
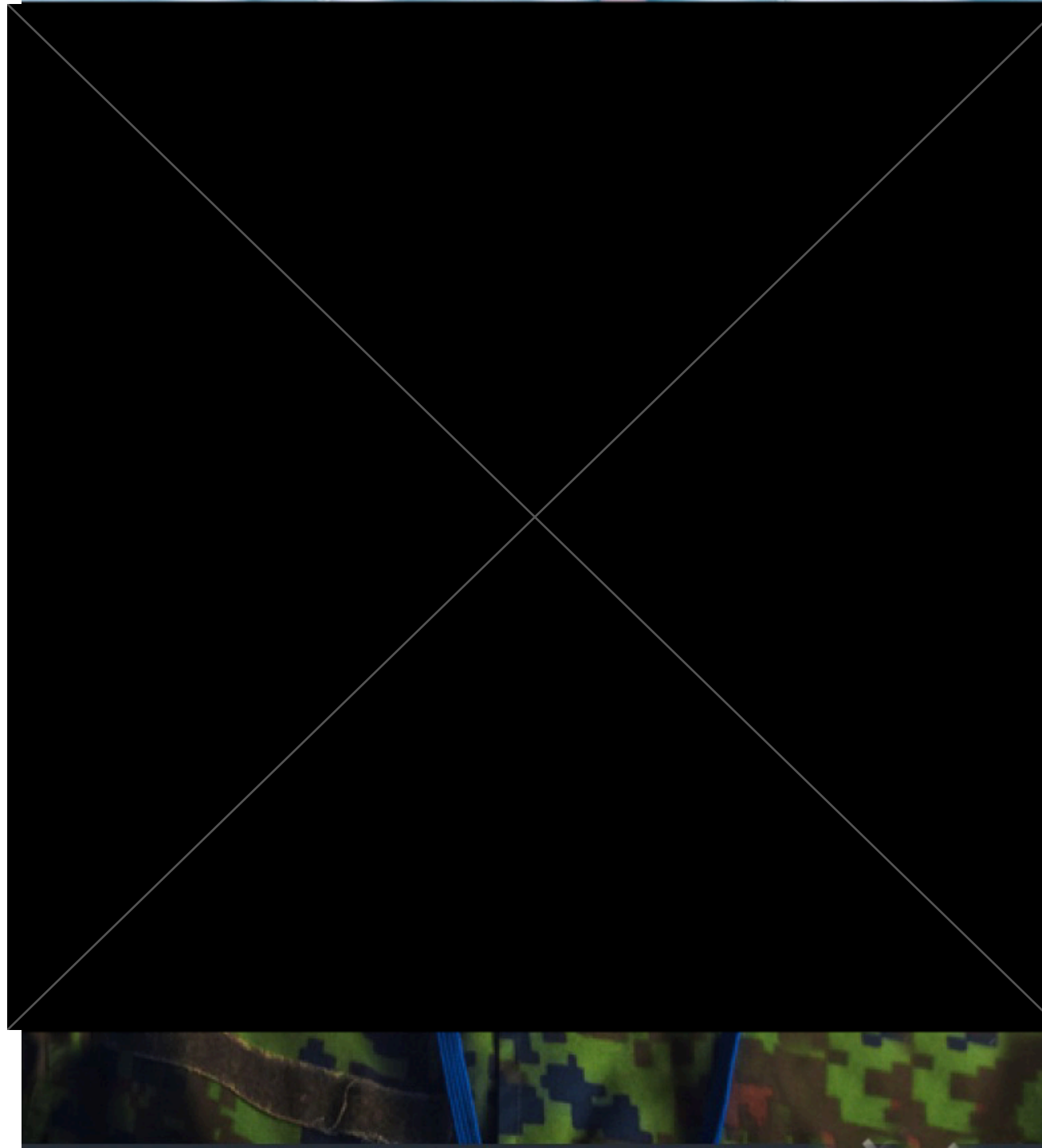


# Hoodies & Hoodlums


A Match Made in (Heaven | Hell)?

