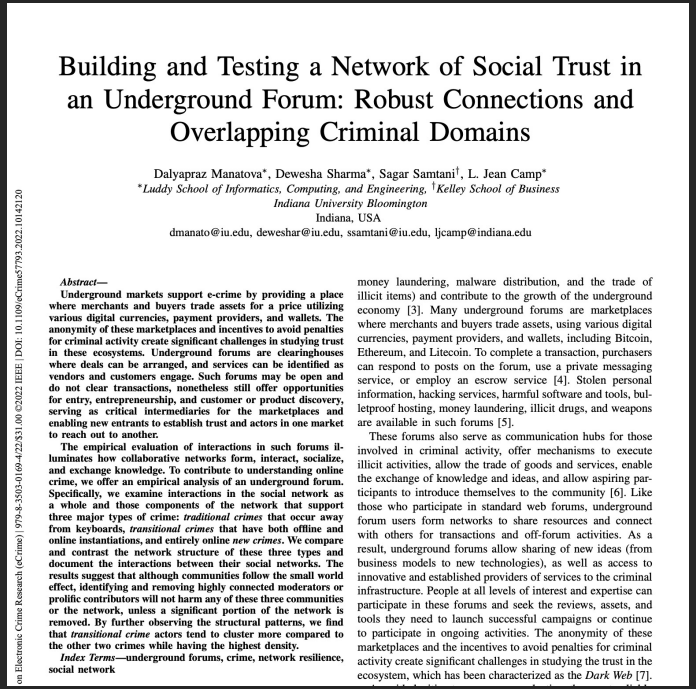
Building and Testing a Network of Social Trust in an Underground Forum: Robust Connections and Overlapping Criminal Domains

Dalyapraz Manatova, Indiana University, Bloomington
Dewesha Sharma, Indiana University, Bloomington
Sagar Samtani, Indiana University, Bloomington
L. Jean Camp, Indiana University, Bloomington



Building and Testing a Network of Social Trust in an Underground Forum: Robust Connections and Overlapping Criminal Domains

Dalyapraz Manatova*, Dewesha Sharma*, Sagar Samtani†, L. Jean Camp*
*Luddy School of Informatics, Computing, and Engineering, †Kelley School of Business
Indiana University Bloomington
Indiana, USA
dmanato@iu.edu, deweshar@iu.edu, ssamtani@iu.edu, ljcamp@indiana.edu

on Electronic Crime Research (eCrime) | 979-8-3503-0169-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/eCrime57793.2022.10142120

***Abstract*—**
Underground markets support e-crime by providing a place where merchants and buyers trade assets for a price utilizing various digital currencies, payment providers, and wallets. The anonymity of these marketplaces and incentives to avoid penalties for criminal activity create significant challenges in studying trust in these ecosystems. Underground forums are clearinghouses where deals can be arranged, and services can be identified as vendors and customers engage. Such forums may be open and do not clear transactions, nonetheless still offer opportunities for entry, entrepreneurship, and customer or product discovery, serving as critical intermediaries for the marketplaces and enabling new entrants to establish trust and actors in one market to reach out to another.

The empirical evaluation of interactions in such forums illuminates how collaborative networks form, interact, socialize, and exchange knowledge. To contribute to understanding online crime, we offer an empirical analysis of an underground forum. Specifically, we examine interactions in the social network as a whole and those components of the network that support three major types of crime: *traditional crimes* that occur away from keyboards, *transitional crimes* that have both offline and online instantiations, and entirely online *new crimes*. We compare and contrast the network structure of these three types and document the interactions between their social networks. The results suggest that although communities follow the small world effect, identifying and removing highly connected moderators or prolific contributors will not harm any of these three communities or the network, unless a significant portion of the network is removed. By further observing the structural patterns, we find that *transitional crime* actors tend to cluster more compared to the other two crimes while having the highest density.

***Index Terms*—underground forums, crime, network resilience, social network**

money laundering, malware distribution, and the trade of illicit items) and contribute to the growth of the underground economy [3]. Many underground forums are marketplaces where merchants and buyers trade assets, using various digital currencies, payment providers, and wallets, including Bitcoin, Ethereum, and Litecoin. To complete a transaction, purchasers can respond to posts on the forum, use a private messaging service, or employ an escrow service [4]. Stolen personal information, hacking services, harmful software and tools, bulletproof hosting, money laundering, illicit drugs, and weapons are available in such forums [5].

These forums also serve as communication hubs for those involved in criminal activity, offer mechanisms to execute illicit activities, allow the trade of goods and services, enable the exchange of knowledge and ideas, and allow aspiring participants to introduce themselves to the community [6]. Like those who participate in standard web forums, underground forum users form networks to share resources and connect with others for transactions and off-forum activities. As a result, underground forums allow sharing of new ideas (from business models to new technologies), as well as access to innovative and established providers of services to the criminal infrastructure. People at all levels of interest and expertise can participate in these forums and seek the reviews, assets, and tools they need to launch successful campaigns or continue to participate in ongoing activities. The anonymity of these marketplaces and the incentives to avoid penalties for criminal activity create significant challenges in studying the trust in the ecosystem, which has been characterized as the *Dark Web* [7].

The 17th Symposium on Electronic Crime Research APWG

Outline

- What we know about eCrime communities and participants
- Key observations we want to test
- Our approach
- Our findings

