Data science approaches to understanding key actors on online hacking forums

Andrew Caines

Theoretical & Applied Linguistics
Faculty of Modern & Medieval Languages

Sergio Pastrana

Cambridge Cybercrime Centre
Department of Computer Science and Technology

Third Annual Cybercrime Conference, Cambridge
July 12, 2018

UNIVERSITY OF CAMBRIDGE

Outline

Underground forums bring together individuals interested in cybercrime

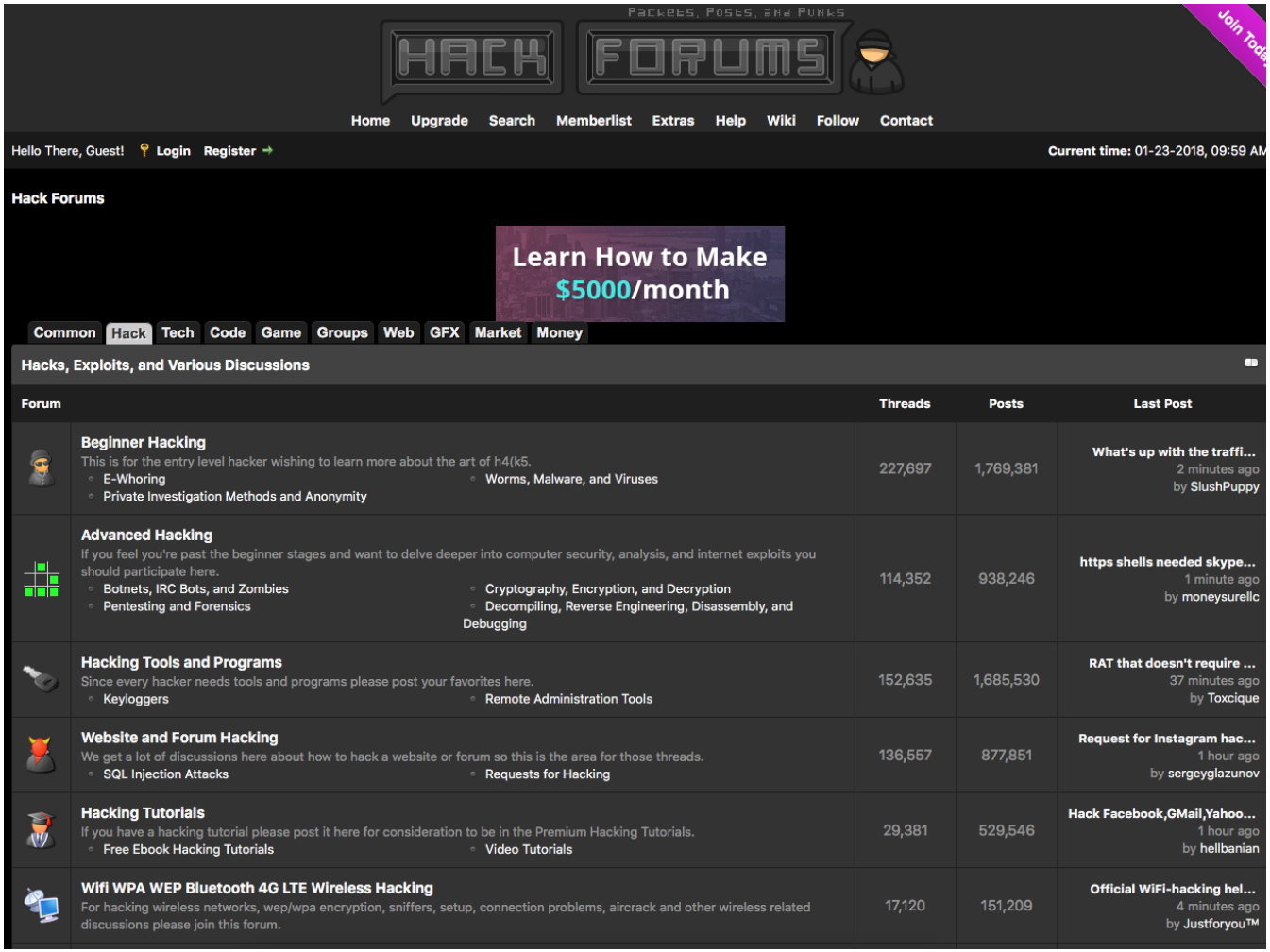
Internet Organized Crime Threat Assessment (IOCTA) 2017,EUROPOL

Places where cybercriminals **learn** from their peers and betters and **buy and sell** the services and tools needed to commit crime online

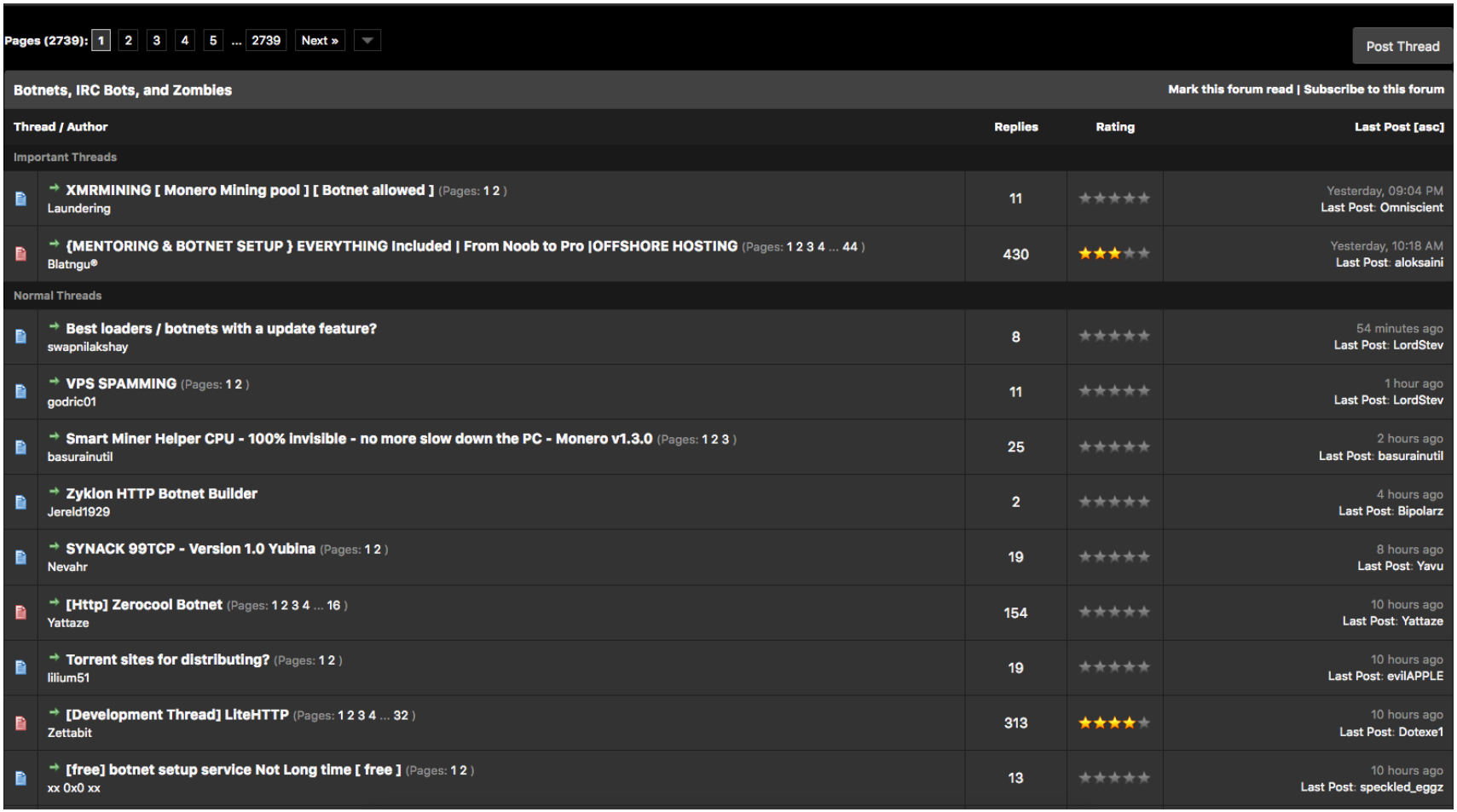
Intelligence Assessment on Pathways Into Cyber Crime 2017, UK NCA

- Availability of **low-level hacking tools** encourages criminal behaviour
- Offenders begin to participate in gaming [...] forums and **progress** to criminal hacking forums
- Forum **interaction** [...] drives young cyber criminals

Forums are organized in sub-forums or boards, threads and posts



Forums are organized in sub-forums or boards, threads and posts



Pages (2739): 1 2 3 4 5 ... 2739 Next »

Post Thread

Botnets, IRC Bots, and Zombies

Mark this forum read | Subscribe to this forum

Thread / Author	Replies	Rating	Last Post [asc]
Important Threads			
XMRMINING [Monero Mining pool] [Botnet allowed] (Pages: 1 2) Laundering	11	★★★★★	Yesterday, 09:04 PM Last Post: Omniscient
{MENTORING & BOTNET SETUP } EVERYTHING Included | From Noob to Pro |OFFSHORE HOSTING (Pages: 1 2 3 4 ... 44) Blatngu®	430	★★★★★	Yesterday, 10:18 AM Last Post: aloksaini
Normal Threads			
Best loaders / botnets with a update feature? swapnilakshay	8	★★★★★	54 minutes ago Last Post: LordStev
VPS SPAMMING (Pages: 1 2) godric01	11	★★★★★	1 hour ago Last Post: LordStev
Smart Miner Helper CPU - 100% invisible - no more slow down the PC - Monero v1.3.0 (Pages: 1 2 3) basurainutil	25	★★★★★	2 hours ago Last Post: basurainutil
Zyklon HTTP Botnet Builder Jereld1929	2	★★★★★	4 hours ago Last Post: Bipolarz
SYNACK 99TCP - Version 1.0 Yubina (Pages: 1 2) Nevahr	19	★★★★★	8 hours ago Last Post: Yavu
[Http] Zerocool Botnet (Pages: 1 2 3 4 ... 16) Yattaze	154	★★★★★	10 hours ago Last Post: Yattaze
Torrent sites for distributing? (Pages: 1 2) lilium51	19	★★★★★	10 hours ago Last Post: evilAPPLE
[Development Thread] LiteHTTP (Pages: 1 2 3 4 ... 32) Zettabit	313	★★★★★	10 hours ago Last Post: Dotexe1
[free] botnet setup service Not Long time [free] (Pages: 1 2) xx 0x0 xx	13	★★★★★	10 hours ago Last Post: speckled_eggz

This project is funded by the Alan Turing Institute. The Cambridge Cybercrime Centre provided the data

- Part of this research is funded by The Alan Turing Institute's Defence and Security Programme [DS/SDS/1718/4]
  - PI. **Dr. Paula Buttery** (Natural Language & Information Processing)
  - Co-I. **Dr. Alice Hutchings** (Cambridge Cybercrime Centre)
  - 6 months: 01 October - 31 March

