Cyber Attacks for Sale

Per Håkon Meland
Norwegian University of Science and Technology
and *SINTEF Digital*
Trondheim, Norway
per.hakon.meland@ntnu.no

Guttorm Sindre
Norwegian University of Science and Technology
Trondheim, Norway
guttorm.sindre@ntnu.no

***Abstract*—The infamous darknet hosts an underground economy for illegal goods and services, some of which can be purchased and used for cyber attacks. By analyzing the properties and popularity of such items, we can get indications about the type and capabilities of potential attackers, what assets they are targeting and which vulnerabilities they are likely to exploit. We have conducted an online study of eleven marketplaces residing within the darknet, addressing what kind of cyber attack items are available and where the profit lies. The results have been used to create a detailed categorization of items, showing a distribution based on item type and availability. This has been compared to the number of sold items and revenue from four of the marketplaces, and we discuss these different views. Aided by related studies, we have identified trending cyber threats such as phone hacking, information theft and bitcoin stealing.**

Type of submission: Full/Regular Research Paper

Symposium: CSCI-ISCW

***Index Terms*—cyber threat, darknet, underground economy**

I. Introduction

The infamous darknet hosts an underground economy for illegal goods and services, where the identities of vendors and buyers stay hidden through cryptographic mechanisms. Within popular marketplaces residing here, there are numerous types of software and services that are sold for the purpose of performing cyber attacks, and which allow actors with limited technical expertise and resources to obtain malicious capabilities. Knowledge of mechanisms and trends in this market can improve our situational awareness about threats towards our systems [1], i.e. the popularity of malicious digital goods may indicate the type and capability of potential attackers, what assets they target and which vulnerabilities they are likely to exploit. This is comparable to the military arms market; high demand for aggressive weapons indicates a potential threat. If the buyer of these weapons happens to be a group or country with a grudge against you, then it is wise to install defense mechanisms that can counter such weapons. In the cyber world, these dynamics works at a much higher pace, giving the defenders a preparation time of maybe a few days only.

The purpose of this paper is to provide an overview of contemporary marketplaces and items related to cyber attacks. We do this by addressing the following research questions:

- RQ1: What kind of cyber attack items are available on the darknet marketplaces?
- RQ2: What are the most profitable items for the vendors?

Answering these might give us *forward-looking indicators* [2] of the cyber threat landscape, and according to Broadhurst et al. [3], a way for tracking trends in potential victimization.

Section II describes how we have conducted our study and the research space. Section III presents the categories, exclusions and different views on the market, which are further discussed in Section IV. Section V concludes the paper.

II. Method

We have conducted an online study of the virtual community residing on darknet marketplaces, with a specific focus on tools and services that can be purchased and used for cyber attacks. Kozinets [4] uses the term *netnography* for such online studies, and we have followed his guidelines for planning, ethical considerations, data collection and interpretation. It was important to us that the research would not cause harm to individuals or groups. Users on the darknet are anonymous, and we would not collect any data that could be used to reveal their identities. We have also been conscious not to put ourselves or others at risk. In practice this means a passive data collection of archival data already available in the public space. To avoid supporting illegal activities we have not purchased anything. Finally, we have not tried to deceive, intimidate or confuse people within this research space, e.g., pretending to be a vendor, customer (though we had to create user accounts), malware software writer or marketplace administrator.

DarknetLive [5], found to have the most up-to-date index of TOR market links and mirrors, was used to identify marketplaces for our study, supplemented with a few extra links from TheDarkWebLinks [6] and DarknetStats [7]. Screened out dead and seized markets, as well as irrelevant ones (e.g., only dealing drugs, no malware), yielded the sample shown in Table I. Data from this sample were collected during the month of September 2019. For each market we identified the relevant inventory categories, and did a manual inspection of the items enlisted in each of these. Due to variance in functionality between the marketplace platforms, the data recorded from each market differed somewhat. We could record item name and price for almost all, while for instance number of successful sales and views were only visible for some (detailed in Table I). Where possible, we filtered out items with zero sales to

TABLE I
MARKETPLACES INCLUDED IN OUR STUDY.

