Lighting up the Canadian Darknet
Financially

Milind Bhargava
Phillip Shin
Peter Desfigies
About the Speakers

- Peter Desfigies is a Security Consultant at TELUS Communications Inc. where he works with a team of other operations analysts to proactively investigate and analyze customer traffic, while also providing threat intelligence on attacks, campaigns, and zero-days in order to protect customer’s environment and enhance their security posture.
About the Speakers

• Philip Shin is a Security Consultant with TELUS Communications Inc. based out of Vancouver where he works with a team of other operations analysts to proactively investigate and analyze customer traffic, while also providing threat intelligence on attacks, campaigns, and zero-days in order to protect customer’s environment and enhance their security posture.

• Phil couldn’t make it. He is busy hacking someone.
About the Speakers

• Milind Bhargava is a Senior Security Consultant with TELUS Security Solutions. He is also a part time faculty at George Brown College in Toronto where he teaches Cryptography, Forensics and Network Auditing to students of the Network and System Security Analysis (NaSSA) Post Grad program.

• He has been involved on and off with Darknet research over 7 years.

• It all started back in 2009 when he first came to know about Bitcoins…

Image from: https://getlogdog.com
What is Darknet?

Not the TV Show!

Most are familiar with the term
Many have ventured a few times out of curiosity

Yes, its kind of like the show Mr. Robot

For us, Darknet is an untapped source of Threat Intelligence and in some cases amusement 😊
How to connect to Darknet?

Google it!
If you are still too lazy, there are youtube videos describing the same
Now before you go ahead

NSA likely targets anybody who's 'Tor-curious'

Whether you're a regular user of Web privacy tools like Tor and Tails, or you've just checked out their websites, the NSA could be tracking your online movements, a new investigation reveals.

by Seth Rosenblatt @sethr / July 3, 2014 6:20 PM PDT

Care about privacy? You’re a terrorist! XKeyscore exposed: How NSA tracks all German Tor users as ‘extremists’

The former NSA director General Keith Alexander stated that all those communicating with encryption will be regarded as terror suspects and will be monitored and stored as a method of prevention, as quoted by the Frankfurter Allgemeine Zeitung in August last year. The top secret source code published here indicates that the NSA is making a concerted effort to combat any and all anonymous spaces that remain on the internet. Merely visiting privacy-related websites is enough for a user’s IP address to be logged into an NSA database.

Surface Web vs Deep Web vs Darknet

The Surface Web is anything that can be indexed by a typical search engine like Google, Bing or Yahoo.

Deep Web is anything that a search engine can’t find.

The Darknet then is classified as a portion of the Deep Web that has been intentionally hidden and is inaccessible through standard web browsers.
SURFACE WEB

Google
Bing
Wikipedia

DEEP WEB

Academic Information
Medical Records
Legal Documents
Scientific Reports
Subscription Information

Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.

Multilingual Databases
Financial Records
Government Resources
Competitor Websites
Organization-specific Repositories

Social Media

(DARK WEB)

A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. Deep Web Technologies has zero involvement with the Dark Web.

Illegal Information
TOR-Encrypted sites
Political Protests
Drug Trafficking sites
Private Communications

Image from http://deepwebtech.com
Interac Logins for EFT

Canada Bank Login Info - for EFT/Interac

Uname: [Redacted] Pass: [Redacted]
Q1: What city were you born in? [Redacted]
Q2: What is your mother's middle name? [Redacted]
Q3: What is your father's middle name? [Redacted]
Email: [Redacted] Epass: [Redacted]

Canada Bank Login Info - for EFT/Interac

Uname: [Redacted] Pass: [Redacted]
Q1: What is your best friend's first name? [Redacted]
Q2: What is the name of your first pet? [Redacted]
Q3: What is your favourite hobby? [Redacted]
Q4: What is your favourite movie? [Redacted]
Q5: What was the name of the street on which you grew up? [Redacted] st.
Epass: [Redacted]

Canada Bank Login Info - for EFT/Interac

Available Banks: [Redacted] Questions: [Redacted]
Ontario Host: [Redacted]
Uname: [Redacted] Pass: [Redacted]
Q1: What was my first pet's name? [Redacted]
Q2: What is my best friend's first name? [Redacted]
Q3: Which city did I meet my significant other? [Redacted]
Epass: [Redacted]
Bank Logs

Bank Logs + Security Questions

These come with USER + PASS + SECURITY QUESTIONS + IP + UserAgent. Test Account = Low Balance, Low CC. Just for tests, can be used to 3rd party transfers.

Sold by mastercorp - 520 sold since Jun 2, 2016

Vendor Level 3 Trust Level 4

Product Description

These come with USER + PASS + SECURITY QUESTIONS + IP + UserAgent.

Test Account = Low Balance, Low CC. Just for tests, can be used to 3rd party transfers.

Under 2k balance = $90
Over 2k balance = $150
Size Log = 200

Bank Login + Security Questions

*** ONLY UNDER 2K LOGS LEFT *** These logins come with the following information:

CREDIT LINE AVAILABLE FUNDS.

