TERBIUM LABS

RESEARCH REPORT

DATA:

THE BUSINESS WORLD'S MOST VULNERABLE COMMODITY

April 2020

terbiumlabs.com | contact@terbiumlabs.com

TABLE OF CONTENTS

INTRODUCTION

The internet is a powerful place for connecting buyers with sellers – and it's led to the meteoric rise of ecommerce giants like Amazon and eBay. Known for their competitive pricing, speed-of-light shipping and reliable customer service, these big box retailers have sealed their place in consumers' minds as the best place to do their online shopping. And selling on these sites is undeniably a viable way to make money. In fact, 61 percent of Amazon sellers said their profits increased in 2019 and 92 percent plan to continue to sell on Amazon in 2020.

Over the years, cyber criminals have been hard at work to create the same type of explosive growth on the dark web. This has led to the rise of major dark web marketplaces, where criminals can buy anything you can think of – drugs, counterfeit currency, illegal pharmaceuticals, stolen data and a variety of other illicit goods. For the purpose of this report, we'll focus on the stolen data on three of the largest dark web marketplaces. What you need to understand is that data comes in many forms. On the one hand, there's personal and financial data – from emails, addresses and zip codes to credit/debit card data, account details and online credentials. On the other hand, there's the "how-to" type of data – fraud guides, templates and tools that give criminals the knowledge they need to use the stolen data to gain access to systems, commit financial fraud, launch phishing attacks and more.

What's most noteworthy is that cyber criminals have completely transformed the operational structure of the dark web marketplace to mimic big box retailers like Amazon and eBay – complete with search capabilities, ecommerce (including escrow options and Bitcoin) and seller ratings. As we'll outline in this report, the data itself is relatively easy and cheap (and the value decreases over time). But the fraud guides and templates (and the knowledge contained within them) sold on dark web marketplaces are far more valuable and can lead to even greater damage, as it gives criminals the tools to turn commodity data into financial crime.

In this report, we will examine the costs of buying and selling data, the different categories of data that are sold on these marketplaces and the 'dark' business of creating, distributing and selling fraud guides, tools and templates to enable a multitude of specific, targeted attacks. We will also provide examples of how the damage and risk of repeat exposure increases progressively over time.

SURVEY METHODOLOGY & OBJECTIVES

We analyzed goods for sale on the dark web from today's three top major multi-good marketplaces – "The Canadian HeadQuarters," "Empire Market," and "White House Market." In the analysis we present the aggregated data, which is representative of the distribution of goods for sale amongst other major multi-good marketplaces. Ultimately the goods for sale on these types of dark web marketplaces are fairly consistent and commoditized, but because each market organizes itself, and its goods, slightly differently, we created standard categories to accurately present the makeup of these retailers' listings.

DATA

- **Personal Data**
- **Accounts & Credentials (Financial)**
- **Accounts & Credentials (Other)**
- **Payment Cards**
- **Tools & Templates**
- **Fraud Guides**
- Services
- Drugs

We then surveyed each listing on the two markets (23,862 in aggregate) and assigned each to one or more categories. For the sake of accuracy, when a listing was assigned to multiple categories, its contribution was weighted proportionately. The appropriate category was impossible to determine for approximately 1200 listings, and that data was discarded.

LISTING CATEGORIES

We examined three specific “big box” marketplaces, consisting of all types of goods that are sold and bought by cybercriminals. These categories and the percentages within these types of marketplaces are not representative of the dark web at aggregate. What they provide insight into is the commoditized world of goods for sale with microtransaction available to the masses of cybercriminals whether they are novices or highly sophisticated.

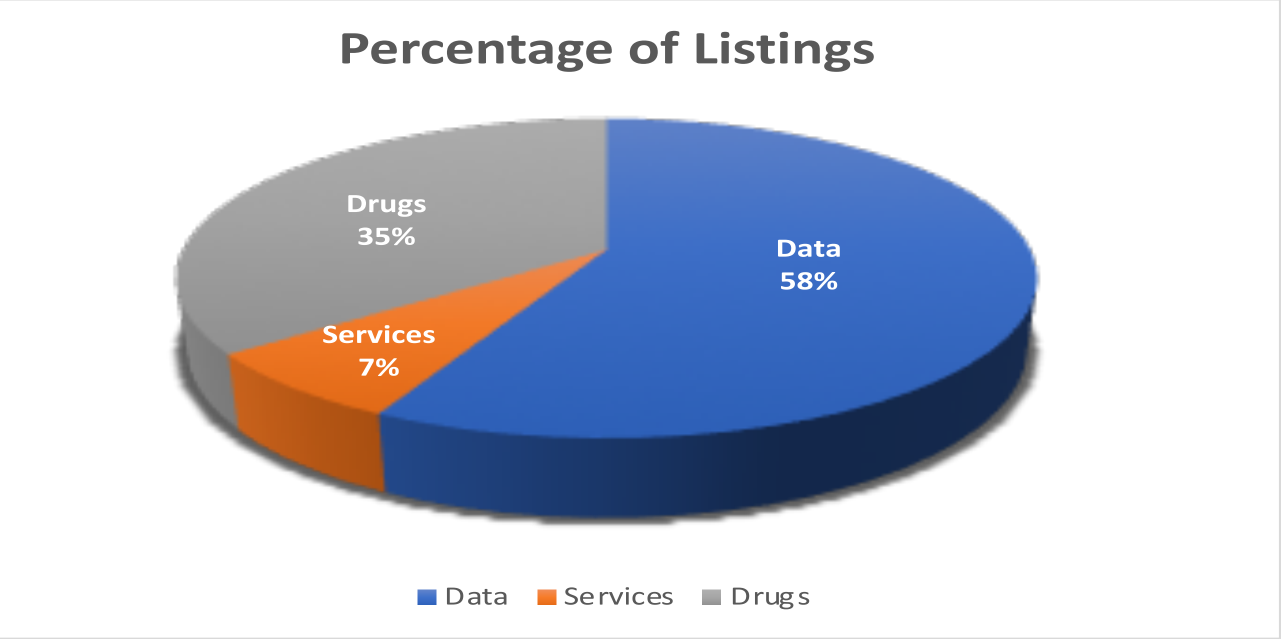
The types of listing are grouped into the following categories with the following descriptions:

- Data: Any personal data, financial data, organizational data, credentials or materials that are leveraged to further expose individuals or organizations to further fraud or misuse.

