the IRC protocol [11], [33]. IRC would serve as a marketplace where clients could visit various channels and acquire the service of their choosing. Channels were also used for internal communication between the cybercrime actors and aspiring hackers, some of which are still operational [33], [58]. Along with IRC channels, presently there are dedicated websites and forums, which clients can simply visit though their browser, providing higher ease of access. After establishing communication, further contact with the vendors, can include other means, such as the instant messenger application *Wickr*, which has lately emerged as very popular, the encrypted mail service provider *ProtonMail,* or other platforms such as *Google+, Telegram, ICQ, Facebook, Twitter, AIM, Jabber, Reddit, Signal*, and *WhatsApp* [36, 92].

2.1 Darkweb Marketplaces & Forums

The darkweb is an Internet overlay network that requires special software to access, has special configuration and access authorization, and it is a subset of the Deep Web. The Deep Web can be described as every part of the Internet that is not accessible to the average user and it represents around 96% of the overall Internet. Apart from providing anonymity to legitimate users, the darkweb can be abused by cyber criminals to perform illegal activities as well. Over

Market	Icarus Market	Canada HQ	Dark0de Reborn	Deep Sea Market	White House Market	Dark Market	ToRReZ Market	The Versus Project	Monopoly	Neptune Market	Hydra Market
Forced PGP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
2FA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Payment methods	BTC, XMR, Litecoin	BTC	BTC, XMR	BTC	BTC, XMR	BTC, XMR	BTC, XMR, Litecoin, Zcash	BTC, XMR	XMR	BTC, Litecoin, XMR	BTC

Table 1. Example of darkweb marketplace authentication mechanisms and payment methods [30].

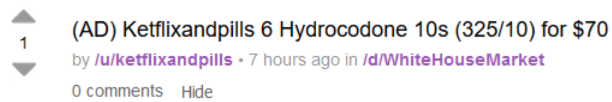

Fig. 2. Drug vendor advertisement in the Dread forum.

the years, marketplaces [122, 123] and forums [27, 88] have been established on the darkweb, and mainly on the Tor network, where cybercriminals can take advantage of the protocol's anonymity and obfuscation properties to conduct their operations. The anonymity provided by the darkweb works in two ways:

- **The Sellers**: Tracing sellers that are operating in the darkweb is much more challenging for Law Enforcement Agencies (LEAs). Furthermore, cybercriminals can control the level of access control they want for their marketplaces, depending on the how they advertise the onion address of their Tor hidden service [139] their marketplace is running on, what payment methods they accept (e.g. escrow [50]), which cryptocurrencies are available, like Monero (XMR) [28] and Bitcoin (BTC) [13, 79, 104], and which authentication mechanisms they implement (see Table 1). This leads to LEAs and researchers, also finding it difficult to gain access to some marketplaces, to gather and analyze data, in an effort to disrupt the marketplaces' operation.
- **The Buyers:** Individuals interested in acquiring services from these marketplaces, can effectively maintain their identities hidden when visiting them. This makes these marketplaces more appealing to the clients by offering a sense of security against being discovered or even, in many cases, being prosecuted for breaking the law.

The darkweb' s anonymity properties extend to the forums as well, where potential buyers can discuss with former buyers, read reviews and receive guidance on ways they could go about making a purchase on the marketplaces.

2.1.1 *Forums vs Marketplaces.*

Forums are fundamentally different digital platforms than marketplaces[2]. In forums, there is constant communication among members of the illegal trading community, be it sellers or buyers, with discussions on several topics, such as marketplaces, vendors, services, and payment. Furthermore, forums serve as platforms where vendors can advertise their products and services (Figure 2).

This makes forums a great place for buyers to navigate through, in an effort to find the best source offering what they need. They can read existing posts, directly ask other users, and generally use the feedback of more experienced buyers, as a guide, to make the right choices. Negative feedback will serve as a cautionary tale for future users (Figure 3).

[2]In this paper, for the sake of simplicity, when mentioning marketplaces, we also include vendors shops, which in truth are a more elementary version of marketplaces with far fewer features, and include products and services from a single seller [50].

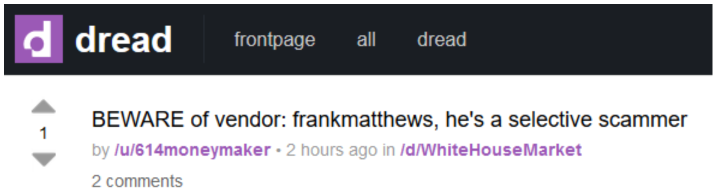

Fig. 3. Dread forum discussion thread on a marketplace scam.

Marketplaces on the other hand, are where the transactions between buyers and sellers take place. This is where botmasters can list their services, providing buyers with the advantage of browsing through the available options and choosing according to their needs. On Table 2 we present some product and service examples along with their prices, but the variety is far greater, with some vendors even trading in *COVID-19* vaccines and vaccination certificates [51]. Furthermore, there are reviews and reputation systems [50] (Figure 3.2.1), available to help the buyers choose the best combination of product and vendor, depending on their needs. In some cases, marketplaces may also have dedicated forum sections (e.g. *Hydra* [89]), and some forums may offer the capability to promote, or even sell products [62], usually of limited variety. The following personal advertisement example was taken from the *Dread* forum in February 2021:

> *"Hey I am a black hat hacker I can write a custom made (custom made means not recognizable by anti viruses) botnet malware with root privilege access for mining crypto, ddos site, password hijack and steal user data or bank data I don't care and i wont judge. but I expect to get paid afterwards. I can design for windows macos and linux but not phones (ios android) will write the code in python so victim MUST have python preinstalled If interested PM so we talk details."*

Lastly, it should also be mentioned that there is a special type of marketplace called Automated Vending Cart (AVC), which, as the name suggests, can be used to carry out automated purchases of illegal products on the darkweb, completely taking interaction with the vendors, out of the equation [57]. Some of the most popular marketplaces operating today include *Torrez* [90] and *White House Market* [91], popular forums include *Dread* [88] and *Freehacks* [27], but there are many more out there [122, 123].

2.1.2 Marketplace Takedowns.

Coordinated efforts have been successful in taking down illegal marketplaces operating in the dark web, like *Silk Road* [66], which was the first darkweb marketplace of its kind, with proof of its impact visible even to this day [60], the *Wall Street Market (WSM)* [128], *AlphaBay and Hansa Market* [100]. The most recent takedown is that of *DarkMarket* [17], which was considered to be the biggest illegal marketplace worldwide, operating in the darkweb, with 500,000 users, 2,400 sellers, 320,000 transactions and more than 4,650 BTC and 12,800 Monero XMR transferred, amounting to more than $140 million at the current rate (Jan 2021). The effort was a coordinated operation of many countries involving Germany, Australia, Denmark, Moldova, Ukraine, the United Kingdom and the USA, along with Europol.

2.2 Cybercrime-as-a-Service: Business Models

Since cybercrime has taken the form of a business, it is only natural that it has some common properties with legitimate businesses and follows some of the same principles. Depending on its size , different models can be applied to the way

Category	Product-Service Type	Average Price
Credit Card Data	Cloned Mastercard with PIN	$15
	Cloned American Express with PIN	$35
	Cloned VISA with PIN	$25
	Credit card details, account balance up to $1000	$12
	Credit card details, account balance up to $5000	$20
	Stolen online banking logins, minimum $100 on account	$35
	Stolen online banking logins, minimum $2000 on account	$65
	UK bank log - £3,000 GBP balance	$50
	Germany bank log - €3,500 EUR balance	$300
	Japan bank log - ¥400,000 JPY balance	$350
Payment Processing Services	Stolen PayPal account details, minimum $100	$198.56
	PayPal transfer from stolen account, $1000 – $3000	$320.39
	PayPal transfers from stolen account, $3000	$155.94
	Western Union transfer from stolen account, above $1000	$98.15
Forged Documents	US driving license, average quality	$1500
	US driving license, high quality	$550
	Rutgers State University student ID	$70
	US, Canada, or Europe passport	$1500
	Europe national ID card	$550
DDoS Attacks [114]	Unprotected website, 10-50k requests per second, 1 hour	$10
	Unprotected website, 10-50k requests per second, 24 hours	$60
	Unprotected website, 10-50k requests per second, 1 week	$400
	Unprotected website, 10-50k requests per second, 1 month	$800
	Premium protected website, 20-50k requests per second, multiple elite proxies, 24 hours	$200

Table 2. Example of Darkweb service-product average prices in 2020 (as reported by [45, 52]).

the infrastructure of each organisation functions, describing the different components and entities that coexist and interact with one another internally. Two prime examples are the *Value Chain Model*, created by Michael Porter[108] and Alexander Osterwalder' s *Business Model Canvas* [102]. Both of the models are implemented in the context of a botnet business in Sections 3.2 and 3.3.

2.2.1 Value Chain Model. Porter's Value Chain Model [1, 64, 108, 133], describes a profit organisation as a system composed of activities that revolve around the production, marketing, delivery and support of a product or service. This system' s ultimate goal is to provide a competitive advantage over other organisations, but it also focuses on maintaining it. It is divided into two main sets of activities: *Primary* and *Support*, with *Margin* being the outcome of the two sets' cooperation.

Primary Activities. The *primary activities* are the vital elements needed for the business to be in a position of competitive advantage, which will eventually lead to more financial profit. They are *inbound logistics, operations, outbound logistics, marketing & sales*, and *service.*

Inbound logistics are connected to the all the activities needed to acquire the raw materials used in the production process. They also include the handling of the acquired materials, namely the warehousing and inventory control, as well as the communication between the organisation and the suppliers. In cybercrime, inbound logistics translate into processes like vulnerability discovery research and communication with the suppliers of these vulnerabilities [121], like hacking groups that are pouring resources into vulnerability research (e.g. networks, protocols, software, applications) for exploitation and profit. They can also include the management of these vulnerabilities, after they have been acquired, like inventory and updates.

Operations refer to processes though which the raw materials are turned into the final product or service, which will subsequently be put out in the market, creating value for the organisation. In cybercrime the raw materials can be vulnerabilities, making the final product the exploit kit developed.

Outbound Logistics include actions related to the storage, distribution and delivery of the final product to the client. A cybercrime example is delivery of the final product/exploit kit to the buyers, though digital or physical means.

The actions associated with advertising and promoting the product/service to the costumers, as well as encouraging them to carry out the purchase, belong in the *marketing & sales* set of activities. In a cybercrime scenario, marketing and sales can include forums where products and services can be advertised, as well as marketplaces where clients can browse through and carry out purchases.

Lastly, *service* is always an important factor that can affect how successful an organisation becomes over time. It describes the activities aiming at offering customer support, repairs, warranties and replacements, and it mainly takes effect after a product/service has been sold. With darkweb drug trading as a cybercrime example, service can refer to customer support in case of an issue, such as dispatching the wrong product or quantity of a product (e.g. drugs).

Support Activities. Having a dependable foundation, that can serve as a support system for the primary activities, is of vital importance for every organisation. The *support activities* include *procurement, technology development, human resource management,* and *firm infrastructure*, and constitute the backbone of the organisation.

Firm infrastructure translates into elements such as accounting, legal, and quality assurance, and is considered as the supporting mechanism for all of the activities described in the model, both primary and support. In cybercrime, one example element belonging in this segment would be money laundering services.

Human resource management includes the management of the business' personnel such as, recruitment and hire, training, and lay offs. In cybercrime context, this segment could include staff management such as vulnerability researchers, hackers, exploit developers, and support staff.

Technology refers to the hardware, software and every action performed, with the purpose of turning the raw materials into the finalised product. Actions that aim towards improving the efficiency of these processes are also included. An example in cybercrime would be hardware, like servers and computers, as well as software such as encryption tools, password crackers, packet sniffers, communication apps, and websites.

Procurement describes the physical acquisition of the inputs, such as raw materials and resources, making this segment the implementation of the planning executed by the inbound logistics' set of activities. In an exploit trading cybercrime scenario, this segment could describe acquiring information of vulnerabilities from the researchers, or exploit kits, mainly through digital means.

Margin: *Margin* refers to the interaction between the activities of the *Primary* and *Support* activity groups. This interaction is considered as efficient when the cost of creating the service or product, which is equivalent to the cost of each activity of the two groups, is lower than the price at which it is made available to the customers [78], leading to profit. In cybercrime, margin would simply be the difference between the total costs of developing a vulnerability exploit kit and its selling price.

2.2.2 Business Model Canvas.

The *Business Model Canvas* [34, 101, 102] is composed of nine building blocks. The *customer relationships, customer segments, channels* and *revenue streams* blocks, are mainly focused on the customer, while the *key partners, key activities, key resources* and *cost structure* blocks, focus on the business itself. Lastly, *value propositions* is the block that brings all of the other blocks together.

Customer Segments: This block refers to the customer groups that the business' product/service is directed towards. In cybercrime, the costumer segments can include drug substance users, individuals interested in buying fire-arms, as well as individuals interested in acquiring botnet and malware related services.

Value Propositions: Value propositions describes the value exchange taking place between the business and its clients, and are in essence the products and services the business is offering, in order to satisfy the needs of a customer segment. Value propositions, in a cybercrime scenario, could refer to services such as phishing services [127] and botnet attacks [72], and products such as exploits, ransomware and illegal drugs.

Channels: The channels building block refers to the means of communication the business uses to reach the customer segments, such as digital platforms, social media, and the means used to maintain that communication, once it has been established. The purchase and delivery mechanisms, such as online sales/stores and digital/physical delivery, and after-sale support, are also included in this segment. In cybercrime context, this block can refer to darkweb marketplaces and forums, messaging and E-mail applications [36], as well as postal services [92].

Customer Relationships: Depending on the business, there is a degree of personalised business/client relationship needed, in order to acquire, keep and subsequently grow the client base. In cybercrime, relationships between vendors and buyers, can be established and maintained mainly through forums, marketplaces, and messaging/E-mail applications [36].

Revenue Streams: The method (e.g. subscription, licensing fee) and amount of payment, that the clients are willing to provide to acquire the product/service offered by the business, belong in the revenue streams block. One-time purchases (e.g. phishing kits [109]), subscriptions(e.g. phishing services [127]) and commissions, such as money laundering services [112], are all cybercrime examples for the activities related to revenue streams.

Key Resources: This block describes all the resources needed for a business, to be able to accomplish its goals, such as office space, hosting servers, computers, staff and Internet access. In cybercrime, this building block can refer to hardware like servers and computers, internet access, software, like operating systems, web applications, Virtual Private Network (VPN) software, communication applications, and staff for the different parts of the operation.

