black hat USA 2021

The Mass Effect:

How Opportunistic Workers Drift into Cybercrime

Masarah Paquet-Clouston (GoSecure)
Serge-Olivier Paquette (SecureWorks)
Sebastian Garcia (Stratosphere Lab)
Maria Jose Erquiaga (Cisco Systems)

MASS EFFECT

Geost

Found investigating HtBot

Android banking trojan botnet

Infected 800,000 Russian phones

Chatlog found on VirusTotal

Geost

Found investigating HtBot

Android banking trojan botnet

Infected 800,000 Russian phones

Chatlog found on VirusTotal

The Chatlog

6,000 messages from June 2017 to April 2018

Discuss Geost key information

3 key actors:

- Entrepreneur
- Developer
- Webmaster

Geost

Found investigating HtBot

Android banking trojan botnet

Infected 800,000 Russian phones

Chatlog found on VirusTotal

The Chatlog

6,000 messages from June 2017 to April 2018

Discuss Geost key information

3 key actors:

- Entrepreneur
- Developer
- Webmaster

The Forum

Searchengine.guru with ~ ½ million users

Russian-speaking internet marketing platform

Sparked the notion of **informal workforce**

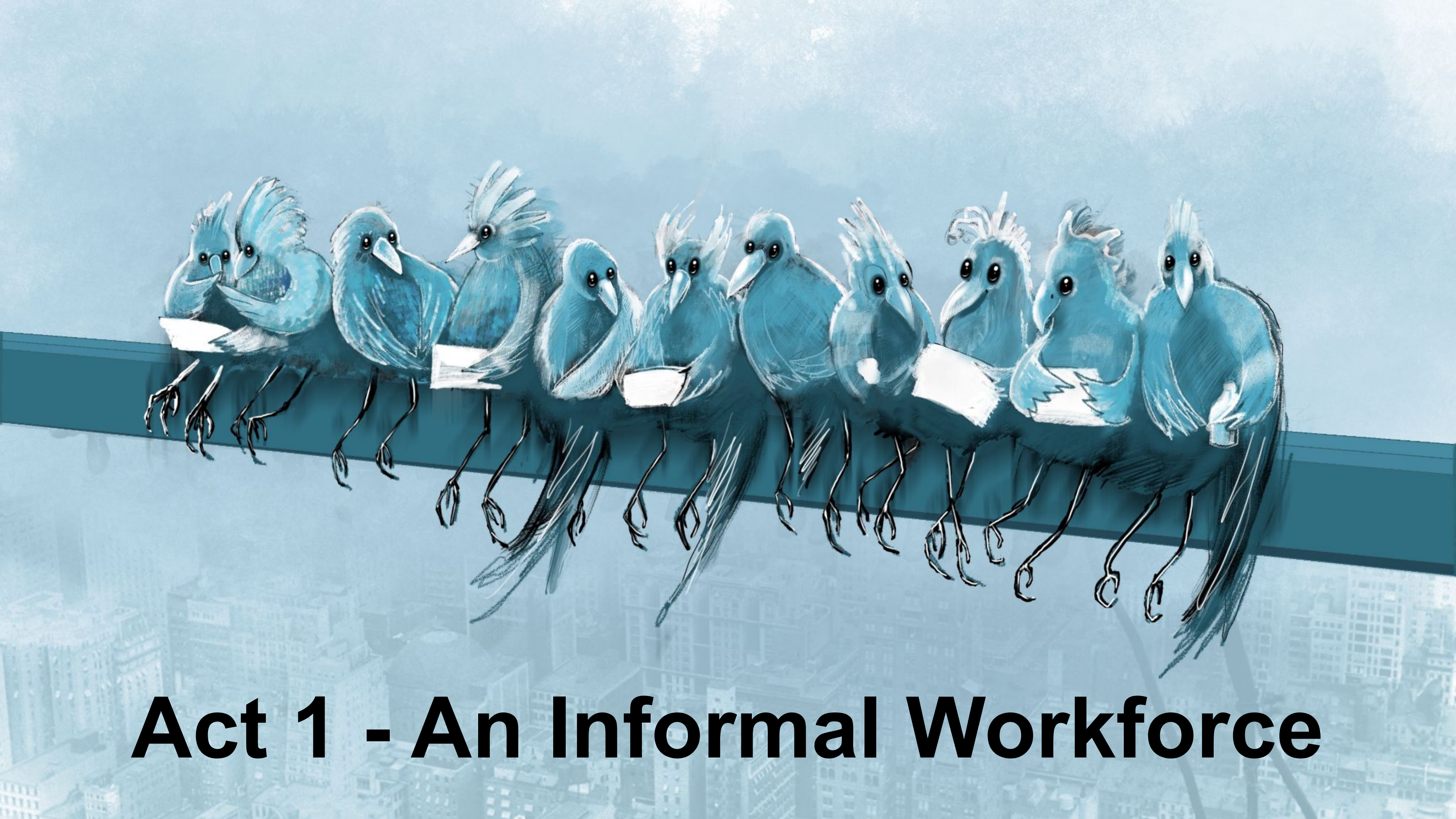
Act 1 - An Informal Workforce

Act 2 - Dancing on the Crime Line

Act 3 - Drifters

Act 4 - Migration

Act 5 - Mass Effect



Act 1 - An Informal Workforce

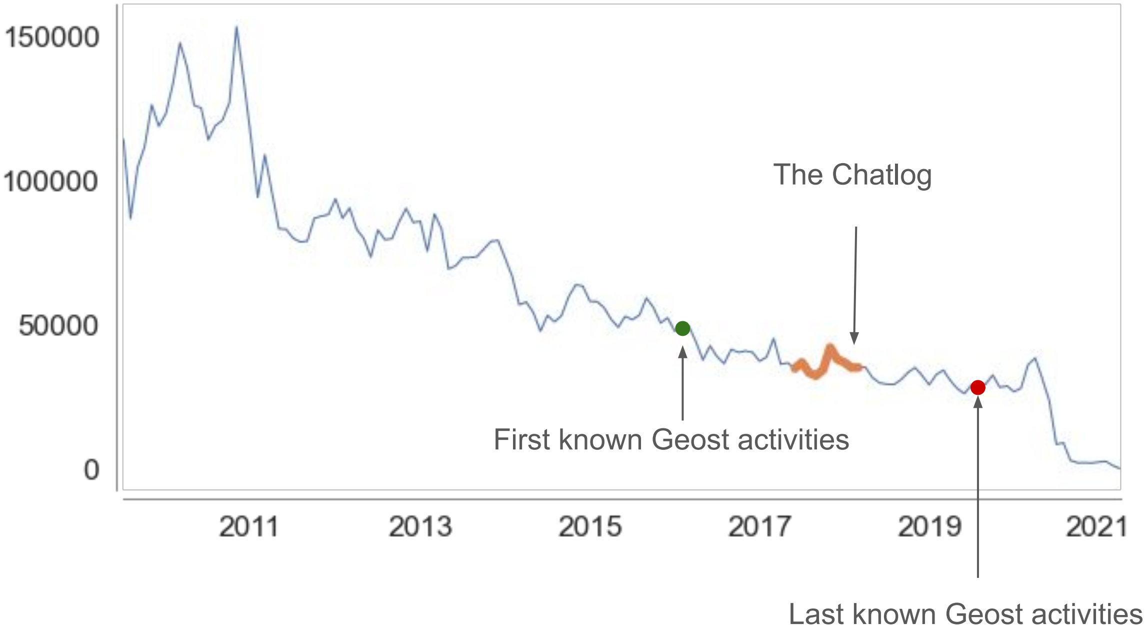
The Forum

“[...] a website allowing users to discuss issues related to creating and promoting websites on the Internet.”[1]

[1] searchengine.guru

Is the Forum in decline?

Posts/Month



20 years old

400,000 users

14,000,000 posts

Uncovering an Informal Workforce

Category	Subcategories	% of Posts
About Monetizing Sites	Partnership Programs, General Questions about Making Money on Sites, YouTube Monetization	20%
Not About Work	Meetings and Gatherings, Smoking Room, About the Site and Forum	17%
Site Building	Domain Names, Hosting and Servers for Websites, Web Analytics, Copywriting	16%
Communication of Professionals	Cryptocurrencies, Ecommerce, Social Media Marketing	14%
Practical Optimization Issues	Popular SEO and SEO Newbie Questions, **Doorways and Cloaking**, General Optimization Issues	13%
Search Engine	Yandex, Site Directories, Google	10%
Exchange and Sale	Buying and Selling Sites, Digital Goods, Programs and Scripts	5%
Work and Service for Webmaster	Copywriting Translations, Social Media Marketing Services, Optimization Promotion and Audit	3%
About Purchased Traffic for Websites	Teaser and Banner Advertising, Contextual Advertising, Yandex Direct, Google Ads	2%

Informal Economies

Hence, workforce...

All income-earning activities that are not regulated by the state in economic environments where similar activities are regulated.

How can forum users be mapped?