Name	Description and data recorded	Selected categories (available items)
Apollon Market	Established in March 2018, selling a large variety of items (12 836 in total) in all kinds of categories, but mostly *drugs*, *digital goods* and *fraud*. We recorded relevant items, their price and number of sales, but filtered out items with zero sales.	Software and malware (72) Services - Social engineering (16) Services - Hacking (38) Services - Cracking (6)
Berlusconi Market	Established in July 2017 and had the largest inventory (150 034 items) in our sample until it died right after our observation period. Clearly dominated by *drugs* and *counterfeit* items, but contained digital goods as well. We recorded items, sales and price. Filtering: At least one sale per item, vendor activity within the last 30 days.	Software and malware (1 459) Digital products (8 555) - Fraud software Services (2 759)
Canadian HeadQuarters	Established early in 2018. The market has a particular focus on *fraud related items* (2 117 items, such as bank logs, personal information profiles, utility bills, passports and bar code generators) and one of the few markets we saw that was not dominated by *drugs* (184 items). We recorded all relevant items and price.	Fraud - Scampages (84) Services - Other (87)
Cave Tor	A small marketplace of unknown origin with 464 items in total, whereas *financial services* (cloned credit cards, fake identity cards, etc) and *drugs* were the main categories. We recorded 31 *hackers-for-hire* services and 1 *phishing kit*, but these were not enlisted with price.	Service (85)
DarkBay	A market named DarkBay was originally shut down in 2014, and it is unclear whether the current operating is related. It had 4 213 items where *guides & tutorials* (44%) was the most comprehensive category, followed by *digital goods* (99,8% e-books) and *drugs*. We recorded relevant items and price.	Fraud software (2) Services (12) Software and malware (2)
Dream Alt	Established early in 2019 and should not be confused with the original Dream Market that was shut down in March 2019. Out of 21 646 items in total, 40% were found under *digital goods* (32% e-books) and 34% under *drugs & chemicals*. We recorded relevant items and price.	Digital goods - Software (220) Digital goods - Security (110) Services - Hacking (374)
Empire Market	Established around April 2018 and regarded as the successor of the seized Alphabay market. Out of 49 501 items in total, 68% were related to *drugs & chemicals*. We recorded relevant items, number of views and successful sales per item. Filtering: At least one sale per item.	Software and malware (364) Services - Social engineering (108) Services - Other (237) Digital Products - Other (1 443) Fraud - Other (569) Guides & tutorials - Hacking (363)
Grey Market	Officially launched July 2019, enlisting 3 360 items in total. Out of these, 62% were related to *digital* and 33% related to *drugs*. We recorded relevant items, number of views and successful sales per item.	Digital - Information - Other (1 160) Digital - Fraud - Other (12) Digital - Fraud - Software (140) Service - Hacking (32) Service - Other (68)
Samsara	Samsara opened in July 2019 and is an updated and rebranded version of Dream Market. Out of 28 859 items in total, 54% were related to *drugs* and 43% to *digital goods*. We recorded relevant items and price.	Digital goods - Hacking (209) Digital goods - Fraud (340) Digital goods - Software (627) Services - Hacking (23)
Tochka	A.k.a. *Point*, has been operating since 2015. We found 6 669 items in total, divided into categories *drugs* (70%), *prescriptions* (21%) and *steroids* (5%) (the remaining 4% was unaccounted for). Under *drugs*, there was a subcategory *other* that contained relevant digital goods. We recorded relevant items and price.	Drugs - Other (389)
Undermarket 2.0	Marketplace of unknown origin where vendors are enlisted under each category, and items under each vendor. The total number of vendors was 70, where *carding* (17%) and *drugs* (17%) were the most prominent categories. We recorded relevant vendors, their items, prices, successful sales and number of reviews.	Services (9)

let the buyers help us rule out untrustworthy or undesirable items. Observations were listed in a spreadsheet, all currencies converted to USD, and we took screenshots of interesting items and wrote descriptive and reflective field notes during the study.

