Examining Russian-language Cybercriminal Marketplaces

digitalshadows.com/blog-and-research/examining-russian-language-cybercriminal-marketplaces/

May 18, 2021

Our blogs have covered the fate of numerous cybercriminal marketplaces on the clear, deep, and dark web over the years. Our research has uncovered several factors determining a platform's chances of success, including market share, USP, security, and convenience. We've mainly focused our attention and threat intelligence articles on the rise and fall of several English-language marketplaces. Still, we thought the Russian-language scene also deserved some of our attention. In this blog, we'll dive into why there's traditionally been a focus on forums over marketplaces in the Russian-language cybercriminal underground and take a look at some active and defunct platforms that have made an impact on the scene.

Why a focus on forums in the Russian-language cybercriminal scene?

Threat intelligence looking at Russian-speaking threat actors tends to focus on cybercriminal forums, and for a good reason, Russian-language forums are characterized by their remarkable longevity. Unlike the many English-language forums that pop up for a few months before disappearing under suspicious circumstances, big names like Exploit and XSS have been around—in one incarnation or another—for decades now.

Exploit and XSS's popularity shows no sign of waning:

- Membership numbers and thread counts are consistently increasing.
- The sites' commercial sections are a hive of activity.
- The forum communities are engaged in the future of the platforms.

They're even starting to gain global media attention due to the presence of representatives of several well-known ransomware groups.

For those Russian-speaking threat actors looking to transact on a platform using a different format, the options are much more limited, especially if they're interested in digital goods rather than the narcotics that most marketplaces sell. Many once-prominent automated vending card sites (AVCs) focusing on carding, such as Rescator, have fizzled out. Several automated platforms selling other wares, such as the RDP shop xDedic, are no longer active.

Notable Russian-language marketplaces

MarketMS (Now Defunct)

The most significant disruption of the Russian-language marketplace scene in recent years—and a great example of the struggle Russian-language platforms face trying to break into this arena—was MarketMS.

Current and former members of the forum team at Exploit established MarketMS in a pre-alpha working stage in January 2015. Its founders included Exploit's former administrator (who now runs XSS). MarketMS tried to differentiate itself from the drugs-focused marketplaces by focusing on digital goods such as databases, compromised accounts, malware, exploits, and counterfeit documents. The website described itself as an "automated safe trading platform" and promoted its high-security levels, simple interface, and escrow-guaranteed trading to distinguish itself from competitors. Despite its unique offering, excluding illicit substances to the benefit of technical goods and services, and its founders' impressive pedigree, MarketMS closed down operations in December 2019 citing "a lack of financial profits." Yet another example of a failed marketplace, but somewhat of a surprise, especially considering its due diligence to evade law enforcement and instill trust in its user base. MarketMS's failure highlights how difficult it is for Russian-language marketplaces to attract enough custom to survive.

HYDRA

Launched in 2015, the site is notable for its large user base and evading takedown by law enforcement agencies.

Hydra is likely successful due to three factors:

1. FSU-based drop locations
2. A diversified offering of goods/services
3. User-friendliness and discipline

FSU-based drop locations—Hydra's vendors' use of secret drop locations around Russia and other former Soviet Union (FSU) nations to which they dispatch their products. This means buyers can only collect purchases if they are based in—or willing to travel specifically to—one of these countries. Drops are not unique to HYDRA; they are commonplace across marketplaces serving many language communities. But the method does make it much harder for Western law enforcement agencies to successfully carry out tracking operations, a scourge that has led to the downfall of many an English-language marketplace.

Another potential determinant in HYDRA's profitability, which ran to USD 1.2 billion between June 2019 and July 2020 according to the Blockchain analysis company Chainalysis, might be the diversity of items offered for sale. Although HYDRA is most well-known for its mainstay of narcotics, many vendors sell digital goods and services, leading to a vibrant and mixed cybercriminal scene on the site. At first glance, HYDRA's digital goods sections may appear unimpressive when compared to the sheer volume of drugs-based content. There are

only four dedicated subsections: hacking, databases, information extraction, and “other.” But looks can be deceptive. Listings offering items such as fake passports, SIM cards, counterfeit cash, VPN subscriptions, and cashing out services can all be found within these sections.

HYDRA is no cybercrime boutique; the lack of malware for sale may be disappointing for a sophisticated hacker. But it might be the case that the absence of specialist hacking content on HYDRA is intentional. After all, HYDRA made a name for itself by conquering the drug trade market, not attracting hackers. Focusing on digital goods other than malware may provide reasonable cover from the security services, ensuring that the site lies just beneath the threshold that might attract unwanted attention from law enforcement agencies’ cybercrime departments.