- The dataset is provided by the Cambridge Cybercrime Centre under legal agreements
  - Use the data only for cybercrime research and analysis
  - Not reverse engineer the data or use it for any commercial purpose
  - Secure the data at all times; and to respect the law, particularly data protection law

https://www.cambridgecybercrime.uk

Outline

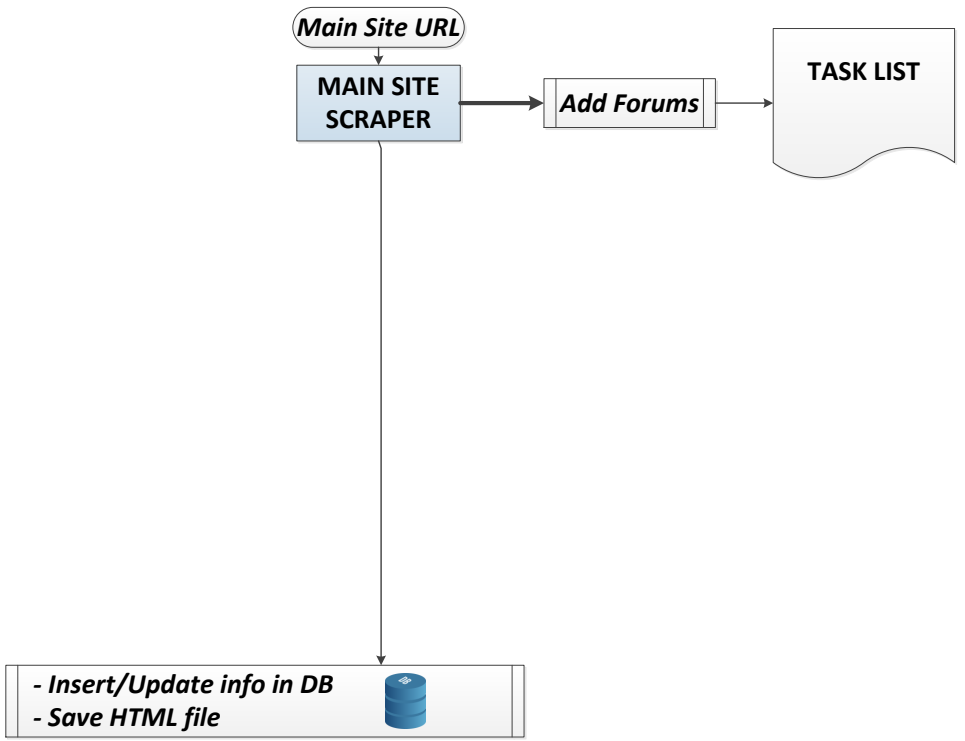
Research on underground forums is limited by the availability of datasets

- Leaked databases.
  - ✓ Full dump, including private messages, registration emails, etc.
  - ✘ Ethical and legal issues
  - ✘ Observer effect
  - ✘ Outdated
- Partially crawled
  - ✓ Focused
  - ✘ Incomplete
  - ✘ Manual effort
  - ✘ Outdated

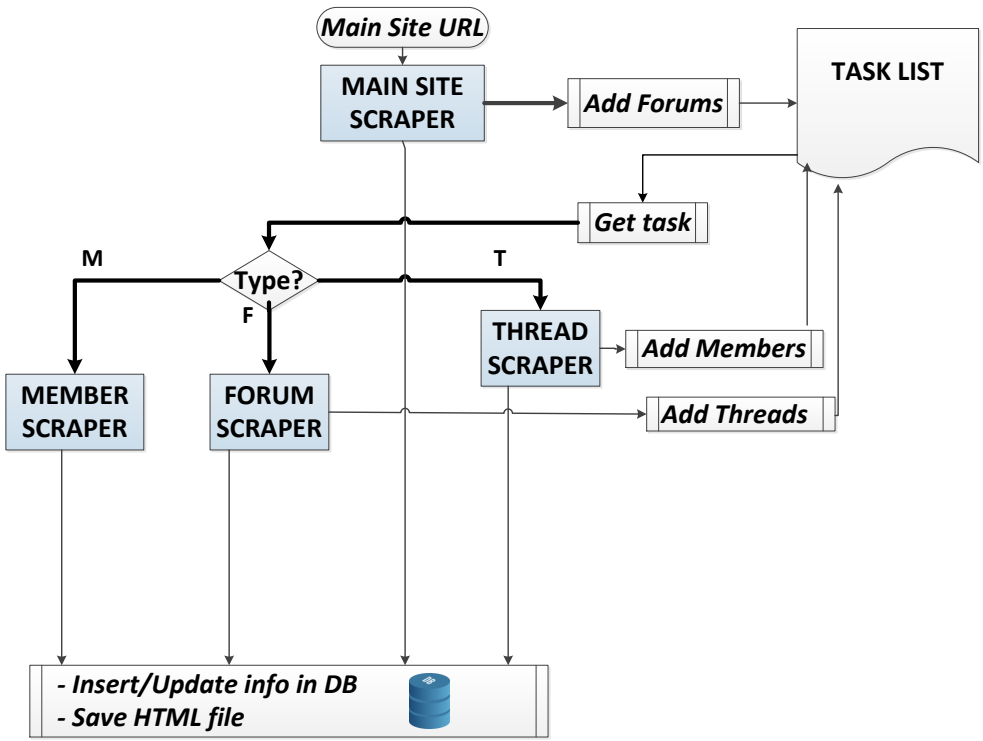
We fill the gap by providing a complete, updated dataset of operative underground forums

1. **CrimeBot** is a tool designed to crawl and scrape underground forums
2. **CrimeBB** is a dataset containing more than 48m posts made from 1m accounts in 7 different forums
3. Both the tool and dataset are **available** for other academic researchers **under legal agreements to prevent misuse**

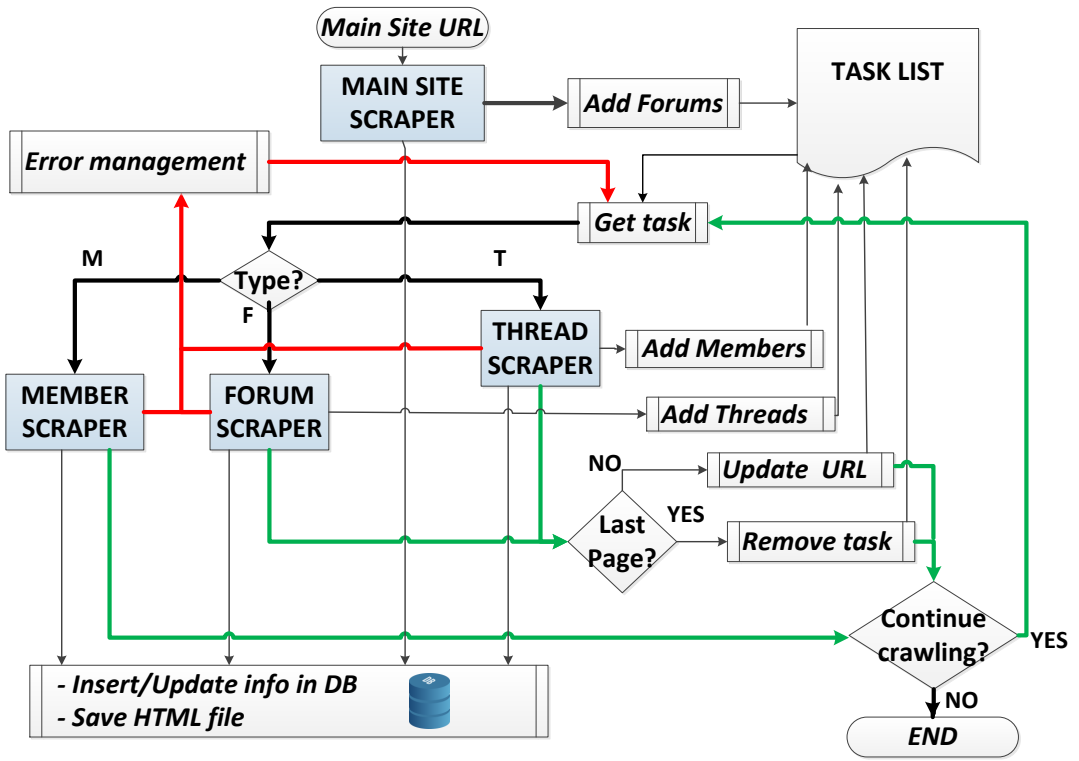
CrimeBot addresses particular challenges to crawl underground forums



