



Understanding and Analyzing Appraisal Systems in the Underground Marketplaces

Zhengyi Li, Xiaojing Liao

Indiana University Bloomington

Formal Definition of Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence (CTI) is

Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about **an existing or emerging** menace or hazard to **assets** that can be used to **inform decisions** regarding the subject's response to that menace or hazard.

-- Gartner

An Example of Cyber Threat Intelligence (CTI)



Malware:

- Name: *Zbot*
- Type of malware: *trojan*
- Programming language: *Java*
- Filename: *malicious.exe*
- IP address: *122.118.1.1*
- Hash: *c4c...849b*
- Behavior pattern: *disable antivirus*
- ...

Underground Marketplaces

- ▼ Fraud 1310
- ▼ Hacking 4
- ▼ Digital Goods 767
- ▼ Counterfeits 306

Carding Ware 87

Services 92

Guides & Tutorials
1373

Security & Hosting 38

Software & Malware
281

rat spreading latest guide 2023



Escrow

USD 10.4
k1to (2) (4.5 ★)

BTC | XMR
Afghanistan
-> WorldWide

ORDER

shinobu clipper # crypto currency stealer...



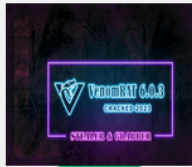
Escrow

USD 6.76
BlueSoft (30) (4.87 ★)

BTC | XMR
Afghanistan
-> WorldWide

ORDER

venomrat 6.0 source code - stealer & ...



Escrow

USD 9.88
BlueSoft (30) (4.87 ★)

BTC | XMR
Afghanistan
-> WorldWide

ORDER

new android malware makes anonymous calls...



Escrow

USD 5.2
VerrifiedAccounts (130) (4.77 ★)

BTC | XMR
Åland Islands
-> WorldWide

ORDER

redline stealer 2022 # lifetime activatio...



Escrow

USD 7.23
BlueSoft (30) (4.87 ★)

BTC | XMR
Afghanistan
-> WorldWide

ORDER

software cracking and keygen



Escrow

USD 56.16
Spearhead (4) (4 ★)

BTC | XMR
United States
-> WorldWide

ORDER

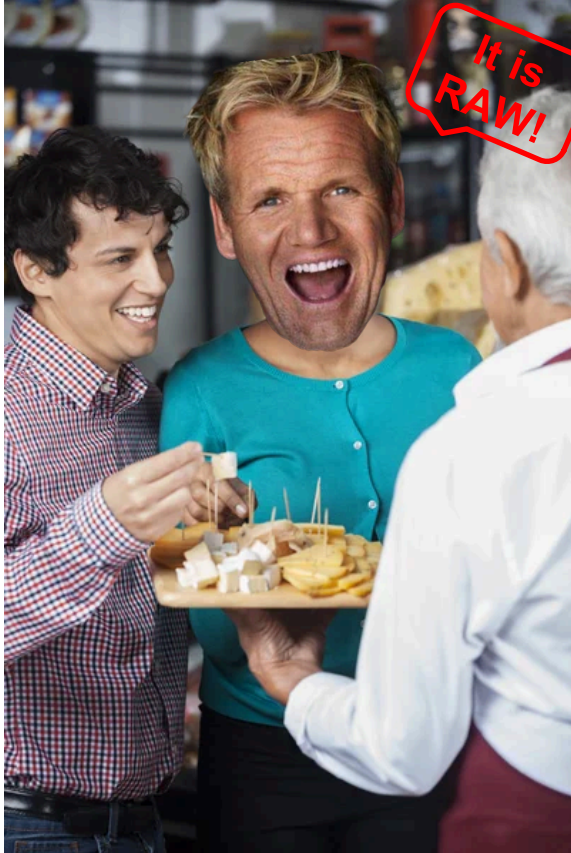
- An underground market is a popular platform where cybercrime commodities are traded between vendors and buyers
- It is a mature ecosystem akin to Amazon/eBay, where different roles collaborate to ensure the market's sustained operation over extended periods

Appraisal System in Underground Markets

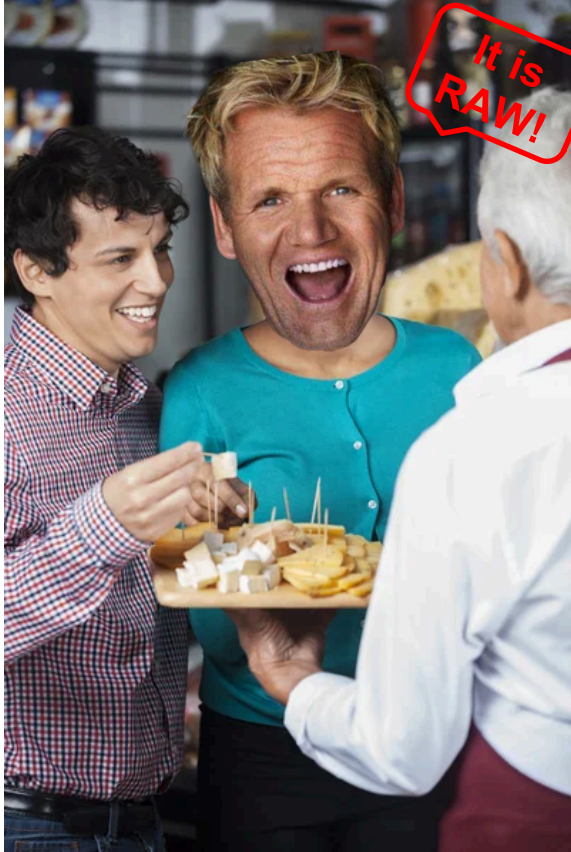


<https://www.henryford.com/blog/2017/06/food-samples-safe-eatc>

Appraisal System in Underground Markets



Appraisal System in Underground Markets



Underground marketplaces:

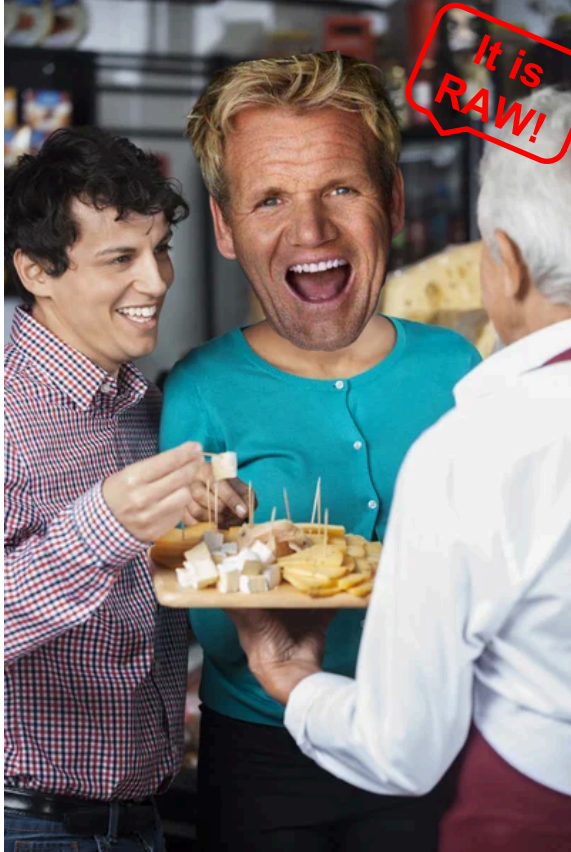


Vendors



Vouch Copy

Appraisal System in Underground Markets



Underground marketplaces:



Vendors



Vouch Copy



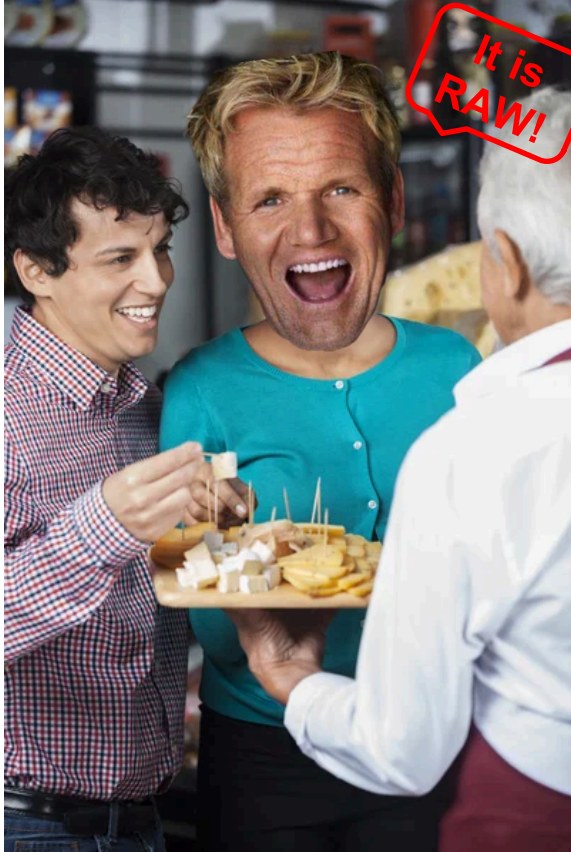
Individual
appraisers



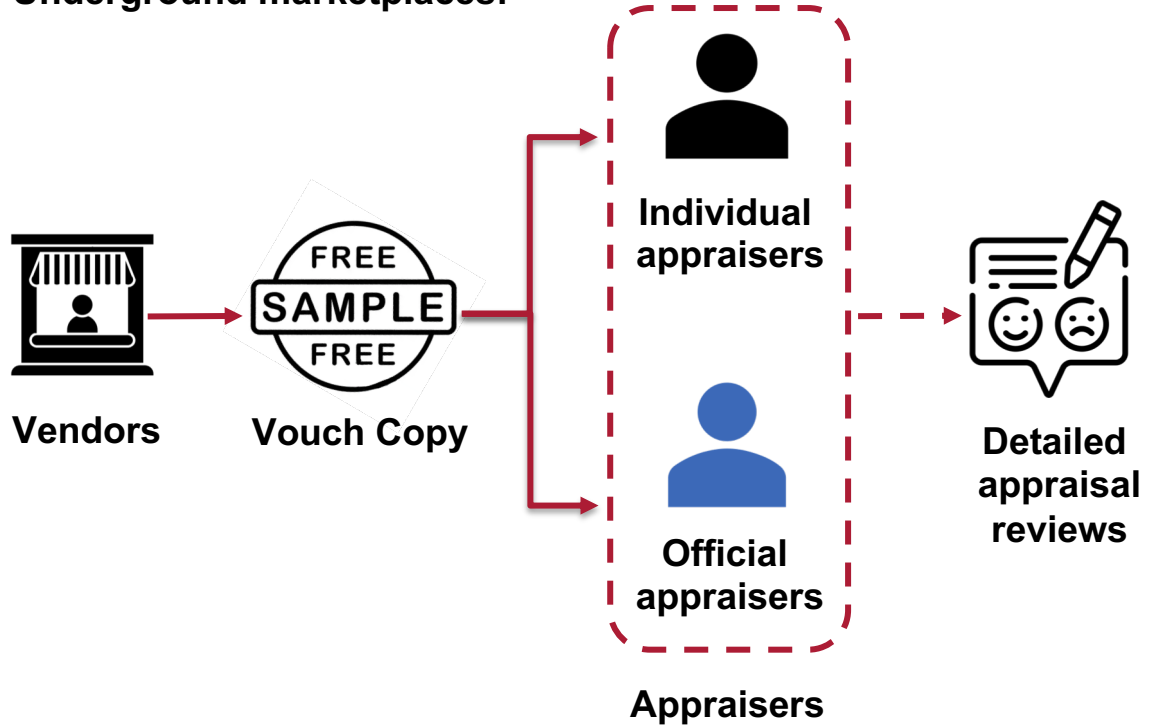
Official
appraisers

Appraisers

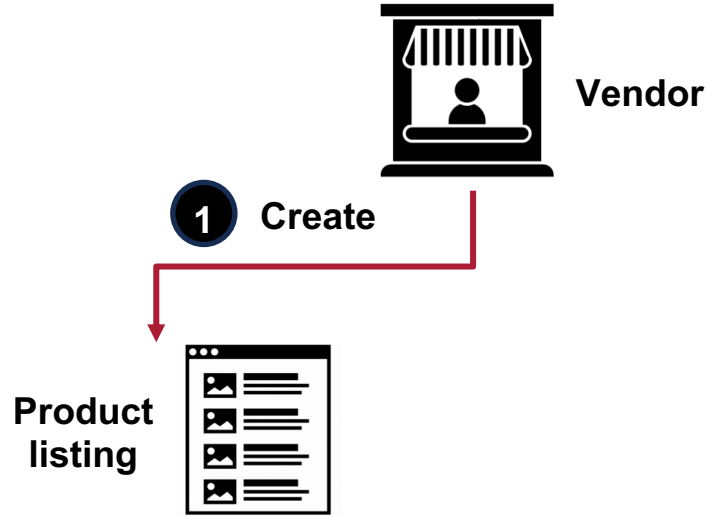
Appraisal System in Underground Markets



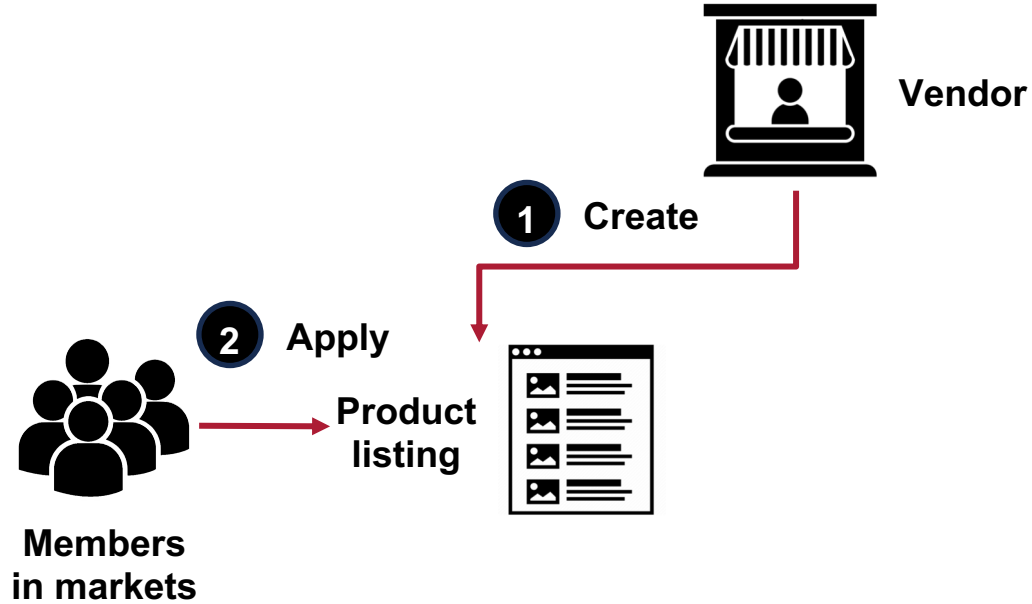
Underground marketplaces:



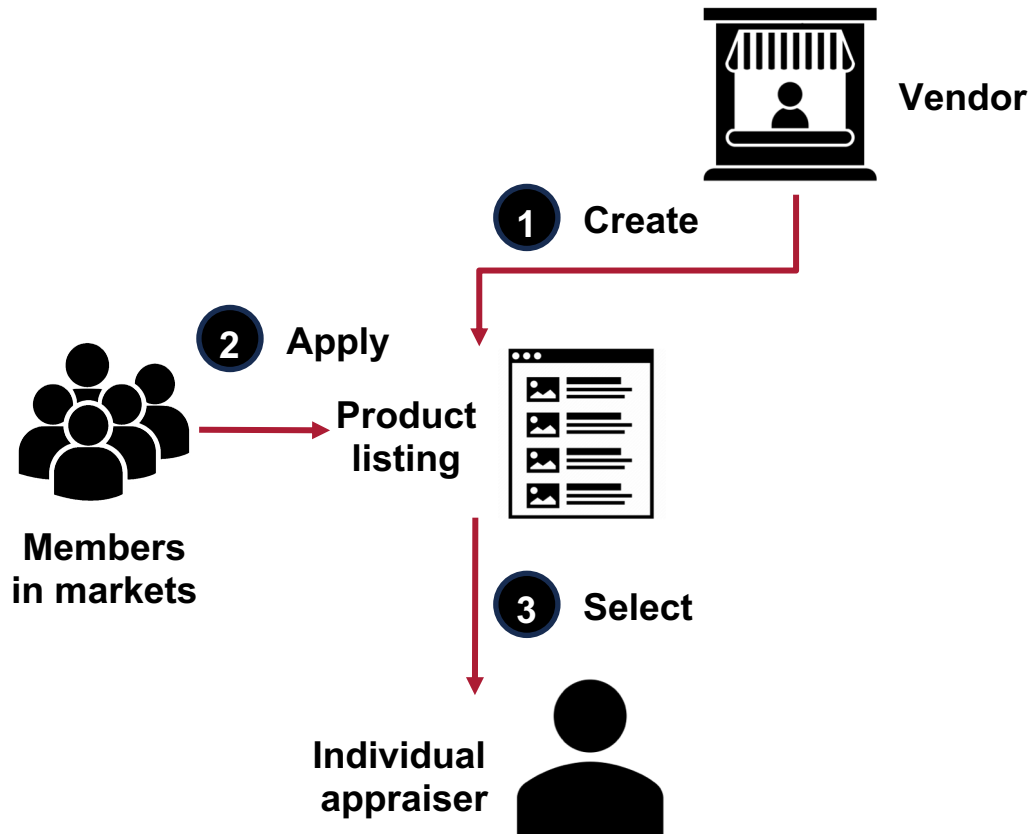
Appraiser Role Selection



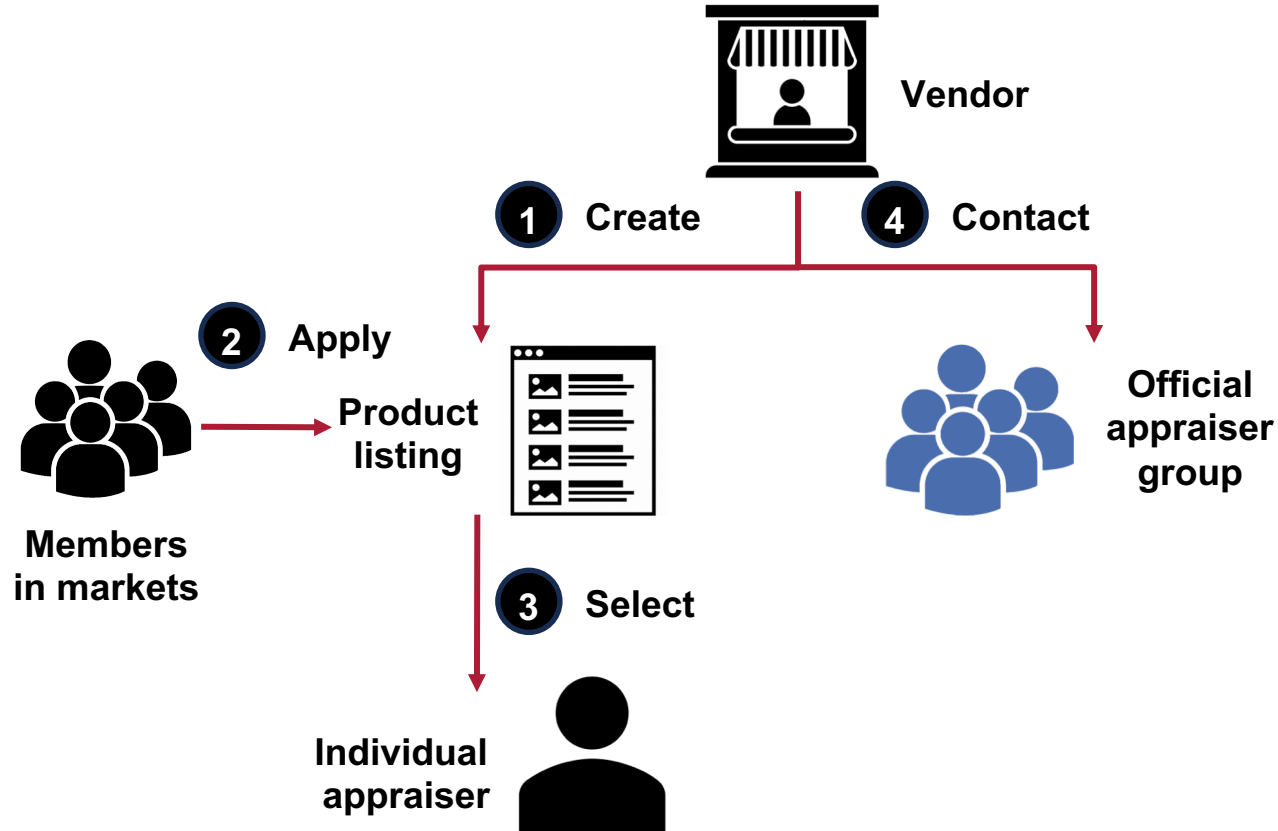
Appraiser Role Selection



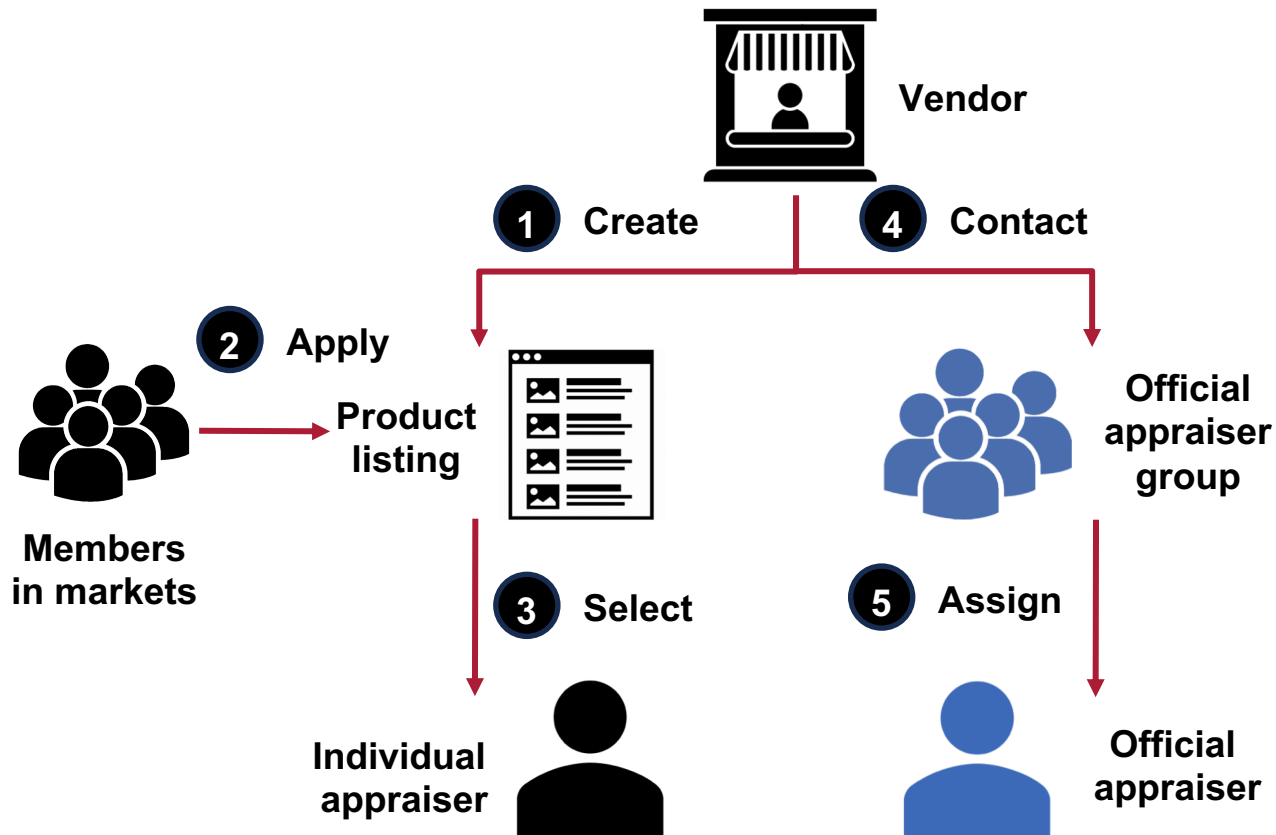
Appraiser Role Selection



Appraiser Role Selection



Appraiser Role Selection



Appraiser Role Selection Criteria

Merits	% of vendor	% of appraiser meet criteria	Appraiser's merit value in avg	Non-appraiser's merit value in avg
Number of posts	29%	96.5%	3,788	242
Whether VIP	67%	90.5%	-	-
Reputation score	9%	94.5%	727.4	62.2
Length of member	3%	91%	876	630
Whether staff	12%	100%	-	-