Key Activities: Key activities are the essential activities that the organisation needs to focus on and prioritise, to be operational and able to produce maximum results, such as production (e.g. factory), problem solving (e.g. hospital), marketing and advertising, and maintenance. Some cybercrime examples are drug sales, attack execution (e.g. DDoS attack), exploit and malware sales, as well as advertising on forums. Furthermore, finding a way to breach a target's security system, by the request of a client, qualifies as problem solving and is included in this building block as well.

Key Partners: In addition to suppliers, working with partners can lead to mutual profit, making it an important stepping stone in order to reach higher levels of growth. Some examples of partners to cybercriminals can be vulnerability researchers and hackers, malware and exploit kit developers, and illegal drug manufacturers.

Cost Structure: This last block refers to all the core costs that are associated with the business' operation. In cybercrime, this building block can include hardware maintenance costs, staff salaries, vulnerability research, exploit kit development costs (in the case of an internal department), and hiring fees (in the case of external associates).

3 APPLYING BUSINESS MODELS TO BOTNETS

The fact that the darkweb is so effective at obfuscating the identities of its users, has made it the perfect marketplace for botnets. Furthermore, the increased popularity of e-coins, and especially BTC and XMR, has contributed towards developing the botnet economy structure into a successful business that provides anonymity to its clients. Therefore, botnets present similarities in their financial functionality, to legitimate businesses, with economic models being composed of common elements. This can be accomplished by mapping out their business' infrastructure according to specific economic models, which can be further customized depending on how the botmaster envisions running their organisation. In Section 2.2, we discussed two well-known business models, namely the *Value Chain Model* and the *Business Model Canvas*, and how they can be applied into the cybercrime context. In this section, we map out the various elements of a botnet organisation through the utilization of the two aforementioned economic models.

3.1 Setting Up A Botnet

A preliminary step that must be executed independently from the economic model of choice, is the initial set up of the botnet. The foundation for the creation of every botnet, is the malware. The botmasters, in many cases, are not the actual developers of the botnet software [113], which means that they need to acquire the malware they will build their organisation on. At this point they have two choices [62]. The first choice is buying (or renting) an established botnet. This option offers more ease for users not as technically competent, but since the botnet is already fully developed, its purpose is already assigned and the botmaster must choose accordingly (e.g. spam botnet or credential theft botnet). In this scenario the buyer is provided with the C&C server's information and is also given administrator's access. The second option is buying a botnet framework [97]. This option includes only the bot application, that is used to infect hosts and further expand the bot army, and the C&C server application. This option is more suitable for users with technical proficiency and offers much more flexibility, by allowing the buyer to develop and personalise the botnet according to their specific needs. In this scenario, the buyer also has the advantage of the seller not knowing the information of the C&C server, which is the case when buying an already established botnet. An additional step to the framework option and in the case where the botmaster is the developer, is the fact that they will have to independently acquire BPHS [6, 54, 62] (see Section 3.2.1), while an already set up botnet, will often be accompanied by these services.

3.2 Value Chain Model

This section is dedicated to illustrating how the Value Chain Model can map into the economic infrastructure of a botnet, both in the scenario where the botnet is made available to clients as a service or product (CaaS), and in the scenario the botnet is only serving the botmaster's own personal agenda. To accommodate for this differentiation between the two cases, along with the specific nature of a botnet as a business, we propose a new implementation (see Figure 4) of the original value chain model (c.f. Section 2.2), which aims at providing a more accurate illustration of the different factors that play a role in the economic ecosystem of a botnet.

Our adapted model presents changes in the *inbound logistics, operations, outbound logistics,* and *marketing & sales* segments from the *primary activities* group (in blue), as well as the *procurement* segment from the *support activities* group (in orange). In specific, operations, as described in Section 2.2.1, do not have a place in the model, due to the fact

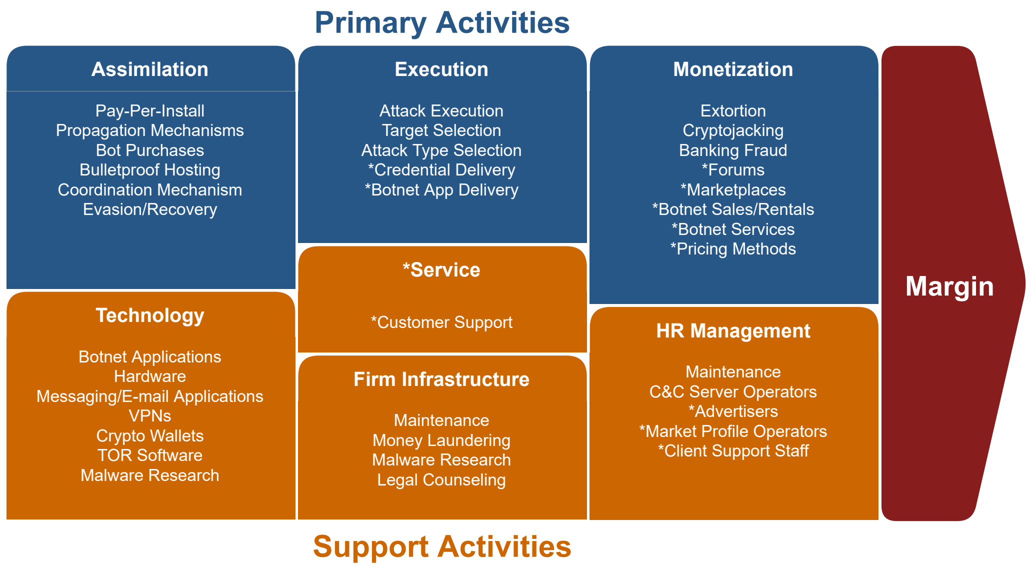

Fig. 4. Botnet Value Chain Model (adapted from the original [1, 64, 108, 133], see also Section 2.2.1). The elements preceded by an asterisk refer to the parts of the segments that are removed if the botnet is only used privately by the botmasters, to serve their own personal agenda.

that there is no actual production procedure, transforming the raw materials into the final products, while outbound logistics have a very restricted role due to the nature of a botnet business. For these two reasons, we implement a new segment in the primary activities, called *Execution*, which replaces both of these blocks and contributes towards a more compact application of the model. In addition, the procurement block is removed from the support activities and merged with inbound logistics (see Section 2.2.1), resulting in the new block *Assimilation*. The reasoning behind this adjustment is the fact that due to the nature of the business, there is no need for a separate block describing the physical acquisition of the raw materials, namely the bots. After the infection of the host, the bots automatically join the network (raw material acquisition), through the coordination mechanism already implemented in the bot binary. Lastly, the marketing and sales segment is renamed into *Monetization*, and repurposed to more accurately describe how the botnet operations can create revenue for the botmaster, both in the presence and absence of a client segment.

3.2.1 Primary Activities. The primary activities of a botnet business are *assimilation, execution, monetization* and *service.*

Assimilation: Assimilation can be summarized as all the activities performed behind establishing a healthy bot supply. Having a healthy supply of bots is vital for every bot network. From time to time, bots may go offline and leave the botnet permanently. The botmaster needs to keep the desired number of bots, at a healthy level, so they need to plan ahead. Bolstering the ranks of the bot army, or simply maintaining a steady number of bots, is a priority, and it can be achieved through propagation mechanisms 1, by acquiring Pay-per-Install (PPI) [19] services, and by purchasing individual bots and "bundles" that include a large number of bots, which can then be used according to the botmaster's vision about the organisation [9, 62].

Apart from the rank bolstering methods, the exact mechanism that is tasked with coordinating the bots, after their creation, is also a crucial part of the assimilation block. In a hybrid or centralised architecture, coordination is achieved through the “phone home” function of the bots. This mechanism is used by every bot for the connection to the C&C server, after which they become part of the bot army. It can be based on domain name usage, IPs, Domain Generation Algorithm (DGA)s [71], the blockchain [48], or Tor hidden services [7]. In the case the botnet is following a P2P architecture, coordination is achieved though the peer communication with the other nodes of the network [56, 143]. Depending on which of these mechanisms are implemented, as well as the botnet’s architecture, botmasters need to acquire the services of domain registrars, in case the botnet is utilising the Domain Name System (DNS) protocol as part of the coordination mechanism or backup channel, but most importantly establishing a C&C server (hybrid or centralised architecture). The fact that C&C servers are the most important component of these types of botnets, renders securing them to as high a degree as possible imperative. For that reason botmasters acquire BPHSs [6, 54] for their servers. These services can also serve as storage for harvested credentials and dump sites for files, exploit kits, and malware. Furthermore they are very often provided along with the purchase of already established botnets, otherwise they must be acquired by the botmaster independently.

Securing the different components of the botnet infrastructure is essential. For this reason, botmasters must implement evasion mechanisms [71, 124], such as *Fast Fluxing*, *Domain Fluxing* and, in case of a botnet utilising the Tor network, *Tor Fluxing* [7]. In case these mechanisms fail to provide the necessary obfuscation, and a takedown effort from LEAs is successful, there must be a secondary operation mechanism to fall back on. For example, a very common takedown attempt against hybrid or centralised botnets, is cutting off the communication between the C&C server(s) and the bots (see Section 4). Hence the secondary mechanism could include having a secondary C&C server, or multiple backup servers, so if a number of servers goes offline, others may take its place, and the botnet can remain fully functional.

Cooperation with other botmasters, is also a part of the backup mechanism, which in case of an emergency (e.g. takedown effort from LEAs), can be used to help regain control of the botnet, and can contribute towards the overall resilience of the botnet against hostile actions (see Section 4.1.14). Such collaborations can also lead to more financial gain by providing assistance and effectiveness in the botnet’s operations, like in the case of the *TrickBot* (see Section 4.1.14) and *Emotet* (see Section 4.1.15) botnets, where the latter, after the infection of a host, would sometimes drop the *TrickBot* malware as well.

Execution: The execution segment refers to all of the activities that take place after the client has paid to acquire a product or service, the delivery after a sale or rental, and the attack execution. In the scenario of a botnet rental, the delivery can be interpreted as providing the buyer with access to the C&C server. Being the backbone of every centralised or hybrid botnet infrastructure, gaining access to this server essentially means gaining full control of a part of the botnet or even the whole infrastructure. This process can be carried out simply by providing the C&C server’s IP, domain name or onion address, and login credentials, namely the username and password [62], though secure communication channels established by the botmaster (see Section 2). Afterwards, the user can easily utilise the botnet through the user interface of the C&C server.

In the scenario of a botnet sale, the process of giving control of the network over to the client, is equivalent to safely proving them with the botmaster application, along with the C&C server information, in the case of an existing central point of control.

If the client is only interested in acquiring botnet services, the execution segment refers to delivering these services. Some examples are carrying out malware installs on hosts (PPI), or delivering stolen credentials harvested by the bots, through safe communication channels (2). In a DDoS attack scenario, this would translate into executing the actual attack, according to the clients’ choice of attack type (e.g. ICMP flood, SYN flood), and attack target. These choices can

Rank	Items Sold
Rank 0	0-9
Rank 1	10-99
Rank 2	100-199
Rank 3	200-299
Rank 4	300-399
Rank 5	400-499
Rank 6	500-599
Rank 7	600-699
Rank 8	700-799
Rank 9	800-899
Rank 10	900-999
Top Seller	from 1000

Fig. 5. Torrez marketplace vendor reputation system.

be made either entirely by the client or in collaboration with the botmaster, namely against a specific IP/specific type chosen by the client, or an attack against a corporation in general, where the botmaster would be tasked with deciding on the optimal attack details, in order to achieve maximum impact.

In the case the botmaster is not following the CaaS model, the delivery to the clients, namely the C&C server credentials and botmaster application, has no place in the segment. Despite the absence of clients, the attack execution, along with the attack type and target, still play a vital role in the revenue generating process. However, in this case, the selection of the optimal attack type and target combination, is solely performed by the botmaster, depending on their purposes and vision. These attacks can be DDoS extortion [3], ransomware extortion [141], banking fraud/credential theft [71] and cryptojacking [37, 96].

Monetization: The main method of advertising botnet services [113, 127], is through darkweb forums [27, 88] and marketplaces [122, 123] (see Section 2.1). In marketplaces botmasters can list the services they can provide (Figure 7), such as selling parts of their network, renting them and providing various types of attacks. Buyers can then easily browse through the available choices, and acquire what they desire. The main function of forums, is to provide a platform where discussions can take place between individuals interested in services provided in the darkweb. An important mechanism that ought to be mentioned, is the *support* mechanism that the majority of marketplaces implement. Users not satisfied with a product or vendor in general, can use this function to report their experience to the marketplace administrators (e.g. in the case of a scam as shown in Figure 3).

This mechanism combined with the reviews and feedback of previous buyers available on the forums and marketplaces, leads to reputation and trust playing a crucial role in the way a botmaster's business is going to evolve and establish itself in the world of illegal trading. There are even dedicated sites, that function as a database of vendors that have performed scams in the past [134], the so-called *"rippers"*. Negative feedback will lead to buyers not trusting the vendor to come through and deliver what was advertised to the expected quality. In some cases, there is no delivery at all. For that exact reason, marketplaces have implemented reputation systems for vendors [50], to provide a sense of security to potential buyers. Some examples are ranks (Figure 5), which usually range from a scale of 1 to 10, depending on the numbers of sales that a vendor has carried out, and marketplace verification levels, according to which each vendor gains one level for each marketplace that they have been verified by, attesting to their legitimacy. An example of this reputation system is showcased on Figure 6, where a vendor from the *Torrez* marketplace has been verified by

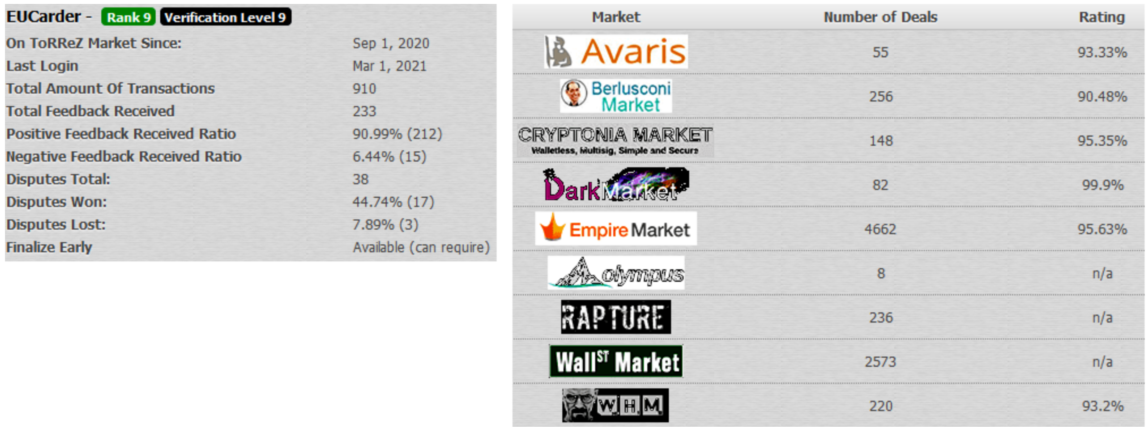

Fig. 6. Vendor reputation example in the Torrez marketplace. *Left:* Vendor profile example, including the reputation metrics. *Right:* List of marketplaces that have verified the specific vendor.

