Loyalty Card Fraud Risk – Dark Web

2019

RICHTER

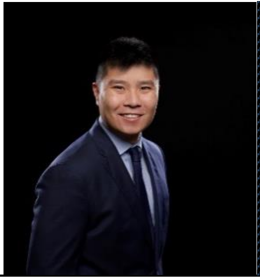
History & Background

Independent firm with Entrepreneurial Mindset

- 90+ year history
- Offices in Toronto, Montreal, and Chicago
- 500 total professionals, with 40+ practitioners specialized in Risk

Thought Leadership

- Risk practice has made a significant impact over past 4+ years
  - Experience working with technology companies
  - Seasoned team with former Big 4 leaders
- Currently providing high tech clients with audit/compliance services

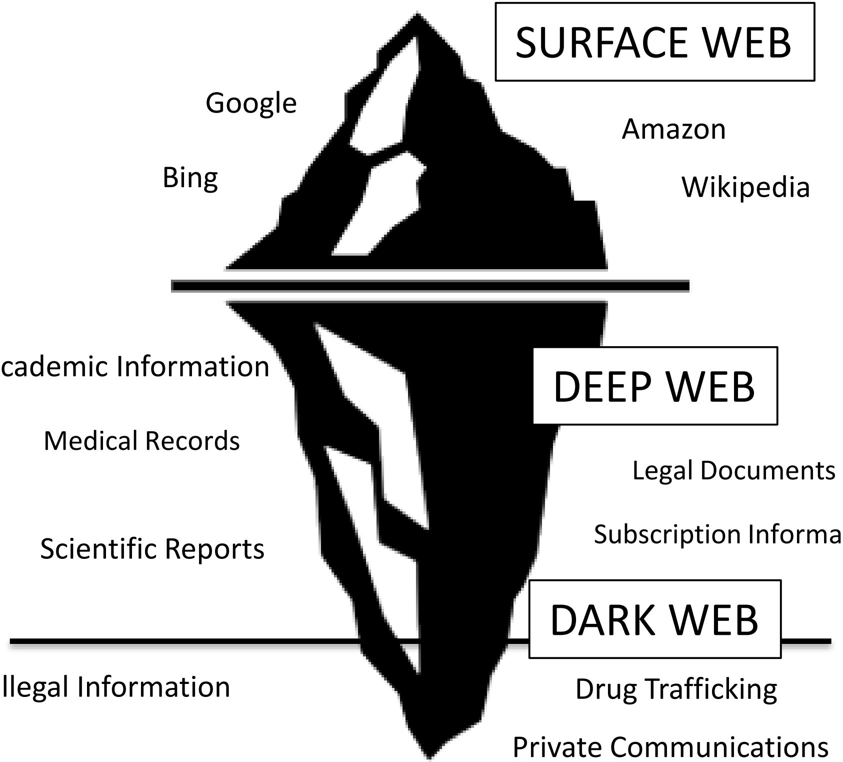


Will Xiang (https://www.linkedin.com/in/willxiang)

Vice President

- CPA, CA, CITP, CAMS
- Focused on Cyber Security

What is the Dark Web?



SURFACE WEB

Google

Bing

Amazon

Wikipedia

DEEP WEB

Academic Information

Medical Records

Scientific Reports

Legal Documents

Subscription Information

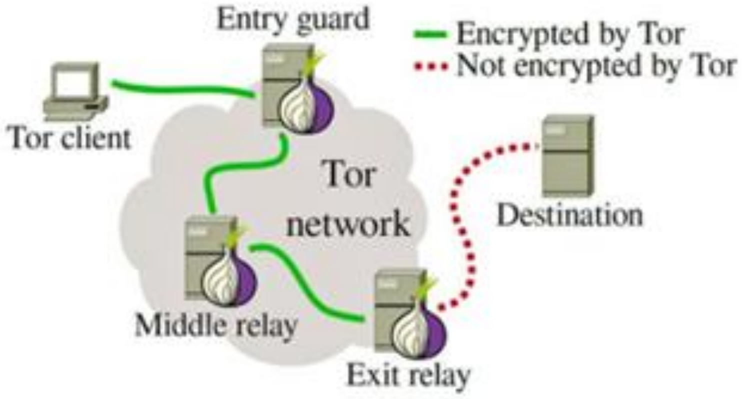
DARK WEB

Illegal Information

Drug Trafficking

Private Communications

TOR – Encrypted Sites



How to access the Dark Web?

1) Download and install TOR Browser

Welcome to Tor Browser

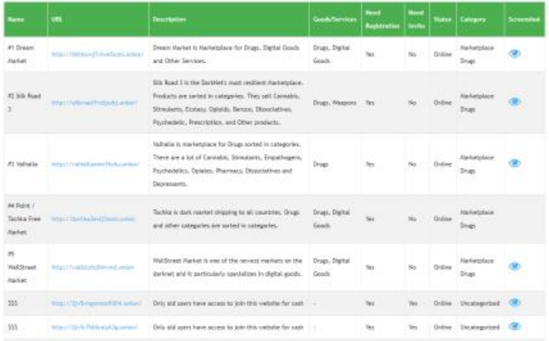
You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with DuckDuckGo.

