Organisierte Kriminalität 🤝 Cybercrime

Alexander Riepl, 13.03.2024

But first ..

- Komplexes, “unterforschtes" Themengebiet
  - Kriminologie, Soziologie, Ökonomie, Geopolitik, Technik, ..
- Diamanten entstehen unter Druck!
  - Etwaige Stilblüten und Holprigkeiten? Gewollt!
  - Eigenwilliger Vortragsstil? Ebenfalls!

Der lange Weg zur Seidenstrasse

- “Silk Road” war der erste moderne “Darknet Market”
  - Gras via ARPANET (1970!)
  - Proto-Silkroad: The Farmer’s Market (2006)
- Gleichzeitig: Beginnende mediale Aufmerksamkeit für das Thema
  - “Drogendealer verwenden das Internet!11!”
  - “Die Mafia verwendet das Internet!1!!1!”
  - “Die Mafia übernimmt Cybercrime!11!”



“The Russian Mafia are the most prolific cybercriminals in the world.”

Dutzende Medienbeiträge, auf die ein oder andere Art und Weise

~~Organisierte~~ Kontrollierte Kriminalität?

- "Gruppe, die einen lokalen kriminellen Markt kontrollieren will”
  - “What is Organized Crime?” - Federico Varese, 2010 / 2017
- "Organisiert" heisst “Kontrolliert”
  - "What Is the Business of Organized Crime?" - Thomas C. Schelling, 1971
- “Governance" ist der entscheidende Faktor
- Mafia ist (in der Theorie) eine Gruppe, die alle kriminellen Märkte kontrollieren will

Cybercrime ist ein krimineller Markt

- Ähnlichkeiten zur analogen Kriminalität
  - Produkte (Drogen / Malware), Dienstleistungen (Auftragsdiebstahl / DDoS)
  - Strukturen verschiedener Organisationsgrade
- Unterschiede zur analogen Kriminalität
  - Wenig lokale Bindung im klassischen Sinn
  - Typischerweise wenige Überschneidungen des Kerngeschäftes

Übernahme? Yeah, no.

Zusammenarbeit? Yeah.

- Wenig Anreiz für organisierte Kriminalität, eine Übernahme zu versuchen
  - Fehlende “Lokalität" erschwert Kontrolle
- Viele Anreize für Cyberkriminelle, nicht in klassische OK-Strukturen “abzurutschen"
  - Gewalt ist jetzt nicht so der “Pull-Faktor” ..
- Dennoch: Eine transaktionelle Zusammenarbeit macht oftmals Sinn

Aber wie?

- Organisierte Kriminalität
  - Ermöglichende Dienstleistungen (z.B. “Money Muling”)
- Cybercrime:
  - Unterstützende Dienstleistungen (“Hacking for hire”)
- Ausnahmebeispiele: Schutz von Cyberkriminellen, finanzielle Investitionen in Cybercrime

Wie sieht das in der Praxis aus?

I: Drogen (.. aber anders!)



2020 war kein gutes Jahr

(Und das ganz ohne Corona)

- Behörden in Costa Rica konfiszieren knapp 4 Tonnen Kokain - Ziel: Europa, Rotterdam
- Ermittlungen vor Ort, aber auch in Europa - insbesondere Holland
- Unbekannte Täter:innen - keine konkrete Hinweise auf die Drahtzieher:innen

2021 wurde nicht besser

Auch ohne Corona

- März: Hausdurchsuchungen und Festnahmen in mehreren Ländern
- Beschlagnahmung von knapp 20 Tonnen Kokain, mehrere Millionen Euro
- Ermittlungserfolge auch in Bezug auf die Beschlagnahmung in Costa Rica

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

De Valk:
1 min

7MIOBC
And afterthat 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

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

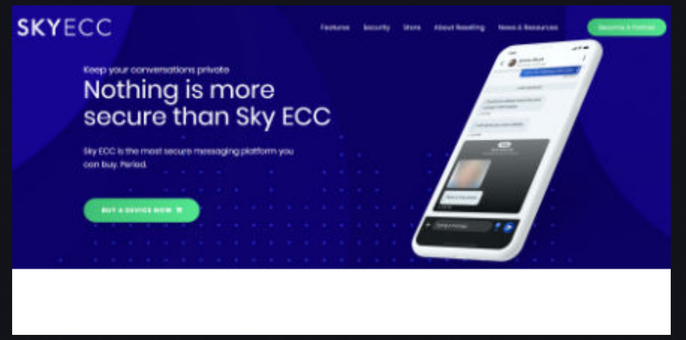
De Valk:
as long as I don't do anything they won't see anything