9 marketplaces (on the right - the total number of sales, along with the reputation score achieved on each of these platforms, are also included), and has consequently gained the verification level 9, which is publicly visible on their vendor profile (on the left). Additionally, as illustrated on the same figure, client feedback/reviews, dispute resolution statistics (complaint tickets created by unsatisfied clients), as well as whether the vendor has the *Finalize Early*[3] badge, also affect the reputation of a vendor. Through these systems, buyers can differentiate between established and more recent sellers, that have a higher chance of being scammers. Figure 7 is an example of service listings on the *Torrez* marketplace. One can notice the service provided, such as DDoS attacks and tutorials, the service category, whether the product is digital (e.g. tutorial PDF file), whether the delivery is instant, the country of origin, payment method supported, which is either escrow or multisignature escrow [50], the price, and the accepted currencies (e.g. Monero (XMR), Bitcoin (BTC) and Litecoin (LTC)). Lastly each listing includes the vendor profile information, which is their name, number of carried out sales, as well as their verification level, rank, and number of positive/neutral/negative reviews received by previous buyers. A detailed overview of reputation systems, currencies used, as well as payment schemes found on darkweb marketplaces, is presented by *Georgoulias et al.* [50].

Depending on the course of action that the botmaster has taken while designing the infrastructure and their personal goals, a botnet can provide income through a number of methods. All of these methods are also a part of the marketing and sales segment of the model. The botnet can be sold as a whole or as separate parts, it can be rented and it can provide services. These services can vary [61] from one-time purchases (e.g. a single DDoS attack, account credentials) [72]) and PPI (e.g. malware) [19], to services that follow the Pay-per-Click (PPC) (e.g traffic redirection [53]) and subscription models (e.g. botnet rental [62] and phishing services [127]).

If the botnet is not aiming to satisfy the needs of a customer group, promoting, advertising, selling, renting and providing services on marketplaces and forums, along with the pricing methods, have no application in the model. The botmaster in this case can create revenue through the ransoms gained out of extortion practises, as DDoS extortion [3]

[3]Marketplaces award the Finalize Early to highly trusted vendors, allowing them to provide services without utilizing the escrow payment mechanism, for speed and ease when carrying out sales [50].

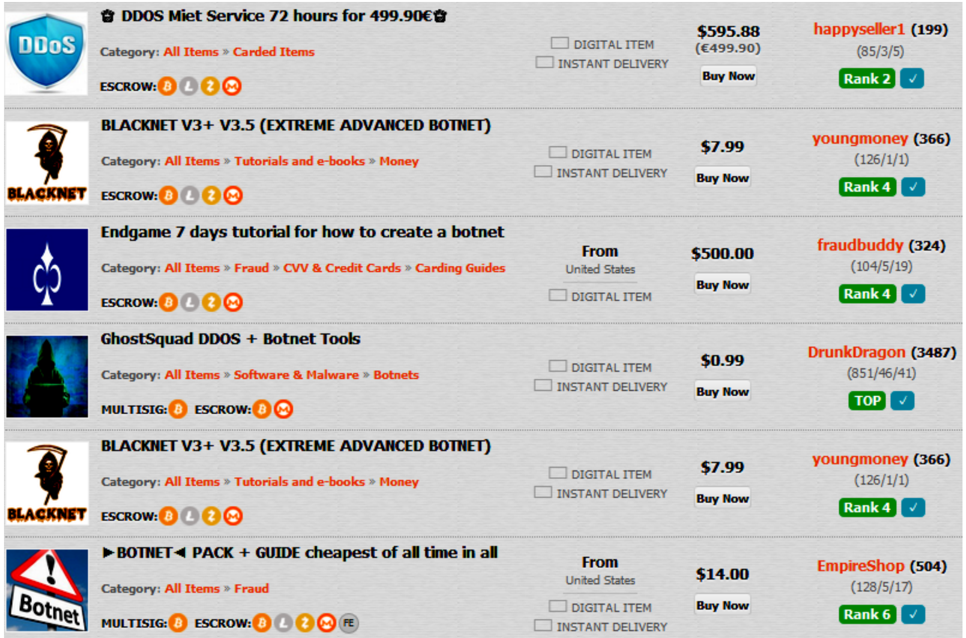

Fig. 7. Torrez marketplace botnet services.

and ransomware extortion [141]. They can also carry out banking fraud/credential theft [71] and cryptojacking [37, 96], which are two methods that can provide direct profit.

Service: The *service* segment translates into activities meant to provide support to the customers of the botnet enterprise. It includes handling issues linked to customer needs, both before and after the purchase or rental of a service. One example is technical assistance in the operation of the C&C server (in case of a rental). This segment also affects the reputation of the botmaster as a vendor, which leads to future clients showing trust and choosing them over other vendors.

If the botmaster is privately utilising his resources, the service segment, namely the customer support, does not have a place in the model.

3.2.2 Support Activities.

Firm Infrastructure: One of the components of the *firm infrastructure* block, is the legal approach of the C&C server's geolocation. The effectiveness of BPHS is heavily dependant on this geolocation. Countries differ in the way that they handle various activities of questionable legality in the cyber space, making some more suitable [54]) than others, to establish a C&C server. Hence, to deal with this state, there is a degree of legal consulting and research needed, which must be recurring, in order to accommodate for potential changes in the legal framework of countries that are either already hosting C&C servers, or that could do so in the future. Furthermore, another variable that could affect which geolocation of the C&C servers, would be optimal, is the possible attack surface. Having the C&C servers and the attack target of the botnet in different countries, is bound to make takedown efforts even more challenging, by being under different jurisdictions, requiring the cooperation and coordination of multiple LEAs and countries. For instance, it would be preferable for a botnet, mainly operating in the U.S, to have its C&C servers hosted in Europe or Asia).

Successful botnet operations, result in revenue, which cannot be justified to the authorities. This leads to botmasters having to either acquire already established *money laundering* services, or to create their own personal money laundering network by employing *"money mules"* [15, 23, 43, 86, 147]. Through these two options they can *"launder"* their money, which in essence means making the money earned through cybercrime activities untraceable and not able to be associated with their illegal operation.

In the botnet business, there is constant need for new ways to breach the security of host systems, so that an oncoming infection can take place and the target host can join the botnet. Hence, the infrastructure set of activities can also include activities aiming at acquiring new means of effectively bypassing system security, which can be accomplished through collaboration with vulnerability researchers, as well as malware and exploit kit developers [14].

Lastly, infrastructure also includes activities related to the maintenance of the botnet, such as the equipment/hardware used by the actors and software updates.

Human Resource Management: Human resource management, handles all the issues related to the staff, such as hires, lay-offs and payment of the organisation's personnel. The personnel can include various roles, such as operation of the C&C server, attack execution, customer support, individuals charged with operating the vendor profiles of the marketplaces on which the products/services are listed, and individuals tasked with advertising [113, 127] those products/services on several forums. Staff also includes individuals that deal with the technical needs of the botnet, such as hardware maintenance and software updates. In the case of the organisation having its own money laundering service, managing that group also belongs in this segment.

If the botmaster is not operating under the CaaS model, the elements that are redacted from the segment, are the advertisers, marketplace profile operators, and customer support staff.

Technology: Technology, refers to the hardware and software necessary for the botnet's operation, optimal performance, and maintenance. In terms of software, technology can include the botnet applications, namely the application running on the C&C server, the application running on each infected host, and the botmaster application, Virtual Private Network applications (VPNs), cryptocurrency wallets (Table 1), software that allows for connections to the TOR network, and communication applications like *Signal*, *Wickr* and *ProtonMail* (see Section 2.1). Concerning the hardware, technology incorporates all of the devices utilized for the botnet's operation, with the main ones being workstations and servers (DNS and C&C). Additionally, since the technology block includes the botnet applications, it is bound to also include actions which revolve around locating new vulnerabilities, developing new exploit kits, and improving on the existing botnet software. As mentioned above, this can also be achieved through the collaboration with third-part actors [14].

3.2.3 Margin. As mentioned in Section 2.2.1, the cost of carrying out the activities in the primary and support activity groups, needs to be lower than the price the products or services are offered at, to create positive margin. The same principle applies to botnets.

3.3 Business Model Canvas

In this section, we describe the application of the Business Model Canvas to a botnet organisation (Figure 8). As discussed in Section 3.2, there is need to differentiate between the two distinct cases of the botnet being directed

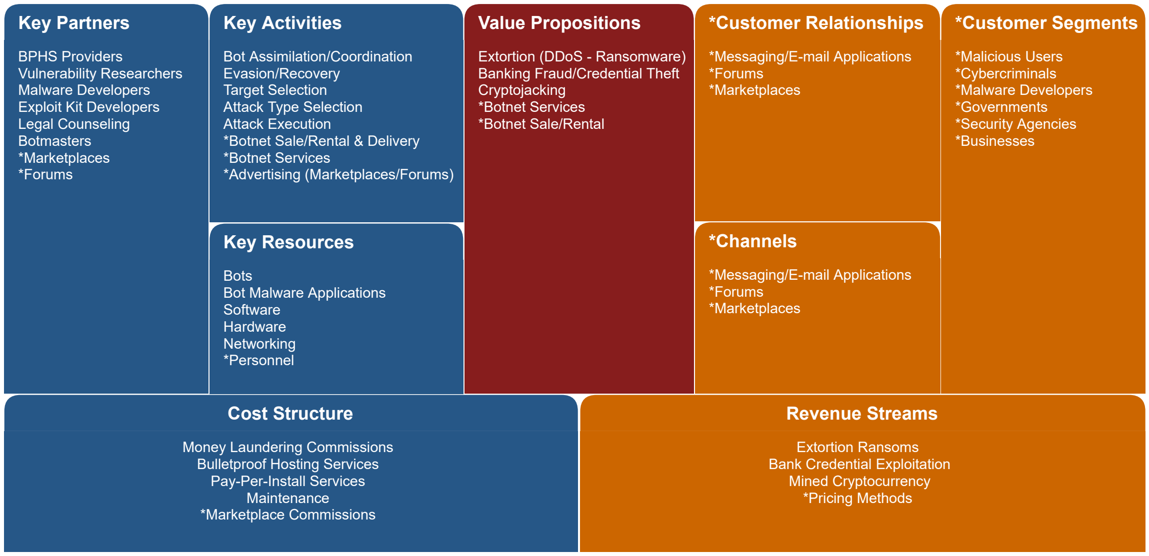

Fig. 8. Botnet Business Model Canvas (adapted from [131]). The elements preceded by an asterisk, refer to the parts of the segments that are removed in the case the botmaster is utilising the botnet privately, to serve their own personal agenda.

towards a clientele, and the case it is not. The same principles apply in this implementation as well, with all of the segments being affected. The components of the canvas can be divided into two distinct categories. The *right* (orange) side describes who the value created by the business is directed towards, how it is generated, and how it is delivered. The *left* (blue) side is focused on fulfilling the necessary requirements needed for the right side to achieve its goals. The *value propositions* segment (red) describes what the value that the business creates is (see Section 2.2.2), and sits in the middle of the canvas, acting as a link between the two sides.

3.3.1 Customer Segments: The *customer segments* of a botnet enterprise, can range from businesses interested in advertising their products or services (e.g. spam mails), corporations aiming at gaining an advantage over rivals (e.g. disruption through DDoS attacks), and ransomware developers that are trying to spread their malware, to governments and security agencies, aiming at disrupting opposing factions, but also at increasing their influence on the cyber digital world. In the absence of clients, this segment is removed in its entirety.

3.3.2 Value Propositions: The *value propositions* building block, refers to all the services and products (see Section 3.2.1), the botmaster will be able to provide to their clients, namely the customer segments. It is heavily dependant on the purposes (see Section 1) that the botnet can serve, and customer group that the products/services are directed towards (see Section 3.3.1).

A botmaster not having interest in providing their services to clients, translates into the removal of botnet sales and rentals, as mechanisms that the botnet creates value through. These mechanisms are replaced by DDoS extortion [3], ransomware extortion [141], banking fraud/credential theft [71] and cryptojacking [37, 96], which are all attacks performed privately by the botmaster themselves.

3.3.3 Channels: Channels refer to the utilisation of marketplaces (see Section 3.2.1) as a platform to showcase the business' products/services and carry out sales, but it also includes the means used in the communication with the clients, along with the delivery methods of the services and products. Botmasters, as illustrated in Section 2, use a variety of communication applications to stay in contact with their clientele, as well as forums to advertise their services and come in contact with potential clients. Delivery methods, due to the nature of the business and service, are mainly limited to digital means. Purchasing or renting a part of the infrastructure, would translate into gaining access to the C&C servers (see Section 3.2.1), while in a credential purchase scenario, the credentials would be sent via the communication applications of choice (see Section 2). In the case of a buyer acquiring a botnet service such as a DDoS attack or a PPC service, the delivery is the successful attack execution itself, or the increase in incoming traffic/website visits, respectively.

The lack of customer segments (see Section 3.3.1) from the organisation's operations, results to the channels segment being removed in its entirety.

3.3.4 Customer Relationships: As mentioned in Section 3.2.1, reputation and trust, play a crucial role in this type of enterprise, and greatly affect its impact on the darkweb market. Hence, every botmaster strives towards maintaining their reputation, not only through delivering the products and services as promised, but by inspiring trust to their clients, through cultivating and preserving a personalised relationship. The degree of personalisation will differ, depending on the client type (e.g. one time buyer, frequent buyer), and it will serve as stepping stone to achieving good marketplace rankings and positive reviews, a concept in common with legitimate businesses.

