AFRL-RI-RS-TR-2020-096

A QUERYABLE PLATFORM FOR ONLINE CRIME REPOSITORIES

CARNEGIE MELLON UNIVERSITY

JUNE 2020

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2020-096 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
TODD N. CUSHMAN for
WILLIAM E. KAHLER
Work Unit Manager

/ S /
JAMES S. PERRETTA
Deputy Chief, Information
Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* JUNE 2020	**2. REPORT TYPE** FINAL TECHNICAL REPORT	**3. DATES COVERED** *(From - To)* MAY 2017 – NOV 2019

4. TITLE AND SUBTITLE

A QUERYABLE PLATFORM FOR ONLINE CRIME REPOSITORIES

5a. CONTRACT NUMBER
FA8750-17-2-0188

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Christin, Nicolas

5d. PROJECT NUMBER
DHS1

5e. TASK NUMBER
7C

5f. WORK UNIT NUMBER
MU

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University
5000 Forbes Ave
Pittsburgh PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2020-096

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09

13. SUPPLEMENTARY NOTES

14. ABSTRACT
University at the behest of the Department of Homeland Security, Science & Technology Directorate. The project led to availing to other researchers data from 12 dark web marketplaces, corresponding to over 22,288 vendors, 348,400 items, and 5,826,115 transactions. The data was availed through 1) a publicly available website (for anonymized data), and 2) a set of databases provisioned through the IMPACT portal (for anonymized and de-anonymized data). The IMPACT portal served 49 distinct requests for data from 28 institutions (academic, industry, government) over six countries (US, Japan, Singapore, Netherlands, UK, and Australia). In addition, our research yielded four peer-reviewed publications (PETS 2018, USENIX Security 2018, KDD 2019, Financial Cryptography 2020). Last, our data contributed to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) 2017 report on "Drugs and the Darknet" and served as the basis of the PI's testimony before the US Congress in March 2018.

15. SUBJECT TERMS

Dark web, measurements, IMPACT

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** **WILLIAM E. KAHLER**
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	17	**19b. TELEPHONE NUMBER** *(Include area code)* **N/A**

TABLE OF CONTENTS

LIST OF FIGURES

1.0 Summary

We present the results of the project “A Queryable Platform for Online Crime Repositories,” carried out at Carnegie Mellon University at the behest of the Department of Homeland Security, Science & Technology Directorate. The project led to availing other researchers data from 12 dark web marketplaces, corresponding to over 22,288 vendors, 348,400 items, and 5,826,115 transactions. The data was made available through 1) a publicly available website (for anonymized data), and 2) a set of databases provisioned through the IMPACT portal (for anonymized and de-anonymized data). The IMPACT portal served 49 distinct requests for data from 28 institutions (academic, industry, government) over six countries (US, Japan, Singapore, Netherlands, UK, and Australia). In addition, our research yielded four peer-reviewed publications (PETS 2018, USENIX Security 2018, KDD 2019, Financial Cryptography 2020). Last, our data contributed to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) 2017 report on “Drugs and the Darknet” and served as the basis of the PI’s testimony before the US Congress in March 2018.

2.0 Introduction

This project stemmed from years of research in collecting large amounts of data from several types of online illicit activity, ranging from illicit sales of pharmaceutical drugs, to online anonymous marketplaces. We have strived to make our data publicly available for others to use, which presents a number of challenges.

First, continuously maintaining these data repositories requires significant software engineering: continuous maintenance of parsers, scrapers, and other data collection primitives in the face of changes in the environment. Second, simple data “dumps” are quite difficult to use, and do not lend themselves to rapid hypothesis testing—this is particularly true for researchers in social sciences (e.g., criminology, economics) who might otherwise have great interest in our data, but not necessarily the ability to write complex, low-level database queries.

The object of this work was to build and deploy query-able online platforms for our online crime repositories. We primarily focused on anonymous online (“dark web”) marketplace data, but also provided data from search-redirection scams, that have been used to defraud customers seeking money.

We built and deployed simple web-based graphical interfaces, accessible to partner institutions and researchers at no cost, and exported most of our data through the IMPACT initiative.

While the work was primarily infrastructural, we have seized the opportunity provided by this grant to also make scientific advances, both in data collection and in data analysis. Namely, we published four papers related to work carried out under this contract.

The next sections describe our data sharing (Section 2), a summary of the scientific papers published under the auspices of this grant (Section 3), as well as plans for future research (Section 4).