- Services: Any “for hire” activities, ranging from DDoS services to dark web hosting to offers to write specific malware at the buyers’ request.

- Drugs: Any illegal, illicit or legal drugs available without a doctor’s prescription.

For the purposes of this research, Services and Drugs were only categorized. No further analysis was completed as part of this research. The results are not representative of the dark web as a whole — other complete markets are exclusively drug focused and based on our previous research we estimate that approximately 50% of the goods for sale on the dark web are drug or substance related. The markets we selected for analysis represent large, multi-good marketplaces likely to stock data damaging to corporations.



DATA LISTING CATEGORIES

We then analyzed six categories of data, which include personal data, payment cards, accounts and credentials (financial), accounts and credentials (other), fraud guides, and fraud tools and templates. (We go into more detail on how we define each category below.) Fraud guides, tools and templates are often resources organizations overlook when identifying digital risks. The materials within these are data-driven insights that allow even the most novice cybercriminal the ability to develop and execute activities targeted at individuals and organizations alike. As a result, these materials have been incorporated into the “data” category because they are, in fact, data.

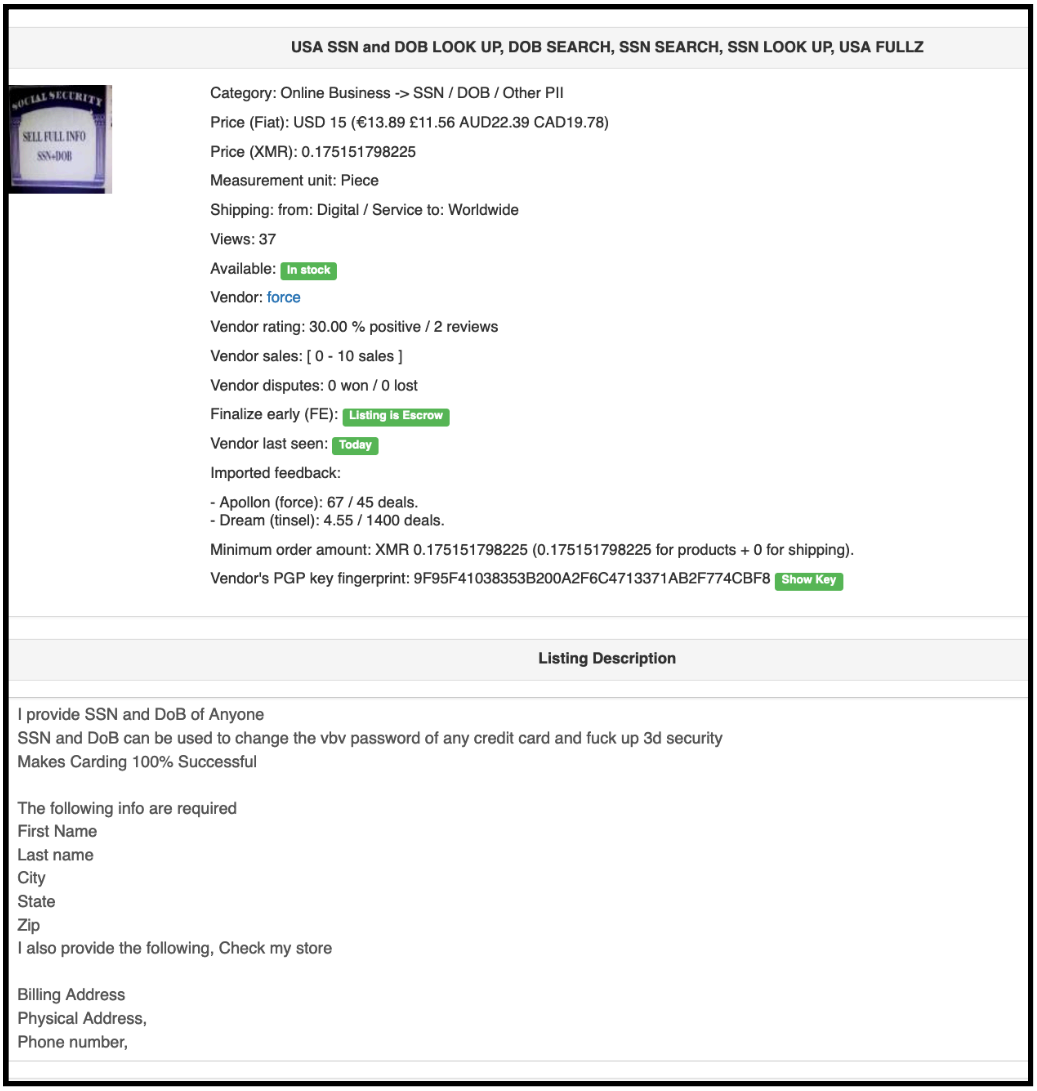
Data Categories

- **Personal Data:** This includes information, such as names, addresses, social security numbers. But it doesn’t include actual account credentials.
- **Payment Cards:** This includes information from actual debit/credit cards, which can be used to execute fraudulent transactions.
- **Accounts & Credentials (Financial):** This includes usernames and passwords for bank/credit card accounts (i.e. Stripe, PayPal, Online banking, etc.).
- **Accounts & Credentials (Other):** This includes accounts with other types of credentials that are valid for everything, except for financial purposes (i.e. Netflix, Domino’s, CrunchyRoll, etc.).
- **Fraud Guides:** This category includes all listings purporting to sell a process - for example, how to open a fraudulent account at a specific financial institution.
- **Fraud Tools & Templates:** This can include a fake mobile app that looks almost identical to a reputable banking institution. Criminals can then use and send the link to the fake app in phishing attacks. And, this category also includes fake HTML templates that allow cybercriminals to build and launch fake websites that look similar to actual retail and/or banking websites.

