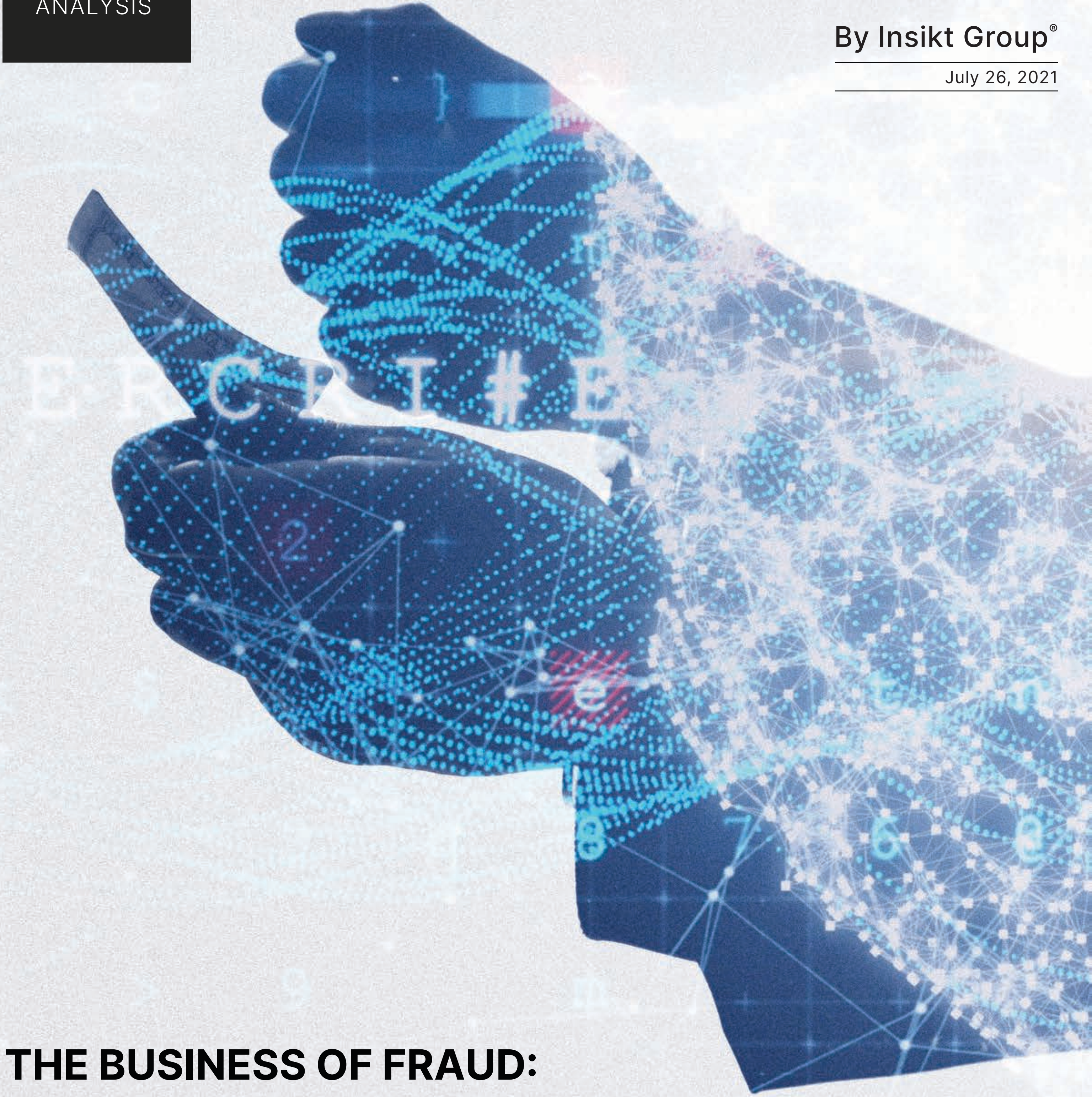
CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

July 26, 2021



THE BUSINESS OF FRAUD: Online Retail Fraud in the Criminal Underground

Recorded Future analyzed current data from the Recorded Future® Platform, as well as dark web and open-source intelligence (OSINT) sources, to review the current landscape of online retail fraud scams and schemes popular with threat actors. This report will be of most interest to anti-fraud and network defenders, security researchers, and executives charged with security and fraud risk management and mitigation. This report expands upon findings addressed in the first report of the Insikt Group's fraud series, "The Business of Fraud: An Overview of How Cybercrime Gets Monetized".

Executive Summary

Online retail fraud is a persistent, multifaceted threat to businesses of all sizes and their customers and is likely to persist for the foreseeable future as consumers engage more with online retailers and shop more online versus at traditional "brick and mortar" stores. Also called e-commerce fraud, online retail fraud is the act of committing some form of fraud, such as a fraudulent transaction, on a web-based retail platform. Generally, cybercriminals will use stolen payment or account information to conduct these transactions. Some elements of online retail fraud also involve social engineering schemes that look to defraud a retail platform directly, as in the case with refunding scams against one's customer service branch, or a third party, such as interception fraud or scams that target shipping companies.

Threat actors engaging in online retail fraud discuss the topic in multiple languages, primarily English, Russian, and Chinese, discussing methods, offering tutorials and guides, and selling various goods and services ranging from significantly discounted stolen gift card information to all-inclusive refunding services targeting major retailers. If major online retailers have implemented various methods of anti-fraud mitigation, threat actors often devise techniques to bypass anti-fraud measures, namely through anti-detection (anti-detect) browsers.

Key Judgments

- Online retail fraud will likely increase in the future as e-commerce platforms continue to grow in the coming years.
- We believe that threat actors will continue to demonstrate flexibility, adaptability, and opportunism amid a shifting e-commerce landscape, targeting emerging retail opportunities such as curbside pickup.
- Gift card fraud is its own type of service across the dark web and a way for cybercriminals to steal and launder money. Threat actors who specialize in gift card fraud operate dedicated shops due to its high demand.
- Refund fraud, or refunding for short, is both an entryway for threat actors to establish credibility on criminal forums and a growing avenue for threat actors to engage in criminal services against online retailers through social engineering.
- We believe that cybercriminals will continue developing and using anti-detection tools to circumvent organizations' security mechanisms.

Background

Online retail fraud is a form of fraud that specifically targets an online e-commerce platform or retailer. To conduct online retail fraud, a threat actor attempts to engage in a fraudulent transaction against an e-commerce platform using compromised credit card information, client or customer information, or false identities to obtain goods or services. Online retail fraud also encompasses gift card and refund fraud and is frequently facilitated by anti-detect and reshipping services.

E-commerce platforms, social media, and financial organizations are targeted by cybercriminals attempting to bypass or disable their security mechanisms, in some cases by using tools that imitate the activities of legitimate users. Although most major online retailers have implemented various anti-fraud measures, such as using cookies and fingerprinting browsers, threat actors have created methods to circumvent many of these measures.

Threat Analysis

Obtaining Victim Data

The initial step for online retail fraud stems from a threat actor's acquisition of a victim's payment information, online retail account profile, or by obtaining one's personally identifiable information (PII), such as name, date of birth, and Social Security number (a complete profile of this information is colloquially known on the dark web as "fullz"). The vectors for obtaining said information vary. Login details can be captured through traditional phishing scams, and credit card information is sometimes gathered through skimmers and shimmers physically installed at point-of-sale terminals. In other cases, direct vulnerabilities lead to the compromise of primary or third-party partners, as in the case with Home Depot in 2014 or [24]7.ai and British Airways in 2018. Threat actors can deploy malware across a retailer's payment systems, potentially exposing customer credit card information en masse. Massive data breach events are highly costly for both online and brick and mortar retailers, both in terms of actual monetary cost (damages, fines) and severe declines in consumer trust in a brand.

Selling and Using Victim Data

Once a victim's account or credit card information is obtained, a threat actor will look to sell the information for a nominal fee or will attempt to use the stolen information to "cash out" by buying goods and services, commonly through an online retailer. Over the years, dark web marketplaces and shops have facilitated the buying and selling of victim information for use in online retail fraud and other illicit activities. Among the leading carding marketplaces and shops in 2021 include Trump's Dumps, CC2BTC, The Canadian HeadQuarters, and PP24 2.0.

With this information in hand, threat actors can engage in various forms of online retail fraud, including credit card fraud, friendly fraud (also called "chargebacks"), account takeover, gift card fraud, refunding, interception, and triangulation.