3.0 Methods, Assumptions and Procedures

A critical aspect of this work was to provide access to the larger community to our datasets of online crime, specifically, dark web marketplace data. We provided access through two media: a publicly accessible website, which only featured *anonymized* data, and a set of databases available both in anonymized or de-anonymized format to researchers; the latter (de-anonymized) required signature of a Memorandum of Understanding between the interested researchers and Carnegie Mellon University. This process was facilitated through the IMPACT cyberportal (https://www.impactcybertrust.com).

Our data sharing eschews potential thorny human-subject issues, as all the data we collect are already publicly available, and should not contain private identifiers (e.g., no IP addresses). We obfuscate textual content that could plausibly contain (unidentifiable) contact information such as “throw-away” email addresses used by questionable businesses. We worked with our IRB and general counsel to ensure the soundness of our proposed approach. The IRB confirmed this was not human subject research; legal indicated specific language to be used on our website.

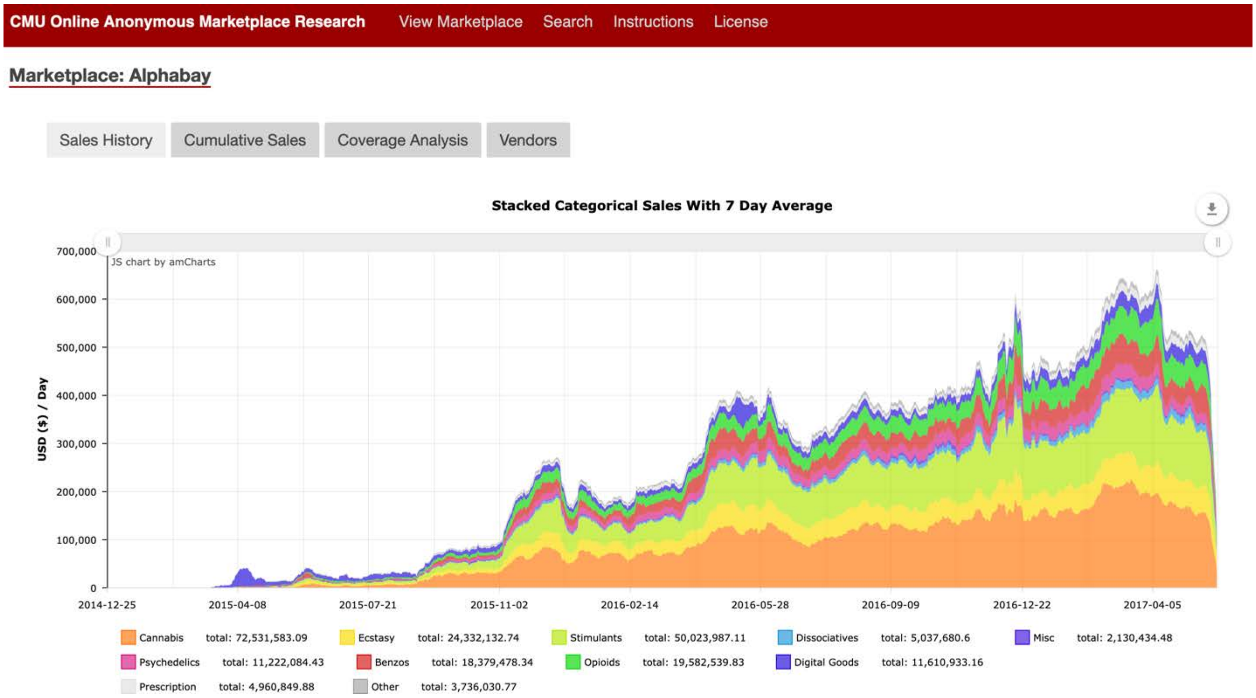
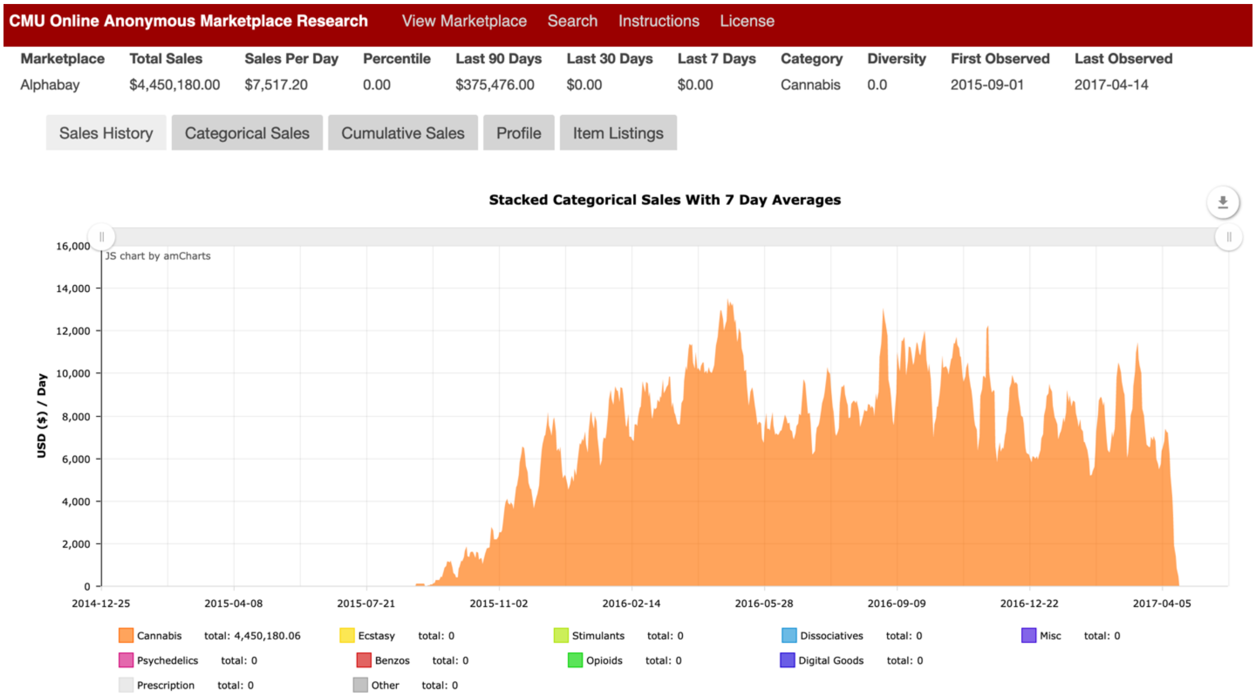