CATEGORY	% OF DATA LISTING	DIGITAL RISKS POSED BY LISTING
Personal Data	15.6%	Phishing, Business Email Compromise, Account Takeover
Accounts & Credentials - Financial	8.2%	Account Takeover, Fraud, Credential Harvesting
Accounts & Credentials - Other	12.2%	Account Takeover, Fraud, Credential Harvesting
Payment Cards	7.0%	Fraud
Tools & Templates	8.0%	Various Cybercriminal Activities, Fraud
Fraud Guides	49.0%	All of the Above

PERSONAL DATA

Amount of Data & Cost: According to our analysis, personal data ranks as the number one type of data being sold on the dark web, at 15.6 percent. We also found that the average price for a single personal record was $8.45. When you think about how that's already too affordable for cybercriminals, the prognosis is far worse. In fact, the cost of a single personal record on dark web marketplaces can dip as low as just $1 – that's less than the price of a pack of gum.



USA SSN and DOB LOOK UP, DOB SEARCH, SSN SEARCH, SSN LOOK UP, USA FULLZ

Category: Online Business -> SSN / DOB / Other PII

Price (Fiat): USD 15 (€13.89 £11.56 AUD22.39 CAD19.78)

Price (XMR): 0.175151798225

Measurement unit: Piece

Shipping: from: Digital / Service to: Worldwide

Views: 37

Available: In stock

Vendor: force

Vendor rating: 30.00 % positive / 2 reviews

Vendor sales: [0 - 10 sales]

Vendor disputes: 0 won / 0 lost

Finalize early (FE): Listing is Escrow

Vendor last seen: Today

Imported feedback:

- Apollon (force): 67 / 45 deals.
- Dream (tinsel): 4.55 / 1400 deals.

Minimum order amount: XMR 0.175151798225 (0.175151798225 for products + 0 for shipping).

Vendor's PGP key fingerprint: 9F95F41038353B200A2F6C4713371AB2F774CBF8 Show Key

Listing Description

I provide SSN and DoB of Anyone
SSN and DoB can be used to change the vbv password of any credit card and fuck up 3d security
Makes Carding 100% Successful

The following info are required
First Name
Last name
City
State
Zip
I also provide the following, Check my store

Billing Address
Physical Address,
Phone number,

What the Data Means: This type of data includes information that is not directly tied to a login or financial data. For example, exposed personal data could include names, addresses, phone numbers, email addresses, zip codes and social security numbers.

Risks to Your Business: When this type of data is purchased by criminals, it exposes organizations to a variety of digital risks, such as phishing attacks, business email compromise and account takeovers. Phishing attacks, for example, are often used to steal personal data, such as login credentials, and occur when an attacker masquerading as a trusted entity sends a malicious email, instant message or text. If and when a user opens a phishing email, the criminal can then access personal information to open new bank accounts/credit cards and steal the identity of the user.

Business email compromise (BEC) is one of the more sophisticated types of scams, whereby criminals target businesses and individuals for a transfer of funds. For instance, an employee who works in the finance department of a global company could receive a scam email from a criminal, which purports to be from a customer or vendor asking for payment of fees. The email could be designed to look just like an email would from the vendor. So if an employee has the ability to transfer funds in and out of the company's bank account, attackers will target them to get them to move money from the business account to the account of the attacker. If the business email compromise left a senior executive's data exposed, this could give attackers more leverage when impersonating bank executives in a phishing campaign.

What To Do When Alerted to Risks: This content exposes organizations to a variety of threats, as the information involved enables criminals to both target individuals more accurately, as well as impersonate them. That's why it's vital to alert businesses to data theft early (and in real-time) so they have the opportunity to flag the data as compromised and prevent criminals from further using the stolen data to verify their identity (for fraudulent activities/accounts).

Moreover, when evaluating threats such as phishing attacks or business email compromise, the IT department can take proactive measures to add two-factor authentication, force password resets and increase security and monitoring of those individuals. And, because it's important for senior-level executives to be made aware of the exposure and to be cautious/suspicious of the appearance of that data in future emails, providing reporting on these proactive measures can further minimize exposed data being used to further attack. By doing so, that will likely thwart phishing attempts being made by cybercriminals.

