



black hat[®]
USA 2024

AUGUST 7-8, 2024
BRIEFINGS

Relationships Matter: Reconstructing the Organizational and Social Structure of a Ransomware Gang

Speaker(s): Dalya Manatova and L Jean Camp

Indiana University



Dalya Manatova

Doctoral Researcher

Ostrom Fellow

Indiana University

L Jean Camp

Professor, IU

Fellow, IEEE

Fellow, ACM

Fellow, AAAS



Modern eCrime

Attackers are described as

- Exciting
- Artists
- Innovative
- Anonymous
- Reputation & profit maximizing



Is Organized

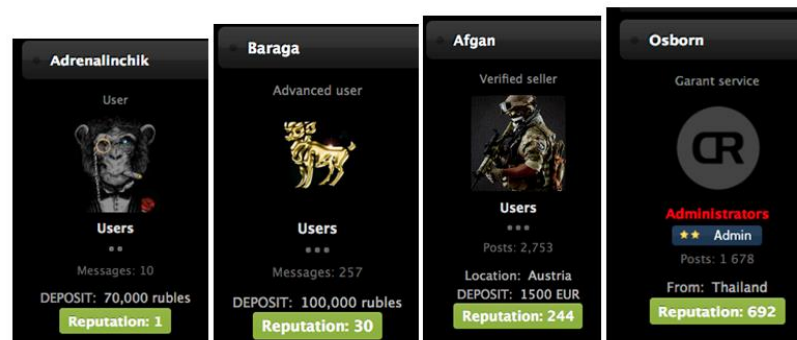
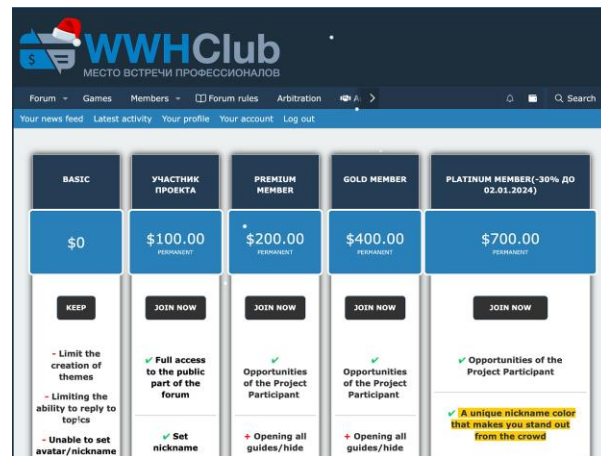
eCrime as a service is a *commodity*

- "Boring"
- Coordinated
- Standardized
- Branded
- Resilience maximizing



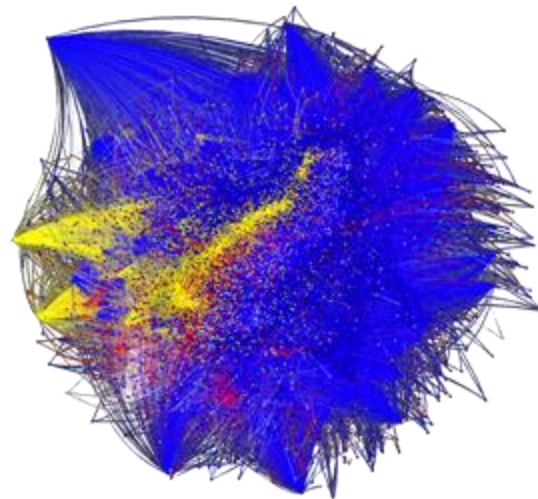
eCrime “communities”

- Have their own social system
 - Friendships – natural connections
 - Hierarchies - connections imposed by the structure
 - Reputations – social validation
 - Patterns of communication – actual behaviors of interaction



eCrime “communities”

- Specialize
 - Tend to cluster in specific forums
 - By topic
 - By type of crime
 - By language



Crime type clusters in a diverse underground forum

We know that eCrime “communities”

- Tend to treat forums as marketplaces

Examples of arbitration threads in a Russian forum (translated)

 Black zoper Mask · Yesterday at 9:04 PM	 Replies: e leven Views: 155	Today at 2:26 PM admin 
 Arbitration Carloson 8500 \$ dumps AL I PENTEST · Sunday at 5:18 PM 2	Replies: 32 Views: 1K	Today at 9:33 AM Karlsson 
 Arbitration Lockbit mīchon · Yesterday at 5:46 PM 4 5 6	 Replies: 111 Views: 6K	Today at 3:06 AM Lockbitsupp 
 Arbitration Big-Bro, \$ 2500 SGL · Sunday at 11:05 PM	Replies: 12 Views: 637	Today at 12:51 AM tsyko 
 Arbitration AppleStore Deposit Compensation (RENT DRAINER) apt-money · Jan 19, 2024	Replies: 14 Views: 922	Yesterday at 9:27 AM apt-money 

Source: cybercrimediaries.com

eCrime “Communities” Organizations

- Are organizations with
 - Roles
 - Tasks
 - Scale
 - Scope
 - Social networks
 - *Resilience — ability to adapt to the environment*

HOW AN ORGANISED CRIMINAL GROUP IS SET UP



TEAM LEADER

Responsible for overall missions and communication with workers



CODER

Malware developers who focus on writing software which infects systems, spreads automatically and evades detection



NETWORK ADMINISTRATOR

Manages a large number of compromised systems used to spread malicious payloads, such as viruses, spam and denial-of-service attack packets



INTRUSION SPECIALIST

These concentrate on making sure any successfully installed malware persists allowing continuing compromise



DATA MINERS

Needed to make sense of the stolen data by organising and reformatting for ease of sale; here they make use of crowdsourcing



MONEY SPECIALIST

These identify ideal ways to make money from all their datasets

Source: raconteur.net

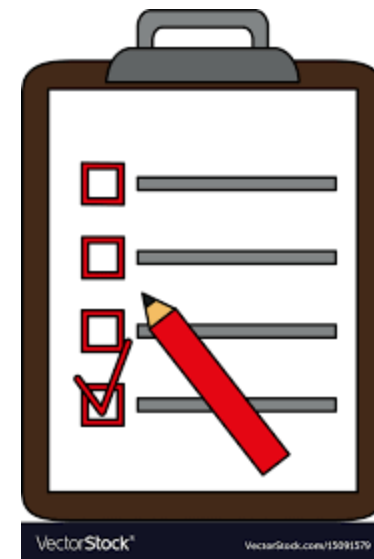
Tools & Techniques for Understanding Sustainable eCrime

