FLASHPOINT Chainalysis

Hydra: Where The Crypto Money Laundering Trail Goes Dark

Sequencing Cryptocurrency Flows on the Russian Cybercrime Market "Hydra"

Key Takeaways

- Hydra is a Russian-language dark web marketplace (DWM) primarily known to facilitate the illicit sales of narcotics. Active since 2015, Hydra opened as a less-antagonistic option to its now-defunct competitor, Russian Anonymous Marketplace (aka, "RAMP"), notorious for eliminating its competition via DDoS attacks and operator doxxing.

- Hydra market activity has skyrocketed since its inception, with annual transaction volumes growing from a total of $9.40 million in 2016 to $1.37 billion in 2020.

- Since July 2018, Hydra has imposed strict limitations on sellers, requiring that their cryptocurrency funds be withdrawn into Russian fiat currency via select regionally-operated exchanges and payment services. Blockchain analysis of Hydra crypto transactions further confirms this movement with the vast majority of funds leaving Hydra move through in-region exchanges and accounts as the next destination in the ongoing illicit financial chain.

- Hydra seller accounts are in high demand, with a new sub-market emerging for cybercriminals willing to pay those with established seller accounts to gain direct access to the marketplace to circumvent Hydra withdrawal restrictions.

- New physical cash withdrawal workaround techniques are increasingly popular, with methods like the "Hidden Treasure" technique, which entails the physical burial of cash.

Hydra Marketplace Operations Stem Back to 2015

Hydra is a Russian-language dark web marketplace that has been active since at least 2015. It opened as a competitor to RAMP (Russian Anonymous Marketplace), which was a dark web marketplace that dominated the Russian drug market at the time. RAMP was notorious for taking down its competition by conducting DDoS attacks and reporting names and IP addresses of competitor operators to authorities. RAMP was opened in September 2012 and **shut down in July 2017** as part of a Russian law enforcement operation. Following the takedown, Russian cybercrime users migrated towards Hydra.

Hydra entered the market with a business model related to its mythical namesake: "if you cut off one head, two more will grow back in its place." Hydra acts as a host for sellers to set up and run their own narcotics shops, with Hydra profiting as the intermediary for all executed transactions conducted. Hydra allows for a greater level of anonymity and security for users and provides "professional quality" deliveries. The marketplace had established direct suppliers in China, enabling it to build a reputation as a marketplace known for its large quantities of cheap synthetic drugs.

Due to its reputable narcotics products and wide range of sellers, Hydra serves an increasingly diverse buyer clientele, ranging from larger wholesale narcotics buyers to individual recreational users, including students and young people. Hydra's seamless arbitrage system, along with easy payment options and strong, enforced encryption, further grew its popularity among cybercriminals. After a DDoS attack closed RAMP for several months, Hydra emerged as the leading Russian dark web marketplace for the illicit trade of narcotics.

Hydra operates exclusively in former Soviet Union countries

AZERBAIJAN

MOLDOVA

TAJIKISTAN

UKRAINE

KAZAKHSTAN

RUSSIA

BELARUS

UZBEKISTAN

KYRGYZSTAN

ARMENIA

There Are At Least 11 Identified Hydra Operators

Hydra is too large to be run by a handful of operators as is likely operated by several dozen people, with clearly delineated responsibilities. Flashpoint has identified at least 11 administrators and operators, known by the following forum aliases:

RESIDENT	ADMIN_DEV
FATALITY	GLAVRED
IRONMAN	SATOSHI NAKAMOTO
DEUS	OBSERVER
HANDSOME JACK	ADMIN
ENTER	

Hydra Suffers Rare Downtime, Blamed on Coronavirus

Due to the alleged difficulties of delivering narcotics amid pandemic-related restrictions, Hydra sellers received a service administrator message on March 31, 2020, reading:

"Dear shops. Due to the imposed restrictions in a number of areas, you need to temporarily remove your products from the online displays, to which access will be limited in the near future. Do not create additional difficulties for yourself, our customers, and the moderators. After restrictions are removed, you can put them back." - HYDRA administration

Изоляция городов

Уважаемые магазины. В связи с вводимыми ограничениями в ряде субъектов, вам необходимо временно снять с витрины клады, доступ к которым ограничен или будет ограничен в ближайшее время. Не создавайте дополнительных сложностей себе, покупателям и модераторам. После снятия ограничений, выставите их обратно. Администрация HYDRA