De Valk:
crazy

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

Sky ECC

NoThInG iS MoRe SeCuRe



- Verschlüsselte Kommunikation auf Basis modifizierter Smartphones
- 6.000 Kund:innen in Belgien, 12.000 in den Niederlanden
  - Hälfte der belgischen Geräte wurden im Hafen von Antwerpen genutzt
- Behörden hatten mehrere Wochen Zugriff auf Kommunikation
  - Knapp 1 **Billion** Nachrichten, die Hälfte davon entschlüsselt

“Hacker" hacken .. Hafenterminals

- Technisch (fast schon lächerlich) rudimentäre Angriffe
  - Malware von der Stange, (meist) via USB-Stick
- Vielzahl von kriminellen Dienstleistungen
  - Empfehlungen zur Vermeidung von Zollkontrollen
  - “Begleitung" von Containern
  - Diebstahl von Container-PIN

Kriminelle Symbiose ..

- Massive Simplifizierung für Schmuggler:innen
  - Wegfallende Notwendigkeit lokaler Helfer:innen
- Einfacher Verdienst für Cyberkriminelle
  - Ein erfolgreich geschmuggelter Container? 500.000 Euro.

- 2022: 160 Tonnen beschlagnahmtes Kokain in Rotterdam
  - Kontrollierte Container? Weit unter 5%.
- Moderne Häfen sind auf Effizienz ausgelegt, nicht Sicherheit
  - Jede weitere Untergrabung schmerzt.
- Das betrifft anscheinend auch die IT ..

II: Geld



Diebstahl? Banküberfall? Ja.

- August 2018: Visa alarmiert Cosmos Co-operative Bank
  - Tausende Barbehebungen in ganz Maharashtra
- Cosmos reagiert, und tut .. nichts.
- Zeit bis zu kalten Füßen: 30 Minuten
  - Dadurch entstandener Schaden: 12.000 Behebungen, etwa 14 Millionen USD

- Weltweit idente Fälle innerhalb von zwei Stunden
  - US, UK, UAE, RU, ..
- Indien: Verhaftungen von 18 Verdächtigen
  - Student:innen, Kellner:innen, Handwerker:innen
- Forensische Ermittlungen finden Unregelmäßigkeiten
  - (Digitale) Forensische Ermittlungen finden die Ursache

Es sind immer Computer ..

- Die Sicherheit der IT-Infrastruktur der Bank ~~war unterirdisch~~ hatte viel Potential
- Angreifer:innen hatten vollständigen Zugriff auf die Systeme
- Manipulation von interner Software
  - Bankomaten sollten alle PIN akzeptieren
  - Konten hatten immer 10.000$, egal wie viel abgehoben wurde

Technically, it’s cybercrime!

(State-sponsored, but whatever ..)

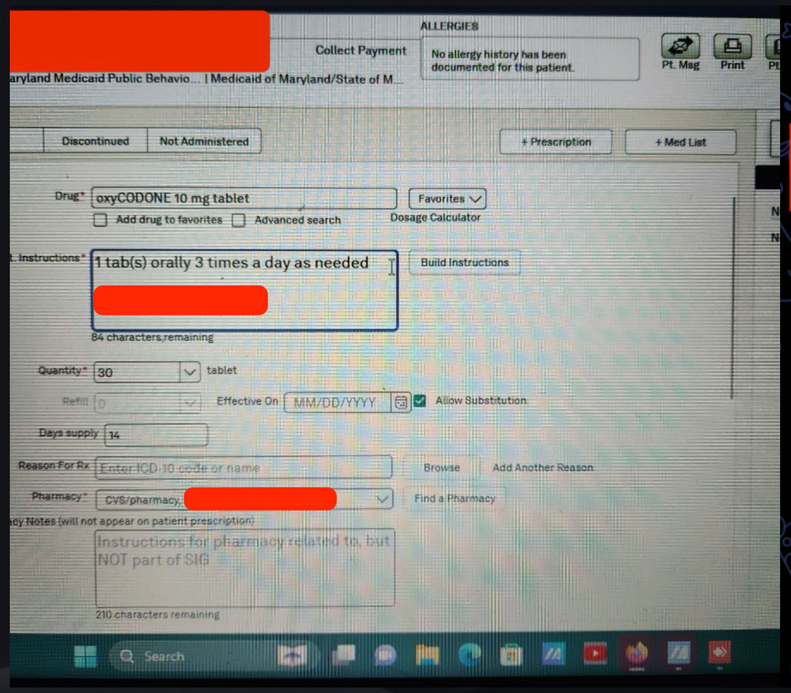
- Angriffe wurden Lazarus Group zugerechnet
  - Teil einer anhaltenden Serie von Angriffen, Schäden im dreistelligen Millionenbereich
- Laut US-amerikanischen Expert:innen: Kapazitäten aus “low level fraud forums”
- Beauftragung der Mules durch lokale OK Strukturen
  - DPRK unterhält Beziehungen dieser Art in ganz SEA