Credit Card Fraud

Credit card fraud (carding) is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services or to make payment to another account controlled by a criminal. The Payment Card Industry Data Security Standard (PCI DSS) is the data security standard created to help businesses process card payments securely and reduce card fraud.

Credit card fraud can be authorized, meaning the genuine customer themselves processes payment to another account which is controlled by a criminal, or unauthorized, meaning the account holder does not provide authorization for the payment to proceed and the transaction is carried out by a third party. Unauthorized transactions happen in 2 ways: "card present" and "card not present":

- **Card-present** fraud is a transaction in which the fraudulent party physically presents the counterfeit credit card to the merchant. Threat actors can obtain the credit card Track 2 data with skimmers, scrapers, sniffers, or simply purchase the previously stolen data online.
- **Card-not-present** fraud occurs in fraudulent transactions where a cardholder does not present a card to a merchant in person. It includes internet, phone, and mail-order transactions. In most cases, this type of fraud happens after a threat actor steals card information such as a card number from hacking, sniffing, or phishing or purchases such data online. This stolen card data then enables a fraudster to carry out unauthorized transactions even if the legitimate card is never lost or stolen.

Chargeback and "Friendly" Fraud

Chargeback fraud involves a buyer contacting their payment card provider and requesting a charge be pulled from a retailer even though a product has been successfully delivered. In cases where the customer has made an honest mistake, this is referred to as friendly fraud: a customer who commits friendly fraud might not have seen a delivery arrive, forgotten they ordered an item, purchased the wrong item by accident, or not realized that another household member placed an order.

Chargeback fraud, however, involves malicious intent on the part of the threat actor, who intentionally makes orders and fabricates reasons for chargebacks that sound plausible. Threat actors may further profit from these falsified orders by reselling the merchandise. For example, a threat actor could place a large order from an e-commerce retailer, perhaps even spreading the order out across numerous payment cards and shipping addresses, then force a chargeback on all the transactions, enabling them to obtain costly items without raising too much suspicion on the payment card side or from the retailer.

Curbside Pickup Fraud

Amid the COVID-19 pandemic, retailers significantly shifted how consumers can continue to purchase goods and services with both safety and convenience in mind. Out of this, retailers have offered agile options for consumers, such as "buy online and pick up in store" (BOPIS) options like curbside pickup. With these emerging retail opportunities, threat actors also demonstrated flexibility, adaptability, and opportunism in targeting BOPIS options where identification or proof of purchase is, in many situations, not required. Many successful schemes require a name, phone number or email address, and product name. Threat actors may also attempt to emulate a friend or a relative, claiming to pick up a product on behalf of a victim.

Account Takeover

Account takeover (ATO) in a retail fraud context is an attack that involves a threat actor compromising a customer's account on an e-commerce website and using it to make purchases of physical goods using saved payment card details or store credit. Threat actors can use several methods to compromise retail website accounts, including phishing messages and password-spraying attacks. ATO attacks can be used to have goods shipped to physical addresses where the threat actor can pick them up.

In some cases, the threat actor could be motivated to get expensive items for free, or they may attempt to accumulate a large number of valuable items to resell for profit. Accounts are sometimes compromised and then resold to other threat actors for use in fraud.

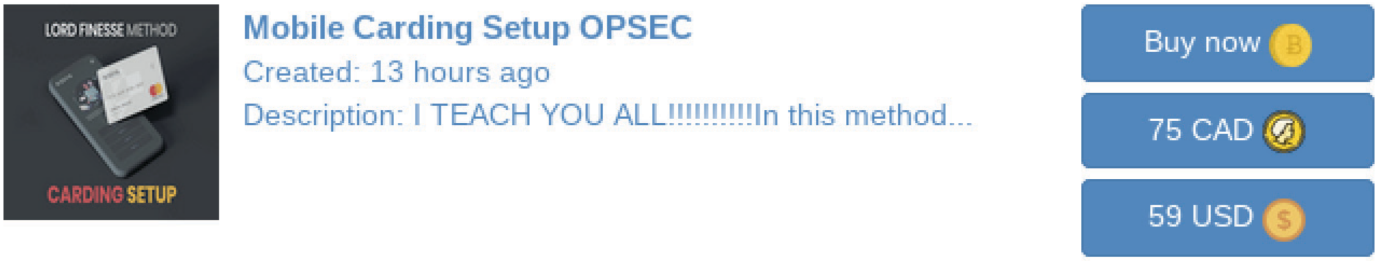
Not only do ATO attacks pose a threat to retailers from a monetary perspective, but also from a brand reputation perspective. Customers surveyed reported being very likely to stop using an online retailer if their data was compromised; this would likely apply even if data were compromised because of a mistake on the customer's part, such as providing credentials in response to a phishing message.

Dark web discussions surrounding ATO can best be categorized into the sale of retailer-specific accounts, many of which are advertised as having payment methods linked to them and also in terms of "bot" sales on sources like Genesis Store.

- Account Sales — Customer accounts for major retailers were located primarily on Cracked Forum but also on sources such as The Canadian HeadQuarters, WWH Club, and ToRRez Market. The accounts are often sold in bulk, with the number of accounts available ranging from a few to hundreds.
- Bot Sales — Bot shops have gained a lot of attention in recent years following the emergence of Genesis Store in 2019. Bot shops sell access to information collected from compromised machines for a small fee depending on the type of accounts linked to the browser of the machine's user. The purchase does not give a threat actor full control over the machine. Advertisements on these shops will often include a list of web addresses that the compromised machine's browser has visited that are relevant, which include not only social media and banking websites but popular retailers as well. Even if the threat actor who purchases the bot cannot access the machine itself, they can use the machine's browser information to access accounts that are logged in to place orders to different addresses and perhaps change email addresses tied to the account so the account owner is not alerted to the order via email. They may even change the credentials and take over the account fully.

Gift Cards

Gift cards are a popular way for cybercriminals to steal and launder money. Gift card fraud is its own type of service across the dark web, with threat actors operating dedicated shops that specialize in the service due to its high demand. The advantages of gift cards for cybercriminals are that they are not necessarily tied to a specific persona, they can be easier to clone since some of them are not PIN- or chip-enabled, and they can be refilled with other compromised payment methods.



Mobile Carding Setup OPSEC
Created: 13 hours ago
Description: I TEACH YOU ALL!!!!!!!!!!In this method...

Figure 1: Threat actor "lordfinesse" selling a manual for mobile carding setup (Source: The Canadian HeadQuarters)

Gift card fraud requires more finesse than other forms of online retail fraud according to the threat actors that specialize in it. Threat actors pay special attention to their system setup and preparation, with some recommending using smartphones as opposed to virtual machines (VM) for operational security and anti-fraud systems bypass. Additional techniques may include using anti-detect browsers, RDP and VNC connections using infected machines to mimic real users or adding an additional layer of anonymity. Threat actors who specialize in gift card fraud state that all this additional anonymity is necessary because companies may treat gift card transactions with elevated fraud risk criteria.

Threat actors can gain access to gift cards by using automated checkers and brute forcers. If threat actors successfully conduct a brute-forcing or credential stuffing attack, they receive access to the targeted user's accounts, which may have linked gift cards that the attackers then attempt to exfiltrate for monetization purposes. Below is an example of a gift card checker advertised by the threat actor "xRisky". According to xRisky, the tool allows cybercriminals to determine the validity of victim accounts and gain unauthorized access to the gift cards linked to victim accounts.

Once threat actors access a victim's gift cards, they can profit by draining the gift card's balance, making unauthorized transfers or purchases, or reselling gift cards on the dark web. One such reseller is the threat actor "GoldRivera", who operates the online shop "Corner Store", reselling stolen gift cards for 35% to 40% of the original price.

