Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service

Zhibo Sun, Adam Oest, and Penghui Zhang, *Arizona State University;* Carlos Rubio-Medrano, *Texas A&M University - Corpus Christi;* Tiffany Bao and Ruoyu Wang, *Arizona State University;* Ziming Zhao, *Rochester Institute of Technology;* Yan Shoshitaishvili and Adam Doupé, *Arizona State University;* Gail-Joon Ahn, *Arizona State University and Samsung Research*

https://www.usenix.org/conference/usenixsecurity21/presentation/sun-zhibo

This paper is included in the Proceedings of the 30th USENIX Security Symposium.

August 11–13, 2021

978-1-939133-24-3

Open access to the Proceedings of the 30th USENIX Security Symposium is sponsored by USENIX.

Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service

Zhibo Sun*, Adam Oest*, Penghui Zhang*, Carlos Rubio-Medrano‡
Tiffany Bao*, Ruoyu Wang*, Ziming Zhao¶, Yan Shoshitaishvili*, Adam Doupé*, Gail-Joon Ahn *§
*Arizona State University, ‡Texas A&M University - Corpus Christi ¶Rochester Institute of Technology, §Samsung Research
*{zhibo.sun, aoest, penghui.zhang, tbao, fishw, yans, doupe, gahn}@asu.edu
‡carlos.rubiomedrano@tamucc.edu, ¶zhao@mail.rit.edu

Abstract

Concession Abuse as a Service (CAaaS) is a growing scam service in underground forums that defrauds online retailers through the systematic abuse of their return policies (via social engineering) and the exploitation of loopholes in company protocols. Timely detection of such scams is difficult as they are fueled by an extensive suite of criminal services, such as credential theft, document forgery, and fake shipments. Ultimately, the scam enables malicious actors to steal arbitrary goods from merchants with minimal investment.

In this paper, we perform in-depth manual and automated analysis of public and private messages from four large underground forums to identify the malicious actors involved in CAaaS, carefully study the operation of the scam, and define attributes to fingerprint the scam and inform mitigation strategies. Additionally, we surveyed users to evaluate their attitudes toward these mitigations and understand the factors that merchants should consider before implementing these strategies. We find that the scam is easy to scale—and can bypass traditional anti-fraud efforts—and thus poses a notable threat to online retailers.

1 Introduction

In concession abuse attacks, scammers leverage social engineering techniques to exploit the return policies of targeted merchants and obtain a *concession* (in the form of a refund or a replacement item) without returning any originally purchased products. Recent news of Amazon being scammed out of € 300,000 and $1.2M in 2017 and 2019 in two targeted *concession abuse* attacks reveals the tremendous (and growing) damage that such attacks can cause [14, 45]. These attacks become particularly heinous when scammers obtain such refunds using stolen accounts that belong to legitimate customers. Once successful, scammers monetize the refunds (often gift cards or replacement goods from the retailer) through services in the underground economy. Because offering concessions to appease distressed customers is a crucial business practice for retailers, these scams place companies in the difficult position of choosing between scam mitigation and the happiness of legitimate customers.

A perception by vendors who fall victim to concession abuse may be that these attacks are isolated incidents and can thus be resolved in an ad-hoc fashion. However, through a comprehensive analysis of underground forums and a concession abuse provider, we find that such attacks operate at scale, target merchants across multiple industry sectors, involve complex coordination between different underground actors, and overcome current industry best practices and mitigations to reliably yield success for the criminals.

In this paper, we show that concession abuse is, in fact, a prevalent criminal *business service* to which even unsophisticated cybercriminals can *subscribe* and subsequently profit with minimal investment. We refer to this ecosystem as *Concession Abuse as a Service* (CAaaS). The unsophisticated customers of CAaaS (*scam initiators*) request that attackers (*service providers*) engage with a targeted merchant to execute the scam. The scam initiator's ultimate goal is to obtain money from a purchased order via a concession from the merchant after paying a nominal commission to the service provider.

Despite its surface simplicity, CAaaS is a sophisticated online criminal industry that coordinates a diverse range of parties to facilitate key stages of the scam. An end-to-end supply chain of illicit services underpins CAaaS and provides components such as stolen account credentials [42], forged documents [17], and reshipping services [15]. Given the fact that existing mitigation approaches cannot effectively protect merchants from CAaaS [14, 45], and the wide range of threat actors that the scam entails, the research community must seek *systematic and proactive mitigations* to stop concession abuse across the entire ecosystem. To propose such mitigations, we first carefully study CAaaS to understand the *economics* and *implementation* of the attacks, and then conduct a survey as a preliminary evaluation of the proposed mitigations.

To this end, we performed an in-depth analysis of criminal communications on four popular underground forums, where we discovered 2,251 service providers of CAaaS scams who, collectively, target 264 merchants. Both scammers and

targeted merchants are distributed globally, and we found that CAaaS has not only remained active but is becoming more prevalent in recent years, despite the evolution of retailer return policies to prevent fraud. We identified underground communities in which users discuss scam questions, share their success and failure experiences, and even post tutorials for beginners. We found that these resources help train ill-intentioned users to become CAaaS service providers *within months*. Additionally, we joined a private discussion group run by a service provider and found the provider helped refund at least $81,159.27 over three months.

Prior work has examined social engineering skills [18, 20] and their applicability to traditional web-based phishing attacks, as well as persuasion techniques that manipulate people into performing actions or divulging confidential information [3, 8, 12, 29] and the phenomenon of criminal reshipping services [15]. General exploitation of merchants' return policies was studied in an *offline* context [37], and CAaaS combines and enhances these areas of cybercrime to target a unique part of the attack surface against retailers.

By performing the first such study of CAaaS, we help identify ways to disrupt the economics of the scam and empower vulnerable retailers to implement proactive defenses. Our contributions are thus as follows:

- We present the first study of the operations of an emerging threat, *Concession Abuse as a Service*, by examining the wide range of actors and supporting services involved in the scam and its economics.
- We characterize techniques that allow CAaaS to effectively defraud merchants, as well as failure cases and limitations of such techniques.
- We identify attributes to fingerprint CAaaS, propose mitigation approaches usable by merchants, and evaluate these approaches through merchant interviews and a user survey.

2 Overview

Concession abuse is a type of cybercrime that typically targets online merchant services.[1] In such scams, a malicious customer seeks to receive a concession—a free replacement or a refund—from a *targeted merchant* by socially engineering the Customer Service Representative (CSR) and exploiting the return process. If the scam succeeds, the criminal will get a free replacement or a refund, either of which can be monetized through additional intermediaries (see Section 3.4).

Concession abuse has evolved from ad-hoc scams into a *service* that has grown both in its complexity and effectiveness. In this transition, each scammer's role has expanded amid an environment in which attacks can occur on a large scale, and where individual cybercriminals can quickly gain expertise in their specific roles. Consequently, the barrier to entry has been greatly lowered such that even unskilled criminals can leverage and profit from concession abuse.

In this paper, we study the ecosystem of concession abuse as a service (CAaaS). In particular, we investigate the following research questions:

1. How does concession abuse work as a service (Section 3)?
2. What are the characteristics of CAaaS, and on what scale does it operate (Section 4)?
3. What do criminals do to execute concession abuse successfully, and when do certain scams fail (Section 5)?
4. How can merchants prevent concession abuse from succeeding at scale (Section 6)?

Analysis Approach. We used a qualitative approach for Question 1, a quantitative approach for Question 2, and hybrid approaches for Questions 3 and 4. For clarity, we describe each approach in its respective section.

Data Sources We base our analysis of CAaaS on four distinct data sources discussed throughout the remainder of this paper: threads and posts from underground forums, messages in private criminal groups, interviews with two large (undisclosed) US-based merchants, and a user survey about possible mitigation strategies.

We sought to identify underground forums with a significant focus on topics related to retail scams (the presence of which might imply the respective community's interest in concession abuse). We started with a large forum that had recently suffered a database breach: Nulled.io [33]. Using this database, we could analyze public threads and private messages. We then crawled all the URLs therein to compile a list of candidate forum URLs.

We manually analyzed each publicly accessible forum on this list, and for each that was still online and had at least 100 threads in scam-related sections, we (1) exhaustively crawled its public content and (2) recursively applied the same process to discover other candidate forum URLs. We ultimately identified and crawled four forums suitable for our analysis: Nulled.io (NULLED), SocialEngineered.net (SENet), Sinister.ly (SIN), and MPGH.net (MPGH). We summarize the relative popularity of these forums, at the time of our data collection in early 2019, in Table 1.

Given the fact that commoditized criminal services cater to less sophisticated criminals [30], we believe that our choice of clearnet forums was appropriate for the analysis of CAaaS.

Ethics. We proactively addressed ethical concerns by working closely with our Institutional Review Board (IRB) to obtain their approval and to develop an accepted ethical protocol for this study. First, we do not attempt to identify users from the collected datasets and use anonymous expressions to represent corresponding sensitive information in this paper. Since our purpose is to analyze CAaaS, we do not focus on particular users in the underground forums.

Second, using leaked or crawling publicly available datasets is an acceptable practice in the study of the underground ecosystem [2, 15, 28, 40]. Since purchasing services from underground forums to collect data with limited affecting other

[1] Although traditional concession abuse can also target brick-and-mortar merchants, in this paper we focus solely on merchants with an online presence, as offline attacks do not have the same scaling potential and are addressable through physical security approaches [19].

Table 1: Popularity statistics for the forums we analyzed.

Forum	# Threads	# Posts	# Users	Data Covered
NULLED	121,486	3,495,593	599,085	Jan 2015 – May 2016
MPGH	325,626	3,614,061	323,772	Dec 2005 – Feb 2019
SENet	55,560	468,659	15,433	May 2011 – Feb 2019
SIN	56,352	499,257	14,583	Aug 2008 – Dec 2018

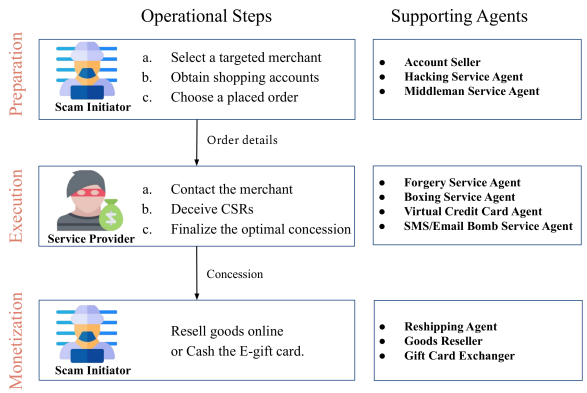

Figure 1: The steps and actors in CAaaS.

users is also acceptable in the research community [22, 38, 41], we pay for upgrading our accounts to access VIP sections of forums to collect more data.

3 Anatomy of Concession Abuse as a Service

To understand the steps and actors involved in Concession Abuse as a Service, we first conduct a manual qualitative study on the crawled forum threads, artifacts (e.g., attachments and tutorials), and private messages. Due to the high number of forum threads, we randomly selected 4,000 threads (1,000 from each forum) for our analysis. We exhaustively reviewed all of other types of data. We then synthesized our findings to gain a thorough understanding of CAaaS.