Appraisers are trustful and reliable role selected through a strict and transparent internal process

Appraisal Products

Step 1. Retrieve the vendors' product listings associated with each appraisal reviews

Step 2. Pre-defined 11 product categories, and manually labelled product listings as training dataset

Step 3. Train an illicit product classifier to categorize the listings of vendors

Step 4. Link each appraisal review to its corresponding listing category

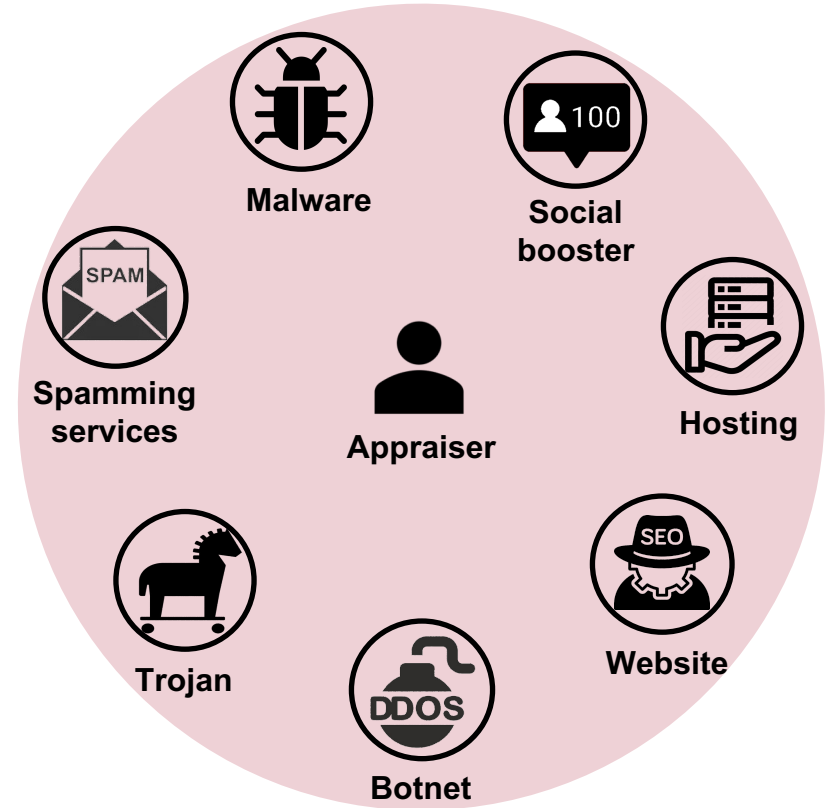
Appraisal Products

Step 1. Retrieve the vendors' product listings associated with each appraisal reviews

Step 2. Pre-defined 11 product categories, and manually labelled product listings as training dataset

Step 3. Train an illicit product classifier to categorize the listings of vendors

Step 4. Link each appraisal review to its corresponding listing category



Appraisal Products

Product	Assessment merit
Malware	Ease of use, file size, price, GUI/panel, design, support, features, detection, stability, installation, functionality , compatibility, performance
Website	Turnaround time (TAT), backlink features (types, number of received backlinks, ranking scores and domain age), communication, price, support, SERP boosting results, keyword features (# of searches, competition and KD value)
Making money guide	Grammar//language, method originality/uniqueness, ease of use, design/layout, content, price, method, support, compatibility, effectiveness, profit, investment/cost

Inspiration: these information provided by appraisers can be considered as CTI!

Methodology

Identifying
target data
source –
appraisal
reviews

Extracting
CTI

Methodology

Identifying
target data
source –
appraisal
reviews



Underground
marketplace dataset



Official appraisers
and
appraisal reviews

Extracting
CTI

Methodology

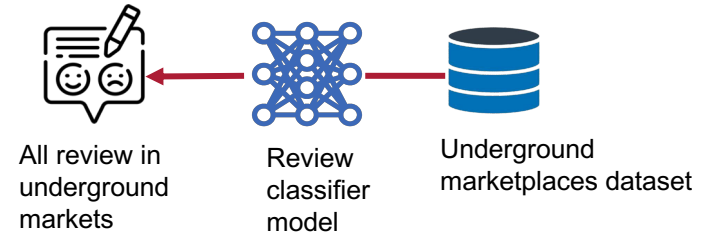


Identifying
target data
source –
appraisal
reviews

Extracting
CTI

Methodology

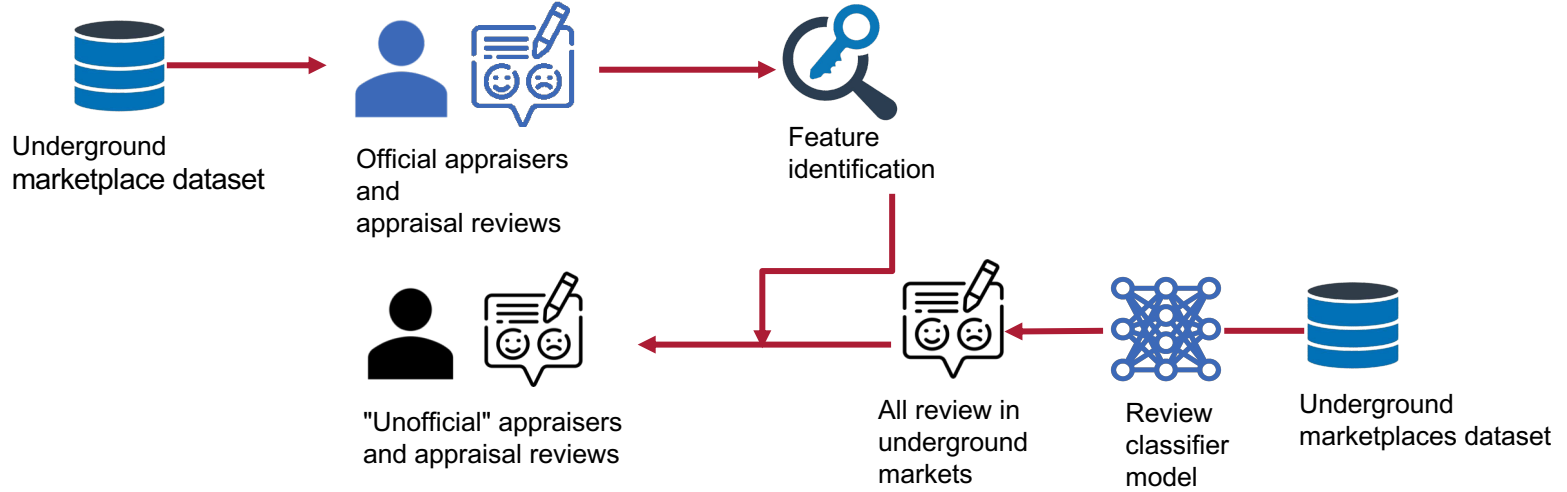
Identifying target data source – appraisal reviews