III. RESULTS

A. An Overall Inventory of Cyber Attacks

We found the granularities of the categories used in the marketplaces to be rather low. In order to get a more detailed view on what kind of malicious cyber items were available on the marketplaces, we defined a more specific categorization of software and services that all recorded items were mapped against. The following bullet list describes this categorization, and shows the percentage of items put in each from the total of 885 we considered relevant. Where suitable, we have adopted definitions from the *Structured Threat Information Expression* (STIX) framework [8].

- Ransomware (4.1%): Encrypts files on a victim's system, demanding payment in return for the access codes required to unlock files [8]. Products offered were typically source code or customized binaries.
- Remote Access Trojans (RAT) (3.8%): A trojan horse capable of controlling a machine through commands issued by a remote attacker [8]. We observed RATs that could activate webcams, take screenshots, monitor user behavior or access sensitive information.
- Keyloggers (4.1%): Malware that monitors keystrokes

and either records them for later retrieval or sends them back to a central collection point [8].
- Scanners and sniffers (1.4%): Network analysis tools typically used during attack reconnaissance. Scanners find IP addresses and look for vulnerable ports, sniffers intercept and analyze network packages.
- Stealers and grabbers (8.1%): Exploit clipboard data. A stealer will look for bitcoin addresses, and replace these with the attacker's account when pasting. Grabbers look for usernames, passwords, bank accounts, etc. that can be stolen or manipulated.
- Hardware stealers (0.5%): Physical attack devices such as custom-made USB-sticks used to copy/steal data or inject malware.
- Account/password crackers (12.4%): Software used to brute force into specific operating systems or user accounts of popular web sites.
- Phone hacking (6.6%): Toolsets used to hack into phones or other devices running an Android/iOS operating system. This category also includes RATs especially made for phones/tablets.
- Cryptominers (2.7%): Malware that steals a system's resources [8], such as code and binaries that illicitly make use of CPU/GPU cycles, RAM and power to mine cryptocurrencies on behalf of the attacker.
- Exploit kits (0.9%): Tools used to automate attacks on popular applications with specific vulnerabilities. These were either sold as collections or single-system attack software.
- Hack packs (9.7%): Large collections of the various hacking tools mentioned here, along with guides. These are often several GBs in size and can contain hundreds of applications.
- Wifi hacking (2.7%): Software for setting up fake wireless access point software or hacking directly into wireless networks.
- Phishing kits (11.6%): Ready-made scam-pages of popular web sites, sold either as collections or individual sites.
- Botnet software (3.4%): Malware for forming and administration tools for botnets, which are mostly used to execute DDoS attacks.
- Injection tools (1.8%): Tools to generate and send malicious input into web pages that gets executed by an interpreter. We saw mostly SQL injection tools.
- Spamming kits (2.4%): Software for sending out large amounts of emails or SMSs to specific addresses. Letter templates in various languages were also registered in this category.
- Spamming/bombing services (3.2%): Services that will send out a specific number of emails or SMSs. Usually in the range of tens of thousands.
- Hackers-for-hire (19.9%): Diverse hacking services, such as breaking into specific social media accounts, changing school grades or site takedowns.
- DDoS services (0.2%): Specific services for taking down sites through DDoS attacks, often advertised with down-time guarantees.
- Botnet services (0.5%): Rent control over a botnet for a specific amount of time.
- RAT services (0.1%): High-level remote access to number of already compromised computers.

Figure 1 shows how the items are distributed by type and among the eleven different marketplaces. In terms of availability, the top three categories were *hackers-for-hire*, *account/password crackers* and *phishing kits*. Items from Samsara dominated the two former (36% and 49%), and Canadian HQ offered 82% of the items from the latter. If we remove these two marketplaces from the sample, the top three becomes *hackers-for-hire*, *stealers and grabbers* and *account/password crackers*.

A general observation is that the type of items and number of items are unevenly distributed among the marketplaces.

