Understanding Crypter-as-a-Service in a popular underground marketplace

Alejandro de la Cruz Alvarado
Universidad Carlos III de Madrid
Madrid, Spain
alcruza@pa.uc3m.es

Sergio Pastrana Portillo
Universidad Carlos III de Madrid
Madrid, Spain
spastran@inf.uc3m.es

***Abstract*—Crypters are pieces of software whose main goal is to transform a target binary so it can avoid detection from Anti Viruses (AVs from now on) applications. They work similar to packers, by taking a malware binary M and applying a series of modifications, obfuscations and encryptions to output a binary M' that evades one or more AVs. The goal is to remain fully undetected, or FUD in the hacking jargon, while maintaining its (often malicious) functionality. The Crypter-as-a-Service model is a popular activity among the commoditization in cybercrime, due to the increased sophistication of detection mechanisms. In this business model, customers receive an initial crypter which is soon updated once becomes detected by anti-viruses. This paper provides the first study on an online underground market dedicated to Crypter-as-a-Service. We compare the most relevant products in sale, analyzing the existent social network on the platform and comparing the different features that they provide.**

***Index Terms*—Crypter, Cybercrime, Underground Forums, Crawler, Social Networks**

1. Introduction

Cybercrime is a growing issue, with an increased prevalence since the 2020 pandemic [1]. The availability of low-level hacking tools in public underground forums lowers the barrier for non-expert users (or script-kiddies as they are known in the community), have ease the access to exploits and hacking material that can be used for malicious intentions [2], [3]. It is thus important to study how it evolves and what is the current status of the different activities [4]. As long as cyberdefenses are improved, cybercriminals also want to adapt in a never-ending cat-and-mouse game [5]. Crypters, our focus in this study, is a type of packer that cryptographically modifies a binary to evade antivirus engines. Since they need to be updated once antiviruses detect them, the Crypter-as-a-Service model emerged which provides such updates as required. It fosters the entrepreneurship of criminal endeavors, allowing to bypass one of the most complex barriers, i.e., the technical skill [6].

Related Work. Previous work have studied malware and other hacking tools traded in underground forums. The work by Valero and García reviews some of the most significant remote access trojan (known as RATs) along the years comparing its functionalities, the forums they used to spread and attacks where they were used [7]. Regarding obfuscation, Efstratios et al. analyzed multiple evasion techniques for antiviruses written in Go, Rust and C++ Also, they analyse the use of ChatGPT to explore its capabilities to generate malware [8]. Sembera et al. analyzed one service providing obfuscation for malware in the Android ecosystem, studying the features and economy of such particular service [9]. We refer to the survey by Muralidharan et al. for a description of the most current techniques for malware obfuscation for PE files [10]. Despite the high amount of academic research on cybercrime, with some works specializing in technical details of obfuscation tools [8]–[10], there is a gap of studies focused on the Crypter-as-a-Service (CaaS) ecosystem, from the marketing and operation perspective. Concretely, in this work we aim to address the following research questions: 1) What is the prevalence of crypters being being traded and sought? 2) Is there any kind of specialization?, or do crypters provide similar features? 3) What is the Social Network of users engaged in the trading of forums?

To answer this questions, we analyze a dedicated marketplace of crypters traded in HackForums, a popular english-speaking underground forum [2], [11]. We analyze their most common properties, the techniques used to advertise their products and attract new customers, and the differences between the most popular ones. We also analyze the social network formed by the actor involved in creating, buying and interacting with the multiple products available.

Overall, the main contributions of this paper are the following:

- We describe the Crypter-as-a-Service model (§2) and provide the first quantitative analysis of the whole CaaS ecosystem in a dedicated forum along with a deeper study of the products sold and the activity in the marketplace.
- We describe our custom crawler for data collection method, that allows us to obtain a total of 1,492 threads or posts and 128,384 comments in those posts along with the information of 17,751 users.
- We conduct an analysis of the collected data, including the top100 crypters being sold, and the social network analysis of the marketplace to find market niches, the most relevant users and differences between products being sold.

Finally, to foster research in the area and allow for reproducibility, we open-source the crawler, the analysis scripts and an extended version of this work with

additional analyses and a practical case study in our repository [12].