3.1 Scam Actors

At a high level, CAaaS involves two parties: the *Scam Initiator* and the *Service Provider*. A scam initiator is the customer of CAaaS who wants to receive a free concession, and a service provider is a scammer who sells concession abuse as a service. In addition to scam initiators and service providers, other criminal agents play various supporting roles to improve the scam's chances of success and to hide the scammers' identities. We divide the process of CAaaS into three steps: preparation, execution, and monetization, as shown in Figure 1.

In the following sub-sections, we describe each step along with the actors involved. To better illustrate the actors in CAaaS, we also show a representative set of their discussions in Table 2.

3.2 Preparation

In the preparation step, a scam initiator and a service provider make a deal for an order or a merchant. For a scamming order, the scam initiator provides to the service provider a placed order and the corresponding information.

To obtain sufficient information and scale up the CAaaS business, a service provider may ask scan initiators to fill out a service form, as addressed in their advertisements *"submit the refund form if your order is already delivered."* The form includes detailed questions regarding the order, account, and the expected outcome (e.g., refund or replacement). For example, if a scam initiator places an order, they need to provide the type of payment, preferably "the last 4 digits of the card", and clarify if they have "received or signed for the delivery." For more information, we present a real-world service form in Table 7 in Appendix A.

Table 2: Quotes from criminals involved in CAaaS.

	Agent	Quote
Preparation	Service Provider	I will be offering my refund service after learning and having successful refunds of my own on many stores. I will list stores that I am the most comfortable refunding ...
	Scam Initiator	I need someone who can replace items from cracked UK amazon accounts, need to be trusted...
	Account Seller	I am selling an amazing Amazon account today, lots of past orders and very easy to get refunds from. I will start the bid at 15$...
	Hacking Service Agent	I'm selling everything you need to start cracking and everything you need to make your own combos, I'm cracking for over 2 years now and i cracked many sites and made nice amount of money, now I'm here selling everything you need for cracking ...
	Middleman Service Agent	you will know me for my SE Guides and HQ Posts on this forum well today I am offering middleman services via Paypal ...
Execution	Forgery Service Agent	I am also now offering general photoshop work, (utility bill, bank statement, etc.) PM me for rates ...
	Boxing Service Agent	Most boxing is $10 – $15, depending on weight and packaging requested. Amazon boxing starts at $15 for under 5 lb, Amazon boxing 5 lb – 10 lb is $20. Want a box with a little weight? ->$12...
	VCC Agents	I'm Selling VCCs for amazon These VCCs have at 2 bucks on it, so they are good for SEing 10 bucks for 1 VCC Add me on skype...
	SMS/Email Bomb Service Agent	I am offering my email bombing service for w/e you needs, i can offer 200 / 50cents I will only accept BTC...
Monetization	Scam Initiator	Since my last deal feel through i am selling the 4 xboxs i have at my reship. I believe they are all start wars.
	Reshipping Agent	LOCATED IN U.S.A. We reship your packages to anywhere in the world! Prices start at $29.99 and up. Package receiver or sender must pay for shipping ...
	Goods Reseller	I have an ebay account with 100% positive feedback. Looking for someone to supply me with products that I can resell. I have done this before with a few members here with great results ...
	Gift Card Exchanger	Looking to buy AGC, can pay via PP or BTC Looking for 70%.

Scam initiators or service providers typically prefer not to use their own accounts for better anonymity. *Account Sellers* provide compromised accounts, and *Hacking Service Agents* provide account attacking toolkits. Furthermore, *Middleman Service Agents* moderate the process, keeping both parties anonymous and avoiding scams in the service.

3.3 Execution

After the deal is made and the initial order is placed, service providers contact the targeted merchant and attempt to deceive the CSR into providing a concession. In the conversation between the service provider and the CSR, there may be conditions that prevent the concession abuse scam from succeeding. In these conditions, the service provider may leverage the services provided by supporting agents. We list these conditions with the associated supporting agents in categories below, and we will elaborate on each category in Section 5.2.

Extra Proof. The CSR may require extra proof for the issued merchandise. A *Forgery Service Agent* helps by providing forged proof such as edited photos.

Return Requirement. The CSR may require the original goods to be returned prior to issuing the concession. A *Boxing Service Agent* helps to craft an otherwise empty shipping box with the weight expected by the merchant. In the case of high-value items, the box may instead be filled with counterfeit goods.

Credit Card Requirement. The CSR may issue a concession before the original product returns yet to ask the service provider for a credit card number as collateral to ensure the return. In such a case, a *Virtual Credit Card (VCC) Agent* is able to furnish a valid credit card number that would be accepted by the merchant with few dollars balance.

Accountholder Notifications. After the concession is processed, the CSR may send a notification to the accountholder via e-mail or SMS. This increases the risk of being detected if the service provider uses a compromised account. In an attempt to minimize suspicion, an *E-mail/SMS Bomb Service Agent* will help flood the accountholder's e-mail or SMS inbox with messages to drown out alert messages from the targeted merchant.

3.4 Monetization

Recall that a scam initiator chooses either refund or replacement. However, the CSR may not provide what the scam initiator wants, and thus the scam initiator must convert the attack outcome to their actual needs. There are three possible scenarios as follows:

Once a service provider succeeds, they will request a refund via an e-gift card or a replacement sent to a specific address.

Replacement to Cash. If the concession is a replacement item, it may be shipped to a *Reshipping Agent* who supplies a third-party address. It is worth pointing out that scammers take advantage of both legal reshipping companies and drops [15] as the reshipping agents. The scam initiator can then resell the goods directly (e.g., by advertising them in underground forums) or hire a *Goods Reseller* with a trusted reputation in online marketplaces (e.g., eBay). Once the goods are sold, the reshipping agent will mail the goods to the buyer, who may be unaware of their fraudulent origin.

By using reshipping agents and goods resellers, the scam initiator is isolated from both the merchant and the buyer, and can therefore remain safe from detection. Reshipping agents are favored as they often offer free storage for a generous period, which lowers costs for the initiator because they do not need to pay for warehousing.[2]

E-gift Card to Cash. To quickly cash out an e-gift card, the scam initiator can employ a *Gift Card Exchanger* to exchange it for digital wallet balance or cryptocurrency such as Bitcoin. However, this method generally carries higher fees (e.g., 30%, see Table 2) due to added risk. To avoid such fees, some initiators will instead use the e-gift card to order an item and then resell it using the aforementioned method.

CAaaS for Buying Discounted Goods. Interestingly, we observe that some service providers even behave as third-party dealers of arbitrary goods. A scam initiator reaches out to the service provider and pays them a heavily discounted price for a specific product (chosen by the initiator). The service provider then uses unrelated orders to obtain one or more refunds from a target merchant that sells this product. Finally, the provider uses the refund(s) to purchase the designated product for the initiator. As a result, the scam initiator gets a product at a price substantially below retail value, and the service provider gets payment for the service.

[2] One legal reshipping company frequently discussed by scammers (*Reship.com*) provides 60 days of free storage.

4 Analysis of CAaaS Features and Scale

As an emerging threat, CAaaS has a number of unexplored aspects, therefore we focus on the following questions:

1. Which merchants and goods do scammers target? (§ 4.2)
2. How much do providers earn from the service? (§ 4.3)
3. What is the geolocation of concession abuse scammers and their targeted merchants? (§ 4.4)
4. Does the scam operate at scale? (§ 4.5)
5. How difficult is it for newcomers to learn this scam? (§ 4.6)
6. Is the financial loss significant? (§ 4.7)
7. What is the overlap between the concession abuse scammers and other types of scammers? (§ 4.8)

4.1 Analysis Approach

To draw insights about large-scale activity in underground forums that extend beyond the qualitative manual analysis described in Section 3, we train a machine learning classifier and apply it to the whole dataset. Our approach is composed of three steps.

Step 1: Data Sampling. We randomly sampled 4,000 threads (1,000 in each forum) from the crawled forum data using *Stratified Random Sampling* [23], and we manually labeled each thread based on its content.

Step 2: Sampled Data Labeling. We designed three separate types of labels for answering the seven questions posed in Section 4, and we synthesized the labels based on the empirical analysis on the 4,000 samples.

CAaaS Topic. We classified threads by four CAaaS topics: Advertisement, Purchasing Request, Discussion and Support, and CAaaS-unrelated. These labels help to identify CAaaS-related posts and actors and will be used to answer all the questions.

Scamming Experience. For Question 5, we classified CAaaS-related threads by scamming experience: Successful, Failed, and Neutral experiences. These labels help to identify the conditions and the time that a scam succeeds or fails.

Forum Activity. For Question 7, we classified underground forum activities by Monetization, Hacking, Scam, and Other, and we specified common scams by Email

Table 3: CAaaS topic statistics for the forums.

CAaaS Topic	# Threads	# Posts	# Users
Advertisement	13,433	280,434	27,089
Purchase Req.	13,817	65,590	9,131
Discussion & Support	30,033	278,590	29,988
CAaaS-Unrelated	501,741	7,452,956	642,167

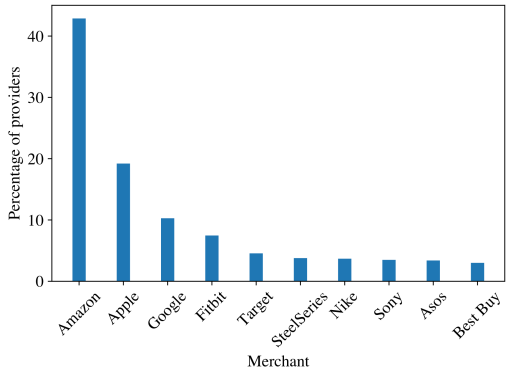

Figure 2: Top ten targeted merchants advertised by CAaaS providers.

Compromise, Data Breach, Denial of Service, Phishing, and Ransomware referred by common underground forum structures and FBI Internet Fraud definition [11].

Step 3: Data Classification. For each label type, we used the labeled samples to train a well-performing machine learning model and applied the model to the full dataset. We performed three steps to process the raw data [39, 44]:

We first converted text to vectorized features with Term Frequency-Inverse Document Frequency after the threads are converted into tokens and stemmed with Natural Language Toolkit [6]. Each thread is represented as a 108,741-dimension vector. We then applied 5-fold cross-validation, training on four folds and testing on one fold for five repeated times, and synthesized and computed the F1 score for all three classifiers. We evaluated six models: Support Vector Machine (SVM), Naive Bayesian, Logistic Regression, K-Nearest Neighbors, Multi-Layer Perceptron, and Random Forest. We chose SVM ultimately as it outperformed other models, having F1 scores of 0.88 for the CAaaS topic classifier and forum activity classifier and 0.90 for the CAaaS experience classifier, which are sufficient for cybercriminal ecosystem analysis, as defined by Bhalerao et al. [4].

Table 3 shows CAaaS topic statistics for the forums. Note that many users do not have any activity but reading after joining forums, so they are not classified into any category.

4.2 Targeted Merchants and Goods

To understand what targeted merchants are advertised, we used Standford NER [13] to tag "ORGANIZATION" tokens in the results labeled CAaaS Advertisements, and then manually reviewed all extracted organizations to remove mistagged ones. By comparing the merchants identified via such an approach with our manually extracted merchants from 200 randomly selected advertisements, the semi-automatic merchant extraction approach can identify 97.8% of targeted merchants. We identify 264 targeted merchants from all advertisements using this semi-automatic approach.