PAYMENT CARDS

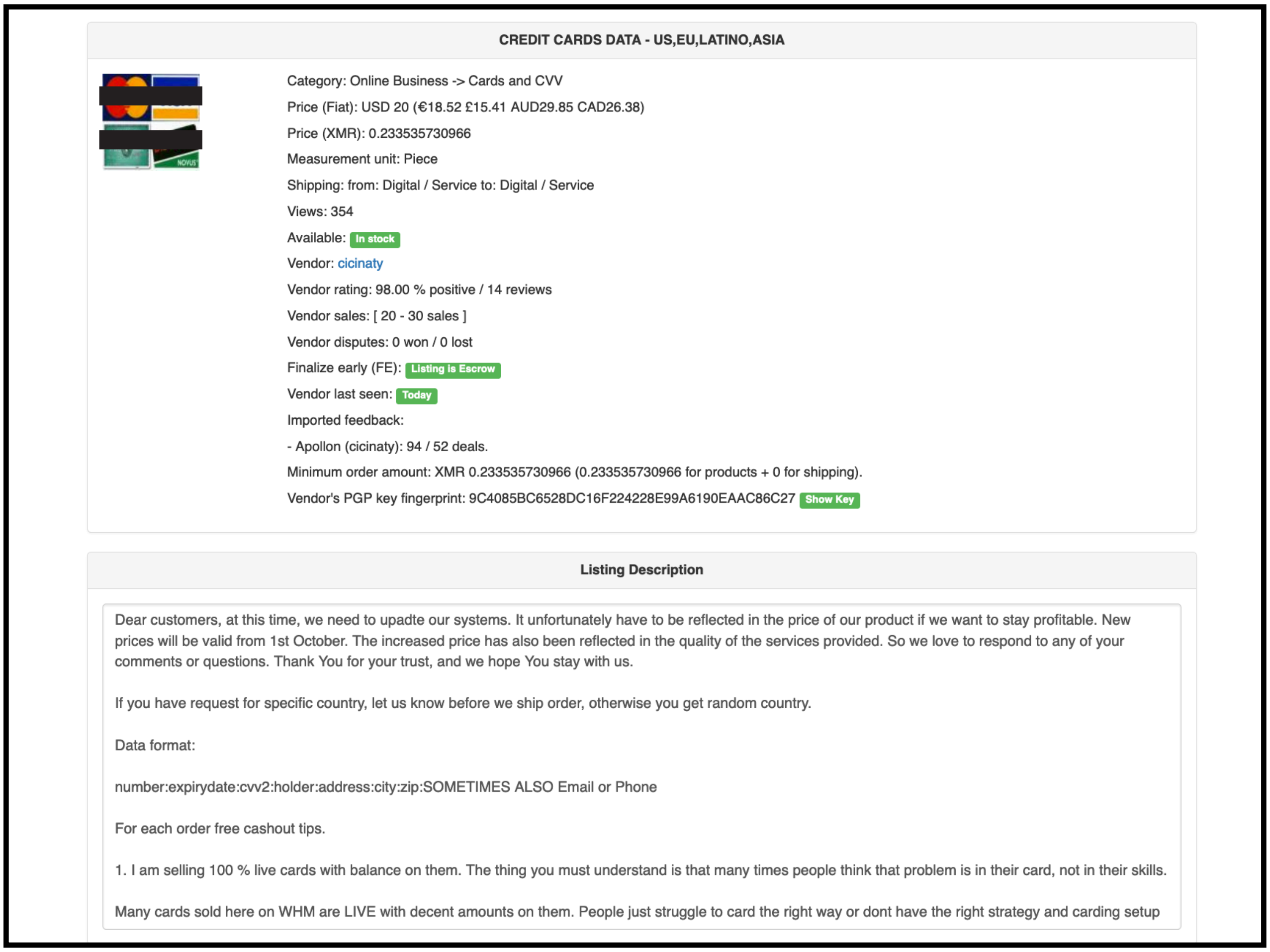
Amount of Data & Cost: Payment card data accounts for 7 percent of the stolen data on the dark web marketplaces we examined. The price for payment cards ranged from as low as $1 to as high as $200 per card, with an average price per card of $18. Similar prices were fetched for payment card data being sold from the 2019 Wawa data breach.

What the Data Means: This includes listings for payment cards (credit or debit) that are up for sale, accompanied by varying degrees of personal data as well that may be needed to make full use of the stolen payment card data. To put this into context, over 23 million credit and debit cards were for sale in dark web forums in the first half of 2019, according to cybersecurity firm Sixgill's Underground Financial Fraud Report.

Risks to Your Business: When sold on the dark web, this type of data opens up users to various types of fraud. If businesses (i.e. retailers, financial institutions) aren't alerted to the fraud early on, it can lead to a serious data breach, which can then expose millions of data records. Credit card fraud increased by 18.4 percent in

2018 and is still climbing. This is a huge problem for financial institutions.

At the same time, card not present (CNP) fraud is now 81 percent more likely to occur than point-of-sale fraud. Why is that important, you ask? As the rate of CNP fraud is on the rise and the average stolen payment card costs are relatively low (between $18 and $200), the risk of exposure will certainly be magnified. If financial institutions and retailers aren't alerted to the exposure of the stolen data quickly, their customers could end up losing large amounts of money, having their identities stolen and even facing criminal charges as a result.



[redacted]

[redacted]

CREDIT CARDS DATA - US,EU,LATINO,ASIA

Category: Online Business -> Cards and CVV
Price (Fiat): USD 20 (€18.52 £15.41 AUD29.85 CAD26.38)
Price (XMR): 0.233535730966
Measurement unit: Piece
Shipping: from: Digital / Service to: Digital / Service
Views: 354
Available: In stock
Vendor: cicinaty
Vendor rating: 98.00 % positive / 14 reviews
Vendor sales: [20 - 30 sales]
Vendor disputes: 0 won / 0 lost
Finalize early (FE): Listing is Escrow
Vendor last seen: Today
Imported feedback:
- Apollon (cicinaty): 94 / 52 deals.
Minimum order amount: XMR 0.233535730966 (0.233535730966 for products + 0 for shipping).
Vendor's PGP key fingerprint: 9C4085BC6528DC16F224228E99A6190EAAC86C27 Show Key

Listing Description

Dear customers, at this time, we need to upadte our systems. It unfortunately have to be reflected in the price of our product if we want to stay profitable. New prices will be valid from 1st October. The increased price has also been reflected in the quality of the services provided. So we love to respond to any of your comments or questions. Thank You for your trust, and we hope You stay with us.