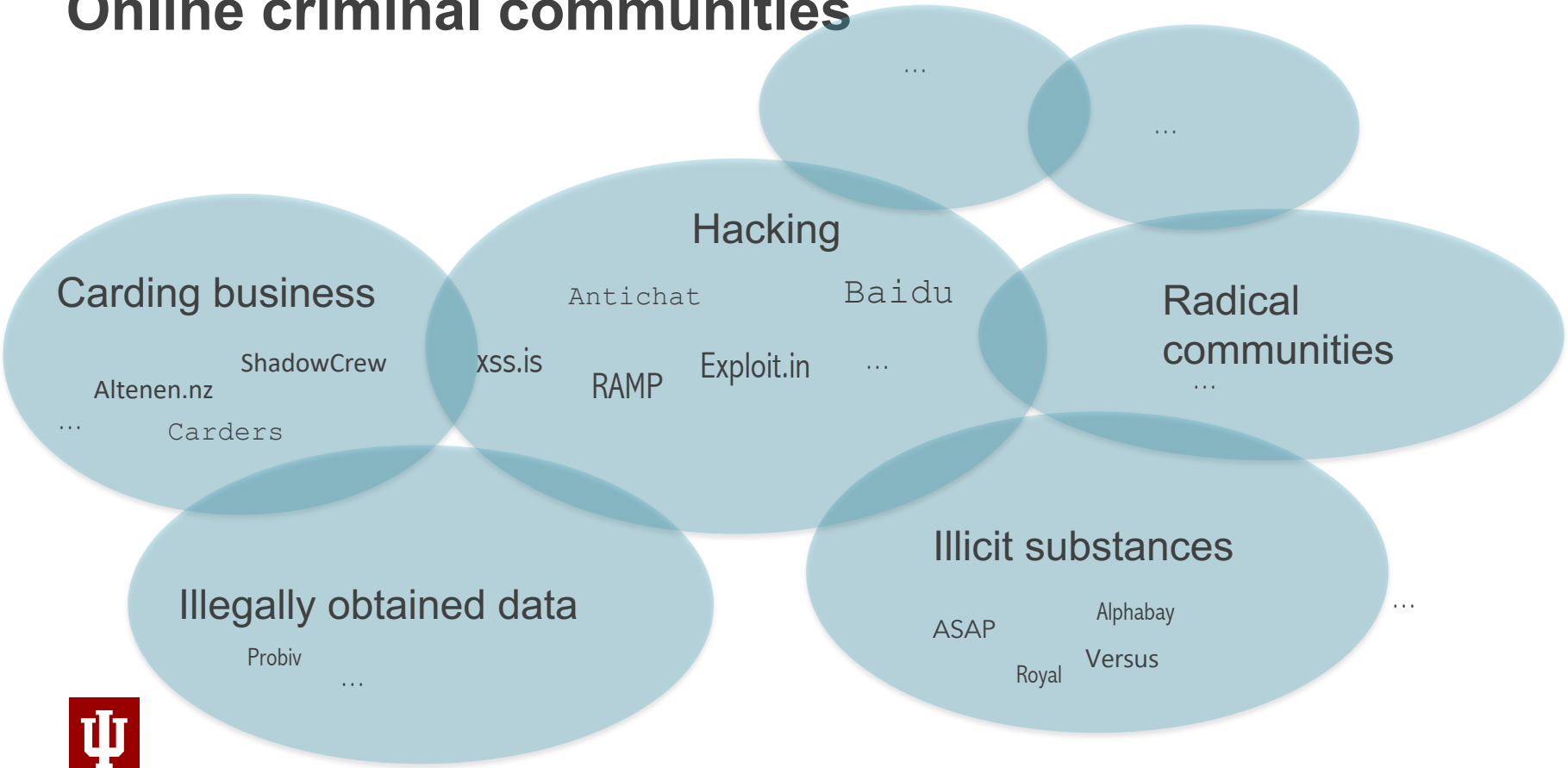
We know that eCrime “communities”

- Tend to cluster in specific forums
  - By topic
  - By type of crime
  - By language
- Tend to treat forums as marketplaces
- **Employ admins and moderators governing such spaces who are involved in the community themselves**
- **When get disrupted, assemble back in new forums or online spaces**

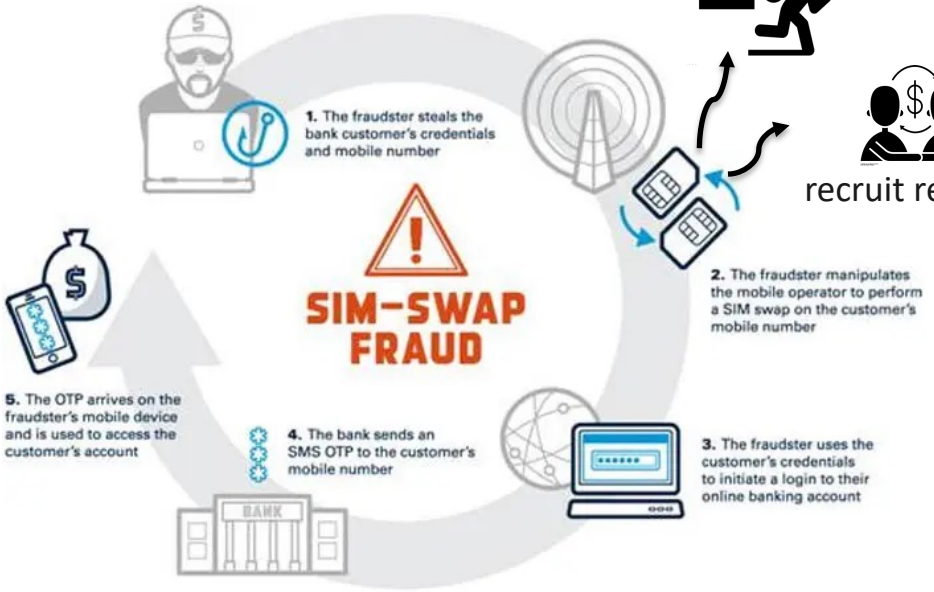
eCrime Participants

- Utilize multiple anonymous identities
- Build branding tied to such identities
- Build communities online through different platforms and forums
- **Build trust over repeated interactions**

Online criminal communities



Example: SIM Swapping



https://cyberhoot.com/cybrary/sim-swapping/

steal tablets from retails workers

"Remo Snatching"

recruit retail workers

Source: https://www.n0sec.io/blog/how-to-rob-a-mobile-carrier
https://flashpoint.io/blog/sim-swap-fraud-account-takeover/

How can we categorize crimes online?

Traditional

Typical conventional crime
(i.e., drug dealing, physical abuse, illicit materials, etc.)

Purely online

Unique to electronic networks
(i.e., hacking services, doxxing, malware, phishing, ransomware, fake AV, DDOS, etc.)

Transitional

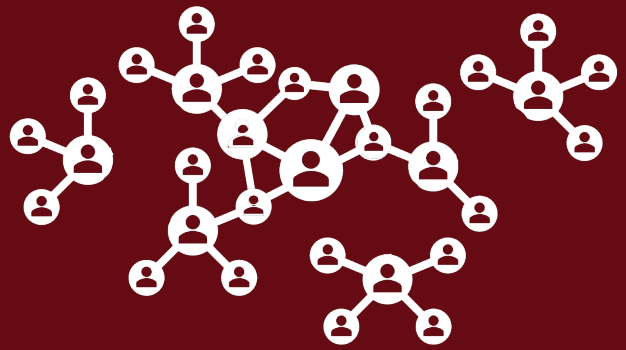
Instantiations in both worlds
(i.e., carding, skimming, tax fraud, forgery, money laundering etc.)

R. Anderson, C. Barton, R. B¨ohme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime,"The Economics of Information Security and Privacy, pp. 265–300, 2013

Observations are that:

- There is an **overlap** of user domain across multiple online spaces and crime domains
- Open eCrime communities are **scale-free** (small % of key members)
- **Moderators** and **admins** are key members and are targets of law enforcement
- But online communities are **resilient** and reassemble back

If key members are ***removed*** how much ***disruption*** it causes for the communities?



How ***resilient*** are the criminal communities online?

How much ***overlap*** and ***connectedness*** between different *types of crimes* online?