## But first ..

- 
- Complex, multi-faceted topic
  - Criminology, sociology, economics, geopolitics, ..
- I'm *not* law enforcement
  - I'm already sorry for causing physical pain



## But first ..

- 
- Complex, multi-faceted topic
  - Criminology, sociology, economics, geopolitics, ..
- I'm *not* law enforcement
  - I'm already sorry for causing physical pain



## A long road to the silk road

- "Silk Road" was the first modern "Darknet Market"
  - Marihuana via ARPANET (1970!)
  - Proto-Silkroad: The Farmer's Market (2006)
- Beginning media attention:
  - "Drug dealers are using the Internet!1!!"
  - "The Mafia uses the Internet!1 1!!"
  - "The Mafia is taking over cybercrime!1 1"

[TLP:AMBER]

**"The Russian Mafia are the most prolific cybercriminals in the world."**

[TLP:AMBER]

## ~~Organized~~ Controlled Crime

- "Group that seeks to control a local criminal market"
  - "What is Organized Crime?" - Federico Varese, 2010/2017
- "Organised" means "Controlled"
  - "What Is the Business of Organized Crime?" - Thomas C. Schelling, 1971
- Governance is a deciding factor

## Cybercrime is a criminal market

- Similarities to "analog" crime
  - Products (Drugs / Malware), services (Targeted theft / DDoS)
  - Structures of varying levels of organization
- Differences to "analog" crime
  - Few to no local context in the typical sense
  - Usually little overlap in the core business of either

## Taking over? Yeah, no.

- No local context makes governance hard
  - Disclaimer: There are a few exceptions
- Little incentive for organised crime to attempt to take over
  - Missing "locality" makes control more difficult
- A lot of incentives for cybercrime to stay clear
  - Violence isn't exactly a pull factor



## Working together? Yeah.

- Transaction-based cooperation often times makes sense
- Both sides offer services that can be helpful
  - Enabling services, e.g. money muling
  - Supporting services, e.g. "hacking for hire"

**How does that look in practice?**

[TLP:AMBER]

I: Drugs, but like .. differently!

[TLP:AMBER]



## 2021 wasn't a good year for organised crime

- March: Raids and arrests in multiple countries, especially BE and NL
- Confiscation of close to 20 tons of cocaine, several millions in cash and assets
- Second time in less than a year where criminals were hit in unexpected ways

## Sky ECC aka "NoThInG iS mOrE sEcUrE"

- Encrypted communication based on modified smartphones
  - 6.000 customers in BE, 12.000 in NL
  - Around half of the BE-devices were used in the vicinity of the Antwerp port
- Around 1 **billion** messages, half of them decrypted

[TLP:AMBER]

7MIOBC  
[She] also asked me how long the USB be plugged in

De Valk:  
1 min

7MIOBC  
And after that you can access that pc we that we infected or multiple pc's

De Valk:  
I have to start there and then I will map the network. Then I have to find the main server there and get all the admin passwords. those passwords are hashed, I have to decrypt them with amazon cloud. can take up to a week



[TLP:AMBER]

7MIOBC  
okay what's the next step

De Valk:  
then they can pick up the stick from me

De Valk:  
alright I will make it tomorrow it will be ready the day after tomorrow i will put the windows on my system.

De Valk:  
put it and test it so it works.

De Valk:  
once I have admin password then I give myself system privileges and then I delete logs

De Valk:  
as long as I don't do anything they won't see anything

De Valk:  
crazy

De Valk:  
don't worry I have been doing this for many years

## "Hackers" hacking .. port terminals

- Utmost basic level of technical complexity
  - Off-the-shelf malware, mostly via thumbdrive
- Enabling the offering of criminal services
  - Support with avoiding customs inspections
  - Theft of container PIN
  - "Full container service"

## Criminal symbiosis

- Massive simplification for smugglers
  - No need for local help
- Low-effort income for cybercriminals
  - One successful run? 500.000 Euros



## Challenges

- 2022: 160 tons of confiscated cocaine in Rotterdam alone
  - Amount of containers inspected? Far below 5%
- Modern ports are designed for efficiency, not security
  - Which seems to apply to the IT environment as well ..
- Even minimal undermining hurts

[TLP:AMBER]

Drug\* oxyCODONE 10 mg tablet

Favorites ▾

Add drug to favorites
  Advanced search

[Dosage Calculator](#)

Pt. Instructions\* 1 tab(s) orally 3 times a day as needed



# III: Drugs, but I swear it's different!

Quantity\* 30 ▾ tablet

Refill 0 ▾ Effective On MM/DD/YYYY  Allow Substitution

Days supply 14

Reason For Rx Enter ICD-10 code or name

Pharmacy\* CVS/pharmacy, [Redacted] ▾

Pharmacy Notes (will not appear on patient prescription)

Instructions for pharmacy related to, but NOT part of SIG

210 characters remaining

Warnings

NO SIGNIFICANT IN

No significant intera

[TLP:AMBER]