If you have request for specific country, let us know before we ship order, otherwise you get random country.

Data format:

number:expirydate:cvv2:holder:address:city:zip:SOMETIMES ALSO Email or Phone

For each order free cashout tips.

1. I am selling 100 % live cards with balance on them. The thing you must understand is that many times people think that problem is in their card, not in their skills.

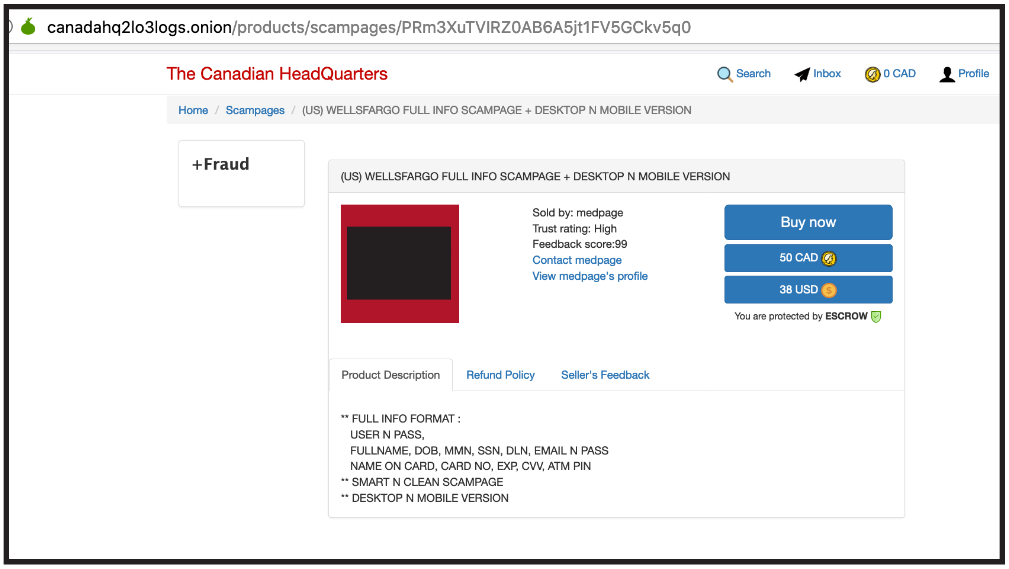
Many cards sold here on WHM are LIVE with decent amounts on them. People just struggle to card the right way or dont have the right strategy and carding setup

There's no doubt that credit card fraud can be damaging for consumers. But while consumers are typically protected against fraudulent purchases made on their debit/credit cards, businesses are often left to cover the costs of those transactions and chargeback fees.

What To Do When Alerted to Risks: When stolen payment cards are detected, organizations can immediately take action to shut down the card before payment card fraud occurs or significant losses occur. These mitigation strategies allow organizations to decrease the overall losses for consumers and financial institutions alike. Organizations can either hire skilled experts to monitor the dark web or leverage software to continually monitor and detect exposure and risk levels in real-time. Having lax procedures could do serious damage to organizations' reputations, customer trust, revenue and long-term growth.

ACCOUNTS & CREDENTIALS - FINANCIAL

Amount of Data & Cost: Accounts and credentials (financial) make up 8.2 percent of the stolen data on these dark web marketplaces. Our analysis found that listings in this category sold for an average of $33.16 per record, with some selling for as low as $5 and others being priced as high as $500.


canadahq2lo3logs.onion/products/scampages/PRm3XuTVIRZ0AB6A5jt1FV5GCkv5q0
The Canadian HeadQuarters
Search
Inbox
0 CAD
Profile
Home / Scampages / (US) WELLSFARGO FULL INFO SCAMPAGE + DESKTOP N MOBILE VERSION
+Fraud
Buy now
50 CAD
38 USD
Product Description
Refund Policy
Seller's Feedback

(US) WELLSFARGO FULL INFO SCAMPAGE + DESKTOP N MOBILE VERSION

[redacted]

Sold by: medpage
Trust rating: High
Feedback score:99
Contact medpage
View medpage's profile

You are protected by **ESCROW**

** FULL INFO FORMAT :
USER N PASS,
FULLNAME, DOB, MMN, SSN, DLN, EMAIL N PASS
NAME ON CARD, CARD NO, EXP, CVV, ATM PIN
** SMART N CLEAN SCAMPAGE
** DESKTOP N MOBILE VERSION

What the Data Means: This category includes account logins for BFSI (banking, financial services and insurance) related accounts, such as bank accounts, payment card accounts, or PayPal accounts. If you think about the costs of these types of records, coupled with the types of digital risks that result from the data being sold on the dark web, businesses cannot afford to be complacent or reactive in monitoring and detecting their digital risk. Doing so would not only lead to various types of fraud for their customers, but it would also severely damage their customer trust, relationships and brand reputation.

Risks to Your Business: This type of data, when stolen and sold on the dark web, can leave both users and businesses vulnerable to certain types of digital risks, such as account takeover, fraud and credential harvesting. It's important to understand that account takeover fraud is not the same as identity theft. Account takeover is when criminals obtain a legitimate user's account details to take over their online accounts. The goal of account takeover fraud is to make a profit by using the value in the account.

Credential harvesting, also known as password harvesting, is related to phishing, but isn't the same thing. For example, a criminal could use a phishing email with a weaponized Microsoft Word document. When the intended recipient opens the Word document, it runs a macro that downloads credential-harvesting malware. But the recipient, in all likelihood, would never even know that their credentials have been stolen.