CMU Online Anonymous Marketplace Research
View Marketplace
Search
Instructions
License
Marketplace: Alphabay
Sales History
Cumulative Sales
Coverage Analysis
Vendors
Stacked Categorical Sales With 7 Day Average
JS chart by amCharts
USD ($) / Day
700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
2014-12-25
2015-04-08
2015-07-21
2015-11-02
2016-02-14
2016-05-28
2016-09-09
2016-12-22
2017-04-05
🟧 Cannabis total: 72,531,583.09
🟨 Ecstasy total: 24,332,132.74
🟩 Stimulants total: 50,023,987.11
🟦 Dissociatives total: 5,037,680.6
🟪 Misc total: 2,130,434.48
🟪 Psychedelics total: 11,222,084.43
🟥 Benzos total: 18,379,478.34
🟩 Opioids total: 19,582,539.83
🟪 Digital Goods total: 11,610,933.16
⬜ Prescription total: 4,960,849.88
⬜ Other total: 3,736,030.77

Figure 1: Online portal (Example of marketplace aggregate data)

Figure 1 gives a glimpse of the online portal we developed.

For 12 different dark web marketplaces (Agora, Evolution, Silk Road, Silk Road 2, Black Market Reloaded, Pandora, Hydra, Alphabay, Dream Market, Traderoute, Berlusconi Market, and Valhalla), we provide panels that allow users to quickly plot the amount of sales (broken by category, e.g. “Cannabis”) over time. Figure 1 shows the entire timeline for the Alphabay marketplace, in which we plot the amount of daily sales on the market, over two years. Users can move the slider to “zoom in” on specific time periods.

By clicking on “Vendors,” users are redirected to a page listing all of Alphabay’s vendors.



Marketplace	Total Sales	Sales Per Day	Percentile	Last 90 Days	Last 30 Days	Last 7 Days	Category	Diversity	First Observed	Last Observed
Alphabay	$4,450,180.00	$7,517.20	0.00	$375,476.00	$0.00	$0.00	Cannabis	0.0	2015-09-01	2017-04-14

Figure 2: Online portal (Example of vendor data)

Subsequently, users can obtain more detailed information simply by clicking on a vendor's record. This, in turn, leads them to a page as depicted in Figure 2. In this case, the vendor was specializing fully in cannabis, and sold approximately 4 million USD of such goods over their lifetime on Alphabay.

