

 BRIEF

RUSSIAN THREAT ACTORS RESPOND TO MILITARY MOBILIZATION ZEROFOX INTELLIGENCE

B-2022-10-18a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Cyber Threat Actor Activity

October 18, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 1:00 PM (EDT) on October 10, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Russian Threat Actors Respond to Military Mobilization

Executive Summary

Deep and dark web actors have begun to broker methods to circumvent Russia's partial military mobilization¹ announced in late September, including options for dodging the draft. Some of the services are likely attempts at scams or honeypots, and in some cases, it is unlikely the actors are capable of delivering what they have promised. However, the speed with which these methods began to appear in underground channels demonstrates anxiety amongst the Russian-speaking threat actor community, which is openly discussing this topic in forums that usually ban such rhetoric.

Details

As of September 21, 2022, general discussions on the vetted Russian-speaking xss[.]is community suddenly switched from the topic of the United States announcing rewards for any actionable information on cyber actors threatening the country to the partial mobilization announced in the Russian Federation. Previous posts on the thread featured opinions about the United States and the European Union (EU) being desperate in light of current economic and cyber threat developments. However, the mobilization announcement changed the tone of the forum completely, and threat actors began asking for help and soliciting various services to assist their scared, Russian-speaking counterparts.

Analyst Commentary

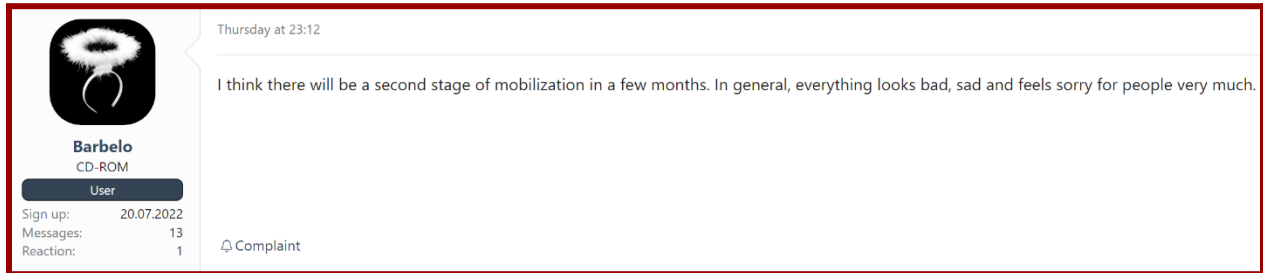
Significant forum activity and response were observed in Russian-speaking threat actor forums after President Vladimir Putin's announcement in late September that 300,000 troops would be called into service. Multiple conjectures were made ranging from a

¹

[hXXps://www.cnbc\[.\]com/2022/09/21/russia-ukraine-war-putin-announces-partial-military-mobilization.html](https://www.cnbc.com/2022/09/21/russia-ukraine-war-putin-announces-partial-military-mobilization.html)



possible second stage of mobilization upcoming in a few months to draft evasion techniques to work opportunities with the military in order to avoid active service.



Barbelo changes the topic on xss[.]is (translated)

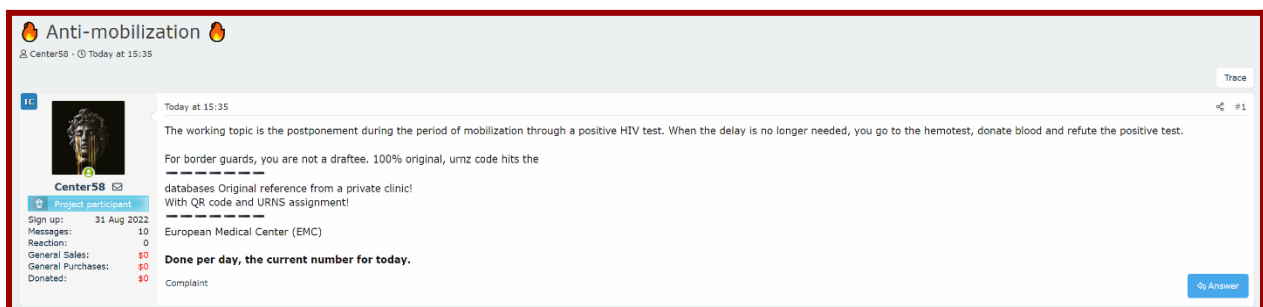
Source: ZeroFox Intelligence



Threat actor advises dodging draft by combining fake arm breaking with fake confirmation by a surgeon

Source: ZeroFox Intelligence

In some cases, threads were observed being promptly closed by forum administrators due to increasing political chatter on the topic of mobilization. However, in other cases, significant back and forth occurred regarding various techniques for draft dodging, including obtaining a postponement of military service due to a positive HIV test.