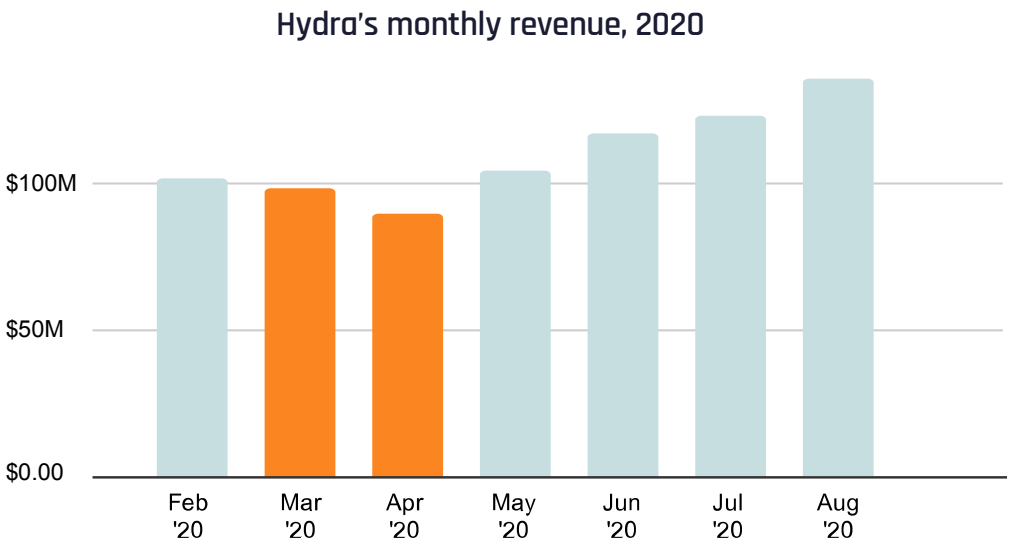
Message sent to Hydra sellers on March 31, 2020

Illicit Goods Available on Hydra

- Marijuana
- Stimulants
- Euphoretics
- Psychedelics
- Entheogens
- Ecstasy
- Dissociatives
- Opiates
- Chemicals/Constructors
- Pharmacy
- BTC cash-out
- SSH, VPN
- Digital goods
- Documents
- Cards, SIM
- Design and graphics
- Outdoor advertising
- Counterfeit money
- Devices and equipment
- Anabolics/Steroids
- Partnership and franchise
- Work
- Other
- Cannabinoid

Blockchain Analysis Shows Transaction Dip During Hydra Hiatus

Using blockchain analysis, we can see how the March slowdown appears to check out, correlating with a temporary blip in Hydra's monthly revenue returns for March and April. Monthly revenue dropped from over $100 million worth of cryptocurrency in February 2020 to $99.5 million in March and $90.7 million in April.



Aspirations of Global Expansion Postponed Indefinitely

Rumors that at least some Hydra operators want to see market operations expand globally have lingered for a few years now. When Hydra went down in March 2020 due to COVID-19, some Russian government sources claimed that the coronavirus explanation was a coverup as Hydra operators used the downtime to "complete the development of services for the drug trade in Europe." Although the timing is somewhat protracted, these government officials were ultimately proven right several months later, on September 1, 2020, when the Hydra website announced it would begin global services of its illicit marketplace.

Now in mid-2021, this global expansion has yet to materialize. Operators ultimately signaled that the major rollout would be postponed indefinitely due, again blaming externalities and operational limitations associated with the ongoing pandemic.