2. The Crypter-as-a-Service (CaaS) model

The commoditization of products and services available in online market and forums [3] fosters the grow of criminal activities. This fosters the rise of Business-to-Business (B2B) services, where criminals provide necessary services and products to others, cultivating criminal 'entrepreneurship' [6]. In the case of malware infection, it requires at least three main services: malware development (e.g., acquiring a customized crytomining malware [13] or banking trojans [14]), malware spreading (e.g., buying 'installs' from botnet operators to spread the malware across several victims [15]), and malware obfuscation, so it remains undetected and allows for persistence on the infected computers [9]. The latter, which is the focus of this paper, is often conducted by means of crypters.

A crypter is commonly composed by two parts: the "builder" and the "stub". The former is responsible for the encryption and obfuscation of the binary and some personalized tuning. Since crypters are commercial products, potentially targeted for users with little or no technical knowledge, the builder usually includes a graphical user interface (GUI), with step-by-step instructions, and even customer support. Other complementary functionalities advertised are icon and name customization, delayed start and persistence (see Section 4). The "stub", which is the most important component of a crypter, is the file being generated as output and in charge of the decryption and execution of the original malware. Since this is the piece that will be installed on a victims' computer, it requires to evade AVs [16].

The builder disguises the malware by obfuscating it using different means, most commonly by shuffling instructions, encrypting it completely and hiding them in a benign (undetected) file or "stub". Then this stub decrypts the actual binary in memory at runtime, and executes the original functionality with a technique known as Dynamic Forking [17], which basically invokes a suspended process and then gets replaced by the malicious process to be executed. Since the stub is a static part, it can be detected by antivirus. Indeed, as soon as a stub is fingerprinted by any AV, any malware using it is quickly detected and the crypter becomes useless. Accordingly, most of the crypters' providers update the stub when needed, to guarantee that it remains 'fully undetected" (or FUD, in the underground jargon). This is the reason for the emergence of the 'Crypter-as-a-Service' business model.

Figure 1 depicts the different stages a crypter goes through from the original binary to a shuffled and obfuscated set of instructions split inside the stub or "FUD" binary.

Crypters can be classified into scantime crypter or runtime crypter, based on the stage when the binary needs to be hidden. A scantime crypter remains static in disk, thus bypassing traditional antiviruses, while a runtime crypter is loaded in memory and needs to be more complex to evade other tools and defenses such as Host IDS, Windows AMSI or Endpoint Detection and Response (EDR) systems.

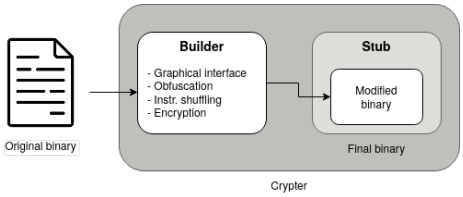

Figure 1. Components of a crypter

The Crypter-as-a-Service paradigm is based on other crime-as-a-service models [18] with several roles which might be operated by the same individual, or they can be diversified with a entrepreneurial approach [6] (see Figure 2). This model is reinforced by our quantitative analysis, detecting multiple duplicated products and authors of posts claiming not to be the developer of the crypter but the reseller. We describe the three most common roles involved:

1) The *developer* team is in charge of programming and updating the main technical components of the crypter.
2) The *commercial* team advertises the service in underground forums or web portal where the crypter is being sold. Its main goal is to attract customers and also to provide customer support.
3) The *finance* team creates and maintains the payment platform. This is often based on cryptocurrencies (e.g., Bitcoin, Ethereum or Monero), or by other online payment systems popular in criminal businesses, such as PayPal or Amazon Gift Cards. It must keep the payments anonymous, and also is responsible for the money laundering.

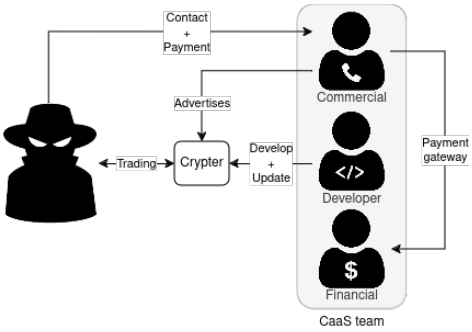

Figure 2. B2B relations in the Crypter-as-a-Service model

The never ending race between antivirus and malware obfuscation makes the crypter-a-service business a relevant aspect in the cyber-criminal landscape, since this is a key component to maintain the kill-chain during malware infection. Accordingly, there are underground marketplaces and forums specialized in the trading of these services. One of the largest belongs to HackForums, which is the focus of our study as we detail in the following sections.