2) Get a VPN and use it

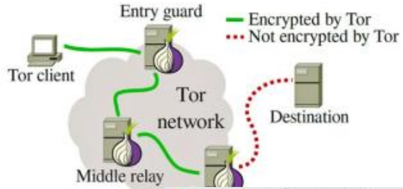
3) Use Google (regular web) to search what .onion sites you want to go to



Name	URL	Description	Goods/Services	Need Registration	Need Invite	Status	Category	Screenshot
#1 Dream Market	[illegible]	Dream Market is Marketplace for Drugs, Digital Goods and Other Services.	Drugs, Digital Goods	Yes	No	Online	Marketplace Drugs	👁
#2 Silk Road 3	[illegible]	Silk Road 3 is the DarkNet's most resilient Marketplace. Products are sorted in categories. They sell Cannabis, Stimulants, Ecstasy, Opioids, Benzos, Dissociatives, Psychedelic, Prescription, and Other products.	Drugs, Weapons	Yes	No	Online	Marketplace Drugs	👁
#3 Valhalla	[illegible]	Valhalla is marketplace for Drugs sorted in categories. There are a lot of Cannabis, Stimulants, Empathogens, Psychedelics, Opiates, Pharmacy, Dissociatives and Depressants.	Drugs	Yes	No	Online	Marketplace Drugs	👁
#4 Point / Tochka Free Market	[illegible]	Tochka is dark market shipping to all countries. Drugs and other categories are sorted in categories.	Drugs, Digital Goods	Yes	No	Online	Marketplace Drugs	
#5 WallStreet Market	[illegible]	WallStreet Market is one of the newest markets on the darknet and it particularly specializes in digital goods.	Drugs, Digital Goods	Yes	No	Online	Marketplace Drugs	👁
$$$	[illegible]	Only old users have access to join this website for cash	-	Yes	Yes	Online	Uncategorized	👁
$$$	[illegible]	Only old users have access to join this website for cash	-	Yes	Yes	Online	Uncategorized	👁

Dark Web News is an example with over 7800 links

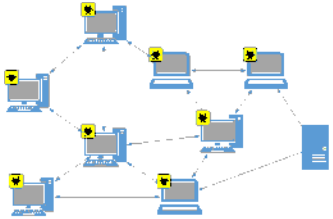
4) Navigate through TOR browser to the Dark Web destination of your choice



Monero maintenance. Will be finished today. Payments (in and out) are paused.

5) Many marketplaces or forums you will need to register with. Don't use your actual name or email.

Typical Dark Web Activities?

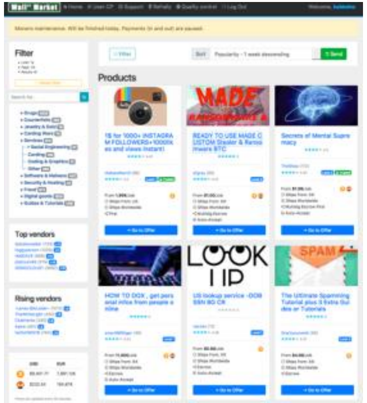


Botnets

Crypto Services

Fraud

Illegal Pornography



1$ for 1000+ INSTAGRAM FOLLOWERS+1000likes and views Instant!