CrimeBot addresses particular challenges to crawl underground forums



CrimeBot addresses particular challenges to crawl underground forums

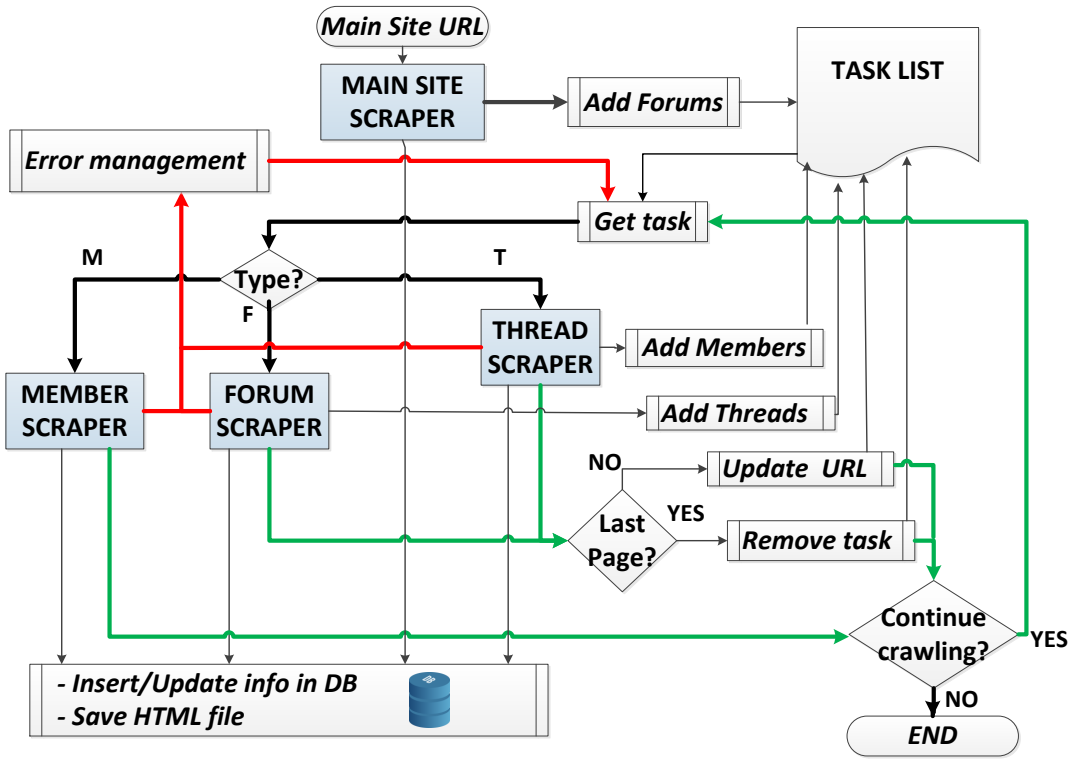


CrimeBot addresses particular challenges to crawl underground forums

- Stealthiness

Avoid observer effect

- Navigation patterns
- Connection times



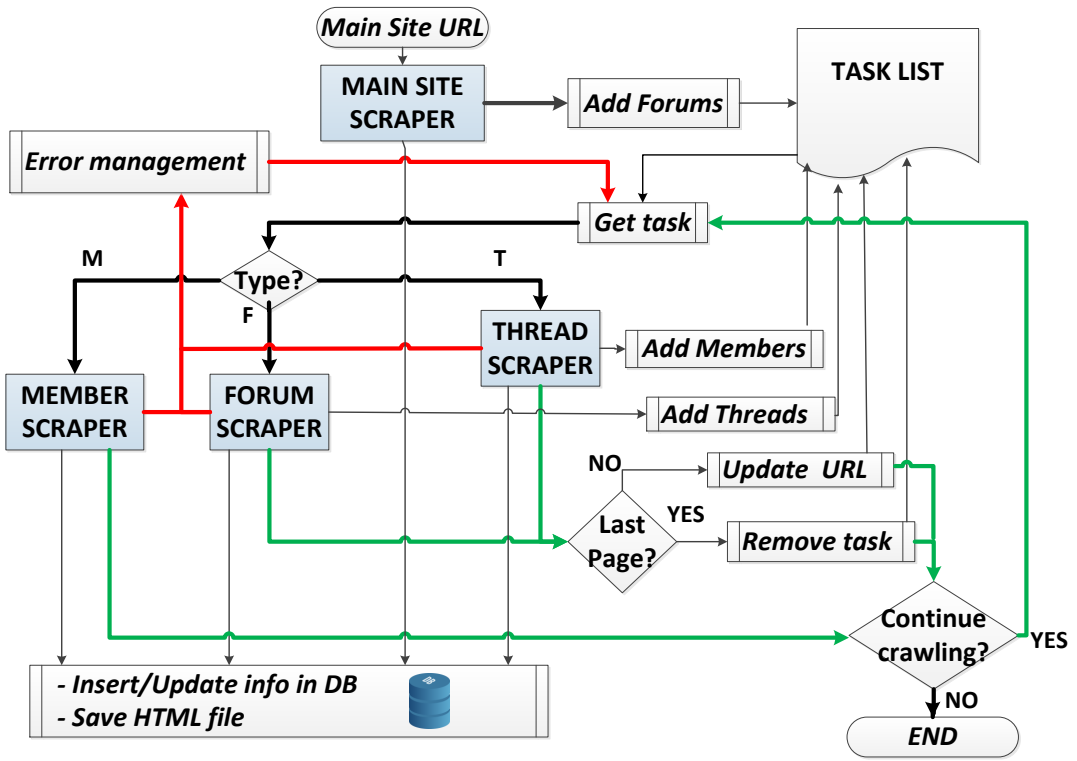
CrimeBot addresses particular challenges to crawl underground forums

- Stealthiness
- Efficiency

Optimize, limit manual effort

Trade-off with stealthiness

- Distributed crawling
- Error management

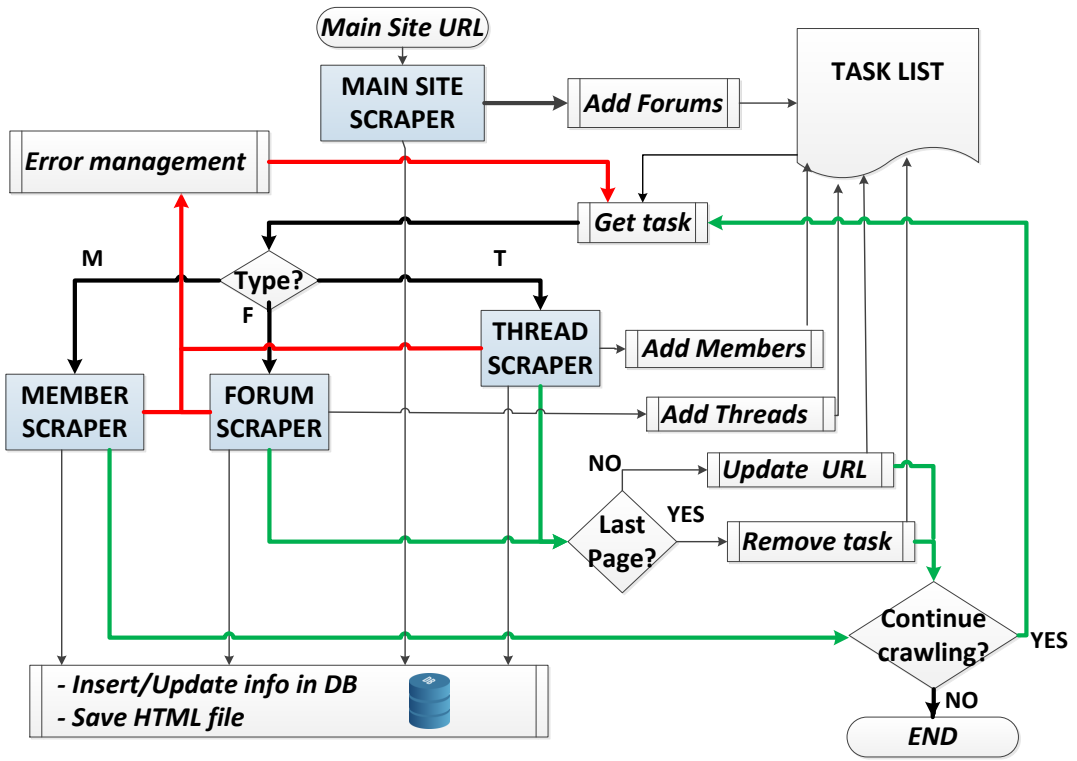


CrimeBot addresses particular challenges to crawl underground forums

- Stealthiness
- Efficiency
- Non-textual content

Annotation

- Images and videos
- Links and attachments
- Source Code

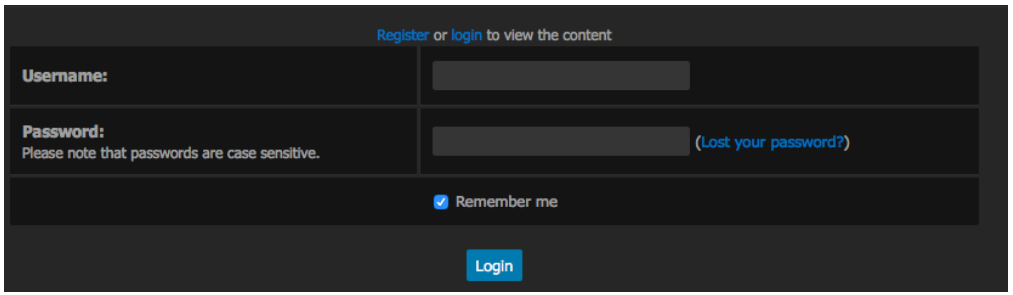


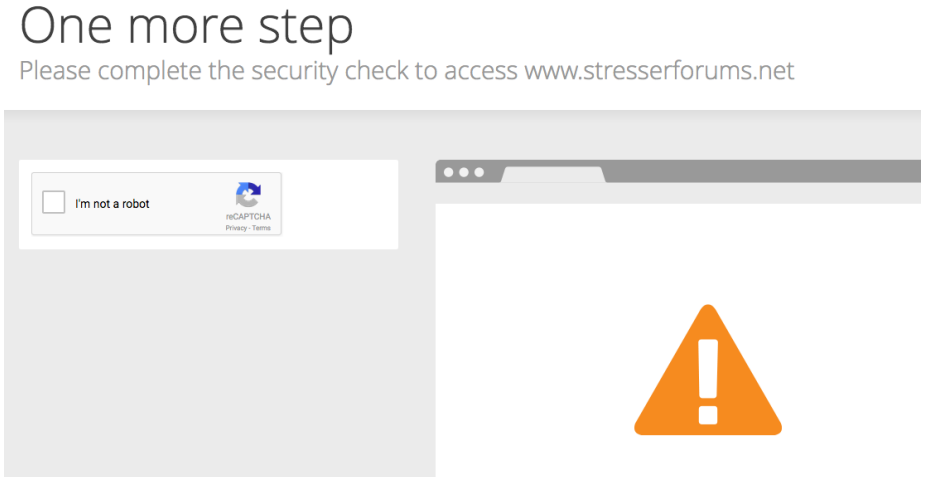
CrimeBot addresses particular challenges to crawl underground forums

- Stealthiness
- Efficiency
- Non-textual content
- Accessibility

Non-cooperative scenario

- Create accounts
- Solve CAPTCHA
- Session cookies





CrimeBot addresses particular challenges to crawl underground forums

- Stealthiness
- Efficiency
- Non-textual content
- Accessibility
- Completeness

  Ideally, reconstruct DB

  - Content and metadata

Table 3: Summary of Hackforums in CrimeBB by category. The percentage calculations are affected by the deletion of threads and posts.

Category	Forums	Posts	Oldest	Threads	Coverage
Gaming	32	4 371 268	02/07	424 826	99.82
Web	9	627 484	01/07	87 582	99.27
Money	9	2 006 809	11/07	154 061	96.41
Hack	23	5 869 600	02/07	666 882	96.13
Coding	15	1 470 806	05/07	173 286	99.43
Tech	17	1 799 708	01/07	215 654	99.6
Common	27	12 735 925	01/07	857 006	99.07
Graphics	10	1 025 316	02/07	138 197	99.46
Market	28	9 541 610	11/07	1 071 780	98.9

CrimeBB currently contains data from 7 forums

Forum	Boards	Members	Threads	Posts	Oldest
Hackforums	175	573 925	3 833 704	39 930 857	01/07
Kernelmode	16	1 441	3 144	25 024	03/10
Offensive Community	63	10 593	18 436	58 779	06/12
Multiplayer Game Hacking	699	449 832	736 426	8 877 993	12/05
Stresserforums	22	764	708	7 069	04/17
Greysec	30	440	1 239	6 969	06/15
Garage4Hackers	35	872	2 096	7 697	07/10

Table 1: Summary of the CrimeBB dataset (updated 09/07/18)

More Info:

CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale.
Sergio Pastrana, Daniel R. Thomas, Alice Hutchings, and Richard Clayton.
In Proceedings of The Web Conference 2018 (WWW 2018), Lyon, France.
https://doi.org/10.1145/3178876.3186178

Outline

CrimeBB & NLP

- NLP as the analysis of texts to ..

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..
  1. Classify posts;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..
  1. Classify posts;
  2. Identify topics;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..
  1. Classify posts;
  2. Identify topics;
  3. Analyse sentiment;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..
  1. Classify posts;
  2. Identify topics;
  3. Analyse sentiment;
  4. Classify individuals.

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..
  1. Classify posts;
  2. Identify topics;
  3. Analyse sentiment;
  4. Classify individuals.
- Future work is to ..

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..
  1. Classify posts;
  2. Identify topics;
  3. Analyse sentiment;
  4. Classify individuals.
- Future work is to ..
  1. Normalise texts;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..
  1. Classify posts;
  2. Identify topics;
  3. Analyse sentiment;
  4. Classify individuals.
- Future work is to ..
  1. Normalise texts;
  2. Deeper analysis;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..
  1. Classify posts;
  2. Identify topics;
  3. Analyse sentiment;
  4. Classify individuals.
- Future work is to ..
  1. Normalise texts;
  2. Deeper analysis;
  3. Identify trends;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- We use NLP to ..
  1. Classify posts;
  2. Identify topics;
  3. Analyse sentiment;
  4. Classify individuals.
- Future work is to ..
  1. Normalise texts;
  2. Deeper analysis;
  3. Identify trends;
  4. Analyse *who is talking to whom about what* (and in what way).