To determine the most popular merchants, we count each merchant's number of times was mentioned in a provider's advertisement. The results show that 1,031 out of the 2,251 service providers explicitly advertise merchants. Figure 2 shows the ten most targeted merchants explicitly advertised by the 1,031 service providers.

By manually analyzing 100 randomly selected providers who never mention merchants, we found that: (1) such service providers do not advertise targeted merchants but request to be contacted privately for details (e.g., *"if you are interested pm me"*), (2) they only mentioned the types of goods (e.g., *"items can consist of electronics and jewelry"*), and (3) they put the prior positive experience from other members in their advertisements and leave contact information.

Case Study. We analyzed a service list from a well-known scam service provider in the SENet forum as a case study. The provider has been active since 2017 and holds a top 1% reputation rating. The provider groups the targeted merchants into eight categories and lists Amazon as one dedicated category because of its popularity. For brevity, we show one category of the services in Table 4, and the full service list in Table 14 in Appendix D. Because there are 157 merchants in the original list, we list five of the highest *Limit* merchants in each category.

As shown in Table 4, we notice that the payment method impacts the service. Scam providers are more confident in working on high-value orders paid by PayPal than by credit or debit cards because of the higher *Limit*, although refunding PayPal orders takes a longer time. Buyer protections offered by third-party payment processors may provide scammers additional avenues for getting refunds. Also, according to one of the companies we collaborated with, some merchants do not actively engage in investigations or disputes from third parties, enabling scam providers to bypass merchants when getting refunds.

Each provider's service list reflects their experience in scamming different merchants, so the *Limit, Items, Region* and *Average Time* can vary between providers. For example, the scam service provider of Table 14 can work on Walmart orders with multiple goods and a $30,000 price limit, but another scam service provider can only refund one item in an order from Walmart with a $600 limit. Note that providers also offer to scam merchants that are not in their service lists.

Targeted Goods. From a service provider's perspective, as shown in Table 14, the provider cares more about the store, payment methods, order value, region, and the number of items than the goods themselves. From a scam initiator's perspective, they either want a refund for orders in compromised accounts (in which case they cannot arbitrarily choose the good), or they use their account and will accept any high-value good. Therefore, scam initiators do not have particular targeted goods; instead, they accept all kinds of goods, from high-value electronics to clothes, food credits, or even baby products (e.g., *"lots*

Table 4: Partial concession abuse service list for a top service provider.

Store Category	Payment Method	Store	Limit ($/€)	Items	Pay Rate (%)	Region	Avg Time
Clothing	Credit/Debit Card	Abercrombie & Fitch	No Limit	Multiple	25%	Worldwide	1 Day
		Macys	No Limit	One	25%	USA	1 Day
		Hollister	No Limit	Multiple	25%	Worldwide	1 Day
		Zappos incl Luxury	30,000	Multiple	25%	USA	1 Day
		Armani	3,000	Multiple	25%	Worldwide	10 Day
	PayPal	Stone Island	No Limit	Multiple	15 – 25%	Worldwide	2 – 3 Weeks
		StockX	No Limit	One	15 – 25%	Worldwide	2 – 3 Weeks
		YOOX	No Limit	Multiple	15 – 25%	Worldwide	2 – 3 Weeks
		Dolce Gabbana	No Limit	Multiple	15 – 25%	Worldwide	2 – 3 Weeks
		Mr Porter	No Limit	Multiple	15 – 25%	Worldwide	2 – 3 Weeks

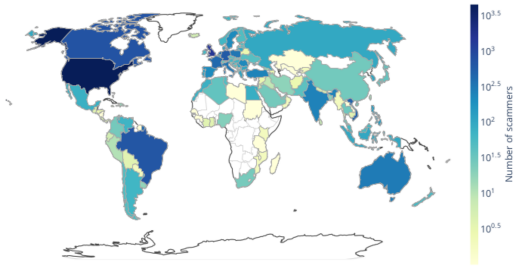

Figure 3: Geographical distribution of concession abuse scammers from the NULLED forum.

of free food (got a $150 store credit for Pizza Hut one time that was amazing) and free diapers when my kids were babies.").

4.3 CAaaS Service Fee

By studying a randomly selected set of 100 service providers from the four underground forums, we discover that service providers will either charge a percentage of the order value (i.e., the requested refund amount), or a minimum fee, whichever is greater. For example, the provider referenced by Table 4 will charge 15% to 25% or a $35 minimum. The fees primarily depend on the merchant, order price, and original payment method: *"Clothing Store PayPal Claims: 25% under $/€ 5,000, 20% under $/€ 7,000, and 15% above $/€ 7,000."*

Additionally, there is no significant difference in the fee percentage and minimum fees between service providers in our data. We conclude this by analyzing these randomly selected providers while considering three factors: (1) their *Reputation*, (2) the number of *Likes*, and (3) *Post Time* of first service advertising. *Reputation* and *Likes* are peer-rated indicators as social proof of a provider's trustworthiness and contribution to the underground forum, whereas the *Post Time* reveals the service starting time. Our results shows that regardless of the rank of providers' *Reputation*, *Likes*, or *Post Time*, each provider's minimum and maximum rates are nearly 15% and 30%, respectively. Also, their minimum fees vary between $30 and $50.

4.4 Geolocation of Scammers and Merchants

We extracted 15,450 IP addresses of members engaged in CAaaS threads from the NULLED database. Then, we used the *IP2Location* service [5], which is accurate at the country level [35], to determine the country of CAaaS scammers.

At the time of the study, we identify 1,674 (10.8%) anonymous IP addresses (e.g., VPN services, open proxies, Tor exits, hosting providers) by using the *IP2Proxy* database [25]. While there may be additional unknown proxies not identified by

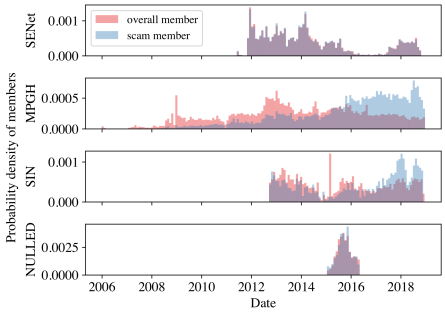

Figure 4: Trends in new scammer registrations and total forum members, monthly from 2006 to 2018.

IP2Proxy, using *IP2Proxy* can provide insights into scammers' geographical distribution by excluding popular and public anonymous IP addresses.

As shown in Figure 3, the remaining IP addresses are globally distributed, and the US, UK, and Canada are the top countries, accounting for 43.3% of these addresses. Also, most service providers (84.8%) are in Europe and North America, and only 11.7% of providers hide their IP addresses in underground forums using an anonymous IP address known to *IP2Proxy*.

Additionally, targeted merchants are distributed worldwide. Table 14 shows the service provider targets, which include merchants in Europe, Asia, and North America, such as YOOX, Lenovo, and Microsoft. Also, scammers target large merchants who have a presence in multiple countries, such as Amazon. In Table 14, the provider explicitly demonstrates his capability of scamming Amazon in seven countries. The provider can refund the highest value orders from Amazon US and take the shortest time from Amazon Netherlands.

4.5 Scam Scale

In this section, we studied the scale of the CAaaS community. We counted the number of newly registered scammers and overall members within a 30-day sliding window by the forum to compare their registration patterns. We used probability density to normalize the count and demonstrated the pattern differences of newly registered scammers and overall members, as shown in Figure 4.

In general underground forums, MPGH and SIN, where CAaaS is not the main content, the number of new CAaaS scammers has been increasing, but the number of new overall members has not increased significantly, and even declined since 2016. Because SENet is a forum primarily for CAaaS, the patterns of new scammers and overall members are very similar, showing an increasing trend since 2017. For

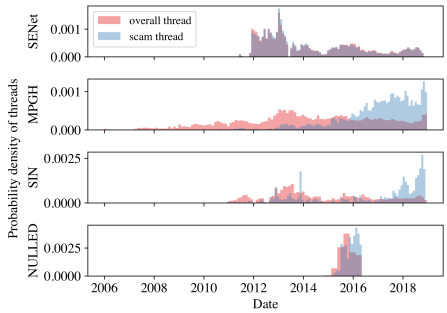

Figure 5: Trends in newly created scam threads and total threads, monthly from 2006 to 2018.

another general hacking forum, NULLED, we do not observe significant pattern differences. One possible reason could be that the data in NULLED is between 2015 and May 2016.

We also studied the activity of users discussing CAaaS in underground forums. We considered the number of newly created scam threads and overall threads in each forum (as opposed to the number of replies) because new threads are indicative of new instances not previously discussed. To compare the thread patterns effectively, we normalized the count and depicted the probability density of new scam threads and overall threads over time by forum in a 30-day sliding window, as shown in Figure 5.

We observe significant climbing trends of new scam threads in MPGH, SIN, and NULLED forums, while overall threads have stable or even decreasing trends. Although there is a slightly increasing trend since 2017 in the SENet forum, fewer threads were started compared with earlier. A possible explanation for these threads could be an active rumor within the underground communities, which states that the SENet forum was taken down by law enforcement, and it now is a trap for scammers.

4.6 From Novice to Seasoned Scammer

Based on our manual analysis of the four forums, we notice the significant amount of resources for novices helps them learn and become expert scammers within a short period of time.

Scam tutorials are widespread in underground forums. For example, Table 8 in Appendix B shows a scammer advertising about tutorials of the concession abuse scam, where customers can buy the core book plus any other selective tutorials from the scammer. These books can lower the learning curve and provide full-service guidance for scammers from learning scam tricks to running their scam services.

Scammers share their scamming experience to inspire and support other scammers as well. For example, one scammer shares that *"It was pretty easy, I ordered a laptop from DX and I contacted them I didn't got it so they sent a new one."*, and another group of scammers provide suggestions as shown in Figure 6.

To understand the difficulty of learning to perform concession abuse scams, we measured the time a novice needs to succeed in their first scam based on their post date

```
Support seeker: ... I've been trying to SE a google pixel xl 2
 ... both times everything went well until they asked for a proof
of purchase. ... I'm not exactly sure what I'm doing wrong ...
Support provider 1: Gift/Giveaway doesn't
work too well anymore for UK. I'm assuming you're trying UK.
Support provider 2: So get a POP and give them fake receipt
Support provider 3: Fake Amazon POP's work. If you want
to be safe you can crop out the order number so they can't verify it
```

Figure 6: Support received from experienced scammers.

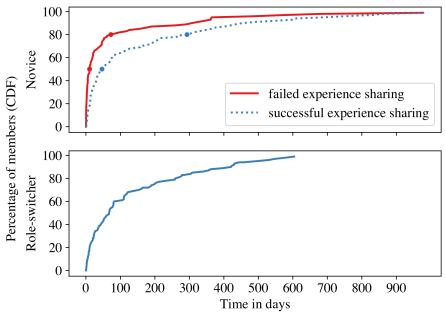

Figure 7: The growth of scammers over time while learning.

and joined date extracted from the raw HTML files. We first identified novices by finding the accounts that initiate a CAaaS-Discussion & Support thread (to seek help), do not provide any services. Then, we leveraged the scamming experience classifier 4.1 to find scammers who share both failed and successful scamming experience, and the first failed experience date should be earlier than the first successful experience date. Through this method, we identified 94 novice scammers that matched this description. Note that there are more novices in underground forums, and we only select those who share their scamming experience. To ensure these identified scammers are indeed novices, we manually analyzed all of their posts in the underground forums: the posts are either learning scam skills or asking for help. Moreover, none of them attempt sophisticated techniques such as starting a scam-related business, based on our manual analysis of their posts.