READY TO USE MADE CUSTOM Stealer & Ransomware BTC

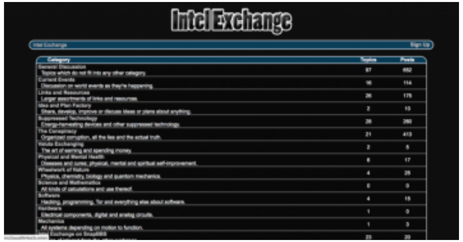
Secrets of Mental Supremacy

HOW TO DOX , get personal infos from people online

US lookup service -DOB SSN BG CR

The Ultimate Spamming Tutorial plus 3 Extra Guides or Tutorials

Marketplaces

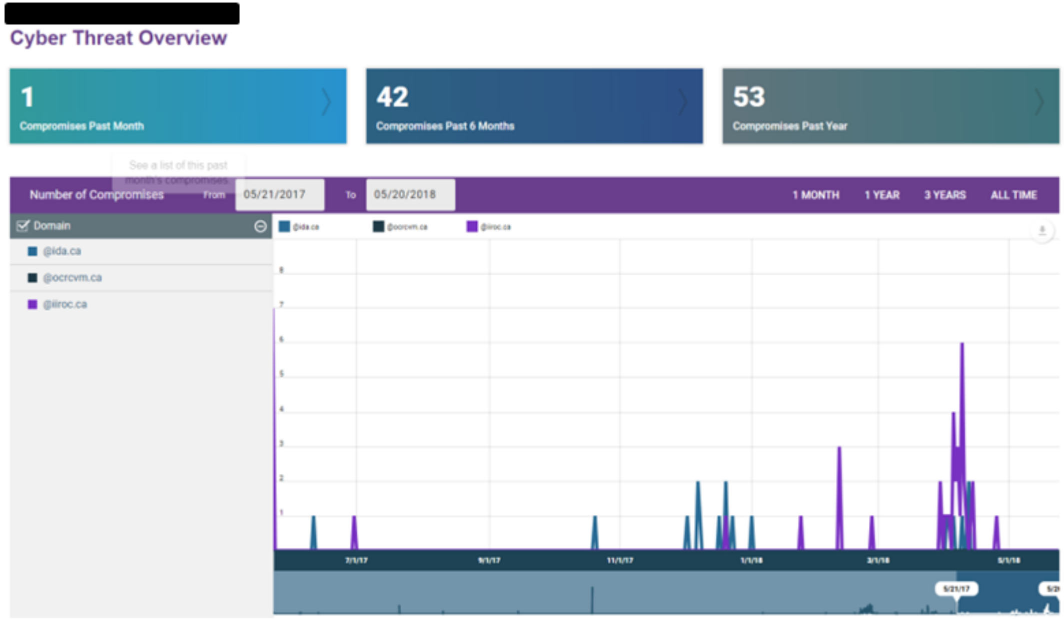


Category	Topics	Posts
General Discussion Topics which do not fit into any other category.	97	662
Current Events Discussion on world events as they're happening.	16	114
Links and Resources Larger assortments of links and resources.	26	175
Idea and Plan Factory Share, develop, improve or discuss ideas or plans about anything.	2	10
Suppressed Technology Energy-harvesting devices and other suppressed technology.	28	260
The Conspiracy Organized corruption, all the lies and the actual truth.	21	413
Valuta Exchanging The art of earning and spending money.	2	5
Physical and Mental Health Diseases and cures, physical, mental and spiritual self-improvement.	6	17
Wheelwork of Nature Physics, chemistry, biology and quantum mechanics.	4	25
Science and Mathematics All kinds of calculations and use thereof.	0	0
Software Hacking, programming, Tor and everything else about software.	4	15
Hardware Electrical components, digital and analog circuits.	1	0
Mechanics All systems depending on motion to function.	1	3
Intel Exchange on SnapBBS	23	20

Hacking Forums / Services
Including compromised accounts

Terrorism

Is my information being sold on the Dark Web?



[redacted]

Cyber Threat Overview

1 Compromises Past Month

42 Compromises Past 6 Months

53 Compromises Past Year

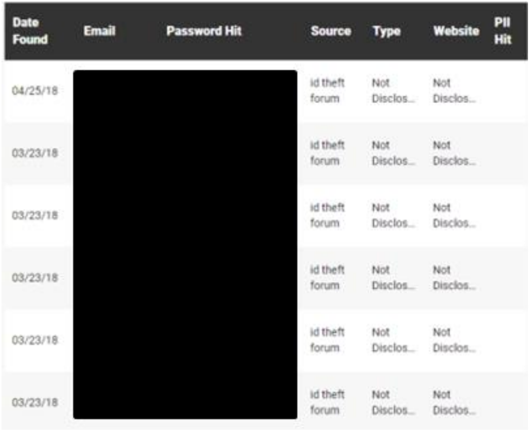
See a list of this past month's compromises

Number of Compromises From 05/21/2017 To 05/20/2018

1 MONTH 1 YEAR 3 YEARS ALL TIME

☑ Domain

- @ida.ca
- @ocrcvm.ca
- @iiroc.ca



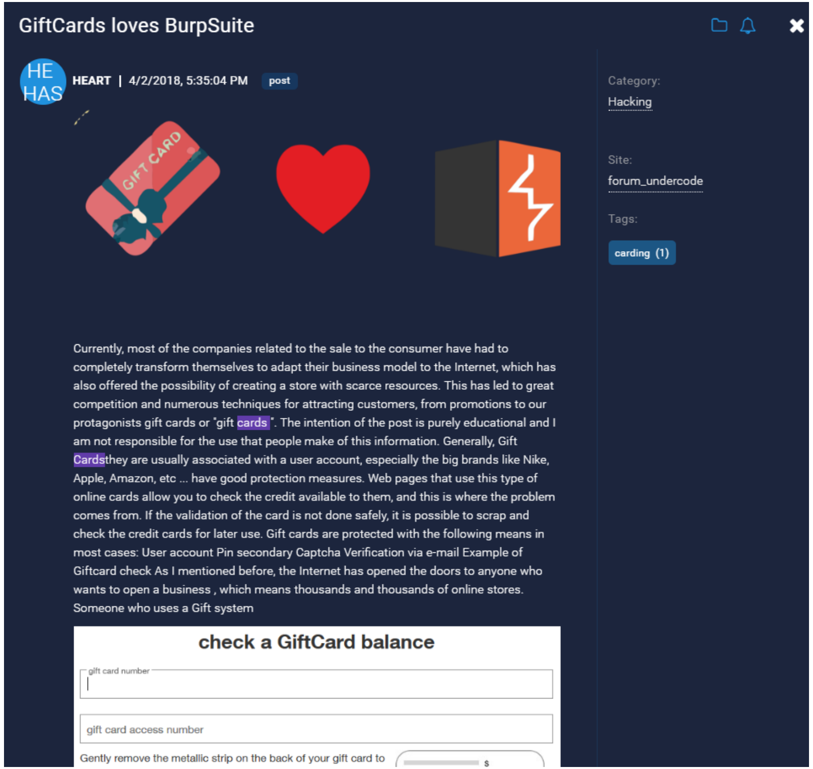
Date Found	Email	Password Hit	Source	Type	Website	PII Hit
04/25/18	[redacted]	[redacted]	id theft forum	Not Disclos...	Not Disclos...	
03/23/18	[redacted]	[redacted]	id theft forum	Not Disclos...	Not Disclos...	
03/23/18	[redacted]	[redacted]	id theft forum	Not Disclos...	Not Disclos...	
03/23/18	[redacted]	[redacted]	id theft forum	Not Disclos...	Not Disclos...	
03/23/18	[redacted]	[redacted]	id theft forum	Not Disclos...	Not Disclos...	
03/23/18	[redacted]	[redacted]	id theft forum	Not Disclos...	Not Disclos...	