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- Standard English:
- The innovative imaging technique of muography uses naturally-occurring background radiation in the form of cosmic-ray muons to characterise a diverse range of complex structures that cannot be imaged using conventional techniques. Research interest in muography is at an all-time high and this proposed meeting aims to unite the global community, encourage international collaboration and engage industry via dedicated user-led sessions.

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- Hackforums:
- "I'm not attempting to steal anything. I just wanna know things like how to break into a friend's computer (for no reason at all)" lol. First step is to not ask on a forum full of 11 year olds who circlejerk memes and "omg i'm a t0t4l 1337 h4x0r. l00k at my $0.10 earnings from ewhoring some poor sap on omegle" ...
  Breaking into someone's computer: well you're not just going to magically press a combination on your keyboard and suddenly, you have the nuclear access codes lol. Break into someone's computer and do what? Do you know what a RAT is? a keylogger? a DNS hijacker? How to get someone to download something?

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How well do we do with off-the-shelf toolkits?

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How well do we do with off-the-shelf toolkits?
- e.g. SpaCy web corpus CNN for PoS-tagging, dependency parsing, named entity recognition;
- (Reported as 97%, 91.7%, 85.3% accurate)
- 1000 tokens from Hackforums:

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How well do we do with off-the-shelf toolkits?
- e.g. SpaCy web corpus CNN for PoS-tagging, dependency parsing, named entity recognition;
- (Reported as 97%, 91.7%, 85.3% accurate)
- 1000 tokens from Hackforums:

Task	**Measure**	**Value**
PoS-tagging	accuracy	.894
Dependency parse	accuracy	.894
Named entity recognition	precision	.16
	recall	.158
	F-measure	.159

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How well do we do with off-the-shelf toolkits?
- Error analysis...

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How well do we do with off-the-shelf toolkits?
- Error analysis...
- PoS-tagging: "dm me" tagged PRONOUN PRONOUN not VERB PRONOUN; "pp only" ('PayPal only') tagged VERB ADVERB not NOUN ADVERB;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How well do we do with off-the-shelf toolkits?
- Error analysis...
- PoS-tagging: "dm me" tagged PRONOUN PRONOUN not VERB PRONOUN; "pp only" ('PayPal only') tagged VERB ADVERB not NOUN ADVERB;
- Parsing: sentences in a word "hmu" have knock-on effect if mis-parsed, e.g. "hmu shitty ovr but..." – erroneous single sentence parse leads to incorrect dependency relations;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How well do we do with off-the-shelf toolkits?
- Error analysis...
- PoS-tagging: "dm me" tagged PRONOUN PRONOUN not VERB PRONOUN; "pp only" ('PayPal only') tagged VERB ADVERB not NOUN ADVERB;
- Parsing: sentences in a word "hmu" have knock-on effect if mis-parsed, e.g. "hmu shitty ovr but..." – erroneous single sentence parse leads to incorrect dependency relations;
- **We need to normalise CrimeBB texts**.

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How well do we do with off-the-shelf toolkits?
- Error analysis...
- NER: words with standard non-hacking meanings which are products or techniques in the context of hacking are missed by standard NER models; e.g. ‘spreading’, ‘crypt’, ‘rat’;

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How well do we do with off-the-shelf toolkits?
- Error analysis...
- NER: words with standard non-hacking meanings which are products or techniques in the context of hacking are missed by standard NER models; e.g. ‘spreading’, ‘crypt’, ‘rat’;
- And in general: computational concepts, hacking methods and tech entities which may or may not be title capitalised (or spelled correctly).

CrimeBB & NLP

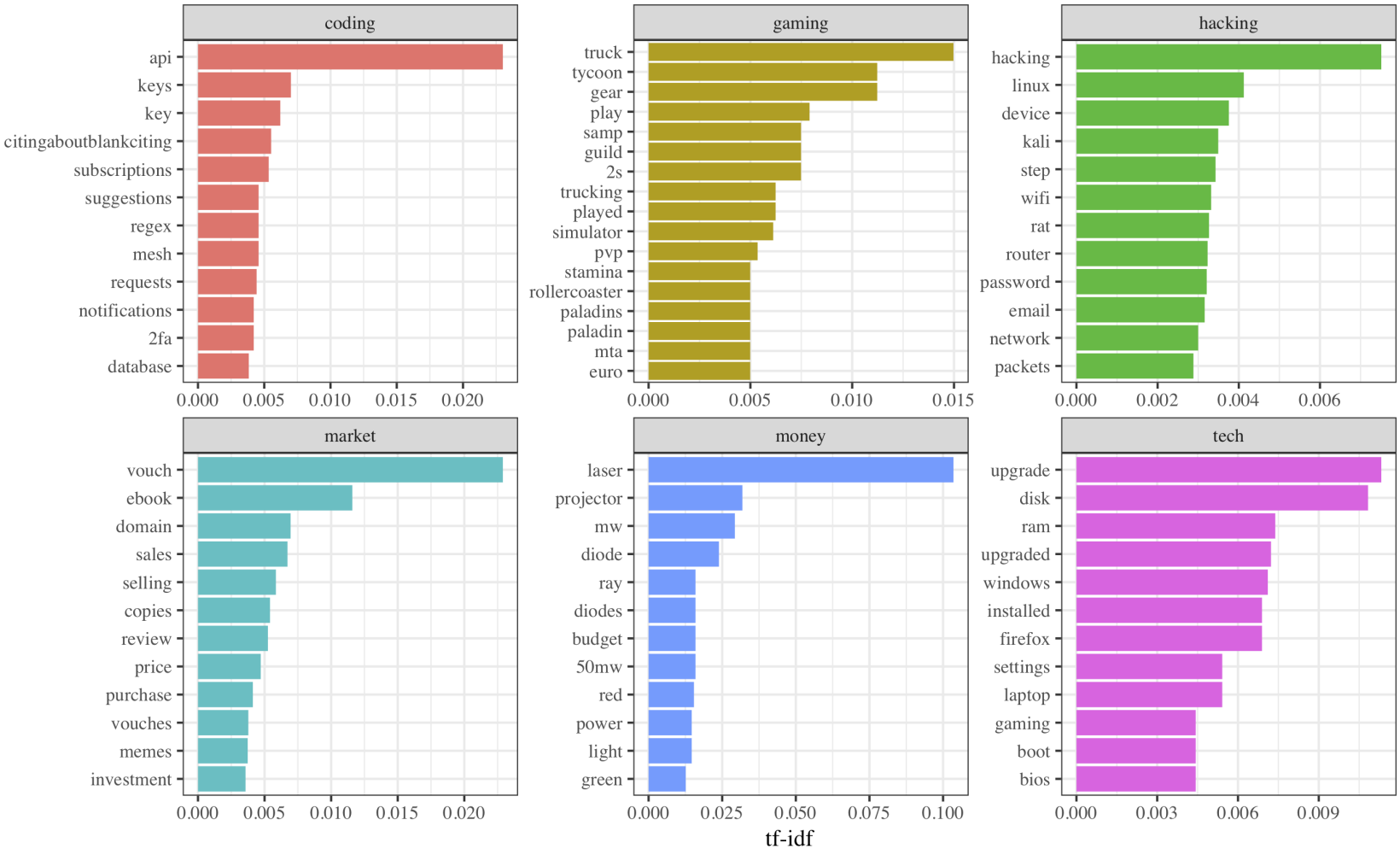
- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to improve our NER?

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to improve our NER?
- Supervised approach: **make lists**!

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to improve our NER?
- Supervised approach: **make lists**!
- Unsupervised approach: learn what the key entities are through topic analysis (here, unigrams from 2200 posts, ranked by tf·idf)


coding
api
keys
key
citingaboutblankciting
subscriptions
suggestions
regex
mesh
requests
notifications
2fa
database
0.000
0.005
0.010
0.015
0.020
gaming
truck
tycoon
gear
play
samp
guild
2s
trucking
played
simulator
pvp
stamina
rollercoaster
paladins
paladin
mta
euro
0.000
0.005
0.010
0.015
hacking
hacking
linux
device
kali
step
wifi
rat
router
password
email
network
packets
0.000
0.002
0.004
0.006
market
vouch
ebook
domain
sales
selling
copies
review
price
purchase
vouches
memes
investment
0.000
0.005
0.010
0.015
0.020
money
laser
projector
mw
diode
ray
diodes
budget
50mw
red
power
light
green
0.000
0.025
0.050
0.075
0.100
tech
upgrade
disk
ram
upgraded
windows
installed
firefox
settings
laptop
gaming
boot
bios
0.000
0.003
0.006
0.009
tf-idf

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to learn about new concepts?

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to learn about new concepts?
- Take a semi-supervised approach like DISCOVER (Sapienza et al, WWW'18)
- Monitoring blogs & Twitter (applied to forums)

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to learn about new concepts?
- Take a semi-supervised approach like DISCOVER (Sapienza et al, WWW'18)
- Monitoring blogs & Twitter (applied to forums)
- Filtration system: English dictionary $\rightarrow$ 'stopwords' $\rightarrow$ domain dictionary (computer, OS, web, etc) $\rightarrow$ threat dictionary (ddos, botnet, phishing, etc) $\rightarrow$ $(count > 1)$ $\rightarrow$ $(n.contextwords > 0)$ $\rightarrow$ **discover terms** (2017: cloudpets, wannacry, ghosthook, etc)

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what*?

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what*?
- NLU = natural language understanding

CrimeBB & NLP

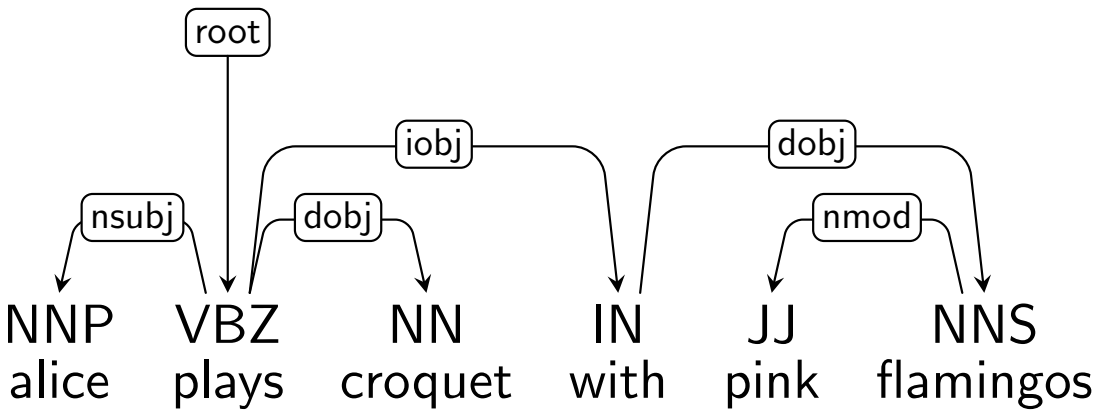
- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what*?
- NLU = natural language understanding
- *Start with*: Dependency parsing & Abstract meaning representation

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- NLU $\approx$ **Dependency parse** & Abstract meaning representation
- Alice plays croquet with pink flamingos (*note the ambiguity*)

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- NLU $\approx$ **Dependency parse** & Abstract meaning representation
- Alice plays croquet with pink flamingos (*note the ambiguity*)