The data and software are too voluminous to be included on disk on in this report. Instead, we provide a download link (accessible until July 1, 2020) at https://arima.cylab.cmu.edu/tmp/02e8e29c01/AFRL/

This directory contains:

- fulldb-anonymized.sqlite3 (12 GB): the full database used in the website described above. This contains only anonymized handles, descriptions, etc.
- fulldb.sqlite3 (11 GB): same as above, but the data is not anonymized.
- marketplaces.tar.gz (4.2 M): complete source code of the software used for scraping, parsing and analysis of the dark web markets considered.

The fulldb databases contain all the data that is shared on IMPACT, as well.

4.0 Results and Discussion

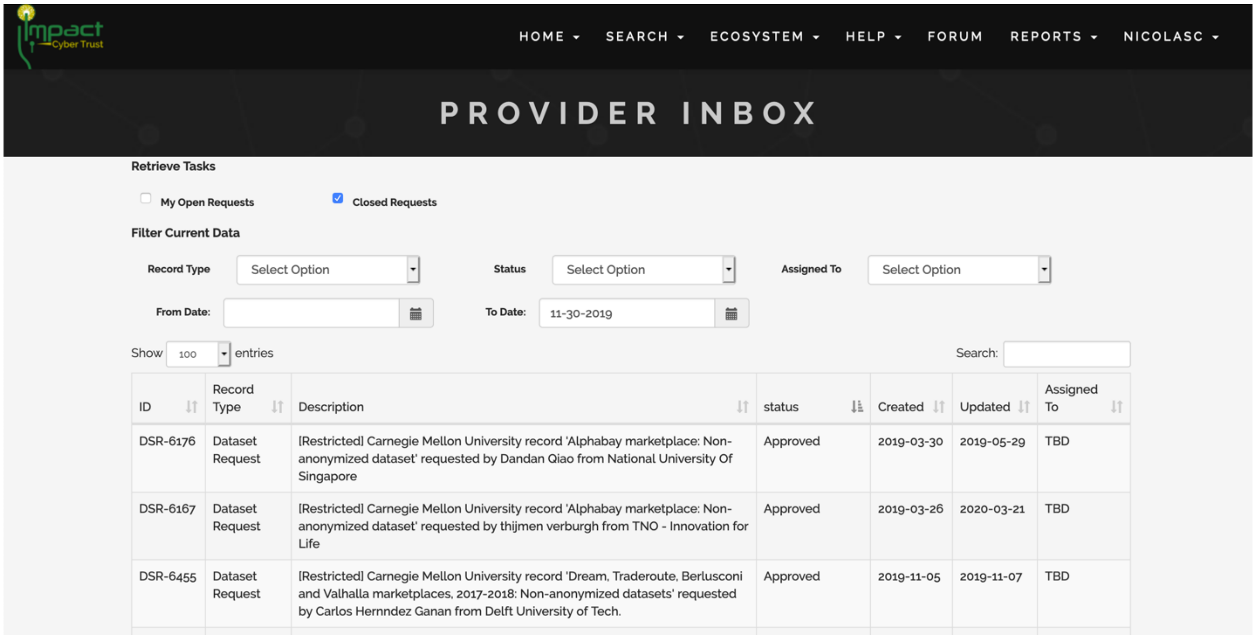
4.1 Website use and data sharing

All in all, our website provides data about:

- 12 different marketplaces as noted earlier
- 22,288 vendors,
- 348,400 items,
- and 5,826,115 transactions.

We believe this is the most comprehensive publicly available archive of dark web data. The website is available at https://arima.cylab.cmu.edu/markets/. Code to generate the website is sent as part of the software bundle we are providing with this final report.

In addition to this website, we provided data through the IMPACT cyberportal. We served 49 distinct requests for data from 28 institutions (academic, industry, government) over six countries (US, Japan, Singapore, Netherlands, UK, and Australia). Figure 3 shows a partial list of three requests that were honored. At the time of this writing, and even though the project is complete and not currently funded, we have served 65 requests (that is, an extra 16 requests after the completion of the project).