Gift Card Fraud

Very similar attacks to those that are perpetrated against online banking.

Using tools like BurpSuite, hackers are able to find web application vulnerabilities through functions like check gift card balance utilities.

Many sites are still not using secondary validation measures, like account pins, captcha or email.



GiftCards loves BurpSuite

HE HAS HEART | 4/2/2018, 5:35:04 PM post

Category: Hacking

Site: forum_undercode

Tags: carding (1)

Currently, most of the companies related to the sale to the consumer have had to completely transform themselves to adapt their business model to the Internet, which has also offered the possibility of creating a store with scarce resources. This has led to great competition and numerous techniques for attracting customers, from promotions to our protagonists gift cards or "gift cards ". The intention of the post is purely educational and I am not responsible for the use that people make of this information. Generally, Gift Cardsthey are usually associated with a user account, especially the big brands like Nike, Apple, Amazon, etc ... have good protection measures. Web pages that use this type of online cards allow you to check the credit available to them, and this is where the problem comes from. If the validation of the card is not done safely, it is possible to scrap and check the credit cards for later use. Gift cards are protected with the following means in most cases: User account Pin secondary Captcha Verification via e-mail Example of Giftcard check As I mentioned before, the Internet has opened the doors to anyone who wants to open a business , which means thousands and thousands of online stores. Someone who uses a Gift system

check a GiftCard balance

gift card number

gift card access number

Gently remove the metallic strip on the back of your gift card to

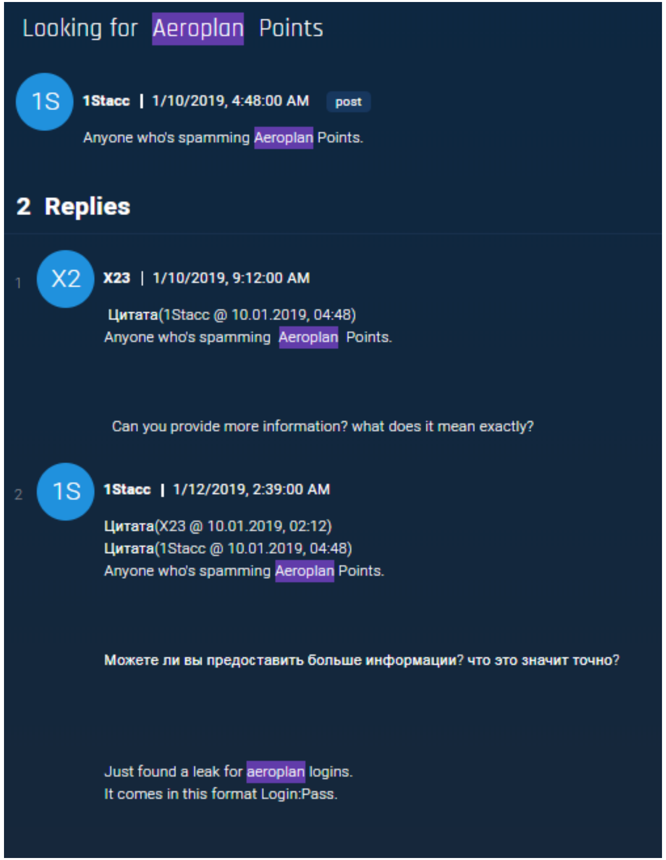
$

Loyalty Card Fraud

A hacker gets a hold of the consumers loyalty account (as illustrated on left).

They sell the login information to other fraudsters who in turn redeem an e-gift card.

They use a service like cardcash.com, or cardswap.ca to get cash.



Looking for Aeroplan Points

1Stacc | 1/10/2019, 4:48:00 AM post

Anyone who's spamming Aeroplan Points.

2 Replies

1 **X23** | 1/10/2019, 9:12:00 AM

Цитата(1Stacc @ 10.01.2019, 04:48)
Anyone who's spamming Aeroplan Points.

Can you provide more information? what does it mean exactly?

2 **1Stacc** | 1/12/2019, 2:39:00 AM

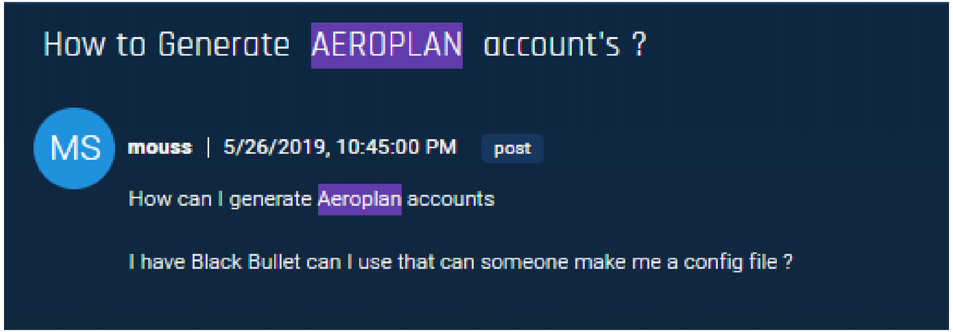
Цитата(X23 @ 10.01.2019, 02:12)
Цитата(1Stacc @ 10.01.2019, 04:48)
Anyone who's spamming Aeroplan Points.