Extracting CTI

Methodology

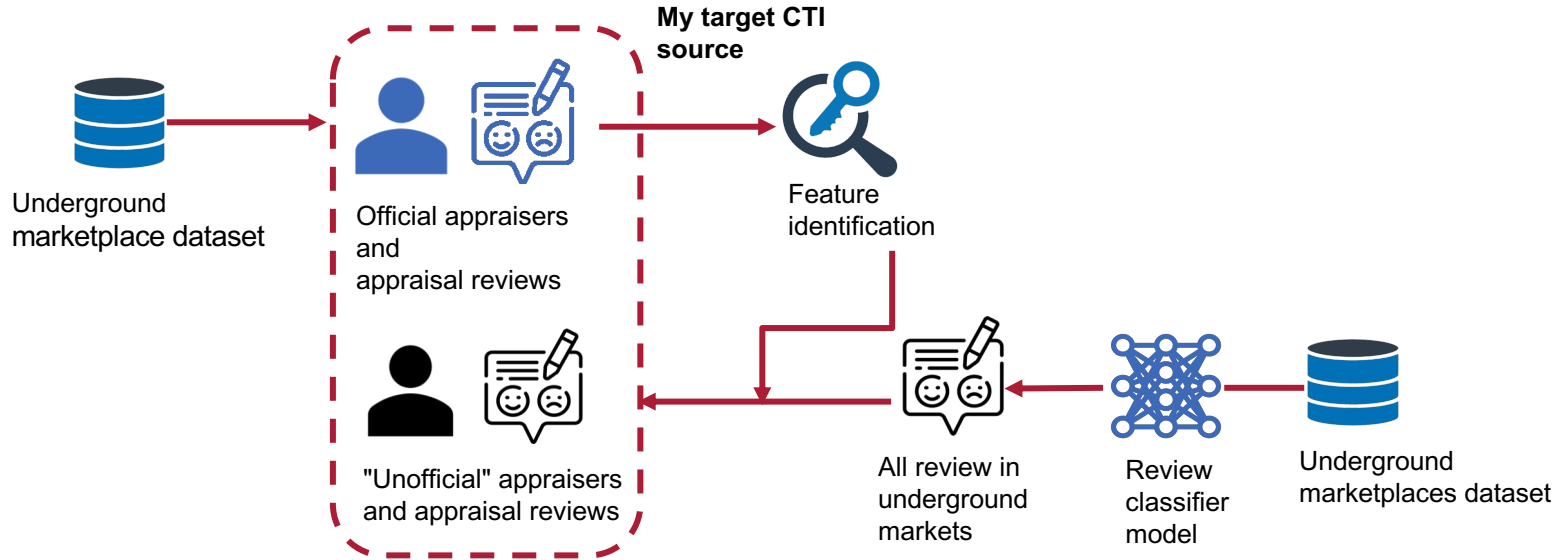
Identifying target data source – appraisal reviews



Extracting CTI

Methodology

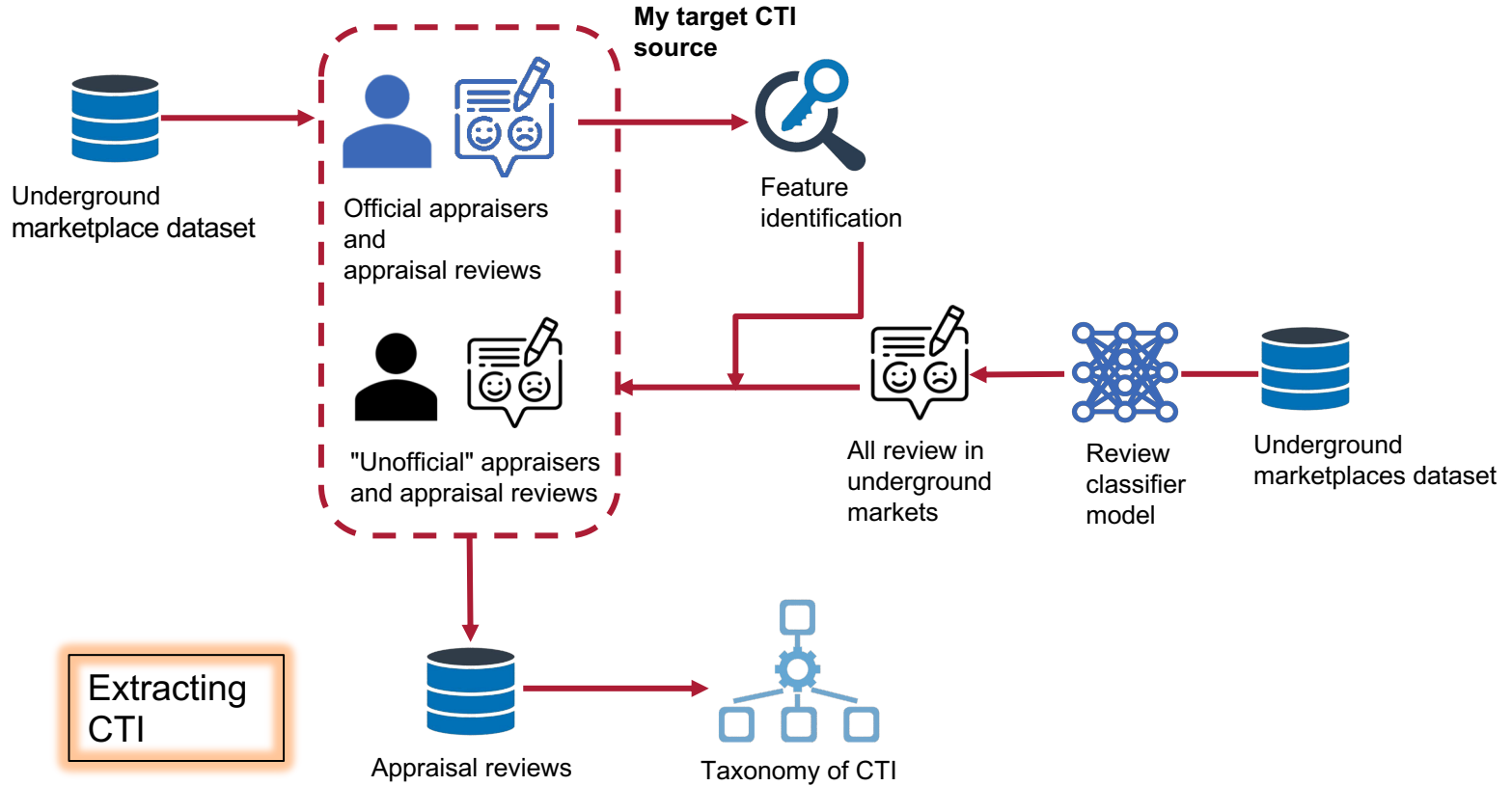
Identifying target data source – appraisal reviews



Extracting CTI

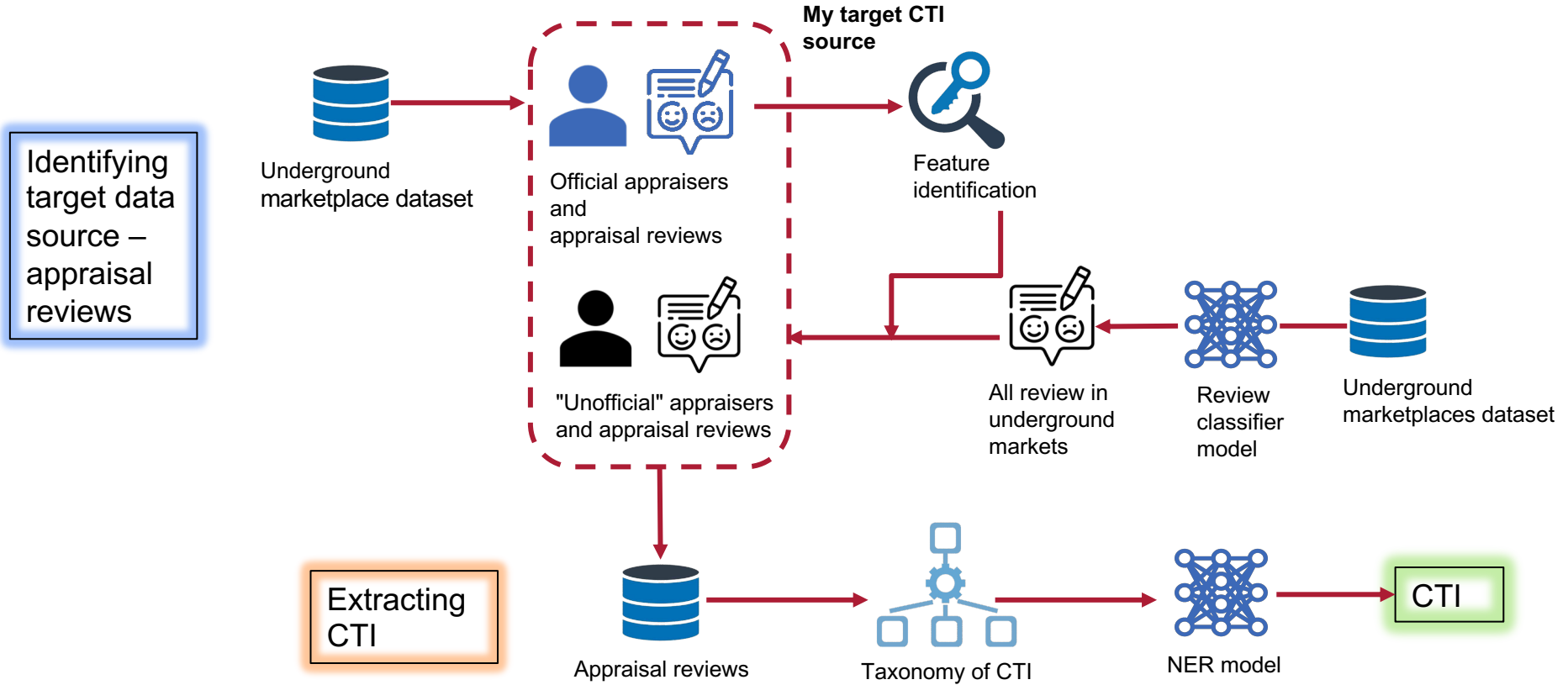
Methodology

Identifying target data source – appraisal reviews



Extracting CTI

Methodology



Taxonomy of CTI



**Academic
papers**

Taxonomy of CTI



Malware



Account



Website



**Academic
papers**

Taxonomy of CTI



Malware

Filename, version, file size, hash, anti-virus detection result, IPs of botnet, dependencies, whether fully undetectable (FUD), FUD types (scan time or run time), ...