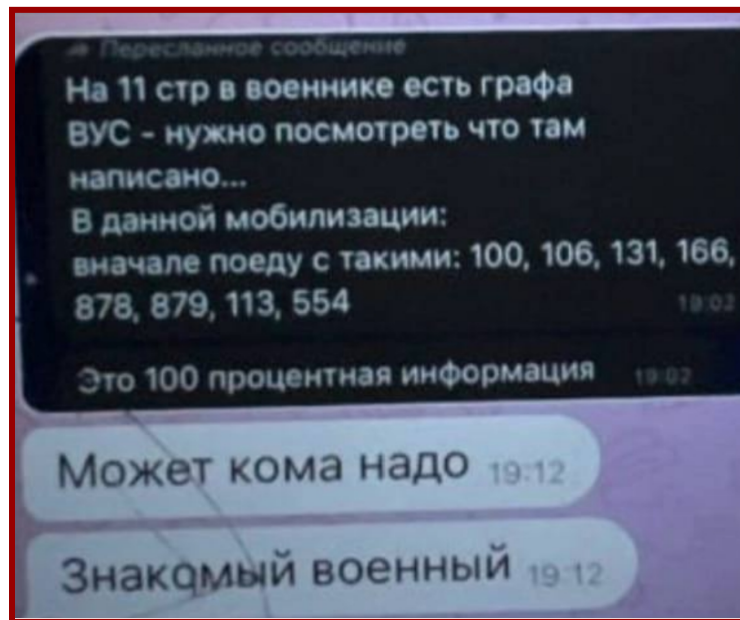
User "Center58" offers positive HIV tests to draft dodgers at wwh-club[.]io/(translated)

Source: ZeroFox Intelligence

In another chat, a user claimed that a specific column in the military ledger pertaining to each Russian male who has completed military service dubbed „BYC“



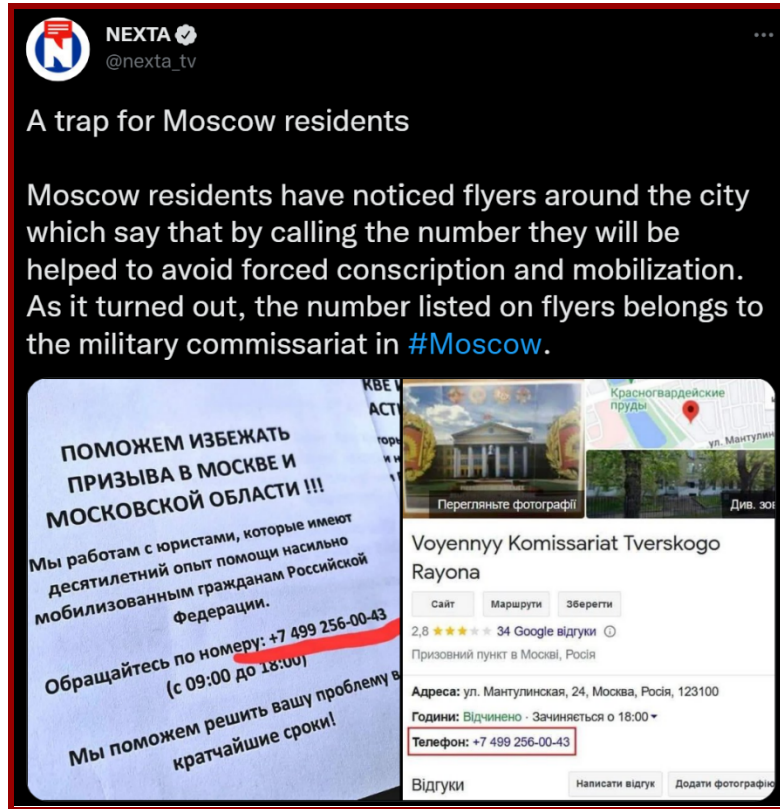
(„Военно-учётная специальность“ or „Declared military specialization“) is indicative of whether a person is going to be mobilized. Allegedly, holders of BYC numbers beginning with 100, 106, 131, 166, 878, 879, 113, and 554 are currently being mobilized. While the usability of such data may be limited, it does provide information on attempts at document forgery on the part of Russian draft dodgers. If the BYC number correlation is accurate, the post likely indicates that sensitive military policy information has been leaked to the Russian public.



User “hools67” giving clues to mobilization efforts

Source: ZeroFox Intelligence

This thread clearly indicates that escaping mobilization at the moment is difficult for Russian-speaking actors to achieve and that attempts to exploit naïve draft dodgers are likely underway in the Russian-speaking deep web ecosystem. Suggestions for draft dodging in these forums may represent sophisticated honeypot campaigns that could be reported to the Russian Ministry of Defense. An example of this was already identified shortly after mobilization was announced; flyers around Moscow offering residents a telephone number to contact for legal help to avoid the draft were observed in the city. It was later determined that this was a trap and that the number on the flyer actually directs callers to the Moscow Military Commissariat.



NEXTA tweet describing Moscow draft-dodging flyers

Source: [hXXps://twitter\[.\]com/nexta_tv/status/1572621878874996736](https://twitter.com/nexta_tv/status/1572621878874996736)

Recommendations

ZeroFox Intelligence expects steadily-increasing disorder in the Russian segment of the deep web as the situation in the Russian Federation deteriorates, which is likely to impact cyber operations. It is well-known that this segment is the largest one in the cyber underground, and the entire cyber threat landscape might be subjected to increasingly significant changes; organizations should expect a shift in behavior and targeting as a result. In addition, organizations with physical operations or sales in EU states, particularly those with close geographic or cultural ties with Russia, should remain prepared for low-level cyber threat activity such as DDoS attacks, as this type of activity still allows Russia to maintain plausible deniability.



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.