Mapping the Forum

Forum Post

```
user_name        colllect
user_id          1120295.0
topic_id         981979
topic_title      Обновление поисковой базы 01.01.18
content          Цитата:Сообщение от raskTC [...]
category         search_engines
sub_category     yandex
date             2018-01-01 23:58:00
post_id          15413443
```

Mapping the Forum

Forum Post

```
user_name       colllect
user_id         1120295.0
topic_id        981979
topic_title     Обновление поисковой базы 01.01.18
content         Цитата:Сообщение от raskTC [...]
category        search_engines
sub_category    yandex
date            2018-01-01 23:58:00
post_id         15413443
```

Numerical Representation

Category \ Username	colllect
Search Engines	22
Not About Work	222
About Monetizing Sites	3
Practical Optimization Issues	1
Communication of Professionals	95
Site Building	19
Exchange and Sales	7
About Purchased Traffic for Websites	1
Work and Services for Webmasters	0

Mapping the Forum

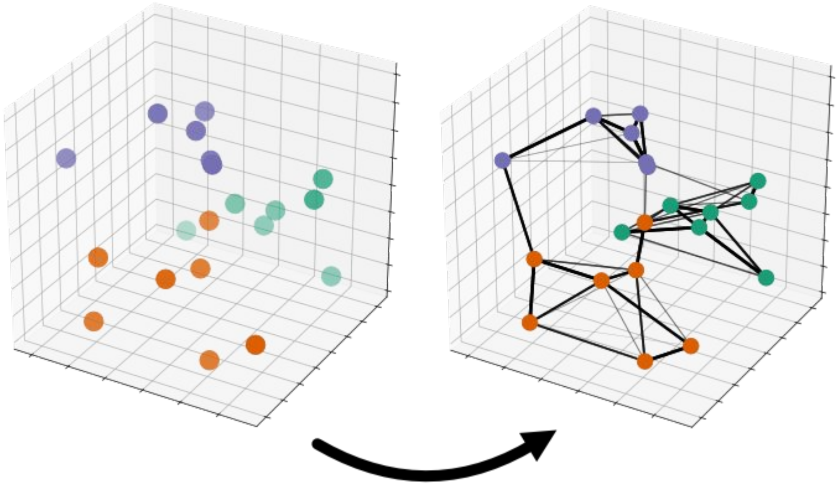
Category \ Actor Name	A	B	C	D	E	F
Search Engines	22	20	0	33	0	0
Not About Work	222	45	0	6	0	0
About Monetizing Sites	3	8	0	0	1	0
Practical Optimization Issues	1	32	0	47	0	0
Communication of Professionals	95	19	7	1	0	0
Site Building	19	64	0	0	0	0
Exchange and Sales	7	0	0	1	0	1
About Purchased Traffic for Websites	1	0	0	0	0	0
Work and Services for Webmasters	0	0	0	1	0	0

Mapping the Forum

Category \ Actor Name	A	B	C	D	E	F
Search Engines	22	20	0	33	0	0
Not About Work	222	45	0	6	0	0
About Monetizing Sites	3	8	0	0	1	0
Practical Optimization Issues	1	32	0	47	0	0
Communication of Professionals	95	19	7	1	0	0
Site Building	19	64	0	0	0	0
Exchange and Sales	7	0	0	1	0	1
About Purchased Traffic for Websites	1	0	0	0	0	0
Work and Services for Webmasters	0	0	0	1	0	0

Mapping the Forum

UMAP finds a convenient 2D representation of multidimensional user data

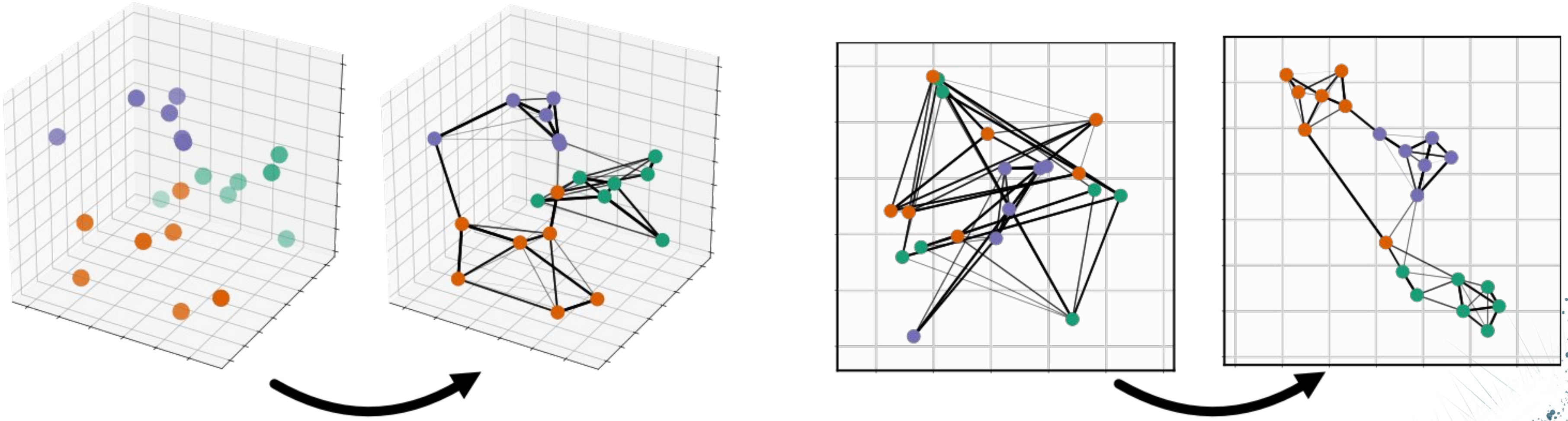


Compute a graphical representation of the dataset

Sainburg, Tim and McInnes, Leland and Gentner, Timothy Q., "Parametric UMAP: learning embeddings with deep neural networks for representation and semi-supervised learning"

Mapping the Forum

UMAP finds a convenient 2D representation of multidimensional user data

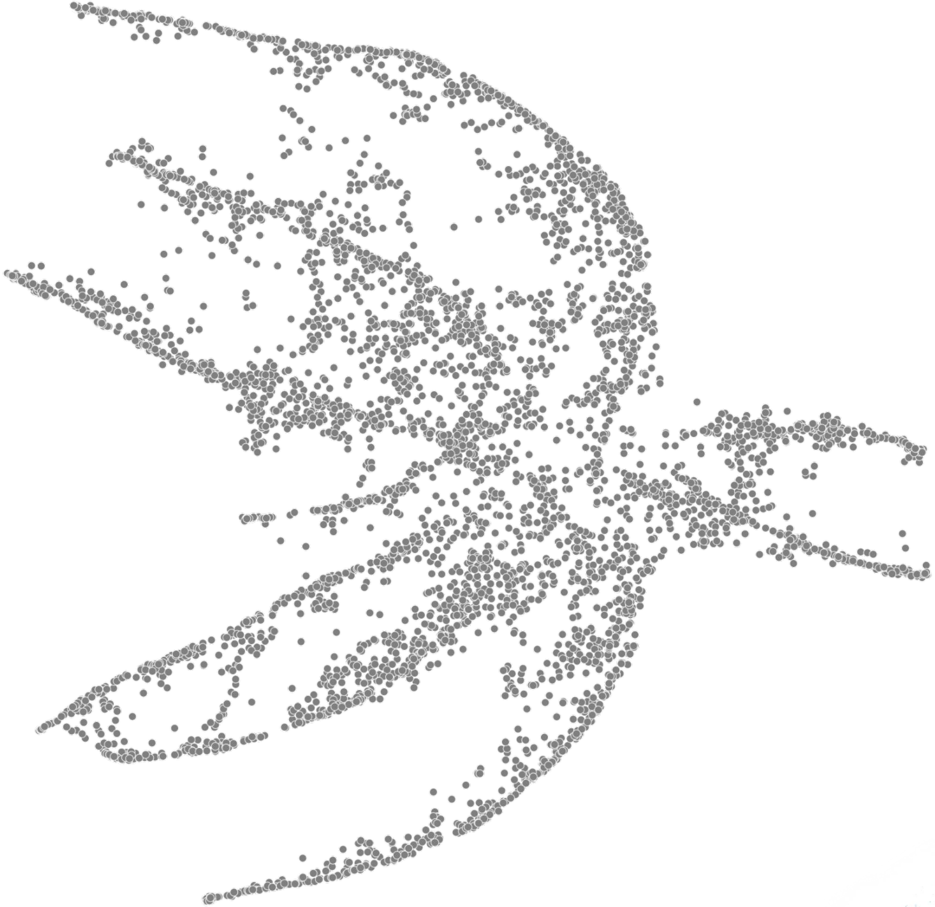


Compute a graphical representation of the dataset

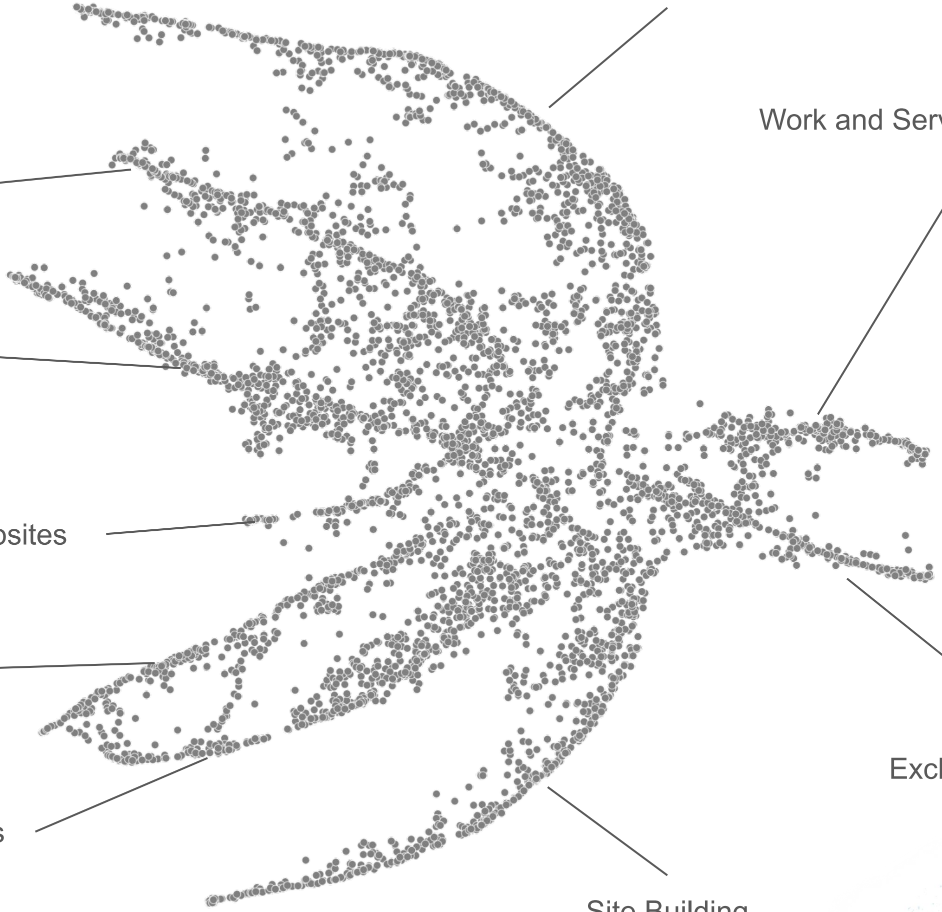
Learn an embedding that preserves the structure of the graph