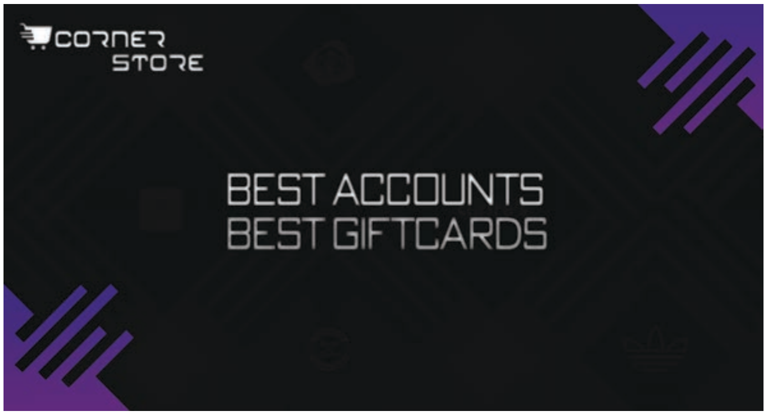
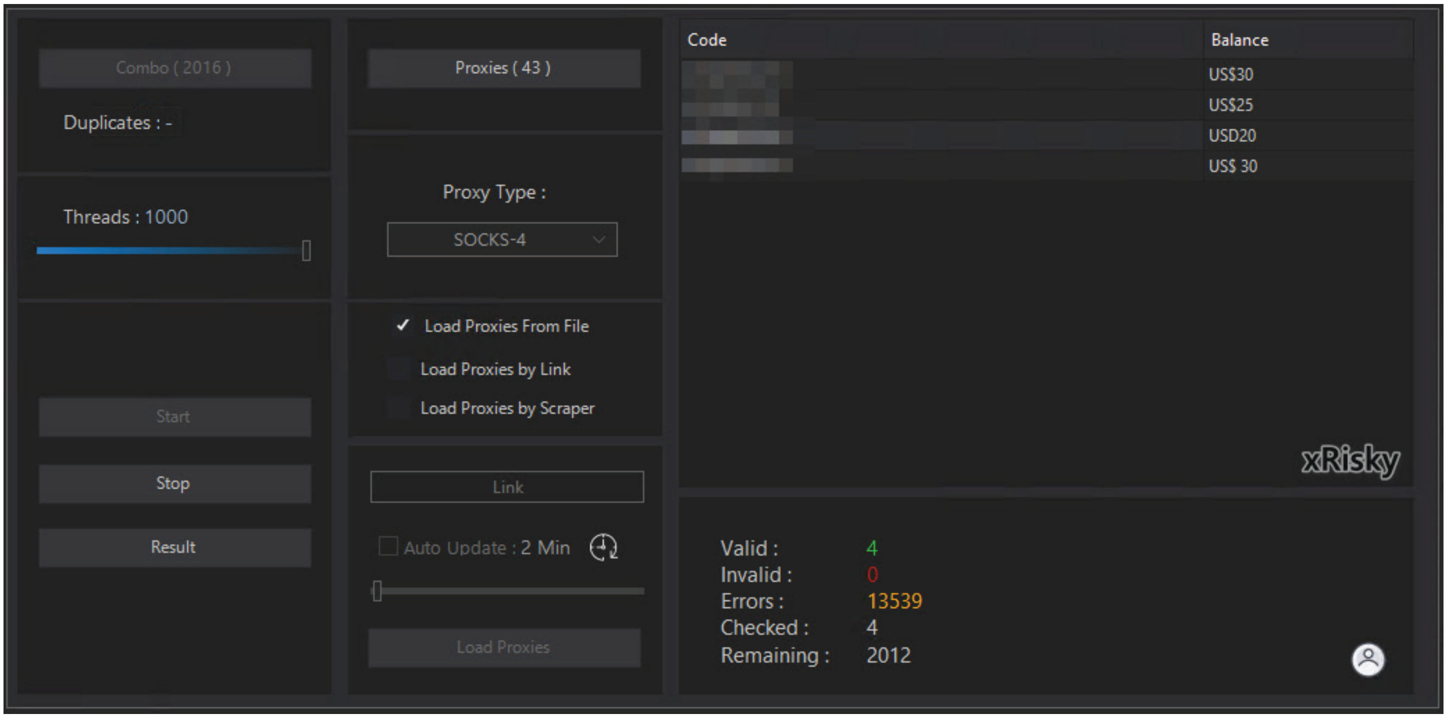


Figure 3: "Corner Store" gift card shop operated by GoldRivera (Source: Nulled Forum)

Refunding

Discussion about refunding tactics as a "do-it-yourself" (DIY) service is more common than refunding services offered on criminal forums and on the clearnet. It is far more common to see threat actors posting methods of refund fraud, either for small fees or often for free, likely as a quick and easy way to gain a positive reputation on a forum that is then used to grant credibility. Based on the discussions we have observed, it appears that this is an activity that threat actors conduct for themselves to obtain free items of value such as computers, software, clothing, shoes, and other small items. These are more one-off activities as opposed to profitable cybercriminal pursuits like credit card theft. Threat actors also generate fake receipts or shipping tracker numbers, which are used to support false claims of lost or stolen packages or missing items from packages.



Duplicates : -

Threads : 1000

Proxy Type : SOCKS-4

☑ Load Proxies From File
□ Load Proxies by Link
□ Load Proxies by Scraper

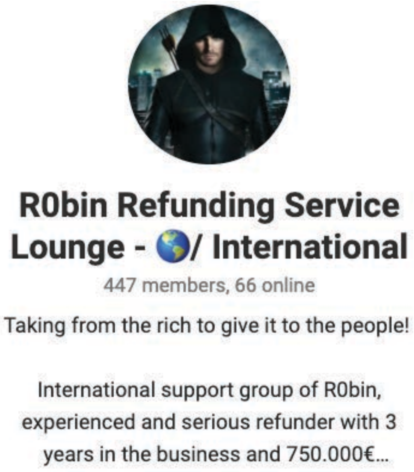
□ Auto Update : 2 Min

Code	Balance
[redacted]	US$30
[redacted]	US$25
[redacted]	USD20
[redacted]	US$ 30

```
Valid :       4
Invalid :     0
Errors :      13539
Checked :     4
Remaining :   2012
```

Figure 2: Screenshot of xRisky's gift card checker (Source: Cracked Forum)

GREENTEA
GREENTEA
GreenTea's SE Services
Cheap Refunding services, Join the discord server!
Also, Cheap Se Services!


R0bin Refunding Service Lounge - 🌎/ International

447 members, 66 online

Taking from the rich to give it to the people!

International support group of R0bin, experienced and serious refunder with 3 years in the business and 750.000€...

Figures 4 and 5: GreenTea Social Engineering and Refunding Services, as advertised on Cracked Forum (left), and a private refunding service Telegram group advertised on Cracked (right)

Discussions of social engineering and refunding fraud often go hand in hand with refund scams on the dark web. Most of these discussions are concentrated on Cracked Forum, but many dedicated chat groups and channels exist, including closed Discord Servers and on Telegram. On Cracked Forum, members often discuss refund scam methods, solicit refunding services, and advertise both paid and free guides and tutorials on refunding scams, such as e-books on social engineering tactics. These books, which mainly concern refunding scams against retail and e-commerce, are often oriented towards beginners looking to start their own scams, but they are highly popular with members of all levels of expertise.

OGUsers Forum is also home to many discussions on refunding services. Here, forum members advertise and discuss refunding services targeting retail, e-commerce, and entertainment entities, with a substantial focus on refund schemes. Within forum posts that advertise these services, prospective customers are encouraged to join dedicated Discord servers and closed Telegram groups. It is likely that discussions of these services take place elsewhere, such as on dedicated group chats or through private messaging.