We then identified the amount of time it took them to post about their first failed scamming experience since joining the forum and their first successful scamming experience. The top figure ("Novice") in Figure 7 shows the growth of novice scammers over the time of their experience.

We find out that 50% and 80% of these novice scammers posted their first failure within 10.6 and 72.4 days, posted their first success within 46.7 days and 293.1 days, and took an average of 16.7 and 99 days to success after their first failures, respectively. Note that scammers may share their experience later than the actual date, and failed experience are more likely to be shared because they are looking for help from sophisticated scammers.

We also discovered instances in which scam initiators become directly entangled in the underground economy by evolving into service providers. We identified 116 scam initiators who begin with posting "CAaaS Purchase Request" and later become service providers, starting "CAaaS Advertisement" threads. The bottom figure ("Role-switcher") in Figure 7

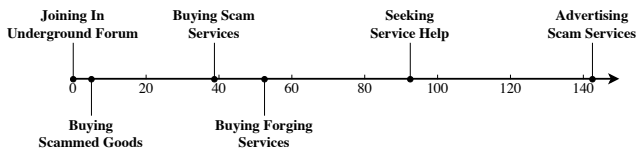

Figure 8: Timeline of the activities of a scammer who eventually switched roles and became a service provider.

shows the growth of these 116 scammers over time: 50% of such service buyers take 67 days to start their business after first buying scam services, and 80% of them take 259 days.

To understand these role-switchers, we present a case study of one concession abuse scammer's journey from a novice to an expert. Figure 8 depicts a timeline of this scammer's activities. The scammer made a request for scam-obtained goods six days after engaging in several scam discussions, and they attempted to hire a service provider 33 days later. Then, after learning about the scam, the scammer started to defraud merchants directly: As evidence, they attempted to buy a forged image and sought help for scamming 51 days and 93 days after joining the underground forum, respectively. Ultimately, they became a service provider 142 days after joining the forum.

4.7 Financial Loss

It is impractical to directly estimate the financial loss caused by CAaaS solely based on the posts in underground forums because: (1) scam initiators do not frequently vouch for service providers, (2) while some shared screenshots show the refund amount, many of them redact the amount, and (3) some screenshots of proofs are reused by multiple service providers in their advertisements.

However, we notice service providers prefer that scam initiators contact them through external messaging platforms (for privacy reasons), and 17.6% of providers manage groups on external platforms (such as Telegram) in which scammers can discuss concession abuse, making it possible to estimate the financial loss caused by individual service providers.

To this end, we joined the Telegram group of a well-known provider introduced in Section 4.2. We collected all public messages, pictures, and member profiles visible in this Telegram group.[3] Due to the popularity of CAaaS, the provider converted the group to a *supergroup* (maximum 100,000 members, from the default of 200) on November 16, 2019. We thus collected data from November 16, 2019 to February 28, 2020.

We found 1,076 members posted 17,898 messages within this period and noticed that the provider is the only service provider in the group. Members are only allowed to advertise their businesses or post links if approved by the provider: for example, certain vetted members offer cash-out services to monetize scam initiators' refunded e-gift cards. Therefore, all CAaaS related vouchers are for the provider's service.

Because the feedback from scam initiators often includes screenshots of refund confirmation, we collected all such screenshots in the group and extracted the text using OCR [27].

[3] Our observational study underwent the IRB review and received approval.

Table 5: The number of CAaaS scammers participating in other illicit activities (total CA actors: 49,720).

(a) Non-scam Activities

Content Category	Scammers	Ratio
Hacking	6,377	12.83%
Monetization	3,249	6.54%
Stolen Credential	12,827	25.80%

(b) Non-Concession Abuse Scams

Scam Type	Scammers	Ratio
Email Compromise	174	0.35%
Data Breach	150	0.30%
Denial of Service	253	0.51%
Phishing	67	0.14%
Ransomware	7	0.01%

We manually verified the results for merchant names. We identified 25 merchants from 227 screenshots, five of which were not listed in the provider's advertisements (see Table 14). Hence, the provider is able to defraud other merchants as requested by initiators.

85 of these screenshots contained refund amounts (the remainder were redacted or incomplete). The provider helped refund the equivalent of $81,159.27 ($41,076.71, € 17,130.4, and £7,393.29) over three months through scamming merchants in North America and Europe. Because not all screenshots had a refund amount, and not all scammers provide feedback, it is likely that the provider refunded a far higher amount.

Although we cannot definitively conclude the authenticity of all collected screenshots, we collaborated with two major (undisclosed) US merchants who confirmed several instances of successful scams. For example, one merchant confirmed that a $374.30 order was refunded to someone who claimed the goods were not delivered. The other confirmed that numerous high-value items were refunded, but would not provide specific details. This feedback from merchants, combined with the high level of activity in this scammer's Telegram group, allows us to conclude that CAaaS has a real financial impact on merchants.

4.8 Scammer Overlap

Next, we analyze the actions of CAaaS actors to see if they are involved in other cybercriminal activity (as evidenced by their observable actions on the underground forums in our dataset). As a recap for the analysis approach, we classified underground forum activities into Monetization, Hacking, Scam, and Other. We then further divided Scam into five primary types, based on the FBI Internet Fraud definition [11]. Finally, we label *all* the posts of CAaaS actors by these activities.

Table 5 shows the number and ratio of CAaaS actors in non-scam activities and in non-CAaaS scams. We observe a reasonable proportion of CA scammers involved in non-scam activities, specifically Hacking (12.83%) and Stolen Credential (25.80%). These activities are closely related to CAaaS: For example, CAaaS may require compromised online merchant accounts, so it is likely that CAaaS actors are involved in the stolen credential activity.

However, few CAaaS actors are involved in other types of scams. This may be because concession abuse shares little in common with other scams and requires a different skillset.

5 The Success and Failure of CAaaS

In this section, we study the tricks that CAaaS scammers use to succeed and as well as cases in which they fail. To perform our analysis, we first leveraged the classifier that labels the successful and failed scam experience (§ 4.1) to randomly select 1,000 threads with each respective label. Then, we manually analyzed these threads and aggregated the various tricks and causes of success or failure. We include representative scammer quotes throughout this section.

5.1 Preparing for the Scam

Choosing merchants to target. CAaaS service providers typically prefer large merchants because they have robust customer service departments and are more willing to risk a financial loss in exchange for customer satisfaction. Such merchants are, therefore, more prone to being tricked into providing concessions; one scammer's advice was to *"just refund big companies, not small shops that can't afford the loss."* Moreover, many service providers caution *"DO NOT refund small businesses and individuals (such as on eBay)."*

Choosing accounts. Service providers prefer to carry out their scams using shopping accounts with a long order history and few refund or return claims, because such accounts closely resemble those of loyal customers. Sellers of compromised accounts emphasize these characteristics in their advertisements in underground forums: *"this is a great account to do the Amazon refund with, because it has a such a good history with no disputes or anything."*

Choosing orders. Because refund requests for recent orders appear routine to CSRs, such requests avoid unnecessary scrutiny and scammers, therefore, actively seek compromised accounts with recent orders: *"I'm willing to pay for cracked amazon accounts with good recent orders yo hit me up."* Additionally, high-value orders are less desirable as they may trigger extra investigations. Therefore, many service providers set an order value limit for each merchant (see § 4.2).

5.2 Tricks During Scam Execution

5.2.1 Contact Method

There are three typical ways to contact a CSR: phone, live chat, or e-mail. Scammers prefer phone calls for two reasons: First, a phone call gives a CSR much less time to respond and, thus, decreases the chance that a CSR will sense unusual behavior. Second, speaking enables a service provider to effectively use social engineering to manipulate the conversation, through which the provider can influence a CSR's decision, or even *"lead the CSR into asking the questions the scammer wants."*

5.2.2 Deception Strategies

Expressing pity and urgency. Service providers fabricate stereotypical stories to evoke feelings of pity and urgency to influence CSRs' decisions. For example, a service provider could request a refund for *"an undelivered gift that was for her sick son's birthday."* Such a story attempts to make a CSR sympathetic with the goal of convincing the CSR to approve an immediate refund.

Being polite. CAaaS service providers usually behave politely when interacting with CSRs. They call CSRs by their names, express understanding of the mistakes, and show appreciation for their help: *"Fear or threats are* not *recommended for scamming"*, as a tutorial says *"Be somewhat charismatic and do not have an attitude with the reps."*

Expoliting legal regulations. Service providers may cite legal regulations to avoid returning the merchandise. For example, a CAaaS service provider may complain about a battery leakage in a purchased laptop and state that he cannot return it due to the *49 CFR 173.185* U.S. Lithium Battery Regulation. The service provider might also first agree to return the merchandise, and later state that they cannot do so because the shipping carrier rejected the shipment. If successful, the provider will receive a concession without returning the goods.

Exploiting incomplete communication between CSRs. Some CAaaS service providers call a merchant multiple times and lie to the latter CSR about an agreement with the previous CSR. For example, a scammer states in a tutorial that if they make two calls a few minutes apart, they are usually connected to a different CSR in the second call. They then lie to the second CSR that the previous call was dropped while the first CSR was processing the refund. In this way, they may receive a concession from the second CSR without needing to provide any concrete justification.

5.2.3 Reasons for Requesting a Refund

Package never delivered. Failure of a package to arrive is the most common fictitious claim used by scammers in concession abuse. Scammers usually contact the CSR a few days after the package is actually delivered, because some online merchants, such as Amazon, require the customer to contact 24 hours after delivery to open a claim. During the conversation, they follow the instructions of the CSR to build rapport and trust. For example, CSRs may ask if the scammer can ask their family members and neighbors or check both front and back doors. Scammers respond: *"Yeah, I asked my parents, they didn't see it. But I haven't checked with my neighbors. Can you wait a minute and I can ask them."* Then a few minutes later, they tell the CSRs that the neighbors do not see it.

Empty box. Claiming an empty box is a popular and straightforward pretext to request a concession: *"I opened my package, there was nothing in it but some packaging paper, styrofoam and my invoice."* When CSRs receive such complaints in the absence of other risk factors, they have to issue the concession unless records show that the mailed package is obviously

heavier than an empty box. Therefore, as long as the goods are not significantly bulky, these claims can be effective.