Sainburg, Tim and McInnes, Leland and Gentner, Timothy Q., “Parametric UMAP: learning embeddings with deep neural networks for representation and semi-supervised learning”

The Map



The Map



About Monetizing Sites

Work and Services for Webmasters

Search Engines

Practical Optimization Issues

About Purchased Traffic for Websites

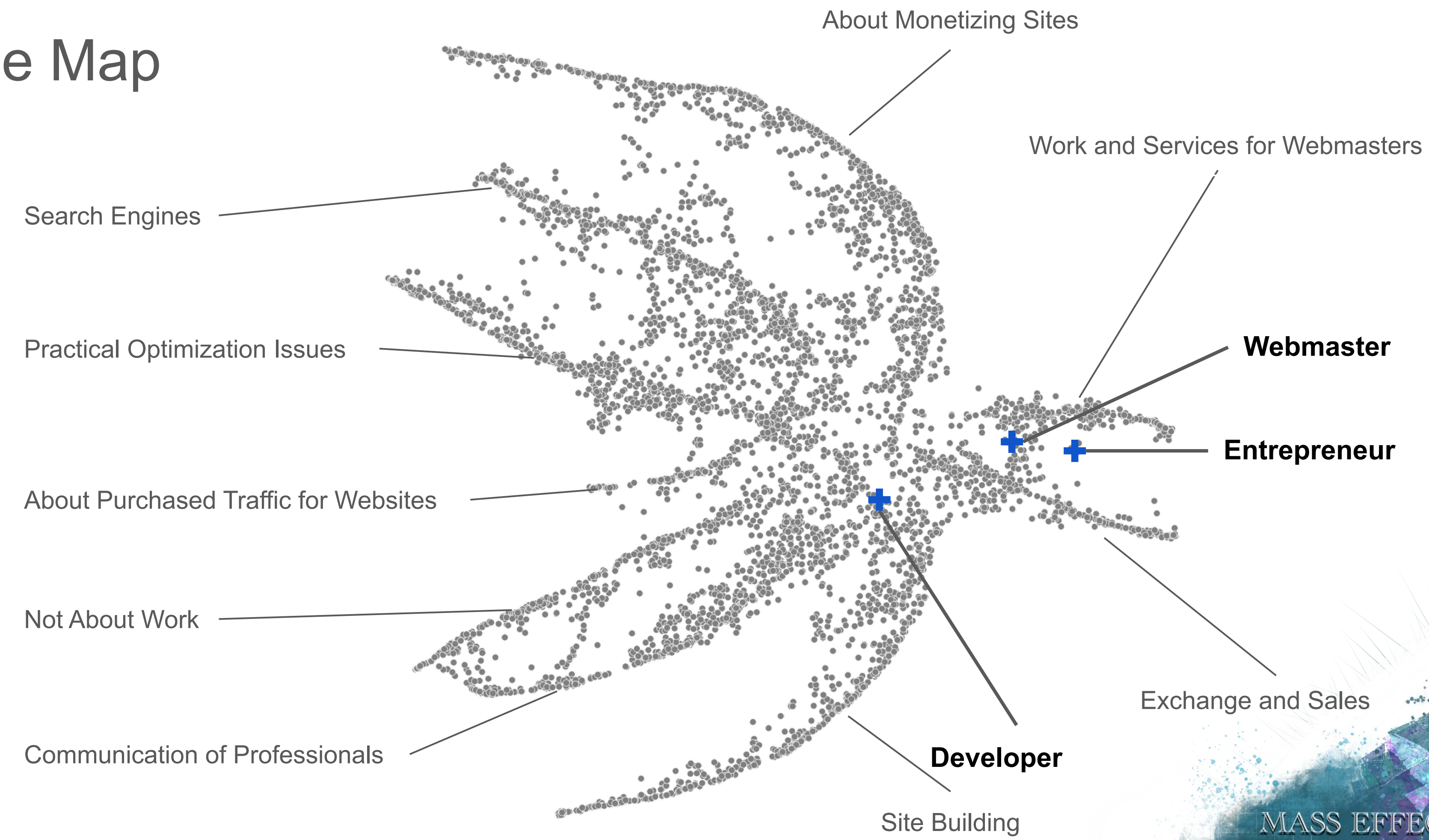
Not About Work

Communication of Professionals

Site Building

Exchange and Sales

The Map



MASS EFFECT

Informal Workforce
Dancing on the Crime Line
Drifters
Migration
Mass Effect

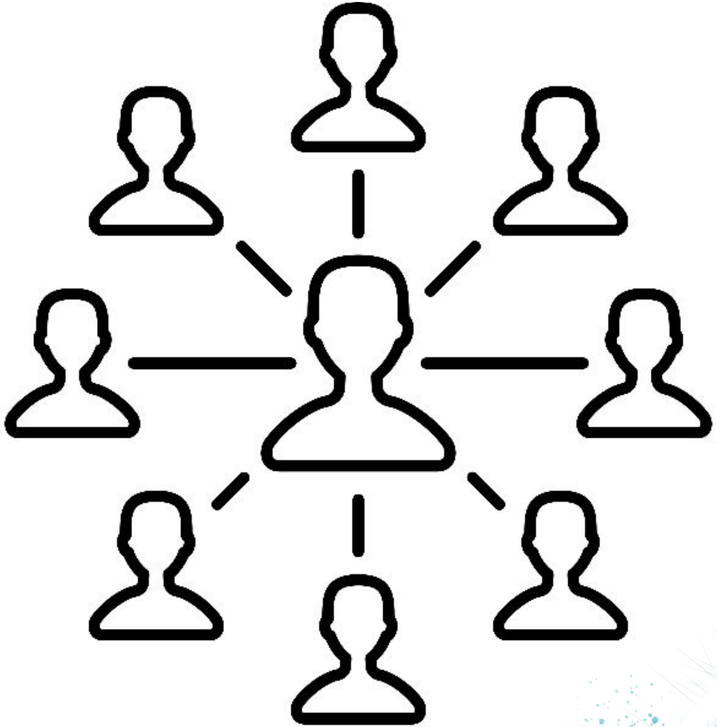
What kind of business are they involved in?

Act 2 - Dancing on the Crime Line

Private Chat Log

6,000 messages

Entrepreneur and 32 of his business partners



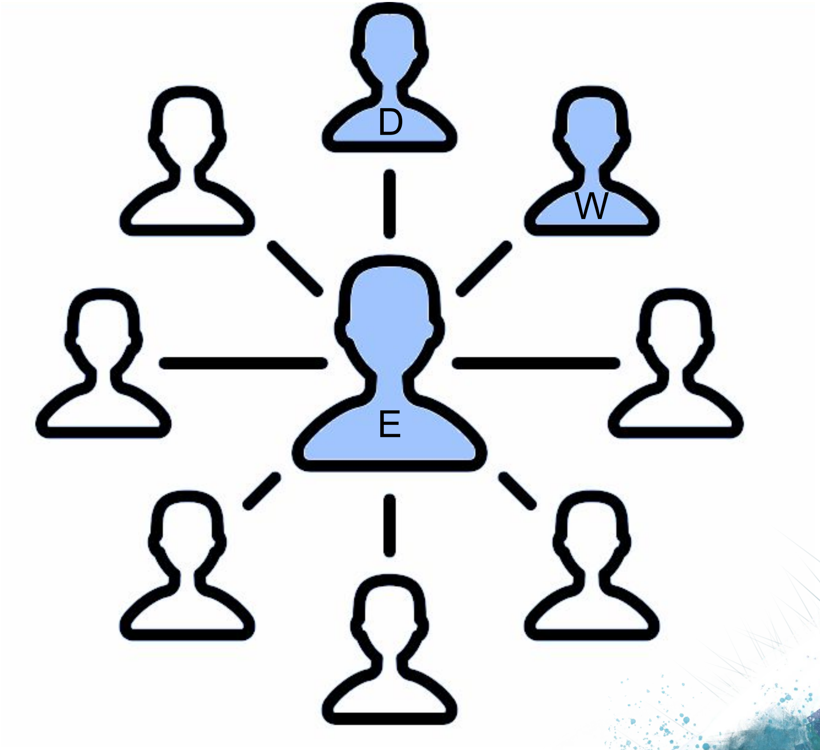
Private Chat Log

6,000 messages

Entrepreneur and 32 of his business partners

2 key partners:

- Developer
- Webmaster



Private Chat Log

6,000 messages

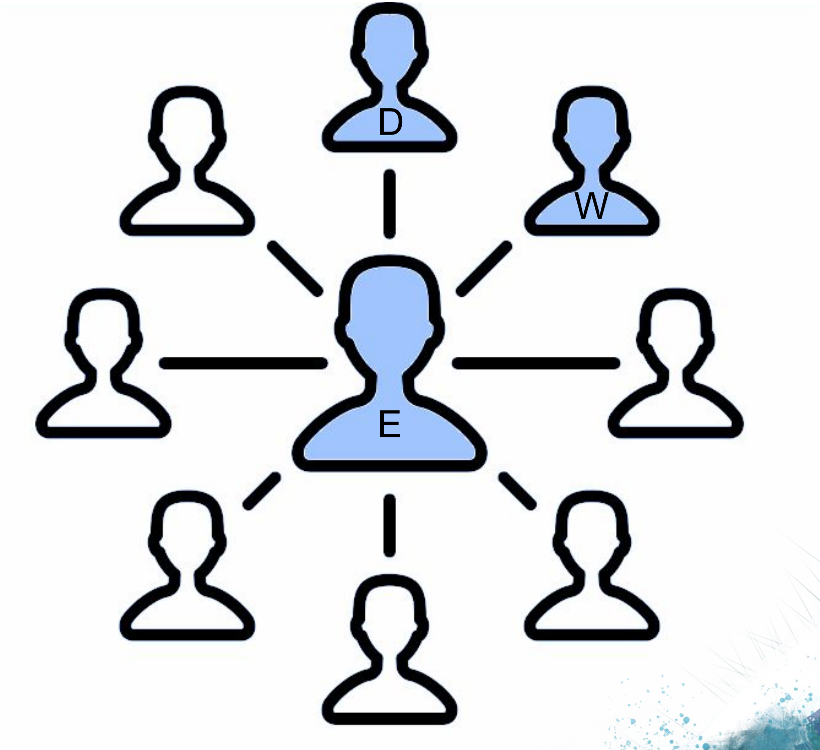
Entrepreneur and 32 of his business partners

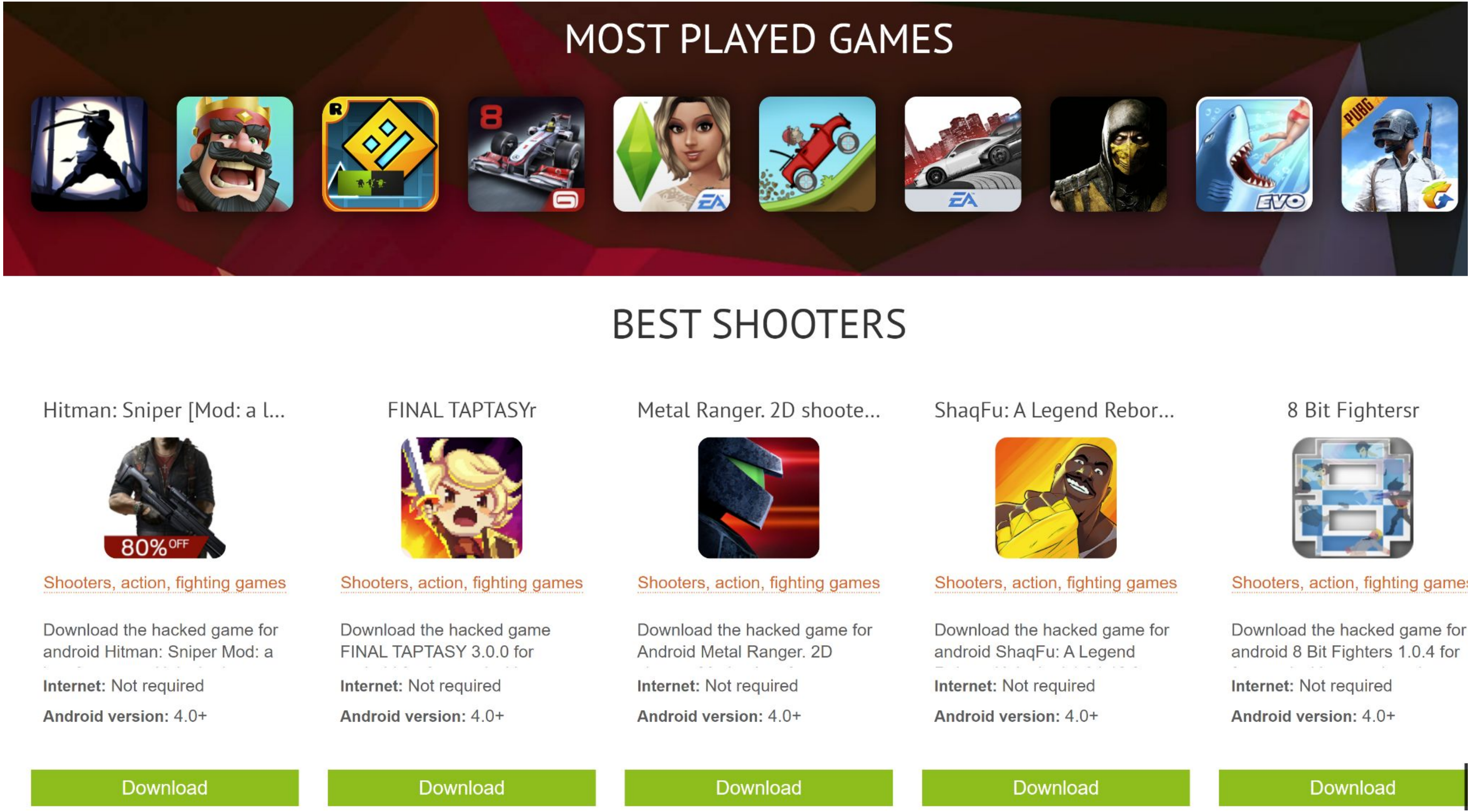
2 key partners:

- **D**eveloper
- **W**ebmaster

Business:

- Develop Android portals (for infected APKs)





MOST PLAYED GAMES

BEST SHOOTERS

Hitman: Sniper [Mod: a l...

Shooters, action, fighting games

Download the hacked game for android Hitman: Sniper Mod: a

Internet: Not required

Android version: 4.0+

Download

FINAL TAPTASYr

Shooters, action, fighting games

Download the hacked game FINAL TAPTASY 3.0.0 for

Internet: Not required

Android version: 4.0+

Download

Metal Ranger. 2D shoote...

Shooters, action, fighting games

Download the hacked game for Android Metal Ranger. 2D

Internet: Not required

Android version: 4.0+

Download

ShaqFu: A Legend Rebor...

Shooters, action, fighting games

Download the hacked game for android ShaqFu: A Legend

Internet: Not required

Android version: 4.0+

Download

8 Bit Fightersr

Shooters, action, fighting game

Download the hacked game for android 8 Bit Fighters 1.0.4 for

Internet: Not required

Android version: 4.0+

Download

Thematic Analysis

Thematic Analysis

Adverse Business Environment

- Unreliable Business Partners
- Unstable Payments
- Declining Business Prospects
- Low profitability

Adverse Business Environment

“*Same story, and the programmer keeps disappearing all the time*”

Webmaster , October 2017

“Well, nothing you can do. You should always be prepared. This business is not stable”

Webmaster, October 2017

“*Installations are very cheap now*”

Entrepreneur, February 2018

“*SMS as in good old times*”

Entrepreneur, April 2018

“*There is nothing like this now*”

Webmaster, April 2018

“*Any news about the money?”*

Webmaster, November 2017

“*They will not give the money yet?*”

Webmaster, December 2017

“*Did they send it [money]?*”

Webmaster, March 2018

Adverse Business Environment

“*Same story, and the programmer keeps disappearing all the time*”

Webmaster , October 2017

“*Well, nothing you can do. You should always be prepared. This business is not stable”*

Webmaster, October 2017

“*Installations are very cheap now*”

Entrepreneur, February 2018

“*SMS as in good old times*”

Entrepreneur, April 2018

“*There is nothing like this now*”

Webmaster, April 2018

“*Any news about the money?”*

Webmaster, November 2017

“They will not give the money yet?”

Webmaster, December 2017

“*Did they send it [money]?*”

Webmaster, March 2018

Thematic Analysis

Adverse Business Environment

Amateur Work

- Lacking Technical Skills
- Working with (and Building) Defective Tools

Amateur Work

“Our sites are not high-quality, they will not last long”

Developer, December 2017

“In order for the protection to be effective, as well as to prevent reinfection, you need to set secure PHP settings.[…]”

SysAdmin Contractor, December 2017

“Hi, fix the parsers as you can, otherwise it’s not good without news (smiley)”

Entrepreneur, March 2018

“I am saying I don’t know how to split the traffic”

Entrepreneur, November 2017

Amateur Work

“Our sites are not high-quality, they will not last long”

Developer, December 2017

“In order for the protection to be effective, as well as to prevent reinfection, you need to set secure PHP settings.[…]”

SysAdmin Contractor, December 2017

“Hi, fix the parsers as you can, otherwise it’s not good without news (smiley)”

Entrepreneur, March 2018

“I am saying I don’t know how to split the traffic”

Entrepreneur, November 2017

Thematic Analysis

Adverse Business Environment

Amateur Work

Leniency Towards Criminality

- Shady Activities
- Fighting Security Measures
- Seeking Economic Independence

Leniency Towards Criminality

“Conversion rate is different, but there is no guarantee that total sum will be better than from legal”

Affiliate Marketer, November 2017

“Yes, I don’t see any prospects, I realized that I was led by the fact that others make good money […]

Developer, January 2018

“Hi, are you here? I have a proposal for you. Are you interested in these sorts of deals, you give cash, and the customer will transfer money to a bank account + 7%?”

Entrepreneur, January 2018

20:49 – Entrepreneur

[file name] the file, right?

20:50 – Website master

Yes

20:51 – Entrepreneur

Try to re-crypt.
and install.

