Alleged Hydra Market Operators Identified

February 19, 2021

› Previous Next ›

02/19/2021

Key Findings

An anonymous author on the hydra[.]expert domain claimed to have uncovered the true identities of the individuals running the Hydra marketplace, one of the largest Russian-language dark web markets for drugs. Gemini has translated and analyzed this investigation, although we have not confirmed the entirety of the evidence.

The anonymous author alleges that Bogdan Koliesniev and Alexander Dyriavin, both Ukrainian citizens, are responsible for Hydra’s operations. Gemini has confirmed only some of the author’s findings.

This anonymous post began with the author purporting to have attempted to blackmail these individuals for monetary gain. According to the author, these individuals did not pay, so the author decided to reveal their identities. Telegra.ph forum user “monarkhov,” who claims to be Bogdan Koliesniev, denied his connection to Hydra.

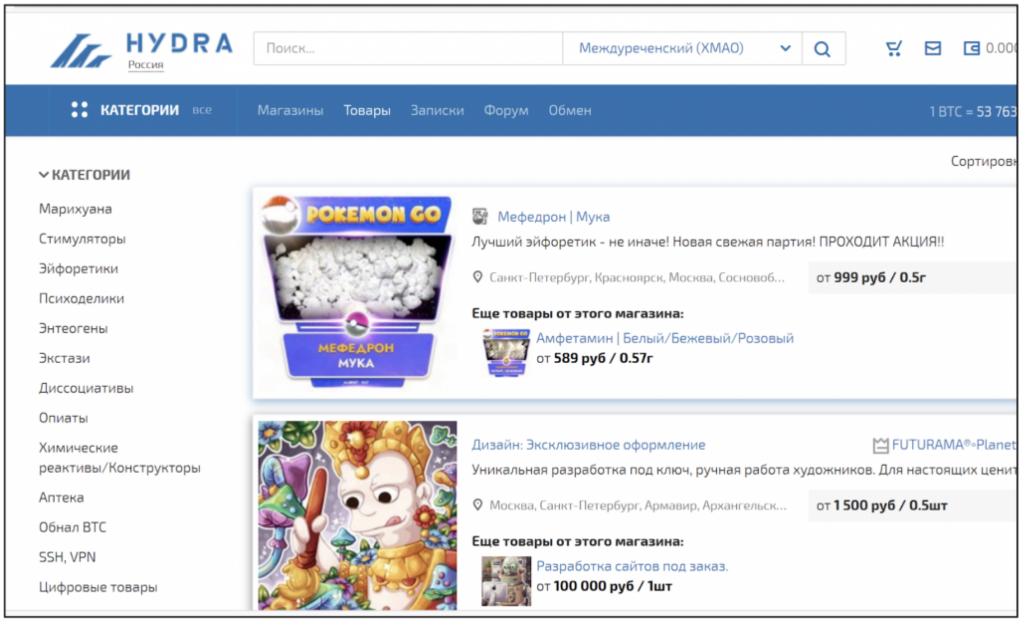
Based on an analysis of the anonymous author’s investigation, Gemini Advisory assesses with moderate confidence that Bogdan Koliesniev is likely one of the perpetrators behind the Hydra dark market due to significant evidence pointing to this individual related to shared infrastructure and linked contact information. However, Gemini assesses with low confidence that Alexander Dyriavin may be involved with Hydra, although likely at a lower level with indirect contributions to their operations.

Background

Gemini analysts have found a post by an anonymous author on the hydra[.]expert domain claiming to have uncovered the true identities of the individuals running Hydra, one of the largest Russian-language dark web marketplaces for drugs. While formerly part of Hydra’s infrastructure, hydra[.]expert now appears to be solely dedicated to identifying Hydra’s operators. Gemini has translated and analyzed the investigation pointing to the identities of Hydra’s alleged operators, although we have not confirmed the entirety of the evidence. The post circulated among multiple dark web channels, including an anonymous image forum and a Telegram channel. It has also reached Russian-language media

Hydra

Hydra was founded in 2015, and gradually conquered the market for illegal goods. The platform has become one of the largest in the world and is the single largest platform for the sale of drugs in the Former Soviet Union (FSU). It serves as an intermediary between sellers and buyers; while it mainly focuses on the sale of drugs, it also has a section on counterfeit bank notes, hacking services, counterfeit documents, and other prohibited items. As of this writing, there are 2.5 million accounts registered on the platform and the number of accounts grows every month.