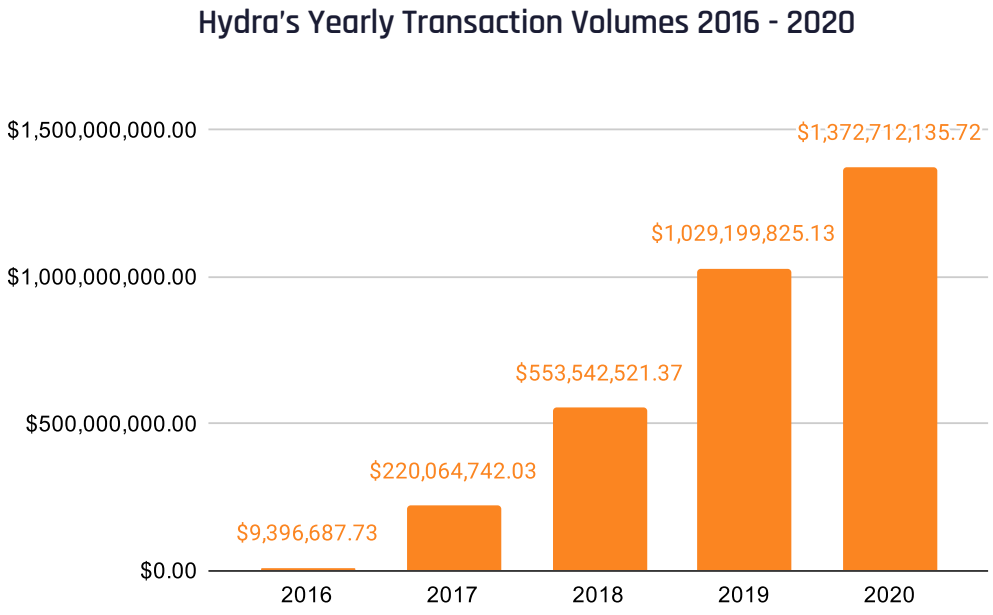
Hydra Market on a Blistering Growth Trajectory

Since its inception in 2015, the Hydra market has flourished. Flashpoint has seen consistent, perpetual growth of Hydra seller posting volumes and user activity engagement frequency.

Blockchain analysis shows that Hydra's revenue has risen dramatically over the last five years, from under $10 million worth of cryptocurrency in 2016 to over $1.3 billion in 2020.

624%

Hydra's transaction volume growth in just three years, 2018-2020.



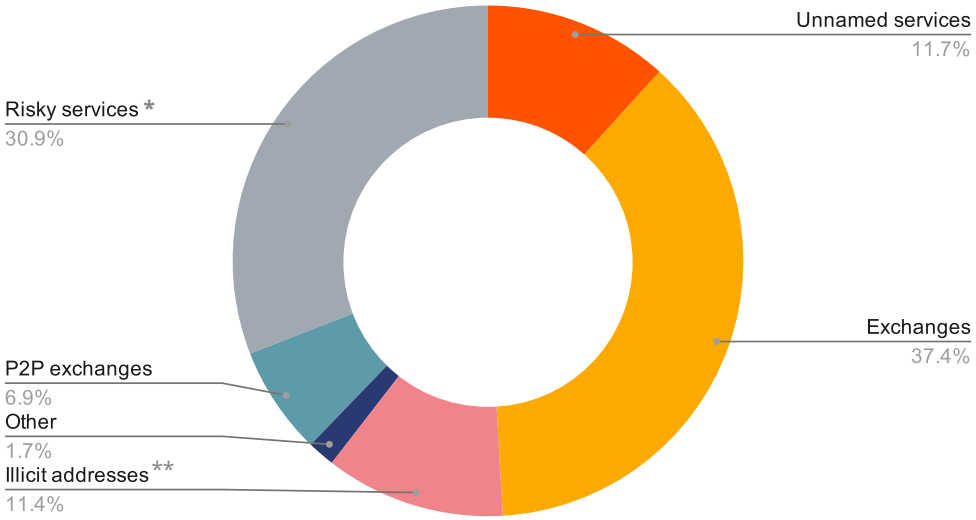
Russian and Other Regional Exchanges and Services Dominate Hydra

Hydra primarily transacts with addresses at cryptocurrency exchanges, both sending and receiving large sums from them. We show some of this activity in the Chainalysis Reactor graph below.

Regional Exchanges and Payment Services Are the Primary Source of Outbound Seller Withdrawals

While we can't name any of them specifically, we can say that Hydra transacts with a diverse array of exchanges. Many are classified by Chainalysis as high-risk, meaning they have lax or non-existent compliance programs, particularly around KYC procedures. However, some of them are more mainstream exchanges, the vast majority of whom's transaction volume is associated with legal, safe activity. In addition, the vast majority of funds sent out of Hydra are routed to accounts and services that primarily operate and service patrons based in Russia.