21:17 – Webmaster

Done

21:26 – Entrepreneur

And again, change file.
Re-deployed

21:49 – Webmaster

Re-deployed

Leniency Towards Criminality

“Conversion rate is different, but there is no guarantee that total sum will be better than from legal”

Affiliate Marketer, November 2017

“Yes, I don’t see any prospects, I realized that I was led by the fact that others make good money […]

Developer, January 2018

“Hi, are you here? I have a proposal for you. Are you interested in these sorts of deals, you give cash, and the customer will transfer money to a bank account + 7%?”

Entrepreneur, January 2018

20:49 – Entrepreneur
[file name] the file, right?

20:50 – Website master
Yes

20:51 – Entrepreneur
Try to re-crypt.
and install.

21:17 – Webmaster
Done

21:26 – Entrepreneur
And again, change file.
Re-deployed

21:49 – Webmaster
Re-deployed

Thematic Analysis

Adverse Business Environment

Amateur Work

Leniency Towards Criminality

What are they doing on the Forum?

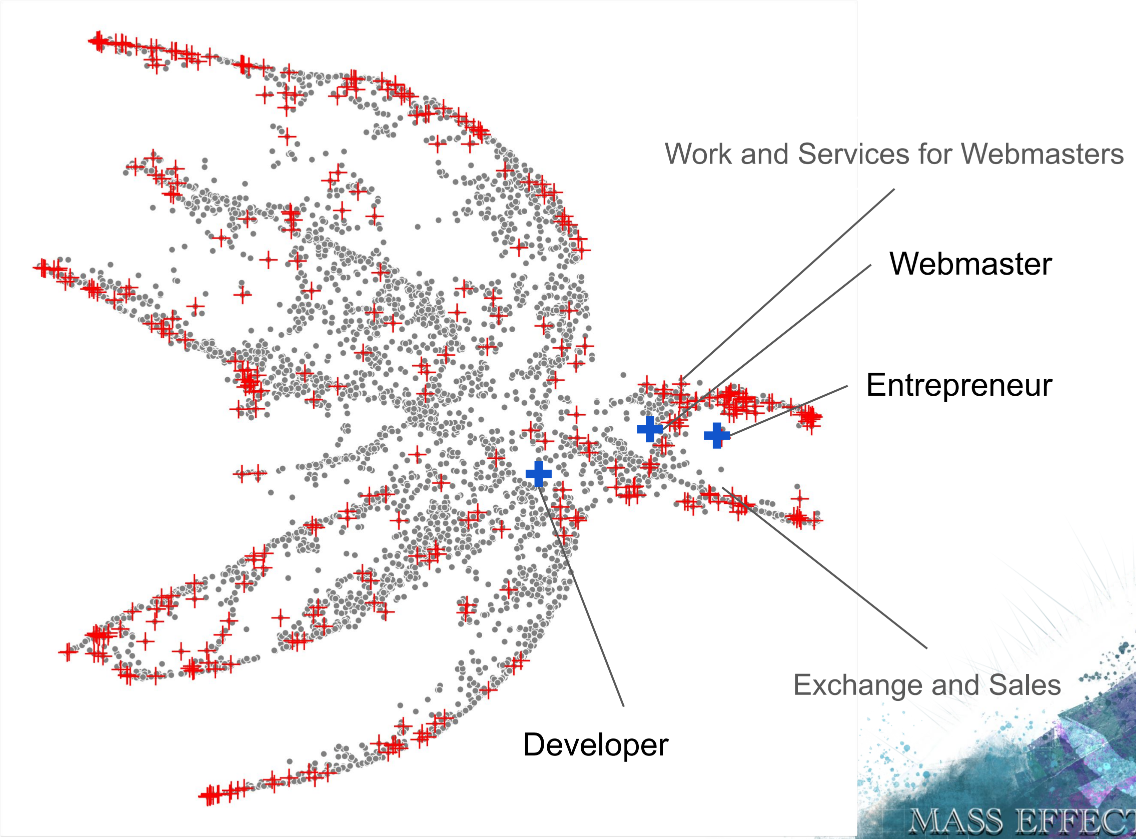
Informal Workers

- **Entrepreneur**: 1,385 comments, 759 threads, 2009 - 2020
- **Webmaster**: 172 comments, 69 threads, 2012 - 2019
- **Developer**: 471 comments, 331 threads, 2010 and 2019

Informal Workers

- **Entrepreneur**: 1,385 comments, 759 threads, 2009 - 2020
- **Webmaster**: 172 comments, 69 threads, 2012 - 2019
- **Developer**: 471 comments, 331 threads, 2010 and 2019

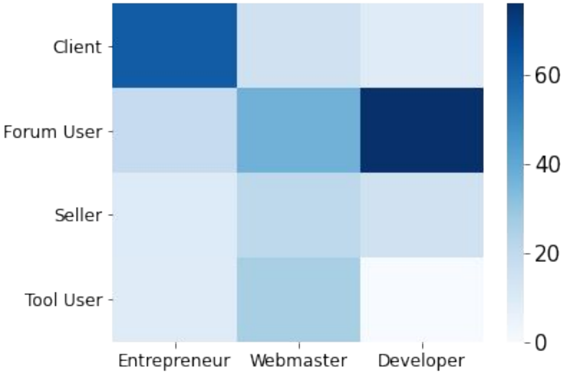
Users who interacted with them (n=509)



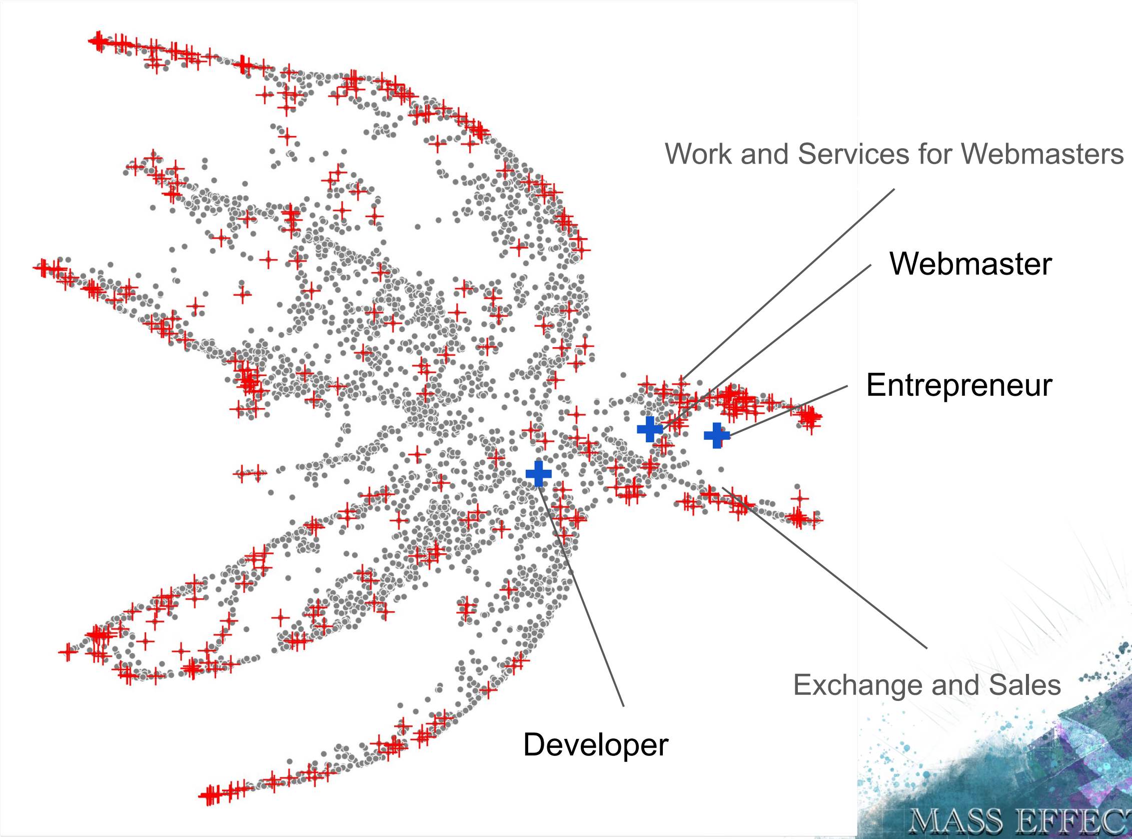
Informal Workers

- **Entrepreneur**: 1,385 comments, 759 threads, 2009 - 2020
- **Webmaster**: 172 comments, 69 threads, 2012 - 2019
- **Developer**: 471 comments, 331 threads, 2010 and 2019

Types of interactions



Users who interacted with them (n=509)



Informal Workforce
Dancing on the Crime Line
Drifters
Migration
Mass Effect

Is this dance commonplace?

