



Epic Cases of Costly OPSEC Failures

~5 min read | Published on 2023-06-23, tagged [Darkweb-Vendor](#), [OPSEC](#) using 1247 words.

In most dark web vendor busts, the vendors are identified not due to complex LE investigations, but because they fail in basic OPSEC.

In a typical vendor bust, the investigators make undercover purchases, conduct surveillance at the post office the drugs were mailed from, and identify the sender who in most cases turns out to be the vendor. The investigators almost always track the bitcoin to the vendor's account at a crypto exchange. In some cases, the vendors are so sloppy, that their identities are uncovered without the undercover purchases.

Let's take a look at vendors whose operations were characterized by bad OPSEC.

Canna_Bars

Jose Robert Porras III was identified as the operator of the Canna_Bars vendor account on Dream Market in investigations that were part of Operation Dark Gold. Vendors busted in the operation sent bitcoin to investigators in exchange for cash mailed to their residences.

In addition to sending Bitcoin to LE, Porras made the mistake of sharing photos that had his fingerprints visible.

According to the [criminal complaint](#), while reviewing the Canna_Bars vendor account on Dream Market, the investigators found out that the account had a verified review from Hansa Market.

The investigators contacted the Dutch National Police who had taken control of Hansa market for over a month in 2017. The Dutch Police provided data for the Canna_Bars vendor account on Hansa.

While reviewing the data the investigators discovered that Canna_Bars had provided a customer with a link to an [Imgur album](#). The album included a high-resolution picture of the vendor's hand holding cannabis buds.



One of the photos in the album

In March 2018, the investigators downloaded the image and had the fingerprints analyzed. The fingerprints in the image were a match to Porras's fingerprints acquired from prior arrests.

Porras and his accomplice were consequently arrested and charged in a 16-count indictment.

Porras pleaded guilty to one count each of distribution of a controlled substance and firearm possession as a felon. He was [sentenced](#) to five years and 10 months in prison in December 2019.

Blime-Sub and BTH-Overdose

Emil Vladimirov Babadjov was identified as the operator of the Blime-Sub and BTH-Overdose, vendor accounts after a brief investigation, thanks to his sloppy OPSEC.

The DEA [launched investigations](#) into "Blime-Sub" and BTH-Overdose on AlphaBay in September 2016. A review of the PGP key associated with the vendor account revealed that the key was registered to the email address: babadjov@gmail.com.

A Facebook search revealed that the email address was associated with an account registered to "Lime Vojdabab," Emil Babadjov in reverse.

In November, the DEA asked Coinbase to provide information on any account registered to the email. Coinbase revealed that in November 2015, the email was used to open an account registered to Emil Babadjov. Coinbase also revealed that Babadjov had attempted to open an account in March 2016 using the email blimesub@gmail.com. This piece of information connected blimesub@gmail.com to the Blime-Sub vendor account.

In October, the investigators made an undercover purchase of heroin

from Blime-Sub on AlphaBay. The white powder the investigators received tested positive for both heroin and fentanyl. The investigators found fingerprints on the package used to mail the drugs. Fingerprint analysis revealed that the fingerprints found were a match for Babadjov. Further investigations revealed that the postage on the drug package had been purchased from a Self Service Kiosk at a post office in San Francisco. Photos taken during the purchase confirmed that Babadjov purchased the postage and mailed the drug package.

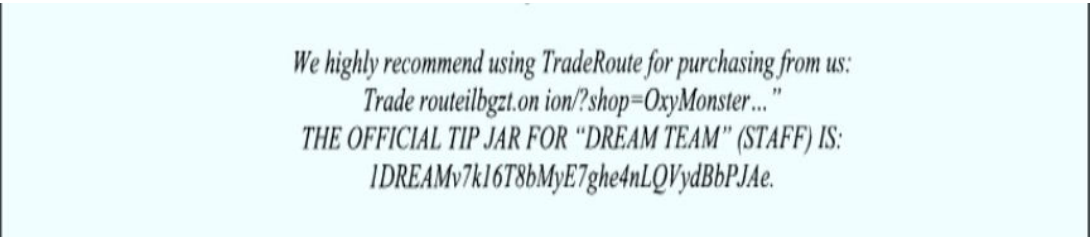
Babadjov was consequently charged with distributing fentanyl and heroin and arrested in December 2016. He pleaded guilty in October 2017.