If only there was Reddit for criminals, where everyone would go…

/d/hacking

RULES NEWBIE? CLICK HERE MANIFESTO SERVICES TUTORIALS

2

Talking to ransom victims safely 1

2 by [redacted] 4 days 3 in /d/hacking 4

how can i talk to my victims without using hsitty services like protonmail and honeypots
can dread messanger do the trick? 5

6 comments

Comments

Sort comments by **Top**

6

[redacted] 1 points 4 days ago

Just use other TOR email service that is known you are not giving them your address you are giving them hopefully XMR address this is no need to be too secret it will be okay to use such an email but not proton mail as you say if you want to be careful but do not do dread messenger that is horrible idea in my opinion it is not meaning to be rude it would just be bad idea to bring random people on to a dark net forum with captcha and these things just for them to figure out how to message you this is not a good idea in my opinion

[redacted] 1 points 2 days ago

Thanks, I did some searching and found some tor-only email services. and some like elude which use both dark and clearnet. which I'm going for so my victims can contact me easier and without downloading anything

About proton mail, i know i don't give 'em my address but there is RaaS criminals like the physician guy (Thanos RaaS owner) who got caught using Proton mail. And what i hate most is they lie about what they do like not storing IP's which is impossible on how the internet is designed. Sure they're servers are in Switzerland and don't give data to other countries but that doesn't mean they don't give them to Switz police

/d/hacking
9,341 subscribers

SUBSCRIBE

SUBMIT A POST

Everything related to hacking, opsec, and programming. Malware, phishing, DDoS, coding, research and news.

Rules:
- Be civil.
- No promotion for paid content or selling of guides.
- No looking for or advertising hacking services. For that please visit /d/Jobs4Crypto.
- Be nice to newbies, you used to be one of them.

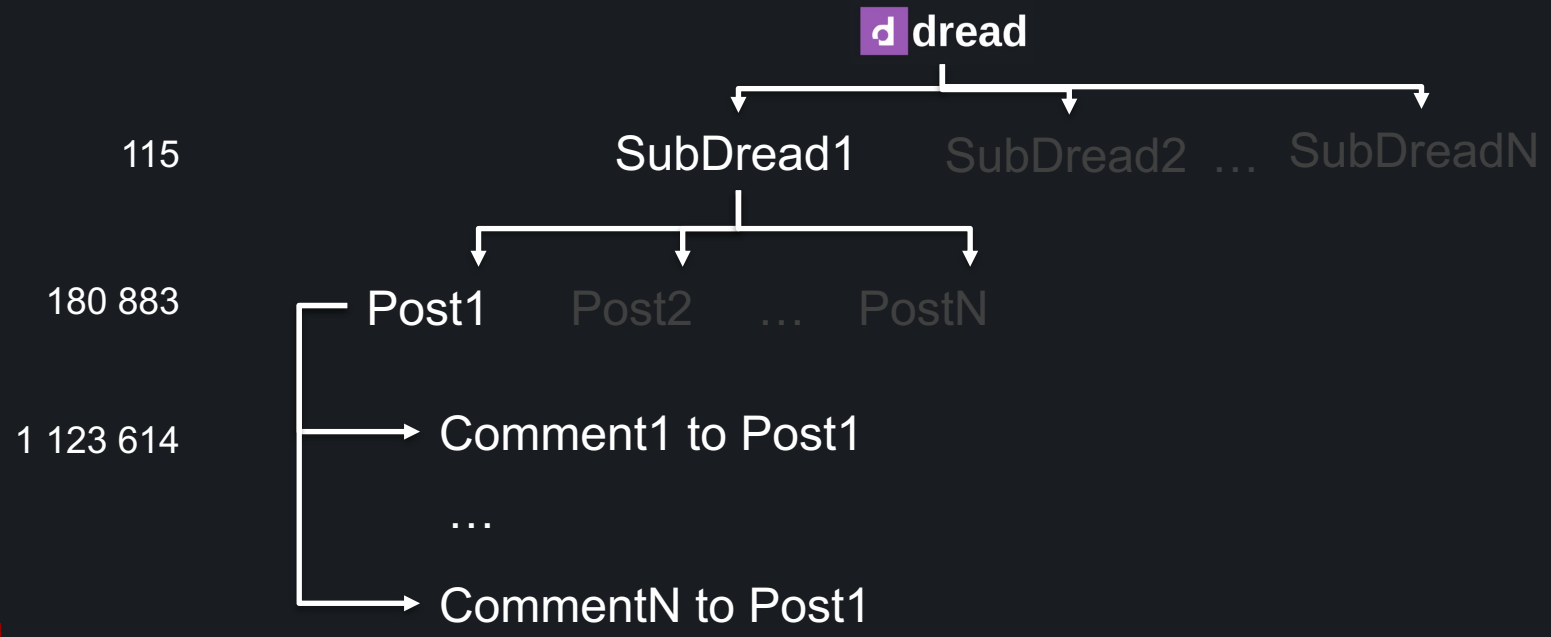
All rules as well as the punishments are here.

Moderators

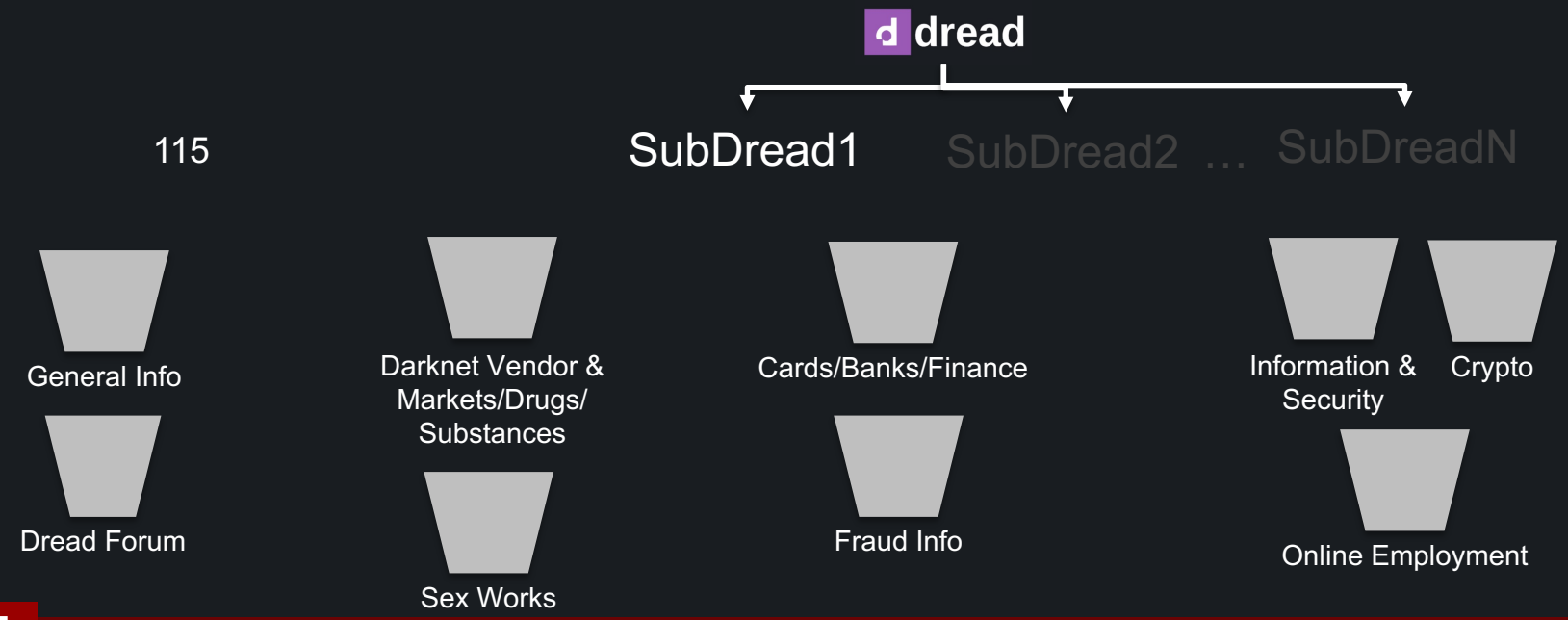
[redacted] A
[redacted] Moderator
[redacted] Moderator