Linguistic

Social

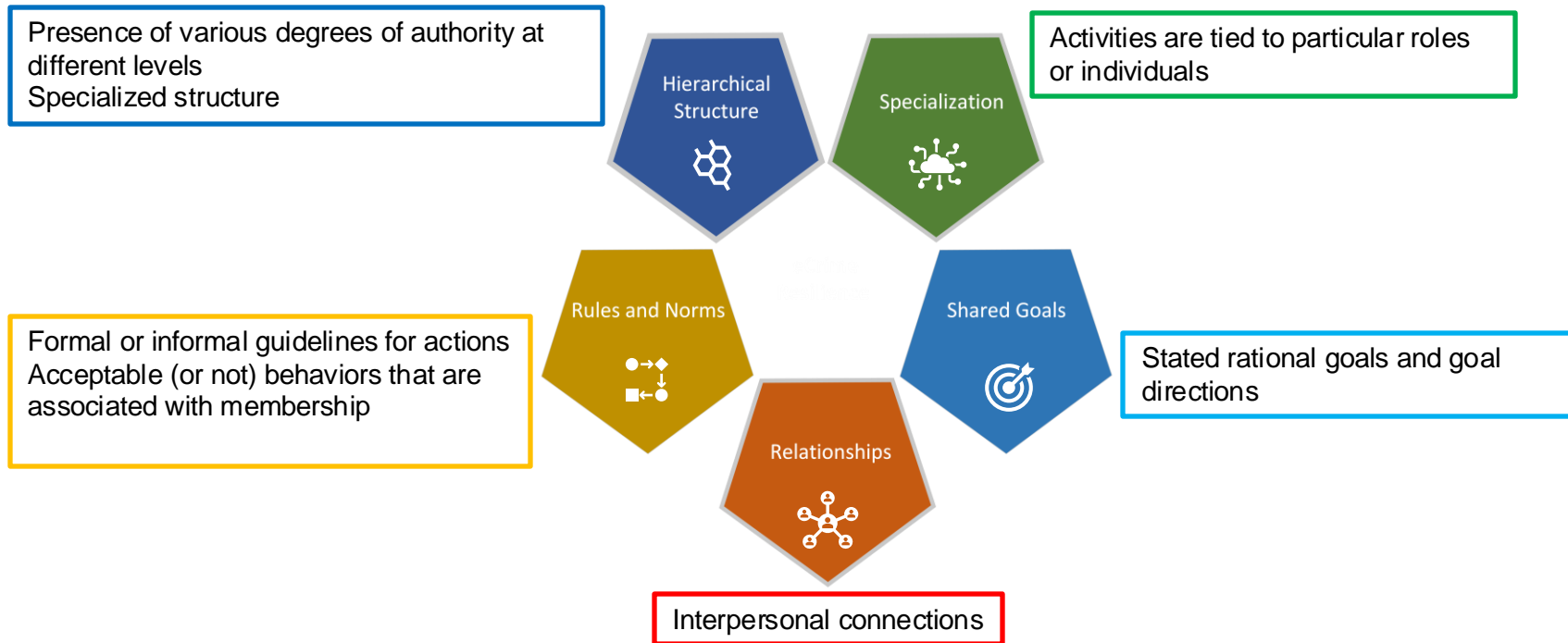
Organizational

Your attack chain is their task
management

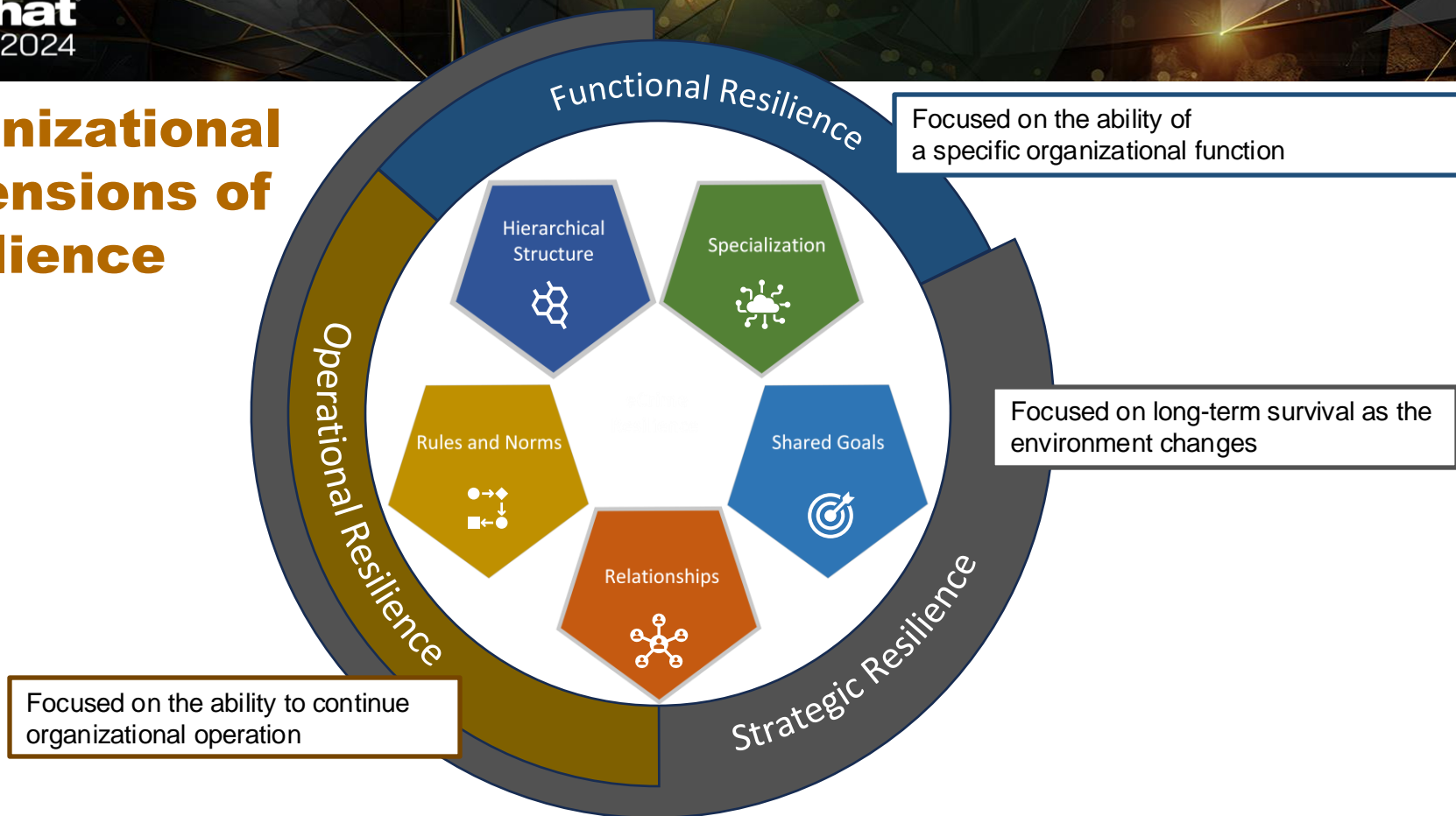


***Cybercrime groups are business organizations.
So, let's study them as such...***

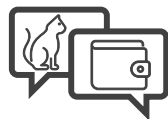
Dimensions of Organization



Organizational Dimensions of Resilience



How can we understand crime forums?



Jargon

Slang and technical jargon
(i.e., wallets, targets, targeting tasks)



Shared culture

Cultural barriers to understanding
(i.e., trust signals, relationships, social norms)



Shared context

Contractual and reciprocity assumptions will not hold
(i.e., alignment of goals, expectations, etc.)

Jargon

Original Text	Translated using Machine Translation	Translated using Human Translation (By Authors)
про битки не забудь, кош выше, я спать)	Don't forget about the bits , kosh above, I'm going to bed)	Don't forget about the bitcoins , the wallet address is above, I'm going to bed [smile]
им декриптор не нужен восстановили-то восстановили но дату свою выливать не хотят	They don't need a decryptor. They restored it, they restored it. but they don't want to spill their date	They don't need a decryptor Though they have restored it [data]... they don't want to release their data
мыло дай	give a soap	give an email
отпишитесь user06 они там уже спамят на мыло и на форму	unsubscribe user06 they are already spamming the email and form there	reply to user06, they are already spamming the email and the [website] form
Вы бы в кску погамали)) Или пабг))	You should play ksku)) Or pabg))	You should play Counter-Strike:GO [two smiles] Or PABG [two smiles]

Understanding an organization requires understanding people; **requires more than simple NLP approach**

Shared Humor Contributes to Resilience and Motivation, but Requires Cultural Context

Analysis of humor requires more than translations:

"Всех с праздником, кибервойска! Нагнем амеров!"

"Happy Holidays, cyber troops! Let's beat the amers!"

correctly translated "beat" should be "bend"

indicates homophobic violence

aligns with a specific domestic political ideology, informs targets selection



Shared Understanding but not aligned goals

English language research may miss illustrative semantics

In response to “*Happy Holidays..*”

“*All who are involved and not. But peace to all of us. Let the bots fight, we have more power over them))*”


Disagrees with the political subtext

Attempting to de-escalate with `))` [hedging]

Threat analysis includes culture and context

Conti Gang statement dated February 25, 2022, in which the group allies itself with the Russian government (Source: Conti.News)

“WARNING”

 The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

 2/25/2022

 39

 0 [0.00 B]

State-supporting (do not confuse with *state-supported*)
State-aligned

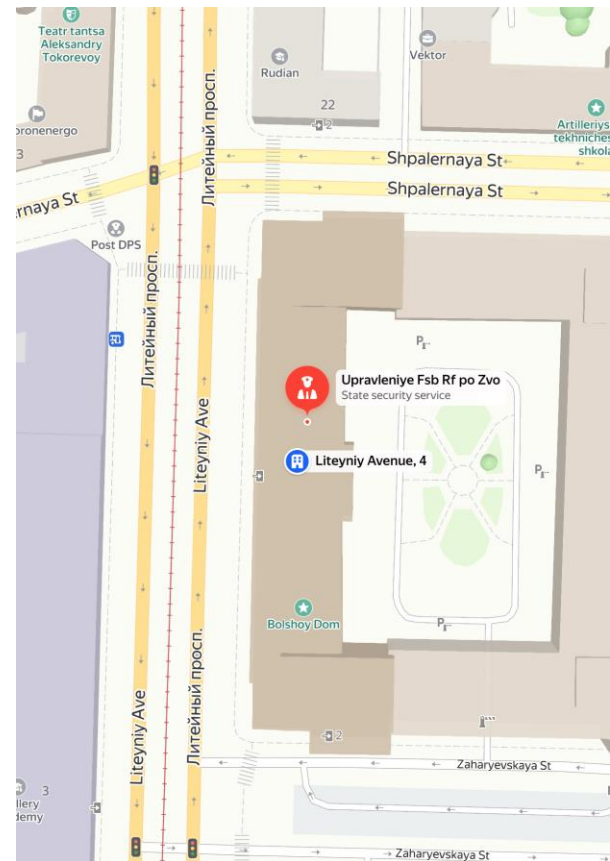
Shared Understanding

A regional expert will quickly notice:

4 Liteyny Avenue corresponds to FSB

discussion includes **journalists**
[Bellingcat] and **Alexei** [Navalny]

D Manatova, L J Camp, J R Fox, S Kuebler, M A Shardakova, I Kouper, “An Argument for Linguistic Expertise in Cyberthreat Analysis: LOLSec in Russian Language eCrime Landscape”, 5th Workshop on Attackers and Cyber-Crime Operations. IEEE European Symposium on Security and Privacy 3 July 2023



How can we understand crime forums?



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.)

Example: SIM Swapping

Connections Across
Different Crimes



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

Observations of forums 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



Online communities are **resilient** and reassemble

eCrime Participants

- Utilize multiple identities
- Build branding tied to such identities
- Choose a nickname according to the identity

I had 3-4 pseudonyms for: 1 – main, as an owner of carder forum, 2 – for my private messages only to my private circle, 3 – for sell dumps, 4 – for sell plastic, 5 – for sell documents

...

It's my way of biz strategy – to sell dumps and recommend to buy plastic and docs from another man who is me...