Vendor Level 6 Trust Level 1

Product Description

*** ONLY UNDER 2K LOGS LEFT ***

These logins come with the following information:

- User
- Pass
- IP
- Useragent
- Security Questions

----------------------

2k+ = $150
Under 2k = $75

Tiny balance/cc test = $50

BALANCE INCLUDES CREDIT LINE AVAILABLE FUNDS.
Phishing page with Hosting
Phishing page with Hosting
Paypal Linked to Canadian CC
Alleged Government Database

Canadian pros for sale

<table>
<thead>
<tr>
<th>Features</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product class</strong></td>
<td>Digital goods</td>
</tr>
<tr>
<td><strong>Quantity left</strong></td>
<td>Unlimited</td>
</tr>
<tr>
<td><strong>Ends in</strong></td>
<td>Never</td>
</tr>
<tr>
<td><strong>Origin country</strong></td>
<td>Worldwide</td>
</tr>
<tr>
<td><strong>Ships to</strong></td>
<td>Worldwide</td>
</tr>
<tr>
<td><strong>Payment</strong></td>
<td>Escrow</td>
</tr>
</tbody>
</table>

Sold by zeus231 - 0 sold since Oct 23, 2015

1 pros - 1 days - USD +100.00 / item
# Credit Cards

<table>
<thead>
<tr>
<th>Bin</th>
<th>Card</th>
<th>Debit/Credit</th>
<th>Mark</th>
<th>Expires</th>
<th>Track 1</th>
<th>Code</th>
<th>Country</th>
<th>Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>02501</td>
<td>MASTERCARD</td>
<td>CREDIT</td>
<td>GOLD</td>
<td></td>
<td></td>
<td>201</td>
<td>Canada, BC</td>
<td></td>
</tr>
<tr>
<td>02501</td>
<td>MAESTRO</td>
<td>DEBIT</td>
<td>ATM CARD</td>
<td></td>
<td></td>
<td>220</td>
<td>Canada</td>
<td></td>
</tr>
<tr>
<td>02501</td>
<td>VISA</td>
<td>CREDIT</td>
<td>CLASSIC</td>
<td></td>
<td></td>
<td>201</td>
<td>Canada, BC</td>
<td></td>
</tr>
<tr>
<td>02501</td>
<td>MASTERCARD</td>
<td>CREDIT</td>
<td>STANDARD</td>
<td></td>
<td></td>
<td>201</td>
<td>Canada, BC</td>
<td></td>
</tr>
<tr>
<td>02501</td>
<td>MASTERCARD</td>
<td>CREDIT</td>
<td>STANDARD</td>
<td></td>
<td></td>
<td>201</td>
<td>Canada</td>
<td></td>
</tr>
</tbody>
</table>
Carding

The Big Question: How do fraudsters “cash out”?

Vendors who claim to do the carding for you

Loyal and professional pp cashout service

Mar 25, 2016 at 2:12 AM.

Im back active on PP CASHOUTS mates!
We also have B&M drops as well.
I have over 70 accounts with the key tool..THE DEBITS...
-the few guys I worked with have become incohsistant due to other projects which is fine..so im moving forward FRESH!...
-Specializing in cashing out PP very fast and some drop cashouts as well. WE ARE FOCUSED ON PP AND STRIPE.
-Many know of me as a fair and loyal CASHIER... (of course u have some guys try to shit your name from time to time but thats this market work).
***WE WILL MAKE EXCLUSIVE PARTNERSHIP WITH TRANSFER VENDORS AND SENDERS WHOM HAVE KNOWLEDGE OF AGING PP ACCOUNTS WITH THE LARGE VOLUME WE HAVE WEEKLY***
***TRE2LOYAL is the only guy with cashout limit of 3k-7k on all accounts...YES I ACN ACCEPT AND CASHOUT 7K in less than 2 hours***
Idiots who ask for help on Facebook

Can anyone do carding for me??? If yes, then msg me for details

i want to work as drop for carders.
also can do as escrower. i take 5% of your transaction.
can provide all proofs of mine for trust anyone need my service. pm me

Image from http://facebook.com
Those who advertise on Facebook
There is always Craigslist

☆ Deep web ✗

Hey I'm a 23 year old female who wants to surf the deep web. I have no idea how tho. I'm looking for someone who can sit down with me and get me set up. I don't have any money or a whole lot to offer but I'm pleasant to be around and I'm a good friend. Educate me!

- do NOT contact me with unsolicited services or offers

☆ Deep Web Tutorial (CHICAGO) ✗

I am interested in someone that is comfortable with the Deep Web. I would like to have someone give me a few basic lessons on how to surf it safely and how to navigate around.

I pay cash and we can work out a price that is fair depending on how much time is needed.

We can meet up somewhere in the city.
Someone offering under USD 250 for Deep Web Search

Fixed Price!
W9 Work Visa required
Why aren’t companies buying their stuff back?