Forum’s structure

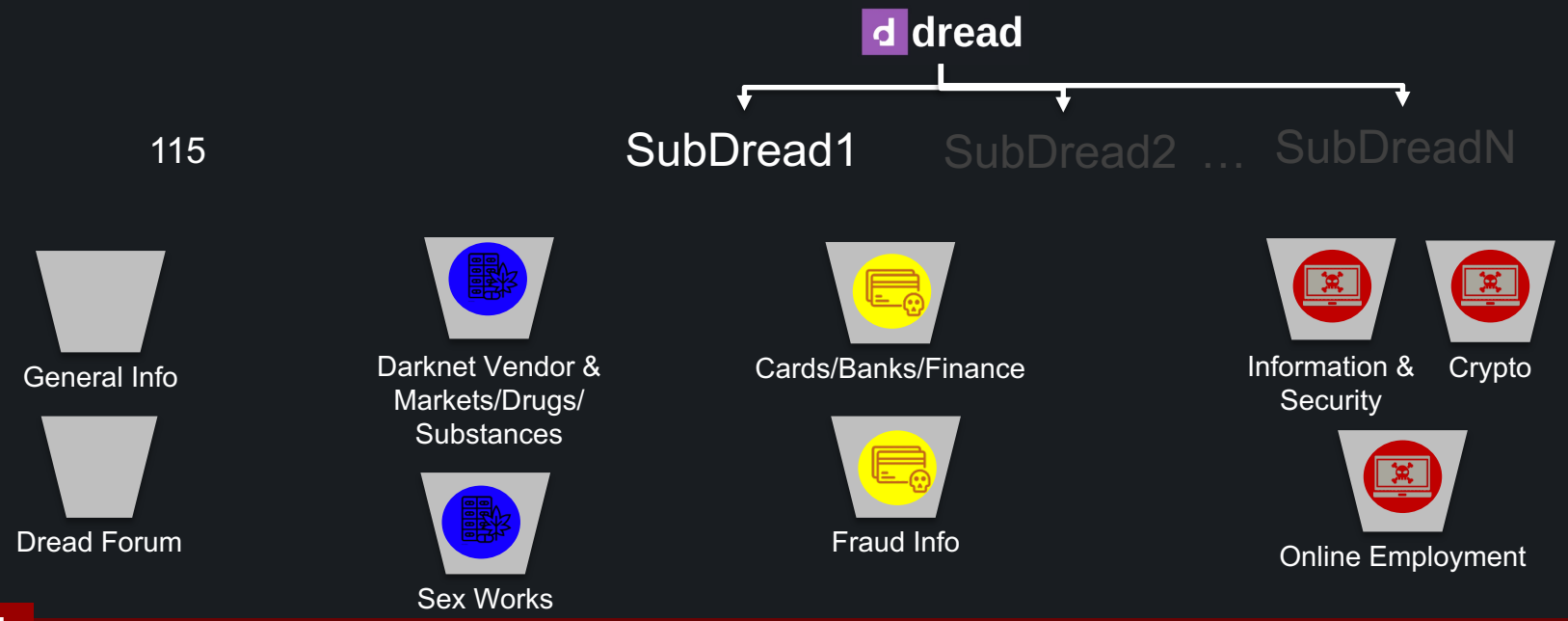
Reddit like



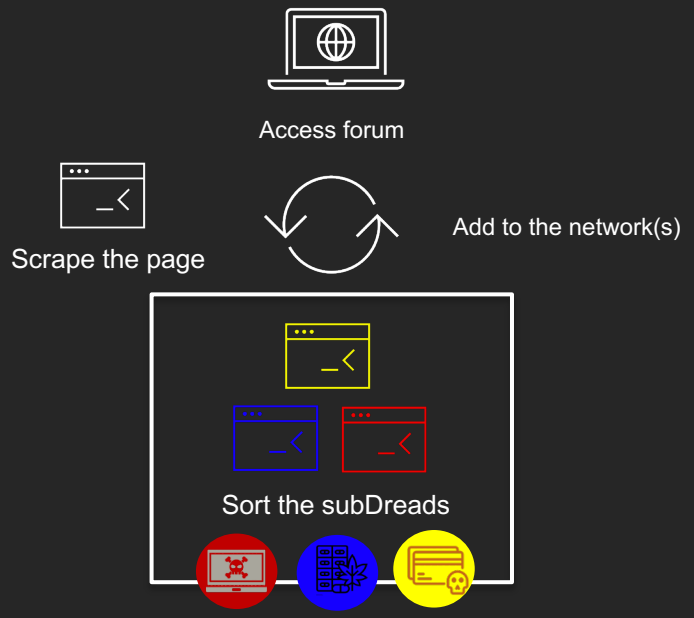
Thematic Analysis of SubForums & Grouped Themes