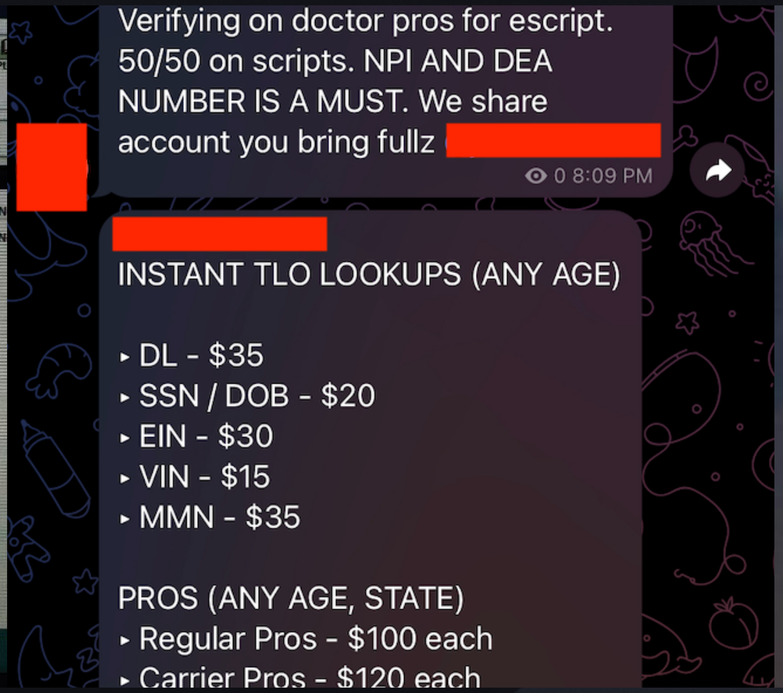
Kriminelle Symbiose ..

- Einfacher Verdienst für Kriminelle
  - Ein paar Mules finden, aus der Portokasse bezahlen - Profit!
- Massive logistische Vereinfachung für "Cyberkriminelle"
  - Wegfallen der Suche nach Mules
  - Bessere Kontrollmöglichkeiten ->

> One gang had a handler who was monitoring the ATM transactions in real time on a laptop, Singh says. CCTV footage showed that whenever a money mule had tried to keep some of the cash for himself, the handler would spot it and gave him a hard slap.

III: Drogen (.. aber anders!)


ALLERGIES
Collect Payment
No allergy history has been documented for this patient.
Pt. Msg
Print
Discontinued
Not Administered
+ Prescription
+ Med List
Drug*
oxyCODONE 10 mg tablet
Favorites
Add drug to favorites
Advanced search
Dosage Calculator
Instructions*
1 tab(s) orally 3 times a day as needed
Build Instructions
84 characters remaining
Quantity*
30
tablet
Refill
0
Effective On
MM/DD/YYYY
Allow Substitution
Days supply
14
Reason For Rx
Enter ICD-10 code or name
Browse
Add Another Reason
Pharmacy*
CVS/pharmacy
Find a Pharmacy
Pharmacy Notes (will not appear on patient prescription)
Instructions for pharmacy related to, but NOT part of SIG
210 characters remaining
Search


Verifying on doctor pros for escript. 50/50 on scripts. NPI AND DEA NUMBER IS A MUST. We share account you bring fullz
0 8:09 PM
INSTANT TLO LOOKUPS (ANY AGE)
▸ DL - $35
▸ SSN / DOB - $20
▸ EIN - $30
▸ VIN - $15
▸ MMN - $35
PROS (ANY AGE, STATE)
▸ Regular Pros - $100 each
▸ Carrier Pros - $120 each


Pick up and drops around Leederville can do S.O.R too
Xanax
alprazolam
tablets, USP
2 mg
50 Tablets

Missbrauch elektronischer Rezepte

“Scrip fraud”