Customer relationships are removed entirely from the model if there are no customer segments (see Section 3.3.1).

3.3.5 Revenue Streams: Botmasters can achieve profit following a number of pricing models for their services, depending on the nature of their botnet (see Section 3.2.1). The most widely used models are one-time purchases, PPC, PPI and subscription.

If the botmaster is neither renting nor selling the botnet, and they are not providing botnet services to customers, the revenue streams mentioned above, are replaced by streams originating from DDoS extortion [3], ransomware extortion [141], banking fraud/credential theft [71] and cryptojacking [37, 96], namely extortion ransoms, stolen bank credential use, and mined cryptocurrency respectively.

3.3.6 Key Resources: The *key resources* building block, describes all the necessary assets required for the business to operate efficiently. These assets can be the bot malware applications, personnel, software, hardware, networking and more importantly, as discussed in Section 3.2.1, the bots, along with the C&C servers and all the coordination mechanism components.

The only change to the components of this segment, in the case of no customer segments, is an alteration to the personnel of the organisations, namely the personnel associated with marketplaces, forums, advertising and customer support (see Section 3.2.2).

3.3.7 Key Activities: The key activities that a botnet business needs to excel at are related to the malware's propagation, bot assimilation and coordination, evasion and recovery, satisfying customer needs, attack execution, delivery, marketing/advertising, and maintenance. These are the priorities that the botmaster must set, in order for their business to reach the highest performance possible, leading to more revenue. As analysed in Section 3.2.1, spreading the malware to new hosts and assimilating more bots into the "army", leads the botnet to a state, where it can be used effectively as a product or service. This is the foundation of the organisation's profits, which the main operational goal and profit source of the botnet, namely making profit trough botnet sales, rentals, and services, depends on. Consequently, sales, rentals, and services, also belong in this block, accompanied by the delivery of credentials or apps, as discussed in Section 3.2.1. Additionally, part of this segment, are also the processes of attack type and target selection (see Section 3.2.1). The effectiveness and impact of each attack's execution, will be a determining factor, in establishing a level of reputation and trust for the organisation (e.g. bring a site offline by performing a DDoS attack of the optimal magnitude). As illustrated in Section 3.2.1, reputation plays a leading role in the growth of the enterprise, making marketing and advertising, another key activity the organisation must prioritise on [113, 127]. Lastly, the botmaster, as discussed in Section 3.2.1 needs to have evasion and fail safe mechanisms in place, to make it as challenging as possible for attackers to hinder their operations, and be able to recover in case an attempt is successful.

Activities related to the sale or rental of the botnet, providing botnet services to clients, along with advertising in marketplaces and forums, are not included in the segment, in the absence of customer segments (see Section 3.3.1). Since the botmaster is the only one orchestrating the attacks and reaping the profits, they are in charge of selecting the targets of the attacks, as well as the type of attack that is best suited, depending on the context of each operation. As discussed in Section 3.3.5, in this case the attacks can be DDoS extortion [3], ransomware extortion [141], banking fraud/credential theft [71] and cryptojacking [37, 96].

3.3.8 Key Partners: Having the right partners can provide ease of operation and efficiency to a business. The same principle applies to botnets. Increasing the revenue of an organisation is certainly affected by choosing the optimal associates for every business compartment. These associates can be of varying legality. In botnets, this translates into choosing the marketplaces that will serve the botnet's goals best, forums to advertise and promote the botnet's services [113, 127], a money laundering network, legal counseling, BPHS, PPI service providers, other botmasters (see Section 3.2.1), vulnerability researchers, and lastly malware and exploit kit developers (see Sections 3.2.1, 3.2.2). The last two types of partners, namely the vulnerability researchers and malware/exploit kit developers, can be a vital component of the organisation, assuring that botnet will keep evolving by being more and more effective at breaching host systems, making it both more profitable and more elusive, since defenders have to adapt yet again, in order to deal with the new version of the malware.

If the botmasters are utilising their resources privately, the only change in the partners segment is the redaction of marketplaces, since there is no longer a need to advertise or promote the organisation, to attract potential clients.

3.3.9 Cost Structure: This last building block describes the overall cost that is required in order to fully support the operation of each and every business segment. It includes the costs associated with staff salaries, external partner fees, namely marketplace commissions [61, 135] and money laundering commissions [61], Research and Development (R&D), BPHS and PPI service providers, and lastly maintenance costs.

Lastly, having no association with customers, results in the cost structure of the organisation, no longer including marketplace commissions as a component, since marketplaces are not a part of the botnet ecosystem (see Section 3.3.8).

An interesting point to be made, is regarding the raw materials of a botnet business. Raw materials play a leading role in every business's plan of operation. Having a never ending source of raw materials, namely bots, can be extremely valuable and can provide ease, both financial and operational, and independence to the organisation.

3.4 Discussion

In both models, one can notice similarities in some of their building blocks. These blocks may differ in title, but in essence they describe the same functions, either individually, or in combination with others. One example is the *value* *propositions* (see Section 3.3.2) and *revenue streams* (see Section 3.3.5) building blocks from the *business model canvas* (Figure 8), in comparison with the *monetization* segment (see Section 3.2) from the *value chain model* (Figure 4). The components of the two business model canvas blocks, are all described, among others, in the monetization segment. These similarities are proof that no matter the business model utilised, the most important element regarding both implementations, is how each individual building block is affected by the botmaster's vision, and then consequently, in turn affects the content of the other blocks, forming the final economic infrastructure of the organisation.

4 BOTNET TAKEDOWNS & BUSINESS MODELS

In this section, our main focus is on successful botnet takedown efforts over the years, in regards to business models. Specifically, we will be illustrating how the mechanisms targeted by these efforts, can be mapped to segments of the business models showcased in Section 3, and then discuss the challenges related to takedown attempts.

4.1 Botnet Takedowns and Disruptions

In this section we go over some of the most notable takedowns through the years, dating all they way back to 2008, and then discuss the various challenges that cyber defense actors are met with, when mounting takedown and disruption attempts.

In the context of this paper, domain seizure and domain preregistering, as well as peer injection and peerlist poisoning, are considered as sinkholing methods, describing different processes individually, but providing very similar results.

4.1.1 Mariposa. *Mariposa*, was a botnet originating from Spain that gained attention in 2009. It is estimated to have spread from 10 to 12 million devices, with active devices ranging from 900,000 to 1.1 million daily, and its main purposes were credential harvesting and PPI services. The botmaster utilised a central C&C server, to which they would connect using VPN software. In order to counter the threat, the *Mariposa Working Group* was formed, which managed to sinkhole the domains (seizure) used in the botnet's infrastructure. What is interesting at this point, is the way the botmaster managed to gain back control of the botnet. They bribed an employee of the registrar they were using to register their domain names, to help them reestablish control over the bots. The bots had kept attempting to connect to the C&C server through the sinkholed domains, so when these domain became available again, the botmaster gained control once more and was able to update the bots with new C&C domain names. The most important factor that eventually led to the botmaster's arrest, was a simple mistake from his side, after the domains were sinkholed. He attempted to connect to the C&C server without using the VPN software, giving away his Internet Protocol (IP) address, which led to his identification and arrest by the Spanish authorities [31, 89, 132].

4.1.2 Grum. *Grum* was considered as the third largest spam botnet in 2012, along with *Lethic* and *Pushdo/Cutwail*. It is estimated to have had around 560,000 to 840,000 infected computers under the command of the botmasters in 2010, which in that year translated into 39.9 billion spam messages, almost 26% of the overall spam volume worldwide. Bots utilised hardcoded IP addresses to coordinate with the main and secondary C&C servers, which contributed towards the uncovering of their geolocation by researchers from *FireEye*, a cyber-security company. Through the cooperation of ISPs located in Russia, Panama and the Netherlands, which were providing hosting services to Grum, the servers were shutdown. The botmasters then tried setting up a backup channel in Ukraine, but these servers were shortly shut down as well, bringing the botnet down [75, 98].

4.1.3 *Conficker.*

The *Conficker* worm was an immense cyber threat in 2008 and 2009, with millions of infected computers. Its purposes were spam and spreading malware that imitated antivirus software. The threat was so large, that at some point *Microsoft* resorted to offering a reward of $250,000 for any information on the individuals responsible for the botnet's operation, which has still not been collected to date[115]. Microsoft also created the *Conficker Working Group (CWG)*, which along partners from the private sector, such as *Facebook, Cisco, IBM, Verisign* and many domain registrars and registries, with non-profit groups such as *The Shadowserver Foundation* and *Internet Corporation for Assigned Names and Numbers (ICANN)*, constituted the task force that took up the task of taking the botnet down [55]. The takedown efforts, which were the outcome of the cooperation between a large number of countries, were successful through reverse-engineering the malware and gaining insight on the DGA's properties. Recreating the DGA allowed for the 50,000 domains, that the bots could potentially use daily to connect to the C&C servers, to be preregistered, making them unavailable for the botnet to utilise, which resulted in loss of bot control by the botmasters [99].

4.1.4 *Citadel.*

Citadel was creating revenue for the botmasters through bank account credential theft. It is estimated that the botnets stole over $500 million, with infected devices reaching 5 million, and spanning over 90 countries. A part of why the network managed to reach such a high number of infections, was the fact that the cybercriminals behind Citadel were distributing pirated Windows Operating System (OS) versions, in which the malware was embedded. In 2013, after the cooperation of law enforcement, tech companies and banks, from over 80 countries, with main actors the Federal Bureau of Investigation (FBI) and Microsoft, the Citadel network of botnets was brought down, after seizing the network's servers [10, 116].

4.1.5 *Shylock.*

The *Shylock* botnet's activity was noticed for the first time in 2011. It was a banking trojan with credential harvesting capabilities, targeting clients of several banks, located all around the world, but with most infections taking place in the UK. It is estimated to have infected at least 30,000 devices running the Windows OS up until 2014, when its operation was disrupted. Through the cooperation of both law enforcement organisations, such as *Europol's European Cybercrime Centre (EC3)*, the *FBI*, and UK's *National Crime Agency (NCA)* and private organisations, such as *Dell SecureWorks* and *Kaspersky Lab*, the C&C servers, as well as the domains used by the bots to connect to these servers, were seized, which led to the botnet's disruption [40, 68].

4.1.6 *GameoverZeuS.*

GameOver Zeus was a botnet utilising the *Zeus* malware kit [69] and is considered as one of the most successful botnets. At its peak, it managed to spread to over one million devices and caused more than $100 million in losses. Its main purpose was banking and other credential theft, and it spread through spam e-mails and phishing messages. The efforts towards its takedown began in 2014, led by the *FBI*, under the title *"Operation Tovar"*, and focused on disrupting the coordination mechanism of the botnet. The plan firstly included injecting law enforcement controlled nodes in the botnet, in order to poison the peerlist and replace the legitimate nodes with the injected ones [142], redirecting the bots to sinkhole-nodes. One more mechanism that stood in the way of the takedown, was the backup channel the botmasters had in place, which was based on the use of a DGA. This channel was dealt with before carrying out the takedown, and it was achieved through preregistering the domain names that would be generated by the bots, to reestablish communication with the C&C server in case of a takedown attempt. Subsequently, through the cooperation of Internet Service Provider (ISP)s, the nodes of the network that were acting as proxies between the C&C server and the bots, were disabled, severing the communication. Lastly, they injected a new node which replaced the C&C server, giving over control of the botnet to the takedown actors [95].

4.1.7 Ramnit. *Ramnit* was a botnet that focused on user credential harvesting and managed to infect around 3.2 million devices all over the world. Its takedown was achieved in 2015, with *Microsoft, Symantec, Anubis Networks, Europol* and law enforcement entities from the UK, Italy, the Netherlands and Germany. The success of the takedown came as result of effectively disrupting the communication between the C&C servers and the bots, by shutting down the C&C servers, and seizing 300 domains used by the botmasters [41, 59]. Unfortunately, the success did not last, due to the fact that the individuals responsible for the botnet's operation were not apprehended by law enforcement. A few months after the takedown, the botnet resurfaced [70], and is still operational to this day [105].

4.1.8 Dorkbot. The *Dorkbot* botnet, also known as *NgrBot*, was discovered in 2011, and it spread through USB drivers, instant messaging apps and social networks. Its main purposes were credential theft, DDoS attacks, spam, and serving as a foundation for further malware infections on the host. In the last year before it was brought down, it was considered to have infected more than 1 million devices. With law enforcement agencies collaborating with partners from the industry, the botnet's takedown was finally achieved mainly through domain seizure [65, 117].

4.1.9 Avalanche. After a large ransomware attack in Germany in 2012 was traced back to the *Avalanche* botnet, the German police initiated efforts towards its takedown. Avalanche' s main purpose of operation was phishing, malware attacks and money mule recruiting. Over the course of its operation (2008-2016), it is estimated to have caused hundreds of millions of euros in damages worldwide, and that is due to the many malware families it has been associated with. In a joint four year long effort from organisations such as the *FBI, Europol, Interpol*, security companies like *Symantec* and some domain registries that the Avalanche group was using, it was eventually taken down in 2016. It was achieved through the reverse-engineering of the malware, the sinkholing of the domains identified (seizure and preregistering), which were around 800,000, as well as C&C server seizure and shutdown. This course of action finally led to the successful identification of the botnet's infrastructure and its physical servers [42, 120, 137].

4.1.10 Andromeda. The *Andromeda* malware botnet surfaced in 2011 and has been associated with more than 80 different malware variants. After a coordinated operation by *Europol's EC3*, the *FBI, Microsoft, ESET* and a number of other organisations, it was finally taken down in 2017. The foundation for the success of the operation, was the analysis of the *Wauchos* malware family, on which the Andromeda's infrastructure had been built on, over the course of 18 months. This allowed for the identification and seizure of approximately 1500 domain names, that the bots were using to connect to the C&C server, which in just 48 hours resulted in visits from 2 million IP addresses from 223 countries, illustrating the magnitude of the botnet's impact [120, 136].

4.1.11 Mirai. The *Mirai* IoT botnet surfaced in 2016 and is considered one of the most notable botnets of the last few years. At its peak, its ranks consisted of 650,000 infected devices and could achieve a record-breaking DDoS attack of approximately 1TBps, while other booter services ranged from 1GBps to 30GBps. The way the FBI managed to finally discover the identities of the Mirai actors, was through the anonymous accounts and aliases that these individuals were using at the timeon platforms such as *Hackforums*, in correlation with information they were publicly listing on social platforms such as *LinkedIn* [76, 145].