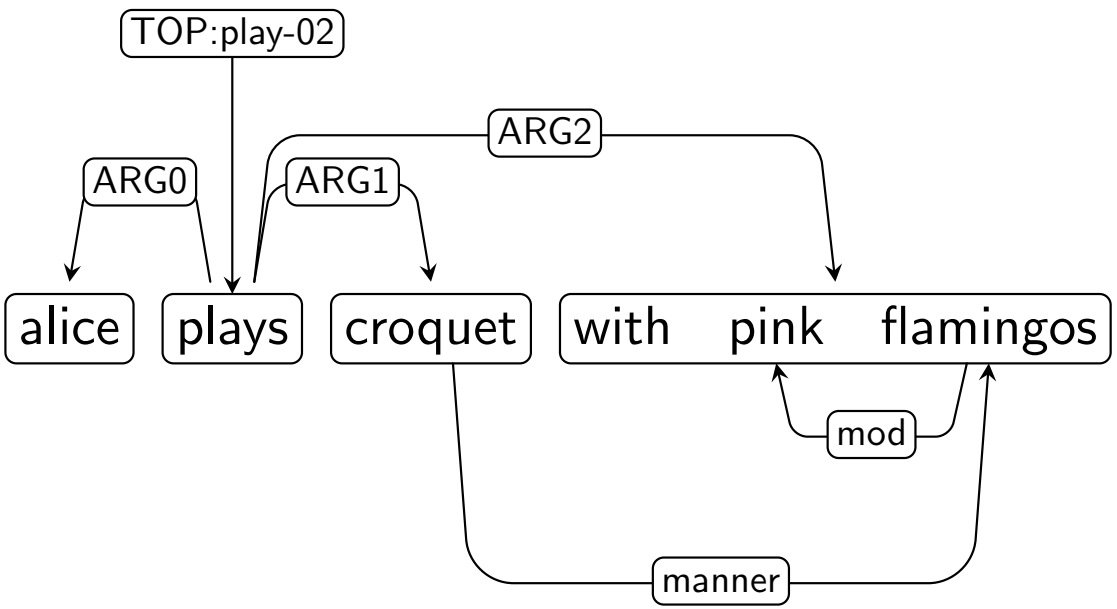


CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- NLU $\approx$ Dependency parse & **Abstract meaning representation**
- Alice plays croquet with pink flamingos

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- NLU $\approx$ Dependency parse & **Abstract meaning representation**
- Alice plays croquet with pink flamingos



CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what* (and in what way)

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what* (and in what way)
- 1, Nemo: Selling a rat for btc

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what* (and in what way)
- 1, Nemo: Selling a rat for btc
- 2, Gill: ur a skid

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what* (and in what way)
- 1, Nemo: Selling a rat for btc
- 2, Gill: ur a skid
- 3, Dory: vouch for nemo

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what* (and in what way)
- 1, Nemo: Selling a rat for btc
- 2, Gill: ur a skid
- 3, Dory: vouch for nemo
- 4, Nigel: yes i will buy

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what* (and in what way)
- 1, Nemo: Selling a rat for btc
- 2, Gill: ur a skid
- 3, Dory: vouch for nemo
- 4, Nigel: yes i will buy
- 5, Nemo: citing*4* thanks. dm me your offer!

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what* (and in what way)
- 1, Nemo: Selling a rat for btc
- 2, Gill: ur a skid
- 3, Dory: vouch for nemo
- 4, Nigel: yes i will buy
- 5, Nemo: citing*4* thanks. dm me your offer!
- 6, Nemo: citing*3* img/smilies/blackhat.gif

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- How to understand *who is talking to whom about what* (and in what way)
- 1, Nemo: Selling a rat for btc
- 2, Gill: ur a skid
- 3, Dory: vouch for nemo
- 4, Nigel: yes i will buy
- 5, Nemo: citing*4* thanks. dm me your offer!
- 6, Nemo: citing*3* img/smilies/blackhat.gif
- 7, Nemo: citing*2* gfy

CrimeBB & NLP

- 1, Nemo: Selling a rat for btc
- 2, Gill: ur a skid
- 3, Dory: vouch for nemo
- 4, Nigel: yes i will buy
- 5, Nemo: citing*4* thanks. dm me your offer!
- 6, Nemo: citing*3* img/smilies/blackhat.gif
- 7, Nemo: citing*2* gfy

Post	Reply-to	Type	Intent	Sentiment	Topic
1	$\rightarrow 0$	offerX	neutral	zero	RATs &
2	$\uparrow 1$	comment	aggression	-ve	BTC
3	$\rightarrow 0$	comment	vouch	+ve	$\downarrow$
4	$\uparrow 1$	requestX	positive	zero	
5	$\uparrow 4$	comment	gratitude,pm	+ve	
6	$\uparrow 3$	comment	positive	zero	
7	$\uparrow 2$	comment	aggression	-ve	

CrimeBB & NLP

- Annotation of 2200 posts from 13 HF bulletin boards by 3 annotators;

CrimeBB & NLP

- Annotation of 2200 posts from 13 HF bulletin boards by 3 annotators;
- Post type: offerX, requestX, exchange, tutorial, info request, comment, social;
- Author intent: positive, neutral, negative, moderate, vouch, gratitude, private message, aggression;
- Addressee: general audience, thread OP, other individual;

CrimeBB & NLP

- Annotation of 2200 posts from 13 HF bulletin boards by 3 annotators;
- Post type: offerX, requestX, exchange, tutorial, info request, comment, social;
- Author intent: positive, neutral, negative, moderate, vouch, gratitude, private message, aggression;
- Addressee: general audience, thread OP, other individual;
- (n.b. skewed toward comment & info request; neutral & positive; thread OP)
- IAA 'substantial' for post type, 'fair/moderate' for author intent, 'moderate/almost perfect' for addressee, using Fleiss kappa;

CrimeBB & NLP

- Annotation of 2200 posts from 13 HF bulletin boards by 3 annotators;
- Post type: offerX, requestX, exchange, tutorial, info request, comment, social;
- Author intent: positive, neutral, negative, moderate, vouch, gratitude, private message, aggression;
- Addressee: general audience, thread OP, other individual;
- (n.b. skewed toward comment & info request; neutral & positive; thread OP)
- IAA 'substantial' for post type, 'fair/moderate' for author intent, 'moderate/almost perfect' for addressee, using Fleiss kappa;
- Classification experiment:

CrimeBB & NLP

- Annotation of 2200 posts from 13 HF bulletin boards by 3 annotators;
- Post type: offerX, requestX, exchange, tutorial, info request, comment, social;
- Author intent: positive, neutral, negative, moderate, vouch, gratitude, private message, aggression;
- Addressee: general audience, thread OP, other individual;
- (n.b. skewed toward comment & info request; neutral & positive; thread OP)
- IAA 'substantial' for post type, 'fair/moderate' for author intent, 'moderate/almost perfect' for addressee, using Fleiss kappa;
- Classification experiment:

Label	**Logic**	**Stat**	**P**	**R**	**F**
Post type	T	linear	.919	.781	.844
Author intent	T	XGboost	.786	.499	.611
Addressee	F	SVM	.820	.810	.815

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- So far: applied classification model to 10.6m posts;
- How to use this information?

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- So far: applied classification model to 10.6m posts;
- How to use this information?
- Identifying trends;
- Social network analysis;
- Characterising key actors (more later..)

CrimeBB & NLP

- NLP as the analysis of texts to ..
  1. extract information;
  2. identify entities;
  3. *learn & understand*.
- So far: applied classification model to 10.6m posts;
- How to use this information?
- Identifying trends;
- Social network analysis;
- Characterising key actors (more later..)
- Also: 'Automatically identifying the function and intent of posts in underground forums', A. Caines, S. Pastrana, A. Hutchings, P. Buttery (submitted).

Outline

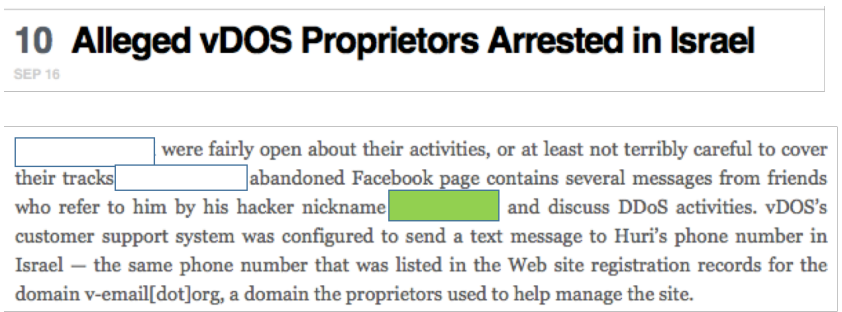
In this study we characterize and predict key actors in Hackforums

- 'Key actor' = forum users indisputably involved in criminal activities
- Methodology:
  1. Identification of key actors
  2. Characterization and evolution
  3. Prediction
- Two potential applications:
  1. Intervention: deter involvement in cybercrime activities at early stages
  2. Cybersecurity: monitor new tools and techniques from the underground world

IDENTIFICATION

We identify 113 key actors from various sources

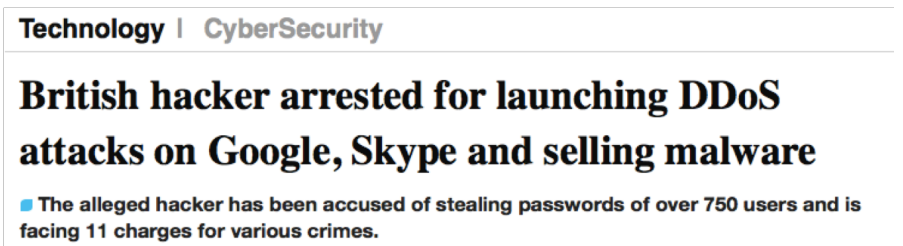
- Public sources (e.g. users arrested): 49 actors
  - News, blogs, social media
  - Official notifications from Law Enforcement
  - Forum threads



10 Alleged vDOS Proprietors Arrested in Israel

SEP 16

[redacted] were fairly open about their activities, or at least not terribly careful to cover their tracks [redacted] abandoned Facebook page contains several messages from friends who refer to him by his hacker nickname [redacted] and discuss DDoS activities. vDOS's customer support system was configured to send a text message to Huri's phone number in Israel — the same phone number that was listed in the Web site registration records for the domain v-email[dot]org, a domain the proprietors used to help manage the site.