In 2018, Iowa's UnityPoint Health confirmed that it was the victim of a credential-harvesting attack, which put the sensitive information of 1.4 million patients at risk. What's especially worrying about this data breach is that the criminals tricked some employees into shared their confidential log-in credentials of one of the company's trusted executives, giving attackers access to their internal email accounts from the period of March 14, 2018 through April 3, 2019. Given that the criminals had access to data in the business email accounts for over a year, the risk spread across the affected email accounts as well as its customers, partners, vendors and larger employee base.

What To Do When Alerted to Risks: When an account takeover is launched, a criminal can do a number of activities – from updating billing/shipping address to changing account passwords to making fraudulent purchases (ecommerce, retailers) and even moving money to other accounts. The repercussions for failing to monitor and detect an account takeover can be severe for financial institutions and retailers. It can lead to an increase in chargebacks on accounts, an increase in customer complaints/transaction disputes, a decrease in customer trust, damage to the brand's reputation and customer churn.

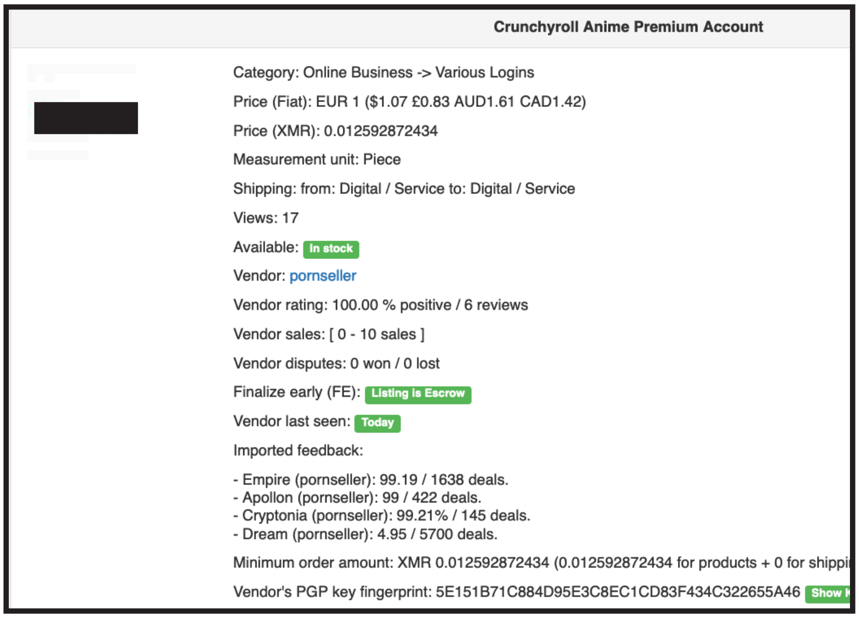
ACCOUNTS & CREDENTIALS - OTHER

Amount of Data & Cost: This type of data accounts for 12.2 percent of the stolen data on the three dark web marketplaces we analyzed. The price of this type of data is quite varied – ranging from as low as $1 all the way up to $973, with an average price of $7 per account.

What the Data Means: This category includes all other types of credentials, which typically covers services like online streaming services, pizza delivery and even pornography.

Risks to Your Business: Stolen or leaked credentials expose organizations to a variety of risks. If those credentials belong to your organization, they represent compromised accounts, which must immediately be secured.

What To Do When Alerted to Risks: Understanding which accounts are compromised is the first step in this process. Even if the credentials in question belong to another organization, your organization still needs to be aware. Credential reuse is as much a problem as ever, and an account that belongs to your customer on another service or with another institution may still share credentials, personal data, or security questions with that customer's account on your service. Understanding that the other service has been compromised allows you to proactively make the changes necessary to secure that user's account on your service.



Crunchyroll Anime Premium Account

[redacted]

Category: Online Business -> Various Logins

Price (Fiat): EUR 1 ($1.07 £0.83 AUD1.61 CAD1.42)

Price (XMR): 0.012592872434

Measurement unit: Piece

Shipping: from: Digital / Service to: Digital / Service

Views: 17

Available: In stock

Vendor: pornseller

Vendor rating: 100.00 % positive / 6 reviews

Vendor sales: [0 - 10 sales]

Vendor disputes: 0 won / 0 lost

Finalize early (FE): Listing is Escrow

Vendor last seen: Today

Imported feedback:

- Empire (pornseller): 99.19 / 1638 deals.
- Apollon (pornseller): 99 / 422 deals.
- Cryptonia (pornseller): 99.21% / 145 deals.
- Dream (pornseller): 4.95 / 5700 deals.

Minimum order amount: XMR 0.012592872434 (0.012592872434 for products + 0 for shippi