Act 3 - Drifters

Drifters

Informal workers (forum users) who also participate in cybercrime forums

Identifying Drifters

Goal: Find the number of drifters on the Forum

Identifying Drifters

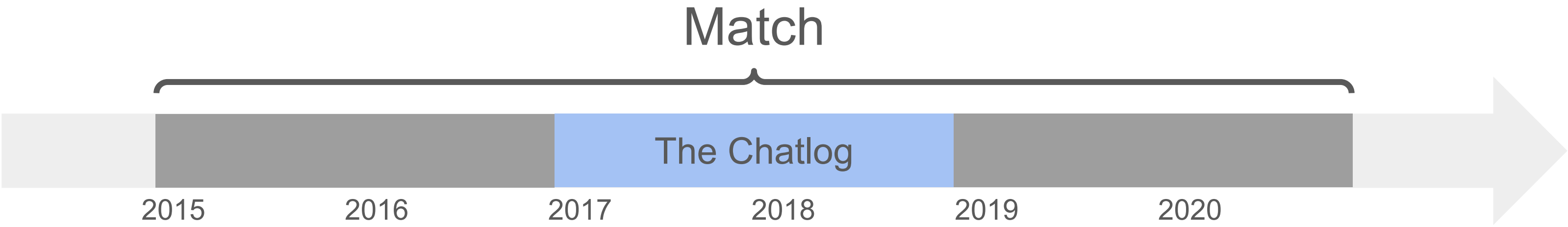
Username Filter: At least 5 characters AND an uppercase OR a number OR one special character

Examples

Match	Don’t Match
'Telin'	‘avadec’
'AndreyUK'	'basterr'
'Maxoo'	'foxi'
'2009bes'	’max’
'Tronix',	’uber’
'FrancisDarroze'	'kuprum'
'Ирина 5577'	'oxg'

Identifying Drifters

Timeframe Filter: Keep comments posted around 2017 and 2018 (+/- 2)



Identifying Drifters

Timeframe Filter: Keep comments posted around 2017 and 2018 (+/- 2)

Username Filter: At least 5 characters AND an uppercase OR a number OR one special character

38 platforms:
17 clearweb + 21 darkweb

Most common:

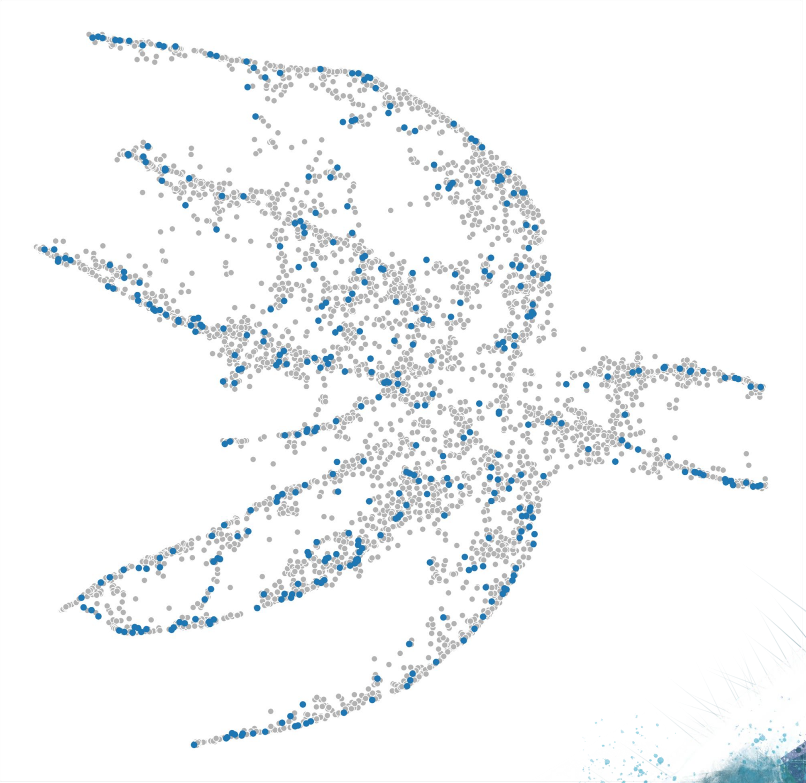
- Nulled.to	(cracking and leaks)
- Darkmoney	(money laundering)
- Besthackforum	(hacking)
- Exploit.in	(hacking)
- Blackhatworld	(black hat SEO)
- Club2crd	(carding)

Mapping Drifters

21,726 users fit the filter

1,557

identified as drifters (**7.2%**)



Are there characteristics that identify drifters on the forum?

Are they special? Do they form a specific group?

Distinguishing Drifters

Characteristics to discriminate?

- Activity Rate
- Diversification Level
- Potential Business Interactions
- Specialized Topics
- Etc.

Distinguishing Drifters

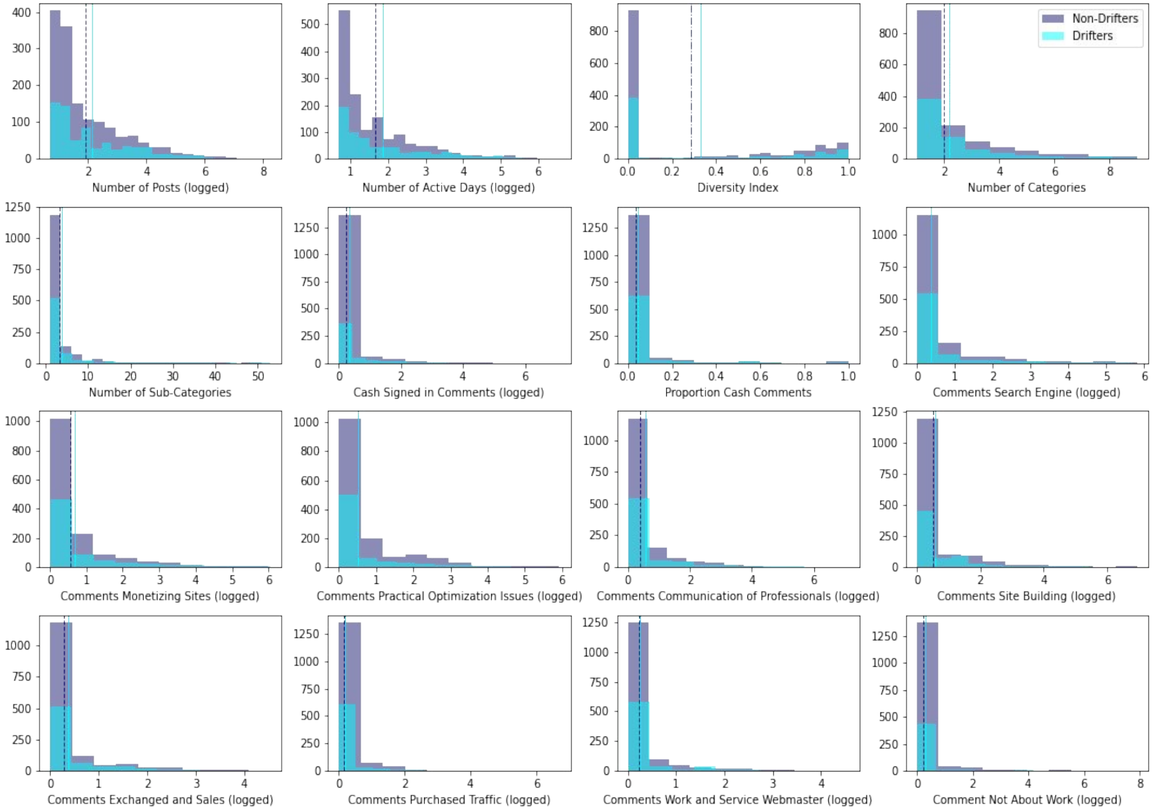
Characteristics to discriminate?

- Activity Rate
- Diversification Level
- Potential Business Interactions
- Specialized Topics
- Etc.

Mann-Whitney U Tests

- Assesses if the distributions differ
- No assumptions on the distributions
- Uses rank instead of direct value

Distinguishing Drifters



Indistinguishable Drifters?

Drifters and non-drifters are indistinguishable

(Based on all discriminatory variables we can think of)

The drifter population must be larger than 7%

Informal Workforce
Dancing on the Crime Line
Drifters
Migration
Mass Effect

Is there a relationship between informality and criminality **over time**?

Act 4 - Migration

Migration Measure

$$E/I\ Ratio_{\ t} = \frac{x_{e,t} - x_{i,t}}{x_{e,t} + x_{i,t}}$$

E/I → 1 --- perfect migration

E/I → 0 --- perfect balance

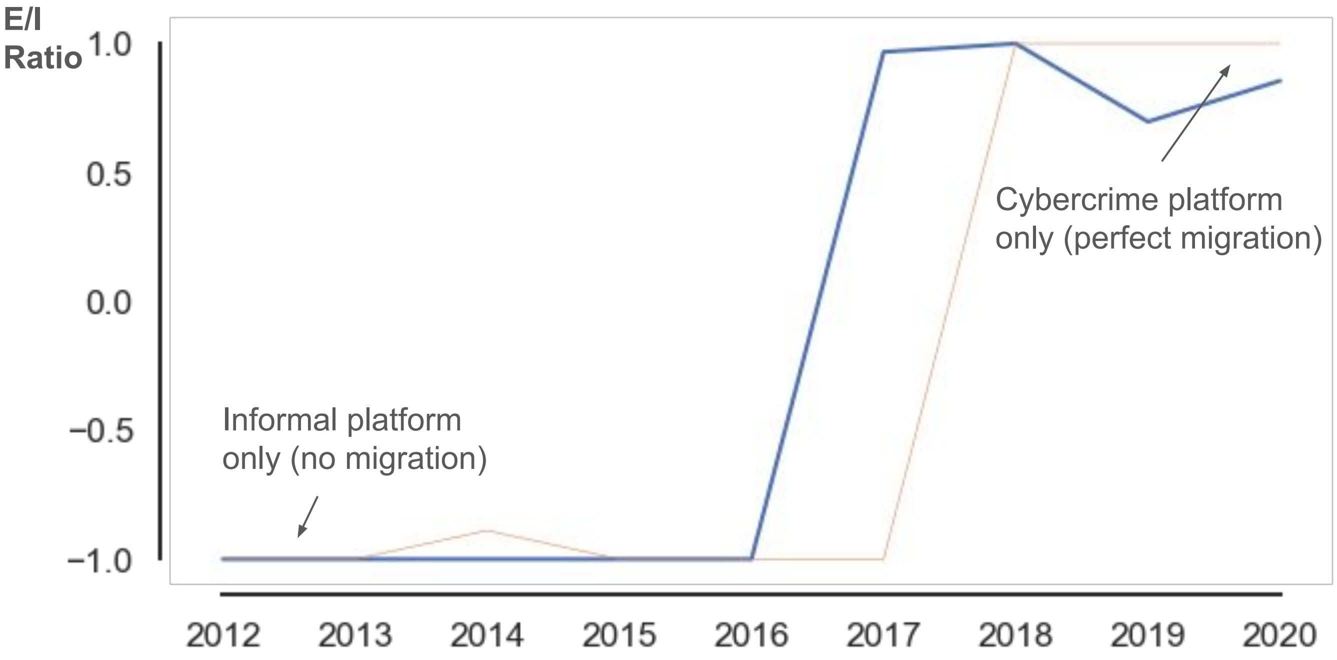
E/I → -1 --- no migration at all

Migration Measure

Methodology: Collect drifter data from 2012 to 2020 and compute the E/I ratio of individuals over the years.

