Plug and Prey?

Measuring the Commoditization of Cybercrime via Online Anonymous Markets

Rolf van Wegberg[1], Samaneh Tajalizadehkhoob[1],
Kyle Soska[2], Ugur Akyazi[1], Carlos Gañán[1],
Bram Klievink[1], Nicolas Christin[2], and Michel van Eeten[1]

[1] Delft University of Technology, [2] Carnegie Mellon University

TU Delft

NEWS March 26, 2018 @ 12:26 PM

Cybercrime-as-a-Service Offerings Include DDoS Attacks Starting at $10, Report Reveals

By Shane Schick

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?

Silk Road
anonymous market

messages 0 | orders 0 | account ฿0.00

a few words from the Dread Pirate Roberts

Search Go

Hi, *logout* 0

Shop by Category

- Drugs *6,625*
  - Cannabis *1,080*
  - Dissociatives *190*
  - Ecstasy *829*
  - Opioids *382*
  - Other *450*
  - Precursors *59*
  - Prescription *1,429*
  - Psychedelics *828*
  - Stimulants *1,079*
- Apparel *310*
- Art *114*
- Biotic materials *1*
- Books *858*
- Collectibles *1*
- Computer equipment *43*
- Custom Orders *60*
- Digital goods *590*
- Drug paraphernalia *247*

Generic XANAX (Alprazolam 1mg): 400 pills Grade A+
฿1.52

Pure Oxycodone HCL Powder (OC, Roxy)- 1/4
฿0.53

TESTOSTERONE CYPIONATE 250mg/ml x 10
฿0.69

25x 130mg MDMA CAPS(FREE SHIPPING)
฿1.62

News

- Closing the Armory
- A brand new look for Silk Road!
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes

100 GR - MDMA 84%

Pack of Five (5) Suboxone (Buphrenorphine) 8mg/2mg

SALE SALE!!!!!! 250 grams METHYLONE!

Bring on the Shadow People! New batch MDPV

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

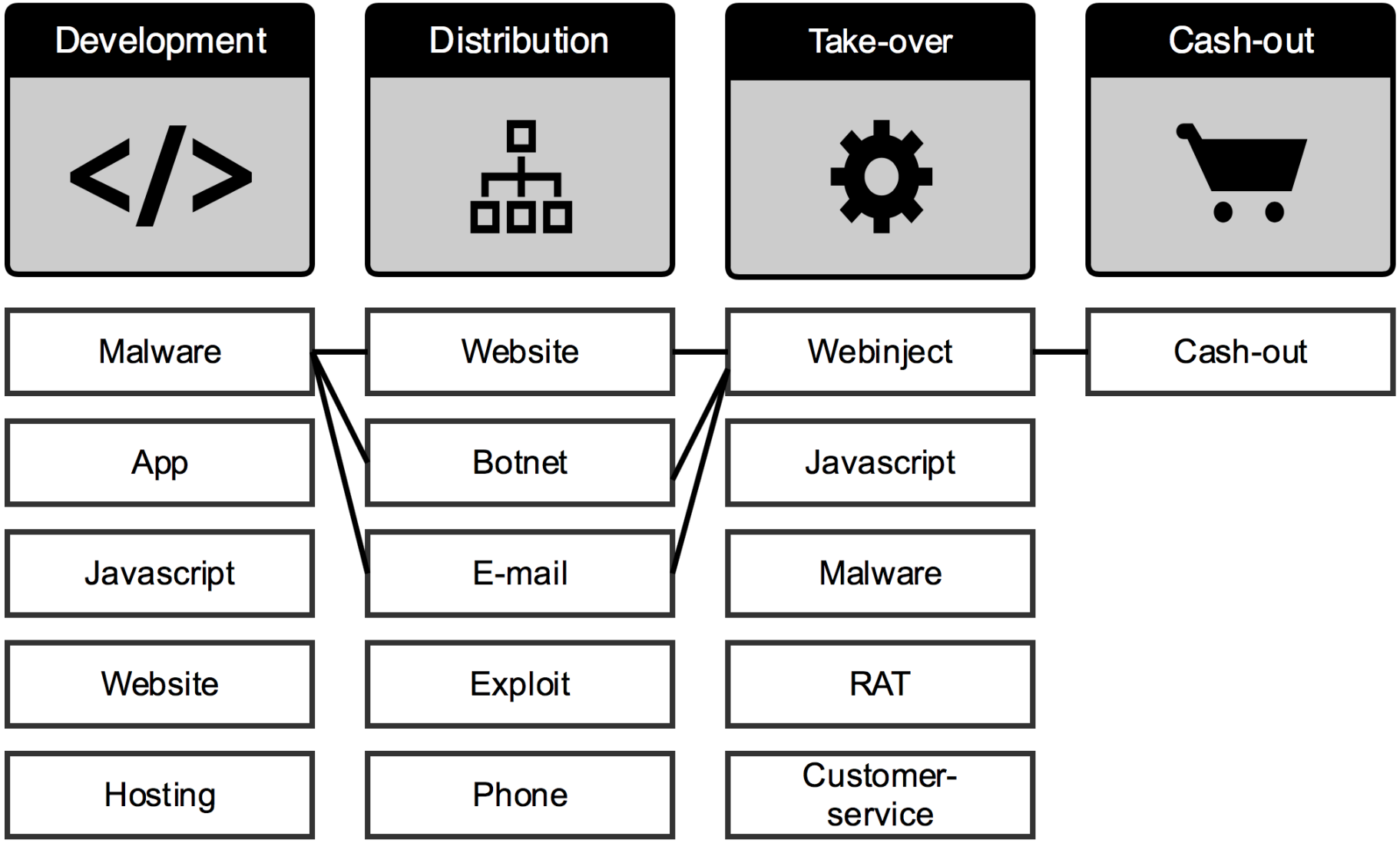
1. **Develop** a conceptual model of the value chain components in dominant cybercriminal business models.