PROVIDER INBOX

Retrieve Tasks

☐ My Open Requests ☑ Closed Requests

Filter Current Data

Record Type: Select Option
Status: Select Option
Assigned To: Select Option
From Date:
To Date: 11-30-2019

Show 100 entries

Search:

ID	Record Type	Description	status	Created	Updated	Assigned To
DSR-6176	Dataset Request	[Restricted] Carnegie Mellon University record 'Alphabay marketplace: Non-anonymized dataset' requested by Dandan Qiao from National University Of Singapore	Approved	2019-03-30	2019-05-29	TBD
DSR-6167	Dataset Request	[Restricted] Carnegie Mellon University record 'Alphabay marketplace: Non-anonymized dataset' requested by thijmen verburgh from TNO - Innovation for Life	Approved	2019-03-26	2020-03-21	TBD
DSR-6455	Dataset Request	[Restricted] Carnegie Mellon University record 'Dream, Traderoute, Berlusconi and Valhalla marketplaces, 2017-2018: Non-anonymized datasets' requested by Carlos Hernndez Ganan from Delft University of Tech.	Approved	2019-11-05	2019-11-07	TBD

Figure 3: IMPACT Cyberportal example (administrator view)

This has yielded a number of additional important publications *by other researchers not affiliated with our group* – for instance, the Silk Road dataset made available through IMPACT led to a paper by Przepiorka et al. to be awarded as the "best paper of 2017" in the European Sociological Review, which is a top-ranked journal in sociology (https://doi.org/10.1093/esr/jcx072).

4.2 Scientific papers published as part of this grant and public outreach

The data collected by this grant led to four papers published by our group [2,3,4,5], and the data were central to the 2017 EMCDDA report on "drugs and the darknet" [1], an influential white paper given to decision-makers in the European Union. (EMCDDA is the EU agency tasked with monitoring drug use in Europe.)

4.2.1 An Empirical Analysis of Traceability in the Monero Blockchain

The first paper describes how much traffic took place on the Alphabay marketplace, and the impact on anonymous currencies such as Monero [2]. It was published at the Privacy Enhancing Technology Symposium (PETS) in 2018, a highly selective venue, and has already garnered 87 citations, a remarkable number in such a short time.

More precisely, our contributions to this work was the study of the importance of mining pools and, directly relevant to this sponsored award, the former anonymous marketplace AlphaBay on the total transaction volume.

On August 22, 2016, AlphaBay announced that it would support Monero, and allowed vendors to list items accepting Monero. On September 1, 2016, buyers were then able to use Monero to purchase items on AlphaBay.

We observed a strong correlation between these events and the overall transaction volume. On August 22, the day of the announcement, the number of transactions in the Monero blockchain increased by more than 80% compared to the previous day, and it peaked at 4,444 transactions on September 3, two days after Monero payments were made available on AlphaBay.

By default, an item listed on AlphaBay only accepts Bitcoin as a payment mechanism. Vendors have to explicitly allow Monero for it to be considered; and can also disable Bitcoin in the process. There are thus three types of items: items that only accept Monero, items that only accept Bitcoin, and items that accept both.

Using AlphaBay data from our crawling platform, we multiplied item feedback instances by item prices, to estimate sales volumes. While sales volume remained fairly modest until mid-2015, it has steadily climbed to reach approximately USD 600,000 a day in 2017, which is more than the combined volume of the major online anonymous marketplaces in 2013—2015 [7]. Of those transactions, we are able to identify that a vast majority only accept Bitcoin.

Starting in September 2016, a modest, but increasing number of items started accepting Monero along Bitcoin. The total amount of sales for these items gives an upper bound for the dollar amount of Monero transactions on AlphaBay—as of early 2017 approximately USD 60,000/day, or 10% of all AlphaBay transactions in volume.

4.2.2 Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets

The second paper [3] relied our data collected as part of this effort to illuminate the sales of "digital goods" (stolen logins, compromised credentials, but also money laundering guides and all sorts of illicit online services) on the dark web. It evidenced that there is a degree of commoditization in these nefarious online activities, and was published at the USENIX Security Symposium in 2018; this is an extremely selective publication, and a top academic computer security forum. Even more importantly, data from this paper were used as the basis for the PI's March 15, 2018's testimony before the Subcommittee on Terrorism & Illicit Finance, Committee on Financial Services, U.S. House of Representatives, 115th Congress, in a hearing entitled After the Breach: The Monetization and Illicit Use of Stolen Data. The written testimony is available online [6].