B. Exclusions

Among the inspected items, there were several types that can be deemed malicious, but not used directly for a cyber attack and therefore excluded from our study. Examples include *credit card data*, *zero-day exploits and vulnerabilities for sale*, *anonymity tools* (private SOCKS, cleaners, antidetection), *software licenses*, *hacked user accounts and digital identities* (studied in detail by Wehinger [9]), *money laundering services*, *tutorials and guides*, *contact details of experienced hackers*, *physical skimming devices*, *automatic account creators*, *fake social media followers and web-site visitors* (or popularity-as-service), *search engine optimizers* (SEOs) and *gift card generators*. Also, we excluded *binders*, used to combine a malicious payload with an executable file, and *crypters*, which can obfuscate malicious code, though both of these types were commonly found within *hack packs*.

C. A better view on the market

The availability and distribution of items is one view on the market, but other studies [9], [10] have indicated that fake items and scams thrive on the darknet. Therefore, we made use of the marketplaces that reported number of successful sales and mapped these to the same categories. In Figure 2, we show the number of sales per category from the Apollon, Berlusconi, Empire and Grey market. Out 371 items with 6257 sales in total, we can see here that the top three cyber attack items are *phone hacking* (26%), *hack packs* (20%) and *stealers and grabbers* (17%).

Another way of looking at the market is where the revenue lies. Multiplying the number of successful sales with the latest listing price per item, we estimated what vendors have earned from sales. In Figure 3, the topmost (blue) bars in each category show the accumulated revenue, and the lower (red) bars show the average revenue per item. The standard deviations are shown as extensions to the red bars, indicating how much the average revenue vary between individual items within the same category. The main takeaway from this view is that *hackers-for-hire* are now back on top due to a high average price. There was one item in particular that had a lot

