

Forenzní analýza temných tržišť

Daniel Dolejška

6. května 2021

Fakulta informačních technologií Vysokého učení technického v Brně
Božetěchova 1/2. 612 66 Brno - Královo Pole
dolejska@fit.vut.cz



- Customisable crawler and scraper
- Highly precise and detailed data
- Automated long-term monitoring
- Complete website archivation
 - Product, vendor, purchase data
 - Insight into current trends
 - Product purchase detection
 - Cryptocurrency correlation
 - Transaction flagging

Darkmarket Forensics

Author: Bc. Daniel Dolejška
Supervisor: Ing. Vladimír Veselý, Ph.D.

<https://excel.bazar.nesad.fit.vutbr.cz>



SURFACE WEB

World Wide Web, indexed
by search engines

DEEP WEB

Log-in sites, accessible
via secure sign-in

DARK WEB

Hidden sites, accessible
via specific software
or hardware



PLATBY NA TEMNÝCH TRŽIŠTÍCH

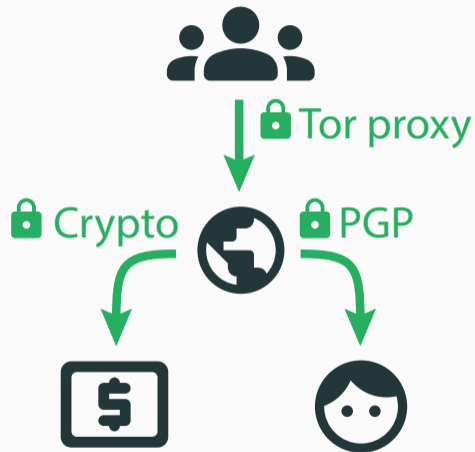


PGP Encryption

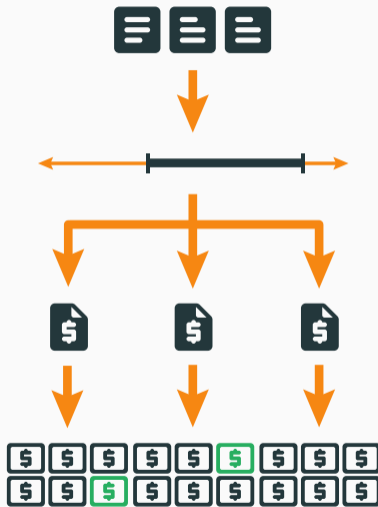
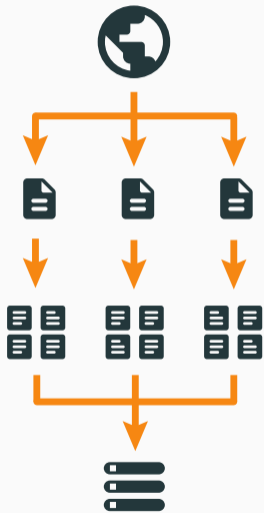


1 0 1 0 0 1
0 1 0 1 0 1
1 0 0 1 0 1

„STAVEBNÍ KAMENY“ TEMNÝCH TRŽIŠTÍ

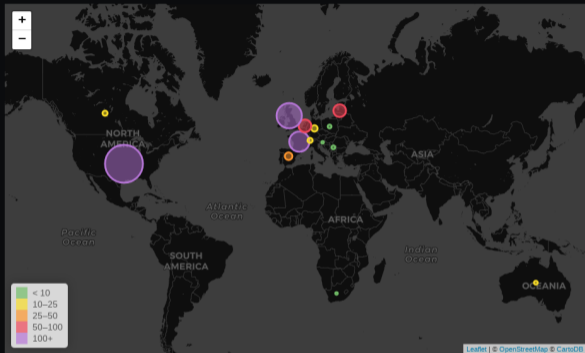


NAVRŽENÝ POSTUP



MONITOROVACÍ GRAFANA DASHBOARD

Product Counts by Country of Origin



New Stat Entries Over the Last Minute



Sales Detected in the Last Hour



Product Sales by Category



Category	Count
Stimulants	7
Psychedelics	4
Ecstasy	4
Cannabis	4

Number of Collected Statistics and Detected Sales



Number of Detected Sales



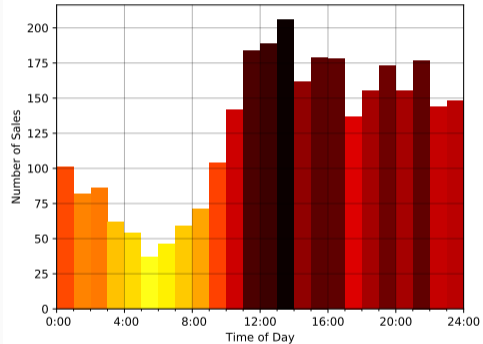
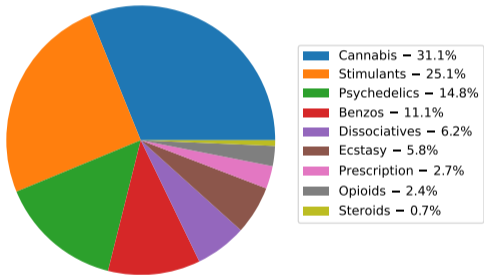
Top 5 Subcategories by Sales (Last 14 days)

Category	Subcategory
Cannabis	Buds & Flower
Stimulants	Cocaine
Benzos	Pills
Psychedelics	LSD
Dissociatives	Ketamine

Top 5 Products by Sales (Last 14 days)

Product	Category	Subcategory
Peruvian FISHSCALE COCAINE	Stimulants	Cocaine
Diazepam 10mg Tabs Kern Pharma 30tabs/box	Benzos	Pills
Speed POWDER	Stimulants	Speed
Amnesia Haze Amsterdarm Quality	Cannabis	Buds & Flower
grainy white ket (really strong)	Dissociatives	Ketamine

AKTUÁLNÍ VÝSLEDKY



KOHO TO ZAJÍMÁ?



- Obrázek „The 3 Tiers of Internet“ (slide 0, PDF strana 4) převzat¹ a upraven
- Obrázek „Tor Browser již oficiálně i pro Android. Slibuje nejbezpečnější surfování“ (slide 1, PDF strana 5) převzat²
- Obrázek „What is Cryptocurrency and How Does It Work?“ (slide 2, PDF strana 6) převzat³
- Obrázek „PGP: Šifrování a podepisování e-mailů na pár kliknutí“ (slide 3, PDF strana 7) převzat⁴
- Obrázek „Odznak Služby kriminální policie a vyšetřování“ (slide 8, PDF strana 12) převzat⁵
- Obrázek „Odznak Národní centrály proti organizovanému zločinu“ (slide 8, PDF strana 12) převzat⁶
- Obrázek „Odznak Kriminalistického ústavu Praha“ (slide 8, PDF strana 12) převzat⁷

¹<https://www.maltego.com/blog/business-risk-intelligence-gathering-insight-into-the-deep-and-dark-web-part-1/>

²<https://www.cnews.cz/tor-browser-alfa-android-stazeni>

³<https://losspreventionmedia.com/what-is-cryptocurrency-and-how-does-it-work/>

⁴<https://cz.emclient.com/blog/pgp--sifrovani-a-podepisovani-e-mailu-na-par-kliknuti-303>

⁵https://commons.wikimedia.org/wiki/File:SKPV_badge.png#/media/Soubor:SKPV_badge.png

⁶<https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpvc.aspx>

⁷<https://www.policie.cz/clanek/kriminalisticky-ustav-ma-novy-znak.aspx>