3. Data collection

This study focuses on the marketplace of crypters traded in HackForums. Thus, following existing methods [2], [19], we crawl and scrape all the threads in

the forum, and dump the information into a database for offline analysis.

3.1. Data structure

HackForums is a public forum which has been the home for various cybercriminals [20], [21]. We focus on the marketplace under the "Cryptography and Encryption" sub-forum, to get all the threads announcing crypters. Marketplaces in HackForums are structured in different threads where the original post is the announcement of a product, in this case, a crypter. In this thread, users leave comments with questions regarding the product, request free trials, test the results against AVs, or to rate the product. The product announcement might include a pamphlet with the main characteristics, the price and in general any information that might be useful for potential customers. On top of that, the thread creator might also share any social media profile where users can reach to purchase the crypter or request further information.

While threads are listed without the need for an account, we need to access the posts (replies) of the thread. This poses an additional challenge, since accessing the contents of a thread requires to be logged into the website, and with the amount of captchas and bot detection it is hard to automate. We those implement common methods to bypass the access barriers [19], e.g., manually solving captchas and re-using the session cookies, or limiting the requests made per minute. From each post, we extract the following information: the original post content, the image (pamphlet) used to announce the crypter (if any), and all the replies (posts) of the thread. These interactions between users and posts allow to visualize the social network of crypter producers and consumers. Overall, we collected 1,492 posts from 279 different users and 128,384 comments in those posts from a total of 15,745 users. We conducted our crawling on April 2023, collecting historical data that spans for 13 years.

4. Data Analysis

We first analyze the data to characterize the information and provide a general measurement. Then, we analyze the most popular crypters (measured by number of views), to have a more precise view over them. Finally, we conduct social network analysis of the forum. The goal of these analyses is to better understand the global ecosystem of the sub-forum, its social network, and to highlight common properties and differences between popular crypters advertised, studying market dynamics.

4.1. General measurement

We analyze the most frequent words to derive insights on the offered features. We took the number of occurrences for every word found in the threads of the marketplace, removed the non-significant words for this study such as pronouns, articles, etc. and limited our study to words with over one thousand appearances.

The most recurrent words obtained are related to properties of the crypter (*"crypter", "FUD"*), ratings of the product, users asking for free *"vouches"* or *"trials"*, the type of stub used (*"private"*, *"runtime"*), topics related to antiviruses (*"antivirus"* being the second most used word, but also *"panda"*, *"avast"* or *"norton"*), and contact info for the seller (*"discord"*, *"email"*). This shows that users are mostly concerned with the product sold and its effectiveness.

Next, we analyze the activity on the forum and its evolution across time. Figure 3 shows monthly activity for both the comments (in red) and threads initiated in the marketplace (in blue). As it can be observed the sub-forum gained rapid popularity from its creation, in 2009.

In 2011 there are two significant events that might have led to the decrease in crypter activity, first the hacktivist group known as "LulzSec" leaked credentials and personal information of nearly 200,000 users from HackForums [22]. The forum reputation took such a hit that it has not really recovered ever since in terms of publications as seen by the sudden drop by that year. Additionally, as explored by Bhalerao et al. [23], in 2014 malware obfuscation alternatives became more frequent and crypters lost their popularity. Also, it's noteworthy a spike in late 2013, which we can not relate to any other public incident or event. Finally, in 2020 there is a slight increase in the activity, potentially derived from the lockdown effects [1].

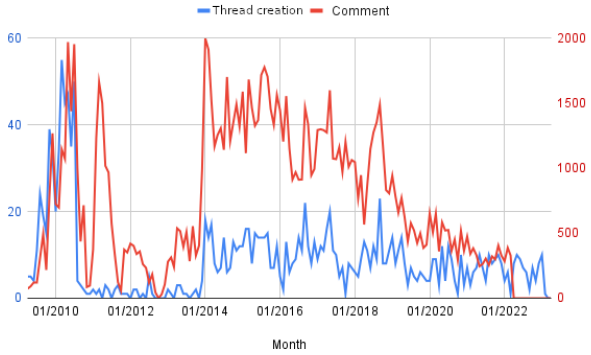

Figure 3. Thread creation and comments over time

The last approach in the general analysis is know the number of posts asking for help, to understand the prevalence of newcomers and actors seeking obfuscation for their cybercriminal goal. A simple –yet effective– way to achieve this classification is by using keywords in the context of asking for help. Concretely: "help", "need", "advice", "advise", "buy", "request", "question", "looking for", "doubt", "seeking".