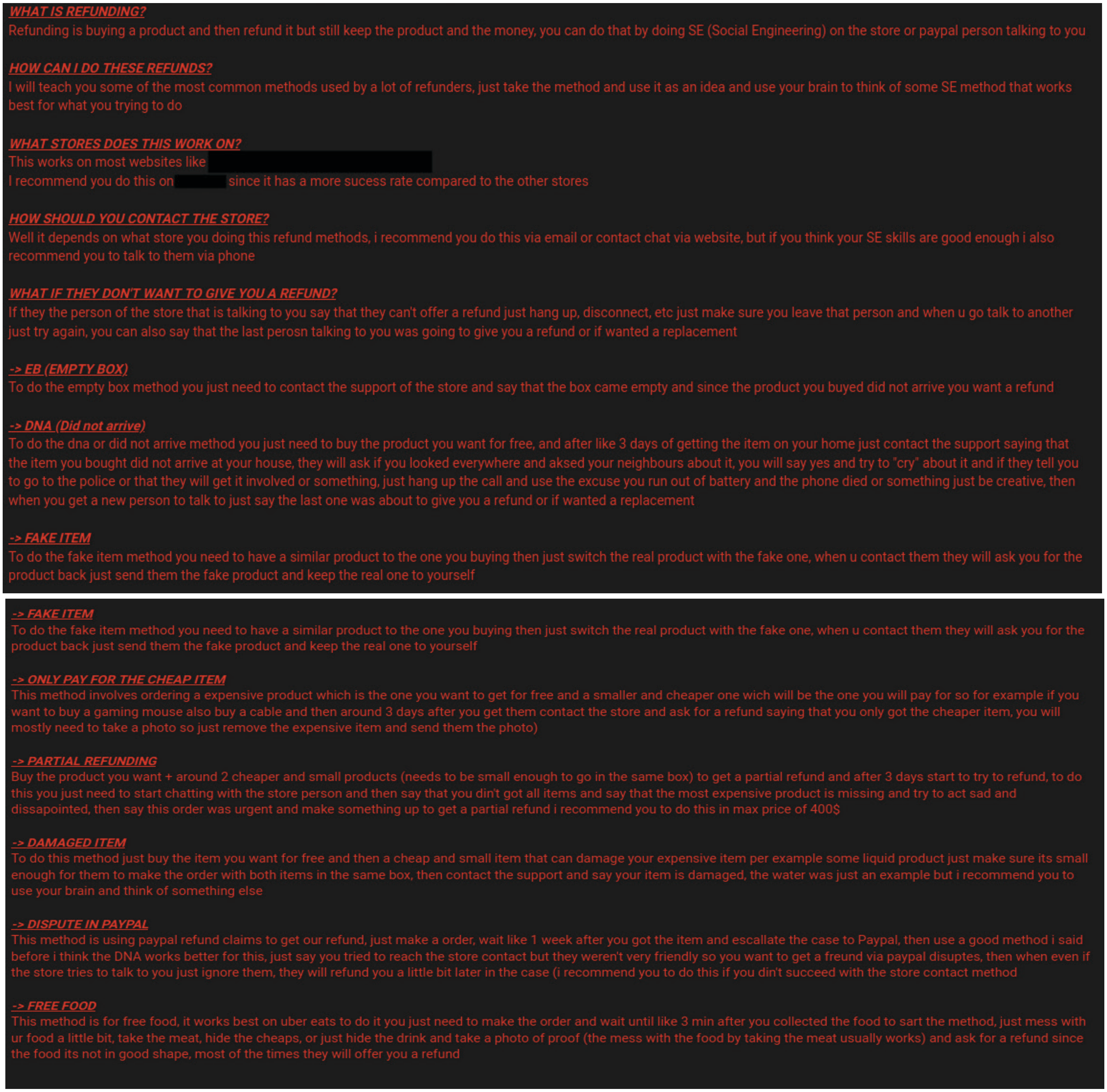
Discussions of refunding scams outside of Cracked Forum and OGUsers Forum are less frequent but not uncommon. Over the past year, regular advertisements for refunding services were discussed on dark web special-access forums such as Best Hack Forum and YouHack Forum. At a much lower level of discussion activity, we identified advertisements for e-books on the closed dark web market Berlusconi Market, as well as few mentions (fewer than 5 each) on Demon Forums, The Hub Forum, DNMAvengers Forum, and Verified Carder Forum. Advertisements for methods of fake receipt generation and specifically methods of getting refunds from e-commerce businesses were also observed on The Canadian HeadQuarters and Raid Forums.

Refund Fraud Tactics, Techniques, and Procedures (TTPs)

Refund fraud TTPs fall under 3 primary categories: receipt generation, tracking number manipulation, and general social engineering. The following sections will highlight how threat actors discuss and use each to engage in successful refunding fraud.

Receipt Generation

Receipt generation is a tactic that is commonly referenced in refund fraud discussions. Many of the postings can be obtained by searching our data sets from dark web forums using the keyword "receipt". Fake receipts are made in several ways, including photoshop templates and automatic receipt generators. With these methods, threat actors can create receipts for products they never purchased or potentially manipulate a receipt to make it appear that a different number of products was purchased from the number received. This tactic could presumably be used for most e-commerce outlets, and possibly even some physical store locations.



WHAT IS REFUNDING?

Refunding is buying a product and then refund it but still keep the product and the money, you can do that by doing SE (Social Engineering) on the store or paypal person talking to you

HOW CAN I DO THESE REFUNDS?

I will teach you some of the most common methods used by a lot of refunders, just take the method and use it as an idea and use your brain to think of some SE method that works best for what you trying to do

WHAT STORES DOES THIS WORK ON?

This works on most websites like [redacted]
I recommend you do this on [redacted] since it has a more sucess rate compared to the other stores

HOW SHOULD YOU CONTACT THE STORE?

Well it depends on what store you doing this refund methods, i recommend you do this via email or contact chat via website, but if you think your SE skills are good enough i also recommend you to talk to them via phone

WHAT IF THEY DON'T WANT TO GIVE YOU A REFUND?

If they the person of the store that is talking to you say that they can't offer a refund just hang up, disconnect, etc just make sure you leave that person and when u go talk to another just try again, you can also say that the last perosn talking to you was going to give you a refund or if wanted a replacement

-> EB (EMPTY BOX)

To do the empty box method you just need to contact the support of the store and say that the box came empty and since the product you buyed did not arrive you want a refund

-> DNA (Did not arrive)

To do the dna or did not arrive method you just need to buy the product you want for free, and after like 3 days of getting the item on your home just contact the support saying that the item you bought did not arrive at your house, they will ask if you looked everywhere and aksed your neighbours about it, you will say yes and try to "cry" about it and if they tell you to go to the police or that they will get it involved or something, just hang up the call and use the excuse you run out of battery and the phone died or something just be creative, then when you get a new person to talk to just say the last one was about to give you a refund or if wanted a replacement

-> FAKE ITEM

To do the fake item method you need to have a similar product to the one you buying then just switch the real product with the fake one, when u contact them they will ask you for the product back just send them the fake product and keep the real one to yourself

-> FAKE ITEM

To do the fake item method you need to have a similar product to the one you buying then just switch the real product with the fake one, when u contact them they will ask you for the product back just send them the fake product and keep the real one to yourself

-> ONLY PAY FOR THE CHEAP ITEM

This method involves ordering a expensive product which is the one you want to get for free and a smaller and cheaper one wich will be the one you will pay for so for example if you want to buy a gaming mouse also buy a cable and then around 3 days after you get them contact the store and ask for a refund saying that you only got the cheaper item, you will mostly need to take a photo so just remove the expensive item and send them the photo)

-> PARTIAL REFUNDING

Buy the product you want + around 2 cheaper and small products (needs to be small enough to go in the same box) to get a partial refund and after 3 days start to try to refund, to do this you just need to start chatting with the store person and then say that you din't got all items and say that the most expensive product is missing and try to act sad and dissapointed, then say this order was urgent and make something up to get a partial refund i recommend you to do this in max price of 400$

-> DAMAGED ITEM

To do this method just buy the item you want for free and then a cheap and small item that can damage your expensive item per example some liquid product just make sure its small enough for them to make the order with both items in the same box, then contact the support and say your item is damaged, the water was just an example but i recommend you to use your brain and think of something else