Academic papers



Account

Account age, whether verified, verification methods (phone or email), whether has profile, email, # of **followers/tweets/likes**, whether high-retention views, ...



Website

Type of backlinks, # of alive backlinks, search engine ranking, domain age, geolocation of backlinks, keywords competition score, keywords search volume, ...

Results

- 8 underground markets: Hack Forums, Blackhat World, V3rmillion, MPGH, Nulled, OGUUsers, Evolution, and Raid
- 56,229 appraisal reviews posted by 18,701 unique appraisers from 2006 to 2023
- 23,978 artifacts from 41 types of CTI associated with 16,668 (50.2%) appraisal reviews

Unique CTI from Appraisal Reviews

Comparison with non-appraisal (buyers) review:

	CTI density	Overlap
Appraisal review	50.2%	93.5% artifacts are unique to appraisal reviews
Non-appraisal review	2.7%	

Comparison with exiting public CTI source:

	Appraisal review
VirusTotal	2 (0.4%) hashes are labeled as malicious 482 (97.8%) no records
White papers	2 (1%) covers CTI in website and account categories

Q & A

Thank You!

Example of A Vendor Listing

Basic Package ~ \$25

- [+] Reddit Method to generate posts/karma and overall more followers.
- [+] Converting followers to your OF/Fansly
- [+] Tricks to generate 20 - 30\$ per customer per week without PPV
- [+] Utilising OF's policies for improved turnaround.

Gold Package - Fansly Management Oriented ~ \$550 (0/5) Copies Only

- [+] Includes all the basic methodology of Basic Package
- [+] Method I use to reduce model costs/pay. This is great if you pay per content to your model.
- [+] Using method to generate traffic and operate a profitable business without a contracted model. (reduction in operation costs)*
- [+++] Creating a content portfolio without a contracted model + Setting up OF/Fansly without a Contractor

Vouch Copies for Gold Package : 1/1 (Reputed Members only - at my discretion)

Vouch Copy Rules

1. 1k+ Rep, 1k+ Posts, V3NDOR or UB3R only. Has a track record of leaving VC reviews in-depth.
2. 200 posts, 100+ rep, L33T. Has a track record of leaving VC reviews in-depth.

Vouch Given to Navos.

Example of A Vendor Listing

Title: How to Get Free Food From Almost Anywhere!

Author: Bonkers

Pages: 5 pages; 795 words.

Description: This eBook will teach you how to get free food from just about any restaurant. There is a slight investment required but you get the money back instantly (generally under \$5).

Payment Options: PayPal ONLY as a gift.

Copies Available: 31 for now, may add more later.

Review Copies Available: 2 for OFFICIAL REVIEW ONLY. Posters asking for 'free review copies' are not reported.

Resale Rights: Resale rights are available for \$35 however you may NOT sell on HF.

Price: \$3.

How to pay: Send payment as a GIFT (other payments will be considered donations!) from the Buy it Now PayPal button. PM me after your purchase and I will respond within 24 hours (generally within 2 hours, it just depends if I'm sleeping or not) :)

Example of an Appraisal Review

I have received a review copy in return of my review, turn around time was fast, completed just within 2 days.

Seller over delivered in term of words count by 25% more.

Seller followed my instructions carefully, briefing and communication were great.

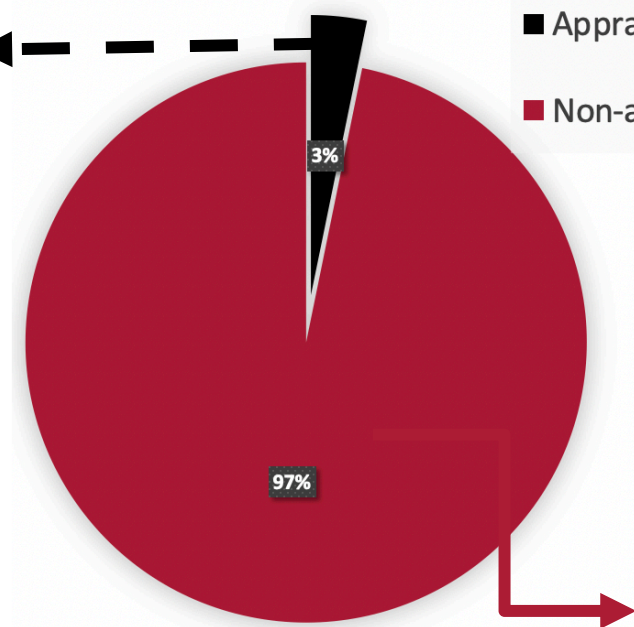
Checked with Grammarly found no mistake, no spelling error.

Content passed Copyscape with no plagiarism found in the rewrite.

I got a green light signal from the Yoast's reading guidelines as below:

- The copy scores 72 in the Flesch Reading Ease test, which is considered fairly easy to read.
- None of the paragraphs are too long, which is great.
- 2.1% of the sentences contain more than 20 words, which is less than or equal to the recommended maximum of 25%.
- 31.4% of the sentences contain a transition word or phrase, which is great.
- 7.1% of the sentences contain passive voice, which is less than or equal to the recommended maximum of 10%.

Literature Review

- 
- 1. Longer and more detailed review
 - 2. User background check
 - 3. Official organization
 - 4. Unexplored yet...

■ Appraisal review

■ Non-appraisal review

- 1. Consider feedback as a proxy to derive the lower bound of sales volumes and revenue [46,48, 99,110]
- 2. Use feedback ratings and customer's review texts to reflect the sellers' product quality and reliability [46,70]
- 3. The impact on sellers' reputations, sales and prices of goods [59,61]

Official Appraiser Recruitment

- 2 official appraiser groups
 - Post public recruitment
 - Member application
 - Selection

Official Appraiser Recruitment

NOW RECRUITING

What is Appraisers?

Appraisers is a group of high quality and community trusted members who will work together to make the marketplace a safer place.

Appraisers will unbiasedly and incorruptibly review as well as appraise any/all marketplace offerings.

Appraisers will confirm account ownership, NFA holdings, BTC backing, and other deal-breaking metrics.

Appraisers will help to facilitate on-site deals by confirming vendor identities, product completeness, product quality.

Appraisers do not accept any form of payment for favorable appraisals, with no exemptions.

Group's Userbar



Requirements

- Member of Hack Forums for at least 1 year.
- Must be an Ub3r member. (Approved but not upgraded does not count)
- Minimum of 500 posts made
- No open/unresolved scam reports.
- Reputation is subject to inspection.

Official Appraiser Application

Graphics:	8/10
Layout:	9/10
Quality of information:	10/10
Quality of method:	7/10
Response time:	10/10
Overall quality:	9/10

It is a very high-quality guide, well laid out and organized. Not only does he include various ways to use the method and also how this method differs from similar methods, but he also includes sources to even more information. The graphics are well done but in small numbers. However, having a small number of graphics means the author was focused on the information rather than the look which is a good sign. The author includes where the method has its advantages and disadvantages as well as what it would take to succeed using the method. The e-book/guide could easily sell for \$150+. However, due to the nature, risk, and overuse/knowledge of the method, it could go for around \$80-\$100 depending on where he is selling.

For the Instagram account:

<https://hackforums.net/showthread.php?ti...id56573235>

Official Appraiser Reviews

Official Review

4/5 Quality of Information: Based on the concept of this eBook explained in very understandable ways.