Technology | CyberSecurity

British hacker arrested for launching DDoS attacks on Google, Skype and selling malware

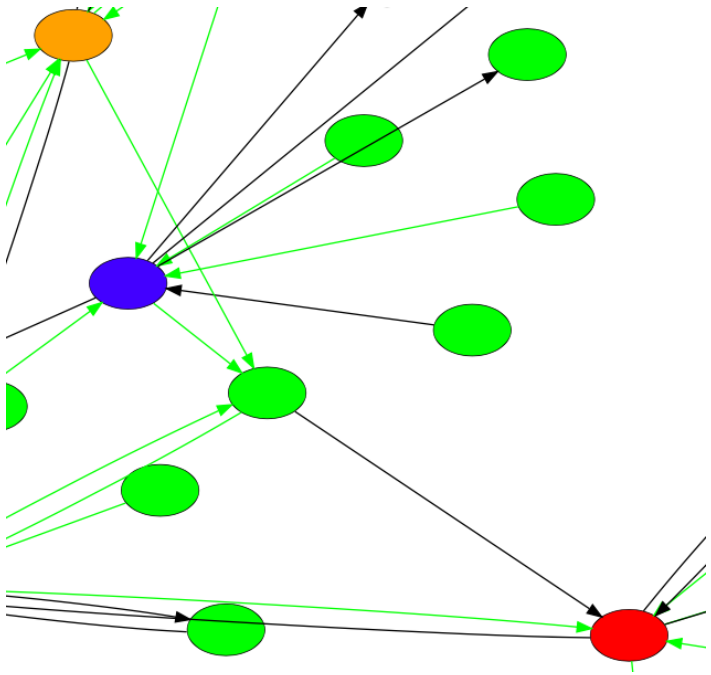
The alleged hacker has been accused of stealing passwords of over 750 users and is facing 11 charges for various crimes.

We identify 113 key actors from various sources

- Public sources (e.g. users arrested): 49 actors
  - News, blogs, social media
  - Official notifications from Law Enforcement
  - Forum threads
- Flashpoint: 9 actors

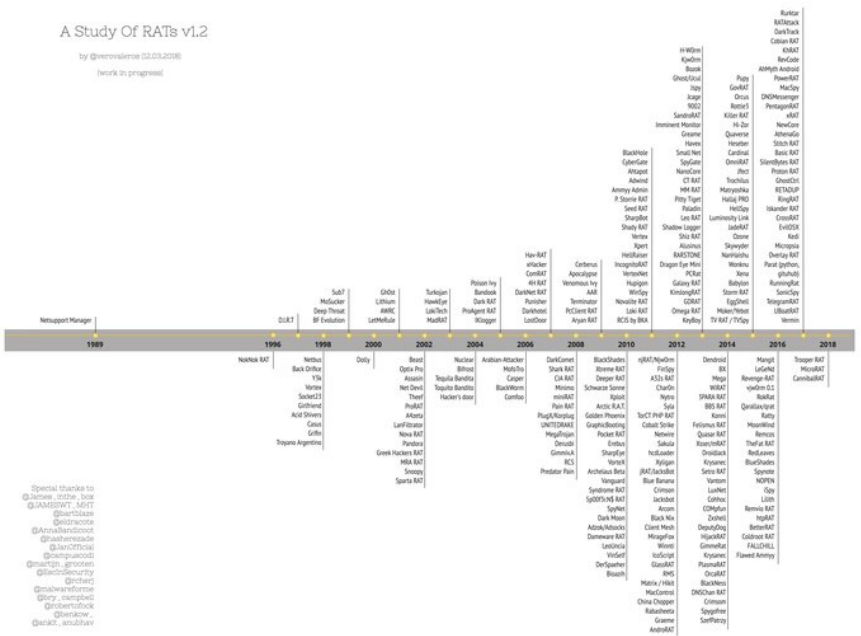
We identify 113 key actors from various sources

- Public sources (e.g. users arrested): 49 actors
  - News, blogs, social media
  - Official notifications from Law Enforcement
  - Forum threads
- Flashpoint: 9 actors
- SNA + manual review: 22 actors



We identify 113 key actors from various sources

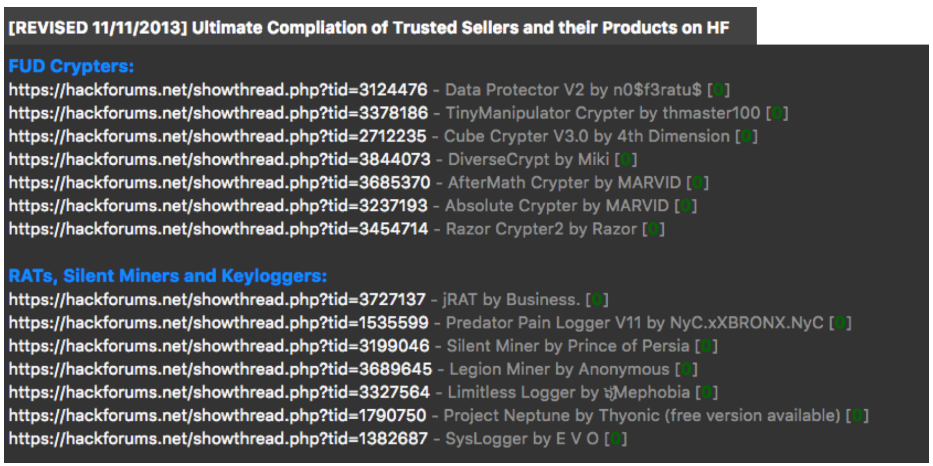
- Public sources (e.g. users arrested): 49 actors
  - News, blogs, social media
  - Official notifications from Law Enforcement
  - Forum threads
- Flashpoint: 9 actors
- SNA + manual review: 22 actors
- Providers of malware or malicious services
  - RAT list: 35 actors



https://www.veronicavaleros.com/blog/2018/3/12/a-study-of-rats-third-timeline-iteration

We identify 113 key actors from various sources

- Public sources (e.g. users arrested): 49 actors
  - News, blogs, social media
  - Official notifications from Law Enforcement
  - Forum threads
- Flashpoint: 9 actors
- SNA + manual review: 22 actors
- Providers of malware or malicious services
  - RAT list: 35 actors
  - "Compilation" threads: 15 actors


[REVISED 11/11/2013] Ultimate Compilation of Trusted Sellers and their Products on HF

FUD Crypters:
https://hackforums.net/showthread.php?tid=3124476 - Data Protector V2 by n0$f3ratu$ [0]
https://hackforums.net/showthread.php?tid=3378186 - TinyManipulator Crypter by thmaster100 [0]
https://hackforums.net/showthread.php?tid=2712235 - Cube Crypter V3.0 by 4th Dimension [0]
https://hackforums.net/showthread.php?tid=3844073 - DiverseCrypt by Miki [0]
https://hackforums.net/showthread.php?tid=3685370 - AfterMath Crypter by MARVID [0]
https://hackforums.net/showthread.php?tid=3237193 - Absolute Crypter by MARVID [0]
https://hackforums.net/showthread.php?tid=3454714 - Razor Crypter2 by Razor [0]

RATs, Silent Miners and Keyloggers:
https://hackforums.net/showthread.php?tid=3727137 - jRAT by Business. [0]
https://hackforums.net/showthread.php?tid=1535599 - Predator Pain Logger V11 by NyC.xXBRONX.NyC [0]
https://hackforums.net/showthread.php?tid=3199046 - Silent Miner by Prince of Persia [0]
https://hackforums.net/showthread.php?tid=3689645 - Legion Miner by Anonymous [0]
https://hackforums.net/showthread.php?tid=3327564 - Limitless Logger by Mephobia [0]
https://hackforums.net/showthread.php?tid=1790750 - Project Neptune by Thyonic (free version available) [0]
https://hackforums.net/showthread.php?tid=1382687 - SysLogger by E V O [0]

CHARACTERIZATION

We apply data science to characterize actors

- Social Network Analysis. Directed graph
  - Nodes are members
  - Edges are interactions

We apply data science to characterize actors

- Social Network Analysis. Directed graph
  - Nodes are members
  - Edges are interactions
- Natural Language Processing. Question predictor
  - Annotated dataset
  - Hybrid Statistical-logical approach
  - Support Vector Machine
  - Precision=0.88, Recall=0.85, F1=0.86

We apply data science to characterize actors

- Social Network Analysis. Directed graph
  - Nodes are members
  - Edges are interactions
- Natural Language Processing. Question predictor
  - Annotated dataset
  - Hybrid Statistical-logical approach
  - Support Vector Machine
  - Precision=0.88, Recall=0.85, F1=0.86
- k-means clustering
  - k=5
  - Feature extraction ...

We build a feature vector for each actor

Forum activity

- Number of posts/threads in each category
- Number of posts/threads in Currency Exchange
- Days posting