Можете ли вы предоставить больше информации? что это значит точно?

Just found a leak for aeroplan logins.
It comes in this format Login:Pass.

Loyalty Card Fraud

A hacker will use brute force tools like Black Bullet to get access to Aeroplan accounts.



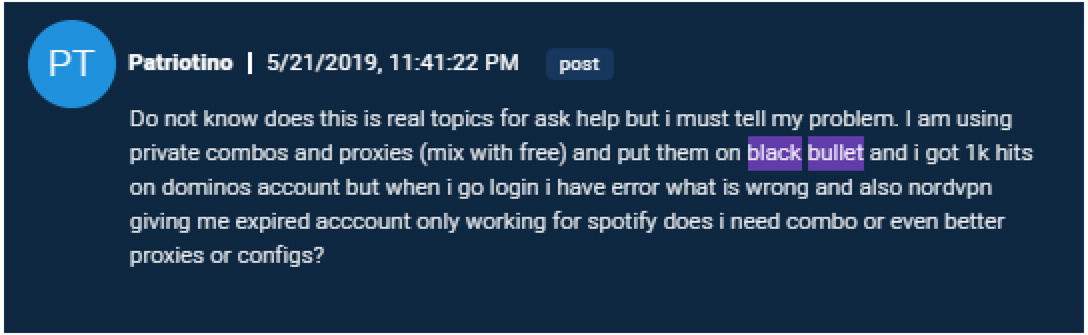
How to Generate AEROPLAN account's ?

mouss | 5/26/2019, 10:45:00 PM post

How can I generate Aeroplan accounts

I have Black Bullet can I use that can someone make me a config file ?

And Dominos Pizza account, because hackers get hungry after booking flights.



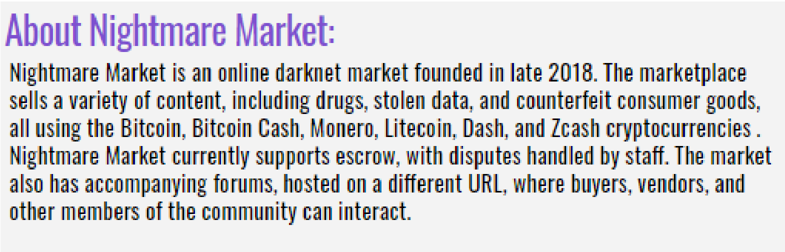
Patriotino | 5/21/2019, 11:41:22 PM post

Do not know does this is real topics for ask help but i must tell my problem. I am using private combos and proxies (mix with free) and put them on black bullet and i got 1k hits on dominos account but when i go login i have error what is wrong and also nordvpn giving me expired acccount only working for spotify does i need combo or even better proxies or configs?

Loyalty Card Fraud

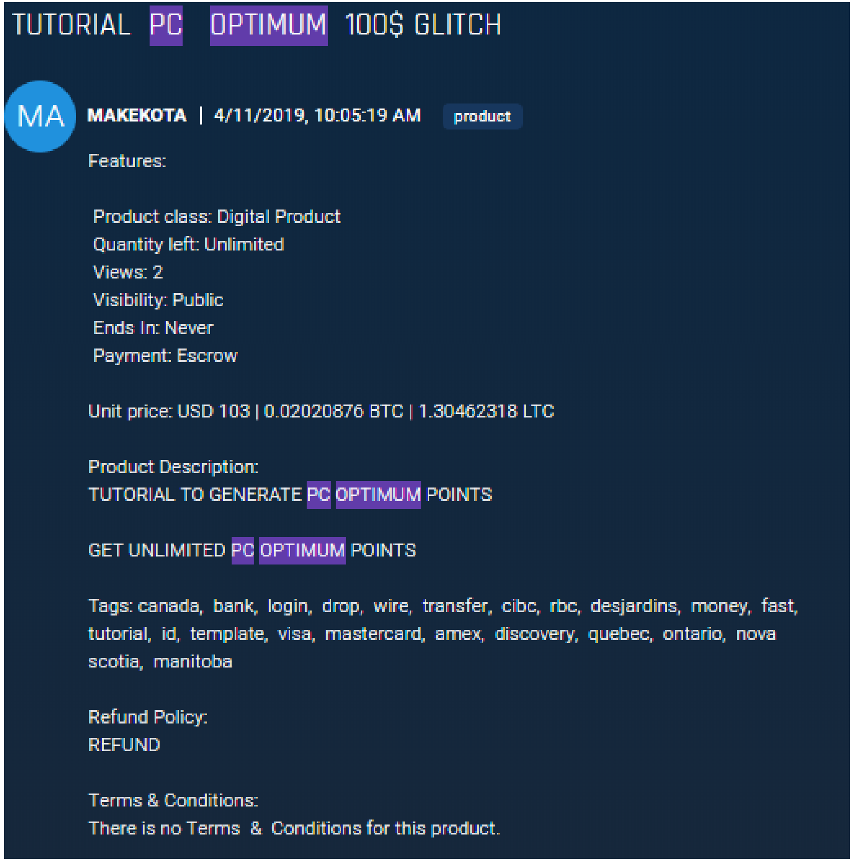
This fraudster is selling a technique to run up unlimited PC Optimum points.

If it doesn't work, no worries, there is a refund policy and payment will be in escrow.



