Plug and Prey?

Measuring the Commoditization of Cybercrime via Online Anonymous Markets

Rolf van Wegberg¹, Samaneh Tajalizadehkhoob¹, Kyle Soska², Ugur Akyazi¹, Carlos Gañán¹, Bram Klievink¹, Nicolas Christin², and Michel van Eeten¹

¹ Delft University of Technology, ² Carnegie Mellon University
Would-be cybercriminals only need $10 to send distributed denial-of-service (DDoS) attacks that could cripple an organization, according to a recent research report.

Security firm Armor provided an in-depth examination of the emerging cybercrime-as-a-service sector in “The Black Market Report: A Look Inside the Dark Web.” Instead of
Commoditization of cybercrime

- Which parts of cybercrime value chains are successfully commoditized and which are not?
- What kind of revenue do these criminal business-to-business services generate and how fast are they growing?
Online anonymous markets

- Characteristics of commodities are highly congruent with characteristics of online anonymous marketplaces.
- The one-shot, anonymous purchases require suppliers to offer highly commoditized offerings.
- If cybercrime offerings can be commoditized, online anonymous markets should be a highly attractive place to sell.
Measuring commoditization

1. **Develop** a conceptual model of the value chain components in dominant cybercriminal business models.

2. **Collect** and parse longitudinal data on eight online anonymous marketplaces, between 2011 and 2017.

3. **Classify** cybercrime-related listings to these components to track trends in listings and transaction volumes.

4. **Identify** the best-selling clusters of listings and compare these offerings to the capabilities, resources and services needed.
Cybercriminal business models

- Development: Malware, App, Javascript, Website, Hosting
- Distribution: Website, Botnet, E-mail, Exploit, Phone
- Take-over: Webinject, Javascript, Malware, Exploit, RAT
- Cash-out: Cash-out, Customer-service
Data collection

- Leveraged the parsed and analyzed dataset of Soska and Christin (2015) on seven prominent online markets.
- We then extended this data with 16 complete and parsed scrapes of AlphaBay between 2014 and 2017.
- This resulted in a longitudinal dataset covering eight prominent markets between 2011 to 2017.
Leveraged the parsed and analyzed dataset of Soska and Christin (2015) on seven prominent online markets. We then extended this data with 16 complete and parsed scrapes of AlphaBay between 2014 and 2017.

<table>
<thead>
<tr>
<th>Market</th>
<th>#Listings</th>
<th>#Vendors</th>
<th>#Feedbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agora</td>
<td>27,974</td>
<td>1,961</td>
<td>234,372</td>
</tr>
<tr>
<td>AlphaBay</td>
<td>101,999</td>
<td>6,262</td>
<td>2,223,992</td>
</tr>
<tr>
<td>Black Market Reloaded</td>
<td>9,075</td>
<td>980</td>
<td>62,876</td>
</tr>
<tr>
<td>Evolution</td>
<td>35,015</td>
<td>2,352</td>
<td>464,146</td>
</tr>
<tr>
<td>Hydra</td>
<td>2,343</td>
<td>133</td>
<td>43,701</td>
</tr>
<tr>
<td>Pandora</td>
<td>7,674</td>
<td>459</td>
<td>89,065</td>
</tr>
<tr>
<td>Silk Road 1</td>
<td>24,363</td>
<td>2,336</td>
<td>605,744</td>
</tr>
<tr>
<td>Silk Road 2</td>
<td>22,174</td>
<td>1,201</td>
<td>662,497</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>230,617</strong></td>
<td><strong>15,684</strong></td>
<td><strong>4,386,393</strong></td>
</tr>
</tbody>
</table>
**Description**

For sale is **SELECT FIRE** AK 74 built from beginning as such. Not a converted semi auto, legit full auto function just like factory rifle. I built the rifle with original **UNISSUED** Bulgarian AK 74 parts and quality US made barrel and receiver. Headspace checked to ensure safe operation. Because gun was made of brand new parts, some of them still covered in anti-rusting grease.

Bulgarian made polymer stocks.

I can add extra parts and accessories at you cost.

Select fire shoot both semi auto and full auto. Rifle is **BRAND NEW** only 30 rounds fired for test. Include 1 magazine and 30 rounds of 5.45x39mm surplus Russian ammo.

Full escrow.
Pre-filtering


- Categories:
  - Benzos
  - Cannabis
  - **Digital Goods**
  - Dissociatives
  - Drug Paraphernalia
  - Electronics
  - MDMA
  - **Miscellaneous**
  - Opioids
  - Other
  - Prescription drugs
  - Psychedelics
  - Sildenafil
  - Stimulants
  - Tobacco
  - Weapons
For labeling ground truth, we randomly selected 1,500 items from all *Digital Goods* or *Miscellaneous* listings (n=44,060).

We excluded *JavaScripts*, *web-injects*, and *customer service*. For these products we found no listings in our random sample.

We did find *business-to-consumer* (B2C) cybercrime listings, so we added additional categories to map these.