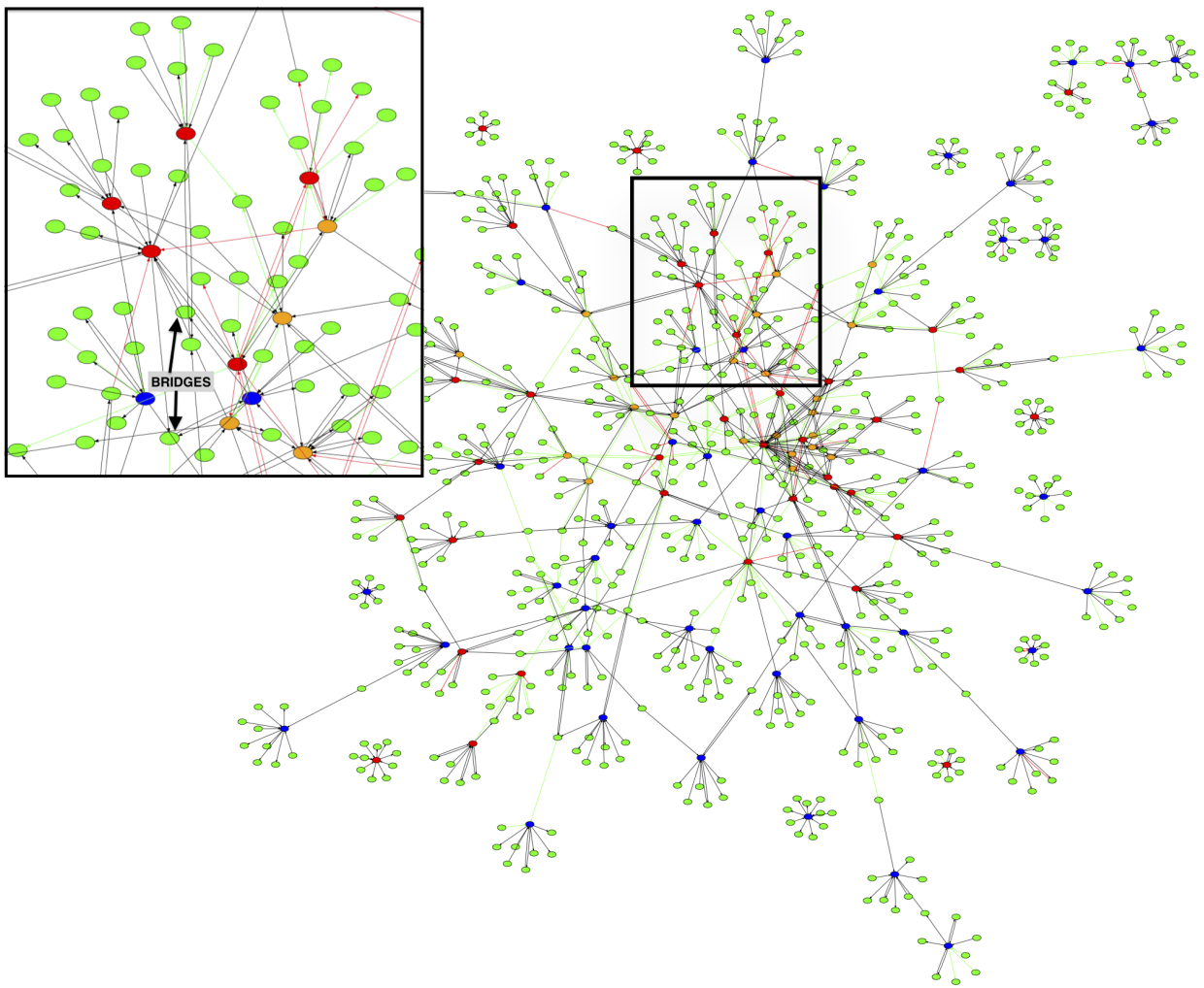
Networking metrics

- In/Out-degree and eigenvector
- H-index
- i-10, i-50 and i-100 indexes

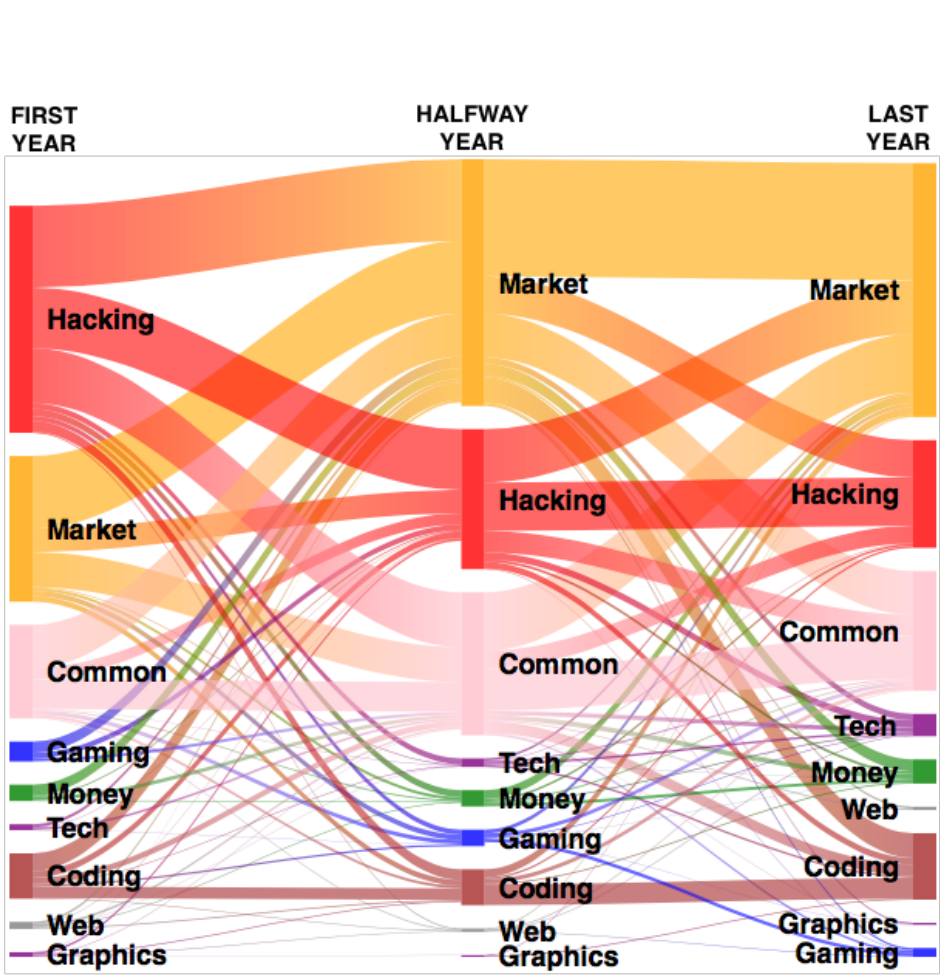
Reputation metrics

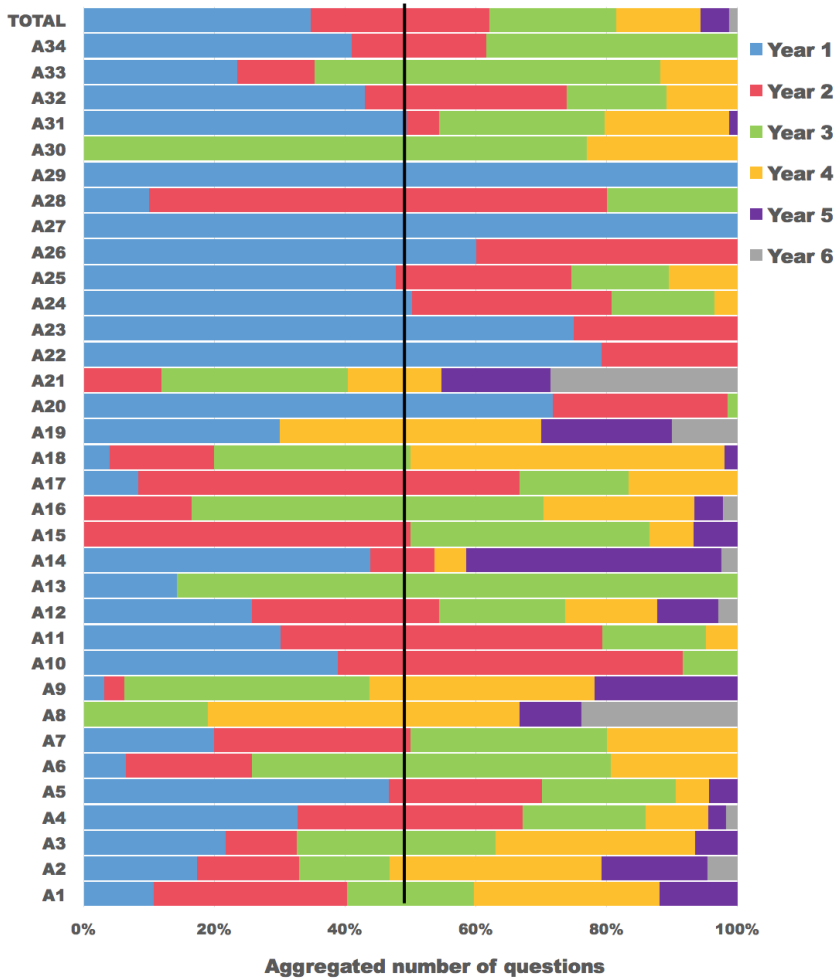
- Reputation score
- Positive, negative and neutral reputations received

Key actors are closely connected in the social network



Interests and expertise of key actors evolve over time





We characterize key actors based on common patterns

Table 1. Average values for key actors grouped in 5 clusters. The Interests columns show the top 3 categories and number of posts/threads in currency exchange. W=Web, G=Game, D=Code, T=Tech, C=Common, H=Hack, $=Money, X=Graphics, M=Market. +=positive reputations, 0=neutral reputations and -=negative reputations. EV=Eigenvector

#KeyActors	Activity		Interests				Reputation	Social relations			
	Days	Threads/Posts	cat1	cat2	cat3	#CurExc	Total (+/0/-)	H	i10	i100	EV
27	1298.4	74.1/1138.4	M	H	C	3.9/7.6	229.8 (61.3/2.3/4.3)	10.4	15.4	1.1	0.00
37	1595.0	163.8/3338.1	M	C	D/H	6.4/19.9	482.8 (230.9/7.4/6.9)	17.6	41.7	3.0	0.01
5	1951.0	831.0/18086.2	C	M	H	23.8/125.4	896.8 (578.2/68.8/99.0)	53.6	373.0	23.2	0.04
24	796.4	18.0/413.0	H	M	C/D	0.0/1.0	120.1 (58.0/2.4/3.2)	5.0	4.5	0.3	0.00
20	1895.7	383.6/10989.2	M	C	H	27.4/141.8	667.9 (311.6/27.0/48.3)	28.4	99.8	7.2	0.02

5 actors are well known in the community, they have high reputation and social impact

We characterize key actors based on common patterns

Table 1. Average values for key actors grouped in 5 clusters. The Interests columns show the top 3 categories and number of posts/threads in currency exchange. W=Web, G=Game, D=Code, T=Tech, C=Common, H=Hack, $=Money, X=Graphics, M=Market. +=positive reputations, 0=neutral reputations and -=negative reputations. EV=Eigenvector

#KeyActors	Activity		Interests				Reputation	Social relations			
	Days	Threads/Posts	cat1	cat2	cat3	#CurExc	Total (+/0/-)	H	i10	i100	EV
27	1298.4	74.1/1138.4	M	H	C	3.9/7.6	229.8 (61.3/2.3/4.3)	10.4	15.4	1.1	0.00
37	1595.0	163.8/3338.1	M	C	D/H	6.4/19.9	482.8 (230.9/7.4/6.9)	17.6	41.7	3.0	0.01
5	1951.0	831.0/18086.2	C	M	H	23.8/125.4	896.8 (578.2/68.8/99.0)	53.6	373.0	23.2	0.04
24	796.4	18.0/413.0	H	M	C/D	0.0/1.0	120.1 (58.0/2.4/3.2)	5.0	4.5	0.3	0.00
20	1895.7	383.6/10989.2	M	C	H	27.4/141.8	667.9 (311.6/27.0/48.3)	28.4	99.8	7.2	0.02

20 actors are prolific market traders, with high activity in currency exchange

We characterize key actors based on common patterns

Table 1. Average values for key actors grouped in 5 clusters. The Interests columns show the top 3 categories and number of posts/threads in currency exchange. W=Web, G=Game, D=Code, T=Tech, C=Common, H=Hack, $=Money, X=Graphics, M=Market. +=positive reputations, 0=neutral reputations and -=negative reputations. EV=Eigenvector

#KeyActors	Activity		Interests				Reputation	Social relations			
	Days	Threads/Posts	cat1	cat2	cat3	#CurExc	Total (+/0/-)	H	i10	i100	EV
27	1298.4	74.1/1138.4	M	H	C	3.9/7.6	229.8 (61.3/2.3/4.3)	10.4	15.4	1.1	0.00
37	1595.0	163.8/3338.1	M	C	D/H	6.4/19.9	482.8 (230.9/7.4/6.9)	17.6	41.7	3.0	0.01
5	1951.0	831.0/18086.2	C	M	H	23.8/125.4	896.8 (578.2/68.8/99.0)	53.6	373.0	23.2	0.04
24	796.4	18.0/413.0	H	M	C/D	0.0/1.0	120.1 (58.0/2.4/3.2)	5.0	4.5	0.3	0.00
20	1895.7	383.6/10989.2	M	C	H	27.4/141.8	667.9 (311.6/27.0/48.3)	28.4	99.8	7.2	0.02

2 similar groups (27+37 actors) with interest in market but different reputation and social impact

We characterize key actors based on common patterns

Table 1. Average values for key actors grouped in 5 clusters. The Interests columns show the top 3 categories and number of posts/threads in currency exchange. W=Web, G=Game, D=Code, T=Tech, C=Common, H=Hack, $=Money, X=Graphics, M=Market. +=positive reputations, 0=neutral reputations and -=negative reputations. EV=Eigenvector

#KeyActors	Activity		Interests				Reputation	Social relations			
	Days	Threads/Posts	cat1	cat2	cat3	#CurExc	Total (+/0/-)	H	i10	i100	EV
27	1298.4	74.1/1138.4	M	H	C	3.9/7.6	229.8 (61.3/2.3/4.3)	10.4	15.4	1.1	0.00
37	1595.0	163.8/3338.1	M	C	D/H	6.4/19.9	482.8 (230.9/7.4/6.9)	17.6	41.7	3.0	0.01
5	1951.0	831.0/18086.2	C	M	H	23.8/125.4	896.8 (578.2/68.8/99.0)	53.6	373.0	23.2	0.04
24	796.4	18.0/413.0	H	M	C/D	0.0/1.0	120.1 (58.0/2.4/3.2)	5.0	4.5	0.3	0.00
20	1895.7	383.6/10989.2	M	C	H	27.4/141.8	667.9 (311.6/27.0/48.3)	28.4	99.8	7.2	0.02