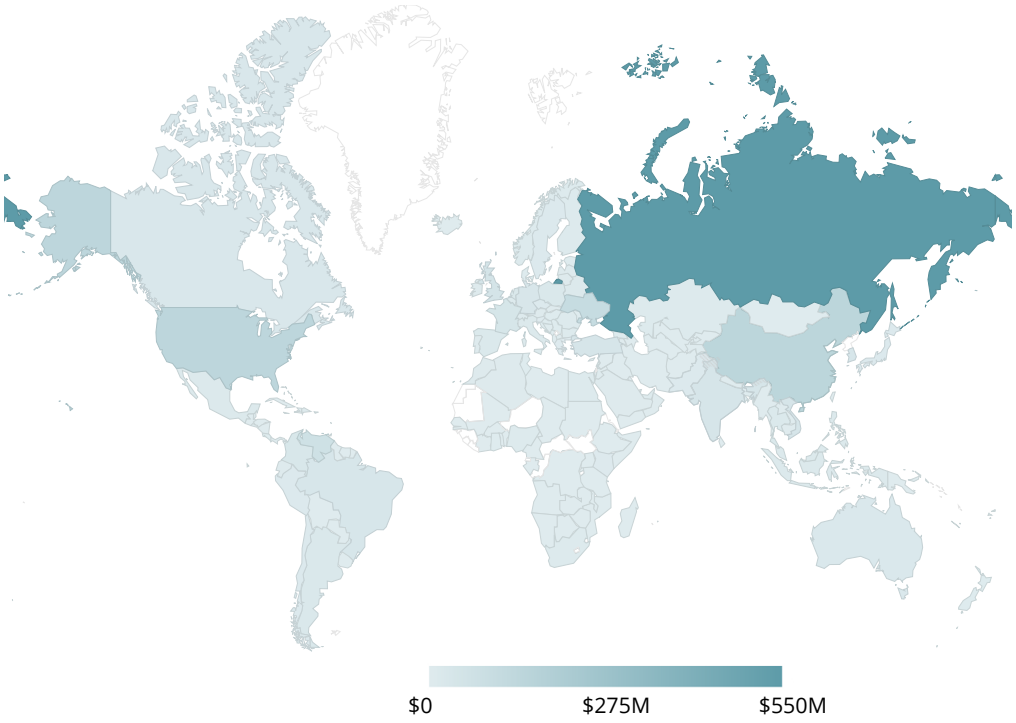
Destination of funds sent from Hydra



*** "Risky services"** refer to the exchanges, mixers, gambling platforms, and other payment services that Chainalysis observes during its research, determining those that are "high-risk" by the regulatory adherence, security, and reliability of their associated systems, infrastructure, operational jurisdiction, and participating entities and users.

**** "Illicit addresses"** refer to eWallets and online accounts holding cryptocurrency funds that are either owned by known cybercriminal actors or groups or linked directly to the illicit activities or transactions themselves (e.g., proceeds of narcotics sales on cybercriminal marketplaces).

Destination Country of Funds Leaving Hydra, Jan 2020 to Feb 2021

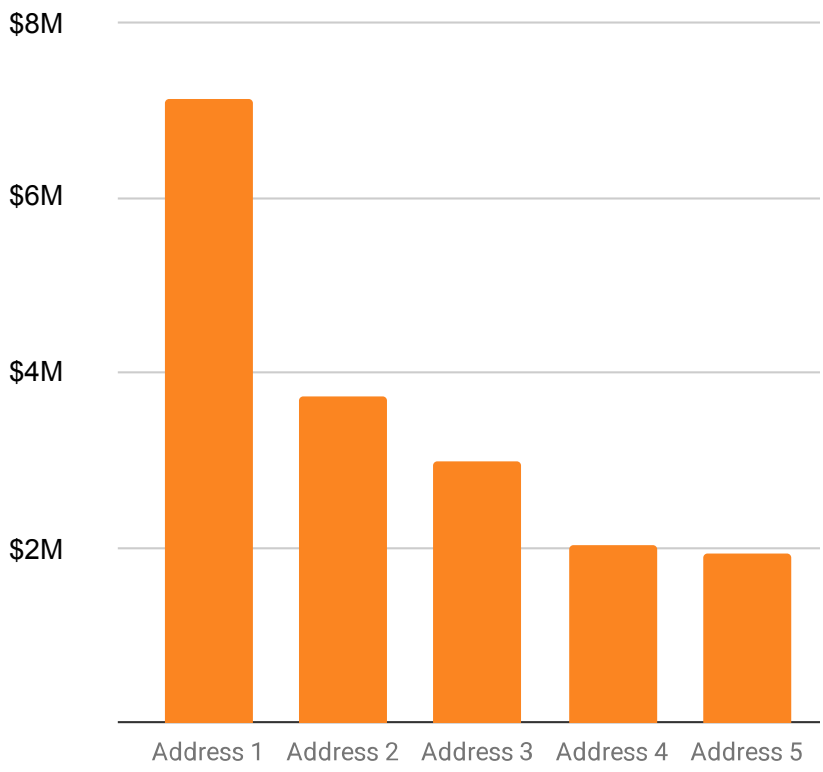


High-Volume Deposit Addresses Further Obfuscated by OTC Brokers and Nested Services