About Nightmare Market:

Nightmare Market is an online darknet market founded in late 2018. The marketplace sells a variety of content, including drugs, stolen data, and counterfeit consumer goods, all using the Bitcoin, Bitcoin Cash, Monero, Litecoin, Dash, and Zcash cryptocurrencies . Nightmare Market currently supports escrow, with disputes handled by staff. The market also has accompanying forums, hosted on a different URL, where buyers, vendors, and other members of the community can interact.



TUTORIAL PC OPTIMUM 100$ GLITCH

MA MAKEKOTA | 4/11/2019, 10:05:19 AM product

Features:

Product class: Digital Product
Quantity left: Unlimited
Views: 2
Visibility: Public
Ends In: Never
Payment: Escrow

Unit price: USD 103 | 0.02020876 BTC | 1.30462318 LTC

Product Description:
TUTORIAL TO GENERATE PC OPTIMUM POINTS

GET UNLIMITED PC OPTIMUM POINTS

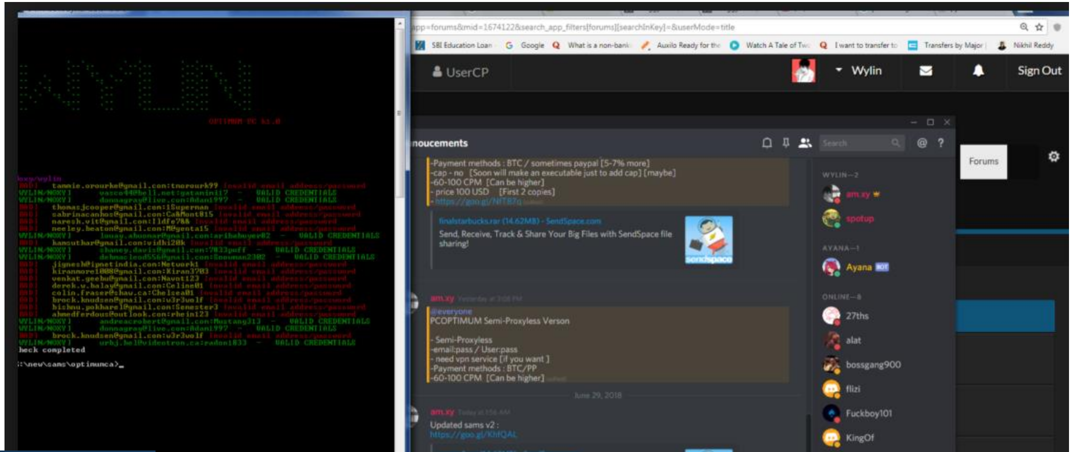
Tags: canada, bank, login, drop, wire, transfer, cibc, rbc, desjardins, money, fast, tutorial, id, template, visa, mastercard, amex, discovery, quebec, ontario, nova scotia, manitoba

Refund Policy:
REFUND

Terms & Conditions:
There is no Terms & Conditions for this product.

Loyalty Card Fraud

This is a buyer looking to purchase compromised PC Optimum accounts. They can validate balances on specially developed proxies [Discord] before they buy.



```
OPTIMUM PC k1.0

oxy/wylin
BAD|    tammie.orourke@gmail.com:tnorourk99 Invalid email address/password
WYLIN/MOXY]       vasco44@bell.net:gatanini17  -   VALID CREDENTIALS
WYLIN/MOXY]       donnagray@live.com:Adani997  -   VALID CREDENTIALS
BAD|    thomasjcooper@gmail.com:1Superman Invalid email address/password
BAD|    sabrinacanhos@gmail.com:Ca&Mont815 Invalid email address/password
BAD|    naresh.vit@gmail.com:lldfe78& Invalid email address/password
BAD|    neeley.heaton@gmail.com:M@genta15 Invalid email address/password
WYLIN/MOXY]       louay.abuomar@gmail.com:aribabuyer82  -   VALID CREDENTIALS
BAD|    kamsuthar@gmail.com:vidhi20k Invalid email address/password
WYLIN/MOXY]       shaney.davis@gmail.com:7833puff  -   VALID CREDENTIALS
WYLIN/MOXY]       debmacleod556@gmail.com:Snowman2382  -   VALID CREDENTIALS
BAD|    jignesh@ipnetindia.com:Network1 Invalid email address/password
BAD|    kiranmore1008@gmail.com:Kiran3783 Invalid email address/password
BAD|    venkat.geebu@gmail.com:Navat123 Invalid email address/password
BAD|    derek.w.halay@gmail.com:Celine01 Invalid email address/password
BAD|    colin.fraser@shaw.ca:Chelsea01 Invalid email address/password
BAD|    brock.knudsen@gmail.com:w3r3wolf Invalid email address/password
BAD|    bishnu.pokharel@gmail.com:Semester3 Invalid email address/password
BAD|    ahmedferdous@outlook.com:rhein123 Invalid email address/password
WYLIN/MOXY]       andreacrobert@gmail.com:Mustang313  -   VALID CREDENTIALS
WYLIN/MOXY]       donnagray@live.com:Adani997  -   VALID CREDENTIALS
BAD|    brock.knudsen@gmail.com:w3r3wolf Invalid email address/password
WYLIN/MOXY]       urbj.hel@videotron.ca:radon1833  -   VALID CREDENTIALS
heck completed

:\new\sams\optimumca>_
```