24 actors have few social impact, are interested in hacking and don't exchange currencies

PREDICTION

We developed tools to predict the likelihood of forum members being key actors

- Focus on the subset of **246k actors** with more than 5 posts and active after 2009
- Step 1. Selection of potential candidates:
  - **Backward Stepwise Logistic regression** to identify those variables that are more suitable for prediction
  - **Clustering** (k-means), with k=14 to get actors with similar behaviours
  - **Social Network Analysis**, to get common neighbours
- Step 2. **Topic Analysis** to confirm involvement in cybercrime-related activity

Logistic Regression provides the most relevant features for detection of key actors

Table 2. Logistic regression model predicting key actors

							95% C.I. for Exp(B)	
		B	S.E.	Wald	Sig.	Exp(B)	Lower	Upper
Step 15	DAYS_POSTING	.001	.000	19.407	.000	1.001	1.000	1.001
	REPUTATION	.001	.000	7.712	.005	1.001	1.000	1.001
	PRESTIGE	.006	.001	37.754	.000	1.006	1.004	1.008
	POSTS_HACK	.001	.000	25.397	.000	1.001	1.000	1.001
	POSTS_MARKET	.002	.000	65.945	.000	1.002	1.001	1.002
	POSTS_GAME	-.006	.001	15.670	.000	.994	.991	.997
	POSTS_GRAPHICS	-.009	.005	3.639	.056	.991	.982	1.000
	POSTS_CODE	.0005	.000	5.144	.023	1.0005	1.0001	1.0008
	POSTS_COMMON	-.0005	.000	4.945	.026	0.9995	.9991	0.9999
	POSTS_MONEY	-.003	.002	3.718	.054	.997	.994	1.000
	POSTS_CURRENCY_EXCHANGE	-.006	.003	6.041	.014	.994	.988	.999
	THREADS_GRAPHICS	-.044	.029	2.339	.126	.957	.905	1.012
	THREADS_COMMON	-.007	.003	5.637	.018	.993	.987	.999
	H_INDEX	.178	.017	108.025	.000	1.195	1.155	1.236
	NEGATIVE_REPUTATION	.018	.006	7.383	.007	1.018	1.005	1.031
	Constant	-9.372	.191	2397.372	.000	.000		

Using the model from Logistic Regression, we can query for likelihood of each actor being a key actor

Clustering uncovers small groups with high proportion of key actors

Table 3. Average values for actors grouped in 14 clusters. The Interests columns show the top 3 categories and number of posts/threads in currency exchange. W=Web, G=Game, D=Code, T=Tech, C=Common, H=Hack, $=Money, X=Graphics, M=Market. +=positive reputations, 0=zero reputations and -=negative reputations. EV=Eigenvector

#KeyActors / Total	Activity		Interests				Reputation	Social relations			
	Days	Threads/Posts	cat1	cat2	cat3	#CurExc	Total (+/0/-)	H	i10	i100	EV
1/8397	388.9	6.6/50.2	T/H	H/C	C/M	0.0/0.1	1.3 (0.4/0.0/0.1)	2.2	0.5	0.0	0.00
32/10323	1322.2	114.5/1310.2	M/C	C/M	G/H	3.5/9.8	113.9 (50.0/3.2/5.0)	11.6	17.4	0.5	0.00
0/4590	326.2	5.3/48.0	W	H	M/C	0.0/0.1	1.8 (0.6/0.1/0.1)	1.5	0.3	0.0	0.00
13/55364	338.6	7.3/46.4	H	M	C	0.0/0.1	0.7 (0.5/0.1/0.2)	2.3	0.5	0.0	0.00
9/41774	518.7	13.9/109.9	M	H/C	C/H	0.3/1.3	9.6 (3.4/0.3/0.5)	2.9	1.2	0.0	0.00
1/24202	310.9	5.7/56.2	G	H/C	M/H	0.0/0.1	2.0 (0.8/0.1/0.3)	1.9	0.7	0.0	0.00
0/36392	246.8	6.9/75.4	C	H	M	0.0/0.2	2.5 (1.1/0.2/0.4)	2.1	1.0	0.0	0.00
0/3474	296.3	3.8/90.6	T	H	C	0.0/0.1	4.1 (1.0/0.1/0.1)	1.1	0.3	0.0	0.00
0/14050	339.4	4.2/46.6	$	H	M/C	0.0/0.1	0.9 (0.4/0.1/0.1)	1.3	0.4	0.0	0.00
22/223	2111.7	611.2/11614.6	C	M	G/H	30.7/187.6	1170.7 (711.8/20.8/31.5)	32.2	162.8	8.2	0.03
3/9177	403.4	7.7/75.9	D	H	C	0.0/0.1	3.1 (1.1/0.1/0.2)	2.2	0.6	0.0	0.00
0/4845	302.2	6.9/71.0	X	H/C	M/H	0.0/0.1	5.1 (1.2/0.1/0.1)	2.1	0.8	0.0	0.00
31/2387	1723.8	295.9/4339.6	C	M	G	11.5/31.8	360.5 (170.2/9.8/13.8)	19.3	57.9	1.9	0.01
1/30437	215.8	0.2/18.2	H	M	C/$	0.0/0.0	0.2 (0.1/0.0/0.1)	0.1	0.0	0.0	0.00

We select potential actors that are likely involved in cybercrime

- Logistic Regression (*LogReg*): **88 potential actors** with 10% or more of likelihood of being a key actor
- Clustering (*Clust*): **201 potential actors** from the cluster with highest ratio of key actors
- Social Network Analysis (*SNA*): **42 potential actors** that are directly connected with at least 3 key actors
- Some actors appear in different groups:
  - LogReg & Clust & ¬SNA: 26
  - SNA & Clust & ¬LogReg: 7
  - LogReg & SNA & Clust: 10

Topic analysis is applied to confirm involvement in cybercrime-related conversations

- First, we compute the terms most frequently used by the key actors

Table 4. Most frequent terms used by the key actors. In parentheses are the number of key actors using each term. In bold are terms related to cybercrime.

rat (46), help (45), paypal (43), need (36), free (34), btc (34), **account** (33), thread (31), lr (28), server (26), new (25), **crypter** (25), pp (25), source (23), **fud** (23), service (22), **bot** (21), question (20), hf (16), code (15), steam (15), site (14), **shell** (14), cheap (14), money (14), skype (14), **booter** (13), window (12), anyone (12), tut (12), file (12), uid (11), someone (11), system (10), vbnet (10), vpn (10), **installs** (10), please (10), member (10), php (10), problem (10), **ddos** (10), password (10), website (10), update (10), setup (9), minecraft (9), email (9), game (9), vps (9), facebook (8), list (8), proxy (8), design (8), **darkcomet** (8), **keylogger** (8), irc (8), java (8), coder (8), day (8), time (8), net (7), post (7), product (7), tool (7), beta (7), sale (7), **exploit** (7), people (7), bitcoin (7), buying (7), **stealer** (6), version (6), **stresser** (6), live (6), feature (6), **botnet** (6), domain (6), signature (6), shop (6), black (6), omc (6), web (6), year (6), support (6), official (6), youtube (6)

Topic analysis is applied to confirm involvement in cybercrime-related conversations

- First, we compute the terms most frequently used by the key actors
- Second, we obtain terms for potential key actors and predict based on:
  - A Number of terms that coincide with those of key actors ($> 20\%$)
  - B Presence of cybercrime-related terms (> 2)

Table 5. Summary of prediction using topic analysis

Subset	Predicted/Total (%)	Avg. distance	Farthest	Closest
LogReg	22/52 (42.31)	0.43	0.10	0.72
Clust	34/165 (20.61)	0.66	0.29	0.93
SNA	9/25 (36.00)	0.57	0.36	0.75
LogReg & Clust	8/26 (30.77)	0.63	0.36	0.89
SNA & Clust	0/7 (0.00)	0.66	0.50	0.79
LogReg & Clust & SNA	7/10 (70.00)	0.60	0.43	0.68

Topic analysis is applied to confirm involvement in cybercrime-related conversations

- First, we compute the terms most frequently used by the key actors
- Second, we obtain terms for potential key actors and predict based on:
  - A Number of terms that coincide with those of key actors ($> 20\%$)
  - B Presence of cybercrime-related terms (> 2)

- Overall, we predict **80 new key actors**. We manually inspected their forum content, confirming that all of them are key actors

Topic analysis is applied to confirm involvement in cybercrime-related conversations

- First, we compute the terms most frequently used by the key actors
- Second, we obtain terms for potential key actors and predict based on:
  - A Number of terms that coincide with those of key actors ($> 20\%$)
  - B Presence of cybercrime-related terms (> 2)

- Overall, we predict **80 new key actors**. We manually inspected their forum content, confirming that all of them are key actors
- More Info:

"Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum", S. Pastrana , A. Hutchings, A. Caines, P. Buttery. Accepted at Research in Attacks, Intrusions and Defences (RAID) , Heraklion, Crete, September 2018 `https://www.cl.cam.ac.uk/~sp849/files/RAID_2018.pdf`

Outline

Our research follows ethical guidelines and has been approved by our REB

- Follow guidelines from Computer Laboratory Ethics Committee
  - Exempted for collection, required approval for analysis
- Research is ethical if benefits outweigh potential harms
- Collection:
  - Terms of agreements of criminal communities are unenforceable [Martin & Christin 2016]
  - We do not break CAPTCHA.
    - Session cookies are provided by the sites
  - Informed consent is not required if:
    1. Data is collected from the Internet and thus it is public
    2. Data is used for analysing collective behaviour without identifying particular members
- Analysis:
  - Neither identify humans nor focus on social groups
  - Present results objectively

Data science approaches are needed to analyse underground forums!

- CrimeBB enables cybercrime research. Ask for it!

  https://www.cambridgecybercrime.uk

- Traditional NLP techniques must be adapted for language used in underground forums
- We characterize key actors and predict new accounts
- Future work includes
  - Include new forums (also non-English)
  - Improve/extend data science
  - Study particular business models. Key actors might differ

Data science approaches are needed to analyse underground forums!

- CrimeBB enables cybercrime research. Ask for it!

  https://www.cambridgecybercrime.uk
- Traditional NLP techniques must be adapted for language used in underground forums
- We characterize key actors and predict new accounts
- Future work includes
  - Include new forums (also non-English)
  - Improve/extend data science
  - Study particular business models. Key actors might differ

Contact details: Andrew Caines
apc38@cam.ac.uk

Contact details: Sergio Pastrana
Sergio.Pastrana@cl.cam.ac.uk

Data science approaches to understanding key actors on online hacking forums

Andrew Caines

Theoretical & Applied Linguistics
Faculty of Modern & Medieval Languages

Sergio Pastrana

Cambridge Cybercrime Centre
Department of Computer Science and Technology

Third Annual Cybercrime Conference, Cambridge
July 12, 2018

UNIVERSITY OF CAMBRIDGE