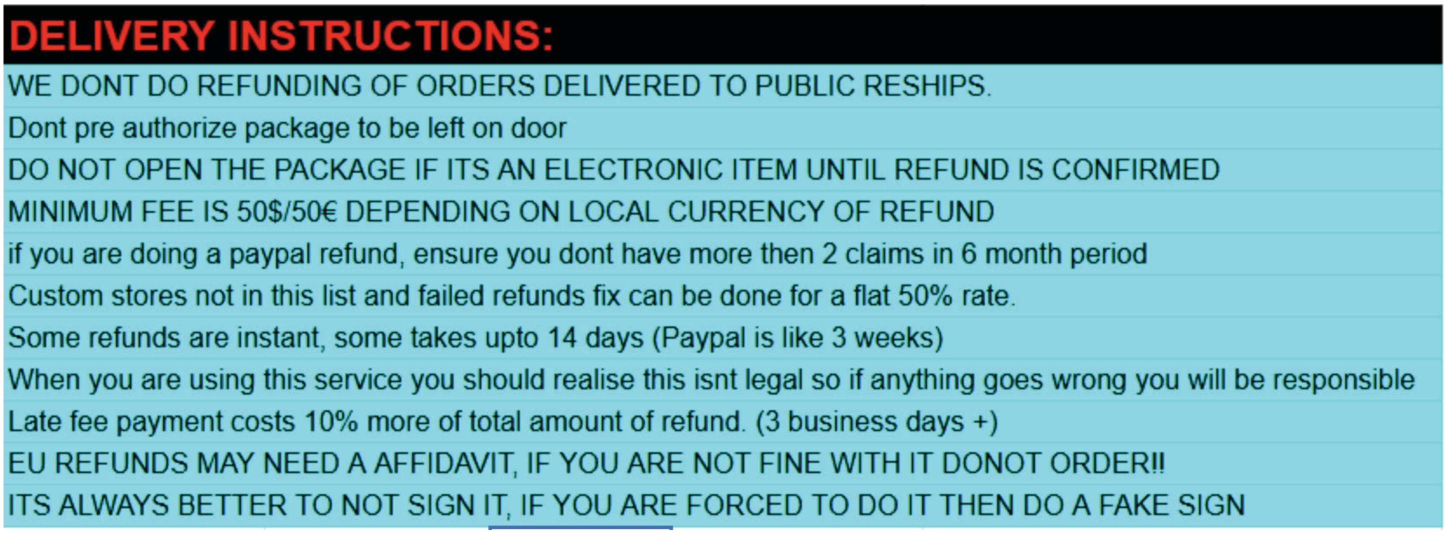
-> DISPUTE IN PAYPAL

This method is using paypal refund claims to get our refund, just make a order, wait like 1 week after you got the item and escallate the case to Paypal, then use a good method i said before i think the DNA works better for this, just say you tried to reach the store contact but they weren't very friendly so you want to get a freund via paypal disuptes, then when even if the store tries to talk to you just ignore them, they will refund you a little bit later in the case (i recommend you to do this if you din't succeed with the store contact method

-> FREE FOOD

This method is for free food, it works best on uber eats to do it you just need to make the order and wait until like 3 min after you collected the food to sart the method, just mess with ur food a little bit, take the meat, hide the cheaps, or just hide the drink and take a photo of proof (the mess with the food by taking the meat usually works) and ask for a refund since the food its not in good shape, most of the times they will offer you a refund

Figure 6: Threat actor "Try" illustrating refund fraud scams on Cracked Forum



DELIVERY INSTRUCTIONS:

WE DONT DO REFUNDING OF ORDERS DELIVERED TO PUBLIC RESHIPS.

Dont pre authorize package to be left on door

DO NOT OPEN THE PACKAGE IF ITS AN ELECTRONIC ITEM UNTIL REFUND IS CONFIRMED

MINIMUM FEE IS 50$/50€ DEPENDING ON LOCAL CURRENCY OF REFUND

if you are doing a paypal refund, ensure you dont have more then 2 claims in 6 month period

Custom stores not in this list and failed refunds fix can be done for a flat 50% rate.

Some refunds are instant, some takes upto 14 days (Paypal is like 3 weeks)

When you are using this service you should realise this isnt legal so if anything goes wrong you will be responsible

Late fee payment costs 10% more of total amount of refund. (3 business days +)

EU REFUNDS MAY NEED A AFFIDAVIT, IF YOU ARE NOT FINE WITH IT DONOT ORDER!!

ITS ALWAYS BETTER TO NOT SIGN IT, IF YOU ARE FORCED TO DO IT THEN DO A FAKE SIGN

Figure 7: Delivery instructions tied to Krommy refund service (Source: Private Google Drive link shared on Telegram)

Tracking Number Manipulation

One tactic for engaging in refunding fraud is to manipulate or fabricate tracking identification (ID) numbers. Threat actors share guides for creating fake tracking ID numbers for shipping vendors targeting e-commerce platforms. In some cases, these postings receive upwards of 10,000 views on Cracked, suggesting a large amount of interest.

General Social Engineering

Much of the refunding fraud landscape revolves around pure social engineering combined with basic operational security to hide the real identity of threat actors. These operational security methods involve using a physical address other than a primary residence for delivery, using a burner phone purchased with cash and a VPN for ordering and corresponding with customer service, and using false identities at different points in the process. We also observed threat actors referencing tools that could help bypass fraud mitigation technology, specifically AntiDetect, which assists threat actors in hiding their system's digital fingerprints.

We have discovered other similar e-books that explain a number of different methods combined with scripts on how to deal with customer service representatives through email, phone, and live chat features. These scripts give threat actors instructions on exactly how to phrase things and speak to customer service representatives in a number of different situations, some of which include:

- Order is dropped off and not signed for
- Order is signed for with a fake name
- Order is signed for with real name
- Refunding electronics
- Orders with multiple packages
- Refunding while also keeping every item in the box
- Refunding for store credit

These various situations are included with detailed instructions in instruction manuals on not only what to say, but also how to provide picture evidence of damage to boxes, how to fake damaged products, or how to report missing or stolen products. Most of the methods involve convincing the customer service representatives that a package was never received, was stolen from a residence, or arrived missing part of the order or missing all the items.

Anti-Detection Browsers

Multiple e-commerce, social media, and financial organizations around the world are targeted by cybercriminals attempting to bypass or disable their security mechanisms, in some cases by using tools that imitate the activities of legitimate users. Threat actors who have obtained compromised payment cards will then attempt to access the funds on those cards. If the payment card information was obtained from a compromised online merchant, for example by using a sniffer, that information will contain everything needed to attempt online retail fraud. This includes basics like the card number and the victim's name, physical address, and security code. Although most major online retailers have implemented various methods of anti-fraud mitigation, such as using cookies and fingerprinting browsers, threat actors have come up with means to circumvent many of those methods.

Every web browser has a unique fingerprint known to legitimate websites, with e-commerce companies and banks often using this type of fingerprinting to block transactions from browsers that have previously been recognized as insecure or involved in fraudulent activity. The practice by cybercriminals of using various virtual machines (VMs), proxies, and VPN servers is not that effective since the anti-fraud systems have capabilities to identify suspicious IP addresses and VMs. As a result, cybercriminals have developed anti-detection software that are in popular use on the dark web, such as Linken Sphere, AntiDetect, Multilogin, Che Browser, and FraudFox. These anti-detection software services allow threat actors to change all web browser configurations dynamically and generate an unlimited number of new ones, imitating the activities of legitimate users.

It is worth noting that anti-detection tools are widely available not only on dark web forums but also on legitimate sources operated by legal companies. Anti-detection browsers are in demand not only by financially motivated cybercriminals but also such customer categories:

- Penetration testers
- Social media professionals
- Specialists working with advertisements based on keyword searches
- Web traffic arbitrage professionals
- Bonus hunters who create multiple accounts for online gambling and gaming to earn monetary bonuses from specific deals offered by organizers
- Privacy advocates

As a rule, these tools are available for rent. Some developers offer free trial versions, but typically the monthly rental prices may range from $15 to $500 depending on account privileges. Some anti-detection browsers offer lifetime licenses.