*from an interview with a former cybercriminal
"Industry of Anonymity" by J Lusthaus*

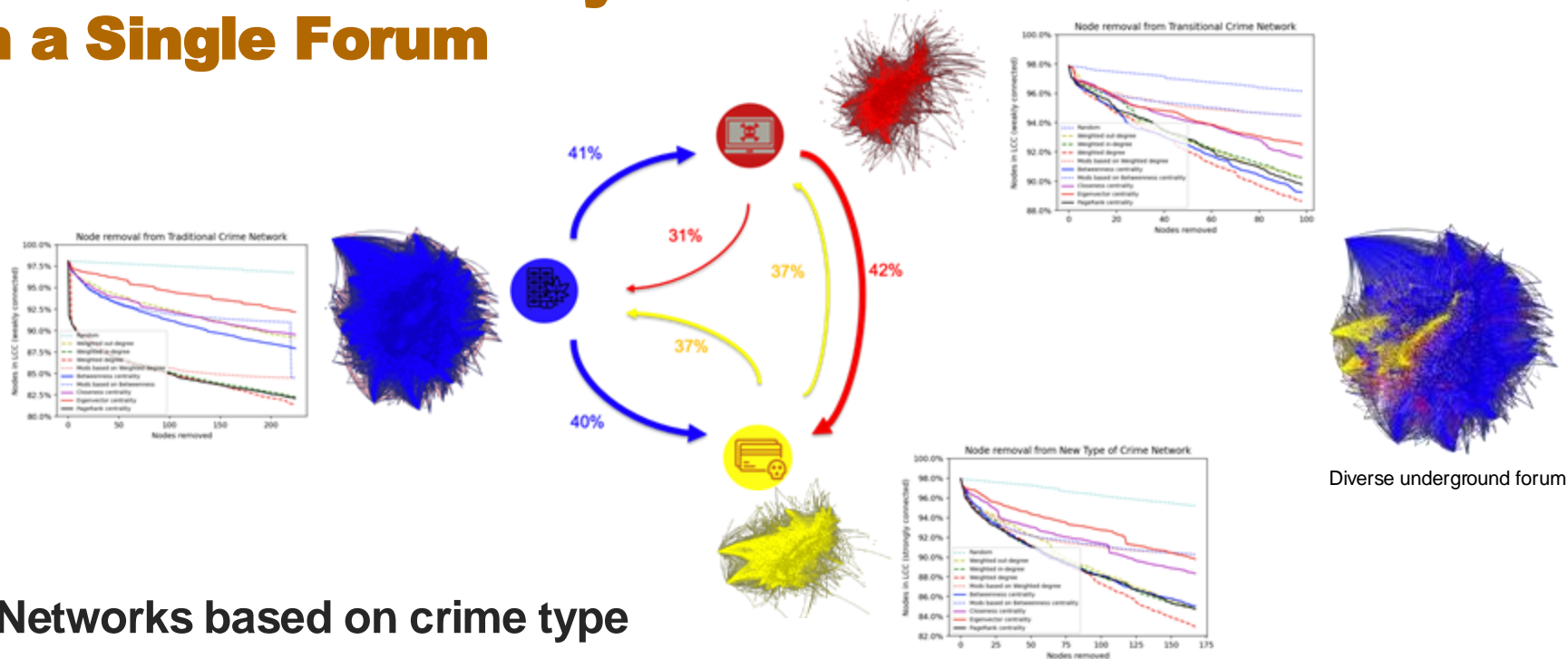


eCrime Participants

- Build trust over repeated interactions
- Signal trust with shared
 - Knowledge background
 - Cultural background
 - Language



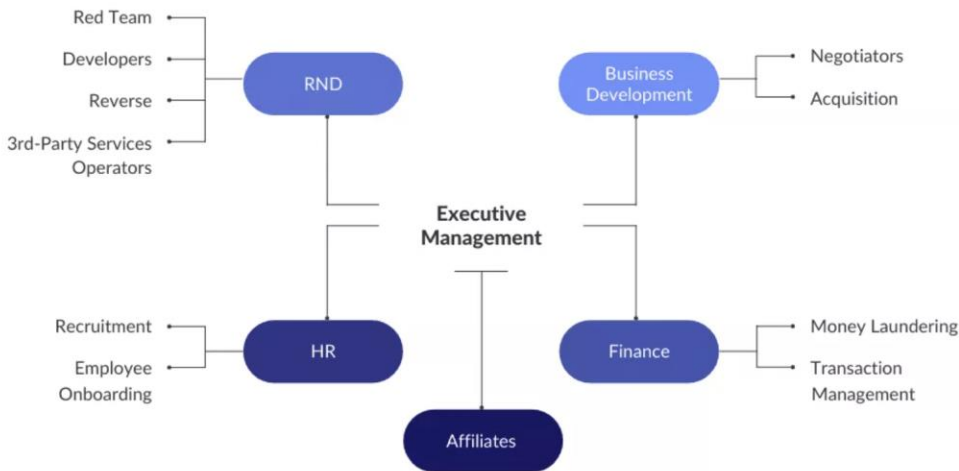
Social Networks Vary Even in a Single Forum



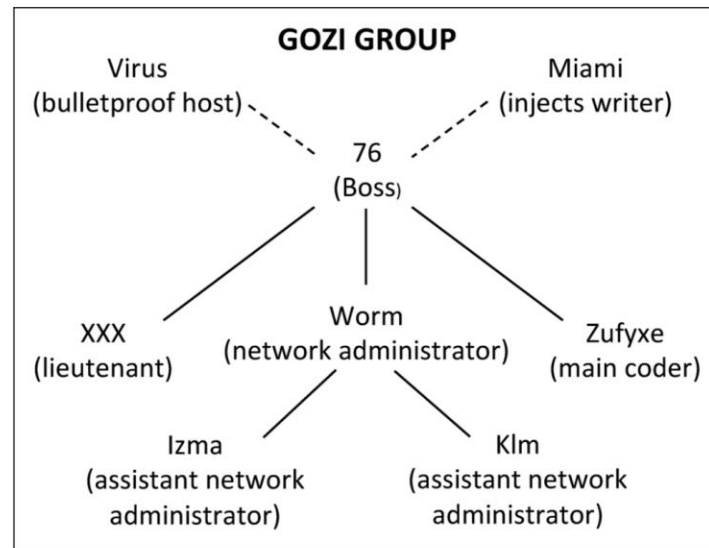
Networks based on crime type

D. Manotova, D. Shama, S. Samtani and L. J. Camp, "Building and Testing a Network of Social Trust in an Underground Forum: Robust Connections and Overlapping Criminal Domains," 2022 APWG Symposium on Electronic Crime Research (eCrime)

Hierarchy & partnership together facilitate resilience

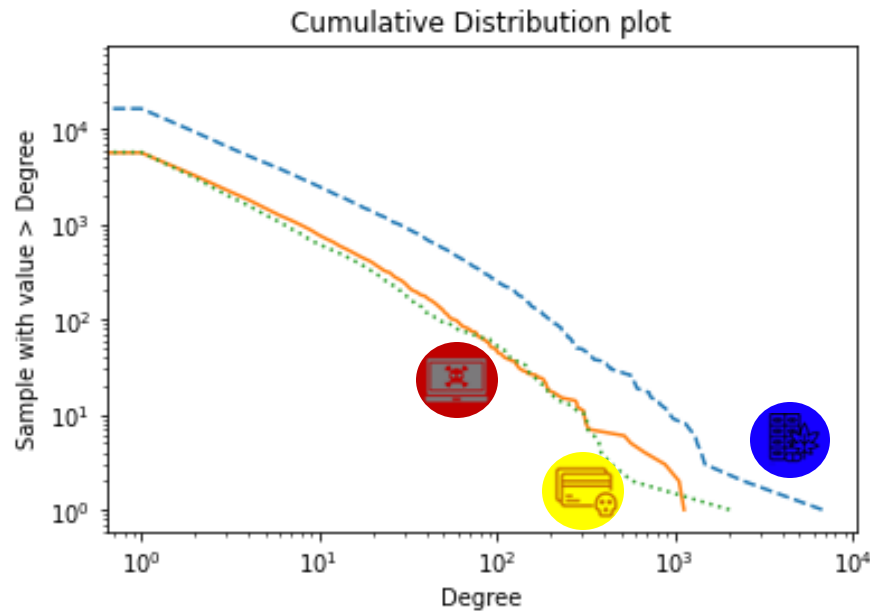


Shmuel Gihon, "To Be CONTInued? Conti Ransomware Heavy Leaks", *Cyberint*

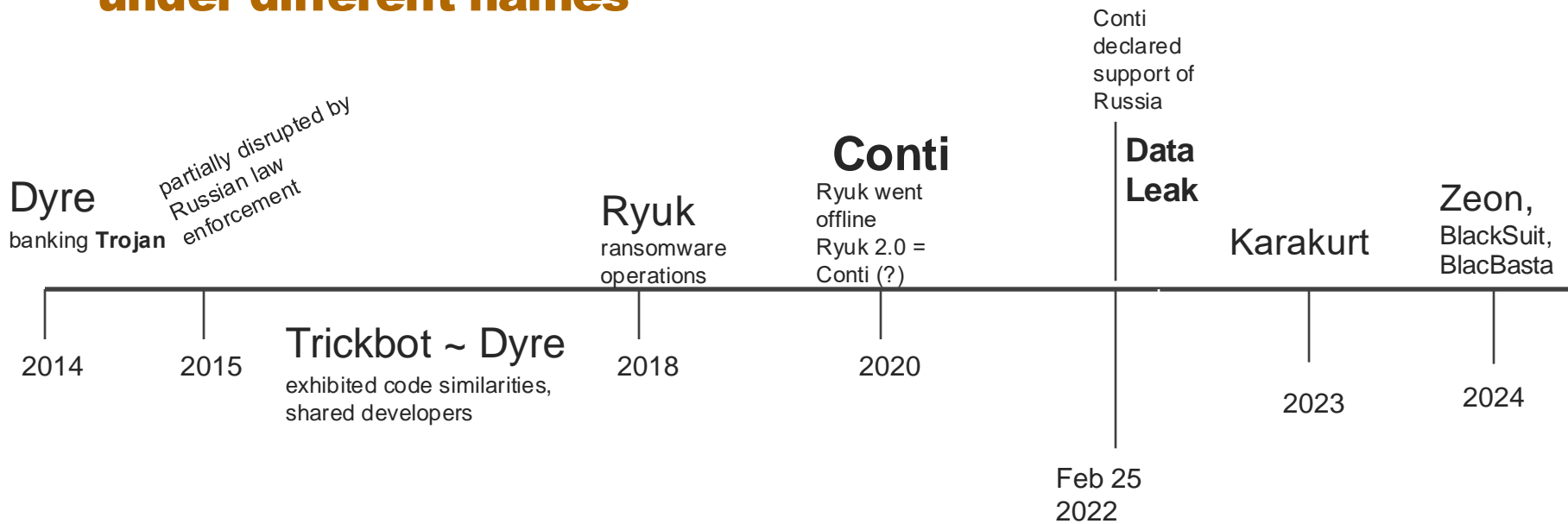


Lusthaus, J., van Oss, J., & Amann, P. (2023). The Gozi group: A criminal firm in cyberspace? *European Journal of Criminology*, 20(5), 1701-1718.