Out of 1,492 posts, 371 of them (24.87%) are asking for something instead of selling a product. Examples of these threads are: "Crypter NEEDED!! PLEASE READ!!", "PDF EXPLOIT NEEDED ASAP" or even "I want to buy infected computers" 6 Signs of a Poorly Dressed Man — Men's Fashion Mistakes . This shows that this community is a marketplace providing both products and assistance, confirming the role of crypters on the supply chain within the cybercrime ecosystem [24].

4.2. Top100 crypters

To better understand the CaaS ecosystem, we conduct a detailed analysis of the top 100 cryters (by number

of views) to ensure we analyze the most significant and popular products of the sub-forum. Posts usually combine written text with image pamphlets, which hardens the text extraction. While we attempted the use OCR (optical character recognition) [25], the data extraction was inexact and led to multiple errors, hindering automatic analysis. Thus, we opted to conduct the analysis manually.

Even though these products are intended for malicious purposes, they are also commercial products being sold in a public marketplace. Thus, they apply marketing techniques to attract customers, build a brand and gain reputation. The marketing aspect is often provided in the pamphlet that summarizes the specific features of the crypter, price, payment methods and contact details. To foster confidence, they often give away free vouchers after publishing a product, to show the bypass rate and gain trust and reputation in the community [26]. Customer satisfaction is an important factor. Most of the services announce 24/7 customer support, reply to comments in the forum and update the original post of the thread quite often to appear active. As they are products with potential misuse being sold in a public website, they often disengage from any responsibility with a disclaimer, typically forbidding their usage for illegal activities.

Out of the top 100 posts, 11 of them were currently closed or paused at the time of the analysis, and only 15 have been active since 2020, which is in accordance with the timeline analysis provided in the previous section. Regarding crypter providers, there are 13 users that have created (or advertised) two, three or four of them, the most remarkable of them is User 2 in Table 1, who is tied in the top one creators and three of his posts have been active in the past three years, even though two of them seem to be duplicates of the same crypter "FLOW CRYPTER PRO V7" This user resembles the role of a reseller o "commercial", i.e. users who are only in charge of the marketing and selling of products, thus hiding the actual creator and allowing them to remain anonymous. Regarding pamphlets, we observe that 27 use this method. This shows that the use of pamphlets does not necessarily reflect a higher impact of the product.

Crypters offer similar technical functionalities (custom startup, customer icon, virtual machine and sandbox detection), platform and payment methods. The latter often rely on cryptocurrencies such as Bitcoin or Ethereum, and sometimes also PerfectMoney, which is a system that does not force verification, allowing for anonymous payments.

Table 1 compares the fifteen posts within the top100 that are still active since 2020, their overall position in the top 100, name, id of the creator (that has been anonymized), creation and last interaction years, price and the type of stub provided. There are three types of stubs: private, which allegedly means a different one for every buyer; standard, which is shared by all the users (or by every N users); and the unique stub generator, that uses a standard generator with some parameters to output some kind of pseudo-private stub. A private stub implies more work than a standard one, which is reflected in the price since it is always up to 10 times more expensive. But the advantage it poses is that the less users using the same stub, the lower the probability of it being fingerprinted and detected by AVs.

It is very common for creators to provide new stubs each time they are detected so customers can re-encrypt their malware in order to stay undetected as long as possible, they will usually notify them via the forum, on Telegram channels or other chosen channels.

4.3. Social Network

We finally analyze the social connections in the sub-forum dedicated to crypters on HackForums. We analyze the types of users based on their forum activity: number of posts they create, prevalence of users than only leave comments, users interactions with each post, and how frequency of these. This information allows to better understand user engagement in this forum, since it informs whether there is some specialization among users, or whether users who sell crypters also participate in discussions on others, or they just stick to their own product. The information is reflected in Table 2. A vast majority of the users (98.23%) only comment, instead of publishing threads, which is expected in a forum-like marketplace. Two-thirds of the users only interact with one post, which suggests the general tendency for low interaction with the sub-forum apart from buying and help-seeking. Lastly, we have the 'creators', i.e., users that publish one or more crypters, where the most common case is users that create one post and comment on several others.