Babadjov was [sentenced](#) to 5 years and 10 months in prison in January 2018.

OxyMonster

Gal Vallerius, a French national, started as an Oxycodone and Ritalin vendor on Evolution Dream and TradeRoute as OxyMonster. He later became a senior moderator and admin at Dream Market.

All the investigators had to do to link Vallerius to OxyMonster was [track bitcoin](#) transactions. Blockchain analysis of a bitcoin address used by OxyMonster to receive tips revealed that the address sent bitcoin to a Localbitcoins account registered to Vallerius.



*We highly recommend using TradeRoute for purchasing from us:
Trade routeilbgzt.on ion/?shop=OxyMonster..."*
THE OFFICIAL TIP JAR FOR "DREAM TEAM" (STAFF) IS:
1DREAMv7k16T8bMyE7ghe4nLQVydBbPJAE.

The bitcoin address

On August 31, 2017, Vallerius traveled to the US to attend a beard competition in Texas. The investigators searched his laptop at Atlanta International Airport. The investigators found login credentials to Dream Market, and a PGP encryption key entitled "OxyMonster". The key matched OxyMonster's PGP key on Dream Market. The investigators also found bitcoin worth \$500,000 at the time.

Vallerius [pleaded guilty](#) to conspiracy to possess with the intent to distribute controlled substances and conspiracy to launder money. He also agreed to forfeit approximately 99.98 bitcoin and 121.94 bitcoin cash.

Vallerius was [sentenced](#) to 20 years in prison in October 2018.

Area51 and DarkApollo

The identification of Abdullah Almashwali and Chaudhry Farooq as the

operators of the "Area51" and "DarkApollo" vendor accounts on Alpha Bay, was made easier by the fact that they used a personal email to create the PGP keys for the vendor accounts.

While [reviewing the vendor accounts](#) in March 2016, a DEA agent discovered that the vendors' PGP keys were registered using the same email address: Adashc31@gmail.com. A social media search of the terms "Adashc31" and "Adashc" led them to Twitter, Instagram, and Facebook accounts used by Farooq.



Farooq's Twitter account

In April the investigators subpoenaed Facebook for information on the account registered to Farooq. The information acquired from Facebook gave the DEA access to a phone number associated with Farooq's account. The DEA later established that the phone number was part of an investigation into heroin trafficking in Brooklyn.

In May the agent purchased heroin from Area51 and DarkApollo. In each of the drug packages the agent received, the heroin was placed in a clear zip bag placed inside a silver Mylar envelope. Fingerprints found on the drug packages matched those of Almashwali.

Investigations by the USPIS revealed that the postage for one of the undercover drug packages had been purchased from a self Service Kiosk at a post office in Brooklyn. Photos captured during the purchase confirmed Almashwali mailed the package.

The USPIS also found out that the credit card used to make the purchase had been used to make postage purchases multiple times. Photo's taken during the transactions showed either Almashwali or Farooq purchasing postage.

Almashwali was sentenced to six and a half years in prison on July 2017. Farooq was [sentenced](#) to a year and 11 months in prison in January 2018.

ChInsaint

ChInsaint was a fentanyl, heroin, and oxycodone vendor on Empire Market. Chaloner Saintillus put little effort into the security of his drug trafficking operation. To begin with, he used the abbreviation of his real name as his vendor name.

The investigators made the first undercover purchase in April 2020. USPS records revealed that the package's postage was purchased at a Self Service Kiosk. Images taken during [the purchase](#) showed Saintillus made the purchase. The card used to pay for that and other purchases belonged to Saintillus.