3/5 Ease of Use: It's more of a physical thing, can you go out e

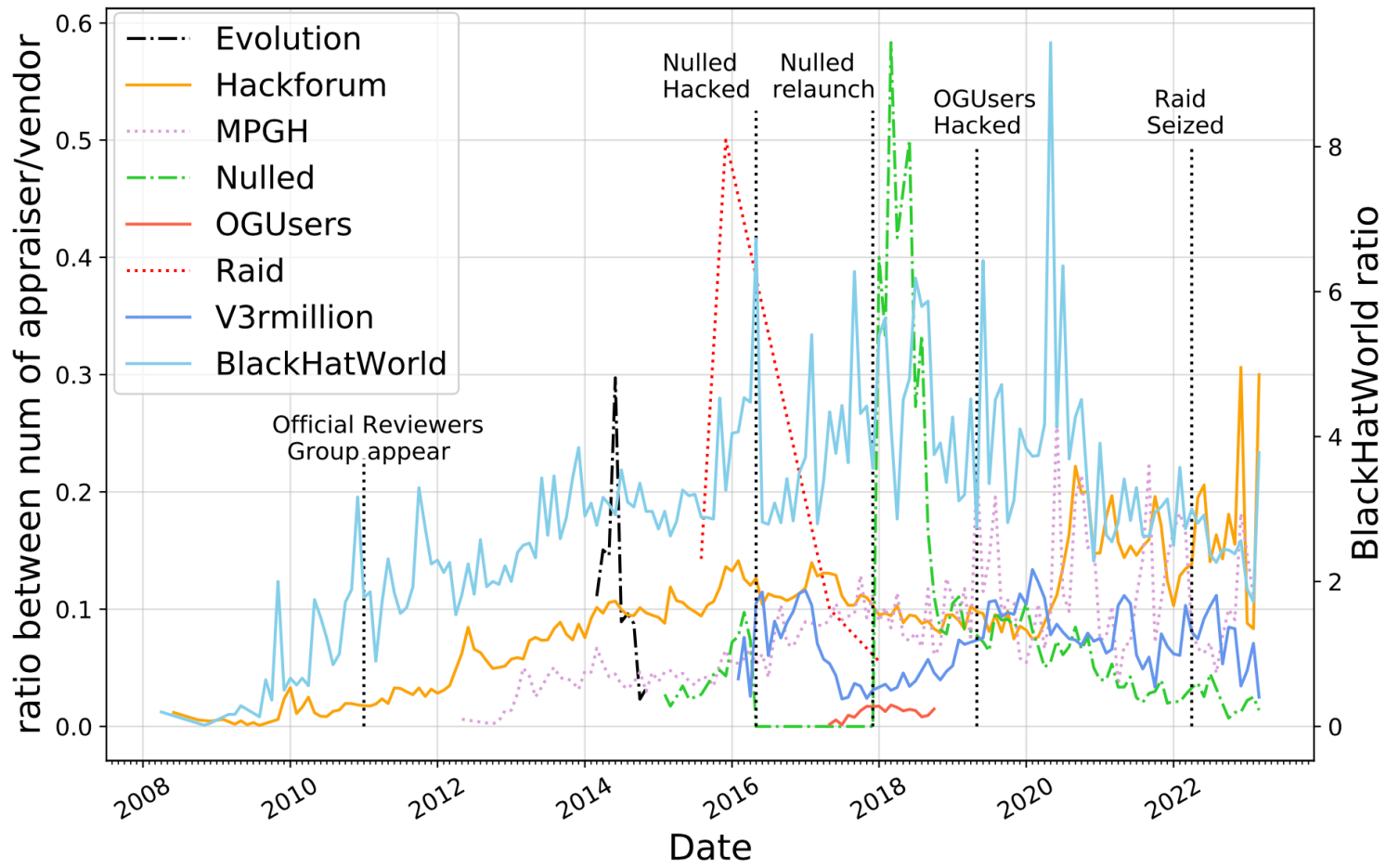
2/5 Layout: Layout was general

4/5 Grammar: None found

4/5 Originality: I have seen a few of these eBooks around before added a little "What not to do" section which can be helpful.

Notes / Comments: N/A

Appraiser Role



Less Trusted Appraisers

Less trusted appraisers

- Method
 - Scam reporting
 - Dependency parser to extract subject, object, etc
- Cases
 - Friend of vendor; get paid to write appraisal review
 - Multiple accounts own by same vendor
 - Fake appraisal group

Review Classifier Evaluation

TABLE III: The evaluation of review classifier

Review classifier	Evaluation metrics	
	Recall (%)	Precision (%)
LSTM	96.4	93.1
BiLSTM	94.4	91.9
TextCNN	93.1	92.3
SVM	93.2	89.0
Naive Bayesian	95.1	79.6
Logistic Regression	87.5	90.7
K-Nearest Neighbors (neighbors=3)	3.7	87.3
Multi-Layer Perceptron	89.3	89.8
Random Forest (max depth=2))	67.5	95.4

Data Completeness

TABLE II: Comparisons on dataset volume between our study and other works

Market	Author / Measurement Date	Traces	Users
HackForums	Zhang et al. [124] (– 09/2018)	238,212	74,909
	Our work (– 09/2018)	12,916,668	480,101
Nulled	Zhang et al. [124] (– 09/2018)	356,605	118,738
	Our work (– 09/2018)	525,169	76,668
	Sun et al. [101] (01/2015 – 05/2016)	121,486	599,085
	Our work (01/2015 – 05/2016)	121,499	599,085
MPGH	Sun et al. [101] (12/2005 – 02/2019)	3,614,061	323,772
	Our work (12/2015 – 02/2019)	9,363,422	477,517
BlackHatWorld	Portnoff et al. [91] (10/2005 – 03/2008)	7,270	8,718
	Our work (10/2005 – 03/2008)	75,975	14,133