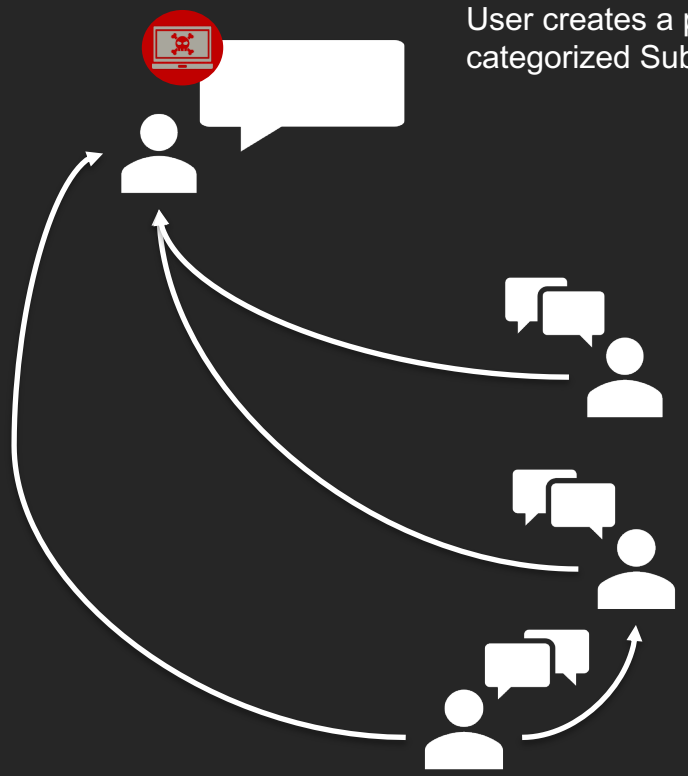


Categorization by Crime Type



Social Network Construction





Results: Different Crime Types, Different Structures

86,465 users

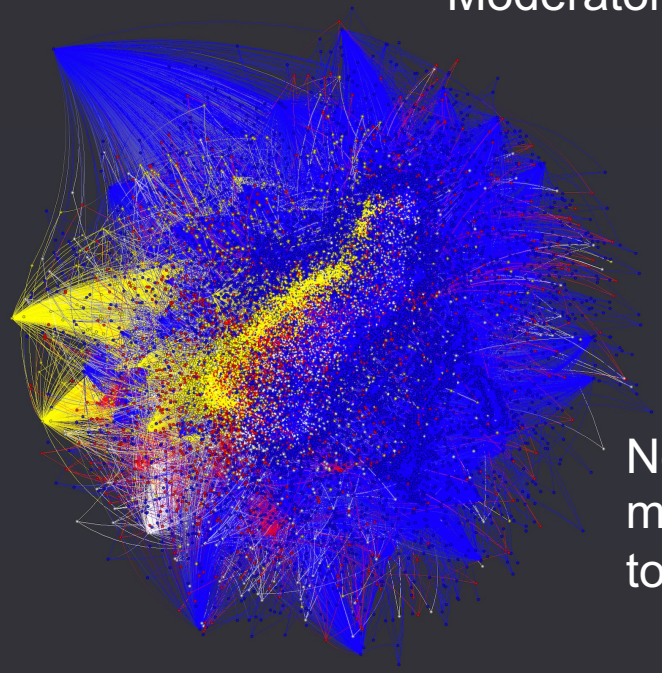
326 moderators

480,119 edges

5.81 average degree

794,318 sum of all weights

Moderator Assortativity = -0.0142

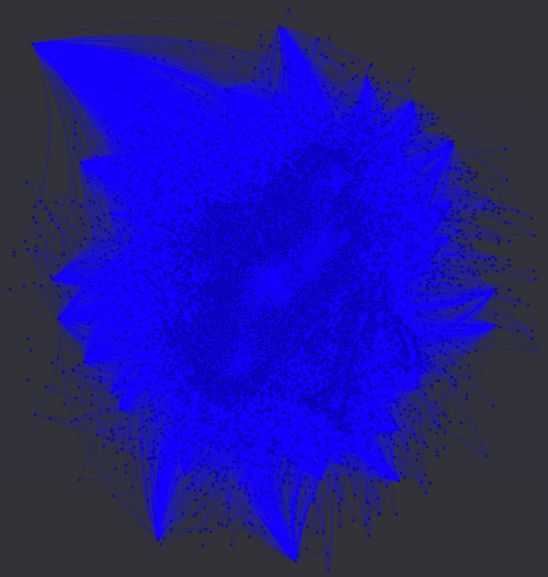


Negative tendency of the moderators
to connect with each other

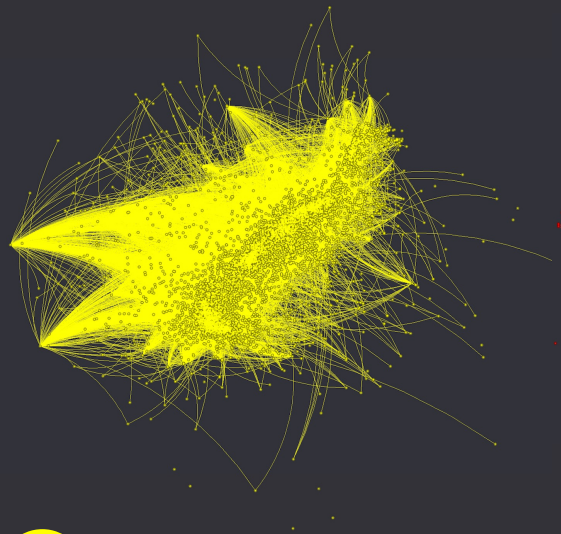
Results: Different Crime Types, Different Structures

Type of Crime Assortativity = 0.505

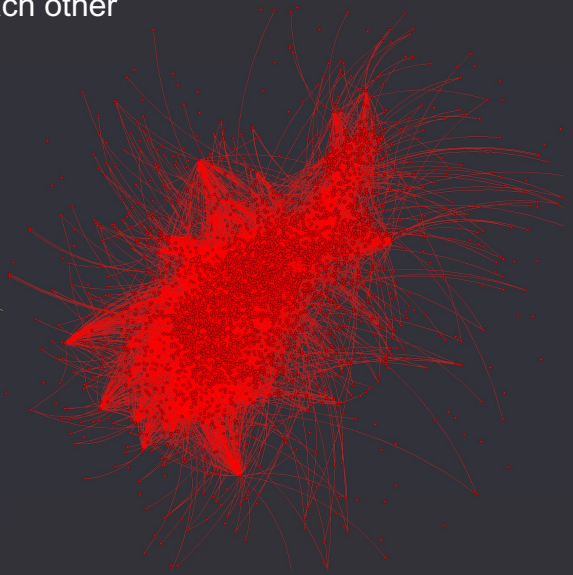
High tendency of the users from the same crime to connect with each other