Missing item. Scammers may buy multiple goods in one order and lie that some items are missing. For example, one scammer shared, *"I ordered keyboard and mouse mat, then contacted amazon live chat. Said they were birthday gifts and only received the mouse mat, so I was given a refund for the keyboard."*

Wrong items. A service provider may claim that they were sent the wrong item, which is of similar weight but lesser value compared to the ordered item. If a return is requested, they will mail back a cheaper alternative and keep the actual item, as a scammer says *"I ordered a ralph lauren polo on zalando. Received the item, and returned an old polo and pretend I got the wrong item."*

Broken items. A service provider may claim that they received a broken item. For example, they may deliberately buy a specific item together with liquid goods and claim that the item was damaged due to a leak and cannot be returned: *"I received the box and it was leaking everywhere with this profusely smelling liquid and it looked like some of it had dried. It was doing this when you guys shipped it and I threw it immediately out to make sure my family didn't get hurt by this."*

5.2.4 Dealing with Return Requests

Standard shipping. This is the return policy adopted by most merchants, including Amazon. Per this policy, the merchant issues the concession only after receiving the return. If the targeted merchant uses this policy, the CAaaS service provider will send an empty box back and claim the returned item was stolen in shipment. In fact, many merchants will immediately issue the concession once the warehouse scans the box. Because shipping carriers typically measure the weight and size of the box, criminals often add junk totaling the same weight as the original item. Scammers may also deliberately seal the box poorly to help convince merchants that the box was opened in transit. The preparation of empty return shipments can be outsourced to *Boxing Service Agents*: criminals who specialize in such services.

Cross-shipping. Per this policy, merchants send out replacements once they see that the prepaid shipping label for the return is scanned by the carrier. Criminals adopt similar approaches to standard shipping, and the boxing service is widely used. Because criminals do not need to explain the empty box before receiving the concession, reshipping agents or drops are frequently employed to shield the scammer.

Advance replacement. Some companies have a policy under which they ship replacement products before the return shipping label is scanned, as long as their customers provide valid credit card information. In this case, the scammer will provide a Virtual Credit Card (VCC) purchased from VCC agents. One scammer advised: *"you will need a VCC with a dollar or two on it. Once the company you're SEing has your VCC, they will usually charge you the amount of the item once they ship it out. "*

5.3 Monetization Tactics

Scammers who use compromised accounts prefer refunds via e-gift cards over the original payment method because e-gift cards enable them to cash out. Additionally, if a scammer employs a reselling agent (§ 3.4) to monetize the refund, they would buy goods that can be shipped quickly. For example, the scammer will buy goods sold by (or at least fulfilled by) Amazon and select the fastest shipping option to minimize potential delays. Therefore, even if merchants notice the scam later and flag the e-gift card, scammers will have already spent the balance and monetized the refund.

To improve safety and convenience, many scam initiators leverage Bitcoin shopping websites (such *Purse.io*, which is frequently discussed by scammers in underground forums) to monetize their refunds without wasting time on advertising and sharing profits with individual resellers. Such a strategy work as follows: (1) a user posts a shopping list on the website, along with a discounted price they are willing to pay; (2) if the refund is similar to the cost of the shopping list, and the discounted price is acceptable, then the scam initiator will accept the order; (3) the user sends the discounted amount in Bitcoin to the website, and then the scam initiator starts to purchase the products and make the merchants ship them to the user; and (4) after the package is delivered, the website will release the Bitcoin to the scam initiator. In this way, scam initiators safely exchange their e-gift card balance to Bitcoin.

5.4 Failure Causes

Investigations. The most-discussed failure cases involve investigations by reshipping agents and merchants: (1) Legal reshipping companies that are abused by scammers may verify the receiver's identity and confirm the goods received with suppliers when there is a high volume of packages sent to the same account. Also, such reshipping agents may contact merchants to verify if these goods can be shipped internationally if the reshipping address is not domestic.

(2) Merchants investigate cases of fraud using internal systems and external parties, such as shipping carriers. For example, a merchant could use *"geocode timestamp, information at the point of delivery, and package weight and condition"* to validate if the package is delivered.

Value of goods. High-value goods are more likely to trigger investigations, which is why service providers explicitly list price limits in their advertisements. If the goods are too valuable, a scammer may fail because of an automatic investigation.

Account activity. Unusual activity on the merchant accounts may attract scrutiny and subsequent investigation. Therefore, scammers seek to ensure that such accounts have a clear history of legitimate activity. We observed failures for three main reasons: (1) scammers attempt to use accounts having concession abuse claims, (2) scammers use an account linked to other accounts which were closed for abuse, and (3) account owners notice unusual account activity and report it.

Proof. Insufficient or unconvincing documentation is another key cause of failed scams. There are two types of failures related to proof: (1) scammers cannot provide the requested proof, which may happen if the CSR requests a video or other type of evidence that is difficult to forge (scammers also try to avoid interaction with law enforcement, so they prefer not to provide police reports), and (2) certain forged evidence fails a verification check. For example, scammers may make mistakes when forging documents; also, they may reuse certain types of proof, such as order receipt templates. Moreover, merchants may verify proof with other parties, which could disrupt scammers.

Delivery. Scammers prefer to avoid risks, and some have therefore reported failures if they are asked to reveal their real identities or be seen in-person to receive the goods (i.e., when a signature or local post office pickup is needed).

Returning goods. Although scammers have tricks to avoid returning goods to merchants even though a return is required, they sometimes fail because either their return packages are inspected, or they would be forced to reveal their identities. For example, some merchants may either request that goods be returned to a local store, or they may send someone to pick them up, causing the scam to fail because the goods could then be inspected and the scammers would need to show their faces.

6 CAaaS Mitigation

We understand that merchants deploy numerous operational protocols to mitigate scams (e.g., issuing a refund only after receiving the returned goods and launching investigations when needed). However, concession abuse scammers seek to discover loopholes in these mitigations and work to bypass them. For example, Amazon was scammed out of €300,000 by a single person [14] who returned dirt multiple times; the scam likely succeeded due to the lack of inspection of returned goods or detection of compromised accounts, despite the fact that Amazon issues refunds only after receiving the returned goods.

6.1 Analysis Approach

We synthesize key merchant and ecosystem weaknesses that scammers abuse and propose possible mitigation solutions that address these weaknesses. We define criteria that determine the suitability of each mitigation, though we cannot effectively evaluate suitability without merchant data. We divide mitigations into thee different areas: Account Abuse Detection Principles (AADP), CSR Operational Protocols (CSR-OP), and Merchant Operational Protocols (MER-OP).

We then interviewed two large merchants to discuss the proposed mitigations. Although they confirmed to suffer from concession abuse scams, one merchant voiced concerns about *"an easy customer experience for legitimate customers."* Therefore, we also conducted a survey to more thoroughly evaluate defense solutions that could affect a customer's shopping experience. Our survey consisted of two general sections and six scenario-based sections that aimed to gauge user attitudes toward such mitigations in practice. Although participants' attitudes in the survey and real-world behavior or preferences might differ, the results can still reveal their concerns and comfort levels with the proposed mitigations.

Table 6: Overview of participants' attitudes toward our security protocols.

Security Protocol	Non-negative Attitude	Willingness to Continue Shopping
Investigation | CRS-OP (2)	93.2%	90.2%
Providing Proof | CRS-OP (3)	75.4%	68.6%
ID Verification | CRS-OP (5)	94.9%	93.6%
Local Return | MER-OP (3)	80.1%	86.0%
Separate Shipping | MER-OP (4)	94.5%	93.6%
PIN for E-gift Card | MER-OP (5)	92.8%	92.4%
Secondary Contact | MER-OP (6)	86.9%	87.7%

Table 6 shows an overview of the participants' attitudes towards our security protocols. The "Non-negative Attitude" column shows the percentage of participants who neither *mind* nor *strongly mind* the security protocol. Both studies (merchant interviews and user surveys) received approval from our IRB.

6.2 Account Abuse Detection Principles

Because criminals commonly leverage CAaaS to profit from compromised accounts, proactively detecting compromised accounts can prevent concession abuse at an early stage, potentially well before merchants are contacted by scammers. Furthermore, identifying accounts being accessed by scammers can help mitigate the damage caused by CAaaS.

Although general account fraud protection systems have been developed [7], such systems may not effectively prevent concession abuse on their own.

Therefore, we propose additional Account Abuse Detection Principles (AADP) to enhance such systems to protect against concession abuse scams.

AADP (1): Compromised account alerts. Scams involving compromised accounts may fail if the actual owner of the account is notified in a timely manner. Therefore, proactive monitoring and securing accounts sold in underground communities or in known data breaches can help prevent subsequent fraud [43].

AADP (2): Account history. Per our failure case analysis (Section 5.4), the use of accounts with abnormal historical activity is one of the primary reasons that a scam attempt might fail. Hence, the frequency of refund requests, especially for non-returnable claims, the dates of recent requests, and the number of attempts to refund the same order can determine the riskiness of an individual account. Moreover, if a compromised account is used in a scam, then it is difficult for attackers to ensure that the account has a very recent order (e.g., there is an average 7-day delay between credentials being phished and appearing in dumps [32]), so the date of the placed order can be a notable risk factor.

AADP (3): Account age. When unable to obtain compromised accounts, scammers may use newly created accounts to avoid placing their main accounts at risk while defrauding merchants. Therefore, a concession request from a new account with a short order history should be considered for investigation.

Furthermore, if a fresh account is linked to an account closed due to a scam, merchants should flag this new account and treat its concession claims as suspicious because they are likely tied to the same attacker.

AADP (4): Customer authentication. Our analysis of chat logs in underground forums suggests that most answers to CSRs' questions can be found in the corresponding account profiles, such as verifying the customer's address. Therefore, technical authentication schemes can be used to mitigate attackers' use of compromised accounts, such as two-factor authentication for accessing account profile data or comparing the IP address and location of the user accessing the data with those of the accountholder.

AADP (5): E-gift card abuse detection. Detecting e-gift card abuse is another approach for finding compromised accounts that are being monetized via CAaaS. For example, if the time between the refund deposit into the e-gift card and the spending of the balance is short, and the purchased goods are shipped to a new address (especially to a known reshipping agent), then it is more likely that the account has been exploited by scammers.

6.3 CSR Operational Protocol

Deceiving CSRs into believing the pretexts is an essential step to successfully defrauding the merchant through concession abuse. To protect CSRs and mitigate such scams, we propose additional CSR Operational Protocols (CSR-OP). Implementing some protocols (CSR-OP 2, 3, and 5) may influence customers' shopping experience, so we surveyed users and show their feedback in Table 6.

CSR-OP (1): Maintain clear customer service logs. Maintaining clear and complete customer service logs will help representatives better understand each request and more effectively synthesize any relevant historical context. In particular, the log should include any prior decisions made by other CSRs to avoid attackers' exploitation of gaps in information between CSRs, as discussed in Section 5.2.2.

CSR-OP (2): Investigations for high-value goods. CSRs should initiate investigations when customers request a concession without returning goods above a certain value threshold. This will help mitigate the loss of high-value items.

CSR-OP (3): Extra proof when original goods not returned. Merchants should require customers to provide extra proof if they are not going to return the original goods. Because scammers routinely forge proof, merchants should require proof that is difficult to forge, such as a video of the product with a handwritten reference number (which is currently known to be difficult to forge, as discussed in Section 5.4). Additionally, scammers wish to avoid law enforcement involvement, so requesting a police report can stop some scammers using the *"package not delivered"* pretext.

According to our user survey, this protocol had the most negative attitudes because participants think providing extra proof is inconvenient and that their moral character is being questioned. In general, 24.6% of participants either *mind* or *strongly mind* providing proof. However, we notice that if the proof does not require excessive effort, then 25.9% of participants who mind providing proof would still be willing to provide it for valuable goods.