- Primär in den USA, Kanada - aus systematischen Gründen
  - Vereinzelte (erste?) Fälle in Deutschland
- Ähnlich professionell wie (z.B.) Ransomware
  - Zugangsdaten über eigene Access Broker
  - Missbräuchliches Ausstellen von validen Rezepten
  - Strassenverkauf durch “reguläre" Dealer

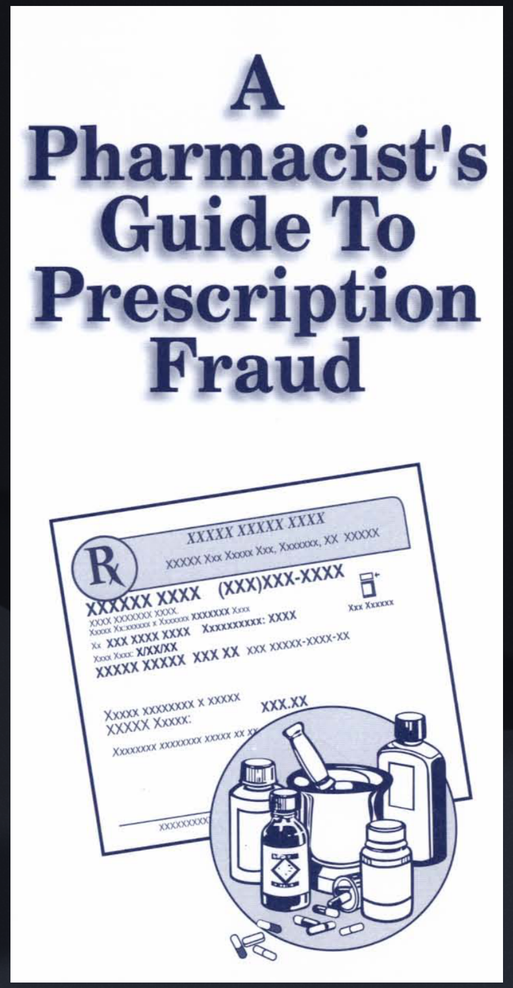
- Betrugsbekämpfung durch Betrugserleichterung 👌
- Verstärkung des Betrugsausmaßes
- Nebeneffekt: Verstärkung von Knappheit



Kriminelle Symbiose ..

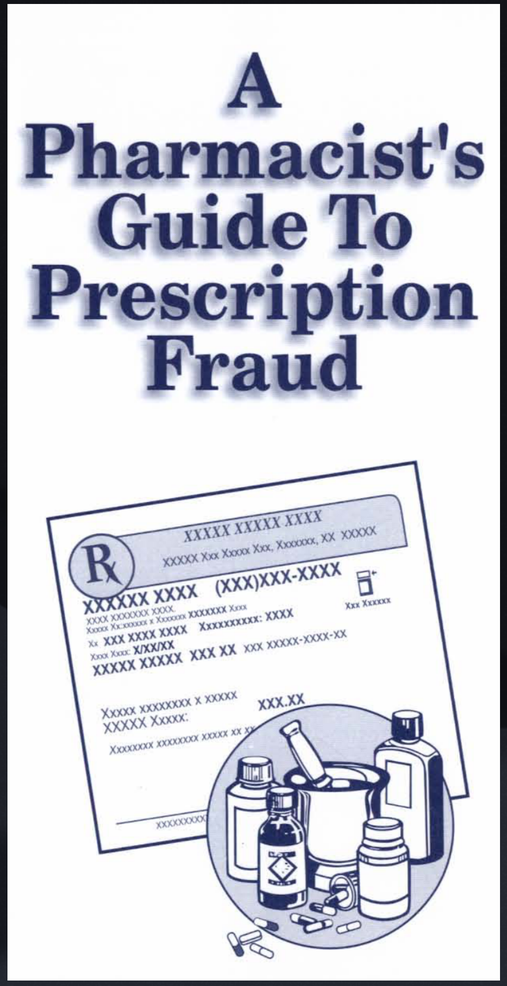
- Simplifizierung für Dealer:innen
  - Keine Abhängigkeit von Helfer:innen mehr
- Einfacher Verdienst für Cyberkriminelle
  - Andere Größenordnung, immer noch gut
- Risikominimierung für beide Seiten

- Apotheken sind kaum in der Lage, den Betrug zu erkennen
- Strafverfolgungsbehörden verlieren wichtige Ansatzpunkte
  - Vielzahl verschiedener digitaler Systeme erschwert Ermittlungen
  - Weniger Chance auf “schlechtes Gewissen”