Most Discussed and Advertised Anti-Detection Browsers on Dark Web Sources

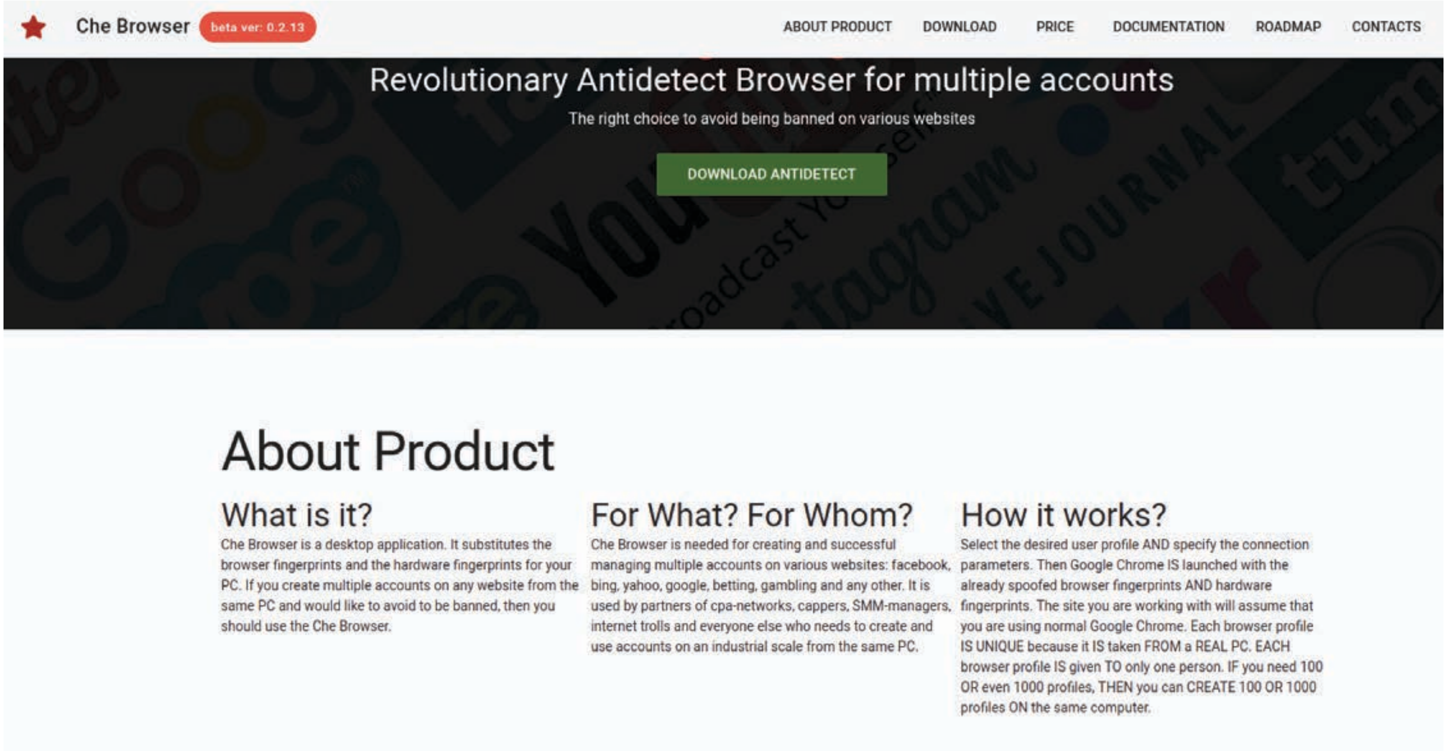
Linken Sphere (ls.tenebris[.]cc) is a Chromium-based web browser that allows cybercriminals to bypass anti-fraud systems of various organizations by imitating real user behavior. The product was launched in July 2017 and quickly obtained high recognition on the dark web due to its substantial functionality, affordability, high-quality technical support, and advertisements across major underground forums. Linken Sphere was first introduced on the Russian-language forums Exploit, Club2CRD, and WWH Club on July 4, 2017, by the threat actor "nevertheless", who is an administrator of the Tenebris Team forum, the official forum of Linken Sphere. The developers offer 3 types of licenses for customers:

- "Light" for $100 per month
- "PRO" for $500 for 6 months, which provides access to the store with configs, including a 1 month free trial of the product
- "Premium" for $900 for 12 months, which provides access to the store with configs and priority service, including a free 3-month trial

AntiDetect (antidetect[.]org) is an anti-detection browser for creating browsers with different configurations. The configuration is a collection of JavaScript files copied by a special method from real browsers. The most popular versions of AntiDetect are 7.7 and 8. According to the developers, AntiDetect v.7.7 is tailored both for professionals and beginners, whereas version 8 is created exclusively for professionals. AntiDetect has been known on the dark web since at least 2013 and was created by the threat actor "bite.catcher". The price for an AntiDetect v.7.7 lifetime license is $600, which is linked to a single machine. The price for the monthly license is $100. To link the existing license to a new PC, users have to pay an additional $100. Updates for the AntiDetect v.7.7 can be free or paid but usually cost $100.

Multilogin (multilogin[.]com) is a tool that provides unique fingerprints and the ability to work with multiple accounts simultaneously. The developers created their own anti-detection browsers called "Mimic" based on Chromium and "Stealthfox" based on Mozilla Firefox browsers. According to Multilogin's owners, creating a browsing profile in Multilogin creates a completely separated virtual browsing environment. Cookies, local storage, and other cache files become completely isolated and cannot leak between profiles. Instead of trying to prevent websites from reading the computer's fingerprint, Multilogin allows reading it but replaces original fingerprints with different ones. Technical support service is available in English, Russian, and Chinese. The service provides the following monthly subscription plans:

- "Solo" (saves up to 100 browser profiles) for $120
- "Team" (saves up to 300 browser profiles and 3 team member seats) for $240
- "Scale" (saves up to 1,000 browser profiles and 7 team member seats) for $482
- "Custom" (saves more than 1,000 browser profiles with additional features upon request) - the price is negotiable.
- "Automate S" (creates and launches up to 5,000 profiles daily) for $242.



Revolutionary Antidetect Browser for multiple accounts

The right choice to avoid being banned on various websites

About Product

What is it?

Che Browser is a desktop application. It substitutes the browser fingerprints and the hardware fingerprints for your PC. If you create multiple accounts on any website from the same PC and would like to avoid to be banned, then you should use the Che Browser.

For What? For Whom?

Che Browser is needed for creating and successful managing multiple accounts on various websites: facebook, bing, yahoo, google, betting, gambling and any other. It is used by partners of cpa-networks, cappers, SMM-managers, internet trolls and everyone else who needs to create and use accounts on an industrial scale from the same PC.

How it works?

Select the desired user profile AND specify the connection parameters. Then Google Chrome IS launched with the already spoofed browser fingerprints AND hardware fingerprints. The site you are working with will assume that you are using normal Google Chrome. Each browser profile IS UNIQUE because it IS taken FROM a REAL PC. EACH browser profile IS given TO only one person. IF you need 100 OR even 1000 profiles, THEN you can CREATE 100 OR 1000 profiles ON the same computer.

Figure 8: Che Browser product description (Source: beta.chebrowser[.]site)

Che Browser (beta.chebrowser[.]site) is a desktop application that substitutes the browser and hardware fingerprints of user PCs. According to a developer's statement, the tool is needed to create and successfully manage multiple accounts on various websites. It is used by partners of CPA networks, cappers, SMM managers, and internet trolls who create and use accounts on an industrial scale from the same PC. The tool allows selecting the desired user profile and connection parameters such as navigator, WebGL, Canvas, window (window value substitution), WebRTC, time zones, media devices, geolocations, fonts, screen objects (screen resolution, number of colors, display orientation), audio context (API interception, value substitution, and fingerprints spoofing). Cybercriminals can use Google Chrome with the already spoofed browser and hardware fingerprints to defraud websites they visit. Each browser profile is unique because it is taken from a real PC, and each browser profile is given to only 1 person. The browser has been actively advertised across multiple dark web forums since at least April 2019 by a threat actor with the usernames "CheBrowser", "Che_Browser", and "gcc". Prices for the service subscription are as follows:

- Daily rental for $5
- Weekly rental for $14
- Monthly rental for $30

Prices for additional services:

- Create a default profile for $1
- Customize profile for a target domain for $1

FraudFox (fraudfox[.]net) is a tool aimed at spoofing browser fingerprints based on a modified Mozilla Firefox web browser. According to the developers, FraudFox is a Windows 7 Enterprise-based virtual machine, which is compatible with VMWare Workstation, VMWare Fusion, and VirtualBox. Users can move and copy it from one location to another, storing it online or on a USB. The browser provides regular updates and 48-hour technical support service. FraudFox does not allow users to save a specific set of fingerprint parameters to match each online account and ensure consistency with every login, and it is not intended to work with multiple accounts. Prices for FraudFox subscriptions are as follows:

- A monthly rental for $100
- A 6 month rental for $450
- A lifetime license for $1,200

Other Popular Anti-Detection Browsers

Besides the aforementioned anti-detection browsers, the following is a list of popular tools with similar functionalities openly advertised on the clearnet.