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



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.

Data set

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

Categories

- Drugs (2762)
- Services (1331)
- Data (633)
- Weapons (210)
- Collectables (30)
- Metals/Stones (29)
- Other (354)
- Software (165)
- Movies (27)
- Tobacco (169)
- Counterfeits (248)
- Alcohol (11)
- eBooks (1667)
- Weight Loss (17)

Exchange

- Exchange

User Menu

- Home
- Inbox (0/0)
- Account
- Purchases
- Favorites
- Deposit Addresses
- Forum

Rates

(AK-74 BRAND NEW FULL AUTO 5.45x39mm

More images:



Price	19.93779 BTC
	$ 2,500.00 £ 1,554.92 € 1,844.20
Ship from	USA
Ship to	Worldwide
Stock	2
Created in	2013-08-26 02:31 UTC
Last update	2013-09-16 15:29 UTC
Listing Feedback	0/0/0

Your balance isn't enough to buy this item! Please deposit the needed funds before.

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.

Shipping Table	
Description	Price
US/mexico mild stealth 1-3 days with tracking	0.79751 BTC
Worldwide high stealth 6-10 days with tracking	2.39254 BTC

Questions to Vendor

Question by: Battosai at 2013-09-17 05:07 UTC

Select fire ? can you have ammo ?

Seller Info

User lereyjenkins47
Feedback 3
Reg. Date 2013-07-19 01:16 UTC
Last login 2013-09-19 19:05 UTC

View Profile
Other Listings
Contact seller
Add to Favorites

Pre-filtering

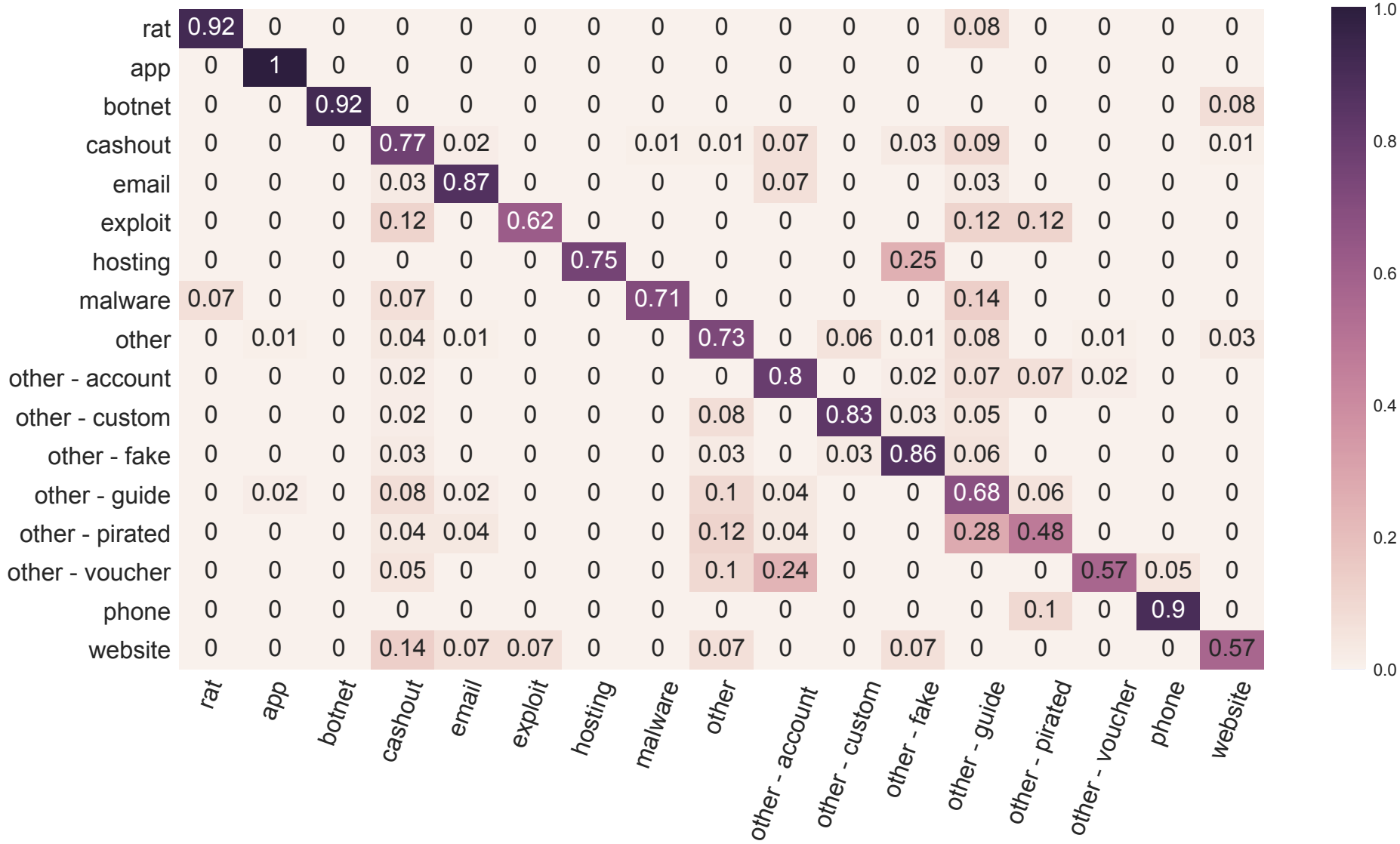
- Prediction from Soska & Christin (2015).