A further review of USPS records revealed that there existed three USPS accounts associated with Saintillus. Two of the accounts had been created with an email address: chInsaint@gmail.com.

USPS Account 1

Username: ChInsaint
Name: Chaloner Saintillus
Address: 222 SW 3rd Ave, Delray Beach, FL 33444
Phone: 561-853-4220 and 561-774-4760
Email: chInsaint@gmail.com

USPS Account 2

Username: ChInsaint@gmail.com
Name: Chaloner Saintillus - S and S Corporation
Address: 222 SW 3rd Ave, Delray Beach, FL 33444
Phone: 954-605-4135
Email: chInsaint@gmail.com

USPS Account 3

Username: shalamalielbey@gmail.com
Name: Chaloner Saintillus
Address: 222 SW 3rd Ave, Delray Beach, FL 33444
Phone: 561-774-4760
Email: shalamalielbey@gmail.com

The USPS accounts

An open internet search of Saintillus led the investigators to a dating site profile with the username "ChInsaint". The profile had Saintillus' photo.

The Investigators arrested him on October 2020 and seized large quantities of drugs, approximately \$25,000 in XRP, and a loaded firearm after searching his residence.

In April 2023, Saintillus [pleaded guilty](#) to distributing controlled substances. He will be sentenced in July.

Foolproof security measures may not exist but studying mistakes made by other vendors and avoiding similar mistakes could go a long way in making sure vendors are not caught.

Comments (14)

Ahmed Farooq looks goofy as hell bro

[Reply](#)

SexyWaffle 2023-06-24

[cb8200cc](#)

I'm just excited to hear Chlnsaint's album that I'm sure he'll record from prison.

[Reply](#)

Froni Smith 2023-06-24

[f2055c3e](#)

Senders must avoid to publish in Clearnet their activities.
Stupid faults are stupid until you get caught.

Even presidents and dictators were murdered only because they did not leave their country soon enough.

[Reply](#)

Mike Oxlong 2023-06-24

[69d7f943](#)

That first one who posted pictures of his hands with his fingerprints visible is hilarious. That's like when Andrew Tate gave away his location to police by showing a pizza box with the name and number of the pizzeria on his twatter account.

[Reply](#)

andrew tate 2023-06-26

[68f1a230](#)

thats reall funy

(.)(.) 2023-07-29

[5b4fdc3c](#)

He didn't "gave away his location", genius. It's not like he was on the run from LE or something during that time. It's just that LE weren't sure if he was in the country or not because Tate travels a lot but the pizza box thing was what confirmed to them that he was in the country. They were gonna get him eventually no matter what.

THEYCALLMEBIG 2023-06-26

[8ffd2082](#)

one thing i dont know why it doesnt even matter how hard you try

[Reply](#)

pgpkey9349300340 2023-07-13

[d61baff2](#)

LOL LOL LOL LOL LOL LOL LOL LOL LOL LOL LOL LOL LOL LOL LOL LOL

assblaster 2023-06-27

[94c8c487](#)

Youd think someone would have made a multiple choice test for new vendors so they can see if they are clinically retarded.

[Reply](#)

hey chat 2023-06-28

[a67168ff](#)

what is blud doing 🧠🧠🧠🧠🔥🔥🔥🔥🔥

[Reply](#)

YFmEvR 2023-07-13

[a8d5fb0e](#)

Dont mess with a vendor at the beginning or end...

[Reply](#)

Quandale Dingle 2023-07-17

[e9c2cc24](#)

Ah hell naaah,

shout out to Cardi B

[Reply](#)

rm001 2023-07-26

[50d20c64](#)

Interesting...

[Reply](#)

cleoassfatra 2023-07-30

[cbee3603](#)

that's crazy I personally wouldn't take that just me though

[Reply](#)

Your thoughts

Your Name



Captcha

Submit

[Donate](#) [PGP Key](#) [Mirrors](#) [Canary](#) [Contact](#) [RSS](#) [Atom](#) [JSON](#)

DarkNetLive©2023