Based on Hydra transaction activity with one of the top mainstream cryptocurrency exchanges on the market today, we can see that some of the largest deposit addresses (by total funds received) have total transactions of more than 1,000 unique deposit addresses and transaction values upwards of $7 million USD worth of cryptocurrency. Other large, mainstream exchanges have similarly active transaction activity and volumes with individual deposit addresses.

The actors behind these deposit addresses remain largely anonymous and unknown. Based on Chainalysis research, however, it's likely that many of them are likely nested services—such as over-the-counter (OTC) brokers—to further obfuscate the cryptocurrency money trails of these funds.

Top 5 Exchange Deposit Addresses by Hydra funds Received



Address	Time Active	Number of transfers	% received from illicit sources
Address 1	05/31/2020 - present	1,026	30.1%
Address 2	08/18/2020 - 03/09/2021	24	16.5%
Address 3	11/25/2019 - 03/28/2021	2,467	11.6%
Address 4	01/22/2021 - present	97	91.3%
Address 5	01/21/2020 - 03/01/2021	4,215	26.2%

Navigating Hydra: Why Money Trails Go Dark

After a few years of rapid growth, Hydra underwent significant changes stemming back to at least July 2018. Based on Flashpoint Intelligence, Hydra administrators at this time in 2018 imposed new restrictions disabling the ability for buyer users to transfer cryptocurrencies out of the marketplace. Sellers also faced similarly tight restrictions, only able to withdraw cryptocurrencies and funds from their electronic Wallets (eWallets) into Russian fiat currency. While certainly restricting for buyer users on Hydra, the new limitations introduced in 2018 were more onerous on Hydra sellers.

While we explore the reasons for such changes in more detail in the following sections below, the actual impetus for instituting these new rules still remains largely unknown. What we can say objectively is that:

1. Whether or not intended, the elimination of more widely-used cryptocurrencies and eWallets for sellers, along with the heavily restricted seller withdrawal mandates, primarily benefit the remaining few entities, individuals, and services allowed.
2. Hydra's sanctioned fiat currencies, eWallets, and payment services all appear to be largely—if not exclusively—Russian-based.
3. Given the regional scope of Hydra's operations and its permitted services and currencies since 2018, visibility into the trail of financial transaction records is meaningfully impaired. Upon completion of the buyer portion of the transaction, the money trail goes dark as more veiled, in-region financial operators and service providers manage the sellers' finances and convert cryptocurrency withdrawals into difficult-to-trace Russian fiat currencies as the next step in the financial chain.

Justification for 2018 eWallet Restrictions Fails to Mention Clear Ulterior Interests

At the time of the announcement of new seller restrictions in July 2018, Hydra admins justified the crypto moratorium as a necessary security measure to protect their users against account takeovers and phishing attacks. As with all messages from DWM operators, however, they must be taken with a massive grain of salt.

In some rarer instances, Flashpoint sees DWMs prioritizing platform reliability and user experience—such as with the once-dominant carding marketplace Joker's Stash—but it's far more common for DWM operators to hold ulterior, self-serving motives at heart rather than their users' best interests. In this case, who stands to benefit most from these policy changes? The Hydra operators and the remaining sanctioned sellers, entities, and service providers can still operate and complete transactions under these stricter guidelines.

Seller Restrictions Appear to Benefit Russian-Based Entities and Users

Sellers on Hydra seeking to withdraw their earned—albeit illicit—sales proceeds must first convert the funds into accepted "fiat" (i.e., official, government-backed currencies) through exchange services and electronic wallets, which are strictly limited to Russian rubles. Sellers face similarly heavy restrictions imposed on their eWallets, permitting only Russian-owned or -approved payment providers, such as Qiwi or Yandex Money (aka, "YooMoney" or "ЮMoney").