-Payment methods : BTC / sometimes paypal [5-7% more]
-cap - no [Soon will make an executable just to add cap] [maybe]
-60-100 CPM [Can be higher]
- price 100 USD [First 2 copies]
- https://goo.gl/NfTB7q

finalstarbucks.rar (14.62MB) - SendSpace.com
Send, Receive, Track & Share Your Big Files with SendSpace file sharing!

am.xy Yesterday at 3:08 PM
@everyone
PCOPTIMUM Semi-Proxyless Verson

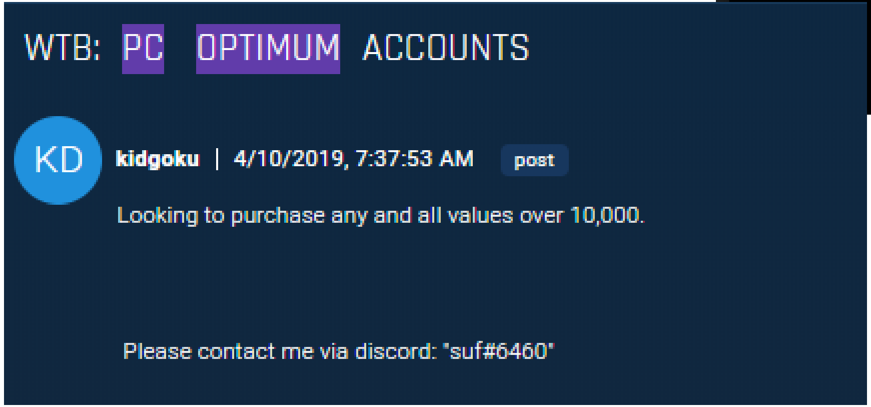
- Semi-Proxyless
-email:pass / User:pass
- need vpn service [if you want]
-Payment methods : BTC/PP
-60-100 CPM [Can be higher]

June 29, 2018

am.xy Today at 1:56 AM
Updated sams v2 :
https://goo.gl/KhfQAL

samsv2.rar (14.62MB) - SendSpace.com
Send, Receive, Track & Share Your Big Files with SendSpace file sharing!

Message #annoucements



WTB: PC OPTIMUM ACCOUNTS

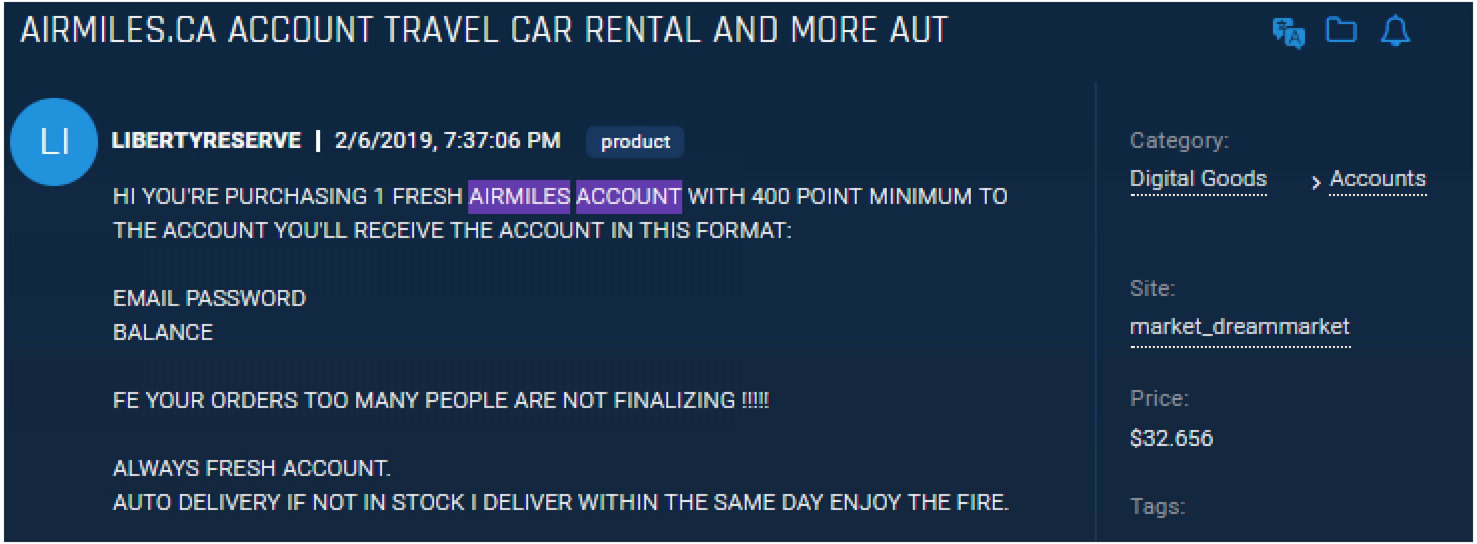
KD kidgoku | 4/10/2019, 7:37:53 AM post

Looking to purchase any and all values over 10,000.

Please contact me via discord: "suf#6460"

Loyalty Card Fraud

A seller on a dark web market [dreammarket] selling an airmiles account with 400 point minimum for $32.65



AIRMILES.CA ACCOUNT TRAVEL CAR RENTAL AND MORE AUT

LI

LIBERTYRESERVE | 2/6/2019, 7:37:06 PM product

HI YOU'RE PURCHASING 1 FRESH AIRMILES ACCOUNT WITH 400 POINT MINIMUM TO THE ACCOUNT YOU'LL RECEIVE THE ACCOUNT IN THIS FORMAT:

EMAIL PASSWORD
BALANCE

FE YOUR ORDERS TOO MANY PEOPLE ARE NOT FINALIZING !!!!!