We implemented a *Linear Support Vector Machine* (SVM) classifier to predict ten B2B and seven B2C product classes.
Classifying listings to cybercrime components

<table>
<thead>
<tr>
<th>Category</th>
<th># Listings</th>
<th># Vendors</th>
<th>Total revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>App</td>
<td>144</td>
<td>75</td>
<td>$12,815</td>
</tr>
<tr>
<td>Botnet</td>
<td>125</td>
<td>79</td>
<td>$46,904</td>
</tr>
<tr>
<td>Cash-out</td>
<td>12,125</td>
<td>2,076</td>
<td>$7,864,318</td>
</tr>
<tr>
<td>E-mail</td>
<td>550</td>
<td>216</td>
<td>$97,280</td>
</tr>
<tr>
<td>Exploit</td>
<td>115</td>
<td>75</td>
<td>$17,603</td>
</tr>
<tr>
<td>Hosting</td>
<td>20</td>
<td>15</td>
<td>$1,182</td>
</tr>
<tr>
<td>Malware</td>
<td>310</td>
<td>162</td>
<td>$57,598</td>
</tr>
<tr>
<td>Phone</td>
<td>261</td>
<td>148</td>
<td>$74,587</td>
</tr>
<tr>
<td>RAT</td>
<td>105</td>
<td>65</td>
<td>$16,070</td>
</tr>
<tr>
<td>Website</td>
<td>664</td>
<td>293</td>
<td>$286,405</td>
</tr>
<tr>
<td>Accounts</td>
<td>3,759</td>
<td>577</td>
<td>$598,491</td>
</tr>
<tr>
<td>Fake</td>
<td>3,386</td>
<td>815</td>
<td>$2,877,184</td>
</tr>
<tr>
<td>Guide</td>
<td>5,049</td>
<td>1,020</td>
<td>$2,620,635</td>
</tr>
<tr>
<td>Pirated</td>
<td>1,420</td>
<td>338</td>
<td>$129,961</td>
</tr>
<tr>
<td>Voucher</td>
<td>1,293</td>
<td>386</td>
<td>$753,116</td>
</tr>
<tr>
<td>Custom</td>
<td>6,310</td>
<td>1,887</td>
<td>$5,793,064</td>
</tr>
<tr>
<td>Other</td>
<td>8,424</td>
<td>2,652</td>
<td>$7,749,788</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>44,060</strong></td>
<td><strong>5,552</strong></td>
<td><strong>$28,997,006</strong></td>
</tr>
</tbody>
</table>
Active vendors on markets over time

<table>
<thead>
<tr>
<th>Date</th>
<th>Nr. of active vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>0</td>
</tr>
<tr>
<td>2013</td>
<td>0</td>
</tr>
<tr>
<td>2014</td>
<td>1,000</td>
</tr>
<tr>
<td>2015</td>
<td>2,000</td>
</tr>
<tr>
<td>2016</td>
<td>3,000</td>
</tr>
<tr>
<td>2017</td>
<td>4,000</td>
</tr>
</tbody>
</table>
Listings, feedbacks and revenue over time

- **Listings**
  - Total monthly count
  - Dates range from 2012 to 2017
  - Data shows an increase over time

- **Feedbacks**
  - Total monthly count
  - Dates range from 2012 to 2017
  - Data shows an increase over time

- **Revenue (1,000s USD)**
  - Dates range from 2012 to 2017
  - Data shows fluctuations over time
Total revenue per category per month

![Graph showing average monthly revenue per category from 2012 to 2017.](image-url)
Number of active vendors per month

![Graph showing the number of active vendors per month from 2012 to 2017. The graph compares different categories of vendors, including RAT, App, Botnet, Cash-out, E-mail, Exploits, Hosting, Malware, Phone, and Website. The x-axis represents the years from 2012 to 2017, while the y-axis represents the number of active vendors ranging from 0 to 6,000. The graph indicates a significant increase in the number of active vendors over the years, particularly in the categories of Malware, E-mail, and Exploits.](image-url)
Cumulative percentage of listings across vendors

Cumulative distribution function

Number of vendors

Listings
Revenue
Product portfolios of markets

% of total nr. of listings (logged)

Agora
AlphaBay
BMR
Evolution
Hydra
Pandora
Silk Road 1
Silk Road 2

RAT
App
Botnet
Cash-out
E-mail
Exploits
Hosting
Malware
Phone
Website
Best-selling clusters

- Identify the three best-selling clusters within each category

- Only partial fulfillment of cybercriminal demand
  - Credit cards dominant in the cash-out category
  - Office exploit dominant in the exploit category
  - Ransomware dominant in the malware category

- Outsourcing not trivial, given
  - Niche supply
  - Broad demand
Takeaways

- There is evidence of commoditization, but outsourcing options are restricted and transaction volume is often modest.

- Similar to narcotic sales, a significant amount of revenue is in retail cybercrime, rather than business-to-business.

- We conservatively estimate the overall revenue for cybercrime commodities on online anonymous markets to be at least US $15M between 2011-2017.

- While there is growth, commoditization is a spottier phenomenon than previously assumed.
Plug and Prey?

Measuring the Commoditization of Cybercrime via Online Anonymous Markets

Get in touch
r.s.vanwegberg@tudelft.nl
@RolfvanWegberg

Open data
All data is publicly available in anonymized and non-anonymized form through IMPACT (https://www.impactcybertrust.org/)

See also web interface at https://arima.cylab.cmu.edu/markets/