To better reflect the interactions of users with posts, we have created a weigthed graph of the social connections of posts and users within the top 100 posts, with two type of edges, i.e., creation and commenting of posts. The weight reflects the number of comments of a given user in a given post.. This allows to navigate and better analyze all these interactions in the marketplace in a visual way, e.g., focusing on a single node and get the number of comments left on it, or to differentiate users that have created a post (and which is it) from those that have not. The graph is fully interactive and available online [27], and Figure 4 shows a local representation. The analysis of the graph show that this is an homogeneous network, suggesting that the community is equally distributed, with no particular niches and specialized topics.

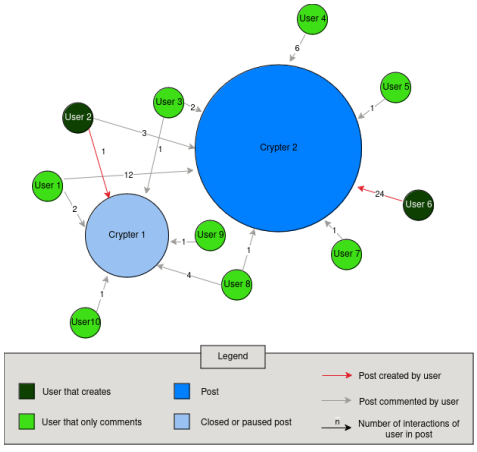

Figure 4. Screenshot of the social network graph

Additionally, we rely on common network metrics to find the most important nodes in our social network [28].

TABLE 1. 15 POSTS FROM THE TOP 100 THAT REMAIN ACTIVE SINCE 2020 (AS OF MAY'23)

Position	Name	Creator	Created	Last Comment	Views	Comments	Stub	Min cost	Max cost
3	ByteCrypter v3	User 1	2017	2023	205 721	3 282	Generator	35$ 3months	60$ lifetime
4	FLOW CRYPTER PRO V7	User 2	2017	2023	204 256	2 483	Standard	39,95$ 1month	147$ lifetime
11	CyberSeal	User 3	2017	2020	112 744	1 390	Standard	No info	No info
13	DATAPROTECTOR v4	User 4	2018	2020	109 893	1 865	Standard	50$ 45days	300$ lifetime
22	BetaCrypt	User 5	2014	2022	86 765	842	Private	210$ 1month	No info
27	PURE CRYPTER	User 6	2021	2023	73 027	885	Standard	No info	No info
30	Data Encoder Crypter	User 6	2020	2023	66 704	909	Both	60$ 1month Standard	175$ 180days Private
32	RAZ PRIVATE CRYPTS	User 7	2020	2023	56 526	619	Private	25$ 1crypt	285$ 15crypts
46	Cassandra Crypter	User 8	2019	2021	43 196	533	Generator	24.99$ 1month	No info
52	Code Protector	User 9	2019	2022	40 241	570	Standard	25$ 1month	65$ lifetime
61	STATIC CRYPT	User 10	2019	2022	27 663	359	Standard	50$ 1month	500$ lifetime
62	FLOW CRYPTER PRO V7	User 2	2018	2023	27 049	381	Private	20$ 1crypt	399$ 3months
63	PRIVATE CRYPTS	User 2	2020	2023	26 350	387	Private	20$ 1crypt	399$ 3months
65	TRILLIUM SECURITY FILE PROTECTOR V1.60	User 11	2020	2023	25 868	385	Both	125$ 1month Standard	550$ 1year
86	AtillaCrypt V2	User 12	2019	2020	16 119	280	Generator	35$ 1month	120$ 6months

TABLE 2. TYPES OF USERS IN THE MARKETPLACE

Description	Number	Percentage
Only commenting one post	9 999	63.5%
Commenting more than one post	5 467	34.72%
Creating and commenting one post	54	0.34%
Creating multiple posts and commenting one	11	0.07%
Creating one post and commenting multiple	154	0.98%
Creating and commenting multiple posts	60	0.38%
Total	15 745	100%

TABLE 3. EIGENVECTOR CENTRALITY

Position	Name	Eigenvector
3	ByteCrypter v3	0.3964
4	FLOW CRYPTER PRO V7	0.3815
13	DATAPROTECTOR v4	0.2258
27	PURE CRYPTER	0.2183
11	CyberSeal	0.2012

Concretely, degree centrality, i.e., the number of interactions to foreign posts (out-degree) from a user and the comments left in posts created by a user (in-degree); and the eigenvector, which measures the relevance of a node from the importance of its neighbor nodes.