ALWAYS FRESH ACCOUNT.
AUTO DELIVERY IF NOT IN STOCK I DELIVER WITHIN THE SAME DAY ENJOY THE FIRE.

Category:
Digital Goods › Accounts

Site:
market_dreammarket

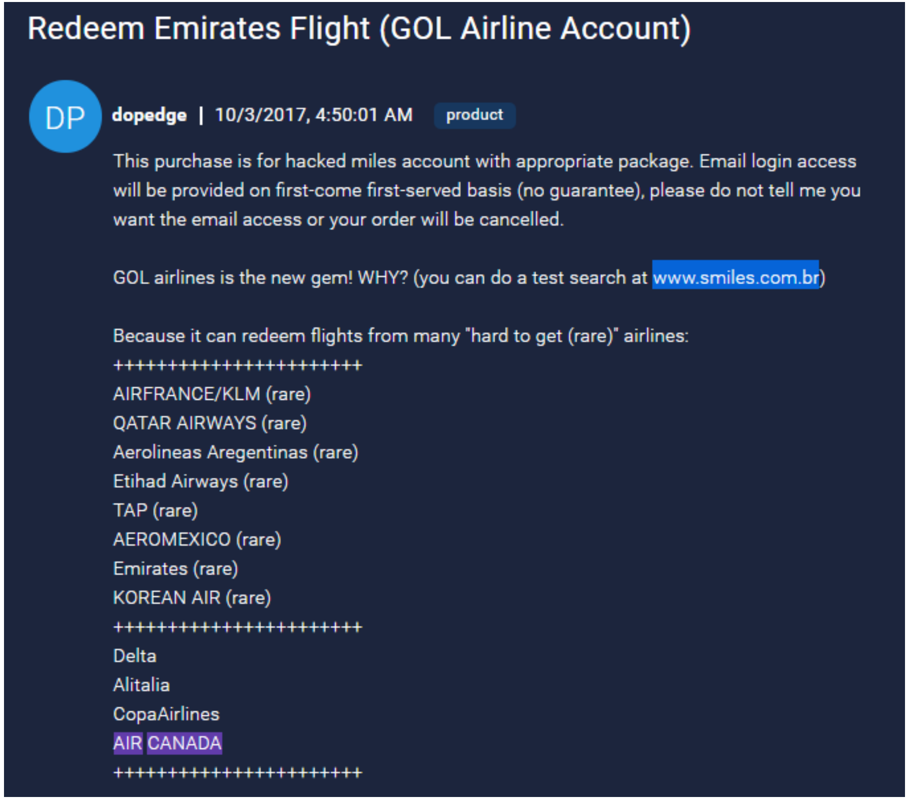
Price:
$32.656

Tags:

Loyalty Card Fraud

RICHTER

A seller on a dark web market named DreamMarket, selling hacked GOL Airline accounts that will allow the redemption of points for many other airlines, including Air Canada.



Redeem Emirates Flight (GOL Airline Account)

dopedge | 10/3/2017, 4:50:01 AM product

This purchase is for hacked miles account with appropriate package. Email login access will be provided on first-come first-served basis (no guarantee), please do not tell me you want the email access or your order will be cancelled.

GOL airlines is the new gem! WHY? (you can do a test search at www.smiles.com.br)

Because it can redeem flights from many "hard to get (rare)" airlines:
++++++++++++++++++++++
AIRFRANCE/KLM (rare)
QATAR AIRWAYS (rare)
Aerolineas Aregentinas (rare)
Etihad Airways (rare)
TAP (rare)
AEROMEXICO (rare)
Emirates (rare)
KOREAN AIR (rare)
++++++++++++++++++++++
Delta
Alitalia
CopaAirlines
AIR CANADA
++++++++++++++++++++++

Risk

- Loyalty cards are becoming more popular as a target for fraud as credit card fraud is becoming more difficult. (Jump from 4% - 11% year over year by 2017[1])
  - Perishable good (i.e. Airplane tickets) has a shorter detection window
  - User awareness relatively low
  - Transactions can be easily anonymous

- Reliance on Convenience Increases, for example:
  - 40% of global travel bookings are made online
  - 1/3 of millennials prefer to book travel last minute

Tackling Trust vs Convenience

[1] *Source: https://blog.siftscience.com/2018/loyalty-program-fraud/*

Impact

Compromises will affect the core value proposition in the loyalty or gift card model

- **Expectations:** 93% of customers expect loyalty programs to have fraud detections in place
- **Relationship Killers:** 17% of customers will likely end the relationship with the loyalty program after breach
- **Grapevine Effect:** 37% of customers will tell, on average, 24 other users

Source: Connexions Loyalty – Loyalty Fraud: A Case for Protecting Your Most Loyal Customers

What can be done?

Reliance on rule-based monitoring programs

- Negate individual behavior patterns
- Predictability countered by malicious actors

Reliance on manual intervention

- Sample based approach will be difficult to detect time sensitive fraud

Monitoring

- Proactive monitoring of actors

New Technologies

- Machine Learning
- AI

Discussion

Thank You