4.1.12 Kelihos.E. The *Kelihos* botnet had been active since 2010, with many variants surfacing over the years and various takedown efforts against them. The *Kelihos.E* variant, was responsible for millions of spam emails daily, phishing attacks, and malware delivery, including banking trojans. It was successfully taken down in April 2017, in a joint effort by *The Shadowserver Foundation*, the FBI and researchers from *CrowdStrike*. The takedown attempt focused the disrupting the P2P network through sinkholing both the peers and the C&C backup domains, and by seizing and disrupting the C&C server infrastructure, which was following a hybrid P2P architecture [87, 119]. The individuals responsible for the botnet's operation are considered to have been located in Russia.

4.1.13 Necurs. In 2020, the *Necurs* botnet was one of the biggest cyber threats worldwide. It had a wide variety of purposes, including stock scams, fake pharmaceutical spam email scams, dating scams, along with credential theft, cryptomining, as well as financial malware and ransomware distribution. *Microsoft*, along with a number of private and public partners across 35 countries, after an analysis on the DGA used by the bots to communicate with the C&C servers, were able to effectively precalculate approximately 6 million domain names, which were to be generated by the bots in the upcoming 25 months. These domains were reported to the registries they belonged, so that their registration could be blocked. Furthermore, Microsoft's legal team managed to get a court order from the *U.S. District Court*, allowing for the takeover of preexisting C&C servers, operating under U.S. jurisdiction. The individuals responsible for the botnet's operation are considered to have been located in Russia [16, 24].

4.1.14 TrickBot. *TrickBot* was discovered in 2016, as a bank credential theft botnet, but through the years it has been also purposed as a harvester of various credentials, such as Outlook, and malware dropper, with the *Ryuk* malware [84] being a prime example. Its main spread method is through spam campaigns containing embedded URLs or malicious attachments, and was through the *Emotet* botnet's operation, until the botnet's takedown in January 2021 4.1.15, which would drop the TrickBot malware [85]. In October 2020, Microsoft, with the assistance of legal authorities, took down 19 U.S. IP addresses used by the botnet, and provided a configuration file to the infected hosts that would stop their devices from connecting to the botnet control points. After some help from the Emotet botnet and through rotating the C&C servers' IPs, TrickBot continued spreading to more hosts. The botmasters also implemented the usage of Tor onion services for coordination purposes, increasing the resilience of the servers. Microsoft, along with their global partners, then took more action and with the help of hosting providers managed to successfully shut down 120 of the 128 servers of the botnet, which also included two C&C servers (94% of the infrastructure), that were known to be operational at the time, along with 7 IoT devices that were being used as assisting control points for the botnet [63]. Unfortunately, the efforts were ultimately unsuccessful in putting an end to the botnet's operation. Now (February 2021), months after the takedown attempt, and after the Emotet botnet takedown (see Section 4.1.15), TrickBot has managed to replace Emotet, and climb to the top of the malware families ranking [105], still making a big impact on the cyber world.

4.1.15 Emotet. *Emotet*, active since 2014, when it started as a banking trojan, had managed to become on of the most dangerous malware [44], as a means for cybercriminals to buy access to already compromised devices, namely a Malware-as-a-Service PPI botnet. This service was available for hire, offering the choice to clients to exploit the hosts they had bought access to, however they saw fit. The way it propagated was through malicious attachments, such Word documents and PDF files, included in automated emails, which in 2020-2021, among others, also translated into COVID-19 information emails. Emonet's infrastructure was composed of hundreds of control servers throughout the world, tasked with different roles , offering versatility and resilience against takedown efforts. *"Operation Ladybird"*, involved law enforcement authorities from the Netherlands, Germany, France, the United Kingdom, the United States, Canada, Ukraine and Lithuania through *Europol* and *Eurojust*, along with the *Dutch National Cyber Security Center*, non-profit organisations and various private parties. After fully understanding how the botnet infrastructure was laid out, the authorities, though coordinated action, simultaneously seized control of the network, physically seizing servers, stolen data, such as email credentials of infected hosts, cash and computer equipment [44, 77, 107].

4.1.16 Other notable takedowns. Some notable efforts against botnet operations over the years, have been on *DNSChanger* (2011) by seizing the DNS servers on which the whole infrastructure was founded [74], *Nitol* (2012) by seizing the *3322.org* domain used for the coordination of the bots, and eventually sinkholing them [81], *Bredolab* (2010) by seizing the C&C servers, and *Torpig* (2009) by reverse engineering, analysing the DGA utilised by the botnet, and using it to preregister domains the C&C server was bound to use in the future. The *Ozdok* (2009) takedown was a collaborative effort from the company *FireEye*, a number of ISPs, and domain registrars, using domain seizure and preregistering as the main methods, while the *Coreflood* (2011) [73] botnet was eventually taken down through domain seizure and sinkholing [31]. *Rustock* (2011), which was a spam botnet of significant impact, was finally taken down through seizure of the physical servers, following a civil legal process. *Waledac* (2010) was taken down through domain seizure, sinkholing, and peerlist poisoning, while *Pushdo/Cutwail* (2010) was briefly disrupted through the cooperation of ISPs that were in control of a large number of the C&C servers [31]. The *Srizbi* botnet (2008) takedown attempt focused on shutting down the C&C servers of the network, by cooperating with the controlling ISPs, and then preregistering domain names after reverse engineering the botnet's DGA, but unfortunately the botmasters managed to gain control though that same DGA [4]. In 2014, the *ZeroAccess* botnet was the target of a coordinated operation from both the private and public sector, which disrupted the botnet through identifying IPs used by the network and blocking all communication with them, as well as seizing the domains utilised by the botmasters [21]. In 2013, the *Kelihos.C* botnet variant was taken down by *CrowdStrike*, after a successful operation utilising peer injection and peerlist poisoning [138, 142]. Lastly, *3ve* was an ad fraud botnet that managed to infect more than 1.7 million hosts, and its estimated daily profit ranged from $3 to $5 million daily. In 2018 the *FBI* managed to takedown the network, through sinkholing 31 domains (seizure), and by getting control of 89 physical servers. *"Operation Eversion"*, as it was dubbed, included the cooperation of both the private sector and law enforcement agencies [144].

4.2 Takedown Methods and Business Model Relations

As can be noticed on Table 3, the main methods that have been used in takedowns over the years, in the majority of the cases, are domain sinkholing, through domain seizure and/or domain preregistering, seizure of the infrastructure's physical servers, shutdown of the servers and peer sinkholing through peer node injection and/or peerlist poisoning (in the case of P2P or hybrid botnets botnets e.g. 4.1.6, 4.1.12). These methods are often used in combination with one another. An overview of the takedown methods, in relation to the business models, can be seen on Table 4.

What is of value at this point, is how these methods can be translated into building blocks of the business models analysed in Section 3.

Value Chain Model: In regard to the *Value Chain Model* (see Section 3.2, Figure 4), domain sinkholing, through domain preregistering and/or seizure, is connected to *assimilation*, since it affects the bot supply through bringing down the coordination mechanism of the network. Seizing or shutting down the physical C&C servers (or DNS servers), can both be mapped to *technology* and *assimilation*, because they can be associated with the hardware, broadband (shutdown), bot supply and coordination, as well as BPHS providers. Peer sinkholing, through node injection or peerlist poisoning [142], can be applied to botnets following a P2P or hybrid architecture. This method is connected to the *assimilation*, due to the fact that it essentially targets the bot supply and coordination mechanism, but also the *technology* block since it is related to the bot application. Lastly, in the case of *Mirai* (see Section 4.1.11), metadata and data from the anonymous profiles that the botmaster was using in the context of their operation, can be correlated to *monetization*, which includes platforms such as forums and marketplaces.

Botnet	Year	Takedown/Disruption Methods	Reference
Srizbi	2008	Domain sinkholing (preregistering), server shutdown	4.1.16
Mariposa	2009	Domain sinkholing (seizure)	4.1.1
Torpig	2009	Domain sinkholing (preregistering)	4.1.16
Ozdok	2009	Domain sinkholing (preregistering and seizure)	4.1.16
Bredolab	2010	Server shutdown and seizure	4.1.16
Waledac	2010	Domain sinkholing (seizure), peer sinkholing (peerlist poisoning)	4.1.16
Pushdo/Cutwail	2010	Server shutdown	4.1.16
DNSChanger	2011	DNS server seizure	4.1.16
Coreflood	2011	Domain sinkholing (seizure)	4.1.16
Rustock	2011	Server seizure	4.1.16
Nitol	2012	Domain sinkholing (seizure)	4.1.16
Grum	2012	Server shutdown	4.1.2
Conficker	2012	Domain sinkholing (preregistering)	4.1.3
Citadel	2013	Server seizure	4.1.4
Kelihos.C	2013	Peer sinkholing (peer injection and peerlist poisoning)	4.1.16
ZeroAccess	2014	Domain seizure/sinkholing	4.1.16
Shylock	2014	Domain sinkholing (seizure) and server seizure	4.1.5
Gameover ZeuS	2014	Peer sinkholing (peer injection and peerlist poisoning), server shutdown, domain sinkholing (preregistering)	4.1.6
Ramnit	2015	Domain sinkholing (seizure), server shutdown	4.1.7
Dorkbot	2015	Domain sinkholing (seizure)	4.1.8
Avalanche	2016	Domain sinkholing (seizure and preregistering), server seizure and shutdown	4.1.9
Andromeda	2017	Domain sinkholing (seizure), server seizure and shutdown	4.1.10
Mirai	2017	Anonymous profile data and metadata	4.1.11
Kelihos.E	2017	Peer and domain sinkholing, server shutdown and seizure	4.1.12
3ve	2018	Domain sinkholing (seizure), server seizure	4.1.16
Necurs	2020	Domain sinkholing (preregistering), server seizure	4.1.13
TrickBot	2020	Server shutdown	4.1.14
Emotet	2021	Server seizure	4.1.15

Table 3. The 28 most notable botnet takedown attempts from 2008 to 2021.

Business Model Canvas: Following the same principles applied in the previous paragraph, in the case of the *Business Model Canvas* (see Section 3.3, Figure 8), domain sinkholing via preregistering and/or seizure, points to the *key resources* and *key activities* blocks, targeting bot assimilation and coordination. C&C (or DNS) server seizure or shutdown, are both related to *key resources*, *key activities* and *partners*, since apart from disrupting the bot assimilation and coordination, they also aim at the hardware and networking of the infrastructure, affecting BPHSs in the process. Peer sinkholing, through node injection or peerlist poisoning, also affect bot assimilation and coordination, and are additionally directly related to the bot application, hence they are also mapped to the *key activities* and *key resources* segments. Finally, the case of *Mirai* can be linked to the *key activities* and *channels* blocks, since the specific takedown correlates to the profiles of platforms such as forums and marketplaces.

4.3 Takedown Challenges

Taking down botnets has repeatedly proven to be a challenging and elusive task. Organisations mounting takedown efforts, are met with issues mainly related to lack of resources, jurisdiction, especially when it comes to operations carried out in foreign countries, legal framework constraints [146], and coordination with other organisations. On the contrary, it is easier for botmasters to invest in a resilient infrastructure, that will make hostile attempts against them

Takedown Method	Value Chain Model	Business Model Canvas
Domain sinkholing (seizure or preregistering)	Assimilation	Key Resources, Key Activities
Server seizure (C&C or DNS)	Assimilation, Technology	Key Resources, Key Activities, Partners
Server shutdown (C&C or DNS)	Assimilation, Technology	Key Resources, Key Activities, Partners
Peer sinkholing (peer node injection or peerlist poisoning)	Assimilation, Technology	Key Resources, Key Activities
Anonymous profile data and metadata	Monetization	Key Activities, Channels

Table 4. Takedown methods characteristics and issues.

even more challenging. For this reason, efforts that are the product of cooperation between different organisations, tend to be quite more efficient. This is not only due to the increased resources available, but because these collaborations allow for the easier utilisation of different methods, namely civil, legal, and technical. These organisations can be security and law enforcement agencies, ISPs, domain registrars and registries, legal authorities, voluntary working groups, and large corporations from all over the globe. Despite each organisation's individual underlying motives, be it cyber defense, profit, marketing/public relations or even plain goodwill, they share the common goal of taking down botnets, and they are willing to pool their resources towards that cause, increasing the chances of success [2, 31].

What is of interest at this point, is the overall difficulty and issues (see Table 5) that can arise in a takedown operation, depending on the methods employed. As illustrated in the previous section (see Tables 3 and 4), in most of the takedown attempts, success is accomplished through a combination of methods. Combining technical and legal methods, has proven to be more effective (e.g. Waledac, Rustock, Coreflood, Kelihos) than only taking the technical approach (Torpig, Ozdok, Pushdo) or only the legal approach (Ozdok initial takedown attempt) [31]. Some of the methods, are more challenging to implement than others, and can offer a varying degree of contribution towards the end goal.

4.3.1 Domain Preregistering & Seizure. Domain preregistering, can be employed against botnets utilising the DNS protocol in their infrastructures, and leads to the bots being sinkholed. DNS can be a part of the main coordination mechanism of the bots and/or the backup channel, which bots will use in case the main mechanism becomes the target of an attack. Both of these mechanisms can come in the form of a DGA, which dynamically generates the domains, or domains hardcoded in the bot binary that the bots use to acquire the C&C information. In many cases, discovering these domains requires the reverse engineering of the malware, which raises the technical difficulty of takedown operations.

Another method that is commonly used in takedown operations, is sinkholing through the seizure of already registered domains, which in most cases, presents the same challenge as domain preregistering, namely the malware's reverse engineering. In this case, the main difference is that this method needs to be accompanied by non-technical actions. Seizing existing domains, requires legal warrants and/or the cooperation of domain registrars. Private parties providing DNS services to the botmasters very often do not fall under the jurisdiction of the takedown actors, and can be located all over the globe. Coordination with LEAs and other partners from different countries is vital in these situations, in order for legal action to be plausible. However, legal action at that stage is sometimes rendered redundant because some private entities such as ISPs and domain registrars, sometimes after being informed of the situation, namely the fact that one of their users is utilising their services as a stepping stone to commit cyber crimes, choose to cooperate and contribute towards the takedown of the botnet.