traditional crime discussions



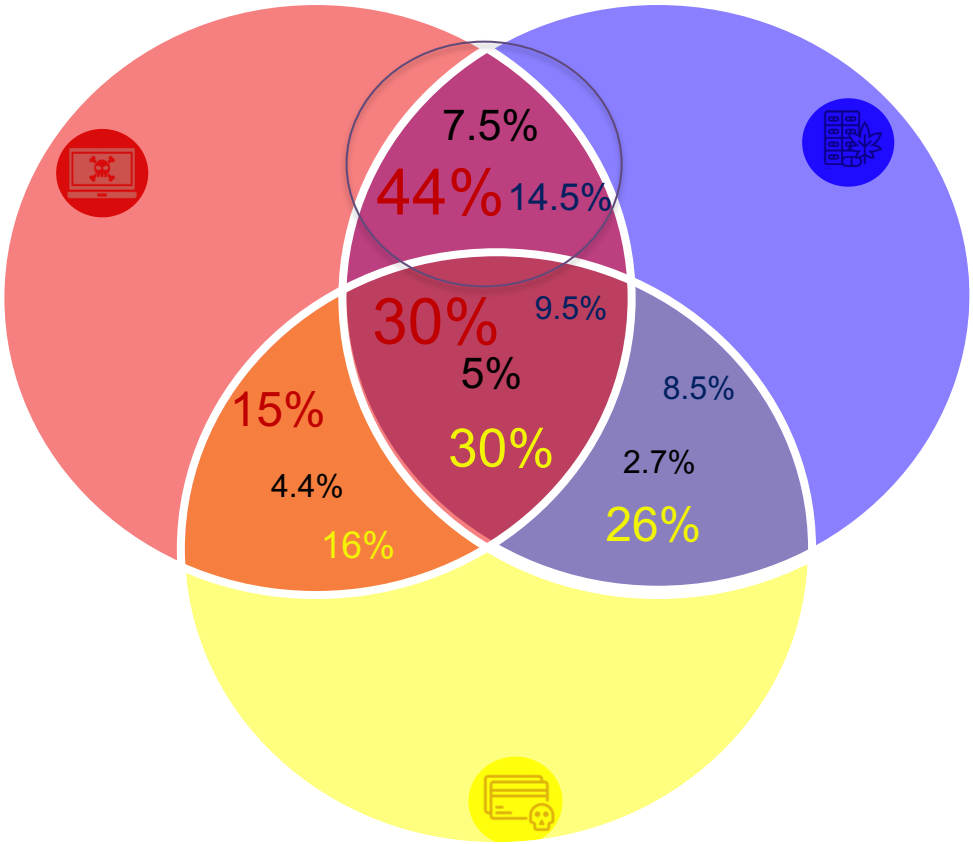
transitional crime discussions



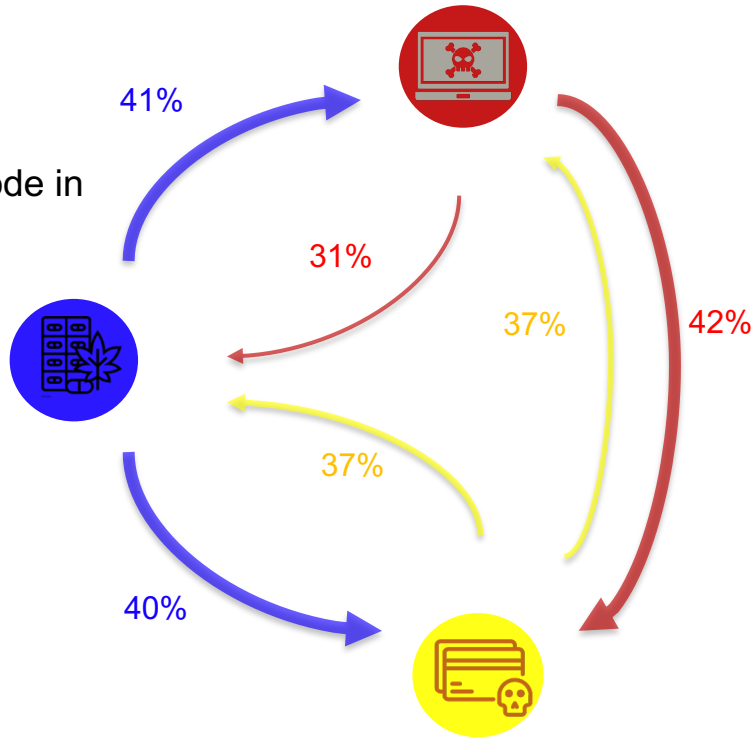
purely online crime discussions

	Traditional Crime	Transitional Crime	New Crime
Statistics of the networks without isolated nodes:			
Nodes	21,902	7,870	8,328
Edges	97,355	30,031	25,050
Sum of All Weighted Edges	165,464	42,189	37,054

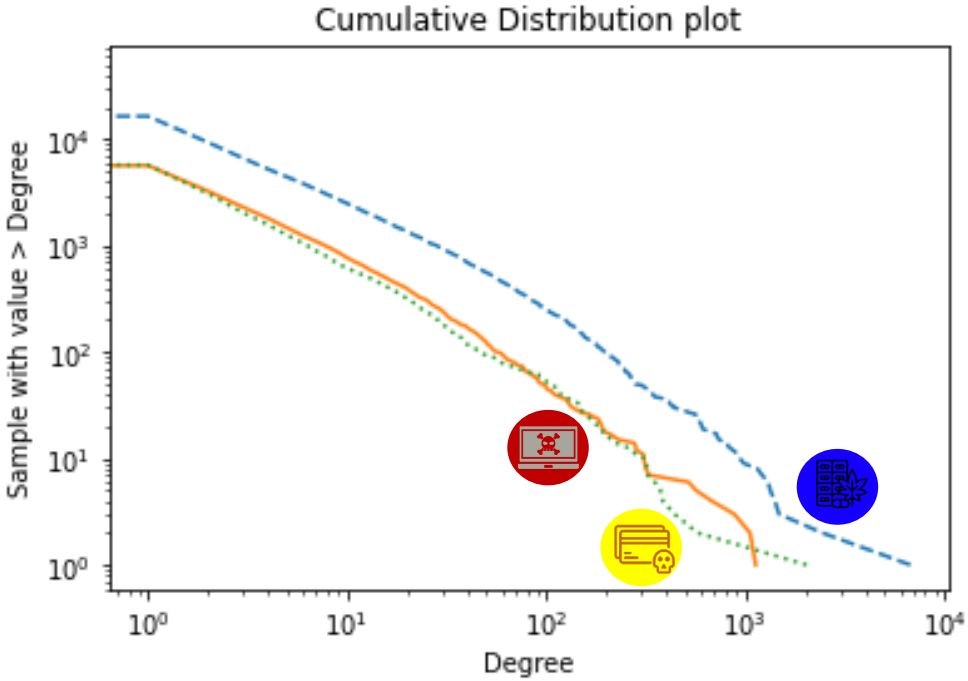
Overlap & Connectedness of Users from Different Crimes



nodes from one crime network
that have connection to any node in
another crime network