- Categories:
  - Benzos
  - Cannabis
  - **Digital Goods**
  - Dissassociatives
  - Drug Paraphernalia
  - Electronics
  - MDMA
  - ***Miscellaneous***
  - Opioids
  - Other
  - Prescription drugs
  - Psychedelics
  - Sildenafil
  - Stimulants
  - Tobacco
  - Weapons

Classification approach

- 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.

Classifier performance

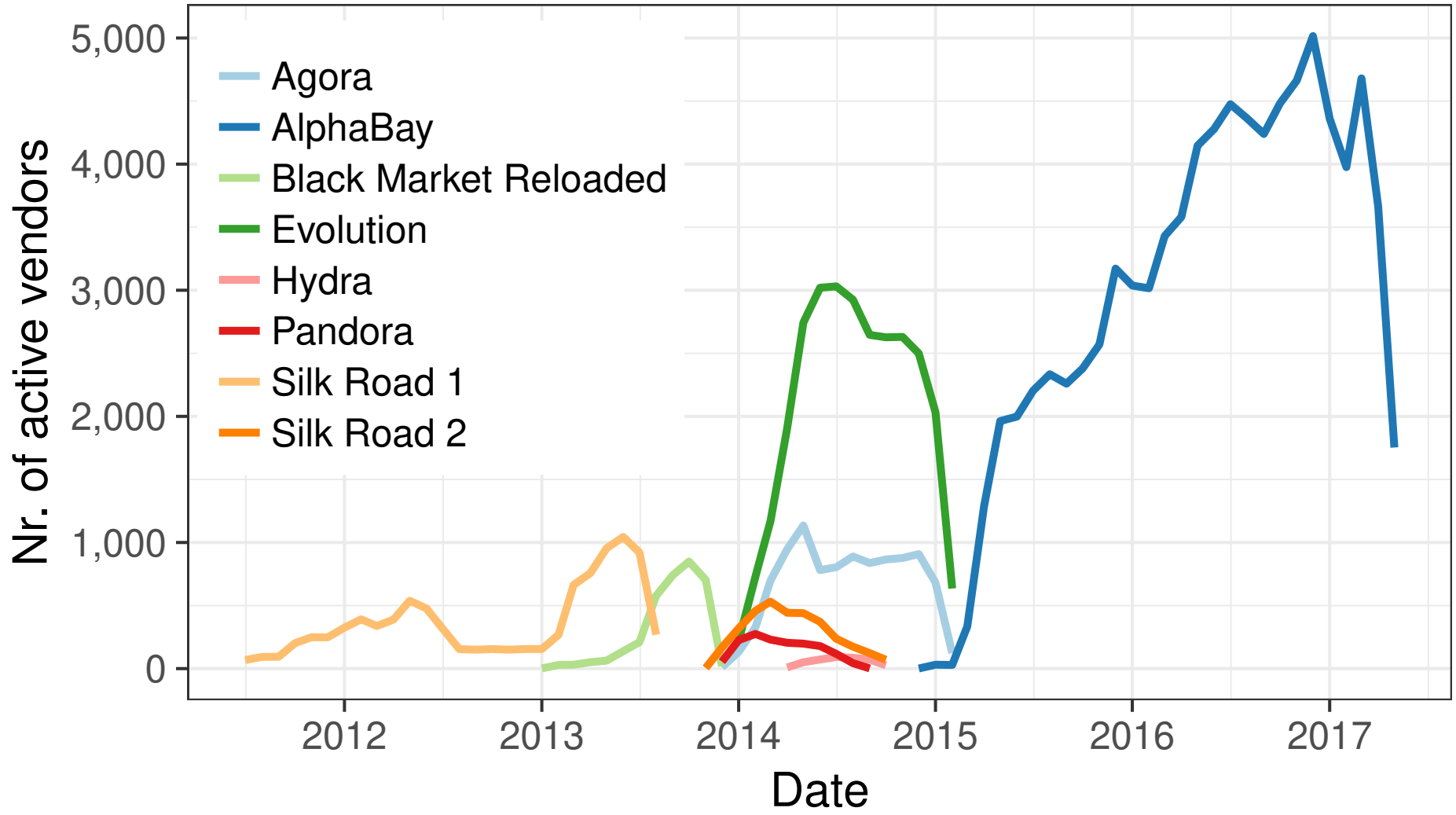