Мефедрон | Мука

Лучший эйфоретик - не иначе! Новая свежая партия! ПРОХОДИТ АКЦИЯ!!

Санкт-Петербург, Красноярск, Москва, Сосновоб...

от 999 руб / 0.5г

Еще товары от этого магазина:

Амфетамин | Белый/Бежевый/Розовый

от 589 руб / 0.57г

Дизайн: Эксклюзивное оформление

FUTURAMA®◦Planet

Уникальная разработка под ключ, ручная работа художников. Для настоящих ценит

Москва, Санкт-Петербург, Армавир, Архангельск...

от 1 500 руб / 0.5шт

Еще товары от этого магазина:

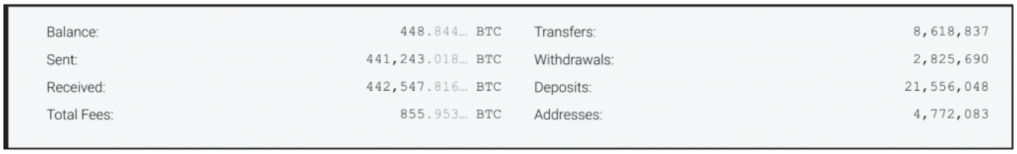
Разработка сайтов под заказ.

от 100 000 руб / 1шт

Image 1: The main page of the Hydra dark web marketplace. The top advertisement offers the synthetic stimulant drug Mephedrone and the bottom offers counterfeit documents.

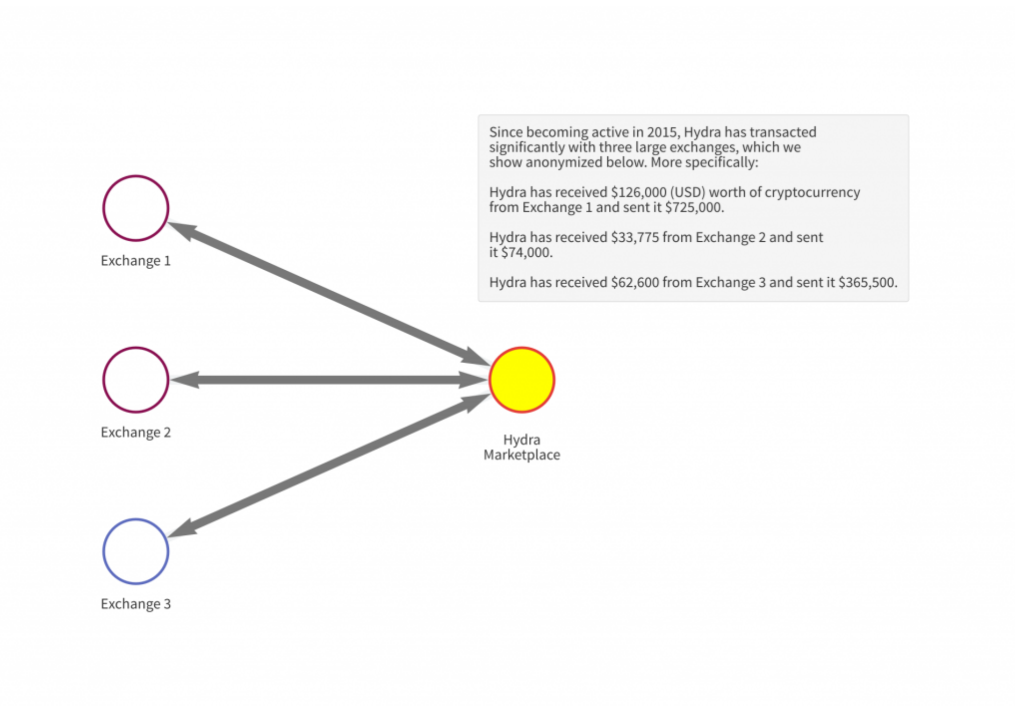
In-Depth Analysis

OperationsBlockchain analysis company Chainalysis examined the Bitcoin wallets associated with this market and estimated that over the lifetime of the shop, there were at least $3.4 billion worth of transactions. The Hydra market has also had $1,260,875 in transactions with three crypto currency exchanges. While only about $430,000 in direct exposure could be confirmed with one large international exchange, its indirect sending exposure was much larger – $1,875,000 USD. Such activities could indicate that the market's operators were using legitimate exchanges to launder some of the illicit profits.