Data Completeness

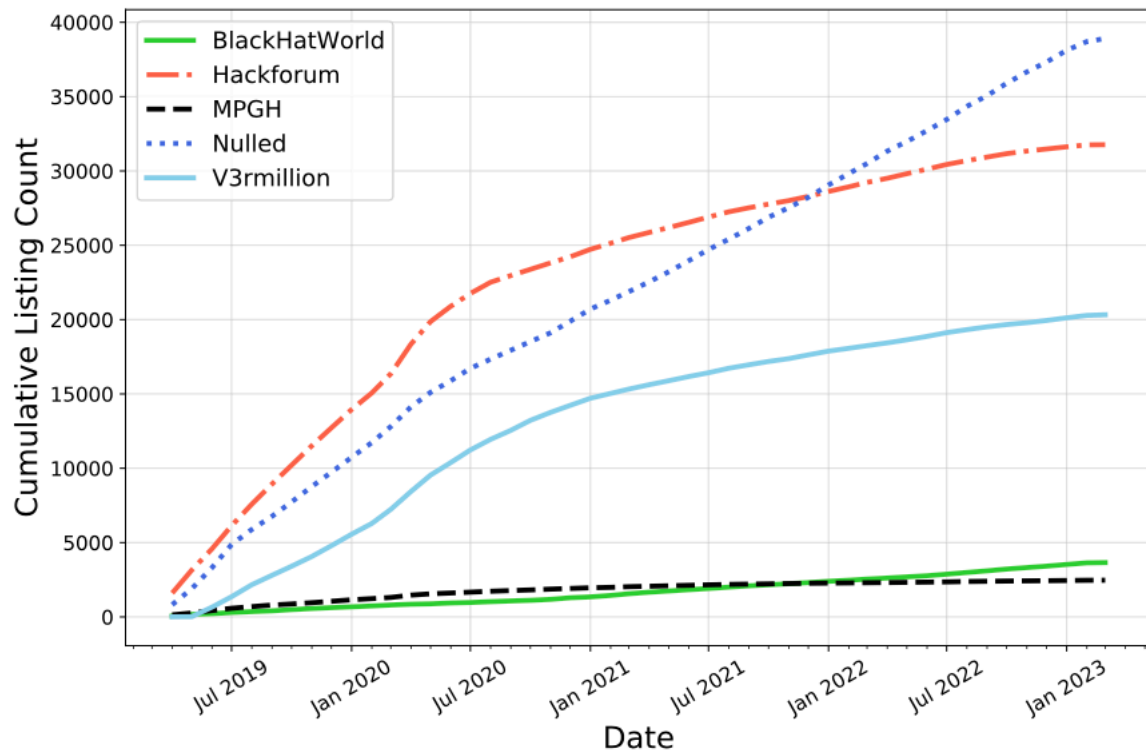


Fig. 2: Cumulative listing count of our scrape over time

Data Summary

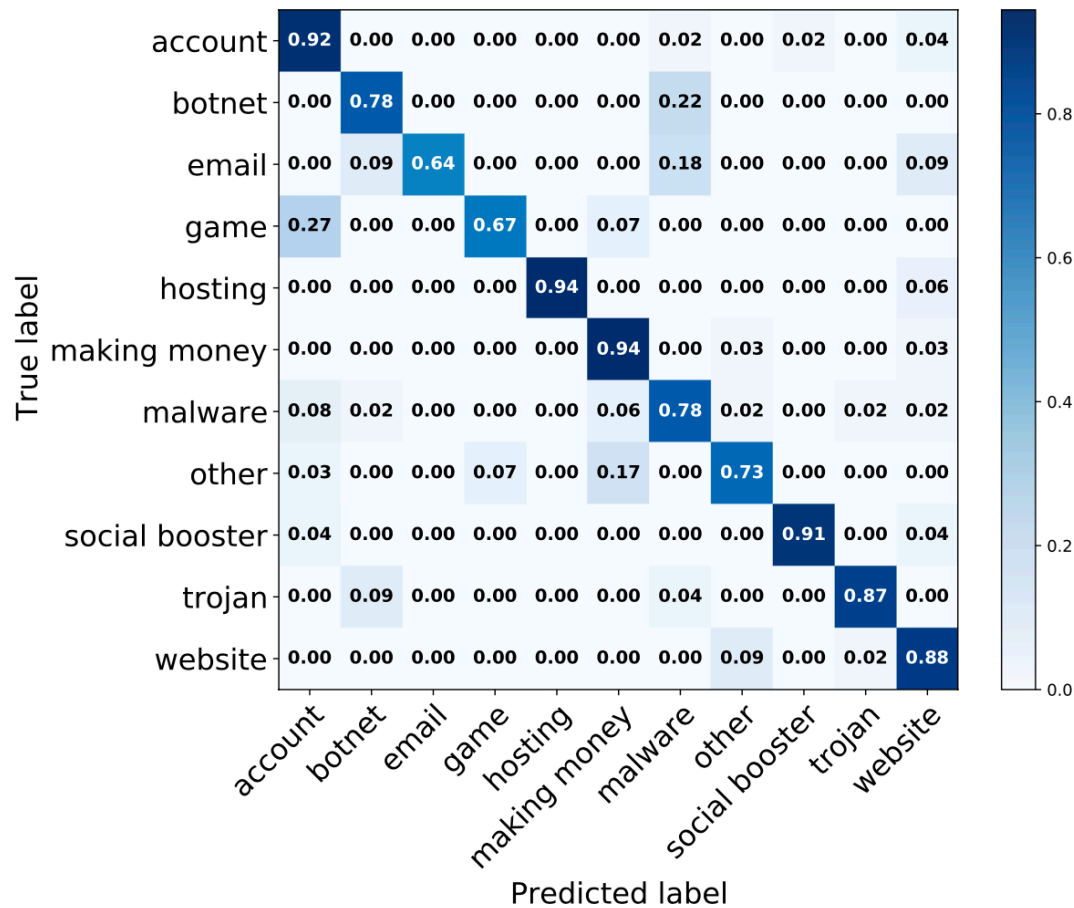
Type	Marketplace	Data source	Measurement date	# traces	# appraisal review (%)	# appraiser (%)	# appraisal listing (%)	# non-appraisal review (%)	# non-appraiser (%)
Groundtruth <i>D_{gt}</i>	Hack Forums	Our scrape	02/07 – 03/23	9,312,519	1,927 (3.4%)	379 (2.0%)	1,256 (4.9%)	-	-
	MPGH	CrimeBB	12/06 – 03/23	1,532,961	2,127 (3.8%)	100 (0.5%)	966 (3.7%)	-	-
Detected <i>D_{det}</i>	BlackHatWorld	Our scrape	03/08 – 03/23	2,434,465	26,304 (46.8%)	6,505 (34.8%)	4,230 (16.4%)	366,884 (21.6)	63,003 (17.6%)
	HackForums		02/07 – 03/23	9,312,519	19,414 (34.5%)	8,067 (43.1%)	13,678 (52.9%)	829,301 (48.9%)	204,199 (57.1%)
	MPGH	11/17 – 03/23	12/06 – 03/23	1,532,961	2,127 (3.8%)	881 (4.7%)	1,734 (6.7%)	147,911 (8.7%)	41,389 (11.6%)
	V3rmillion	CrimeBB	02/16 – 03/23	1,330,279	3,330 (5.9%)	1,797 (9.6%)	2,347 (9.1%)	257,484 (15.2%)	24,368 (6.8%)
	OGUsers	12/06 – 06/20	04/17 – 02/19*	1,665,800	442 (0.8%)	219 (1.2%)	355 (1.4%)	51,851 (3.1%)	5,331 (1.5%)
	Raid		05/15 – 08/18†	1,556	4 (0.007%)	3 (0.02%)	4 (0.02%)	54 (0.03%)	46 (0.01%)
	Nullled	Our scrape 01/18 – 03/23 CrimeBB 01/18 – 07/19 Nullled DB 02/15 – 05/16	02/15 – 03/23	1,053,825	1,504 (2.7%)	681 (3.6%)	1,203 (4.7%)	42,720 (2.5%)	18,333 (5.1%)
Evolution	DNM Archives	02/14 – 11/14**	9,384	69 (0.1%)	69 (0.4%)	63 (0.2%)	979 (0.06%)	979 (0.3%)	
Total	-	-	12/06 – 03/23	17,340,789	56,229	18,701	25,836	1,697,184	357,648

Appraiser – Product Data

TABLE VII: Appraiser and appraisal review per category

Category	# appraisal review (%)	# appraiser (%)	# appraisal listing (%)
Website	19,765 (35.2%)	4,002 (21.4%)	3,803 (15.1%)
Making money	14,819 (26.4%)	4,189 (22.4%)	8,881 (35.3%)
Account	5,940 (10.6%)	2,618 (14.0%)	3,798 (15.1%)
Other	5,374 (9.6%)	2,431 (13.0%)	2,581 (10.3%)
Social booster	3,372 (6.6%)	1,851 (9.9%)	1,838 (7.3%)
Malware	2,443 (4.3%)	1,281 (6.8%)	1,768 (7.0%)
Game	1,246 (2.2%)	703 (3.7%)	700 (2.8%)
Hosting	847 (1.5%)	467 (2.5%)	517 (2.1%)
Botnet	655 (1.2%)	374 (2.0%)	503 (2.0%)
Trojan	649 (1.2%)	355 (2.0%)	498 (2.0%)
Email	759 (1.3%)	430 (2.3%)	241 (1.0%)
Total	56,229	18,701	25,836

Product Classifier Evaluation



NER Evaluation

TABLE XI: Evaluation of adapted spaCy's NER model

Category	CTI	Precision	Recall	F1-Score
Social booster	Followers	84.4%	87.1%	85.7%
	Views	83.2%	82.1%	82.6%
	Likes	84.3%	85.1%	84.6%
	Subscribers	85.1%	83.2%	82.4%
Website	PageRank	89.5%	88.5%	89.0%

CTI Extraction – Name Entity Recognition (NER)

Person

Company

Elon Musk, the CEO of Tesla, is known for his visionary leadership...

CTI in underground:

Price

\$150 worth of vouchers for \$5...

Page ranking

I was given a backlink with page ranking 7, and 2 more with PR6 and PR5 bonus links with less than 40 OBL!

CTI Extraction – Name Entity Recognition

Challenges:

18 named entities that existing NER model can extract:

person,
facility,
organization,
location,
event,
date,
money,
quantity ...



**CTI-relevant
entities,**

as existing NER
models are not
trained for my
problem domain

CTI Extraction – Name Entity Recognition

Step 1. Identify all types of CTI in appraisal reviews

Step 2. Manually annotate appraisal reviews with each type of CTI as training data, using BIOES-style tagging strategies.

Sequence	backlink	with	page	ranking	7	,	and
BIOE	O	O	B	I	E	O	O

Step 3. Fine tune the existing spaCy NER model

Step 4. Apply the model to wild appraisal reviews