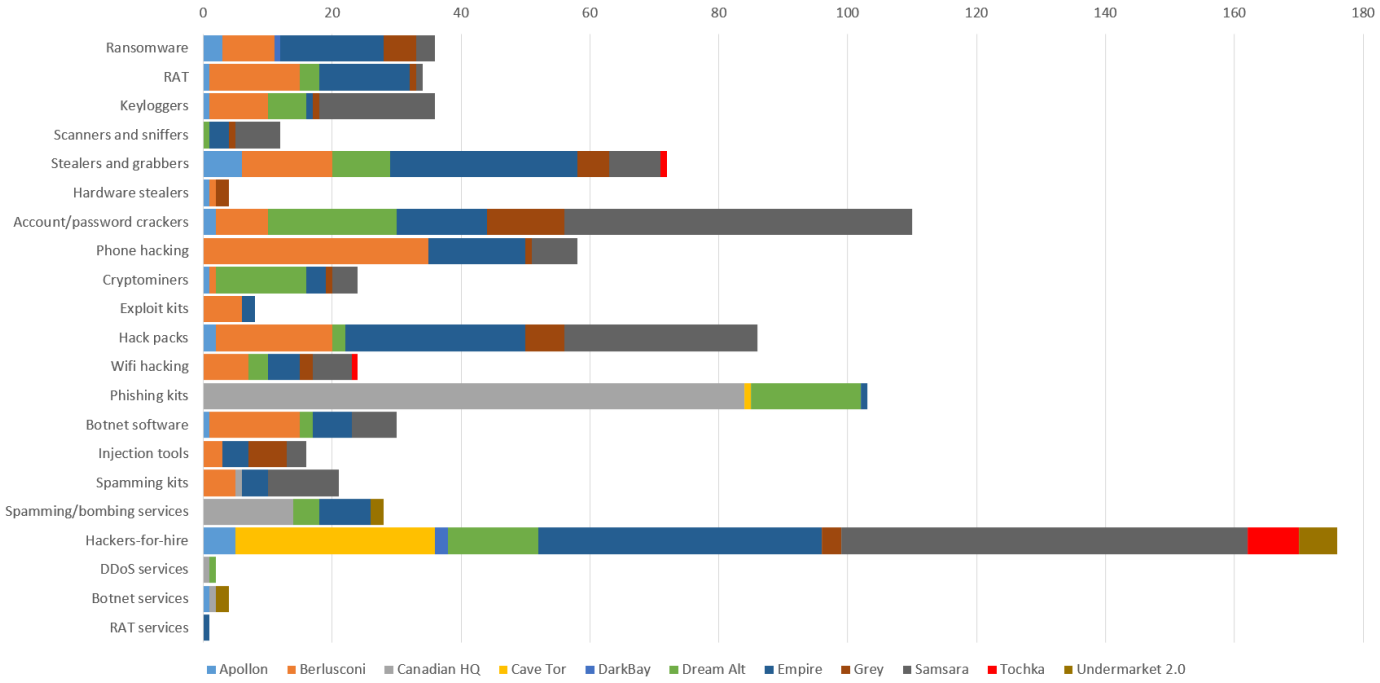

Fig. 1. Categorical distribution of items from eleven marketplaces.

of sales (311 successful sales, 39% of the total revenue). In the following three places we find the same top three cyber attack items as with the number of sales, no surprise since these items have a similar average price (97-113 USD). For all of these, the standard deviation is quite large, as the number of sales is unevenly distributed among the items. The most sold items also tend to be the most pricy ones, benefiting from buyers that will use the high number of sales as a sign of legitimacy and therefore are willing to pay more. A similar trend could be seen from the ratio between number of sales and views, where the most successful items stayed between 0.05 and 0.10, while unpopular items were several factors of ten lower.

As seen from Figures 1 and 2, the Apollon, Berlusconi and Grey markets are weak when it comes to availability and sales of services. Undermarket 2.0 reports number of successful sales per vendor, with two vendors that specialized in cyber attack services such as *DDoS*, *spamming*, *information theft* and *account hacking* at the time of our observations. The sales figures of these were 32 540 and 72 259, exceeding the combined sales of all relevant items in the four marketplaces stating those figures. Either, these are among of the most successful cyber attack service providers on the darknet, or the numbers are fabricated and the marketplace a scam. Some darknet forum posts claim the latter, and the number of reviews (mostly positive) for each of these two vendors are exactly 85% of the number of sales, possibly indicating that reviews are automatically generated.

IV. Discussion

We have addressed our first research question by categorizing and looking at the distribution of cyber attack items found in our largest sample of eleven marketplaces. The second research question is addressed by looking at number of successful sales and prices from a smaller sample of four marketplaces. Except for *hackers-for-hire*, the top items differ between the views, and an obvious limitation is the difference between the samples. Therefore, it is debatable which view, if any, gives us the best indication of what kind of cyberthreats we should worry about based on darknet trade. In our opinion, there is more confidence in the view based on sales. This is based on a more qualitative assessments of the items offered in the marketplaces that do not state sales figures, where we noted the following:

- Many of the offered items have descriptions which are short, vague or written in poor English, hence difficult for potential buyers to assess.
- Only a few vendors have many reviews, and these seem to be obtained more from drugs and carding items, less from cyber attack items.
- Many vendors put out the same or similar items multiple times, seeking visibility by flooding the market.
- Many of the items sold seem to have little value. E.g. the tools are old or can be found for free on the surface web (e.g. *Oracle VirtualBox*, the *Mirai* source code, various password crackers).

In contrast, items with a significant amount of sales have clearer descriptions, prices seem more appropriate and duplicate entries are more sparse.

Our dataset consists of a snapshot from September 2019, lacking trends over time. In previous work [11] we studied availability and price fluctuations for ransomware over a longer period aided by archival datasets. Such studies are