Balance:	448.844… BTC	Transfers:	8,618,837
Sent:	441,243.018… BTC	Withdrawals:	2,825,690
Received:	442,547.816… BTC	Deposits:	21,556,048
Total Fees:	855.953… BTC	Addresses:	4,772,083

Image 2: Total transaction amounts over Hydra's lifespan, according to Chainalysis.



Since becoming active in 2015, Hydra has transacted significantly with three large exchanges, which we show anonymized below. More specifically:

Hydra has received $126,000 (USD) worth of cryptocurrency from Exchange 1 and sent it $725,000.

Hydra has received $33,775 from Exchange 2 and sent it $74,000.

Hydra has received $62,600 from Exchange 3 and sent it $365,500.

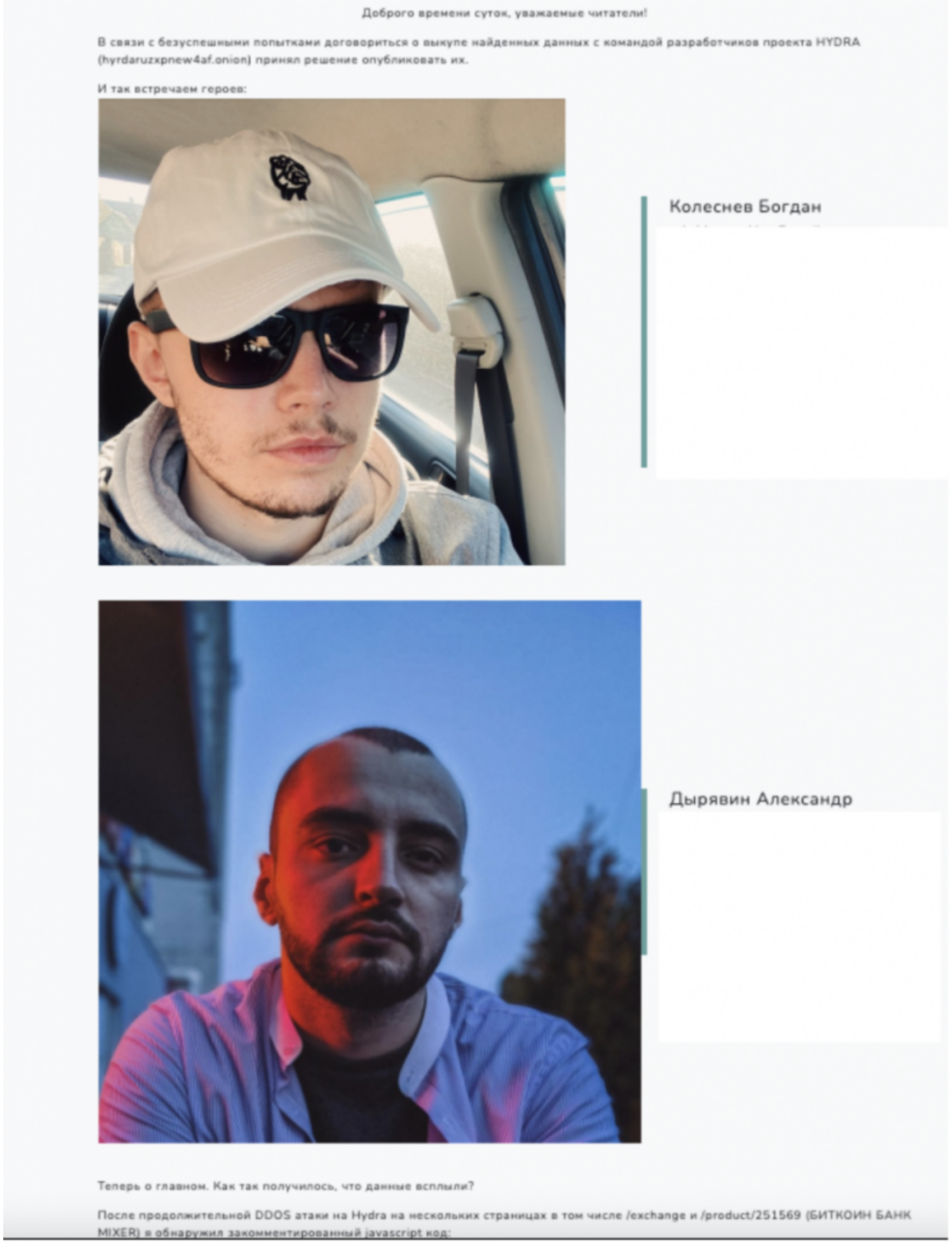
Image 3: The Hydra market was linked to three cryptocurrency exchanges.

