

 BRIEF

KILLNET INVOLVEMENT IN DARKNET MARKETS

ZEROFOX INTELLIGENCE

B-2022-10-19a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Cyber Threat Actor Activity

October 19, 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 10:00 AM (EDT) on October 17, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Killnet Involvement in Darknet Markets

Executive Summary

Killnet has been one of the most vocal threat actor groups since the start of Russia's invasion of Ukraine. The pro-Russian hacktivist collective, identified as early as January 2022, initially sold Distributed Denial of Service (DDoS) tools as part of a subscription model. After the Ukrainian Anonymous hacking collective expressed public support for Ukraine in February 2022, Killnet declared war on the collective and changed from being a cybercriminal service provider to a hacktivist group. Killnet is dissimilar to well-known, Russia-sponsored Advanced Persistent Threat (APT) groups, as the group is not as efficient; unsophisticated; lies about targets and intentions, as well as about its success in attacking targets; and manipulates its audience regarding the help the group receives from alleged sympathetic actors. Killnet is most successful at spreading pro-Russian propaganda and drumming up attention for its purported activities—which are also being propagated by actors on darknet drug market Solaris Market, among others.

Details

Recently, significant chatter has been observed with regard to threat actors on Solaris Market promoting Killnet activities. Solaris Market is a relatively new Russian darknet drug market established in 2022. It works in the same way as the now-defunct Hydra Market did; all types of drug vendors create outlets on the market and pay fees to maintain their presence. The relationship between Killnet and Solaris Market is not known to be ideologically motivated; instead, it is likely an agreement between two lowly-regarded groups of so-called hackers in the underground economy: drug vendors and DDoS attackers.

Analyst Commentary

Solaris Market is the successor to Hydra Market. After Hydra was shut down at the end of March 2022, Rutor remained the largest Russian deep web drug market. Killnet has



attacked Rutor continuously since August 2022, claiming ideological motivation. After Rutor was suppressed, Solaris began developing as the largest entity in the Russian-speaking deep web drug ecosystem. The way in which Solaris aids Killnet is unclear, but it most likely simply pays fees for Killnet's DDoS services.

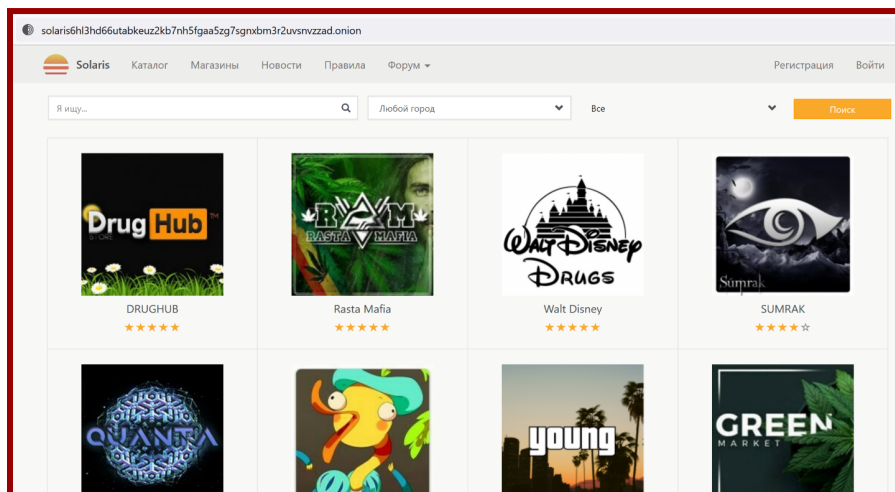
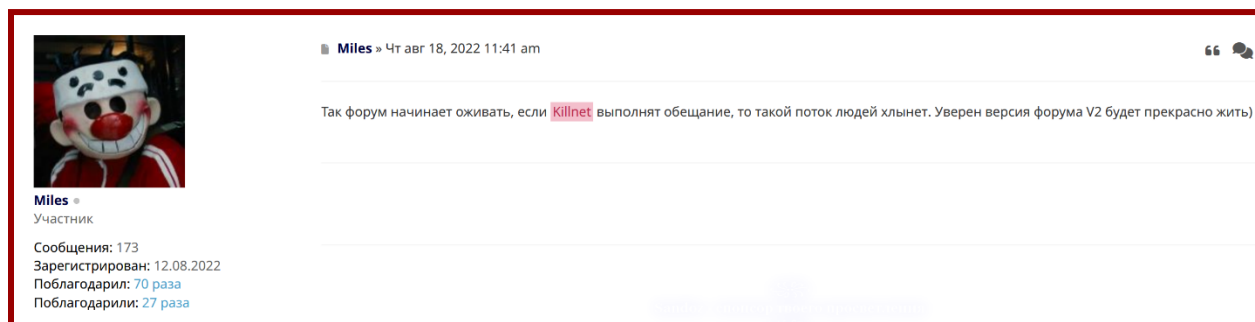


Figure 1: Solaris Market

Source: ZeroFox Intelligence

As with many other darknet markets, Solaris Market also runs its own community board. ZeroFox has observed several conversations revealing Killnet's connection with Solaris Market. For example, on August 18, 2022, well-regarded threat actor "Miles" claimed that the users would pour into Solaris' forum if Killnet fulfilled its promise.