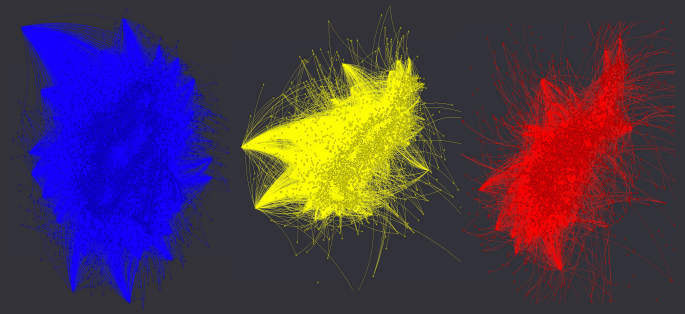
Scale-free crime networks



Average Degree	4.445	3.816	3.007
Max In-Degree	2,346[a]	470	773[b]
Max Out-Degree	6,753	1,128	2,033[b]
Density	0.000203	0.000485	0.000361
Diameter of LCC	13	14	14
Strongly Connected Components	7	4	2
Size of Strong LCC	24.45%	19.89%	12.85%
Weakly Connected Components	181	76	79
Size of Weak LCC	98.10%	97.87%	97.97%
Average Clustering Coefficient	0.00182	0.00484	0.00197
Average Shortest Path	1.473	1.441	1.185

[a] Only contributed to the single type of crime discussions
[b] Same user

Method



Remove top nodes & measure the size
of Largest Connected Component (LCC)

There are Strong LCC and Weak LCC

Calculated metrics
&
Find top users

Centrality metrics

Weighted in-degree

~ attention from others

Weighted out-degree

~ responding to others

Weighted degree

Betweenness centrality

~ "middleman" for others
or key member for the information flow

PageRank score

~ attention from influencers

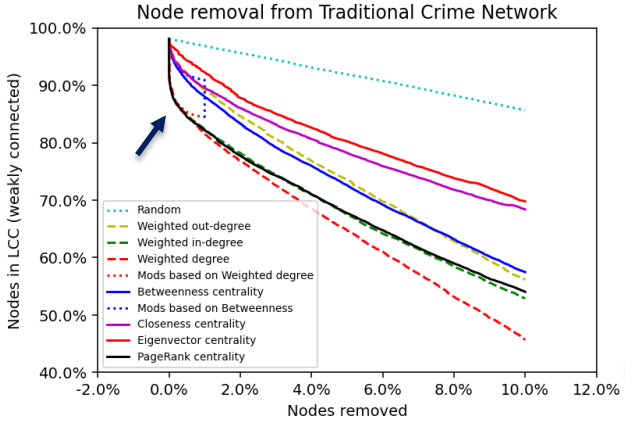
Closeness centrality

~ easy access to all other users

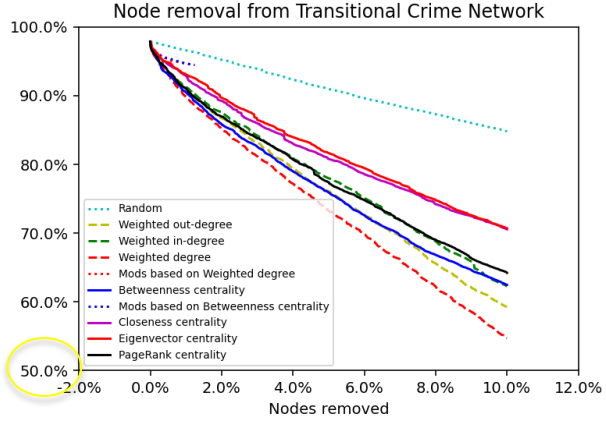
Eigenvector score

~ wide-reaching influence

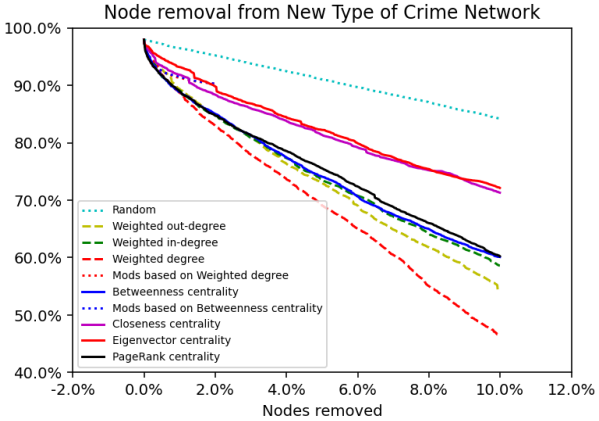
Weak connections (directions are not important)



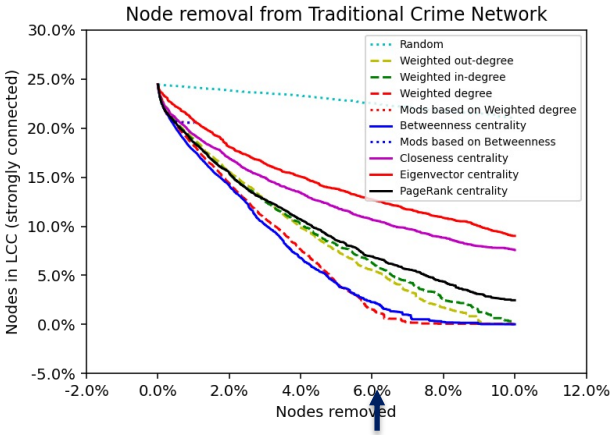
PageRank



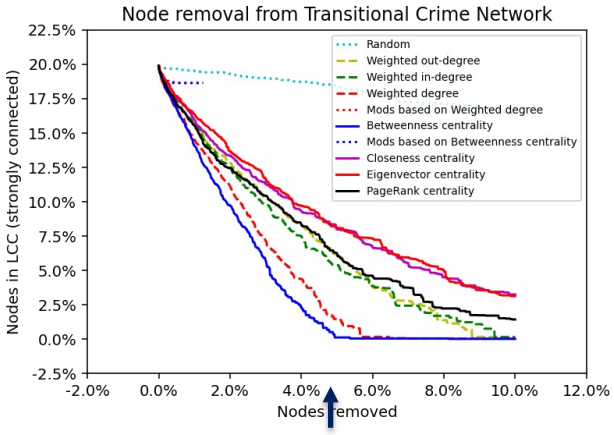
Clustering is significantly higher



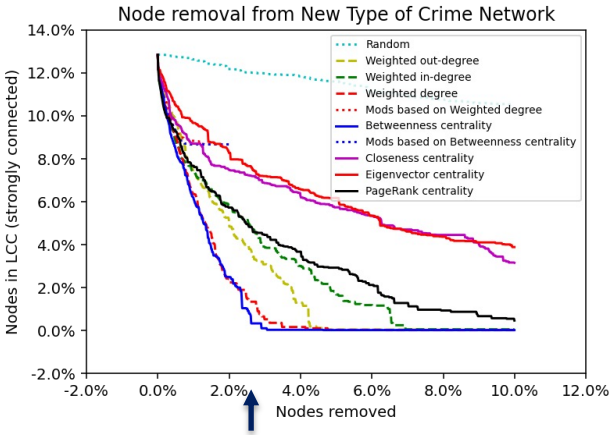
Strong connections (directions are important)