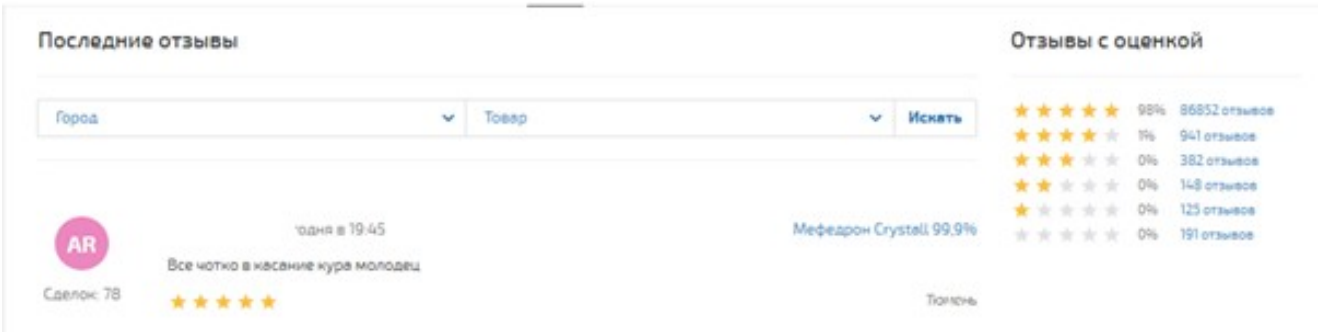

Figure 1. Hydra’s review system for users

HYDRA’s digital goods sections reflect considerable supply and demand, feature steady prices, and offer ease of access. The majority of digital goods on HYDRA cost less than RUB 10,000 (USD 134). Goods in this price range include stolen accounts and digital wallets; information extracted from stolen documents, IDs, and databases; as well as document forgery services. These aren’t necessarily one-time transactions either: One listing can be distributed to multiple buyers, especially if a service is being offered.

Lastly, while the volume and diversity of goods on HYDRA are significant, the platform’s user-friendliness and functionality likely contribute to its smooth operation. Reviews are simple on HYDRA, allowing a potential customer to make a quick, well-informed purchase decision. There is a starred rating system, an important feedback metric for evaluating a seller’s reputation. While this is not out of the ordinary for a cybercriminal marketplace, HYDRA implements the system seamlessly, ensuring would-be buyers gain instant insight into vendors’ legitimacy.

HYDRA operates and enforces a notably strict set of rules, including a ban on the sale of fentanyl, weapons, assassination services, viruses, and pornography. We have repeatedly observed that users on Russian-language forums are much more likely to obey regulations than those on English-language counterparts, which tend to be characterized by a lack of discipline. This replication of common Russian-language forum conformity on a rarer Russian-language marketplace might also contribute to HYDRA’s longevity.

RAMP (Now Defunct)

At its height, RAMP was competing with the English-language marketplace AlphaBay to become Silk Road's successor after the latter fell victim to a law enforcement operation (see Figure 2). RAMP was profitable, had considerable market share, and didn't appear to be the target of Western law enforcement agencies.

Yet RAMP appears to have felt threatened by emerging competition in the form of HYDRA and attempted a hostile takeover, mobilizing hackers to launch DDoS attacks against HYDRA. HYDRA responded to RAMP's attack in kind with its own flurry of botnet and DDoS attacks, at which point RAMP began to unravel. RAMP's constant shutdowns cost the marketplace tons of money and led to internal spats. The shutdowns also likely led to much of RAMP's once-loyal customer base carrying out a mass exodus to HYDRA.