Classifying listings to cybercrime components

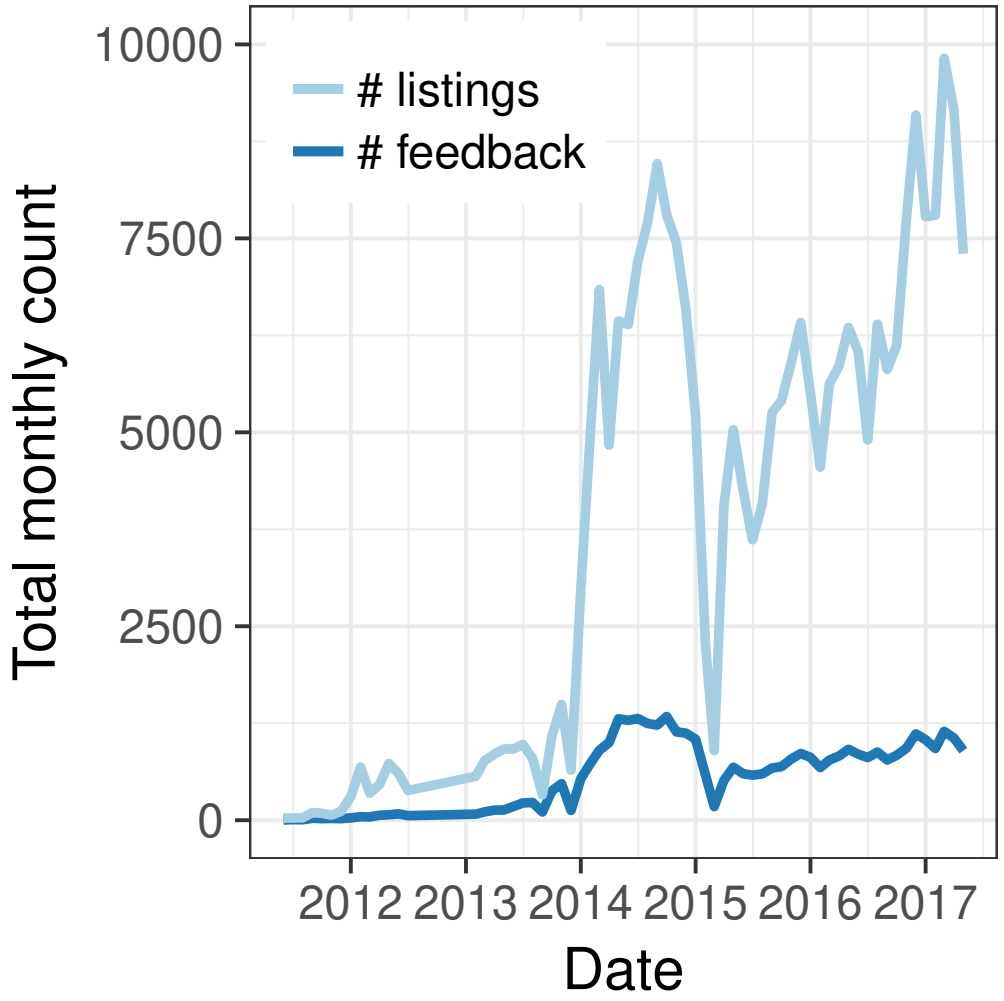
Category	# Listings	# Vendors	Total revenue
App	144	75	$ 12,815
Botnet	125	79	$ 46,904
Cash-out	12,125	2,076	$ 7,864,318
E-mail	550	216	$ 97,280
Exploit	115	75	$ 17,603
Hosting	20	15	$ 1,182
Malware	310	162	$ 57,598
Phone	261	148	$ 74,587
RAT	105	65	$ 16,070
Website	664	293	$ 286,405
Accounts	3,759	577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