Vendor's PGP key fingerprint: 5E151B71C884D95E3C8EC1CD83F434C322655A46 Show

FRAUD GUIDES

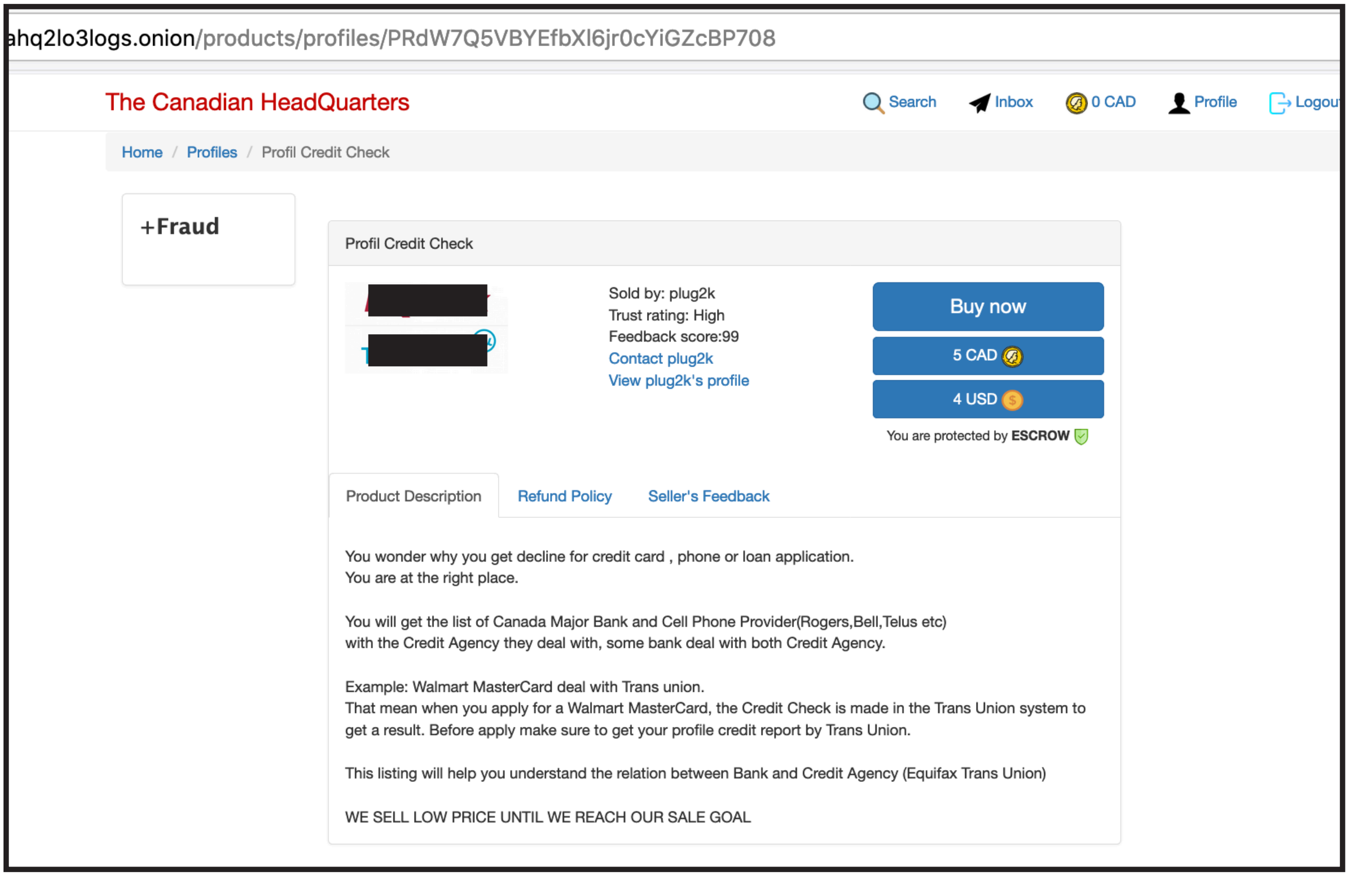
Amount of Data & Cost: Fraud guides are, by far, the most frequently sold category of data on dark web marketplaces, at 49 percent. The average cost of a single guide is $3.88, whereas a collection of guides sold under a single listing costs $12.99. The average price across all listings was $7.80.

What the Data Means: This category includes all listings purporting to sell a process - for example, how to open a fraudulent account at a specific financial institution.

Risks to Your Business: This category targets organizations in a variety of ways. What they have in common is detailed information on how to export an organizations' current policies. Oftentimes, the content in fraud guides doesn't require any prior knowledge from the reader (criminal) and can realistically lead to successful execution of the outlined steps.
Understanding their appearance on the Internet and contents is immediately actionable, as it allows organizations to change vulnerable policies before they can be exploited at scale.

It's advantageous for organizations to think that many guides are fraudulent. Here's why. Criminals who purchase a fraud guide from a seller typically have relatively little confidence that a guide is accurate. So as soon as a guide is tested, if it proves unreliable, they will immediately lose faith in the seller's credibility. This is a good thing for businesses – if a business purchases a fraud guide early, they can change the affected internal policies immediately and thereby, render that fraud guide useless. As a result, the seller of that fraud guide will be discredited and likely deemed untrustworthy by other criminals.

What To Do When Alerted to Risks: One of the first steps to minimize the risk is to understand the parameters of the dark web as best as possible – or to add people to the teams with the necessary knowledge and skills. Fraud guides shouldn't be underestimated, yet they often are. Of course, knowledge of how the dark web works isn't enough. Organizations must implement a plan to track their data in real-time so they can understand the ways in which it could potentially be compromised – and act fast if and when the compromise occurs. From there, they should then conduct an in-depth analysis into the types and amounts of data that were exposed, where the exposure occurred and the varying levels of risk to their organization, customers and employees.



ahq2lo3logs.onion/products/profiles/PRdW7Q5VBYEfbXl6jr0cYiGZcBP708

[redacted]

[redacted]

Sold by: plug2k
Trust rating: High
Feedback score:99
Contact plug2k
View plug2k's profile

You are protected by **ESCROW**

You wonder why you get decline for credit card , phone or loan application.
You are at the right place.

You will get the list of Canada Major Bank and Cell Phone Provider(Rogers,Bell,Telus etc)
with the Credit Agency they deal with, some bank deal with both Credit Agency.

Example: Walmart MasterCard deal with Trans union.
That mean when you apply for a Walmart MasterCard, the Credit Check is made in the Trans Union system to get a result. Before apply make sure to get your profile credit report by Trans Union.