Migration Measure

Methodology: Collect drifter data from 2012 to 2020 and compute the E/I ratio of individuals over the years.

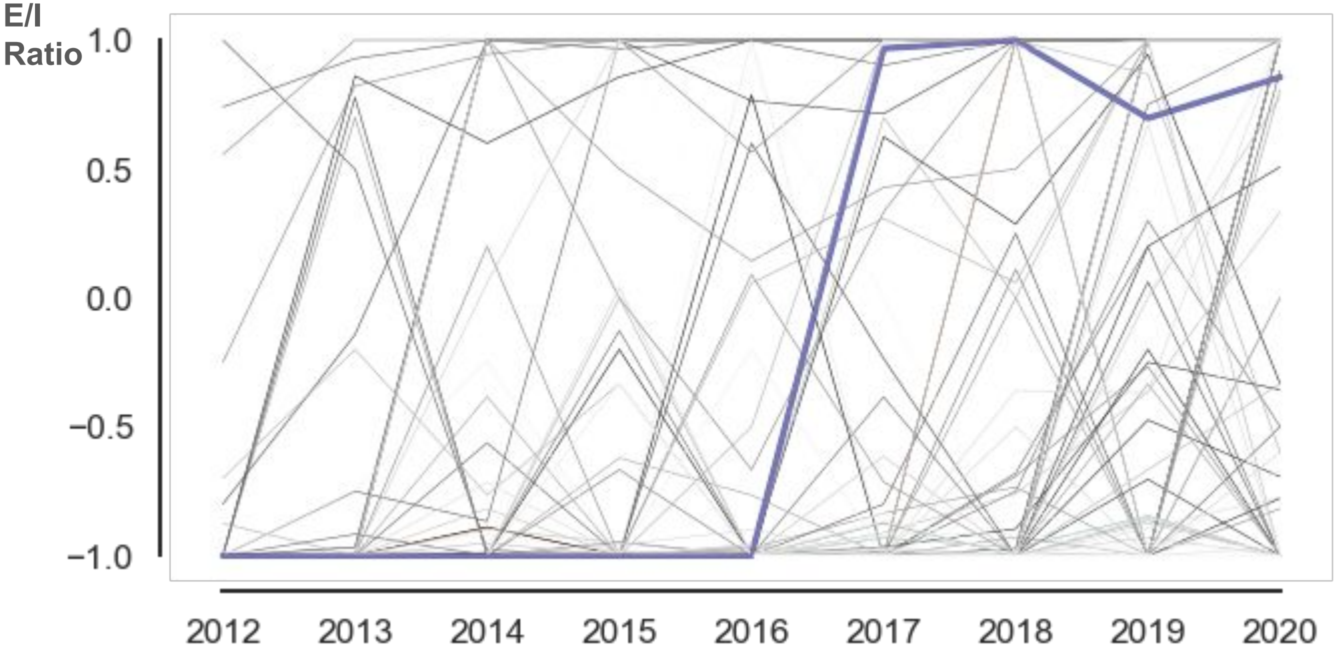


Trajectory:

The evolution of an individual’s outcome variable over time (e.g. E/I ratio)

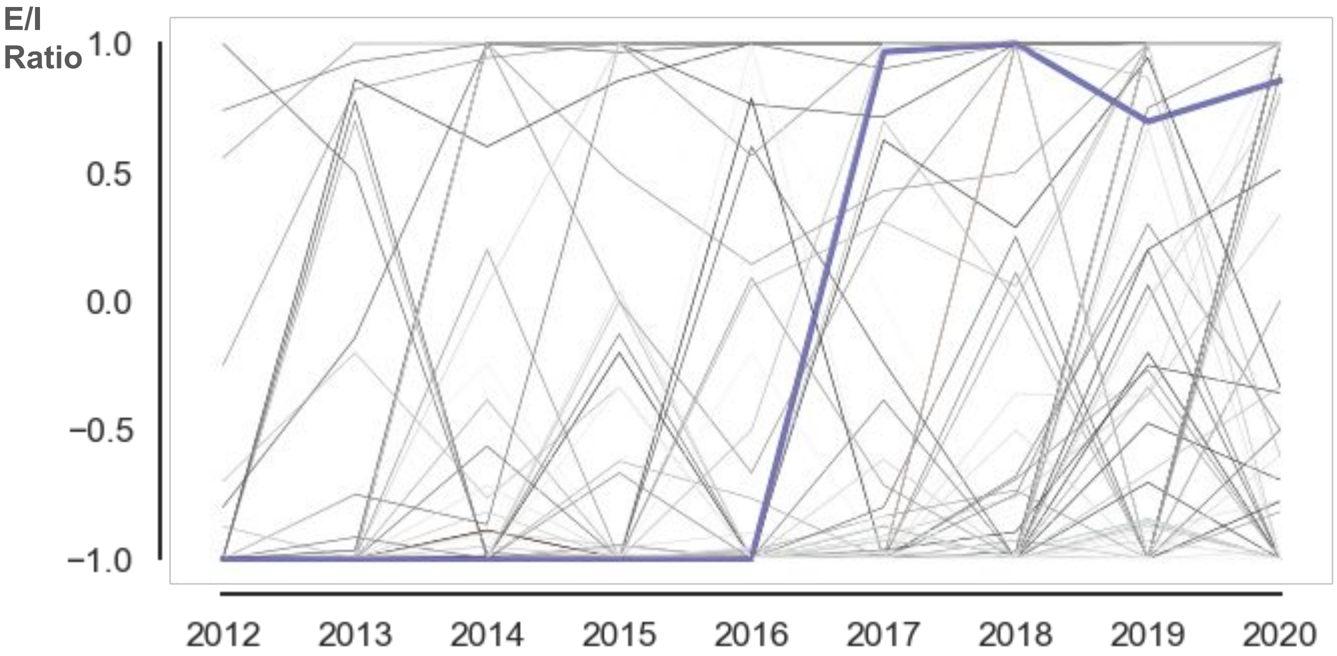
Migration Measure

Methodology: Collect drifter data from 2012 to 2020 and compute the E/I ratio of individuals over the years.



Migration Measure

Methodology: Collect drifter data from 2012 to 2020 and compute the E/I ratio of individuals over the years.



Can we find groups of similar users?

Group Based Trajectory Modeling

Group Based Trajectory Modeling

Latent explanatory variable

As opposed to observable variables, latent variables are not directly observed but are rather inferred

Step 1 - Determine optimal number of groups

Group Based Trajectory Modeling

Latent explanatory variable

As opposed to observable variables, latent variables are not directly observed but are rather inferred

Step 1 - Determine optimal number of groups

Mixture models

Probabilistic model for representing the presence of subpopulations within an overall population

Step 2 - Determine the shape of their distribution

Group Based Trajectory Modeling

Latent explanatory variable

As opposed to observable variables, latent variables are not directly observed but are rather inferred

Step 1 - Determine optimal number of groups

Mixture models

Probabilistic model for representing the presence of subpopulations within an overall population

Step 2 - Determine the shape of their distribution

Maximum likelihood

Method of estimating the parameters of the models

Step 3 - Fit the best model from the data

Group Based Trajectory Modeling

Latent explanatory variable

As opposed to observable variables, latent variables are not directly observed but are rather inferred

Step 1 - Determine optimal number of groups

Mixture models

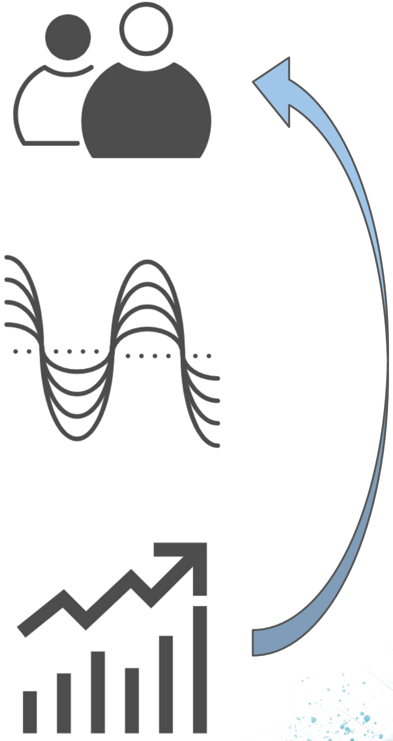
Probabilistic model for representing the presence of subpopulations within an overall population