CSR-OP (4): Verification of proof. Merchants need to adequately verify the proof provided by the customer before issuing the requested refund or replacement. To balance the cost of the required information and inconvenience upon potentially innocent customers, merchants can use automatic verification first, which is fast yet might be less precise than a comprehensive manual verification. For example, if a customer provides a police report to claim a refund, then two possible automatic verification processes could be: (1) verifying that the same proof does not already exist in the merchant's database (because scammers often reuse proof shared in underground forums, discussed in Section 5.4), and (2) using image analysis techniques to check if the metadata of the photo matches the customer's profile, such as the city, and whether the photo was edited or otherwise tampered with. If any red flags are raised by the automated system, then a manual analysis could be performed, such as contacting the police station to verify the authenticity of a police report or asking the customer for additional evidence.

CSR-OP (5): Limiting changes to shipping address. CSRs should not change the shipping address for replacement items unless the new address is confirmed by accountholders through two-factor authentication. Verifying the identity of the customer is important because scammers frequently try to send items to reshipping agents or drops.

The primary concern about this protocol is that it is a time-wasting inconvenience. However, most survey participants expressed a willingness to use this protocol to secure their accounts.

6.4 Merchant Operation Protocol

To have comprehensive mitigations, we design a Merchant Operation Protocol (MER-OP) that can be used by merchants to help CSRs avoid being deceived. The MER-OP is designed to apply to general merchant operations, instead of a specific customer or request, as in the case of CSR-OP. We show participants' corresponding attitudes (MER-OP 3, 4, 5, 6) in Table 6.

MER-OP (1): Intelligence support for CSRs. Merchants should provide a dashboard of the caller and accountholder information side-by-side. In the meantime, a risk score indicating possible account abuse should be shown to help CSRs verify the authenticity of the caller. Moreover, CSRs operational protocols and other scam detection tools, such as image analysis tools, should be available in the dashboard. Also, the prior chat records of the same order should be shown to help CSRs have a comprehensive understanding of the claim. Therefore, this protocol also supports our AADP and CSR-OP recommendations.

MER-OP (2): Taking pictures during packaging. Taking pictures of the goods placed in the box during packaging is a straightforward yet effective approach for mitigating malicious

Missing item, *Wrong item*, and *Empty box* refund claims. Such evidence would significantly reduce the believability of such claims compared to what is possible based solely on knowing the weight of the package, as discussed in Section 5.4.

MER-OP (3): Local returns for special items. Merchants can supplement online returns with an offline return policy to avoid return tactics used by scammers for high-value goods. In offline returns (i.e., processed in-person at the merchant's store or with a partner retailer), goods can be directly inspected, and the accountholder's identity can be verified.

19.9% of participants either mind or strongly mind offline returns due to inconvenience (e.g., *"I am in a rural area and would have to drive a long ways."*) Upon deeper analysis, these participants may have misunderstood that they must return goods to merchants' local stores. Customers could bring the goods to a shipping carrier and let the staff there pack them (e.g., one participant said *"I already bring the item to UPS store when I return something, so there's no difference."*). Hence, we believe that the implementation of selective offline returns remains feasible.

MER-OP (4): Separating shipments of high-value goods. Placing high-value goods in separate packages, especially when multiple expensive items are included in a single order, helps defend against tactics such as *Missing items*, *Empty box*, and *Broken items*, as discussed in Section 5.2.3.

Merchants should consider participants' concerns, however, such as wasting packaging materials or increasing overall shipping costs.

MER-OP (5): Extra checks for e-gift card refunds. Merchants should ask customers to use enhanced authentication (e.g., a PIN) for their e-gift card payments to counter scammers' monetization methods discussed in Section 5.3.

Some participants said they would be annoyed if they had to remember more than one password, though most were satisfied with this protocol to secure their gift cards.

MER-OP (6): Securing contact information. Customers' contact information, such as email addresses and phone numbers, should be hidden in the system and differentiated from their publicly disclosed information to ensure accountholders can receive notifications about account activity even if the accounts are breached by attackers. Alternatively, customers could provide a secondary email address or phone number for such notifications, which would be different from the email or username used to log in.

According to the survey, some participants do not want to provide a secondary notification contact because they neither have a secondary email address nor want to share their private email addresses. However, 81.8% of participants had a secondary email address that they could use as a secondary notification contact.

MER-OP (7): Collaboration with payment processors. Merchants should positively engage in any investigations or disputes from third parties, because scammers may attempt to bypass merchants' own anti-fraud systems by filing a fraudulent claim with a payment processor to get their refund or replacement. If ignored, such requests could also damage the merchants' reputation.

6.5 Survey of Customers' Attitudes to Proposed Defenses

To better understand the inconvenience that shoppers might experience from the aforementioned security measures, we surveyed users' attitudes and concerns using Amazon Mechanical Turk (MTurk) [24, 34].

Design. We categorized the defense schemes that involve customers and designed a survey with eight sections. In the first two survey sections, we collect: 1) participants' demographic information, and 2) general security experience related to online shopping. Six sections follow, each corresponding to a scenario with mitigations against concession abuse: 1) investigations and requests for proof following a claim, 2) identity verification for changing the shipping address, 3) local store returns for high-value goods, 4) separate shipments for high-value goods, 5) payment PIN for e-gift cards, and 6) secondary contact information for security notifications. The six scenario-based survey questions can be found in Table 13 in Appendix C. We measured user attitudes on five-point Likert scale ranging from *strongly not mind* (the user approves of the mitigation) to *strongly mind* (the user does not).

Participants. To obtain reliable survey data, we must recruit an appropriate set of participants. To this end, we conducted two pilot surveys: the first pilot was open to any MTurk worker from North America with at least 1,000 approved HITs, or a HIT approval rate higher than 95%, which indicates attentive participation [34]. The second pilot was open to Master Workers from North America (users recognized by Amazon for the reliability of their work) [16].

To analyze the response quality, we compare the participants' attitudes toward our security protocols with their short answers explaining their reasons. We found that Master Workers performed better than workers screened by approved HITs or HIT approval rates because 60% of responses in the first pilot were illogical or appeared rushed. For example, some participants in the first pilot indicated that they strongly minded one protocol while explaining that they did not mind in the short answer. We, therefore, recruited only Master Workers from North America in our main survey and paid $1 for participation.

In total, 247 workers participated in our survey. After removing low-quality responses and duplicate participants, we were left with the 236 responses upon which we based our analysis.

Results. The detailed survey results can be found in Appendix C. Table 9 and Table 10 show the demographics and the general security experience of our participants, respectively. Table 12 summarizes participants' attitudes toward the security protocols. In Table 11, we show representative short answers to highlight participants' key concerns about different scam prevention approaches.

7 Limitations

Because CAaaS is an emerging attack technique and an underground service industry, it is challenging to study. This section discusses these challenges and encourages future researchers to investigate these aspects of the underground economy.

Ground truth from merchants. In our conversations with merchants, we found that they are reluctant to share ground truth data about attacks that they experienced or to closely collaborate on the development and evaluation of preventative mitigations. Thus, we based our study on crawled and leaked data from underground forums, relying on strategies, successes, and failures self-reported by cybercriminals in communications with each other.

Of course, there is no guarantee of the veracity of such information or the real-world effectiveness of our suggested intervention protocols. However, we provide the first look into the supply chain of CAaaS. Additionally, we acknowledge that participants' attitudes in the survey and real-world preferences might differ, which can be further studied in the future.

Ground truth from cybercriminals. Cybercriminals are, understandably, a secretive group, which increases the difficulty in studying their activity. Our forum data is an approximation of the behavior of cybercriminals, and its veracity is impossible to quantify. While we could add additional underground forums to our dataset (anecdotally, recent observation of underground forums revealed an increase in sub-forums dedicated specifically to concession abuse), the data on which we base this paper presents a clear picture of the structure and impact of CAaaS.

We cannot be certain in our estimate of the difficulty of learning how to perform concession abuse scams. Because our time interval analysis is based on scammers' post timestamps, and scammers may not immediately (or always) share their experiences, we can only make estimates of these intervals.

Similarly, without ground truth from retailers, it is impossible to verify the actual financial loss caused by the scam. We hope that as CAaaS continues to impact merchants financially, they will evaluate and implement potential mitigations.

8 Related Work

Underground forum analysis. Underground forums are used as rendezvous locations for cybercriminals who want to exchange information and sell illicit products and services [48]. Our research builds on several techniques used in prior work, including studies of the economics of cybercrime based on criminals' discussions in underground forums [9, 10] and studies that analyze forum user structure and interactions [1, 26]. Motoyama et al. evaluated how inherent distrust among criminals in underground communities affects their mutual interactions [28]. Afroz et al. tried to identify anonymous forum posters by analyzing their writing styles [2]. Also, Zhao et al. proposed an approach for mining evidence in underground forums to expose the social dynamics among adversaries involved in Internet-based attacks [47].

Specific cybercrime services in underground forums were also studied. Hao et al. studied reshipping services, which were found to contribute as much as $1.8 billion to overall reshipping scam revenue [15]. Researchers have analyzed phishing kits and services in underground forums [30, 31, 36, 46] to reveal phishing service costs, operational steps, actors, and reasons for profitability. Karami et al. analyzed DDoS-as-Service in underground forums to show the internal operations, usage patterns, and attack infrastructure [21, 22].

Social engineering. Scammers use social engineering tactics to manipulate victims into sharing confidential information or performing specific actions. Atkins et al. and Ferreira et al. studied the persuasion techniques used in social engineering [3, 12]. By analyzing 74 scenarios, Bullée et al. showed which persuasion principles are most effective for social engineering attacks [8]. Irani et al. studied reverse social engineering attacks that deceived people to visit malicious websites by abusing social networks, without the need for direct contact with victims [18]. Researchers also conducted studies of web-based social engineering attacks that trick users into downloading malicious software [20, 29].

9 Conclusion

In this paper, we identify and describe CAaaS, an emerging scam threat fueled by the underground economy. Through manual and automated analysis of crawled and leaked data from four underground forums, we describe different types of actors involved in CAaaS, the anatomy of the scam and service itself, tricks used to increase the likelihood of success, and the potential victims (as advertised by actual scammers themselves). Our analysis shows that CAaaS impacts numerous online merchants globally and is becoming more prevalent in underground forums. Moreover, given the wealth of resources and services available in these forums, 50% of novices learn how to successfully defraud merchants within 47 days or less.

Additionally, we analyzed attackers' tactics and failure cases to identify potential limitations, and we proposed several defenses—which could be adopted directly by merchants and payment processors—to detect and mitigate instances of this scam. Moreover, we surveyed users to evaluate their attitudes and understand their concerns toward the proposed mitigations.

Acknowledgments

We thank our shepherd, Paul Pearce, and the anonymous reviewers for their helpful suggestions. We also thank the two industry organizations for their valuable insights and collaboration. This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2017-0-00168, Automatic Deep Malware Analysis Technology for Cyber Threat Intelligence), and by the NSF grant NSF-2000792.

References

[1] S. Afroz, V. Garg, D. McCoy, and R. Greenstadt. Honor among thieves: A common's analysis of cybercrime economies. In *eCrime Researchers Summit (eCRS)*, 2013.

[2] S. Afroz, A. C. Islam, A. Stolerman, R. Greenstadt, and D. McCoy. Doppelgänger finder: Taking stylometry to the underground. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2014.

[3] B. Atkins and W. Huang. A study of social engineering in online frauds. *Open Journal of Social Sciences*, 1(03):23, 2013.