The degree provides the "popularity" in the network, which we compare with the actual "reputation" of users in the forum, to figure out if there is any correlation between these two. We, however, observe few relation between the in and out degree in the graph and the popularity within the forum, showing that the crypter marketplace is an isolated environment, they are not as active in the rest of marketplaces and discussions in the website. For example, User 13 has the highest reputation in the forum (6596) and it only has an out-degree of 3 with no in-degree whatsoever. Meanwhile, the user with the highest in-degree is User 4, with 4543 and 1388 of reputation (almost a fifth of what user 13 has). When sorting by out-degree our top scorer is user 14 with 480 and a much lower (in comparison) popularity of 214. Sorting out users based on degree (combination of both in-degree and out-degree) user 4 is the highest , meaning that creating popular posts such as "DATAPROTECTOR v4" (top 13) is the most significant factor when becoming a relevant user in the marketplace.

The eigenvector offers more valuable results. As seen in Table 3, the top 5 nodes with highest eigenvector values are present in the top posts that are still active since 2020, compared in Table 1. The different order in these lists might be due to factors like the relevance of the users that comment on those posts, or the number of different users interacting with the post rather than the raw number of views and comments of the post.

5. Conclusions

In this paper, we study the Crypter-as-a-Service ecosystem in HackForums, observing a high prevalence of product and services being sold (though in decrease). Most of the advertised products and services offer similar features in their adverts, with similar properties, payment methods, customer support and close prices. The differentiating part is the way each crypter creates the stub (i.e., the encryption process), and also the customer support, i.e., the treatment given to customers once the service or product is delivered (e.g., quality of the support, how often they update stubs, or whether the actual stub is generic or private). We observe that crypters focus on PE files, although we also observe crypters for other platforms such as Android [9]. Finally, the social network analysis shows that most users do not engage actively in the market, with few actors acting as (re)sellers or developers. These insights may assist enforcement, since it suggest that an effective tactic would be to focus on the common techniques (e.g., for antivirus industry) and actors (e.g., for law enforcement officers).

Acknowledgments

As part of the open-report model followed by the Workshop on Attackers & CyberCrime Operations (WACCO), all the reviews for this paper are publicly available at https://github.com/wacco-workshop/WACCO/tree/main/WACCO-2024. This paper was partially supported by INCIBE grant APAMCiber within the framework of the Recovery, Transformation and Resilience Plan funds, financed by the European Union-NextGenerationEU, and by grant TED2021-132170A-I00 from the Spanish Ministry of Science and Innovation, funded by MCIN/AEI/10.13039/501100011033, and the European Union-NextGenerationEU/PRTR.

References

[1] D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, and N. Díaz-Castaño, "Cybercrime and shifts in opportunities during covid-19:

a preliminary analysis in the uk," *European Societies*, vol. 23, no. sup1, pp. S47–S59, 2021.

[2] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, "Crimebb: Enabling cybercrime research on underground forums at scale," in *Proceedings of the 2018 World Wide Web Conference*, ser. WWW '18. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2018, p. 1845–1854. [Online]. Available: https://doi.org/10.1145/3178876.3186178

[3] R. van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi, C. H. Ganan, B. Klievink, N. Christin, and M. van Eeten, "Plug and prey? measuring the commoditization of cybercrime via online anonymous markets," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1009–1026. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/van-wegberg

[4] J. Hughes, S. Pastrana, A. Hutchings, S. Afroz, S. Samtani, W. Li, and E. Santana Marin, "The art of cybercrime community research," *ACM Computing Surveys*, vol. 56, no. 6, pp. 1–26, 2024.

[5] A. Hutchings, S. Pastrana, and R. Clayton, "Displacing big data: How criminals cheat the system," in *The Human Factor of Cybercrime*. Routledge, 2019, pp. 408–424.