Lastly, since at least 2019 according to Flashpoint Intelligence, Hydra sellers must also meet two further requirements to withdraw funds: a) They must establish a reliable sales track-record with more than 50 completed transactions on Hydra, and b) They must maintain eWallet balances of USD-equivalent $10,000 or more. In other words, Hydra sellers would not be able to withdraw the funds that they (illicitly) amassed themselves from their completed sales if they don't yet have at least 50 total sales transactions or if their eWallet balance totals remain under USD-equivalent $10,000, whether or not they hit the 50 transaction mark.

Seller Restrictions

To withdraw funds, sellers need **50+** transactions and **$10,000+** eWallet balance

Seller withdrawals must be exchanged into **Russian fiat currency**

Offshoot Market Emerges for Hydra Seller Access

Given the restrictions on withdrawing money from Hydra, some threat actors have begun to sell options and techniques that circumvent these controls in listings on illicit marketplaces outside of Hydra. These offerings vary, with Flashpoint most commonly observing either the sales of compromised seller accounts or "partnerships" in which the paying actor coordinates transactions via an approved Hydra seller.

Dark Web Marketplace Listings for Hydra Seller Accounts Start in 2018

Listings that sell Hydra Seller Accounts go back as far as August 2018, according to Flashpoint Intelligence. For example, in November 2018, the cybercriminal user dubbed "Ololosha" on the Carding Xram Telegram group chat was attempting to sell a privileged Hydra seller account from the Moscow Region of Russia that was registered in 2018 and had an established track record with over 80 completed sales transactions and held full transfer rights. But in 2019, that Hydra seller account appeared to be shut down as other cybercriminals pointed to evidence of the removal of its transfer privileges. Hydra administrators have repeatedly warned users that they can fall victim to phishing scams and that threat actors can easily withdraw funds from seller accounts using third-party exchange services.

New Unique Listings Offer Hydra Market Access In Lieu of Accounts

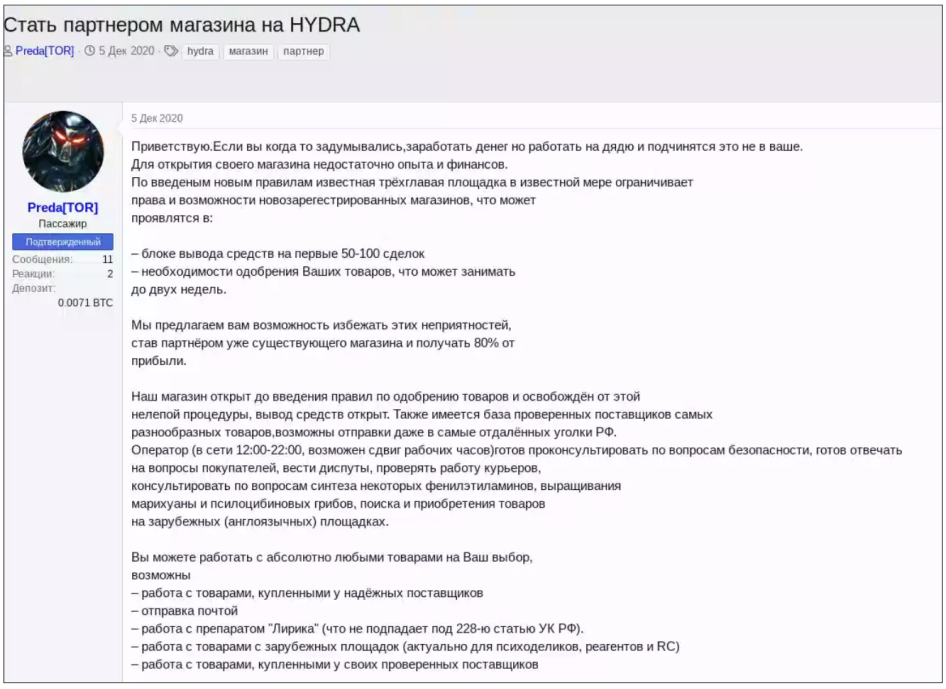
In December 2020, on the RuTor Marketplace, Flashpoint Intelligence observed the user dubbed "Preda[TOR]" post a new listing purportedly selling access to Hydra seller accounts that circumvented Hydra policies and enforcement controls. In Preda[TOR]'s listing, he described the offering as a "partnership," enabling the outsider sellers to gain access to Hydra by registering as couriers for preexisting, approved shops.