4.3.2 Server Shutdown & Seisure. Disabling the C&C servers of a botnet infrastructure can be achieved in two ways, by physically seizing them or disconnecting them through the ISPs. Physical seizure requires legal procedures, in order to acquire the necessary warrants, and is also heavily dependant on the server geolocation. Since the servers can be spread out all across the globe, which is quite common, there are different jurisdictions and legal frameworks, that can surround a takedown operation. This fact makes cooperation between countries and organisations vital for an operation to be successful. This can also be the case, when attempting to disable the C&C servers through their ISPs. In this scenario the takedown actors can contact the ISPs, and try to acquire their assistance in taking the servers offline. Sometimes this approach does not yield any results, making legal warrants necessary. As with domain and server seizure, this can lead to jurisdiction issues, when the servers are located in various countries, making the takedown operation impossible to carry out without the cooperation of the corresponding LEAs and legal authorities. Furthermore, disconnection through the provider, when compared to physical seizure of the server, can prove easier to accomplish, because in some cases the provider might be willing to cooperate, removing the legal barrier confining the operation.

4.3.3 Peer Injection & Peerlist Poisoning. In the case of a botnet utilising P2P communication in its infrastructure, be it the main coordination mechanism, the backup channel, or both, the methods that can be employed are sinkholing through peerlist poisoning, where fake nodes are entered in the list of peers embedded in the botnet malware, and via peer injection (sybil attacks) [142], where fake nodes controlled by the takedown actors are added to the network. Furthermore, these methods are used in combination, like in the cases of the *GameoverZeus* (see Section 4.1.6) and *Kelihos.C* (see Section 4.1.16) botnets, both contributing towards directing the bots to specific nodes controlled by the takedown operation. Both of these methods' implementations are challenging in regard to their technical aspect, requiring the reverse engineering of the malware in order to be able to effectively inject a controlled node or retrieve the list of peers from the bot malware, and do present legal issues, hence the legal framework surrounding the takedown operation must always be taken into account.

4.3.4 Implementation & Legality. After the aforementioned methods have been executed successfully, depending on the implementation, as well as the botnet targeted, the legality of each takedown operation can vary [18]. For example, if law enforcement operated a server in the generated sinkhole, with which the bots would connect instead of the C&C server, and the botnet's purpose was credential theft, then the takedown actors could end up acquiring private user information. Furthermore, in some implementations, the takedown actors decide to gain remote access to the infected devices for remediation purposes (e.g. *Coreflood*, *Citadel*); this can also raise legal and ethical issues [32, 146].

Takedown Method	**Reverse Engineering**	**Legal process**
Domain sinkholing (preregistering)	◐	◐
Domain sinkholing (seizure)	◐	◐
Server seizure (C&C or DNS)	◐	●
Server shutdown (C&C or DNS)	◐	◐
Peer sinkholing (peer injection or peerlist poisoning)	●	◐
Anonymous profile data and metadata	○	○

Table 5. Takedown operation challenges. Depending on the method of choice: ○= Not necessary, ◐= Depends on the case, ●= Necessary.

4.4 Observations and Steps Ahead

From our analysis in Section 4.2, it can be observed that the majority of the takedown methods, can be associated with the *assimilation* and *technology* segments of the *Value Chain Model*, as well as the *key resources* and *key activities* blocks from the business model canvas. It is also clear, that takedown and disruption efforts, have not been targeting elements of the botnet infrastructure that can be strictly related to its financial framework (apart from the *Mirai* isolated incident, see Section 4.1.11), such as the *firm infrastructure* and *monetization* segments of the Value Chain Model. Shifting focus towards these segments, will give takedown efforts a new dimension, by directly aiming at the element that is located in the center of every business, profit. Additionally, such an approach would contribute in alleviating some of the issues takedown operations are met with, such as reverse engineering of the malware, and legal challenges (see Section 4.3.4). We believe that further researching the mechanisms that are related to the revenue creating process of a botnet, with some prime examples being promotion of the products and services, along with reputation and trust towards the botmasters/vendors, has the potential to hit at the heart of these cybercriminals' operations. Hence, we argue that future research should also include this direction, in an effort to leverage potential weaknesses related to botnets' profit generation. Specifically, we believe that exploring the darkweb selling platform framework [50], which is currently supporting the botnet trading market, is a solid starting point, since the operation of these platforms is undeniably linked with the aforementioned mechanisms.

5 RELATED WORK

In this section we go over notable existing research associated with botnets, with a focus on their economic aspect.

5.1 Botnets

Silva et al. [124] survey botnets in terms of evolution, life-cycle, architectures, detection, evasion and defense. *Khattak et al.* [71] take a similar approach, and create taxonomies of botnet behaviour, detection mechanisms, and defense mechanisms. *Rodríguez et al.* [113] present a survey on botnet research, map the life cycle of botnets, and then create a taxonomy of botnet research based on this life-cycle.

In addition to the more generic research on botnets, there are also many efforts focusing on specific botnet aspects, with detection being among the main ones. The work in this field presents a lot of variety. *Alieyan et al.* [5] survey detection methods utilizing the DNS protocol. *Garcia et al.* [49] present a comparison of three botnet detection methods, utilizing a large, real-world, labeled botnet traffic dataset, and evaluate their performance. *McDermott et al.* [94] utilize deep learning in combination with word embedding, to detect botnet activity in IoT devices. The developed model is evaluated using data from attacks associated with the *Mirai* botnet. Lastly, *Prasad et al.* [110] take a bio-inspired approach and propose a model efficient in detecting application layer DDoS attacks.

There is also research focusing on the analysis of specific botnets and their characteristics, such as the work of *Antonakakis et al.* [8] on the *Mirai* botnet. This type of research is in certain occasions carried out in the context of operations against the botnet, with the works of *Stone-Gross et al.* on the *Torpig* [129] and *Pushdo/Cutwail* [130] botnets as two notable examples. On the topic of takedowns there are also more generic approaches, such as the work of *David Dittrich* [31], who illustrates the elements associated with a botnet takedown, and then presents case studies of past takedowns, along with the observations that resulted from these operations. Additionally, *Nadji et al.* [99] propose an analysis and recommendation system called *rza*, which aims to carry out post-mortem analysis of botnet takedowns, but also provide insight on how future takedown operations could be performed. Under the same research umbrella, the legal and ethical aspects of hostile operations against botnets have also been addressed by researchers, such as the works of *Dittrich et al.* [32] and *Sam Zeitlin* [146].

Year	Title	Keywords	Reference
2009	Your Botnet is My Botnet: Analysis of a Botnet Takeover	takedown, Torpig	[129]
2010	A case study in ethical decision making regarding remote mitigation of botnets	ethical and legal challenges	[32]
2012	So You Want to Take over a Botnet	takedowns, case studies	[31]
2013	Beheading Hydras: Performing Effective Botnet Takedowns	takedown analysis, takedown methods	[99]
2013	Botnets: A survey	survey, history, architectures, life cycle, detection, evasion, defense	[124]
2013	Survey and Taxonomy of Botnet Research through Life-Cycle	survey, taxonomy, architectures, detection, life-cycle, purpose and attacks, obfuscation, marketing	[113]
2014	A Taxonomy of Botnet Behavior, Detection, and Defense	taxonomy, architectures, obfuscation, life-cycle, detection, evasion, purposes	[71]
2014	An empirical comparison of botnet detection methods	detection, dataset, evaluation, comparison	[49]
2015	Botnet takedowns and the fourth amendment	takedown legal challenges	[146]
2017	Botnet command and control architectures revisited: Tor hidden services and fluxing	obfuscation, Tor, architectures, DNS	[7]
2017	A survey of botnet detection based on DNS	survey, detection, DNS, machine learning, neural networks	[5]
2017	Understanding the mirai botnet	botnet analysis, Mirai, IoT, DDoS, DNS, honeypots	[8]
2018	Botnet detection in the internet of things using deep learning approaches	detection, deep learning, Mirai, IoT, DDoS, word embedding, dataset	[94]
2020	BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web	detection, bio-inspired, DDoS attacks	[110]

Table 6. Notable research on various botnet-related topics

5.2 Botnet Economics

With financial incentives being the main motivation behind botnet businesses, researching the economic infrastructure, in an effort to gain a better understanding of how botmasters earn revenue, can prove to be critical in disrupting botnet operations. We argue that this can lead to the discovery of weak points, the exploitation of which would add a new weapon to the defenders' arsenal against botnets. There have been efforts towards both gaining insight on the economic infrastructure behind botnets, and inventing new disruption methods, based on economy related elements of botnets' operations (see Table 7).

Ford and Gordon [46] focus on analyzing the economic incentive behind spreading malicious applications such as spyware and adware, credential theft and sale, DDoS attacks and botnet sale/rent, that can be used to generate revenue for botmasters. They argue that emphasizing disruption efforts on the business models utilised by botmasters, shows significant promise.

Friess and Aycock [47] study credential theft and how this botnet activity is used and sold in the black market. They focus on the financial motives behind creating and maintaining this type of botnet, how it creates revenue, and lastly touch upon defensive mechanisms against it.

Li et al. [83] proposed a model which is based on the utilization of honeypots in order to create virtual bots. Every botnet C&C server handles a certain number of bots. By having a substantial percentage of that number be virtual/fake bots, they introduced a level of uncertainty regarding the botnet's effectiveness in an attack, which in essence lowers the quality of the botnet services and their appeal to the potential clients. This can eventually lead to a significant profit decrease for the botmaster.

Year	Title	Keywords	Reference
2007	Cent, five cent, ten cent, dollar: Hitting botnets where it really hurts	spyware, adware, credential theft, DDoS, business model, disruption	[46]
2008	Black Market Botnets	credential theft, business model	[47]
2009	Botnet Economics: Uncertainty Matters	honeypots, reputation, honeypots, disruption	[83]
2011	Click trajectories: End-to-end analysis of the spam value chain	spam, value chain, captive botnets, real-time data	[80]
2011	The underground economy of spam: A Botmaster's perspective of coordinating large-scale spam campaigns	Pushdo-Cutwail botnet, spam, forum, takedown	[130]
2013	Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study	DDoS, economic model	[118]
2014	The Botnet Revenue Model	supply chain, disruption, revenue model	[14]
2014	Toward a Monopoly Botnet Market	botnet monopoly, disruption, economic model	[82]
2016	Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services	DDoS, payment methods, disruption, PayPal	[67]
2018	Business Model of a Botnet	DDoS, credential theft, spam, click fraud, cost-revenue ratio, business model	[111]

Table 7. Botnet economics research

Levchenko et al. [80] present an overview of the overall spam botnet value chain. They use three months of real-time data from captive botnets, spam feeds, and spam advertised URLs to gain an understanding of the botnet infrastructure. They also identified sites that provide botnet services and carried out purchases to gain information about the business economy.

Stone-Gross et al. [130] acquired a number of CnC servers of the *Pushdo/Cutwail* botnet, in an effort to identify the characteristics of spam botnets of that magnitude. Furthermore, they performed an analysis on the *Spamdot.biz* forum, a forum dedicated to spam related activities, giving insight on the botmaster' s perspective.

Segura and Lahuerta [118] attempt to assess the economic motivation behind DDoS attacks. They present a model mapping the financial incentives of botmasters, using data collected both from direct communication with botmasters and from past DDoS extortion incidents.

Bottazzi and Me [14] propose a model that describes the revenue making process of a botnet. In this model the ecosystem of a botnet's operation is divided into four different segments, which together form the *supply chain.* They analyze how these different parts of the chain interact with one another and how their attributes change over time, affecting the botmaster' s revenue. Lastly, they conclude that attacking individual links of the supply chain, could be effective in hindering a botnet's operation.

Li and Liao [82] suggest going after the smaller and newer vendors in order to turn the botnet market into a monopoly. They argue that this may prove beneficial for defenders, because according to their economic model, this will demotivate new botmasters from entering the market and increase the price of these services. This state of the market will ultimately lower the appeal of these services to the clients, reducing the overall output of the botnet industry.

Karami et al. [67], targeted DDoS/booter services, attempting to disrupt their payment infrastructure through a payment intervention. Specifically, they focused on DDoS service providers that were utilising *PayPal* as a payment platform. Through the use of crawlers, they gathered information about the accounts that the booters were using to receive payments, and then collaborated with PayPal to disable them. This effort resulted in a noticeable availability drop of these services, and since the customers were having issues with payment, the customer base was reduced.

Putman et al. [111] focus on the botnet financial infrastructure, applying the *Business Model Canvas* to a botnet business, as well as on the botnet life cycle. They use four case studies in which botnets perform DDoS, bank credential fraud, spamming and click fraud attacks, to assess the attacker's botnet set-up costs and revenue ratio, along with the financial impact on the victims of such attacks.

There are also more broad spectrum approaches, identifying and analyzing CaaS characteristics, as well as how business models can be utilised in cybercrime research to map the elements and factors that are impactful in the formation and profitable operation of a cybercrime business [61, 62, 126, 127].

Lastly, our effort focuses more on the specific market of botnets and the business models implemented by botmasters, in a darkweb context. Additionally, to the best of our knowledge, this is the only work that presents a correlation between business models and botnet takedown methods. Through this correlation we aim to provide a new perspective on how botnet takedown operations can be strategised, and purposed to target a larger variety of botnet components.

6 CONCLUSION

The cyber world is still far from being considered safe from the botnet threat. Darkweb marketplaces and forums constitute a vital part of cybercrime operations, serving the two essential purposes of such a business, namely advertising and selling, while offering anonymity to their users.

Cybercrime keeps evolving, aiming towards new methods of exploitation, evasion and takedown resilience. Hence, the defending side must keep up with the same pace, improving their detection and defense methods, as well as the effectiveness of their takedown operations. Takedown operations are prone to technical, legal and jurisdictional issues, and require a lot of resources along with the cooperation between countries and organisations from both the public and private sector. Hence, we argue that shifting the focus of takedown operations to also target business model segments related to revenue generation, could eliminate some of these challenges (e.g. reverse engineering of the botnet malware, legal constraints) and enhance the impact of takedown operations.

Gaining a better understanding of the botnet economic ecosystem through business models, can contribute towards novel economic disruption methods. Based on our two adapted models, with the *Value Chain Model* as a point of reference (Figure 4), this would translate into directing attention towards components of the *monetization* and *firm infrastructure* segments. Focusing on developing methods specifically targeting the revenue generating related aspects of the botnet business, could prove detrimental for the industry. Developing methods to impair these elements throughout different levels, could assist in taking away the economic incentives and motivation of cybercriminals to further carry out their operations, and even discourage future ones from ever taking their first step into the cybercrime world.