This listing will help you understand the relation between Bank and Credit Agency (Equifax Trans Union)

WE SELL LOW PRICE UNTIL WE REACH OUR SALE GOAL

TOOLS & TEMPLATES

Amount of Data & Cost: Tools and templates account for 8 percent of stolen data on the dark web marketplaces we analyzed. These listings ranged in price from $2 to $724, with an average price of $52.

What the Data Means: This category includes software that enables other criminals to commit crimes. Examples include source code for “Scampages” or fraudulent mobile applications, as well as documents such as Photoshop templates. Templates are typically for fraudulent documents and can include anything from passports to bank statements of a specific financial institution.

Risks to Your Business: The value of fraud guides is increased exponentially with the added offering of tools and templates. While fraud guides provide how-to instructions to help criminals access stolen data, tools and templates simplify, automate and speed up the process by which they can launch attacks based on the content in the fraud guides. So the combination of fraud guides with tools and templates significantly increases the level of risk to organizations.

One example of a tool is a fraudulent mobile app. This is an unauthorized Android or iOS app that mimics the logo, branding and functionality of a legitimate business – all for the purpose of scamming users into downloading the fake app onto their mobile device. Once installed, the fraudulent mobile app is typically programmed to carry out several malicious actions depending on the design/intent of the criminal. It’s also not uncommon to see several hundred iterations of the same fraudulent mobile apps created, which can net the criminal with a significant stream of revenue.

Meanwhile, a cybercriminal could buy a fake HTML template on the dark web that makes it easy to build and launch fake websites that look similar to actual retail and/or banking sites. This is dangerous because a criminal could build a fake banking or retail website that’s then used in phishing scams, the sale of fraudulent goods and even to spread misinformation. Fraudsters could use these fake websites when emailing suppliers to order high-value goods on extended payment terms.

Amidst the current Coronavirus outbreak, the use of fake websites to spread misinformation can have catastrophic effects on society – and for the organization’s reputation. For example, the Digital Shadows Photon Research team recently found that attackers have been observed tempting victims with URLs or document downloads using promises of important safety documentation or infection maps.

What To Do When Alerted to Risks: The best defense is to establish robust policies and procedures that ensure a second set of eyes (and tools) can constantly monitor and validate business transactions and requests for goods, services or payments. It also requires organizations to provide education and training to their employees so that they are aware of the types of fake websites, apps and phishing emails that could be used by cybercriminals. Without that education, employees will inevitably leave corporate data at risk.

CONCLUSION

As we've outlined in this report, selling stolen data is a booming business for cybercriminals. In fact, cybercriminals earned a total of around $600 billion in 2018, according to Cybersecurity Ventures. As troubling as this is, it's even more disturbing that the dark web marketplace operates similarly to big box retailers like Amazon and eBay. Just as these legitimate big box retailers have become the go-to source for online shopping among consumers, these illegitimate, 'dark' marketplaces have built up their reputation as the go-to source for online shopping – except just for stolen and illegitimate goods.

The difference between legitimate big box retailers and those found on the dark web is the constant rise and fall of the marketplaces. Just in the last few years, should we have analyzed the top three marketplaces, we would have included Hansa, Dream Market and AlphaBay. However, all three have been shut down by law enforcement within the past several years. Therefore, a great challenge for organizations is the continuous monitoring within the changing marketplaces and forums.

The risks to businesses are made exponentially worse as the price of stolen records is so incredibly cheap (sometimes as low as $1), and it is easy for criminals to get their hands on fraud guides, tools and templates that give them the know-how to use the stolen data to commit a variety of attacks and scams. This means that it's currently easy for criminals to cause more damage than the cost of the data they need to do their work. It's imperative that organizations take a proactive, diligent approach to monitoring and detecting for their employee, customer and proprietary data, in addition to their brand.

Knowing that selling stolen data is such a profitable business, cybercriminals have targeted and will continue to pursue targets who they perceive to be weak or ill-equipped to protect themselves (and their customers). And, because so many data sets, once available, become repurposed and repackaged by cybercriminals, continuously monitoring and detecting for data allows organizations to mitigate their digital risks. By identifying stolen or leaked information on the Internet quickly, effectively and securely, organizations can become increasingly more aware of the areas of digital risks and threats. Whether it's finding exposed data or guides targeting operational processes, organizations can take action to prevent ongoing attacks. In turn, organizations stay ahead of such risks and mitigate the potential types and amounts of damage that could ensue.

There are tools and software available to provide access to the automation required to continuously discover new sites and new data on existing sites. As markets disappear and re-appear, IT teams can maintain visibility of their digital risks across the dark web. Ongoing monitoring of your organization's specific data (e.g. customer PII, employee PII and propriety) is critical and will allow organization to compare millions of web pages, many that are password protected and difficult to access, to your data to detect and mitigate digital risks.

ABOUT TERBIUM LABS

Terbium Labs empowers organizations to reduce the risk of inevitable data exposure. Matchlight, the company's comprehensive digital risk protection platform, features continual digital asset monitoring, robust analytics, and actionable intelligence, to quickly identify and minimize the impact of exposed data across the Internet – whether it's the open, deep, or dark web. Featuring its patented data-fingerprinting technology that ensures private data stays private, and unique fusion of data science, machine learning, and dedicated analysts, Terbium Labs provides pinpoint accuracy for early detection and remediation to understand risk exposure and keep organizations safe. Learn more about Terbium Labs' unique approach to digital risk protection by visiting www.terbiumlabs.com or on twitter @terbiumlabs.

CONTACT US

For Sales: sales@terbiumlabs.com

For Marketing & Communications: pr@terbiumlabs.com