Preda[TOR] acknowledged in the listing that the outsider sellers wouldn't have their own dedicated Hydra seller accounts, but nonetheless, the proposed technique would enable them to sell their own wares to Hydra buyers and receive cryptocurrency as payment skirting the fiat withdrawal conversion process—all for a 20 percent cut of their profits.

More Listings for Hydra Seller Accounts Are Sprouting Up in 2021

As we begin to head into mid-2021, Flashpoint Intelligence continues to observe more cybercriminal listings on RuTor and other DWMs, offering up Hydra seller access:

- On March 17, 2021, a user "Гоша Куценко" of the RuTor Marketplace offered their store on Hydra for sale for $2,500 USD.
- On March 1, 2021, a user "Мост" of the RuTor Marketplace offered their well-established narcotics store on Hydra for sale for $10,000 USD.


Стать партнером магазина на HYDRA

Preda[TOR] · 5 Дек 2020 · hydra магазин партнер

Preda[TOR]
Пассажир
Подтвержденный
Сообщения: 11
Реакции: 2
Депозит: 0.0071 BTC

5 Дек 2020

Приветствую.Если вы когда то задумывались,заработать денег но работать на дядю и подчинятся это не в ваше.
Для открытия своего магазина недостаточно опыта и финансов.
По введеным новым правилам известная трёхглавая площадка в известной мере ограничивает
права и возможности новозарегестрированных магазинов, что может
проявлятся в:

– блоке вывода средств на первые 50-100 сделок
– необходимости одобрения Ваших товаров, что может занимать
до двух недель.

Мы предлагаем вам возможность избежать этих неприятностей,
став партнёром уже существующего магазина и получать 80% от
прибыли.

Наш магазин открыт до введения правил по одобрению товаров и освобождён от этой
нелепой процедуры, вывод средств открыт. Также имеется база проверенных поставщиков самых
разнообразных товаров,возможны отправки даже в самые отдалённых уголки РФ.
Оператор (в сети 12:00-22:00, возможен сдвиг рабочих часов)готов проконсультировать по вопросам безопасности, готов отвечать
на вопросы покупателей, вести диспуты, проверять работу курьеров,
консультировать по вопросам синтеза некоторых фенилэтиламинов, выращивания
марихуаны и псилоцибиновых грибов, поиска и приобретения товаров
на зарубежных (англоязычных) площадках.

Вы можете работать с абсолютно любыми товарами на Ваш выбор,
возможны
– работа с товарами, купленными у надёжных поставщиков
– отправка почтой
– работа с препаратом "Лирика" (что не подпадает под 228-ю статью УК РФ).
– работа с товарами с зарубежных площадок (актуально для психоделиков, реагентов и RC)
– работа с товарами, купленными у своих проверенных поставщиков

RuTor User Post Selling Hydra eWallet Withdrawal Workaround in December 2020

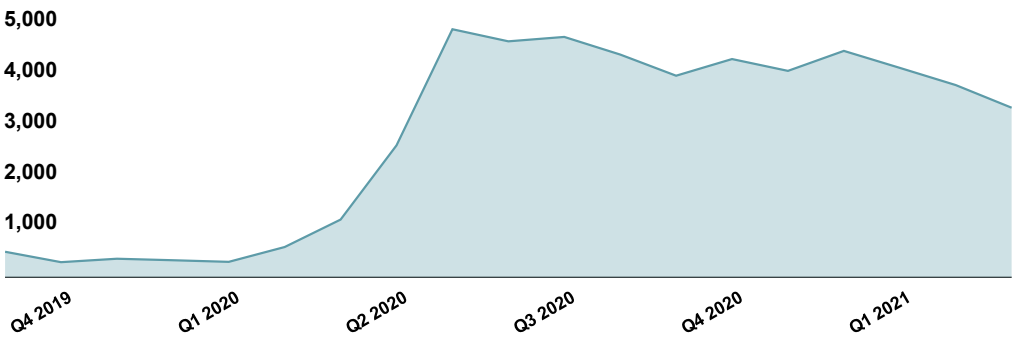
"Hidden Treasure" a Cash-Based Withdrawal Workaround

Due to increased security measures and identification requirements by cryptocurrency exchanges, Hydra users are increasingly seeking alternative methods to extract their funds away from the prying eyes of compliance and regulatory examiners. In particular, the workaround dubbed "hidden treasure" (клад, or klad in Russian) is quickly gaining traction among Hydra cybercriminal circles. This physical withdrawal technique calls upon customer buyers to hire designated couriers ("kladmen") to bury cash underground in vacuum-sealed bags within specific agreed-upon locations for the sellers to dig up later. Once the physical cash is secured in the physical hands of the seller, they then complete the narcotics sale, either burying the sold products or shipping them out as has been done historically.