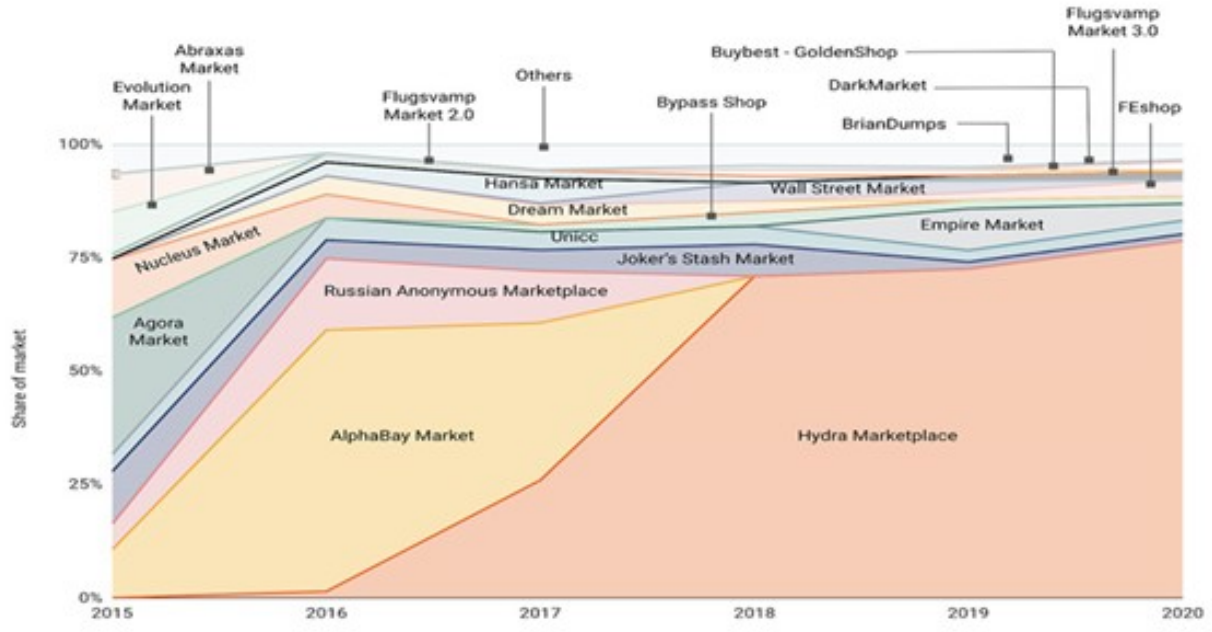

Figure 2. Darknet markets by share of total market size from 2015-2020 (Source:Filtermag)

MEGA

Established in 2015, MEGA is another Russian-language marketplace catering exclusively to Russian-speaking users. DNStats claims that the isolation and smaller market share that results from this lack of English-language content may lead to cheaper prices than on other dark web marketplaces, depending on the product.

Although replete with illicit substances, MEGA offers a sizeable inventory of digital goods such as databases, carding data, counterfeit-related products, and ready-to-use hacking software.