[4] R. Bhalerao, M. Aliapoulios, I. Shumailov, S. Afroz, D. McCoy, K. Levchenko, and V. Paxson. Mapping the underground: Towards automatic discovery of cybercrime supply chains. *arXiv preprint arXiv:1812.00381*, 2018.

[5] H. D. S. Bhd. Identify geographical location by ip address.

[6] S. Bird, E. Klein, and E. Loper. *Natural language processing with Python: analyzing text with the natural language toolkit*. " O'Reilly Media, Inc.", 2009.

[7] M. W. Brown, J. H. McIntyre, M. A. Paolini, J. M. Weaver, and S. L. Winters. Providing account usage fraud protection, Dec. 12 2006. US Patent 7,149,296.

[8] J.-W. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. Hartel. On the anatomy of social engineering attacks: A literature-based dissection of successful attacks. *Journal of investigative psychology and offender profiling*, 15(1):20–45, 2018.

[9] N. Christin. Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the International World Wide Web Conference (WWW)*, 2013.

[10] G. Durrett, J. K. Kummerfeld, T. Berg-Kirkpatrick, R. S. Portnoff, S. Afroz, D. McCoy, K. Levchenko, and V. Paxson. Identifying products in online cybercrime marketplaces: A dataset for fine-grained domain adaptation. *arXiv preprint arXiv:1708.09609*, 2017.

[11] FBI. Internet fraud.

[12] A. Ferreira, L. Coventry, and G. Lenzini. Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 36–47. Springer, 2015.

[13] J. R. Finkel, T. Grenager, and C. Manning. Incorporating non-local information into information extraction systems by gibbs sampling. In *Proceedings of Association for Computational Linguistics (ACL)*, 2005.

[14] I. V. Hagen. 22-year-old allegedly scammed amazon out of $370k with return shipments filled with dirt, Aug. 2019.

[15] S. Hao, K. Borgolte, N. Nikiforakis, G. Stringhini, M. Egele, M. Eubanks, B. Krebs, and G. Vigna. Drops for stuff: An analysis of reshipping mule scams. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2015.

[16] M. Harbach, S. Fahl, and M. Smith. Who's afraid of which bad wolf? a survey of it security risk awareness. In *Proceedings of the IEEE Computer Security Foundations Symposium (CSF)*, 2014.

[17] A. Hutchings and T. J. Holt. A crime script analysis of the online stolen data market. *British Journal of Criminology*, 2015.

[18] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu. Reverse social engineering attacks in online social networks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 55–74. Springer, 2011.

[19] P. A. Jankowski and C.-L. Yen. Return fraud protection system, Jan. 27 2015. US Patent 8,942,990.

[20] M. Junger, L. Montoya, and F.-J. Overink. Priming and warnings are not effective to prevent social engineering attacks. *Computers in human behavior*, 66:75–87, 2017.

[21] M. Karami and D. McCoy. Understanding the emerging threat of ddos-as-a-service. In *Presented as part of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats*, 2013.

[22] M. Karami, Y. Park, and D. McCoy. Stress testing the booters: Understanding and undermining the business of ddos services. In *Proceedings of the International World Wide Web Conference (WWW)*, 2016.

[23] B. J. Kwon, J. Mondal, J. Jang, L. Bilge, and T. Dumitraş. The dropper effect: Insights into malware distribution with downloader graph analytics. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2015.

[24] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, and L. F. Cranor. Fast, lean, and accurate: Modeling password guessability using neural networks. In *Proceedings of the USENIX Security Symposium (USENIX)*, 2016.

[25] X. Mi, X. Feng, X. Liao, B. Liu, X. Wang, F. Qian, Z. Li, S. Alrwais, L. Sun, and Y. Liu. Resident evil: Understanding residential ip proxy as a dark service. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2019.

[26] A. Modi, Z. Sun, A. Panwar, T. Khairnar, Z. Zhao, A. Doupé, G.-J. Ahn, and P. Black. Towards automated threat intelligence fusion. In *Proceedings of the IEEE International Conference on Collaboration and Internet Computing (CIC)*, 2016.

[27] S. Mori, H. Nishida, and H. Yamada. *Optical character recognition*. John Wiley & Sons, Inc., 1999.

[28] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker. An analysis of underground forums. In *Proceedings of the ACM SIGCOMM Conference on Internet Measurement (IMC)*, 2011.

[29] T. Nelms, R. Perdisci, M. Antonakakis, and M. Ahamad. Towards measuring and mitigating social engineering software download attacks. In *USENIX Security Symposium*, pages 773–789, 2016.

[30] A. Oest. Leveraging scalable data analysis to proactively bolster the anti-phishing ecosystem. *Arizona State University*, 2020.

[31] A. Oest, Y. Safaei, A. Doupé, G.-J. Ahn, B. Wardman, and K. Tyers. Phishfarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2019.

[32] A. Oest, P. Zhang, B. Wardman, E. Nunes, J. Burgis, A. Zand, K. Thomas, A. Doupé, and G.-J. Ahn. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *Proceedings of the USENIX Security Symposium (USENIX)*, 2020.

[33] C. Osborne. Nulled.io hacking forum data breach exposes attackers in the shadows, May 2016.

[34] A. C. Plane, E. M. Redmiles, M. L. Mazurek, and M. C. Tschantz. Exploring user perceptions of discrimination in online targeted advertising. In *Proceedings of the USENIX Security Symposium (USENIX)*, 2017.

[35] I. Poese, S. Uhlig, M. A. Kaafar, B. Donnet, and B. Gueye. Ip geolocation databases: Unreliable? *ACM SIGCOMM Computer Communication Review*, 2011.

[36] A. K. Sood and R. J. Enbody. Crimeware-as-a-service: a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, 2013.

[37] D. Speights and M. Hilinski. Return fraud and abuse: How to protect profits. *Retailing Issues Letter*, 17(1):1–6, 2005.

[38] G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Y. Zhao. Follow the green: growth and dynamics in twitter follower markets. In *Proceedings of the ACM SIGCOMM Conference on Internet Measurement (IMC)*, 2013.

[39] A. Sun, E.-P. Lim, and Y. Liu. On strategies for imbalanced text classification using svm: A comparative study. *Decision Support Systems*, 2009.

[40] Z. Sun, C. E. Rubio-Medrano, Z. Zhao, T. Bao, A. Doupé, and G.-J. Ahn. Understanding and Detecting Private Interactions in Underground Forums. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2019.

[41] S. Sundaresan, D. McCoy, S. Afroz, and V. Paxson. Profiling underground merchants based on network behavior. In *Proceedings of the IEEE Symposium on Electronic Crime Research (eCrime)*, 2016.

[42] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, et al. Data breaches, phishing, or malware? understanding the risks of stolen credentials. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2017.

[43] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, et al. Data breaches, phishing, or malware?: Understanding the risks of stolen credentials. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 1421–1434. ACM, 2017.

[44] S. Wang and C. D. Manning. Baselines and bigrams: Simple, good sentiment and topic classification. In *Proceedings of Association for Computational Linguistics (ACL)*, 2012.

[45] M. Zhang. Couple stole $1.2m worth of cameras and electronics from amazon, Oct. 2017.

[46] P. Zhang, A. Oest, H. Cho, Z. Sun, R. Johnson, B. Wardman, S. Sarker, A. Kpravelos, T. Bao, R. Wang, Y. Shoshitaishvili, A. Doupé, and G.-J. Ahn. CrawlPhish: Large-scale Analysis of Client-side Cloaking Techniques in Phishing. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2021.

[47] Z. Zhao, G.-J. Ahn, H. Hu, and D. Mahi. Socialimpact: systematic analysis of underground social dynamics. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2012.

[48] Z. Zhao, M. Sankaran, G.-J. Ahn, T. J. Holt, Y. Jing, and H. Hu. Mules, seals, and attacking tools: Analyzing 12 online marketplaces. *IEEE Security & Privacy*, 2016.

A Service Form in Preparation Stage

Table 7: Service form questions.

No.	Question
1	Which store do you need a refund on? Mention with domain (com/de/uk)
2	When did you place the order?
3	When did you receive your order?
4	Provide the carrier/tracking number?
5	Price of the item?
6	Your order number?
7	Name on your account?
8	The email address used for your account/order?
9	The billing address on the account? (including country & zip code)
10	The shipping address on the account? (including country & zip code)
11	Was a refund already attempted on your order? If yes, What method did you use and what did they say?
12	What type of payment? Example "Master Card" last 4 digits of the card used
13	What do you need, Refund/Replacement?
14	How do you want to pay me?
15	Did you sign for it? or was it left somewhere outside?
16	What was the item you want to get refunded? (Please paste links. In case of multiple items in your order, please include links to all and individual costs of each item)
17	Provide your telegram/discord you used to contact me.
18	Phone Number on the order/account?
19	Anything more about the order/account? Anything important that I should know?

B Scam Tutorials

Table 8: Tutorials for Concession Abuse.

Book Name	Book Type	Price	Introduction
E-Book	Core	€ 69.00	Introduction; Information; Q&A; Common refund methods; Amazon System explained; Internal/External Investigation explained; How to profit from refunding; Tips; Support
Fake TID method	Selective	€ 119.90	Best and most effective method of most shops; Step-by-step guide for Amazon
PayPal refunds up to 15,000 EUR	Selective	€ 179.90	New and easy way of refunding through Paypal, even if the seller is replying to your dispute. It comes with nearly 100% success rate for any store.
Amazon bonus methods	Selective	€ 19.90	Detailed step-by-step guide on how to refund Amazon with exclusive methods. It allows you to refund on Amazon (.com/.co.uk); How to get an instant advanced replacement for cracked accounts on Amazon.de
Find refundable stores	Selective	€ 39.90	A simple and extremely powerful way of finding new stores to refund
Telegram refunding group	Selective	€ 14.90	Come and join us! Exchange your ideas and experience with others. Connect with each other and improve your knowledge!
Start your own service	Selective	€ 49.90	Information for your future refund service including how to start, prepare, improve and maximize your business.
1-ON-1 mentorship	Selective	€ 449.90	Providing you help to complete with ongoing refunds and giving extra tips.

C The Survey Results of Customers' Attitudes to Proposed Defense

Table 9: Demographics of participants.

	Metric	Percentage of Participants
Gender	Female	53.8%
	Male	44.9%
	No Answer	1.3%
Age	18 ∼ 29 years	12.3%
	30 ∼ 49 years	62.7%
	50+ years	25.0%
Education	Up to H.S.	10.1%
	Some College	31.8%
	B.S. or above	58.1%
Num of shopping acct	0	0.8%
	1 ∼ 3	35.2%
	4 ∼ 6	31.8%
	7+	32.2%
Freq. of shopping per month	0	0.4%
	1 ∼ 3	60.2%
	4 ∼ 6	21.6%
	7+	17.8%
Expense of shopping in 2019	<= $200	7.6%
	$201 ∼ $500	22.9%
	$501 ∼ $1,000	29.7%
	$1,000+	39.8%

Table 10: General security experience and attitude.

	Metric	Percentage of Participants
Account Hacked (or suspected to be hacked)	Yes	40.3%
	No	59.7%
Financial Loss	Yes	3.4%
	No	96.6%
Adopt Security Measure	1 (Strongly disagree)	0.8%
	2	3.4%
	3	11.0%
	4	32.6%
	5 (Strongly agree)	52.2%

Table 11: Participants' concerns about security approaches.