Anti-Detection Browser	Domain	Monthly Price Range	Technical Functionality
Indigo Browser	indigobrowser[.]com	$120 to $482	The tool has its own unique browser fingerprint database, which allows users to save up to 1,000 transferable fingerprints and create multiple accounts. The product allows working from multiple PCs, and provides unlimited cloud storage. The developers offer 2 browsers, Mimic and Stealthfox. Technical support service is available in Russian.
AntBrowser	antbrowser[.]pro	$27	The tool allows creating multiple accounts with unique IP addresses, UserAgents, TimeZones, Langs, Screen Sizes, Video Cards, and other parameters. Every profile creates and saves its own cookies, cache, and bookmarks. All accounts are transferable and can be synchronized with different devices. Technical support service is available in English and Russian.
AEZAKMI	ru.aezakmi[.]run	1 month subscription: $0 to $249 6 month subscription: $345 to $1,245 12 month subscription: $690 to $2,490	The anti-detection browser provides customers with the option of creating up to 1,000 accounts with unique browser fingerprints and using them simultaneously. The developers offer a free trial version up to 3 accounts. Technical support service is available in English, Russian, and Chinese.
Ghost Browser	ghostbrowser[.]com	$21 to $46 (a free lifetime license is available up to 4 accounts)	Allows creating unlimited identities with unique parameters, proxy servers. Technical support service is available in English.
MultiBrowser	multibrowser[.]com	$199 for a lifetime license	MultiBrowser (formerly Multi-Browser Viewer) is a Windows software application that enables developers to easily test their websites to ensure their correct functionality and rendering across all major web browsers and desktop/mobile devices. MultiBrowser offers a number of standalone web browsers. Each standalone browser is encapsulated, helping for cross-device and cross-browser testing on a single PC, Android, iOS, iPad, etc.
Kameleo	kameleo[.]io	$72 to $242	Kameleo is an anti-detection browser for Windows, iOS, Android OS that allows users to create multiple accounts with consistent browser fingerprints, and history, cookies, proxy connections, and extensions helping with CAPTCHA bypass. Technical support service is available in English.
Accovod	accovod[.]com	$15 (with an annual price of $120)	Accovod, an anti-detection browser that allows creating multiple accounts with unique browser fingerprints and cookies. The tool can work with all popular social media. Technical support service is available in English and Russian.

Anti-Detection Browser	Domain	Monthly Price Range	Technical Functionality
Ivan Iovation	ivanovation[.]ro	1 month subscription: $290 3 month subscription: $777 6 month subscription: $1,314 (with an additional $99 for technical support)	The tool incorporates 14 independent modules that will change the fingerprints of a PC, including hardware, WebGL, WebRTC, Canvas, resolution, fonts, geolocation, flash, plugins, date and time, audio and web camera, peripherals telemetry, web browsers, and profiles. Technical support service is available in English and Russian.
Arbitrage Bets	arbitrage-bets[.]com	$49	Arbitrage Bets for creating multiple accounts that change all system parameters, including hardware, operating systems, browser fingerprints, telemetry, flash, geolocation, etc. It offers customers with Virtual dedicated servers and proxies, as well as the BetStorm browser extension for convenient account management, multi-threading, and smart parameter generation. Technical support service is available in English, Russian, and Chinese.
swSpy Browser	samara-weblab[.]ru	$44.90	This is an anti-detection browser applicable only for Windows OS. At this moment, the service temporarily terminated the registration of new customers. Technical support service is available in Russian.

Many of the aforementioned anti-detection browsers (tools) position themselves as legitimate software released by legitimate legal entities, and not all of them are listed on dark web sources:

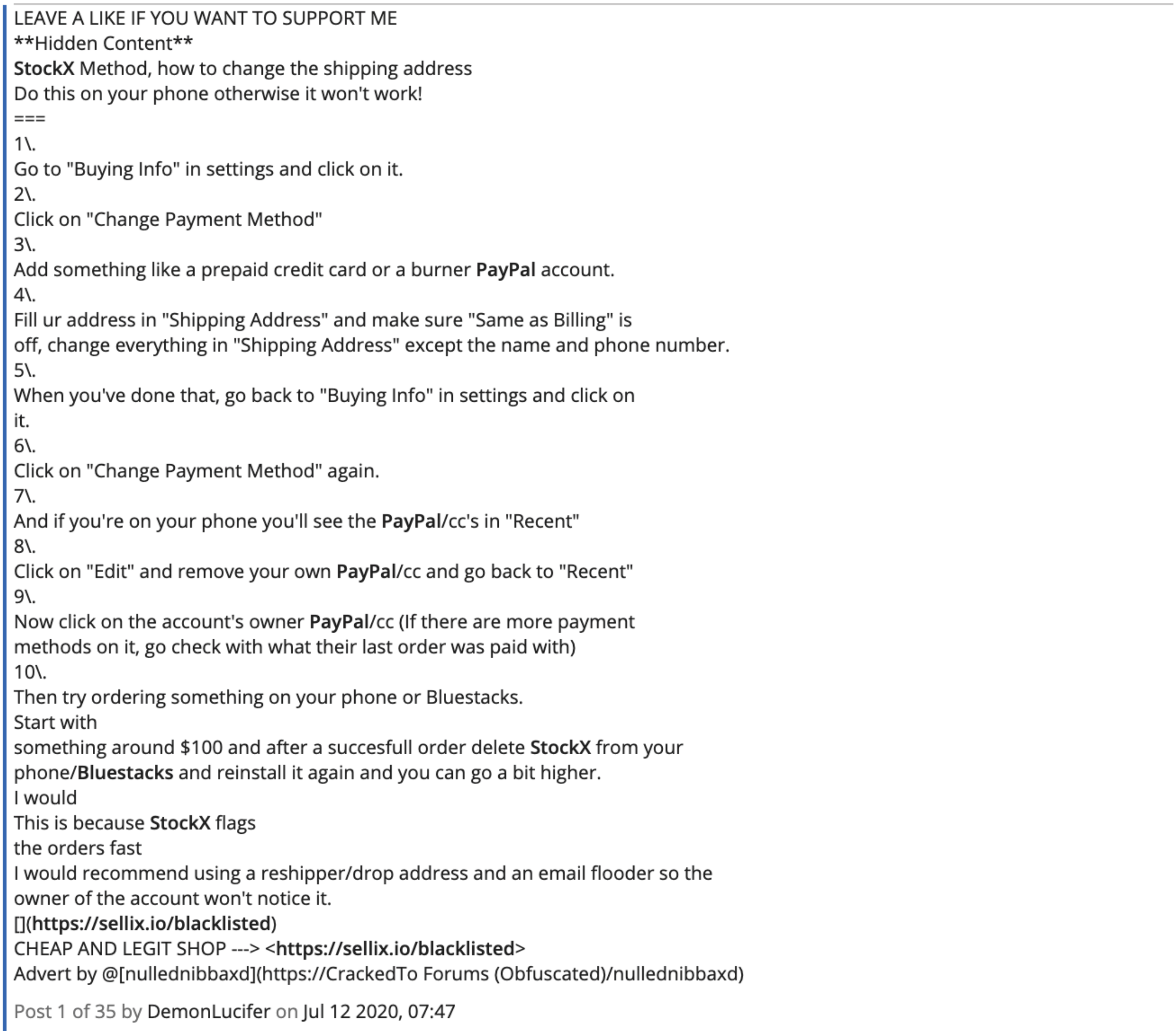
- Multilogin, operated by Multilogin Software Ltd., is located in Tallinn, Estonia
- Ghost browser is located in Denver, US
- MultiBrowser is located in Istanbul, Turkey
- Kameleo, operated by Outis Nemo Ltd., is located in Budapest, Hungary
- Ivan Iovation, operated by Ivan Iovation S.R.L, is located in Bucharest, Romania

Fraud committed with stolen user web browser fingerprints, session cookies, and other system data from compromised host machines is quite popular among cybercriminals. There are a number of dark web shops that offer these types of data for sale, which can be used by cybercriminals to bypass anti-fraud solutions of various organizations. One of the primary platforms on the dark web for the sales of compromised user system data has been Genesis Store, created in 2018 by the threat actor “GenesisStore”. Genesis Store sells packages of compromised account credentials and associated user data designed to allow threat actors to not only obtain the needed credentials but also to bypass anti-fraud solutions by effectively masquerading as the legitimate user since they are accessing the platform from what is, essentially, a copy of the victim’s machine. Victim data is sold in a single package referred to as a “bot”, which includes account credentials, IP address, browser fingerprint (system information), and cookies. After purchasing a bot, the victim data can be imported into a browser plugin called Genesis Security, allowing the attacker to perform an online identity takeover of the victim to perform attacks such as account takeover or card-not-present fraud. The price for each bot varies depending on the number of account credentials, types of accounts, and geographical location of the victim.