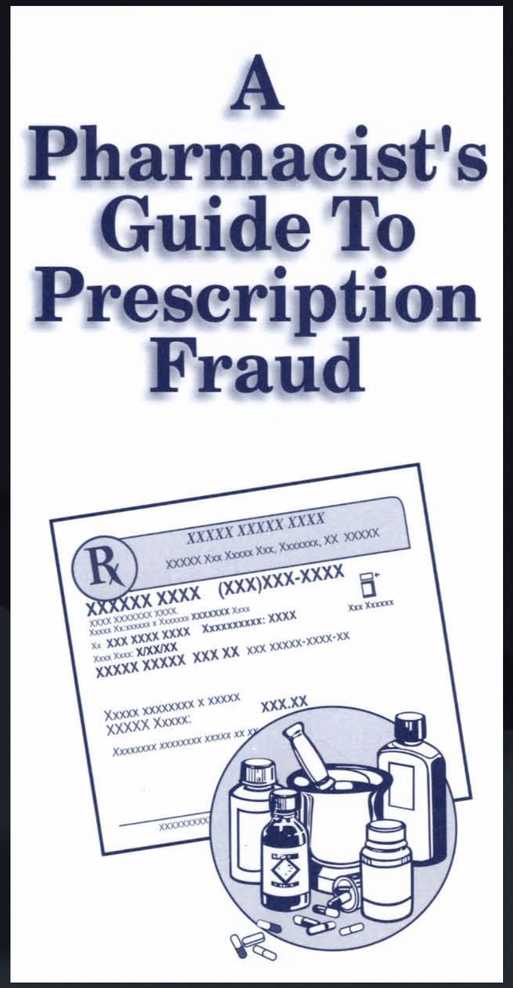


- Apotheker[illegible]age, den Betrug zu erkennen
- Strafverfolgungsbehör[illegible]ige Ansatzpunkte
  - Vielzahl verschiedener digitaler Sy[illegible]mittlungen
  - Weniger Chance auf “schlechtes Gewissen”

● Prescription looks “too good”; the prescriber’s handwriting is too legible;



- Apotheken sind kaum in der Lage, den Betrug zu erkennen
- Strafverfolgungsbehörden verlieren wichtige Ansatzpunkte
  - Vielzahl verschiedener digitaler Systeme erschwert Ermittlungen
  - Weniger Chance auf “schlechtes Gewissen”



Und so weiter ..

Weitere Beispiele

- MPC, EncroChat, Phantom Secure - dediziert kriminelle Kommunikationsinfrastruktur
  - No. 1 BC - ..

Stichwort ..

No.1 BC, as a secure communications provider, designed and brought to life a unique encryption technology: advanced hybrid algorithm. We do realize that industrial espionage can be a serious threat for businesses and created tools to take care of sensitive information and keep it safe from spies. Different governmental and military organizations use No.1 BC solutions to protect confidential information worldwide, including Ministry of Military and Defence of Austria.

Stichwort ..

No.1 BC, as a secure communications provider, designed and brought to life a unique encryption technology: advanced hybrid algorithm. We do realize that industrial espionage can be a serious threat for businesses and created tools to take care of sensitive information and keep it safe from spies. Different governmental and military organizations use No.1 BC solutions to protect confidential information worldwide, including Ministry of Military and Defence of Austria.

Weitere Beispiele

- MPC, EncroChat, Phantom Secure - dediziert kriminelle Kommunikationsinfrastruktur
  - No. 1 BC - angeblicher (weil dementiert) Kunde BMLV. 🙃
  - Vorbehalt: Cybercrime-Involvierung nicht *erwiesen*
- Geldwäsche
- (RUMINT) Diebstahl

Und so weiter ..

So viele weitere Beispiele ..

.. die ich auslassen musste

- Zusammenarbeit zwischen Cyberkriminellen und / in / mit (korrupten) staatlichen Strukturen
  - Vorovskoi mir, wory w zakone, avtoritety ..
  - Naji Technology & Afkar Systems
  - ..

TL;DR

- Digitale und "analoge" Kriminalität kooperiert nicht nur im Bereich des Rauschgifthandels
- Mediale Darstellungen zu dem Thema sind oftmals reisserisch und fragwürdiger Natur
- Die "Übernahme" von Cybercrime-Akteuren durch "die Mafia" ist ein Schreckgespenst
  - Gleichzeitig: Intensivierte Kooperation in den letzten Jahren
- IT-Sicherheit darf bei analogen Sicherheitskonzepten nicht vernachlässigt werden!

Fragen?