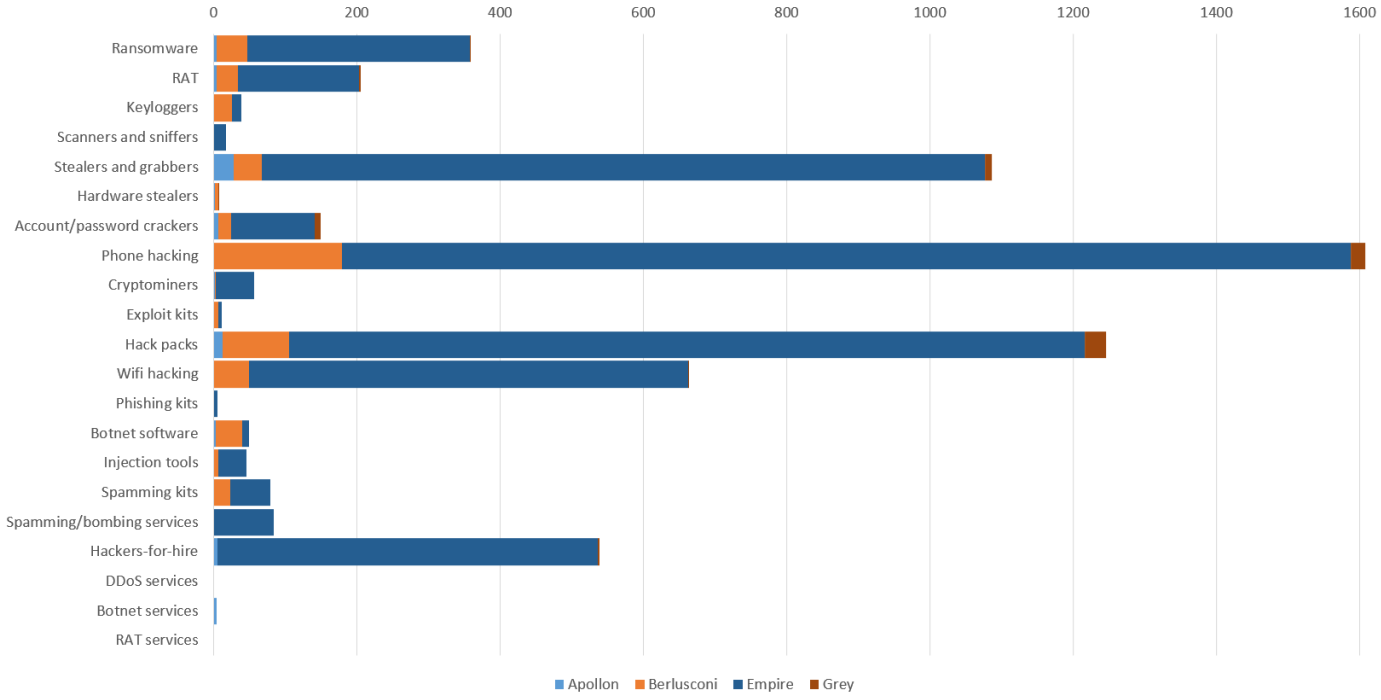

Fig. 2. Number of successful sales per category in four marketplaces.