The Investigation

According to the post on hydra[.]expert, Bogdan Koliesniev (Kolesnev) and Alexander Dyriavin (Daryavin), both citizens of Ukraine, are responsible for Hydra's operations. The post's author claims to have conducted an analysis after a distributed denial-of-service (DDoS) attack hit Hydra, and purportedly uncovered JavaScript code installed on the marketplace. The author's investigation included the following key points, only some of which Gemini has confirmed:

- The JavaScript code was connected to the domain name z[.]team.
- Analysis of z[.]team subdomain qp[.]z[.]team revealed a .json file. The analysis of this file revealed that it was created by "Askold Monarkhov," and also included the email address. Analysis of the subdomain git[.]z[.]team revealed another name, Alexander Dyriavin.
- A search for the above email address led to the GitHub page of "ASKOLDEX," which also displays the name of Bogdan Kolesnev as an event bug fixer.
- A search for ASKOLDEX reveals a YouTube page that has video tutorials on creating Telegram bots and the management of QIWI panels, as well as other videos.
- Additional searches revealed a VK social media page for Askold Monarkhov.
- A Whois record search for the above email indicated that it was used to register the domain name monarkhov[.]pro with the registration name is Bogdan Koliesniev.
- Additional personally identifiable information (PII) was obtained on Bogdan Kolesnev, such as his passport number and telephone number.

- A search for Alexander Dyriavin revealed a profile for an individual with the same name on GitHub. Their Github profile page also indicated that Dyriavin worked with ASKOLDEX.
- Additional searches revealed Alexander Dyriavin’s email address, social media accounts, and other PII.
- The post noted additional links between uncovered IP addresses and various domains, and various directory name overlaps.



Доброго времени суток, уважаемые читатели!

В связи с безуспешными попытками договориться о выкупе найденных данных с командой разработчиков проекта HYDRA (hyrdaruzxpnew4af.onion) принял решение опубликовать их.

И так встречаем героев:

Колеснев Богдан

[redacted]

Дырявин Александр

[redacted]

Теперь о главном. Как так получилось, что данные всплыли?

После продолжительной DDOS атаки на Hydra на нескольких страницах в том числе /exchange и /product/251569 (БИТКОИН БАНК MIXER) я обнаружил закомментированный javascript код:

Image 4: Part of the anonymous post’s investigation on hydra[.]expert included images of the alleged operators.

Blackmail

It is worth pointing out that this anonymous post began with the author claiming to have attempted to blackmail these individuals for monetary gain. According to the author, these individuals did not pay, so the author decided to reveal their identities. It is also worth noting that according to WaybackMachine, in 2018 hydra[.]expert used to be a mirror domain of the Hydra market on the surface web, however, it remains unclear if this was the official mirror of the actual Hydra market, which was primarily hosted in the dark web. Furthermore, according to Whois records, the domain hydra[.]expert was recently purchased, which could indicate that it was purchased for the sole purpose of posting this research.

It Wasn’t Me

On the same day as this post, on Telegra.ph, which is a Russian-language forum for anonymous posts, user “monarkhov” created a post claiming to be Bogdan Koliesniev (hxxps://telegra[.]ph/Kak-ya-stal-razrabotchikom-Gidry-bez-registracii-i-sms-02-19). The user monarkhov indicated that the investigation’s findings were incorrect and that they have nothing to do with Hydra. User monarkhov claimed that they create the framework for making Telegram bots and create admin panels to control Qiwi wallets. Additionally, monarkhov claimed that many of their source codes are available on Github and that anyone could have used them. This purportedly explains why Hydra used infrastructure linked to Koliesniev, although it does not explain why Hydra specifically chose Koliesniev’s code.

Conclusion

Based on an analysis of the anonymous author’s investigation, Gemini Advisory assesses with moderate confidence that Bogdan Koliesniev is likely one of the perpetrators behind the Hydra dark market due to significant evidence pointing to this individual related to shared infrastructure and linked contact information. However, Gemini assesses with low confidence that Alexander Dyriavin may be involved with Hydra, although likely at a lower level with indirect contributions to their operations.

Gemini Advisory Mission Statement

Gemini Advisory provides actionable fraud intelligence to the largest financial organizations in an effort to mitigate ever-growing cyber risks. Our proprietary software utilizes asymmetrical solutions in order to help identify and isolate assets targeted by fraudsters and online criminals in real-time.