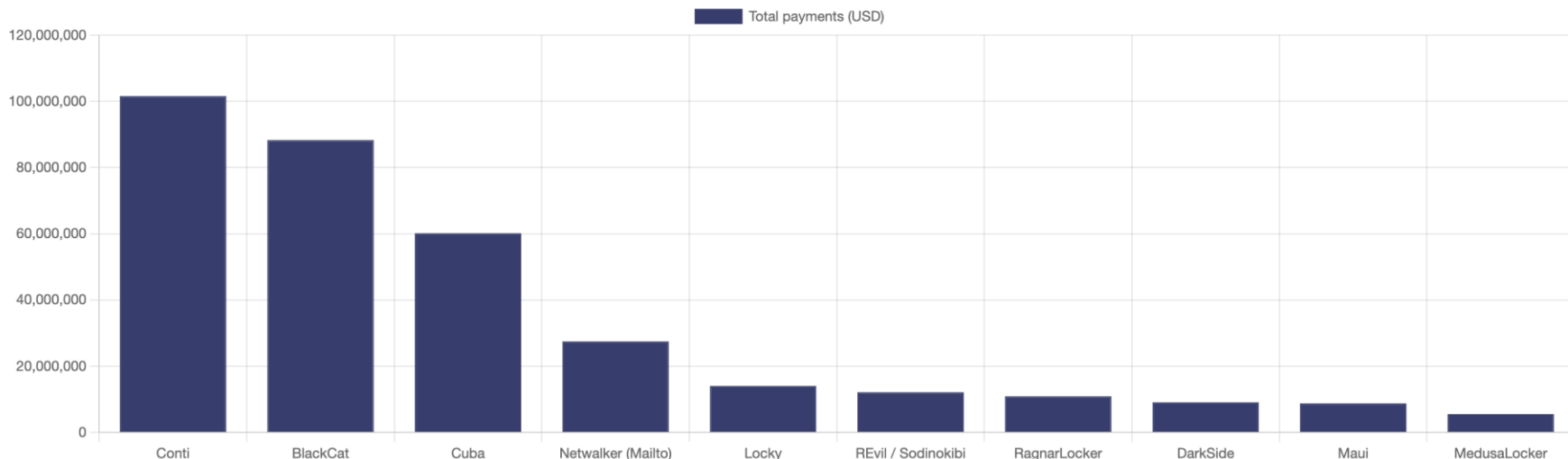
Mature xaaS Yields Scale-free crime networks



Conti has proven a resilient threat under different names



Case Study Conti



Time range: **all time** ▾

Source: ransomwhe.re



One of the major ransomware groups

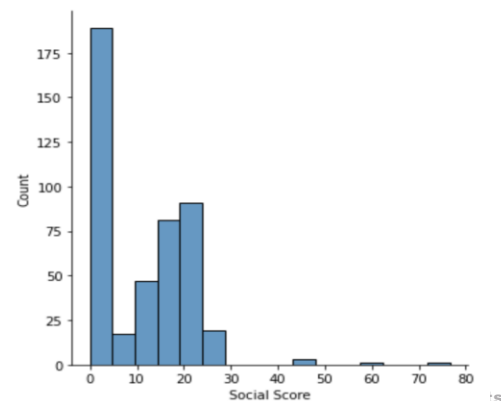
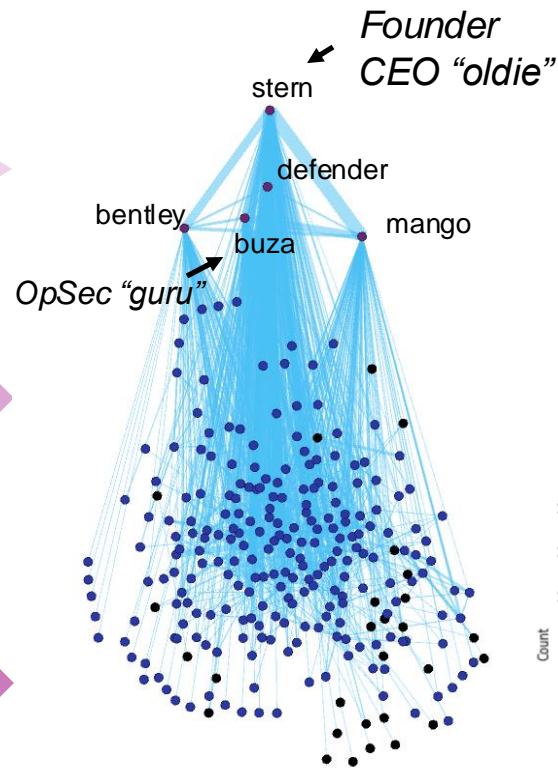
Conti's Social Graph

base on 1-1 messages only

Managers/Leaders are highly connected to many nodes, as they oversee workflows

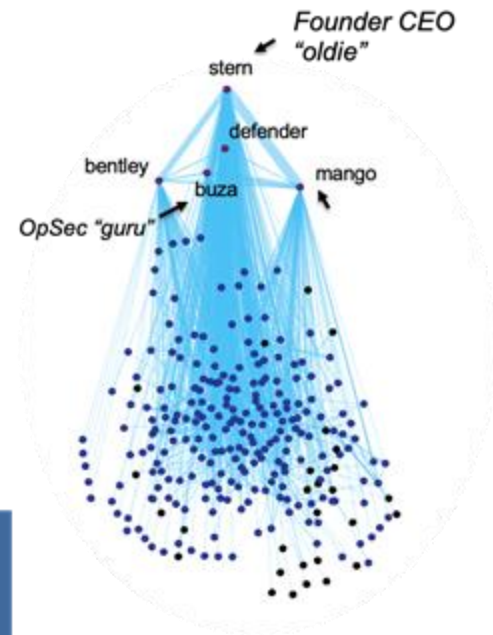
Upper-Level Members have longer lifespans and established positions, ranging from software development to administrative roles

Lower-Level Members have high turnover rate and little connectivity to the rest of the graph, likely contractor positions



Communication Patterns

- Managers/Leaders
 - Are most **active** and **connected** to everyone
 - Are the **bridges** for the group
- Upper Level Members
 - **Cluster** more



Comparison of Stats across Members Levels



Type of Relationships in Organizations

Ibarra's Type	This Study Type	Description
Influence	Authority	Relationships are identified through evidence of a hierarchy of work tasks , including the assignment of tasks, reports on progress or completion, and follow-ups regarding these tasks.
	Mentorship	Relationships are characterized by a request for help or guidance and the provision of advice based on expertise.
Workflow	Workflow Routine	Exchanges based on day-to-day routine or the workflow process
Expressive	Friendship	Relationships are discerned from conversations that diverge from work-related topics , focusing instead on the exchange of personal information, social invitations, or other non-professional interactions

Let's be more rigorous, close to the actual text: Computer-mediated Discourse Analysis

Annotate messages based in Linguistic and Intention analysis

1-1
messages

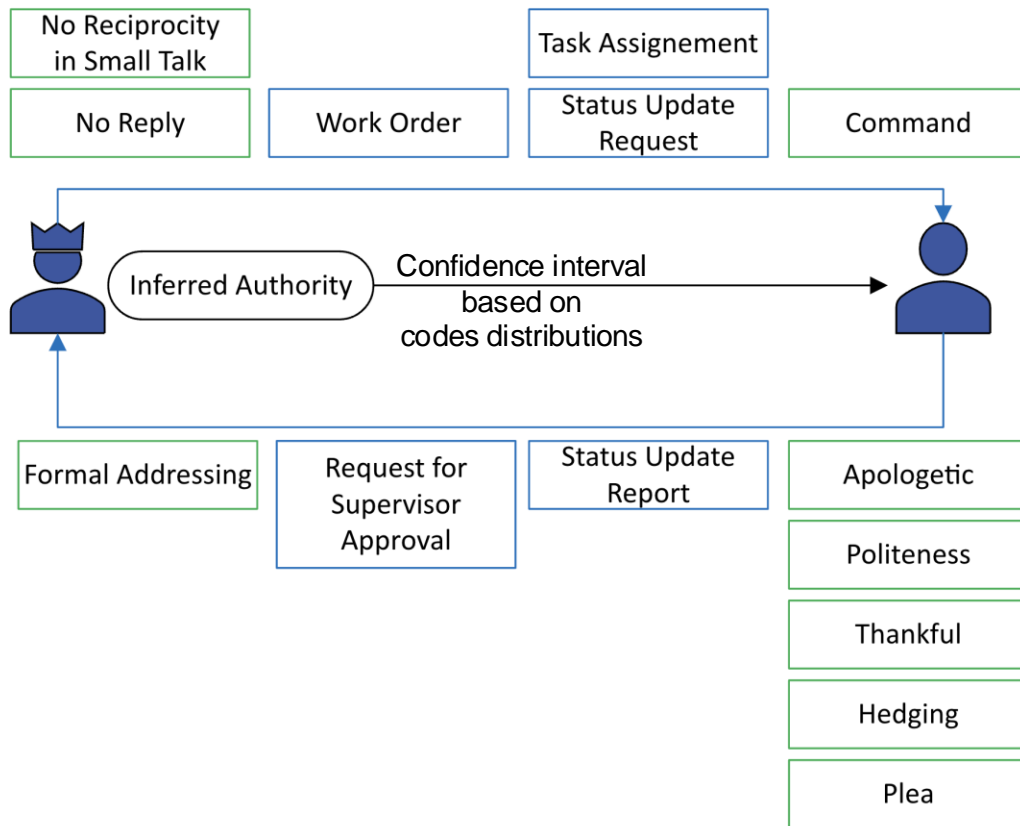
1. Explicit Hierarchy (Formal/Informal Addressing and Relative Roles)
2. Reciprocity (No reply, No reciprocity in Small Talk)
3. Linguistic Markers (e.g., apologetic, command, hedging, politeness, respect)
4. Work Routine
 - Status Update (Request/Report)
 - Task Assignment, Work Order
 - Information Passing
 - ...
5. Non-Work-Related Discussions
 - Sharing opinion
 - Sharing personal information
6. Knowledge and Expertise Sharing
 - Request for help
 - ...