[6] R. Böhme, R. Clayton, and B. Collier, "Silicon den: Cybercrime is entrepreneurship," in *Workshop on the Economics of Information Security (WEIS)*, 2021.

[7] V. Valeros and S. Garcia, "Growth and commoditization of remote access trojans," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2020, pp. 454–462.

[8] E. Chatzoglou, G. Karopoulos, G. Kambourakis, and Z. Tsiatsikas, "Bypassing antivirus detection: old-school malware, new tricks," 2023.

[9] V. Šembera, M. Paquet-Clouston, S. Garcia, and M. J. Erquiaga, "Cybercrime specialization: An exposé of a malicious android obfuscation-as-a-service," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2021, pp. 213–226.

[10] T. Muralidharan, A. Cohen, N. Gerson, and N. Nissim, "File packing from the malware perspective: techniques, analysis approaches, and directions for enhancements," *ACM Computing Surveys*, vol. 55, no. 5, pp. 1–45, 2022.

[11] S. Pastrana, A. Hutchings, D. Thomas, and J. Tapiador, "Measuring ewhoring," in *Proceedings of the Internet Measurement Conference*, ser. IMC '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 463–477. [Online]. Available: https://doi.org/10.1145/3355369.3355597

[12] A. de la Cruz. (2023, Jun.) Hackforums crypters analysis repository. [Online]. Available: https://github.com/PaquitoelChocolatero/HFCrypterAnalysis

[13] S. Pastrana and G. Suarez-Tangil, "A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 73–86.

[14] M. Paquet-Clouston and S. García, "On the motivations and challenges of affiliates involved in cybercrime," *Trends in Organized Crime*, pp. 1–30, 2022.

[15] J. Caballero, C. Grier, C. Kreibich, and V. Paxson, "Measuring {Pay-per-Install}: The commoditization of malware distribution," in *20th USENIX Security Symposium (USENIX Security 11)*, 2011.

[16] T. Micro, "Crypter - definition," https://www.trendmicro.com/vinfo/us/security/definition/crypter, 2013, online: Last accessed 07/28/23.

[17] D. 0x00sec. (2016, May) Crypters - instruments of the underground. [Online]. Available: https://0x00sec.org/t/crypters-instruments-of-the-underground/386

[18] D. Manky, "Cybercrime as a service: a very modern business," *Computer Fraud & Security*, vol. 2013, no. 6, pp. 9–13, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372313700538

[19] K. Turk, S. Pastrana, and B. Collier, "A tight scrape: methodological approaches to cybercrime research data collection in adversarial environments," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2020, pp. 428–437.

[20] A. Hutchings and S. Pastrana, "Understanding ewhoring," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2019, pp. 201–214.

[21] S. Pastrana, A. Hutchings, A. Caines, and P. Buttery, "Characterizing eve: Analysing cybercrime actors in a large underground forum," in *Research in Attacks, Intrusions, and Defenses: 21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12, 2018, Proceedings 21*. Springer, 2018, pp. 207–227.

[22] (2011, Jun.) Have I been pwned? Pwned websites. [Online]. Available: https://web.archive.org/web/20151003211856/https://haveibeenpwned.com/PwnedWebsites

[23] R. Bhalerao, M. Aliapoulios, I. Shumailov, S. Afroz, and D. McCoy, "Towards automatic discovery of cybercrime supply chains," 2018.

[24] ——, "Mapping the underground: Supervised discovery of cybercrime supply chains," in *2019 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2019, pp. 1–16.

[25] (2023, Jun.) tesseract. [Online]. Available: https://github.com/tesseract-ocr/tesseract

[26] Z. Li and X. Liao, "Understanding and analyzing appraisal systems in the underground marketplaces." in *NDSS*, 2024.

[27] A. de la Cruz. (2023, Jun.) Hackforums crypter social network. [Online]. Available: https://paquitoelchocolatero.github.io/HFCrypterAnalysis/social-network/canvas.html

[28] A. Majeed and I. Rauf, "Graph theory: A comprehensive survey about graph theory applications in computer science and social networks," *Inventions*, vol. 5, no. 1, 2020. [Online]. Available: https://www.mdpi.com/2411-5134/5/1/10