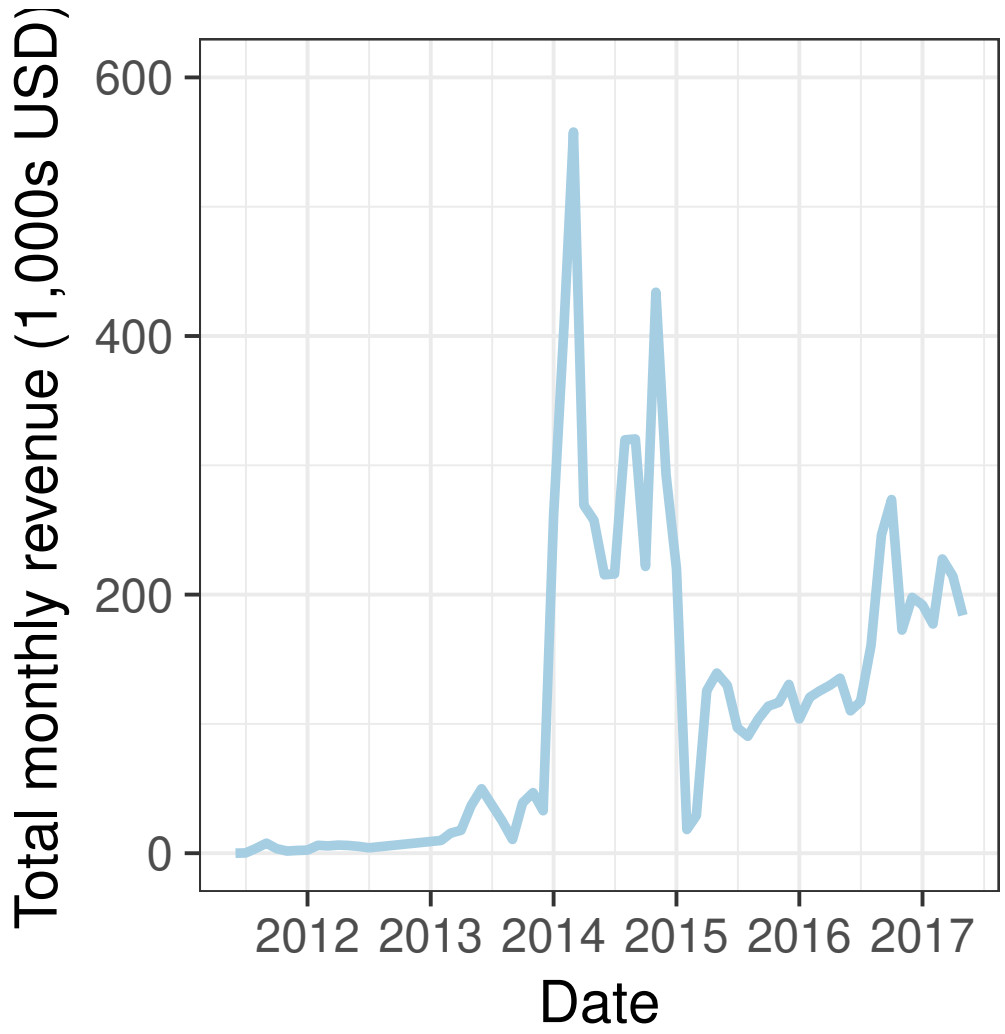
TU Delft

Active vendors on markets over time

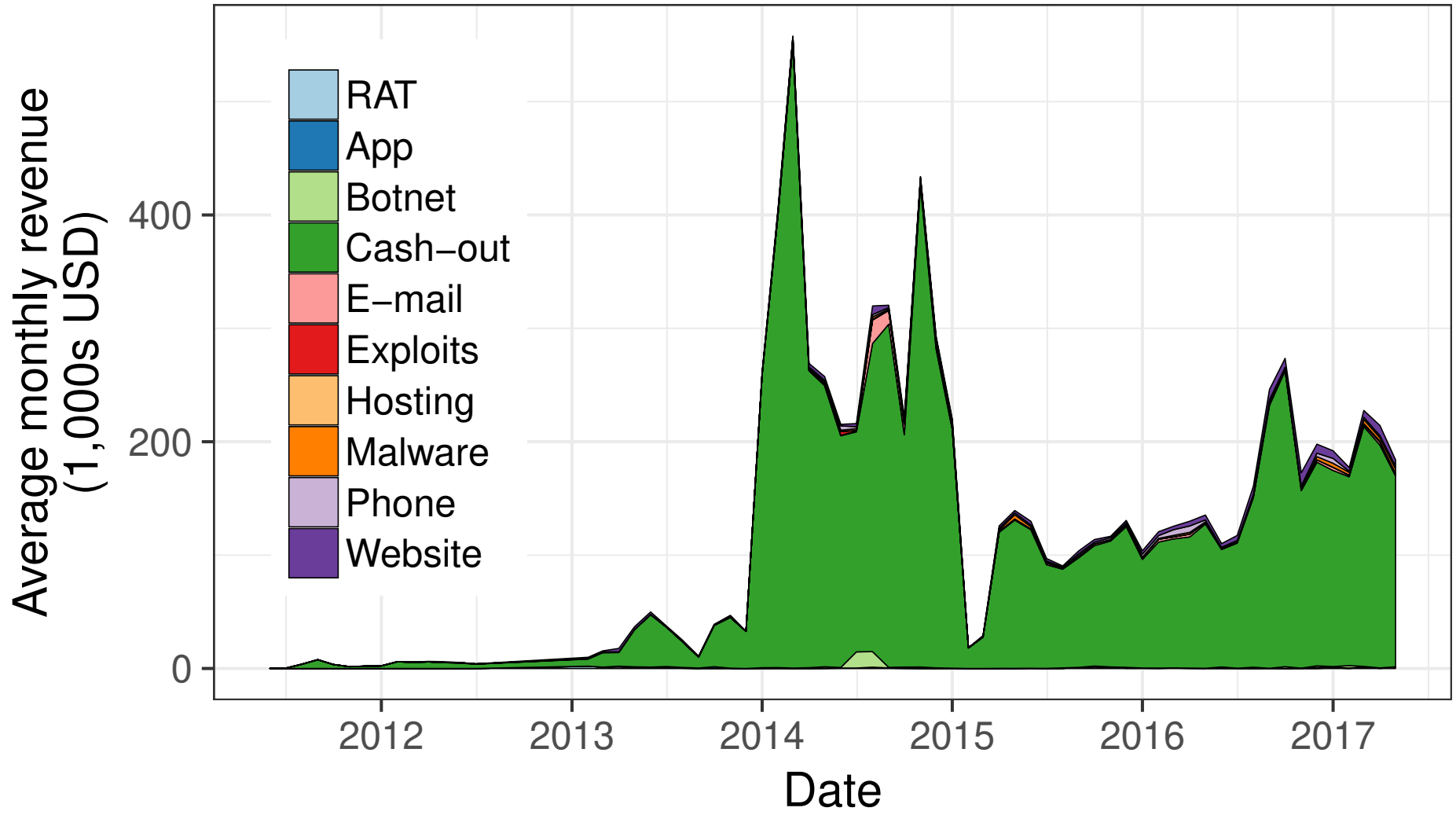