Based on Ibarra's proposed three categories of relationships

1. Authority
2. Work Routine
3. Advice
4. Friendship

Relationship Type: Authority



Example of Authority

Russian	English
<p>stem: Мне надо поднять вторую систему с трик ботом</p> <p>stem: на следующей неделе уже</p> <p>stem: сейчас все закупите</p> <p>stem: только не такую громадную и дорогую</p> <p>stem: чуть поменьше</p>	<p>stem: I need to set up a second system with TrickBot</p> <p>stem: by next week</p> <p>stem: buy everything now</p> <p>stem: just not so huge and expensive</p> <p>stem: a bit smaller</p>
<p>defender: ок</p>	<p>defender: OK</p>
<p>stem: ко вторнику чтобы уже запущена была</p> <p>stem: то есть сейчас надо все начать уже покупать и настраивать</p> <p>stem: и всем отписать чтобы на выходные тоже ставили базы</p>	<p>stem: it should be up and running by Tuesday</p> <p>stem: so now we need to start buying and configuring everything</p> <p>stem: and inform everyone to set up databases over the weekend</p>

Work Order

Work Order
Acceptance

Work Order

Example of Linguistic Markers

Russian	English
---------	---------

baget: Привет!
bentley: Привет
baget: Дружище, на полный прогон бекдор тебе отдавать?
bentley: Да давай.
bentley: У тебя с лоадером?
baget: Да, конечно.
baget: Тебе сбросить исходники или прислать бинарники или как? :-)
baget: Процедурный, так сказать, момент :-)
bentley: Лучше ехю
Мы его криптанем и проверим
baget: ок

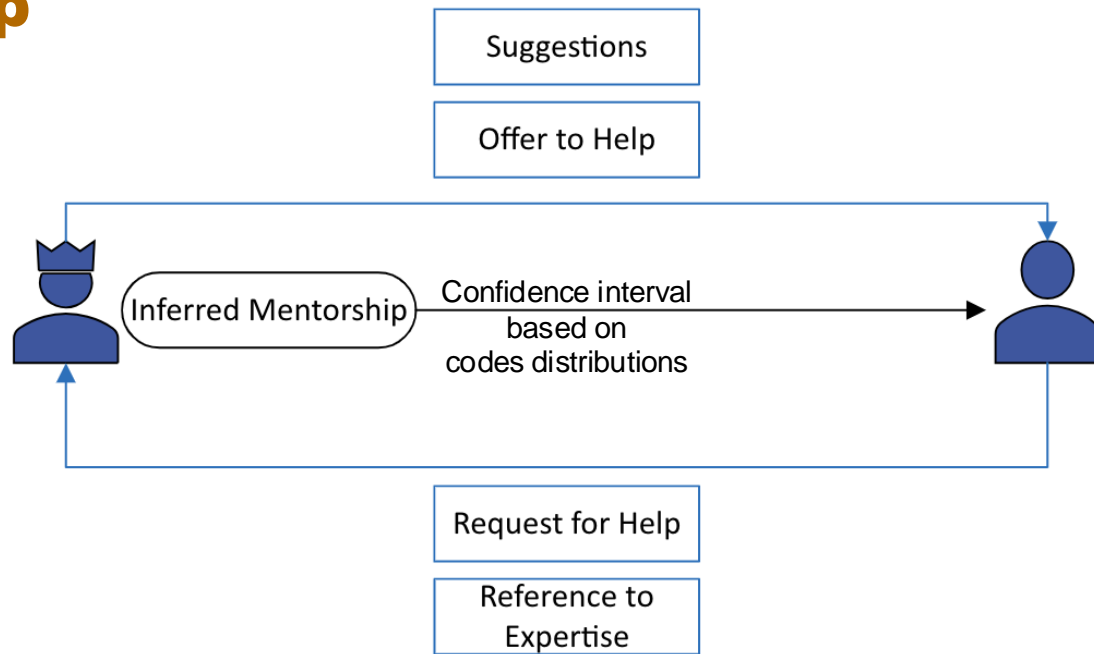
Informal Addressing

Request for Work Order Clarification

Hedging

baget: Hello!
bentley: Hello
baget: Buddy, do you want me to give you the backdoor for a full run?
bentley: Yeah, go ahead.
bentley: Do you have it with the loader?
baget: Yes, of course.
baget: Should I send you the source code or the binaries or what? :-)
baget: It's a procedural matter, so to speak :-)
bentley: Better send the .exe. We'll encrypt it and test it.
baget: OK

Relationship Type: Mentorship



Example of Mentorship Marker

Russian	English
---------	---------

zolotoy: есть по цитриксам у нас кто?))) доступ
закрепить

zolotoy: просто хз кому писать даже, **сори** если не по
адресу

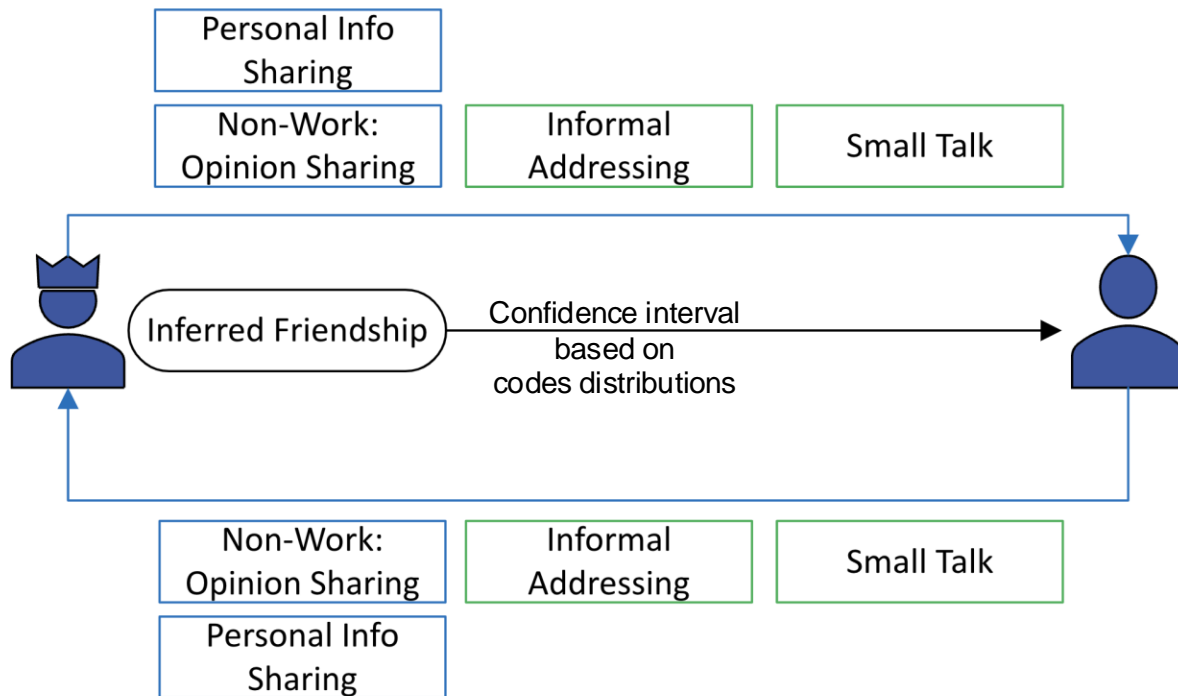
Request for Help

Hedging

zolotoy: Do we have anyone for Citrix?))) Need to secure
access

zolotoy: Just don't know who to write to, **sorry** if you're the
wrong person

Relationship Type: Friendship



Example of Personal Conversations

Russian	English
---------	---------

bentley: Ты не играешь в компьютерные игры?

baget: Играю.

bentley: Вот в какие?

baget: Ну, витчера закрыл, в ассасина греческого прошел.

baget: Шестая цива не в кайф.

baget: Хотя тоже не поленился.

bentley: **О** Я сам в циву люблю

bentley: И Шутаны

bentley: Батл филд 4

Personal Info
Sharing

Excitement

Personal Info
Sharing

bentley: Do you play computer games?

baget: I do.

bentley: Which ones?

baget: Well, I finished The Witcher, completed the Greek Assassin.

baget: Civilization VI is not fun.

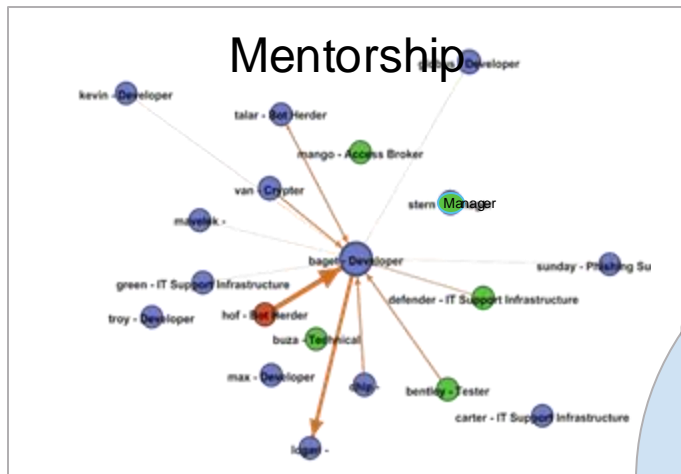
baget: Although I did play it as well.

bentley: **О**, I love Civ myself.