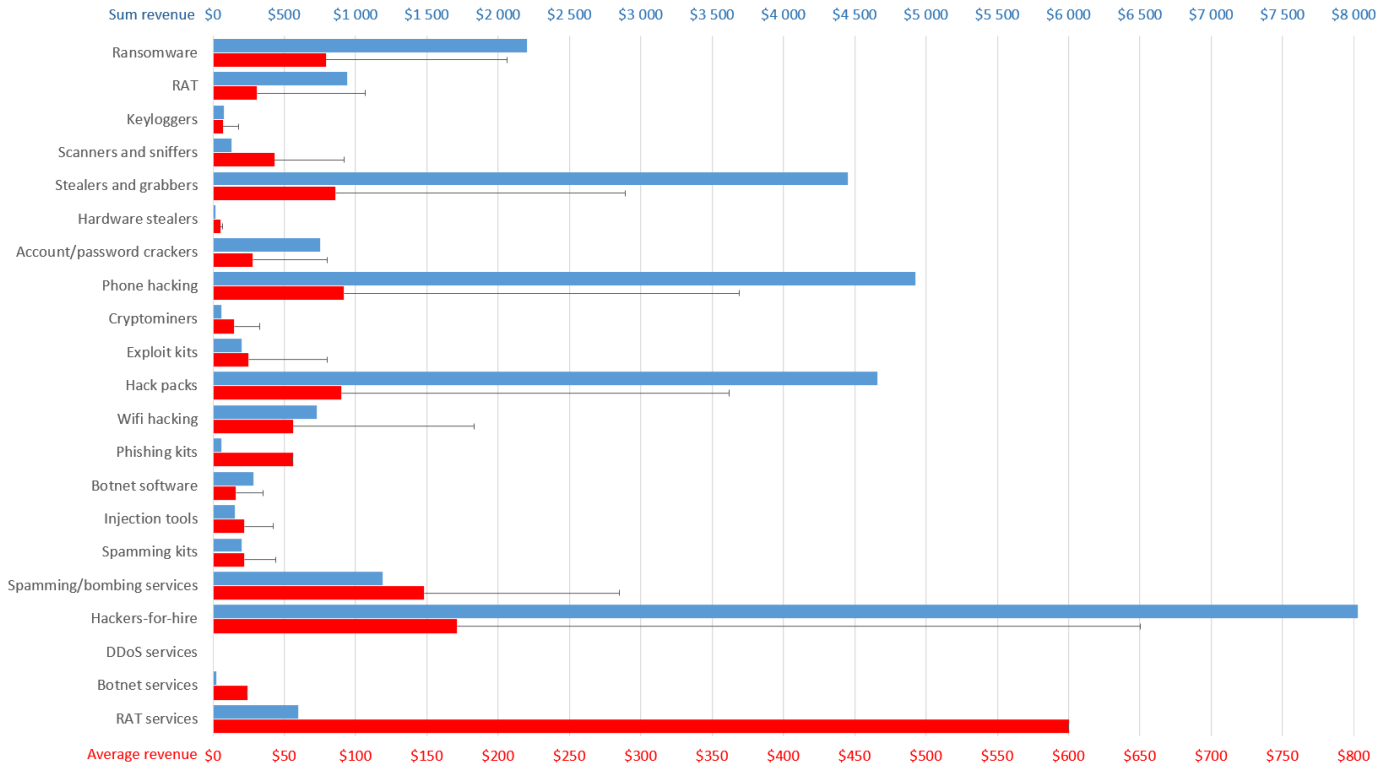

Fig. 3. Accumulated revenue per category and average revenue per item from four marketplaces.

interesting for projections, but also increasingly difficult to perform since law enforcement agencies are more effectively taking down marketplaces. The majority of marketplaces in our largest sample have been established quite recently, while infamous ones such as Silk Road, AlphaBay, Hansa, Dream and WallStreet are now gone. As future work it would be interesting to repopulate the categories with new observations, and analyze how vendors transition themselves in this volatile environment of marketplaces.

A. Related work

Our results can be more informative in the light of related work. In 2014, Ablon et al. [12] classified and exemplified hacking tools and services on black and gray markets. Their approach was to interview subject-matter experts and conduct a literature review. Their classification is more abstract than our categories and lacks elements such as *stealers and grabbers*. For exploit kits and zero-day vulnerabilities, they were able to show price developments over time. The year after, Thomas et al. [13] surveyed existing research in order to develop a taxonomy for reasoning about the flow of capital within the underground economy, making estimations about price and revenue from underground studies and their own investigations. This taxonomy has a broad cybercrime spectrum, but not our level of detail. They also showed that a lot of published studies have an unknown collection methodology. Broadhurst et al. [3] reviewed malware trends on darknet markets and categorized digital products found on Dream Market between September 2017 and April 2018. Again, these categories are fewer and more abstract than ours, but we can for instance see a comparative increase in the presence of keyloggers and a general increase in average prices. Van Wegberg et al. [14] have carried out a six-year longitudinal study tracking the evolution of commoditization on eight marketplaces up until 2017 (all now defunct). Their categorization was based on earlier work by Soska and Christin [15], which is less detailed than ours as well. The way they estimated sales figures was based on customer feedback, which is less accurate than the exact sales from our smallest marketplace sample. They found that ransomware was dominating the malware category, which is different from our data where *stealers and grabbers* prevail. McGuire [16] analyzed fifteen darknet platforms between November 2018 to March 2019. Only Empire and Berlusconi were common with our sample, and their top three were *malware* (25%), *DDoS* (20%) and *RATs* (17%). By comparing their findings with archival data from 2016, they found that there has been a 20% rise in the number of darknet listings that have the potential to harm the enterprise. By responding to ads and actively pretending to be buyers they were also able to get prices for targeted attacks (enterprises around 4 500 USD, individuals 2 000 USD) and espionage (1 000-15 000 USD). They never went through with any of the purchases, but prices are probably more realistic than the ones published within marketplaces.