In this USENIX Security work, we in particular used our crawled data from eight online anonymous marketplaces over six years, from the original Silk Road to AlphaBay, and tracked the evolution of commoditization on these markets. We developed a conceptual model of the value chain components for dominant criminal business models. We then identified the market supply for these components over time. We found evidence of commoditization in most components, but the outsourcing options were highly restricted and transaction volume was often modest. Cash-out services feature the most listings and generate the largest revenue.

Consistent with behavior observed in the context of narcotic sales, we also found a significant amount of revenue in retail cybercrime, i.e., business-to-consumer (B2C) rather than business-to-business. We conservatively estimated the overall revenue for cybercrime commodities on online anonymous markets to be at least US $15M between 2011-2017. We concluded that while there has certainly been growth, commoditization is a spottier phenomenon than previously assumed.

4.2.3 Adversarial Matching of Dark Net Market Vendor Accounts

The third paper [4] focused matching different online anonymous marketplace vendor handles to unique sellers. Using a combination of random forest classifiers and hierarchical clustering on a set of features that would be hard for an adversary to forge or mimic, we managed to obtain reasonable performance (over 75% precision and recall on labels generated using heuristics), despite generally lacking any ground truth for training. Our algorithm performed particularly well for the top 30% of accounts by sales volume and showed that 22,163 accounts with at least one confirmed sale mapped to 15,652 distinct sellers—of which 12,155 operated only one account, and the remainder between 2 and 11 different accounts. Case study analysis further confirmed that our algorithm managed to identify non-trivial matches, as well as impersonation attempts.

This work was particularly important as it built on a very important area of statistics research: record matching. Many datasets feature seemingly disparate entries that actually refer to the same real-world entity. For instance, in a demographic census, a unique individual may appear under several entries (“John Public,” “John Q. Public,” etc.) that have to be reconciled prior to analysis to ensure the quality of the census data.

A similar problem arises when combining information from multiple datasets: entries in different datasets might refer to the same unique entity. For example, death records in Syria's humanitarian crisis have been compiled by different groups, and need to be reconciled to get accurate figures on the number of casualties. This reconciliation process is typically termed *matching*, and has been extensively studied in statistics, commonly under the name *record linkage*. Other matching instances include reconciling disparate casualty reports during disasters or wars, linking census records to other demographic surveys, disambiguating inventors, authors, or movies in patent, bibliographic, or movie databases.

Matching is challenging due to error—including approximations during data collection. Fields between different datasets may be different, and entries may be missing fields. Many matching algorithms tackle these problems, but most do not consider that the presence of separate entries in the original data may be due to malice. In some contexts, however, *adversaries* have a vested interest in seeing the matching process fail, either by finding spurious matches, or by failing to match entries that refer to the same entity.

The dark web marketplaces we studied are one such context. Here again, we used the data we collected as part of the sponsored project to show the viability of our techniques. More specifically, there have been a few previous attempts to match vendor accounts in online anonymous marketplaces.

Some took the simple approach of matching (PGP) cryptographic public keys advertised by different accounts which cannot handle impersonation attacks, since anybody can copy somebody else's public key. Short of verifying a vendor can decrypt a message using the private key corresponding to the advertised public key, one cannot derive conclusive results solely from public key examination. At the other end of the complexity spectrum, the Grams search engine was an elaborate and largely manual and crowdsourced attempt to match accounts across marketplaces. Grams was taken offline in December 2017, reportedly due to the high human cost of operating such a database. Furthermore, crowdsourcing is vulnerable to poisoning, in which an adversary injects malicious content.

We evaluated our algorithms on eight years (2011--2018) of online anonymous marketplace data, and found that 22,163 accounts with at least one confirmed sale map to 15,652 distinct sellers. 12,155 sellers (77%) operate only one account, while the remainder operates between 2 (1,909 sellers) and 11 accounts (2 sellers). Because ground truth in this context is elusive, we compared the performance of our algorithm with data obtained from Grams and from PGP key matching---although these labels are problematic, they give a general sense of model performance. Using these labels, our algorithm achieves more than 75% precision and recall. It works particularly well for vendor accounts with significant sales volume (approximately 90% recall at 75% precision for the top 30% of accounts). We presented a few case studies where ground truth is documented through criminal complaints or forum discussions; we can automatically discover reported impersonation attempts and non-trivial links between accounts. We also discussed scalability limitations of our matching algorithm.