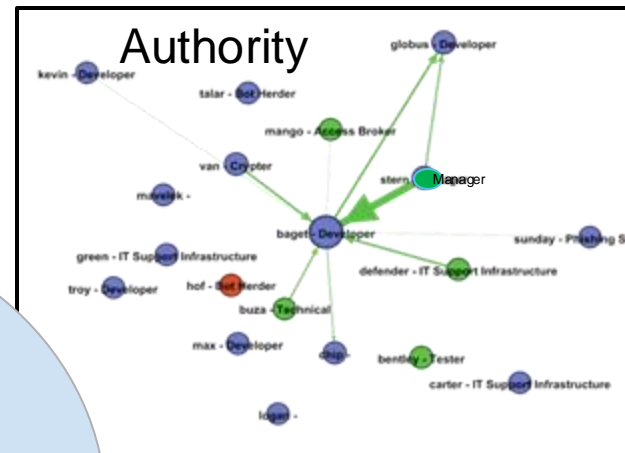
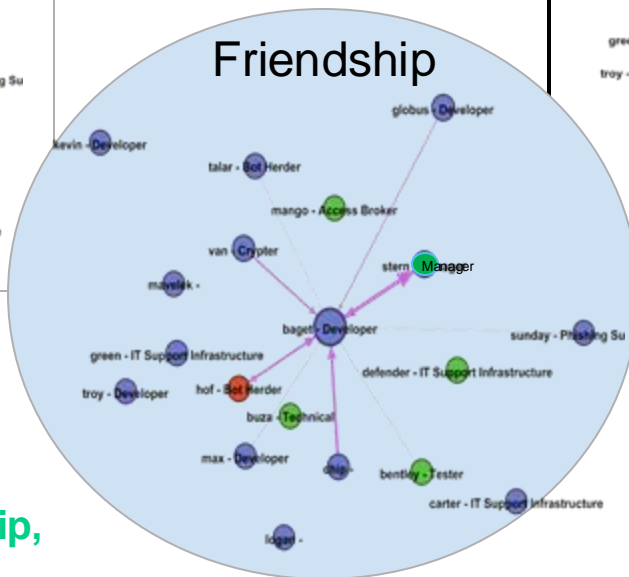
bentley: And shooters.

bentley: Battlefield 4

Initial Social graph of a developer



- Manager/Leader
- Provider
- Specialist



Internal networks built on friendship, mentorship and authority

How can you understand crime forums?



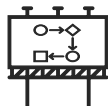
Tasks

Depends on the crime
(i.e., DDoS, ransomware, SIM swapping, etc.)



Roles

Depends on the crime and the organization
(i.e., scope, target size, specialization, etc.)



Workflow

Depends on the crime, organization, and context
(i.e., money laundering, access point, scale, deterrence risk, resilience or lifetime of organization, etc.)

Victim "support"



CONTI Recovery service

Hello, this is ContiLocker Team.
Please, introduce yourself (Company name and your position) and we'll provide all necessary information.
Sometimes our staff is busy, but we will reply as soon as possible.
Be in touch, thank you. 4 days ago

hello 4 days ago

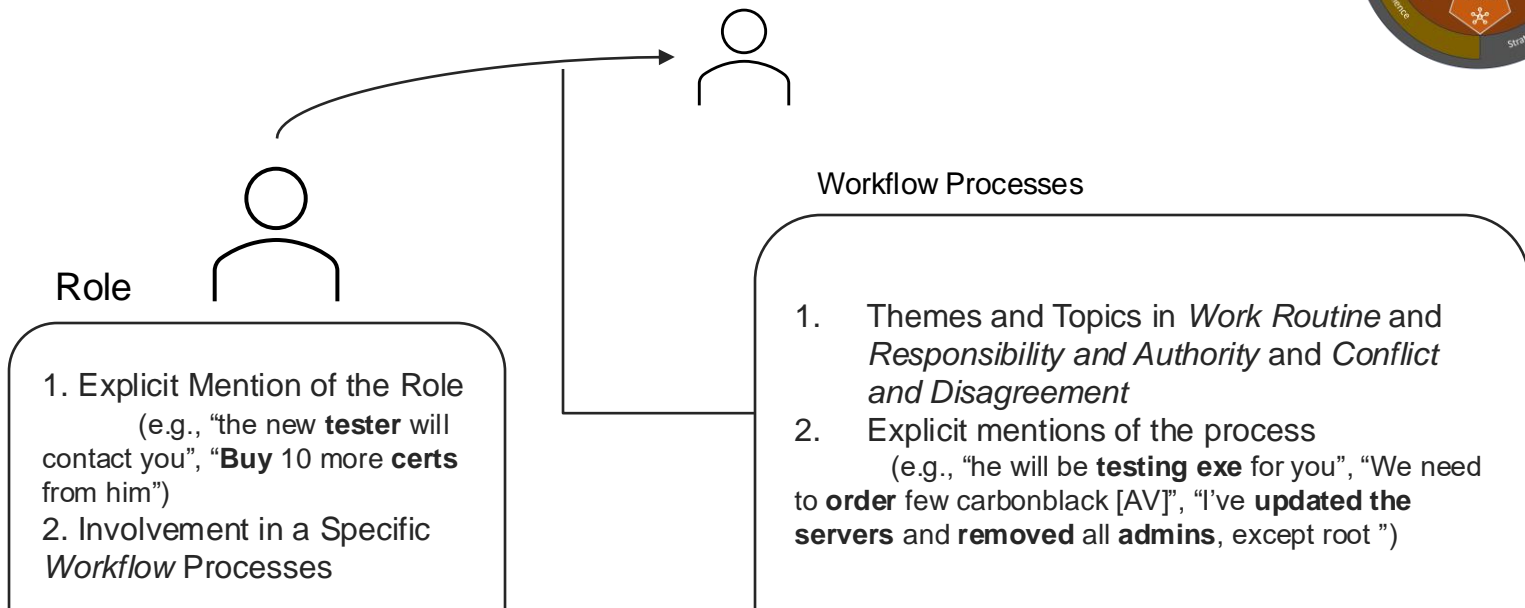
my machine isn't working and i was asked to contact you in a file 4 days ago

can you help? 4 days ago

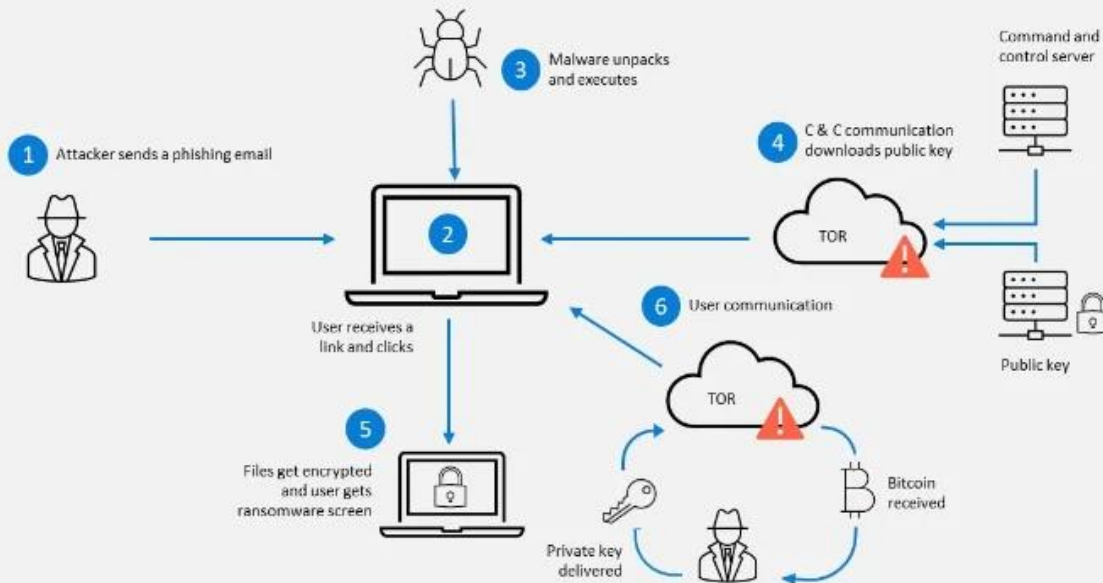
As you already know, we infiltrated your network and stayed in it for more than 2 weeks(enough to study all your documentation), encrypted your file servers, sql servers, downloaded all important information with a total weight of more than 700 GB: personal data of patients(home addresses, phone numbers of the contract), employees (home addresses, employment contracts, scans of personal documents, phone numbers), contracts, customer bases, consolidated financial statements, payroll, settlements with partners, bank statements.
The good news is that we are businessmen. We want to receive ransom for everything that needs to be kept secret, and don't want to ruin your business
The amount at which we are ready to meet you and keep everything as collateral is \$ 19,999,000. 4 days ago