Scenario	Concern	Quote
Invest & Proof	Inconvenience	I don't like being further inconvenienced to prove that I've been inconvenienced.
	Hard to prove	Hard to proof the absence of something, like a delivery. This feels like an additional burden.
	Suspecting moral character	I would not be dishonest in such a case and would be outraged that my honesty would be in question in such a case.
	Not always	It depends on how much proof they need and how easily i can get it to them. also how long they take to respond
ID_Verif	Annoying	Inconvenient and annoying and time-wasting.
Local_Rtn	Inconvenience	I live too far from these types of places for it to be remotely convienent.
	Not always	It depends on how close the store is, whether this would work.
Sep_Ship	Shipping delay	If it delays my shipment I would mind.
	Resource waste	It seems like a waste of packaging and we already waste a lot on packaging/shipping.
Pin_Egift	Annoying	Hard for me to remember regular passwords as it is but now I would have to remember a separate one for the gift cards.
Sec_Notif	Annoying	This is a pain. I don't want to main two email addresses for online shopping.
	Sharing private email address	I use one of my emails for very close and important emails and the other for shopping. I would not want any store whatsoever to have my private email under any circumstances.

Table 12: Participants' attitudes toward security approaches.

Scenario	Security Approach	1 (Strongly Not Mind)	2	3	4	5 (Strongly Mind)	Mean	Continue Buying	Stop Buying
1	Invest	56.4%	25.4%	11.4%	4.2%	2.6%	1.71	86.9%	13.1%
1	Invest_HV	72.0%	15.7%	5.5%	3.8%	3.0%	1.5	90.2%	9.8%
1	Proof	38.6%	19.1%	17.8%	14.0%	10.6%	2.40	68.6%	31.4%
2	ID_Verif	76.3%	14.0%	4.7%	3.0%	2.1%	1.42	93.6%	6.4%
3	Local_Rtn	47.5%	17.8%	14.8%	10.2%	9.7%	2.17	86.0%	14.0%
4	Sep_Ship	81.4%	7.6%	5.5%	3.0%	2.5%	1.38	93.6%	6.4%
5	Pin_Egift	78.0%	9.7%	5.1%	4.7%	2.5%	1.44	92.4%	7.6%
6	Sec_Notif	61.9%	16.1%	8.9%	7.6%	5.5%	1.79	87.7%	12.3%

Table 13: Survey questions.

	Question	Answer Options
S1 (Invest & Proof)	***S1: If you contact a merchant for a refund/replacement WITHOUT returning goods because of a reason such as never receiving the package or receiving an empty package.***	
	Q1: Do you mind if the merchant starts an investigation before issuing the refund/replacement?	Five-point Likert scale.
	Q2: If it is a high-value good (hundreds of dollars), do you mind the investigation?	Five-point Likert scale.
	Q3: If the merchant needs to start an investigation in this scenario, would you stop buying goods from this merchant any more?	(i) Yes, I will STOP buying from it, (ii) No, I will continue buying from it
	Q4: If the merchant needs to start an investigation on high-value goods in this scenario, would you stop buying goods from this merchant any more?	(i) Yes, I will STOP buying from it, (ii) No, I will continue buying from it
	Q5: Do you mind providing extra proof in this scenario? For example, a video of the empty box with a handwritten reference number, or a police report if the package is stolen by someone?	Five-point Likert scale.
	Q6: If the merchant needs you to provide extra proof in this scenario, would you stop buying goods from this merchant any more?	(i) Yes, I will STOP buying from it, (ii) No, I will continue buying from it
	Q7: If you mind the investigation or providing extra proof in this scenario, please briefly explain the reason.	Short Answer
	Q8: If you DO NOT mind the investigation or providing extra proof, please briefly explain the reason.	Short Answer
S2 (ID_Verif)	***S2: To prevent criminals from buying goods using your account, an effective countermeasure could be verifying a customer's identity (i.e., 2-factor authentication; answer security questions through a link) when the shipping address is requested to change.***	
	Q1: Do you mind merchants employing this approach?	Five-point Likert scale.
	Q2: If the merchant employs this approach, would you stop buying goods from this merchant any more?	(i) Yes, I will STOP buying from it, (ii) No, I will continue buying from it
	Q3: If you mind the merchant employing this security approach, please briefly explain the reason.	Short Answer
	Q4: If you DO NOT mind the merchant employing this security approach, please briefly explain the reason.	Short Answer
S3 (Local_Rtn)	***S3: To ensure some high-value goods are properly packaged and avoid any unnecessary loss, customers may be requested to return them to a local store or a shipping agent who will help pack them.***	
	Q1: Do you mind merchants employing this policy?	Five-point Likert scale.
	Q2: If the merchant employs this return policy, would you stop buying goods from this merchant any more?	(i) Yes, I will STOP buying from it, (ii) No, I will continue buying from it
	Q3: If you mind the merchant employing this return policy, please briefly explain the reason.	Short Answer
	Q4: If you DO NOT mind the merchant employing this return policy, please briefly explain the reason.	Short Answer
S4 (Sep_Ship)	***S4: To track and ensure the high-value goods can be delivered to you, high-value goods would be shipped separately with your other packages.***	
	Q1: Do you mind merchants employing this policy?	Five-point Likert scale.
	Q2: If the merchant employs this policy, would you stop buying goods from this merchant any more?	(i) Yes, I will STOP buying from it, (ii) No, I will continue buying from it
	Q3: If you mind the merchant employing this shipping policy, please briefly explain the reason.	Short Answer
	Q4: If you DO NOT mind the merchant employing this shipping policy, please briefly explain the reason.	Short Answer
S5 (Pin_Egift)	***S5: To protect gift cards in customers' accounts from stealing, setting up a payment password/PIN for e-gift cards would be an effective security approach.***	
	Q1: Do you mind merchants employing this approach?	Five-point Likert scale.
	Q2: If the merchant employs this approach, would you stop buying goods from this merchant any more?	(i) Yes, I will STOP buying from it, (ii) No, I will continue buying from it
	Q3: If you mind the merchant employing this security approach, please briefly explain the reason.	Short Answer
	Q4: If you DO NOT mind the merchant employing this security approach, please briefly explain the reason.	Short Answer
S6 (Sec_Notif)	***S6: To ensure customers can receive information about all account activities even if the accounts are hacked, a dedicated notification approach, such as a secondary email address, is needed. This notification approach would be undisclosed in a customer's profile.***	
	Q1: Do you mind merchants employing this approach?	Five-point Likert scale.
	Q2: If the merchant employs this approach, would you stop buying goods from this merchant any more?	(i) Yes, I will STOP buying from it, (ii) No, I will continue buying from it
	Q3: If the merchant needs your secondary email address as the notification approach, do you have a secondary e-mail address you could provide?	(i) Yes, (ii) No
	Q4: If you mind the merchant employing this security approach, please briefly explain the reason.	Short Answer
	Q5: If you DO NOT mind the merchant employing this security approach, please briefly explain the reason.	Short Answer

D Service List of a Scam Service Provider

Table 14: A Concession Abuse service list.

Store Category	Payment Method	Store	Limit ($/€)	Items	Pay Rate (%)	Region	Avg Time
Clothing	Credit/Debit Card	Abercrombie & Fitch	No Limit	Multi	25%	Worldwide	1 Day
		Macys	No Limit	One	25%	USA	1 Day
		Hollister	No Limit	Multi	25%	Worldwide	1 Day
		Zappos incl Luxury	30,000	Multi	25%	USA	1 Day
		Armani	3,000	Multi	25%	Worldwide	10 Day
	PayPal	Stone Island	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		StockX	No Limit	One	15 – 25%	Worldwide	2 – 3 Weeks
		YOOX	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		Dolce Gabbana	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		Mr Porter	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
Electronics	Credit/Debit Card	Walmart	30,000	Multi	25%	USA	1 Day
		Target	30,000	Multi	25%	USA	1 Day
		Google Express	12,000	One	25%	USA	5 – 10 Days
		Apple	5,000	One	25%	USA	1 – 3 Days
		Lenovo	5,000	One	25%	USA	1 – 2 Weeks
	PayPal	Canon	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		Dell	No Limit	One	15 – 25%	Worldwide	2 – 3 Weeks
		Microsoft	No Limit	Multi	15 – 25%	EU/USA/CA	2 – 3 Weeks
		Google Express	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
		HP	No Limit	Multi	15 – 25%	Worldwide	2 – 3 Weeks
Beauty	Credit/Debit Card	Sephora	3,000	Multi	15 – 25%	Worldwide	1 – 5 Days
		Lancome	1,000	Multi	15 – 25%	USA	3 – 10 Days
		MAC Cosmetics	1,000	Multi	15 – 25%	Worldwide	3 – 10 Days
		Urban Decay	1,000	Multi	15 – 25%	USA	3 – 10 Days
		Estee Lauder	1,000	Multi	15 – 25%	USA	3 – 10 Days
Outdoors	Credit/Debit Card	Fanatics	1,000	Multi	15 – 25%	USA	1 Day
		NBA/NFL/NHL Store	1,000	Multi	15 – 25%	USA/CA	1 Day
		Oakley	1,000	Multi	15 – 25%	Worldwide	5 – 7 Days
		Rayban	1,000	Multi	15 – 25%	Worldwide	1 – 3 Days
		Sunglass Hut	1,000	Multi	15 – 25%	USA	3 – 10 Days
Home	Credit/Debit Card	Allmodern	No Limit	One	18 – 25%	USA/CA	1 – 5 Days
		Wayfair	No Limit	One	18 – 25%	USA/CA	1 – 5 Days
		Birch Lane	No Limit	One	18 – 25%	USA/CA	1 – 5 Days
		Joss & Main	No Limit	One	18 – 25%	USA/CA	1 – 5 Days
		Herman Miller	No Limit	One	18 – 25%	USA/CA	1 – 5 Days
Pet Store	Credit/Debit Card	Chewy	1,000	Multi	15 – 25%	USA/CA	1 – 5 Days
		PetCo	1,000	Multi	15 – 25%	USA/CA	1 – 5 Days
		PetSmart	1,000	Multi	15 – 25%	USA/CA	1 – 5 Days
		Petvalu	1,000	Multi	15 – 25%	USA/CA	1 – 5 Days
		PetSupermarket	1,000	Multi	15 – 25%	USA/CA	1 – 5 Days
Adult	Credit/Debit Card	Adam & Eve	1,000	Multi	15 – 25%	USA	1 Day
		Lovehoney	1,000	Multi	15 – 25%	Worldwide	1 Day
Amazon	Credit/Debit Card	Amazon.com	7,000	Multi	25%	Worldwide	2 – 3 Weeks
		Amazon.fr	5,000	Multi	25%	Worldwide	7 – 10 Days
		Amazon.ca	5,000	Multi	25%	Worldwide	2 – 3 Weeks
		Amazon.de	5,000	Multi	25%	Worldwide	2 – 3 Weeks
		Amazon.it	5,000	Multi	25%	Worldwide	2 – 3 Weeks
		Amazon.nl	5,000	Multi	25%	Worldwide	3 – 5 Days
		Amazon.com.au	3,000	Multi	25%	Worldwide	5 – 10 Days