Threat Actor Commentary Regarding Solaris and Killnet Connection

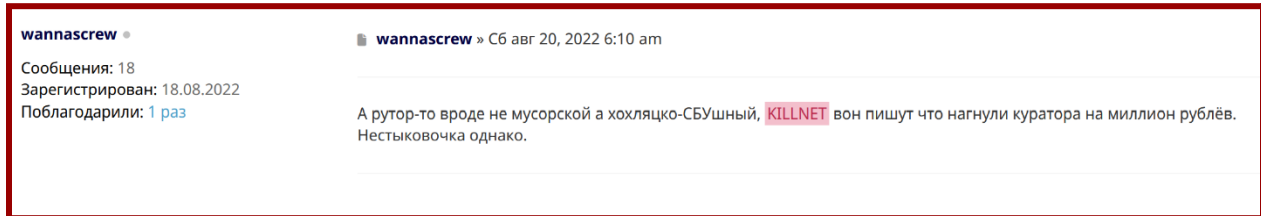
Translation: "So the forum starts to come alive, if Killnet keeps their promise, then a [great] influx of people will pour in. I'm sure the V2 version of the forum will live great :)"

Source: ZeroFox Intelligence

There was no clarity on what Killnet had promised until another thread on the forum was examined. On August 20, 2022, Solaris board threat actor "wannascrew" claimed that the Rutor drug market is run by the Ukrainian Security Service (SBU) and thus was being targeted by Killnet. The claim of SBU's involvement is completely unsubstantiated; previous observations on Rutor seemed to suggest that it is run by



Russian actors. Nevertheless, Killnet was able to scam Rutor's admin for one million rubles.



Claim Regarding SBU Connection to Rutor

Translation: "And the rutor seems to be not a Musorian one, but a Khokhlyatsko-SBU one, KILLNET write that they bent the curator for a million rubles. Inconsistency however:"

Source: ZeroFox Intelligence

An official statement by Killnet was also referenced to support the theory that its incentive in attacking Rutor is ideological; Killnet has professed that Rutor was attacked because it was selling drugs to Russian citizens. Killnet has also claimed that 50 percent of the revenue it received from the Rutor admin was sent to help orphanages in the Russian Federation.

In August 2022, Killnet confirmed that its campaign against various Rutor sites was in motion. Killnet disclosed that Rutor-related domains were under attack, claimed that it had not forgotten about Rutor, and alleged that the attacks were continuous. However, Rutor still rendered normal at that time and was considered fully functional—indicating that Killnet's campaign was not successful, despite the hacking group's aggressive rhetoric on Telegram.

DDoS attacks against darknet markets are nothing new, and their usual purpose is to hinder the online business of a competitor. In Killnet's case, the competitor is Rutor—and the affiliated market that benefits from attacking Rutor is undoubtedly Solaris. Thus, Killnet's attacks on Rutor, although technically ineffective to date, likely have nothing to do with helping orphanages or fighting the SBU; they are instead an indicator of yet another clash between darknet markets for a larger portion of Russian-speaking drug buyers. The announcement about help from Solaris on "Killmilk's" (a founding member of Killnet) channel last week is likely nothing more than an acknowledgment of teamwork between Solaris and Killnet: Killnet attacks Solaris' competitors, and Solaris most likely pays Killnet for the services provided. Since Killnet excels at propaganda, the public justification for its attacks against Rutor, as well as the public claims of benefitting from Solaris' support, is very likely manipulated to create a certain public impression. ZeroFox Intelligence ascertains that it is unlikely that Killnet will obtain any significant operational advantages at this point.



Recommendations

Organizations should ensure that monitoring is configured on Killnet's Telegram channels for any mentions of their domains or any other organizational mentions and expect that low-level cyber activity, such as DDoS attacks, will continue to be Killnet's main attack vector. Organizations should work to reduce their attack surface area, closely monitor network traffic, and utilize load balancers to limit the potential for DDoS attacks.



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.