Hidden Treasure "Kladsmen" Jobs Increasingly Lucrative

As cybercriminal interest in "hidden treasure" schemes mount, so too rises the demand for the roles and services of the requisite courier "kladsmen." According to April 2021 ads on the forum "legalrc," cybercriminals were offering kladsmen upwards of 30,000 rubles (US$400) per day or contracting them for a full week at US$1,000r more. Previously, the use of kladsmen was limited to rarer instances of hiding narcotics underground, to be picked up by clients later on.

Mentions of "Buried Treasure" ("клад") technique on Forums "legalrc" and "WayAway"



More Industries at Risk as Hydra Expansion Looms

Given the sustained and continued growth of Hydra, as well as its largely clandestine approach to its operations and financial controls, there are several important considerations for security, risk, and fraud teams to address. More specifically, security and risk professionals should evaluate the following implications and their associated risks to determine how to best safeguard their unique organizations from Hydra-facilitated cybercrime.

1. Money laundering trails to Hydra are difficult, near impossible, to trace. While the illicit trade of narcotics is problematic in and of itself, the lack of transparency in financial transactions and forced fiat conversions via regional and more veiled payment processors present further challenges for monitoring and combating cybercrime on Hydra.

2. Hydra's expansion to other illicit trades may endanger more industry sectors. While Hydra currently supports the selling of many illicit goods and services, its strongest market, by far, remains narcotics sales. Should Hydra continue to grow, its support of other cybercriminal trades will likely expand along with it. Flashpoint **continues to predict** that we will see the decline of specialty cybercriminal shops and marketplaces as they're replaced with bigger, one-stop cybercrime shops. Whether or not organizations are concerned with the narcotics trade, they should keep close watch of Hydra activity should other illicit markets, such as card fraud or data breach sales, begin to take off.

3. The longer Hydra runs unscathed, the more apparent its regional influence. Despite hits to other well-established Russian-speaking cybercriminal communities and marketplaces in recent months—including **Joker's Stash**, **Verified**, and **Maza**—enforcement scrutiny and competitor chicanery have so far eluded Hydra. This may be a mere coincidence, or it could indicate that Hydra is more resilient to oscillating geopolitics and law enforcement efforts. The longer Hydra operates without major disruption, the more realistic the latter option becomes, with regional financially incentivized stakeholders the only plausible explanation.

Turn Insight into Action with Flashpoint

Schedule a demo with Flashpoint to see where your organization, your assets, and your personnel may be exposed online. Equipped with organization-specific threat intelligence, leading organizations worldwide use Flashpoint to turn threat intelligence into security action: Lock down compromised accounts, identify insider threats, recover exposed strategic and sensitive data, and more.

Credits

Thank you to Flashpoint Contributors Andras Toth-Czifra and Vlad Cuiujuclu and to Chainalysis Contributors Kim Grauer and Henry Updegrave. Special appreciation to the entire Flashpoint Intelligence Analyst team for their ongoing threat research and analysis efforts that make reports like this possible.

ABOUT FLASHPOINT

Flashpoint is the globally trusted leader in actionable threat intelligence for organizations that demand the fastest, most comprehensive coverage of threatening activity on the internet. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across private and public sectors to help them rapidly identify threats and mitigate their most critical security risks. Flashpoint is backed by Georgian Partners, Greycroft Partners, TechOperators, K2 Intelligence, Jump Capital, Leaders Fund, Bloomberg Beta, and Cisco Investments.

For more information, visit **www.flashpoint-intel.com** or follow us on Twitter at **@FlashpointIntel**

ABOUT CHAINALYSIS

Chainalysis is the blockchain analysis company. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 50 countries. Our data platform powers investigation, compliance, and risk management tools that have been used to solve some of the world's most high-profile cyber criminal cases and grow consumer access to cryptocurrency safely. Backed by Accel, Addition, Benchmark, Ribbit, and other leading names in venture capital, Chainalysis builds trust in blockchains to promote more financial freedom with less risk.

For more information, visit **www.chainalysis.com**