V. Conclusion

There are different ways of looking at the underground market for cyber attacks, and we deem threat indicators based on sales to be more reliable than availability of items. This comes at a cost of a smaller sample size of markets, so we recommend considering both views in combination. The demand for *phone hacking* tools is prevalent, which is a natural consequence of our societies increasing use of phones for everyday digital activities. When comparing our result with past related studies, especially *stealers and grabbers* seem to be trending items. Such items were clearly present in most marketplaces and had a high number of sales. They are typically used for digital fraud and information theft, which indicates threat agents with a rational behavior and economic motivation. Bitcoin stealers are the most popular, and even though the price of individual items tends to be low (around 4 USD), the volume of sales suggests a decent revenue to the vendors.

References

[1] S. L. Pfleeger and D. D. Caputo, "Leveraging behavioral science to mitigate cyber security risk," *Computers & security*, vol. 31, no. 4, pp. 597–611, 2012.

[2] R. Anderson, R. Böhme, R. Clayton, and T. Moore, "Security economics and the internal market," *Study commissioned by ENISA*, 2008.

[3] R. Broadhurst, D. Lord, D. Maxim, H. Woodford-Smith, C. Johnston, H. W. Chung, S. Carroll, H. Trivedi, and B. Sabol, "Malware trends on 'darknet'crypto-markets: Research review," Australian National University Cybercrime Observatory and the Korean Institute of Criminology, Tech. Rep., 2018.

[4] R. V. Kozinets, *Netnography*. Wiley Online Library, 2015.

[5] Darknetlive. https://darknetlive.com/. Last accessed: 2019-10-03.

[6] Thedarkweblinks. https://www.thedarkweblinks.com/. Last accessed: 2019-10-03.

[7] Darknetstats. https://www.darknetstats.com/. Last accessed: 2019-10-03.

[8] OASIS, "STIX Version 2.0. Part 1: STIX Core Concepts," OASIS Cyber Threat Intelligence (CTI) TC, Tech. Rep., July 2019.

[9] F. Wehinger, "The dark net: Self-regulation dynamics of illegal online markets for identities and related services," in *2011 European Intelligence and Security Informatics Conference*, Sep. 2011, pp. 209–213.

[10] Ken. (2018, June) Dream market: A hotbed of scammers. https://darkwebnews.com/darkwebmarkets/dream-market/dream-market-a-hotbed-of-scammers/. Last accessed: 2019-06-27.

[11] Y. F. F. Bayoumy, P. H. Meland, and G. Sindre, "A netnographic study on the dark net ecosystem for ransomware," in *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, 2018, pp. 1–8.

[12] L. Ablon, M. C. Libicki, and A. A. Golay, "Markets for cybercrime tools and stolen data: Hackers' bazaar," Rand Corporation, Tech. Rep., 2014.

[13] K. Thomas, D. Huang, D. Wang, E. Bursztein, C. Grier, T. J. Holt, C. Kruegel, D. McCoy, S. Savage, and G. Vigna, "Framing dependencies introduced by underground commoditization," in *14th Workshop on the Economics of Information Security*, 2015.

[14] 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*, 2018, pp. 1009–1026.

[15] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in *24th USENIX Security Symposium*, 2015, pp. 33–48.

[16] M. McGuire, "Behind the dark net black mirror: Threats against the enterprise," Bromium and University of Surrey, UK, Tech. Rep., June 2019.