~ 1 300

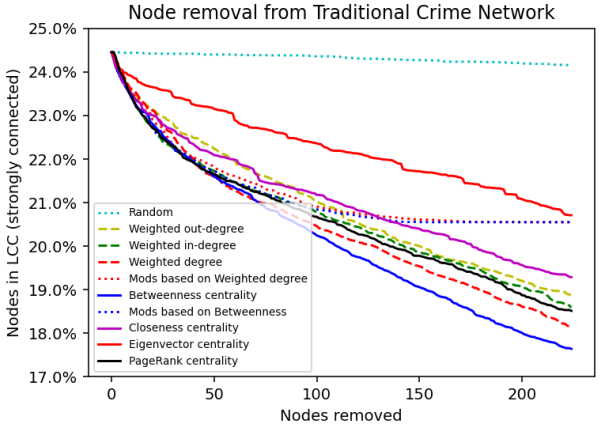


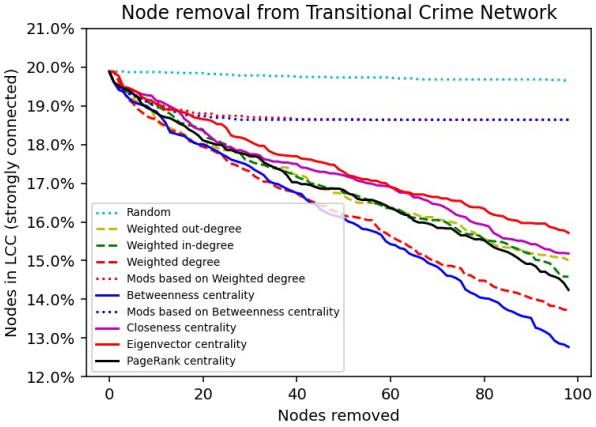
~ 400

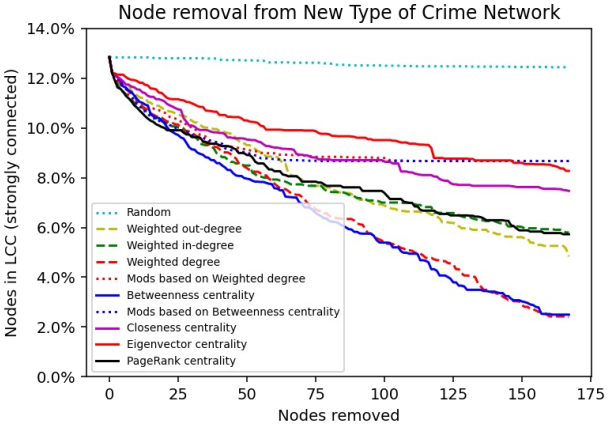


~ 250

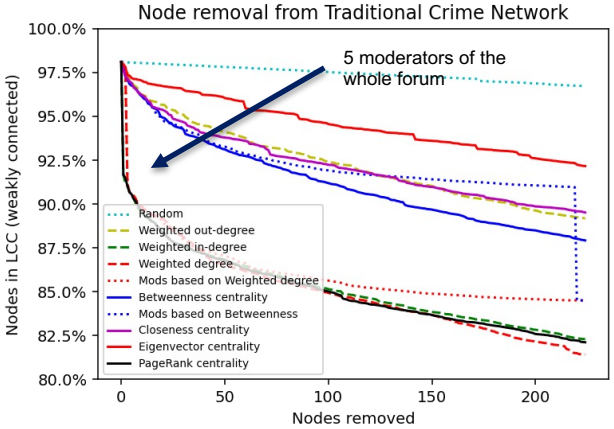
Strong connections of moderators (directions are important)

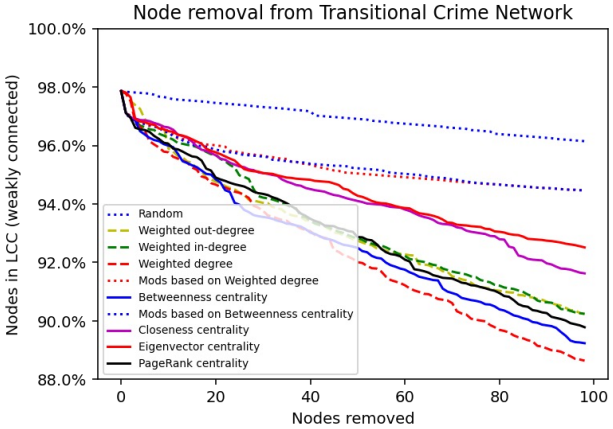


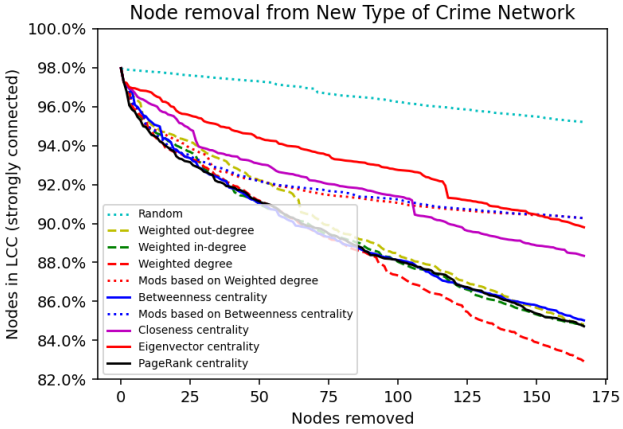




Weak connections of moderators (directions are important)







Concluding Remarks

1. There is an evidence of ***overlap*** between major criminal domains. Overlaps are higher between ***traditional*** and ***online*** crimes.

Deutsche Welle + Follow View Profile

Cambodia: Human trafficking crisis driven by cyber scams

Story by Enno Hinz, Deutsche Welle • Sep 12 React Comments

"They are scamming victims but there are also slavery victims. Those slavery victims are being used to scam the victims to lose their money," she told DW.

Concluding Remarks

1. There is an evidence of ***overlap*** between major criminal domains. Overlaps are higher between ***traditional*** and ***online*** crimes.

2. Although criminal social networks are scale-free, ***removing key nodes*** is ***not an effective*** disruption. Communities have ***robust*** ties.

3. Some ***moderators*** are also ***key members*** of community, but **not all**. And key moderators appear in ***overlaps***.

Thank you!

dmanato@iu.edu