how do i know you have any data? 4 days ago

Specialization: Roles and Workflow

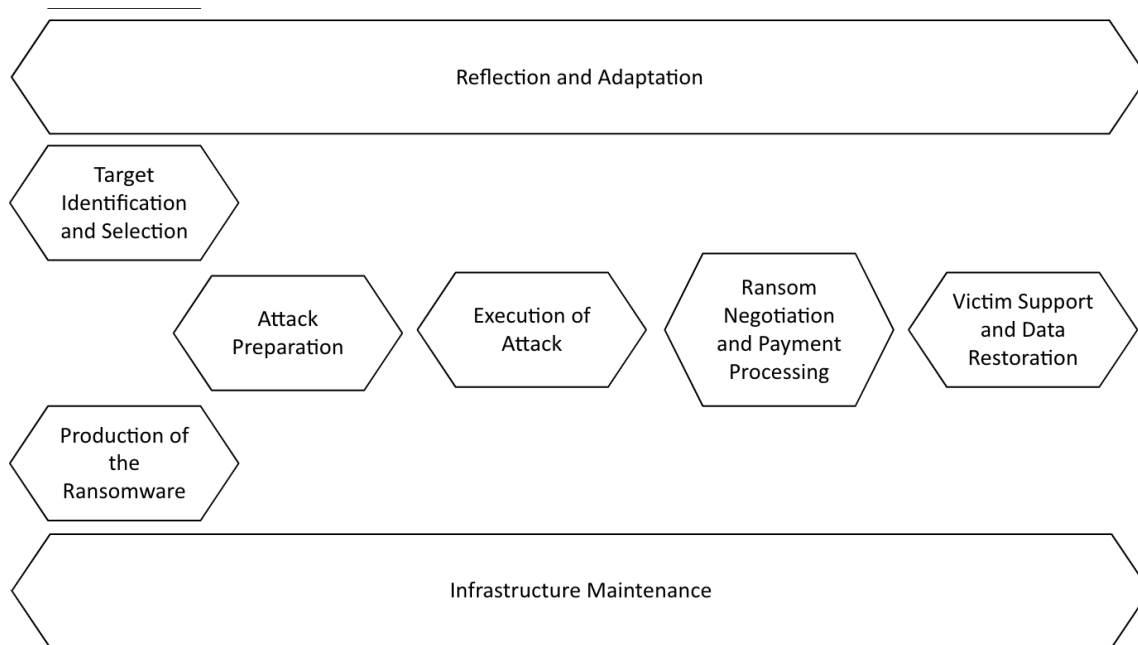


Anatomy of a Ransomware Attack



Source: Proserveit.com

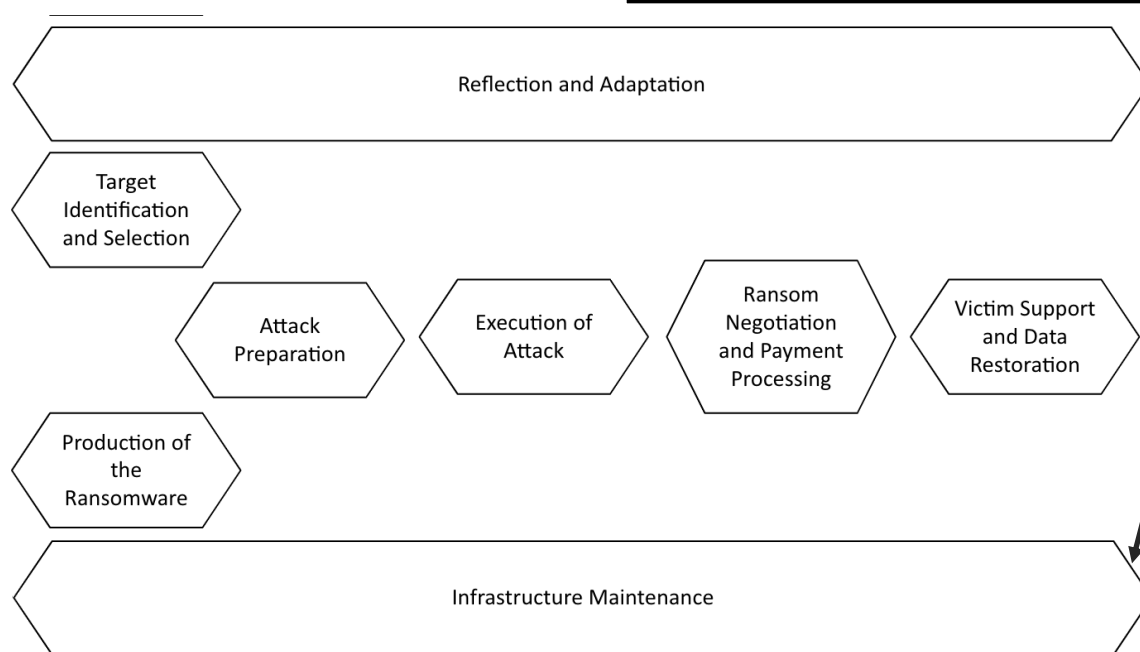
Production Break Down



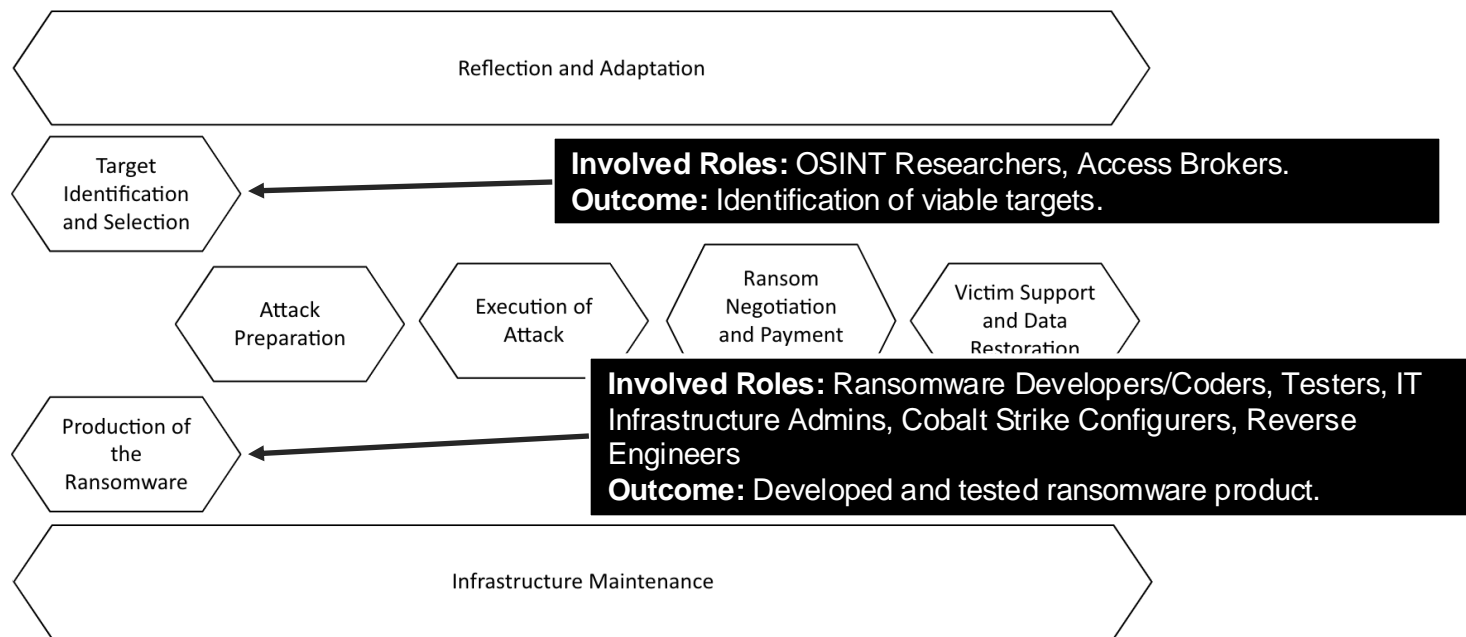
Boring Jobs

Involved Roles: IT Infrastructure Admins, Backend Developers, Group Administrators

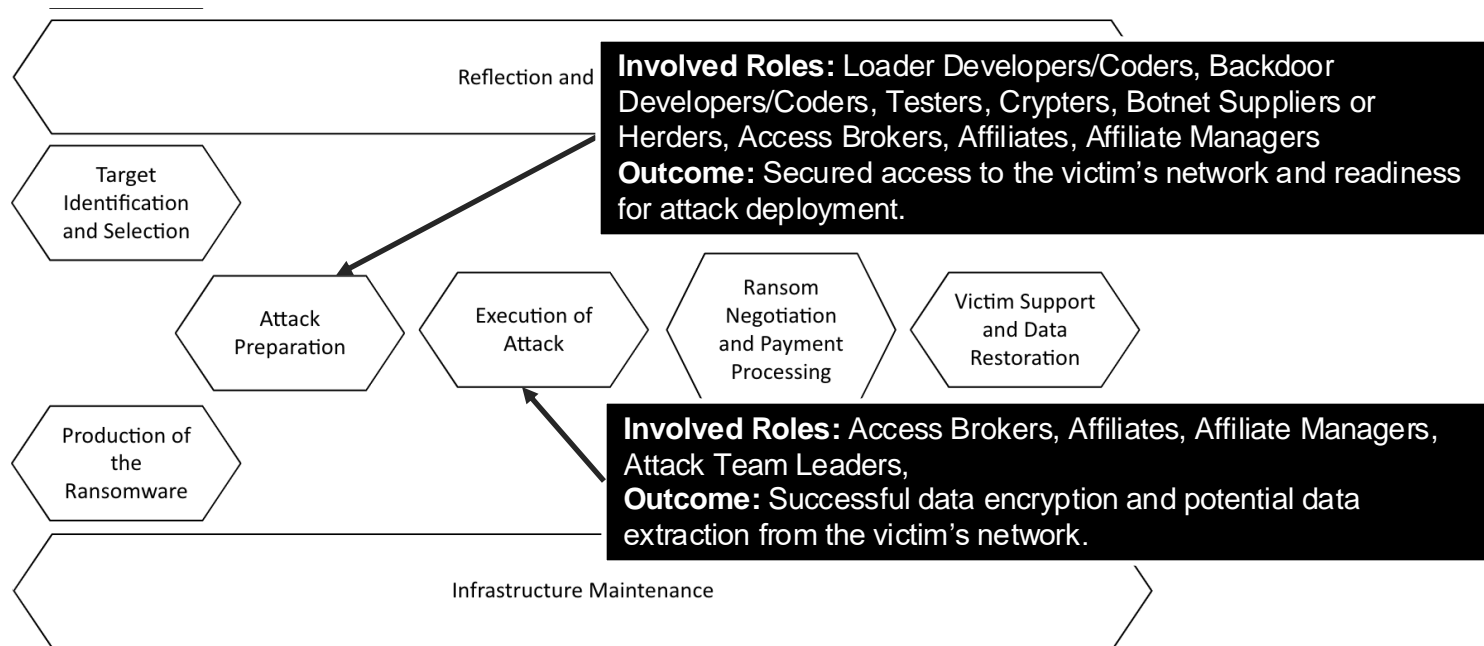
Outcome: Functionality of the group's technical infrastructure.