Listings, feedbacks and revenue over time

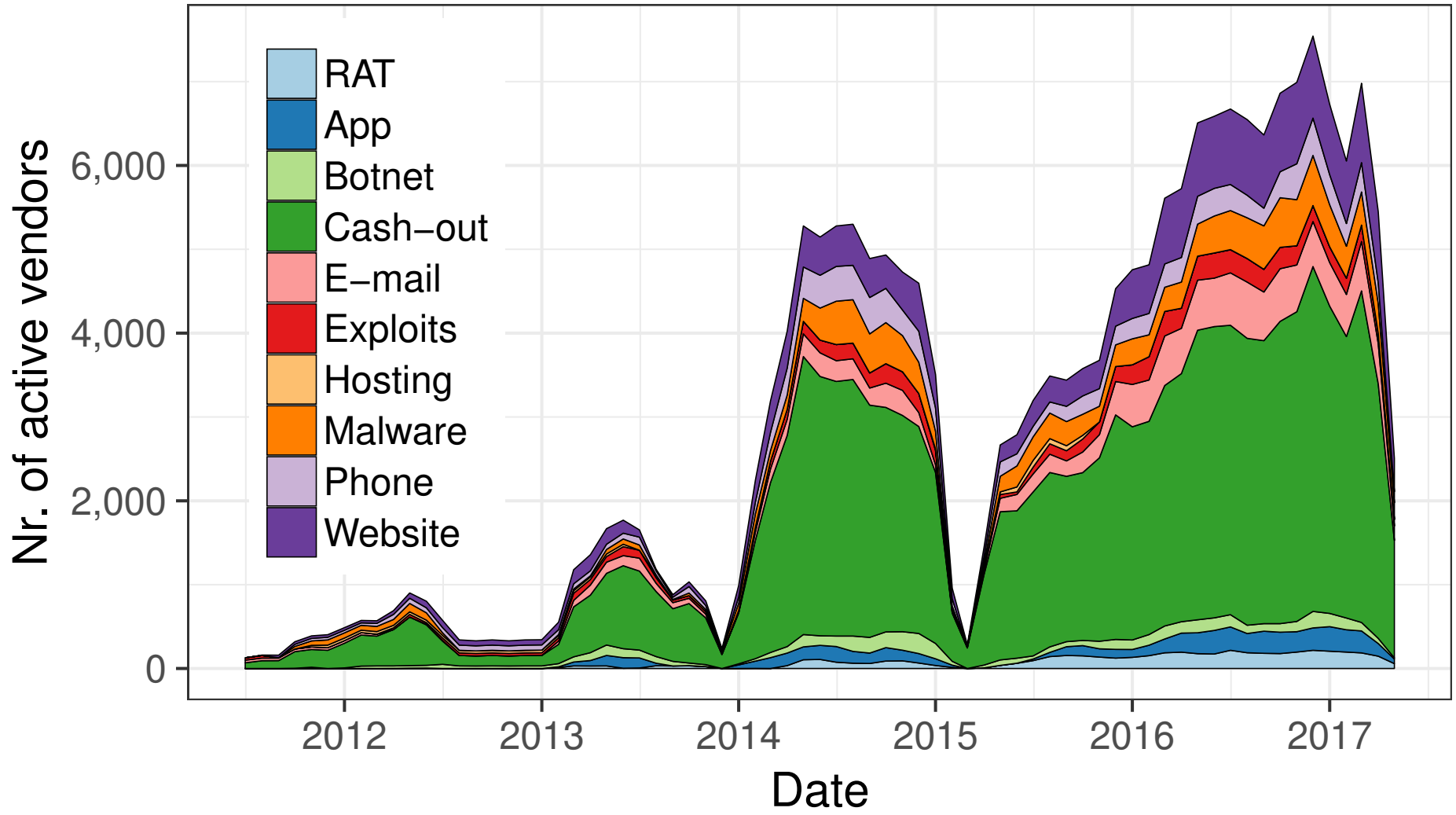




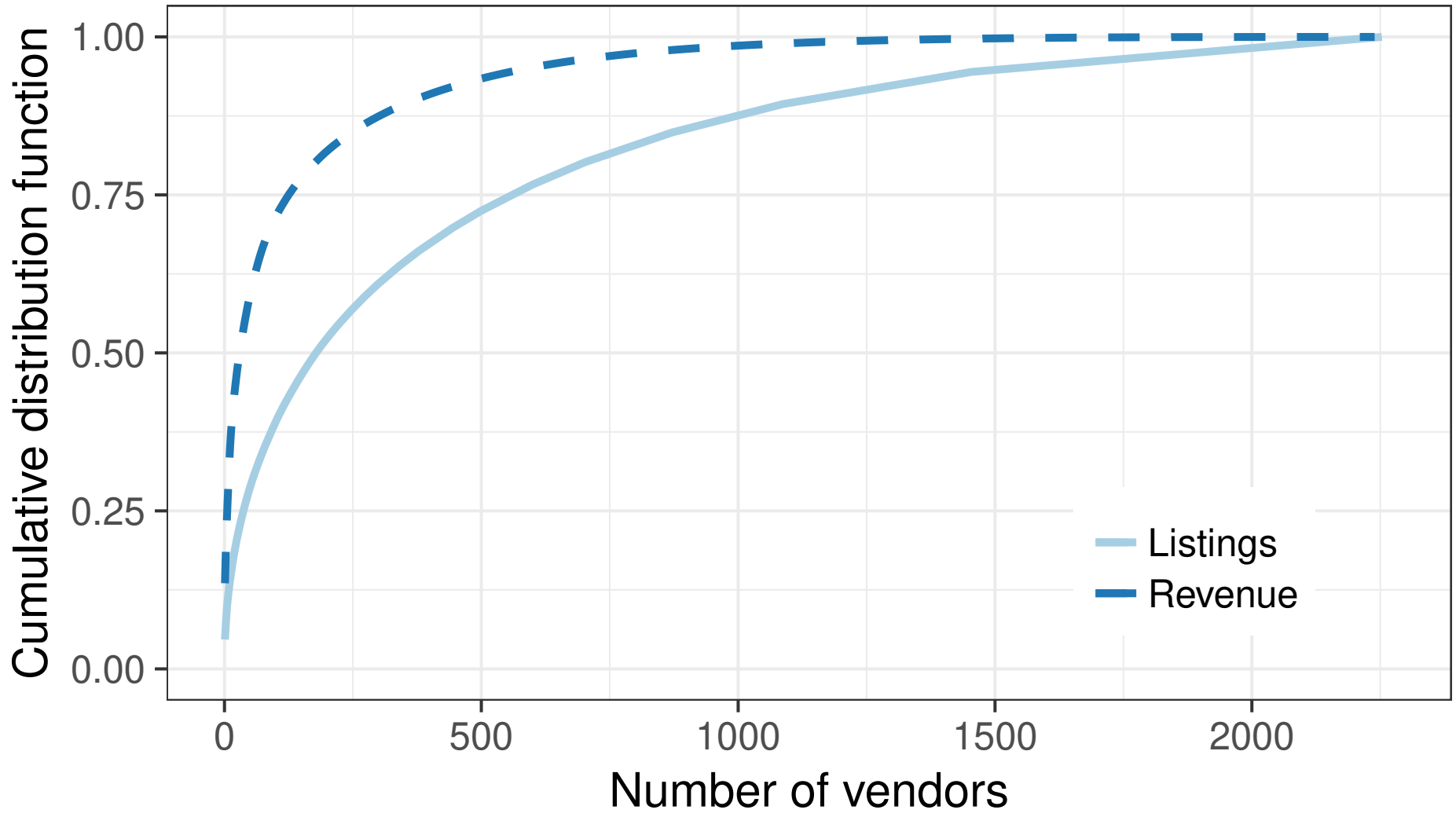