• By buying you are encouraging this behavior
• Not to mention Legal Ramifications

• Exceptions are the Ransomware Issues
Fullz – Complete Information

<table>
<thead>
<tr>
<th>Product Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>***ADDONS: 50,000 canadian fullz for 300$ and 100,000 for 475$ *** 10,000 Complete fullz in this format: Title GivenName Surname StreetAddress City State ZipCode Country MothersMaiden Birthday TelephoneNumber TelephoneCountryCode Pounds Kilograms FeetInches Centimeters NationalID Color Occupation Company Vehicle BloodType Gender Like this:</td>
</tr>
</tbody>
</table>

**10,000 Canadian Fullz [NO CC-ONLY INFO]**

Complete fullz in this format: Title GivenName Surname StreetAddress City State ZipCode Country MothersMaiden Birthday TelephoneNumber TelephoneCountryCode Pounds Kilograms FeetInches Centimeters NationalID Color Occupation Company Vehicle BloodType Gender Like this:

<table>
<thead>
<tr>
<th><strong>Product Class</strong></th>
<th><strong>Features</strong></th>
<th><strong>Features</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital goods</td>
<td>Origin Country: Canada</td>
<td></td>
</tr>
<tr>
<td>28 items</td>
<td>Ships to Canada</td>
<td></td>
</tr>
<tr>
<td>Never</td>
<td>Payment Escrow</td>
<td></td>
</tr>
</tbody>
</table>

- **Message Delivery (AUTO SOON):** 1 days - USD $0.00 / Item
- **50,000 Fullz:** 1 days - USD $152.65 / Item
- **100,000 Fullz:** 2 days - USD $266.59 / Item

- **Sold by phackman - 5 sold since Aug 20, 2015**
Looking for Canadians... Also people from UK/USA. Mainly Canada though.

Hey, I am looking for other Canadians to work with.. I have access to millions of fullz profiles.. And currently have about 300,000 currently in front of me.

I have connections/contacts for this already but all are in eastern Canada (Quebec/Ontario)
I am trying to find people who are preferably in (British Columbia/Alberta).
I am looking for people who can work with these and either can make documents/ID or knows someone who can make ID/Documents. Photoshop skills also an asset...

Also, hoping to find people that already know the basics and what they are doing.. For example looking for people that know how to pull make purchases/orders, credit reports, forward mail etc. I already know these things myself and don’t mind teaching the right person or people. BUT - Please do not waste my time...
Also, looking for people in USA and even UK to work with... As myself and a good friend/partner has fullz profiles for both USA and UK.
Which leads to fake
Gathering all ingredients…

Ok, now that you have a bunch of Credit Cards and Fake IDs, what can you do next?
Hyatt Regency Calgary one of 250 hotels hit by hackers

Published on: January 17, 2015 | Last Updated: January 17, 2015 6:25 PM MST
Other Hotels

05 Trump Hotel Collection Confirms Card Breach

The Trump Hotel Collection, a string of luxury hotel properties tied to business magnate and Republican presidential candidate Donald Trump, said last week that a year-long breach of its credit card system may have resulted in the theft of cards used at the hotels. The acknowledgement comes roughly three months after this author first reported that multiple financial institutions suspected the hotels were compromised.

24 Hilton Acknowledges Credit Card Breach

Two months after KrebsOnSecurity first reported that multiple banks suspected a credit card breach at Hilton Hotel properties across the country, Hilton has acknowledged an intrusion involving malicious software found on some point-of-sale systems.
… And adding them together
You have a million ways things can go wrong

- Two counts of fraud under $5,000
- Three counts of possession of forged credit card
- One count of identity fraud
- Two counts of identity theft
- Two counts of breach of probation
- One count of possession of credit card data

Identity Theft Ring Investigation
Wanted For Credit Card Fraud And Identity Theft

- Possession for the purpose of trafficking
- Possession of instruments for forging credit cards
- Identity theft
- Counterfeiting Mark (Government of Canada)
- Possession of stolen property under $5,000
- Possession of credit card data
- Possession of forged credit card
- Possession of identity documents

Image taken with Permission from Calgary Police Services
Why should the enterprises care?

• Identify criminals targeting you
How can Enterprises benefit?

• Learn Threat Actor attack TTP

need email hacked at [redacted] will pay 500$ for this email.

need username and password, pay 500 after accessing.

not a problem get at me i provide a specialized keylogger service via word documents for word 2010 so its pretty easy also pdf and screen saver file

i give user all 3 for that price the logger and i host the gate for you

can be over tor if u like that will cost the same

if your interested [email] [redacted]
This leads us to

Word macro Download/Execute 0/35 FUD

Word macro Download/Execute 0/35 FUD - $10

Put your .exe hosted somewhere, direct link, place order specifying link to your exe. receive your doc file with the scan4you link that it is FUD.

Choose delivery option. Hosted if want me to put your .exe file on a webserver for the direct link. Send exe file in sendspace.com and I host for you on webserver with this option.
Things for Enterprises to keep in mind

• Not everyone can do this
• Risks Involved
  • Legal
  • Personal Identifiable Information (PII)
Moral of the Story

There are many things available on the Darknet
All kinds of fraud, financial, drugs, weapons and others.
I have certainly not covered all, that talk will take hours 😊

The objective is to light up the Canadian DarkNet for you from a financial point of view and why we shouldn’t ignore it.
References

Questions?
the future is friendly®