Other Forms of Retail Fraud with a Cyber Nexus

Interception Fraud

Though much of e-commerce retail fraud takes place against a victim directly or against an e-commerce platform, interception fraud demonstrates that shipping and logistics companies can also be the subject of a successful fraud attempt. Interception fraud is the act of intercepting physical goods before they are delivered to the individual(s) or physical addresses in an order. The technique involves matching the accurate billing and shipping addresses with the information associated with a stolen payment card upon placing an order on an e-commerce website. In many situations, once the order is placed (typically right before the item is shipped), the threat actor will attempt to alter shipping details to a physical address other than what



```
LEAVE A LIKE IF YOU WANT TO SUPPORT ME
**Hidden Content**
StockX Method, how to change the shipping address
Do this on your phone otherwise it won't work!
===
1\.
Go to "Buying Info" in settings and click on it.
2\.
Click on "Change Payment Method"
3\.
Add something like a prepaid credit card or a burner PayPal account.
4\.
Fill ur address in "Shipping Address" and make sure "Same as Billing" is
off, change everything in "Shipping Address" except the name and phone number.
5\.
When you've done that, go back to "Buying Info" in settings and click on
it.
6\.
Click on "Change Payment Method" again.
7\.
And if you're on your phone you'll see the PayPal/cc's in "Recent"
8\.
Click on "Edit" and remove your own PayPal/cc and go back to "Recent"
9\.
Now click on the account's owner PayPal/cc (If there are more payment
methods on it, go check with what their last order was paid with)
10\.
Then try ordering something on your phone or Bluestacks.
Start with
something around $100 and after a succesfull order delete StockX from your
phone/Bluestacks and reinstall it again and you can go a bit higher.
I would
This is because StockX flags
the orders fast
I would recommend using a reshipper/drop address and an email flooder so the
owner of the account won't notice it.
[](https://sellix.io/blacklisted)
CHEAP AND LEGIT SHOP ---> <https://sellix.io/blacklisted>
Advert by @[nullednibbaxd](https://CrackedTo Forums (Obfuscated)/nullednibbaxd)

Post 1 of 35 by DemonLucifer on Jul 12 2020, 07:47
```

Figure 9: DemonLucifer explaining an interception scam targeting StockX customers (Source: Recorded Future)

was originally listed, typically one accessible to the threat actor or an associate, so that the goods can be successfully picked up by then all while the victim is left paying for the goods. This can be achieved by contacting customer service of the target e-commerce website, or, in the event that a good has shipped to the victim's shipping address, a threat actor who likely has all of the relevant shipping details (tracking number, name, address) will contact the shipping company directly to request rerouting the package elsewhere.

Triangulation Fraud

E-commerce retail fraud has proved itself to be a multifaceted threat for businesses and individuals, and it can be hard to detect when the scam is presented under the guise of a legitimate marketplace with real customers. It is this premise that makes triangulation fraud particularly difficult to detect from the perspective of an e-commerce website, and the end result generally leaves a victim left out to dry. Triangulation fraud is a form of fraud in which an unsuspecting, legitimate customer purchases and receives a product from a third-party marketplace operated by a fraudster, while the product was purchased through an actual retailer using stolen payment information. Triangulation fraud attacks are likely to target products considered to be easy to sell, such as electronics, household supplies, pet products, and clothing.

According to the 2018 "Fraud Glossary" on SkyFraud Forum, triangulation fraud is "considered as one of the most complex e-commerce attack methods, [and] involves three points":

- An unsuspecting customer who places an order on an auction or marketplace using some form of credit, debit, or PayPal tender
- A fraudulent seller who receives the order and then places the order for the actual product with a legitimate e-commerce website using a stolen credit card
- A legitimate e-commerce website that processes the criminal's order

As noted by Brian Krebs in 2015, triangulation is one of many techniques with which a fraudster can "cash out" stolen credit card information. Through "buy now" options or auction sites such as eBay, a fraudster can advertise a product at a strongly discounted rate despite typically not possessing the good until the purchase is made or auction has concluded. The threat actor then purchases the goods through a retailer using previously stolen credit card information and then ships it directly to the purchaser or auction winner. The victim of the initial theft is then left to dispute the suspicious charge(s) with the retailer.

The visual in Figure 10 is dated; however, given the surge in international dependency in e-commerce due to COVID-19, we believe triangulation fraud likely has proved itself as a lucrative opportunity for fraudsters looking to capitalize. This may be especially true for heavily in-demand goods amid international shortages (for example, toiletries or new game consoles), and triangulation fraud is likely evolving by integrating with other emerging forms of fraud targeting a new, unsecure, and dynamic e-commerce environment (namely curbside pickup/BOPIS).

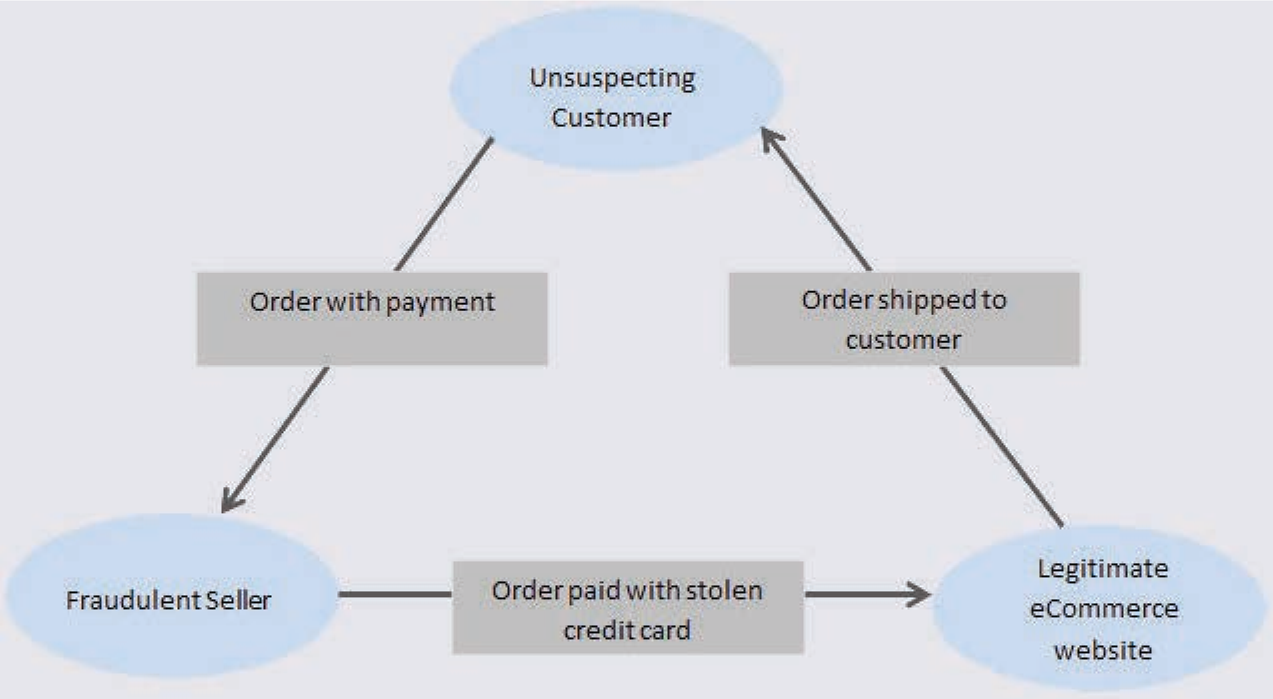

Unsuspecting Customer
Order with payment
Order shipped to customer
Fraudulent Seller
Order paid with stolen credit card
Legitimate eCommerce website

Figure 10: A diagram demonstrating triangulation fraud (Sources: Krebs on Security, eBay)

Outlook and Mitigations

In 2021 and for the foreseeable future, we believe that the sale of compromised customer data and account information, credential stuffing tools, and refund fraud tutorials will each likely remain among the most serious threats targeting online retail organizations and e-commerce platforms. Looking ahead, threat actors likely will continue to use dark web marketplaces, forums, and shops to advertise compromised victim PII, account information and rewards, and payment or gift cards. Threat actors advertising these commodities seemingly do not target specific retailers exclusively, instead regularly selling similar data from many retail and e-commerce entities.

There are several mitigation techniques retail organizations can use to minimize the risk of or potentially avoid online retail fraud:

- Use threat intelligence to monitor underground discussion of one’s enterprise, such as discussion of customer account information for sale. Stay abreast of current retail fraud trends and techniques discussed among criminal threat actors.
- Deploy multi-factor authentication (MFA) across customer and employee login portals.
- At checkout, ensure a customer’s IP address and geolocation match with shipping and billing information on file or are in an acceptably close proximity.
- Do not ship an order before it is fully validated, verified, and processed. Additionally, discourage or limit whether or when a customer can change a shipping address once the order is fully processed.
- Require tracking numbers and signatures for purchases above a certain dollar amount.
- Encourage customers to regularly monitor their accounts for theft or account takeover of loyalty rewards or gift balances.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.