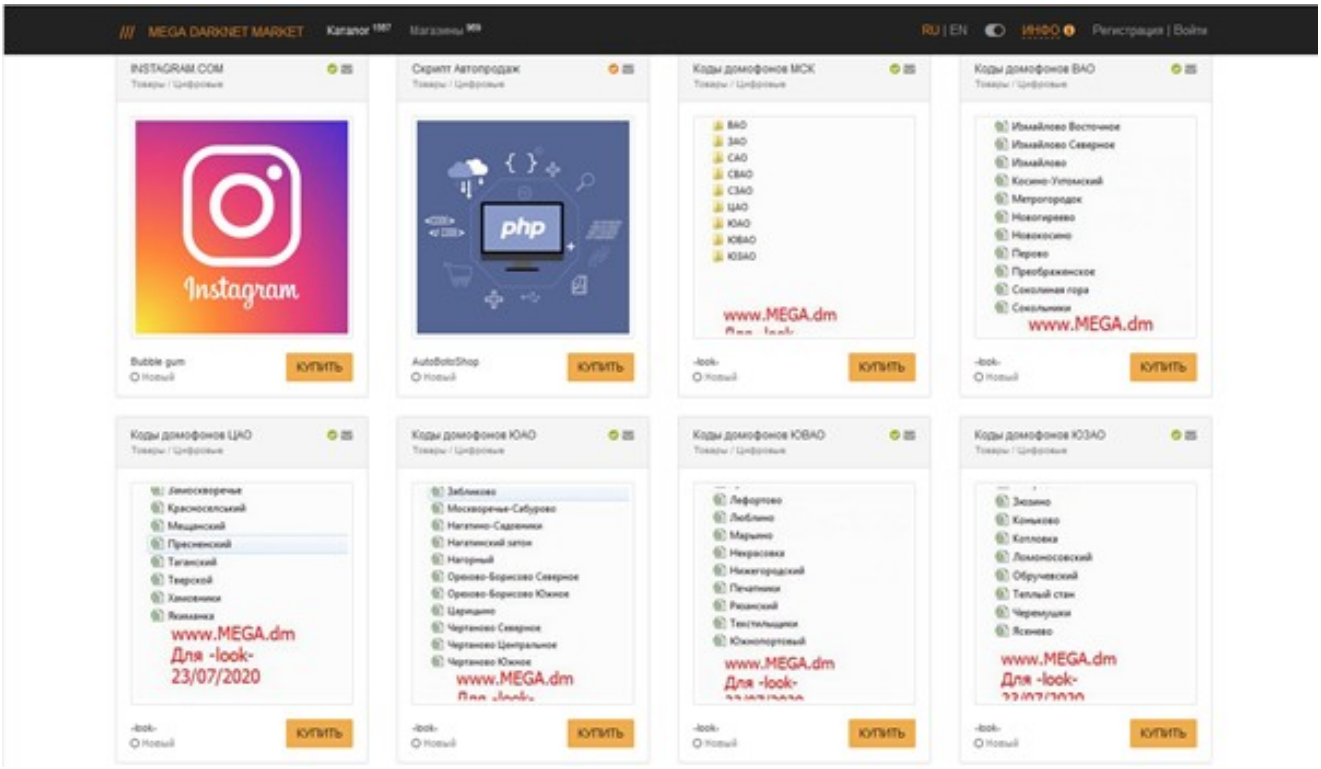

Figure 3. Digital goods for sale on MEGA

BlackMart

Founded in 2017, BlackMart started as a Russian-language cybercriminal marketplace with a focus on the narcotics trade, but also managed a sizeable digital goods inventory. Vendors often advertised their shops on BlackMart's associated forum, RuTOR. However, BlackMart's tenure as a Russian-language narcotics hub was short-lived when the platform abandoned narcotics and shifted focus to carding, document forgery, money transfers, counterfeit money, and sales of various electronics. Moreover, the marketplace's adaptation to an English-language format reflected limitations in the Russian-language marketplace scene and a need to reach a global audience. Since reinventing itself, the marketplace advertises international shipping and sees moderate levels of activity.

Tochka (Now Defunct)

The multi-language marketplace Tochka/Point previously began operations in 2015 selling a variety of physical and digital goods and services. The marketplace's diversified offerings across eight different languages reflected an international approach. Although it focused on narcotics, stolen data, malware, credit cards, bank accounts, and social engineering tutorials were all available for sale. The reason for Tochka's disappearance isn't entirely clear, but it's evident that it left many disgruntled customers in its wake who accused Tochka of committing an exit scam. It lasted only four years, finally going offline in November 2019.

WayAway

After its founding in 2009, WayAway was a staple Russian-language forum with marketplace-like features and even served as a gateway to other Russian-language platforms.

In fact, HYDRA's creation can be attributed to a partnership that was formed between WayAway and Legal RC, another Russian-language forum, in order to compete with RAMP. HYDRA is listed as a WayAway Partner on the forum's footer along with links to the marketplace, and it appears that most of WayAway's user base has moved on to greener pastures at HYDRA. WayAway now serves as a relic for one of the oldest Russian-language darknet forums and sees intermittent levels of activity, often with users returning just for nostalgic purposes.

RuTOR

RuTOR is another excellent example of a Russian-language forum with marketplace-like features. RuTOR has an entire marketplace embedded within its forum where users exchange hacking services, SIM cards, forged documents, weapons, and other cybercriminal services.

The forum's association with BlackMart likely attracts users to the site looking for additional offerings and a sense of community. With more than 120,000 registered members, RuTOR markets itself as the "main black market forum." However, its inflows are nowhere near that of HYDRA's, and it lacks a centralized checkout function and rating system. Instead, users are forced to default to targeted advertisements, hoping to attract buyers that will reach out by commenting on a thread or through private messenger.

Concluding thoughts on Russian-language marketplaces

Despite similarities in functionality and content, Russian-language marketplaces are different from their English-language counterparts in many ways. English-language marketplaces abound, towering over Russian-language marketplaces at least in quantity. There is plenty of competition on the English-language side, which can be attributed to geographical diversity, with English as a lingua franca serving multiple buyer geographies. But for the Russian-speaking cybercriminal scene, HYDRA continues to reign supreme over the rest of its competition.

Digital Shadows will be watching closely over the coming months and years to see how the Russian-language marketplace scene develops – whether HYDRA can retain its crown or whether another upstart like MarketMS will come along to try and shake things up.

If you'd like to learn more about monitoring the dark web for potential leaked databases, compromised accounts, exploits, target attacks and more get a free copy of our*Dark Web Monitoring Solutions Guide*here. Alternatively, you can access a constantly updated threat

intelligence library providing insight on this and other cybercriminal-related trends that might impact your organization and allow security teams to stay ahead of the game. Get a free seven-day test drive of SearchLight here.

Tags: Cybercrime / cybercriminals / Dark web / dark web monitoring / Exploit / Marketplaces / russia / russian / russian language / threat intel / XSS