Total revenue per category per month



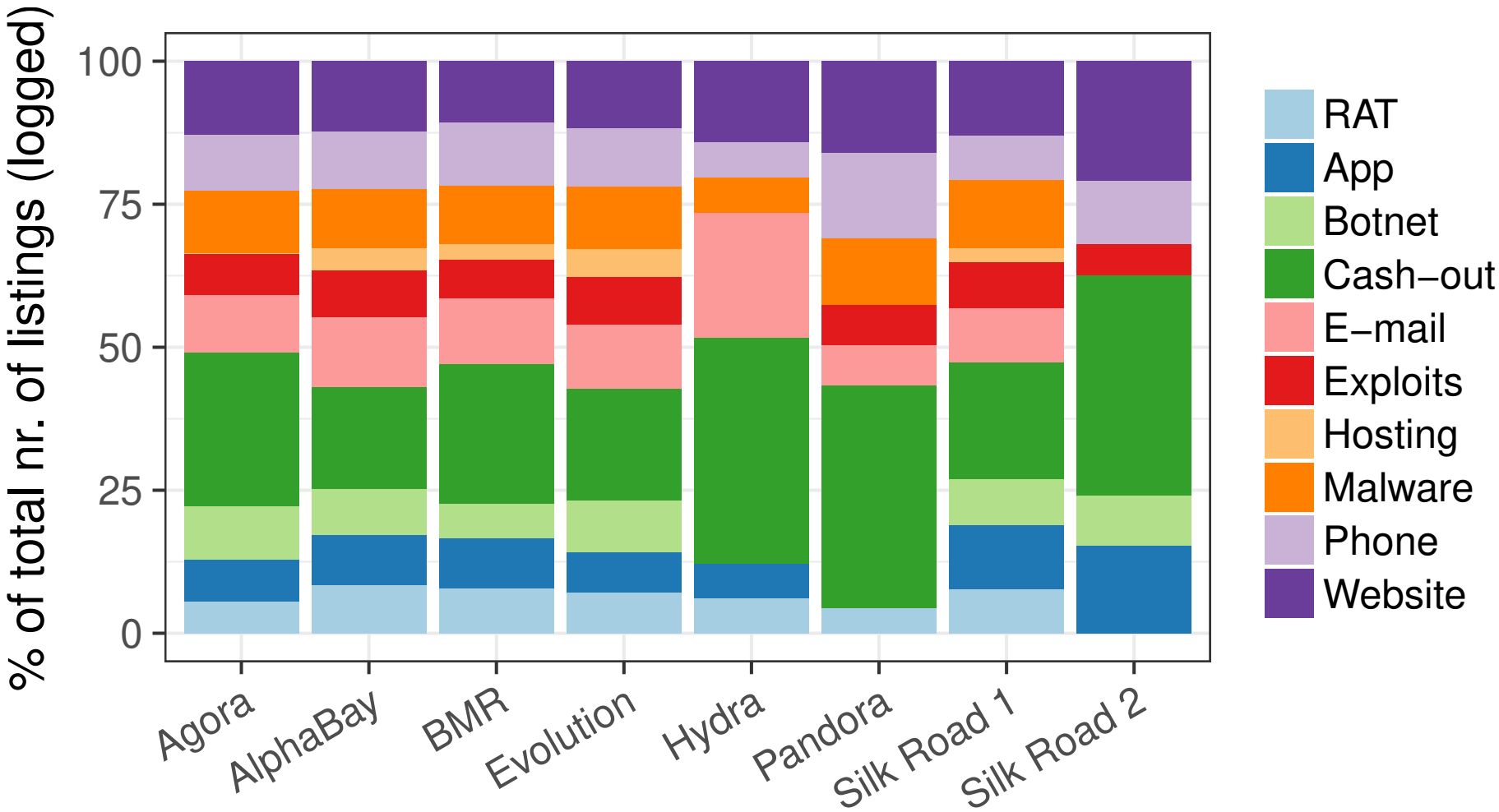
Number of active vendors per month



Cumulative percentage of listings across vendors



Product portfolios of markets



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/