Step 2 - Determine the shape of their distribution

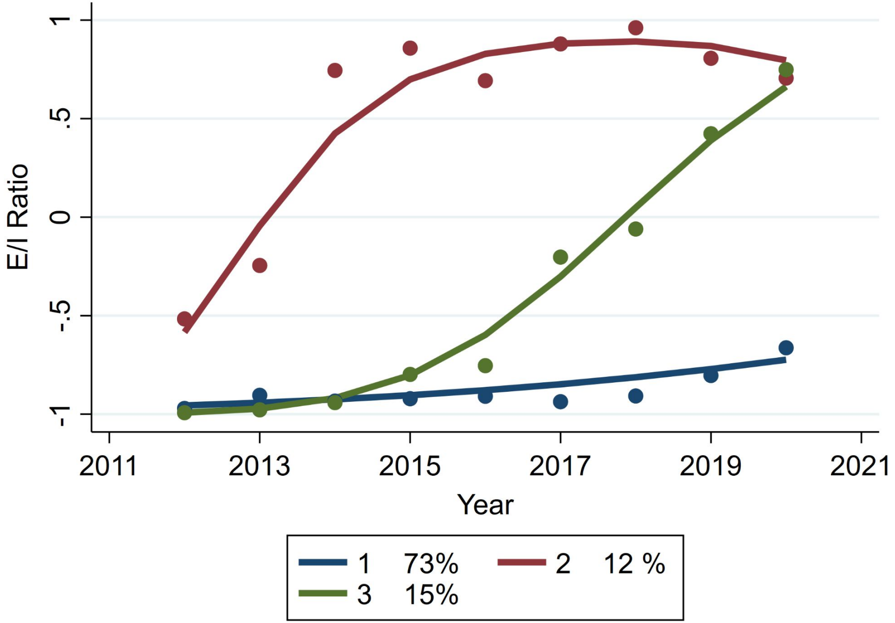
Maximum likelihood

Method of estimating the parameters of the models.

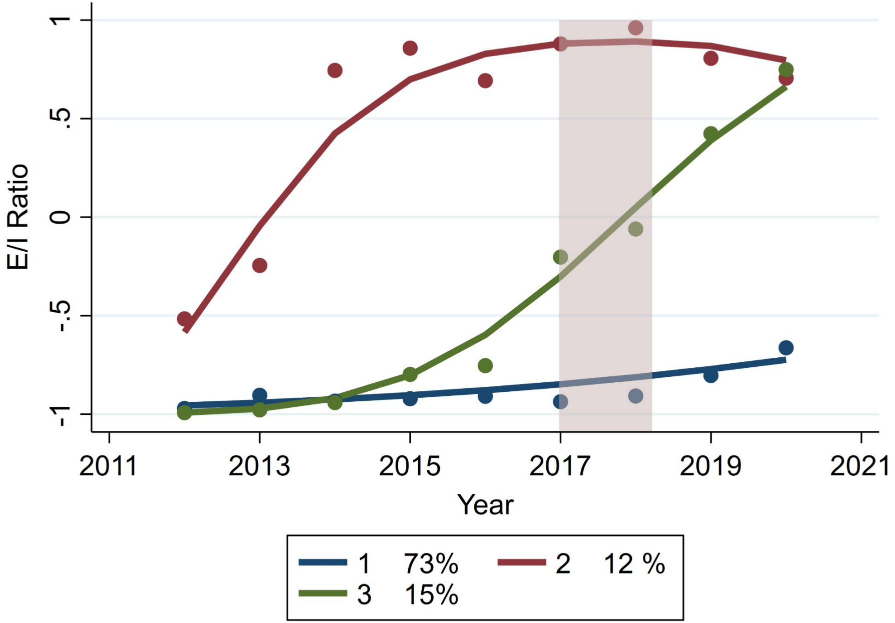
Step 3 - Fit the best model from the data

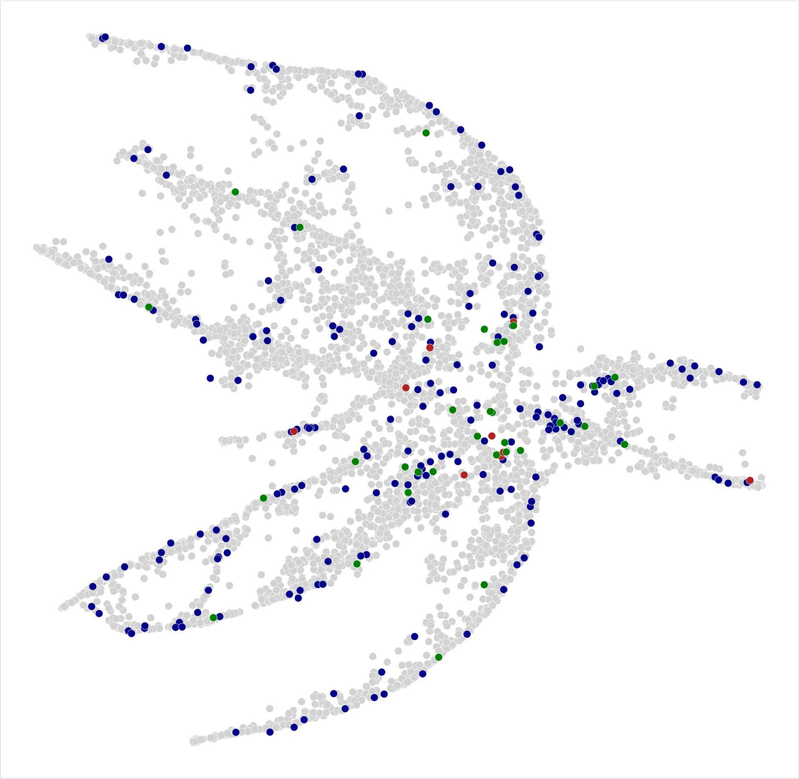


Group Based Trajectory Modeling



Group Based Trajectory Modeling





Take Away

~¾ of drifters favor informal over cybercrime prone spaces

~¼ drift permanently in cybercrime prone spaces

Take Away

~¾ of drifters favor informal over cybercrime prone spaces

Most drifters are only “crimino-curious”

~¼ drift permanently in cybercrime prone spaces

Informal Workforce
Dancing on the Crime Line
Drifters
Migration
Mass Effect

To what extent is this concerning?

Act 5 - Mass Effect

Mass Effect

In medicine, a **mass effect** is the effect of a growing mass that pushes or displaces surrounding tissues and organs, increasing the initial problems scale.

Forum Name	Advertised Users
warriorforum.com	1,598,766
daniweb.com	1200000
affilorama.com	995,991
webhostingtalk	556,830
dreamteammoney.com	490,261
sitepoint.com	260,000
wickedfire.com	222,993
webmasterworld.com	192,023
moneymakerdiscussion.com	123,129
seomastering.com	116937
affiliatefix	114,173
ozzu.com	50380
afflift	46,519
ewebdiscussion.com	37,530
webdevforums	34,625
geekvillage.com	32,075
seomotionz.com	8591
clicknewz.com	2,745

Sum = 6,083,568

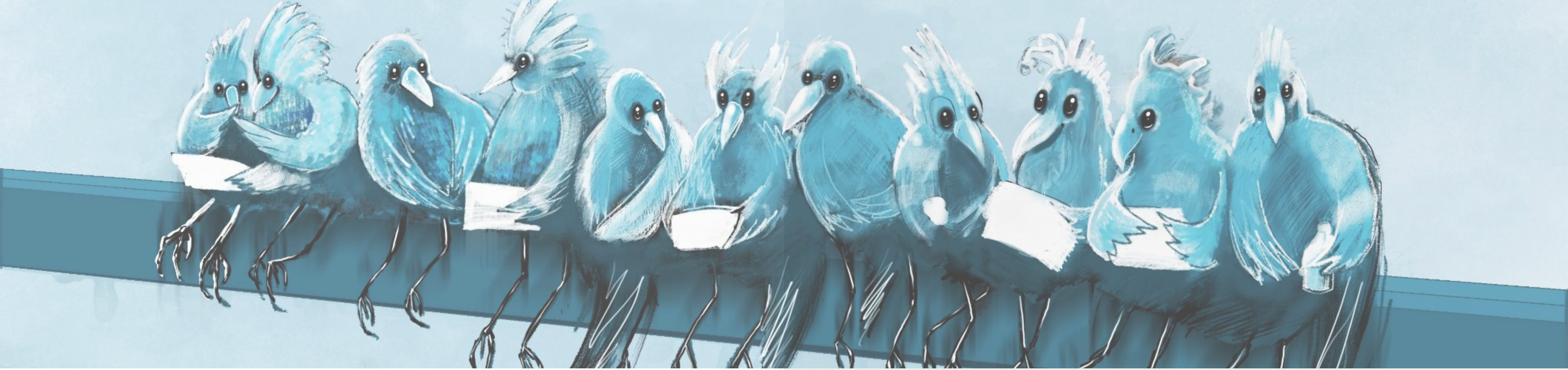
~500k Individuals

6,083,568 * 7.2% = 438,016

There is a large informal workforce evolving at the periphery of the malware industry that is necessary to its operation.

They may or may not contribute directly,

but we believe they would probably rather not.



Take Away

Dig further on the **mass effect** and the role of **informal economies** where **drifters** are **dancing on the line** at the periphery of the cybercrime industry.

Think **beyond** motivated offenders.

Take Out

3 techniques

1. UMAP Dimension Reduction
2. Thematic Analysis
3. Group-Based Trajectory Models

Thank You !

FLARE SYSTEMS

https://flare.systems

Stratosphere Research Laboratory

avast

https://www.stratosphereips.org

https://tunghat.ca

GoSecure

Secureworks®

MASS EFFECT

Thank you !

Masarah Paquet-Clouston
@masarahclouston
mcpc@gosecure.net

Serge-Olivier Paquette
@_soruso
spaquette@secureworks.com

Sebastian Garcia
@eldraco
sebastian.garcia@agents.fel.cvut.cz

Maria Jose Erquiaga
@MaryJo_E
merquiag@cisco.com