Risky Business?

Investigating the Security Practices of Vendors on an Online Anonymous Market using Ground-Truth Data

Jochem van de Laarschot and Rolf van Wegberg

Delft University of Technology
Online anonymous markets

Platforms that facilitate the pseudonymous trade of illicit physical goods and digital items.

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

Our approach

Results

Take-aways
Easy access to OPSEC guides

Given that ‘Operational Security’ (OPSEC) techniques are frequently shared in the underground community…
Law enforcement

... and given the increasing amount of scrutiny by law enforcement ...
However, cybercriminals do not always achieve maximum security:

- the inevitable trade-off between security and efficiency of operations
- ‘Perfect security’ is not economically viable: security comes at a cost

So, how prevalent are poor security practices among online anonymous market vendors?

To find out, we capture certain security practices on a single market: Hansa Market.
Hansa Market

Dutch law enforcement allowed us restricted access to the Hansa Market back-end database.

**Hansa Market**
- ~1750 vendors,
- ~400,000 regular members, 15% active
- 1000-8000 daily visitors
- Estimated revenue $33M

**Back-end database**
- User administration
- Listings (advertisements)
- Orders
- Connection logs
Capturing security practices

Additionally, we leveraged *Have I Been Pwnd*, *Grams* and *Chainalysis*.

- **Have I Been Pwnd**, a database of leaked passwords.
  - 10B+ leaked passwords, of which 573M are unique
  - SHA1-hashes are publicly available

- **Grams**, a “Google for darknet markets”.
  - The search engine indexed listings and vendors
  - Shut down in December 2017, through law enforcement access to offline copy

- **Chainalysis**, a blockchain analysis service.
  - Provides context to raw blockchain data
  - Mainly makes use of co-spend clustering heuristics
  - Chainalysis is able to estimate which bitcoin addresses are controlled by – for example – bitcoin exchanges
1. We **identify characteristics** of vendors and **cluster vendors** that have similar characteristics into distinct ‘**vendor types**’ using latent profile analysis.

2. We **capture** the security practices in our data and **measure the prevalence** of poor security practices **across vendor types**.
Resulting vendor types

The LPA results in a 5-cluster model which clearly differentiates between different types of vendors.
Measuring security practices

We capture six security practices of vendors that are active on Hansa Market.

- **Password strength**: zxcvbn.
  On average: $10^{14.7}$ estimated guesses, median: $10^{10.5}$ guesses.

- **Password uniqueness**: hibp matching.
  185 vendors (17.1%) logged in with a password we could match.

- **2FA-usage**: hansa back-end
  Of the total vendor population, only 60.5% used 2FA.

- **PGP-key adoption and key-strength**: GnuPG
  ~100% adoption, few weak keys.

- **Reuse of PGP-keys over multiple markets**: Grams matching
  265 out of 908 matched.

- **The traceability of their cash-out to bitcoin exchanges**: Chainalysis
  14% of the bitcoin addresses are managed by known online financial service providers.
Traceability of cash-outs

About 10% of the vendors on Hansa Market can be easily linked to a central bitcoin exchange.
Security across vendor types

Comparing Novices, Drug Dealers, Drug Lords, Digital Fraudsters and Cybercrime Elites
Password strength

Passwords of Drug Lords and Drug Dealers are (significantly) stronger, Digital Fraudsters score low.
Security across vendor types

Vendors selling digital cybercrime items are more likely to have insecure practices.

<table>
<thead>
<tr>
<th>Vendors</th>
<th>UNIQUE PW</th>
<th>2FA</th>
<th>2048+ PGP</th>
<th>NO KEY REUSE</th>
<th>NO BTC LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>y/n</td>
<td>sec.%</td>
<td>y/n</td>
<td>sec.%</td>
<td>y/n</td>
</tr>
<tr>
<td>Novices</td>
<td>395/98</td>
<td>80.1</td>
<td>542/446</td>
<td>54.9</td>
<td>466/520</td>
</tr>
<tr>
<td>Drug D.</td>
<td>342/52</td>
<td>86.8</td>
<td>359/150</td>
<td>70.5</td>
<td>273/233</td>
</tr>
<tr>
<td>Drug L.</td>
<td>82/11</td>
<td>88.2</td>
<td>90/20</td>
<td>81.8</td>
<td>62/48</td>
</tr>
<tr>
<td>Dig. Frd.</td>
<td>57/21</td>
<td>73.1</td>
<td>45/58</td>
<td>43.7</td>
<td>30/73</td>
</tr>
<tr>
<td>Cyb. Elt.</td>
<td>20/3</td>
<td>87.0</td>
<td>13/10</td>
<td>56.5</td>
<td>5/18</td>
</tr>
</tbody>
</table>
Take-aways

We found surprising patterns in the security practices of vendors.

- Vendors that specialize in selling digital cybercrime items make ‘mistakes’ in their digital security the most often, while vendors belonging to clusters of successful drug dealers tend to have the best digital security.

- Many vendors – including the highly successful ones – make the mistake of initiating traceable cash-outs to mainstream bitcoin exchanges.
Contact

Jochem van de Laarschot  
Rolf van Wegberg  
[firstname]vandelaarschot@gmail.com  
r.s.vanwegberg@tudelft.nl