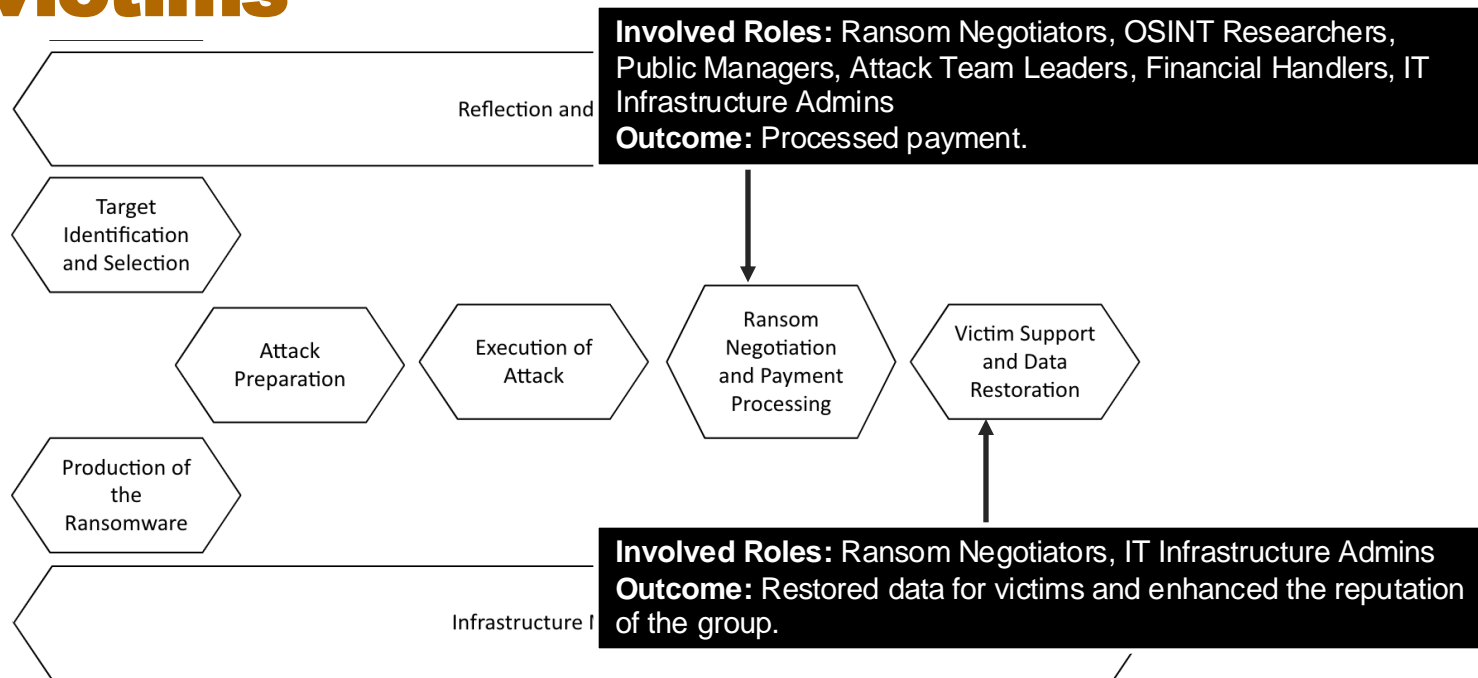
Research & Homework



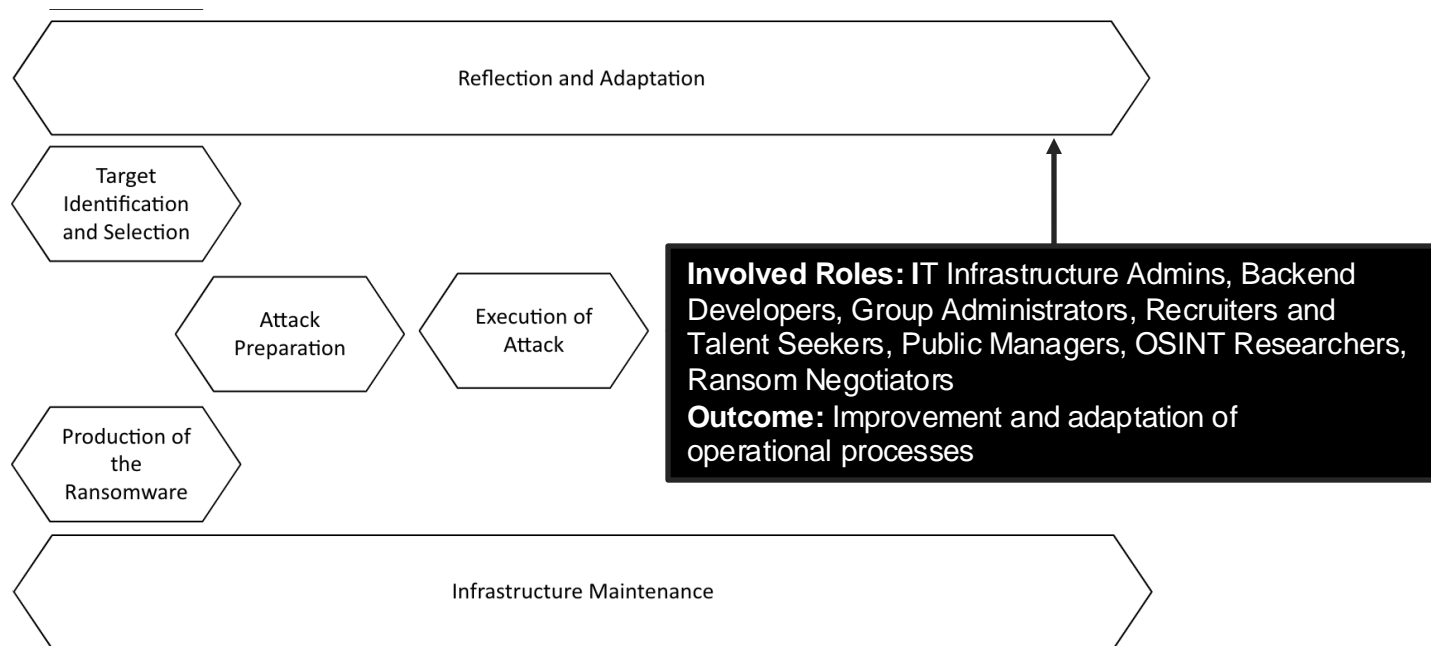
Preparations and the Action



Support your victims



Learn from mistakes



With an understanding of crime forums.



Threats

*To operations and to data
(i.e., understand your value to an attacker)*



Risks

*Differ for different industries and operations
(i.e., C, I, or A?)*



Reevaluate

*Business decisions can change your risk profile
(i.e., new markets, new clients, and new locations of operation, etc.)*

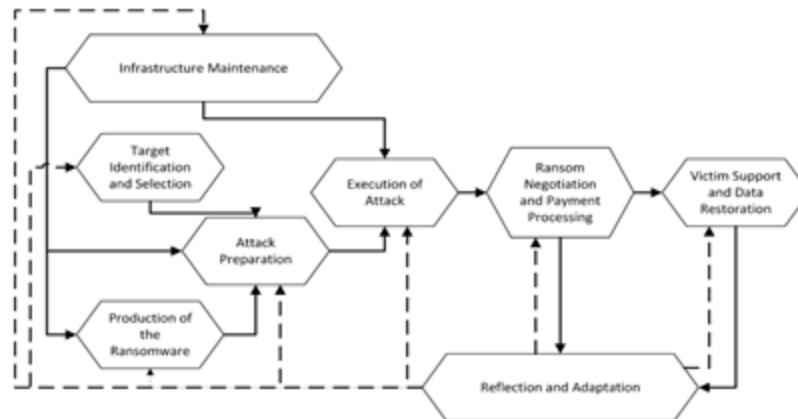
What Is Your Threat?

What tasks have to occur for you to be subverted?

What makes you an (un)attractive target?

What communities are you associated with?

From targeted, "Who is talking about you?" to threat analysis as business analysis



What Are Your Risks?

Ransomware or disclosure of stolen data?

Compliance, reputation, or operational continuity?

What decreases your value as a target?

What are your Options?

Forum monitoring

- which forums, what language, which threats, what purpose?
- what are complements?

Insurance

- against which threats?
- what is your risk pool?

Closing

eCrime organizations are businesses

Understand driving organizational characteristics of eCrime

eCrime organizations are part of the business landscape

eCrime organizations evolve as competitive, resilient organizations as part of the global eCrime industry

Thank you!

dmanato@iu.edu

ljean@ljean.com



INDIANA UNIVERSITY BLOOMINGTON

References

Dalyapraz Manatova, Cathleen McGrath, **L Jean Camp** “A Resilience Model of Organized eCrime Communities” [Under Review]

Dalyapraz Manatova, Cathleen McGrath, Inna Kouper, **L Jean Camp** “Relationships Matter: Reconstructing the Organizational Structure of a Ransomware Syndicate ” [Work in Progress]

Dalyapraz Manatova, Dewesha Sharma, Sagar Samtani, **L Jean Camp** “Building and Testing a Network of Social Trust in an Underground Forum: Robust Connections and Overlapping Criminal Domains”, *2023 APWG eCrime Symposium*

Dalyapraz Manatova, **L Jean Camp**, Julia R Fox, Sandra Kuebler, Maria A Shardakova, Inna Kouper, “An Argument for Linguistic Expertise in Cyberthreat Analysis: LOLSec in Russian Language eCrime Landscape”, 5th Workshop on Attackers and Cyber-Crime Operations. *IEEE European Symposium on Security and Privacy Workshop 2023*

Dalyapraz Manatova “Understanding Cybercriminal Group Dynamics: An Analysis of Conti Using IAD Framework”, Talk at Workshop on Ostrom Research Seminar, 11 December 2023 (Bloomington, IN)

Nadia Sabry, **Dalyapraz Manatova**, **L Jean Camp** “Uncovering the Organizational Hierarchy of a Cybercriminal Group”, Poster Session at *Luddy School of Informatics, Computing, and Engineering 2023*

Maksat Sharshkeev, **Dalyapraz Manatova**, **L Jean Camp** “Social Network of a Hacker”, Poster Session at *Luddy School of Informatics, Computing, and Engineering 2023*

Dalyapraz Manatova, Charles DeVries, Sagar Samtani, Understand Your Shady Neighborhood: An Approach for Investigating Hacker Forum Communities, *Decision Support Systems, 2024*