4.2.4 Open Market or Ghost Town? The Curious Case of OpenBazaar

Finally, the fourth paper [5] investigated the OpenBazaar network. OpenBazaar is a decentralized electronic commerce marketplace, which has received significant attention since its development was first announced in early 2014.

Using multiple daily crawls of the OpenBazaar network over approximately 14 months (June 25, 2018–September 3, 2019), we measured its evolution over time. We observed 6,651 unique participants overall, including 980 who used Tor at one point or another. More than half of all users (3,521) were only observed on a single day or less, and, on average, only approximately 80 users were simultaneously active on a given day.

Thanks to the data collected as part of this project, we were able to compare OpenBazaar economic activity with that of centralized anonymous marketplaces, showing that OpenBazaar-induced sales volume is much smaller than on centralized anonymous marketplaces.

Furthermore, while a majority of the 24,379 distinct items listed on OpenBazaar seem to be legal offerings, a majority of the measurable OpenBazaar economic activity appears to be related to illicit products. We also discovered that vendors are not always using prudent security practices, which makes a strong case for imposing secure defaults.

This paper was published at the 2020 International Conference on Financial Cryptography and Data Security, which has become one of the main academic venues for blockchain and cryptocurrency research. It has garnered significant attention. Coincidentally, the predictions made in the paper turned out to be prescient: the lead developers quit OpenBazaar shortly after the paper was published, presumably due to the relative lack of legal activity on the project.

5.0 Conclusions

As we have shown, in addition to being a lynchpin of a number of research efforts at Carnegie Mellon, our work under IMPACT has facilitated considerable additional research *by others*, as evidenced by the numerous downloads of our data (see Section 4), and their actual use in publications, including award-winning papers.

In that respect, the objectives set forth by the proposal were fully met.

We are currently investigating transition to practice as part of this effort. Specifically, we are in the process of establishing a spin-out company to investigate additional data collection, while pursuing further research at Carnegie Mellon on our existing data corpora.

We are making available all the software and data produced as part of this effort as an online appendix to this technical report, available (until June 1, 2020) at:
https://arima.cylab.cmu.edu/tmp/02e8e29c01/AFRL/

6.0 References

[1] European Monitoring Centre for Drugs and Drug Addiction and Europol. Drugs and the Darknet: Perspectives for Enforcement, Research and Policy. EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg. November 2017.

[2] Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin. An Empirical Analysis of Traceability in the Monero Blockchain. To appear in Proceedings of the Privacy Enhancing Technology Symposium (PETS 2018), volume 3. Barcelona, Spain. July 2018.

[3] Rolf van Wegberg, Samaneh Tajalizadehkhoob, Kyle Soska, Ugur Akyazi, Carlos Gañán, Bram Klievink, Nicolas Christin, and Michel van Eeten. Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets. In Proceedings of the 27th USENIX Security Symposium (USENIX Security'18). Baltimore, MD. August 2018.

[4] Xiao Hui Tai, Kyle Soska, and Nicolas Christin. Adversarial Matching of Dark Net Market Vendor Accounts. To appear in Proceedings of the 25th ACM SIGKDD Conference of Knowledge, Discovery, and Data Mining (KDD'19). Anchorage, AK. August 2019.

[5] James E. Arps and Nicolas Christin. Open Market or Ghost Town? The Curious Case of OpenBazaar. To appear in Proceedings of the 24th International Conference on Financial Cryptography and Data Security (FC'20). Kota Kinabalu, Malaysia. February 2020.

[6] Nicolas Christin. After the Breach: The Monetization and Illicit Use of Stolen Data. Testimony before US Congress, March 2018. http://www.andrew.cmu.edu/user/nicolasc/publications/20180315-testimony-christin.pdf

[7] Kyle Soska and Nicolas Christin. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In Proceedings of the 24th USENIX Security Symposium (USENIX Security'15), pages 33-48. Washington, DC. August 2015.

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
GB	Gigabyte
IMPACT	Information Marketplace for Policy and Analysis of Cyber-risk & Trust
IP	Internet Protocol
IRB	Internal Review Board
KDD	Conference of Knowledge, Discovery, and Data Mining
MB	Megabyte
PETS	Privacy Enhancing Technology Symposium
UK	United Kingdom
US	United States
USD	US Dollar
USENIX	Advanced Computing Systems Association