REFERENCES

[1] Tokunbo Agbolade. 2020. Value Chain Analysis: An Internal Assessment of Competitive Advantage. https://www.business-to-you.com/value-chain/

[2] Wajeeha Ahmad. 2019. Why Botnets Persist: Designing Effective Technical and Policy Interventions. https://internetpolicy.mit.edu/wp-content/uploads/2019/09/publications-ipri-2019-02.pdf

[3] Akamai. 2020. Ransom Demands Return: New DDoS Extortion Threats From Old Actors Targeting Finance and retail. https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html

[4] Atif Mushtaq Alex Lanstein. 2008. Srizbi control regained by original owner. https://www.fireeye.com/blog/threat-research/2008/11/its-srizbi-trun-now.html

[5] Kamal Alieyan, Ammar ALmomani, Ahmad Manasrah, and Mohammed M Kadhum. 2017. A survey of botnet detection based on DNS. *Neural Computing and Applications* 28, 7 (2017), 1541–1558.

[6] Sumayah Alrwais, Xiaojing Liao, Xianghang Mi, Peng Wang, Xiaofeng Wang, Feng Qian, Raheem Beyah, and Damon McCoy. 2017. Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 805–823. https://doi.org/10.1109/SP.2017.32

[7] Marios Anagnostopoulos, Georgios Kambourakis, Panagiotis Drakatos, Michail Karavolos, Sarantis Kotsilitis, and David KY Yau. 2017. Botnet command and control architectures revisited: Tor hidden services and fluxing. In *International Conference on Web Information Systems Engineering*. Springer, Springer, Cham, Puschino, Russia, 517–527. https://link.springer.com/chapter/10.1007/978-3-319-68786-5_41.

[8] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. 2017. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*. USENIX Association, USA, 1093–1110.

[9] Dan WoodsSara BoddyShahnawaz Backer. 2020. Genesis Marketplace, a Digital Fingerprint Darknet Store. https://www.f5.com/labs/articles/threat-intelligence/genesis-marketplace--a-digital-fingerprint-darknet-store

[10] BBC. 2013. FBI and Microsoft take down $500m-theft botnet Citadel. https://www.bbc.com/news/technology-22795074#:~:text=The%20FBI%20and%20Microsoft%20have,million%20machines%20to%20steal%20data.

[11] Victor Benjamin, Weifeng Li, Thomas Holt, and Hsinchun Chen. 2015. Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. In *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, Baltimore, MD, USA, 85–90. https://doi.org/10.1109/ISI.2015.7165944

[12] Leon Böck, Emmanouil Vasilomanolakis, Max Mühlhäuser, and Shankar Karuppayah. 2018. Next Generation P2P Botnets: Monitoring Under Adverse Conditions. In *Research in Attacks, Intrusions, and Defenses*, Michael Bailey, Thorsten Holz, Manolis Stamatogiannakis, and Sotiris Ioannidis (Eds.). Springer International Publishing, Cham, 511–531.

[13] John Bohannon. 2020. Why criminals can't hide behind Bitcoin. https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

[14] Giovanni Bottazzi and Gianluigi Me. 2014. The Botnet Revenue Model. In *Proceedings of the 7th International Conference on Security of Information and Networks* (Glasgow, Scotland, UK) *(SIN '14)*. Association for Computing Machinery, New York, NY, USA, 459–465. https://doi.org/10.1145/2659651.2659673

[15] Danton Bryans. 2014. Bitcoin and money laundering: mining for an effective solution. *Ind. LJ* 89 (2014), 441.

[16] Tom Burt. 2020. New action to disrupt world's largest online criminal network. https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/

[17] Mattha Busby. 2021. Darkmarket: World's Largest Illegal Dark Web Marketplace Taken Down. https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

[18] Leon Böck, Martin Fejrskov, Katerina Demetzou, Shankar Karuppayah, Max Mühlhäuser, and Emmanouil Vasilomanolakis. 2022. Processing of botnet tracking data under the GDPR. *Computer Law & Security Review* 45 (2022), 105652. https://doi.org/10.1016/j.clsr.2021.105652

[19] Juan Caballero, Chris Grier, Christian Kreibich, and Vern Paxson. 2011. Measuring Pay-per-Install: The Commoditization of Malware Distribution. In *20th USENIX Security Symposium (USENIX Security 11)*. USENIX Association, San Francisco, CA, 13. https://www.usenix.org/conference/usenix-security-11/measuring-pay-install-commoditization-malware-distribution

[20] Guy Caspi. 2020. Why Are We Losing The Cyberwar? https://www.forbes.com/sites/forbestechcouncil/2020/01/22/why-are-we-losing-the-cyberwar/

[21] Microsoft News Center. 2013. Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet. https://news.microsoft.com/2013/12/05/microsoft-the-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/

[22] Thomas M Chen. 2010. Stuxnet, the real start of cyber warfare?[Editor's Note]. *IEEE Network* 24, 6 (2010), 2–3.

[23] Kim-Kwang Raymond Choo. 2011. The cyber threat landscape: Challenges and future research directions. *Computers & security* 30, 8 (2011), 719–731.

[24] Catalin Cimpanu. 2020. Microsoft orchestrates coordinated takedown of Necurs botnet. https://www.zdnet.com/article/microsoft-orchestrates-coordinated-takedown-of-necurs-botnet/

[25] Alma Cole, Michael Mellor, and Daniel Noyes. 2007. Botnets: The rise of the machines. In *Proceedings on the 6th Annual Security Conference*. Association for Computing Machinery, New York, NY, United States, Oak Ridge Tennessee USA, 1–14.

[26] Evan Cooke, Farnam Jahanian, and Danny McPherson. 2005. The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets. *SRUTI* 5 (2005), 6–6.

[27] Dylan Curran. 2018. My terrifying deep dive into one of Russia's largest hacking forums. https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety

[28] Mike Dalton. 2020. Can Monero Be Traced? How the U.S. Is Trying to Track the Privacy Coin. https://www.bitrates.com/news/p/can-monero-be-traced-how-the-us-is-trying-to-track-the-privacy-coin

[29] A Decker, D Sancho, L Kharouni, M Goncharov, and R McArdle. 2009. A study of the Pushdo/Cutwail Botnet.

[30] Photon Research Team Digital Shadows. 2020. With The Empire Falling, Who Will Take Over The Throne? https://www.digitalshadows.com/blog-and-research/with-the-empire-falling-who-will-take-over-the-throne/

[31] David Dittrich. 2012. So You Want to Take over a Botnet. In *Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats* (San Jose, CA) *(LEET'12)*. USENIX Association, USA, 6.

[32] David Dittrich, Felix Leder, and Tillmann Werner. 2010. A case study in ethical decision making regarding remote mitigation of botnets. In *International Conference on Financial Cryptography and Data Security*. Springer, Springer, Berlin, Heidelberg, Tenerife, Canary Islands, Spain, 216–230.

[33] Po-Yi Du, Ning Zhang, Mohammedreza Ebrahimi, Sagar Samtani, Ben Lazarine, Nolan Arnold, Rachael Dunn, Sandeep Suntwal, Guadalupe Angeles, Robert Schweitzer, et al. 2018. Identifying, collecting, and presenting hacker community data: Forums, IRC, carding shops, and DNMs. In *2018 IEEE international conference on intelligence and security informatics (ISI)*. IEEE, IEEE, Miami, FL, USA, 70–75.

[34] Mike Ebinum. 2016. How To: Business Model Canvas Explained. https://medium.com/seed-digital/how-to-business-model-canvas-explained-ad3676b6fe4a

[35] EC-Council. 2019. 9 Of The Biggest botnet Attacks Of The 21st Century. https://blog.eccouncil.org/9-of-the-biggest-botnet-attacks-of-the-21st-century/#:~:text=EarthLink%20Spammer%E2%80%942000&text=Over%201.25%20million%20malicious%20emails,the%20information%20to%20the%20sender

[36] EMCDDA. 2020. EMCDDA special report: COVID-19 and drugs – Drug supply via darknet markets. https://www.emcdda.europa.eu/publications/ad-hoc/covid-19-and-drugs-drug-supply-via-darknet-markets

[37] Enisa. 2020. ENISA Threat Landscape 2020 - Cryptojacking. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cryptojacking

[38] Enisa. 2020. Enisa Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

[39] Jose Esteves, Elisabeth Ramalho, and Guillermo De Haro. 2017. To improve cybersecurity, think like a hacker. *MIT Sloan Management Review* 58, 3 (2017), 71.

[40] Europol. 2014. Global Action Targeting Shylock Malware. https://www.europol.europa.eu/newsroom/news/global-action-targeting-shylock-malware

[41] Europol. 2015. Botnet Taken Down Through International Law Enforcement Cooperation. https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation

[42] Europol. 2016. 'Avalance' Network Dismantled In International Cyber Operation. https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

[43] Europol. 2019. MONEY MULING: Public awareness and prevention. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling#:~:text=What%20is%20Money%20Muling%3F,a%20type%20of%20money%20laundering.&text=Even%20if%20money%20mules%20are,the%20proceeds%20of%20such%20crimes.

[44] Europol. 2021. World'S Most Dangerous Malware Emotet Disrupted Through Global Action. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[45] Flashpoint. 2020. Dark Web Marketplaces 2020. https://go.flashpoint-intel.com/docs/flashpoint-pricing-analysis-dark-web-marketplaces-2020

[46] Richard Ford and Sarah Gordon. 2006. Cent, Five Cent, Ten Cent, Dollar: Hitting Botnets Where It Really Hurts. In *Proceedings of the 2006 Workshop on New Security Paradigms* (Germany) *(NSPW '06)*. Association for Computing Machinery, New York, NY, USA, 3–10. https://doi.org/10.1145/1278940.1278942

[47] Nathan Friess and John Aycock. 2007. Black market botnets. https://prism.ucalgary.ca/handle/1880/45380.

[48] D. Frkat, R. Annessi, and T. Zseby. 2018. ChainChannels: Private Botnet Communication Over Public Blockchains. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, Halifax, NS, Canada, 1244–1252. https://doi.org/10.1109/Cybermatics_2018.2018.00219

[49] Sebastian Garcia, Martin Grill, Jan Stiborek, and Alejandro Zunino. 2014. An empirical comparison of botnet detection methods. *computers & security* 45 (2014), 100–123.

[50] Dimitrios Georgoulias, Jens Myrup Pedersen, Morten Falch, and Emmanouil Vasilomanolakis. 2021. A qualitative mapping of Darkweb marketplaces. In *2021 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Boston, MA, USA, 1–15. https://doi.org/10.1109/eCrime54498.2021.9738766

[51] Dimitrios Georgoulias, Jens Myrup Pedersen, Morten Falch, and Emmanouil Vasilomanolakis. 2022. COVID-19 Vaccination Certificates in the Darkweb. https://doi.org/10.1145/3530877

[52] Miguel Gomez. 2020. Dark Web Price Index 2020. https://www.privacyaffairs.com/dark-web-price-index-2020/#6

[53] Max Goncharov. 2012. Russian underground 101. , 51 pages.

[54] Max Goncharov. 2015. Criminal Hideouts for Lease: Bulletproof Hosting Services. https://www.trendmicro.no/media/wp/wp-criminal-hideouts-for-lease-en.pdf

[55] Joan Goodchild. 2011. Conficker Working Group says worm is stopped, but not gone. https://www.csoonline.com/article/2126743/conficker-working-group-says-worm-is-stopped--but-not-gone.html

[56] Julian B. Grizzard, Vikram Sharma, Chris Nunnery, Brent ByungHoon Kang, and David Dagon. 2007. Peer-to-Peer Botnets: Overview and Case Study. In *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets* (Cambridge, MA) *(HotBots'07)*. USENIX Association, USA, 1.

[57] Alex Guirakhoo. 2019. Understanding The Different Cybercriminal Platforms: AVCs, Marketplaces, And Forums. https://www.digitalshadows.com/blog-and-research/understanding-the-different-cybercriminal-platforms-avcs-marketplaces-and-forums/

[58] Hackerspaces. 2020. Hackerspace IRC Channels. https://wiki.hackerspaces.org/IRC_Channel

[59] Juan Hardoy. 2015. Breaking Up a Botnet – How Ramnit was Foiled. https://blogs.microsoft.com/eupolicy/2015/10/22/breaking-up-a-botnet-how-ramnit-was-foiled/

[60] Alex Hern. 2020. Silk Road bitcoins worth $1bn change hands after seven years. https://www.theguardian.com/technology/2020/nov/04/silk-road-bitcoins-worth-1bn-change-hands-after-seven-years

[61] Keman Huang, Michael Siegel, and Stuart Madnick. 2018. Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR)* 51, 4 (2018), 1–36.

[62] Thomas S. Hyslip. 2020. *Cybercrime-as-a-Service Operations*. Springer International Publishing, Cham, 815–846. https://doi.org/10.1007/978-3-319-78440-3_36

[63] Ionut Ilascu. 2020. TrickBot malware under siege from all sides, and it's working. https://www.bleepingcomputer.com/news/security/trickbot-malware-under-siege-from-all-sides-and-its-working/

[64] Cambridge University Institute for Manufacturing. 2016. Porter's Value Chain. https://www.ifm.eng.cam.ac.uk/research/dstools/value-chain-/

[65] Interpol. 2015. INTERPOL supports global operation against Dorkbot botnet. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2015/INTERPOL-supports-global-operation-against-Dorkbot-botnet

[66] Erik Kain. 2013. The Silk Road Shuts Down, But The Black Market Isn't Going Anywhere. https://www.forbes.com/sites/erikkain/2013/10/02/the-silk-road-shuts-down-but-the-black-market-isnt-going-anywhere/?sh=6cff0e987a6c

[67] Mohammad Karami, Youngsam Park, and Damon McCoy. 2016. Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services. In *Proceedings of the 25th International Conference on World Wide Web* (Montréal, Québec, Canada) *(WWW '16)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 1033–1043. https://doi.org/10.1145/2872427.2883004

[68] Kaspersky. 2014. Shylock/Caphaw malware Trojan: the overview. https://securelist.com/shylockcaphaw-malware-trojan-the-overview/64599/

[69] Kaspersky. 2021. Zeus Virus. https://usa.kaspersky.com/resource-center/threats/zeus-virus

[70] Limor Kessem. 2015. The Return of Ramnit: Life After a Law Enforcement Takedown. https://securityintelligence.com/the-return-of-ramnit-life-after-a-law-enforcement-takedown/

[71] S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, and S. A. Khayam. 2014. A Taxonomy of Botnet Behavior, Detection, and Defense. *IEEE Communications Surveys Tutorials* 16, 2 (2014), 898–924. https://doi.org/10.1109/SURV.2013.091213.00134

[72] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and other botnets. *Computer* 50, 7 (2017), 80–84. https://ieeexplore.ieee.org/abstract/document/7971869.