## Prescription fraud

- Primarily in the USA, Canada
  - First, so far isolated cases in DE, maybe NL and CZ
- Professionalization akin to Ransomware
  - Access through access brokers
  - Fraudulent issuing of valid prescriptions
  - Street level dealing by established perpetrators

## Criminal symbiosis

- Simplification for dealers
  - No reliance on potentially shaky helpers
- Simple, easy income for cybercriminals
  - Different ballgame than retail drug smuggling, but still good
- Minimizing risks for both sides

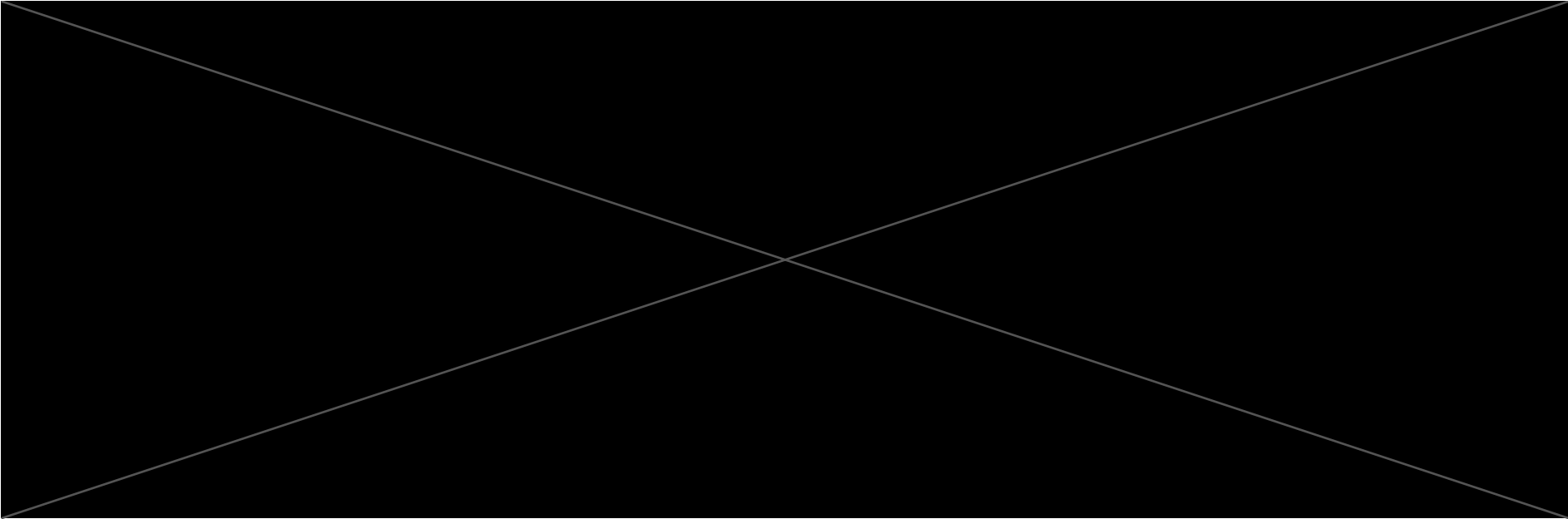
## Challenges

- Pharmacies are barely able to detect the fraud
  - Fun fact: "Too legible handwriting" used to be an indication for fraud
- Law enforcement loses important information
  - A plethora of digital systems makes investigations more challenging
  - The chances of an "insider" struggling with their consciousness decreases

## III: Theft



[TLP:RED]



[TLP:RED]

- [REDACTED] has a security incident
  - Incident is handled by MSP
- Attackers not following "the script"
  - [REDACTED]
  - "[REDACTED]"
- A few weeks later: Significant theft [REDACTED]
  - Perpetrators [REDACTED]



## **(Probably / Obviously) just the tip of the iceberg**

- Money laundering
- (RUMINT) Car theft
- There's (much) more:
  - Cooperation between cybercrime, organised crime, state entities

## TL;DR

- Cooperation between cybercrime and organised crime not just drug-related
- Media coverage about this often lurid and of questionable nature
- The "takeover" of cybercrime by "the mafia" is a boogeyman
  - However: Intensified case-by-case cooperation
- IT-security tends to not be included in "offline" threat assessments - big mistake!

# Thank you for your attention

- [REDACTED]
- [REDACTED]
- [REDACTED]

[TLP:AMBER]

# Questions?

[TLP:AMBER]