[73] Brian Krebs. 2011. U.S. Government Takes Down Coreflood Botnet. https://krebsonsecurity.com/2011/04/u-s-government-takes-down-coreflood-botnet/

[74] Brian Krebs. 2011. 'Biggest Cybercriminal Takedown in History'. https://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/

[75] Brian Krebs. 2012. Top Spam Botnet, "Grum," Unplugged. https://krebsonsecurity.com/2012/07/top-spam-botnet-grum-unplugged/

[76] Brian Krebs. 2017. Who is Anna-Senpai, the Mirai Worm Author? https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

[77] Brian Krebs. 2021. International Action Targets Emotet Crimeware. https://krebsonsecurity.com/2021/01/international-action-targets-emotet-crimeware/

[78] Joseph Kurian. 2018. Value Chain Analysis. http://apppm.man.dtu.dk/index.php/Value_Chain_Analysis

[79] Scott Langdon. 2020. Is Bitcoin Traceable? Things You Must Know. https://www.moneytaskforce.com/money/is-bitcoin-traceable/

[80] Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Márk Félegyházi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. 2011. Click Trajectories: End-to-End Analysis of the Spam Value Chain. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy (SP '11)*. IEEE Computer Society, USA, 431–446. https://doi.org/10.1109/SP.2011.24

[81] John Leyden. 2012. Microsoft seizes Chinese dot-org to kill Nitol bot army. https://www.theregister.com/2012/09/13/botnet_takedown/

[82] Zhen Li and Qi Liao. 2014. Toward a Monopoly Botnet Market. *Information Security Journal: A Global Perspective* 23, 4-6 (2014), 159–171. https://doi.org/10.1080/19393555.2014.931488

[83] Zhen Li, Qi Liao, and Aaron Striegel. 2009. Botnet economics: uncertainty matters. In *Managing information risk and the economics of security*. Springer, Boston, MA, 245–267. https://link.springer.com/chapter/10.1007/978-0-387-09762-6_12.

[84] MalwareBytes. 2021. Ryuk ransomware. https://www.malwarebytes.com/ryuk-ransomware/

[85] Malwarebytes. 2021. Trickbot. https://www.malwarebytes.com/trickbot/

[86] Etay Maor. 2013. No Money Mule, No Problem: Recruitment Website Kits for Sale. https://securityintelligence.com/money-mule-problem-recruitment-website-kits-sale/

[87] MalwareTech Marcus Hutchins. 2017. The Kelihos Botnet. https://www.malwaretech.com/2017/04/the-kelihos-botnet.html

[88] matricksillex. 2020. Dread (Darknet Market Forum) Review and Tutorial. https://darkrebel.net/dread-darknet-market-forum-review-and-tutorial

[89] matricksillex. 2020. HYDRA Review and Tutorial. https://darkrebel.net/hydra-review-and-tutorial

[90] matricksillex. 2020. ToRRez Market Review and Tutorial. https://darkrebel.net/torrez-market-review-and-tutorial

[91] matricksillex. 2020. White House Market Review and Tutorial. https://darkrebel.net/white-house-market-review-and-tutorial

[92] Matt. 2020. How dark web users utilise postal services to buy and ship drugs. https://www.osintme.com/index.php/2020/06/12/how-dark-web-users-utilise-postal-services-to-buy-and-ship-drugs/

[93] Michael McCaul. 2017. The war in cyberspace: Why we are losing—How to fight back. https://www.youtube.com/watch?v=nq__jneFcps&ab_channel=RSAConference

[94] Christopher D McDermott, Farzan Majdani, and Andrei V Petrovski. 2018. Botnet detection in the internet of things using deep learning approaches. In *2018 international joint conference on neural networks (IJCNN)*. IEEE, IEEE, USA, 1–8.

[95] Elliott Peterson Michael Sandee, Tillmann Werner. 2015. Gameover Zeus – Bad Guys and Backends. https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends.pdf

[96] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, and Richard Brooks. 2016. A brief survey of cryptocurrency systems. In *2016 14th annual conference on privacy, security and trust (PST)*. IEEE, IEEE, Auckland, New Zealand, 745–752.

[97] Simon Mullis. 2013. Cybercriminal Intent: How to Build Your Own Botnet in Less Than 15 Minutes. https://www.fireeye.com/blog/executive-perspective/2013/08/cybercriminal-intent-how-to-build-your-own-botnet-in-less-than-15-minutes.html

[98] Atif Mushtaq. 2012. Killing the Beast - Part 5. https://www.fireeye.com/blog/threat-research/2012/07/killing-the-beast-part-5.html

[99] Yacin Nadji, Manos Antonakakis, Roberto Perdisci, David Dagon, and Wenke Lee. 2013. Beheading Hydras: Performing Effective Botnet Takedowns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security* (Berlin, Germany) *(CCS '13)*. Association for Computing Machinery, New York, NY, USA, 121–132. https://doi.org/10.1145/2508859.2516749

[100] Rebecca R. Ruiz Nathaniel Popper. 2017. 2 Leading Online Black Markets Are Shut Down by Authorities. https://www.nytimes.com/2017/07/20/business/dealbook/alphabay-dark-web-opioids.html

[101] Alexander Osterwalder. 2012. The Business Model Canvas. https://www.youtube.com/watch?v=RzkdJiax6Tw&t=1939s&ab_channel=GonzaloAste

[102] Alexander Osterwalder and Yves Pigneur. 2010. *Business model generation: a handbook for visionaries, game changers, and challengers*. John Wiley & Sons, Hoboken, New Jersey.

[103] Mehul Patel. 2019. Cat and Mouse: Understanding the Security Industry's Failure to Stop Cyberattackers. https://securityboulevard.com/2019/08/cat-and-mouse-understanding-the-security-industrys-failure-to-stop-cyberattackers/

[104] Caitlin Ostroff Paul Vigna. 2020. Why Hackers Use Bitcoin and Why It Is So Difficult to Trace. https://www.wsj.com/articles/why-hackers-use-bitcoin-and-why-it-is-so-difficult-to-trace-11594931595

[105] Check Point. 2021. February 2021's Most Wanted Malware: Trickbot Takes Over Following Emotet Shutdown. https://blog.checkpoint.com/2021/03/11/february-2021s-most-wanted-malware-trickbot-takes-over-following-emotet-shutdown/

[106] Robey Pointer. 2021. Eggdrop. https://www.eggheads.org/

[107] Dutch Police. 2021. International police operation LadyBird: global botnet Emotet dismantled. https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html

[108] Michael E Porter and Competitive Advantage. 1985. Creating and sustaining superior performance. *Competitive advantage* 167 (1985), 167–206.

[109] Howard Poston. 2020. Cybercrime at scale: Dissecting a dark web phishing kit. https://resources.infosecinstitute.com/topic/cybercrime-at-scale-dissecting-a-dark-web-phishing-kit/

[110] K Munivara Prasad, A Rama Mohan Reddy, and K Venugopal Rao. 2020. BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web. *Journal of King Saud University-Computer and Information Sciences* 32, 1 (2020), 73–87.

[111] C. G. J. Putman, Abhishta, and L. J. M. Nieuwenhuis. 2018. Business Model of a Botnet. In *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*. IEEE, USA, 441–445. https://doi.org/10.1109/PDP2018.2018.00077

[112] Peter Reuter. 2005. *Chasing dirty money: The fight against money laundering*. Peterson Institute, 1750 Massachusetts Avenue, NW Washington, DC 20036.

[113] Rafael A. Rodríguez-Gómez, Gabriel Maciá-Fernández, and Pedro García-Teodoro. 2013. Survey and Taxonomy of Botnet Research through Life-Cycle. *ACM Comput. Surv.* 45, 4, Article 45 (Aug. 2013), 33 pages. https://doi.org/10.1145/2501654.2501659

[114] Raj Samani and Francois Paget. 2013. Cybercrime exposed: Cybercrime-as-a-service.

[115] Jason Sattler. 2019. What we've learned from 10 years of the Conficker mystery. https://blog.f-secure.com/what-weve-learned-from-10-years-of-the-conficker-mystery/

[116] Mathew J. Schwartz. 2013. Microsoft, FBI Trumpet Citadel Botnet Takedowns. https://www.darkreading.com/attacks-and-breaches/microsoft-fbi-trumpet-citadel-botnet-takedowns/d/d-id/1110261

[117] Mathew J. Schwartz. 2015. Dorkbot Botnets Get Busted. https://www.bankinfosecurity.com/dorkbot-ddos-botnets-get-busted-a-8728

[118] Vicente Segura and Javier Lahuerta. 2010. Modeling the economic incentives of ddos attacks: Femtocell case study. In *Economics of information security and privacy*. Springer, Boston, MA, 107–119. https://doi.org/10.1007/978-1-4419-6967-5_7.

[119] Shadowserver. 2017. Kelihos.E Botnet – Law Enforcement Takedown. https://www.shadowserver.org/news/kelihos-e/

[120] Shadowserver. 2018. Avalanche 1,2,3.... https://www.shadowserver.org/news/avalanche-123/

[121] Howard Shrobe, David L. Shrier, and Alex Pentland. 2018. *CHAPTER 4 Fixing a Hole: The Labor Market for Bugs*. MIT Press, Massachusetts, 129–159.

[122] Signal. 2020. 5 Dark Web Marketplaces Security Professionals Need To Know About. https://www.getsignal.info/blog/5-dark-web-marketplaces

[123] Signal. 2020. 7 Dark web Forums You Need To Monitor For Improved Cyber Security. https://www.getsignal.info/blog/7-dark-web-forums-for-improved-cybersecurity

[124] Sérgio S.C. Silva, Rodrigo M.P. Silva, Raquel C.G. Pinto, and Ronaldo M. Salles. 2013. Botnets: A survey. *Computer Networks* 57, 2 (2013), 378 – 403. https://doi.org/10.1016/j.comnet.2012.07.021 Botnet Activity: Analysis, Detection and Shutdown.

[125] Craig Sirois. 2020. New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion. https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629&utm_source=twitter_mcafee&utm_medium=social_organic&utm_term&utm_content&utm_campaign&sf240838844=1

[126] Aditya K Sood, Rohit Bansal, and Richard J Enbody. 2012. Cybercrime: Dissecting the state of underground enterprise. *IEEE internet computing* 17, 1 (2012), 60–68.

[127] Aditya K Sood and Richard J Enbody. 2013. Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection* 6, 1 (2013), 28–38.

[128] Staff and The Guardian agencies in Berlin. 2019. German police shut down one of world's biggest dark web sites. https://www.theguardian.com/world/2019/may/03/german-police-close-down-dark-web-marketplace

[129] Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '09)*. Association for Computing Machinery, New York, NY, USA, 635–647. https://doi.org/10.1145/1653662.1653738

[130] Brett Stone-Gross, Thorsten Holz, Gianluca Stringhini, and Giovanni Vigna. 2011. The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. *LEET* 11 (2011), 4–4. https://www.usenix.org/legacy/event/leet11/tech/full_papers/Stone-Gross.pdf.

[131] Strategyzer. 2020. Business Model Canvas. https://www.strategyzer.com/bmc_thank_you?submissionGuid=9a5690b9-b0d9-4274-b423-a121993570ec

[132] Matt Sully and Matt Thompson. 2010. The deconstruction of the Mariposa botnet. *Defence Intelligence. Retrieved September* 16 (2010), 2012.

[133] Evan Tarver. 2019. What Are the Primary Activities of Michael Porter's Value Chain? https://www.investopedia.com/ask/answers/050115/what-are-primary-activities-michael-porters-value-chain.asp

[134] Digital Shadows Analyst Team. 2017. Innovation In The Underworld: Reducing The Risk Of Ripper Fraud. https://www.digitalshadows.com/blog-and-research/innovation-in-the-underworld-reducing-the-risk-of-ripper-fraud/

[135] TheDarkWebLinks. 2020. Torrez Market | Torrez Market Links | Torrez Dark Web Links. https://www.thedarkweblinks.com/torrez-market/

[136] Iain Thompson. 2017. International team takes down virus-spewing Andromeda botnet. https://www.theregister.com/2017/12/05/international_team_takes_down_virusspewing_andromeda_botnet/

[137] Iain Thomson. 2016. Online criminals iced as cops bury malware-spewing Avalanche. https://www.theregister.com/2016/12/01/cops_shutter_avalanche_dark_net/

[138] Tillmann. 2013. Peer-to-Peer Poisoning Attack against the Kelihos.C Botnet. https://www.crowdstrike.com/blog/peer-peer-poisoning-attack-against-kelihosc-botnet/

[139] Tor. 2019. Tor: Onion Service Protocol. https://2019.www.torproject.org/docs/onion-services

[140] Ian Traynor. 2007. Russia accused of unleashing cyberwar to disable Estonia.

[141] Trendmicro. 2021. Ransomware. https://www.trendmicro.com/vinfo/us/security/definition/ransomware

[142] Ping Wang, Baber Aslam, and Cliff C Zou. 2010. Peer-to-peer botnets. In *Handbook of Information and Communication Security*. Springer, University of Central Florida, Orlando, Florida 32816, 335–350.

[143] Ping Wang, Lei Wu, Baber Aslam, and Cliff C. Zou. 2009. A Systematic Study on Peer-to-Peer Botnets. In *Proceedings of the 2009 Proceedings of 18th International Conference on Computer Communications and Networks (ICCCN '09)*. IEEE Computer Society, USA, 1–8. https://doi.org/10.1109/ICCCN.2009.5235360

[144] Rob Wright. 2018. Botnet takedown snares 3ve, Methbot ad fraud campaigns. https://searchsecurity.techtarget.com/news/252453401/Botnet-takedown-snares-3ve-Methbot-ad-fraud-campaigns

[145] Rob Wright. 2019. FBI: How we stopped the Mirai botnet attacks. https://searchsecurity.techtarget.com/news/252459016/FBI-How-we-stopped-the-Mirai-botnet-attacks

[146] Sam Zeitlin. 2015. Botnet takedowns and the fourth amendment. *NYUL Rev.* 90 (2015), 746.

[147] Ziming Zhao, Mukund Sankaran, Gail-Joon Ahn, Thomas J Holt, Yiming Jing, and Hongxin Hu. 2016. Mules, seals, and attacking tools: Analyzing 12 online marketplaces. *IEEE Security & Privacy* 14, 3 (2016), 32–43.