



| Brief |

The Underground Economist: Volume 4, Issue 20

B-2024-12-06a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

December 6, 2024

Scope Note

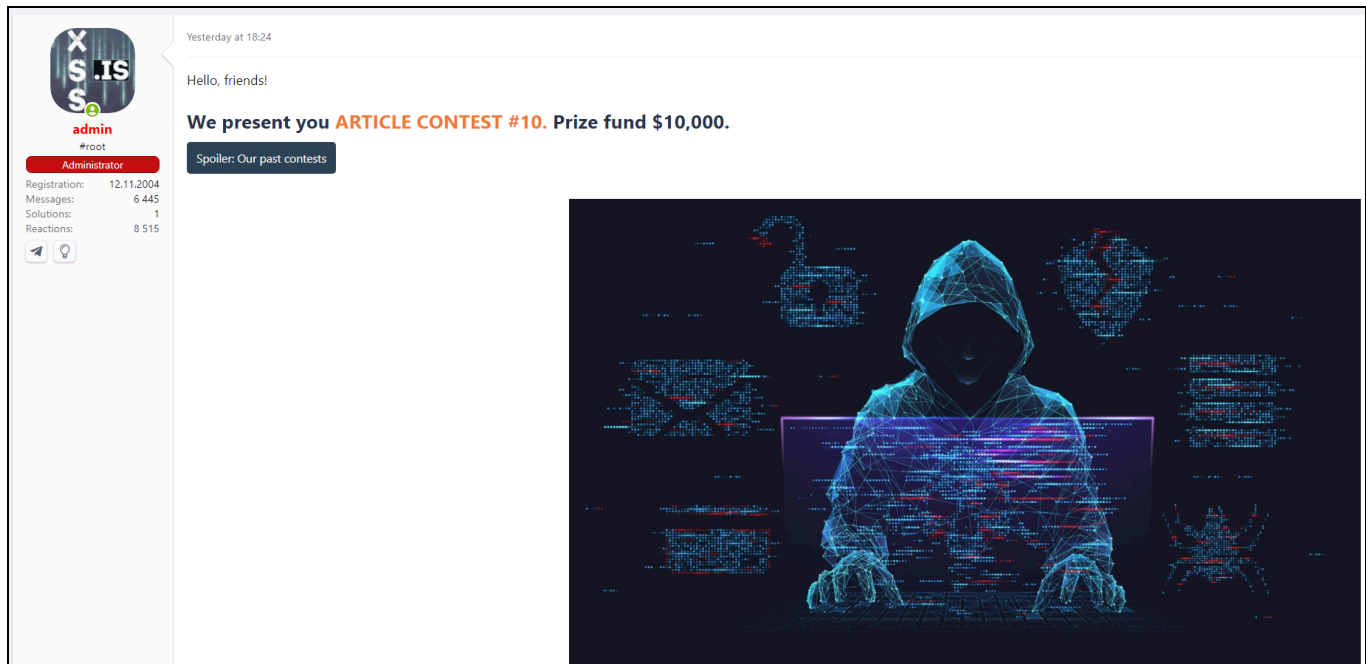
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 9:00 AM (EST) on December 5, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 20

| Dark Web Forum Launches New Iteration of Malicious Article Contest

On December 1, 2024, the administrator of the Russian-speaking dark web forum xss announced the launch of the tenth iteration of the forum's long-standing cyber crime "Article Contest." The competition invites forum members to contribute articles describing tactics, techniques, and procedures (TTPs) that can be employed to conduct various illicit activities. Submissions are to be made before February 1, 2025, after which voting procedures to determine the winner will commence.

- The xss forum has a well-established precedent for conducting competitions, the expectations of which vary each iteration. Since 2018, these contests have sparked significant interest among threat actors and served as a conduit for disseminating valuable knowledge on attack vectors and TTPs.
- Earlier in 2024, the forum hosted the [//XSSware] competition, whereby participants proposed various malicious software solutions. Proposals centered heavily around obfuscation methods, detection evasion, and the impeding of defender attribution efforts.



Admin announcement of new Article Contest on xss

Source: ZeroFox Intelligence

A list of accepted “directions” (appearing to be synonymous with topics) was also provided. These largely coincide with those provided in preceding iterations, with the exception of “AI for blackhat”, which had not previously been included. This inclusion is almost certainly reflective of a cross-threat landscape interest in AI-powered malicious tools, which are being increasingly leveraged to bolster more traditional attack techniques and evade cyber defense infrastructure. Furthermore, a section related to electronic warfare has been removed; there is a roughly even chance that this topic was previously included primarily as a result of increased interest in such TTPs at the onset of the ongoing Russia-Ukraine war.

Accepted directions:

- Web vulnerabilities
- Attacks on networks and working with networks
- Attacks on wireless networks
- Software Vulnerabilities / Exploitation
- Malware and everything connected with it
- Cracking/Reversing
- Hardware hacking
- Cryptography
- Messengers and Social Networks
- Technical anonymity (TOR/Proxy/Socks/VPN/Servers)
- Forensics (criminology)
- Spam, Traffic, Installs
- Phishing
- APT attacks
- AI for blackhat
- Coding and development in blackhat
- Cryptocurrencies/smart contracts

Specification of accepted topics

Source: ZeroFox Intelligence

There is a likely chance that general enthusiasm for and participation in this year's competition will be lower than that previously observed. The prize fund stands at USD 20,000—half the amount observed in the last iteration. The competition's sponsor this year, "posterman", is also unknown, having only made one previous post in the forum which has since been deleted. In contrast, the sponsor for the previous iteration, "Alan Wake", is a ransomware operator with a positive reputation in the forum.

Article requirements:

- We accept original articles. ChatGPT, copy-paste, rewriting **are prohibited**. Violation - disqualification.
- The article can be posted only on XSS.is.
- Minimum number of characters - 7000.
- The article must have **PRACTICAL** application to the forum topic. Theory without practice is not interesting. No need to write fictitious stories. No need to copy-paste official manuals or write boring theory.
- **Recipe for the perfect article** (read **!** carefully **!**): theory + practice + real-life examples + your opinion/experience + thematic analysis of the material + screenshots + video.
- Adequate formatting, spelling and punctuation.
- "Water" and empty talk under the guise of articles are not accepted.

Competition guidelines

Source: ZeroFox Intelligence

There is a likely chance that reduced enthusiasm for the competition stems from uncertainty and reduced levels of trust present in many Russian-speaking deep and dark web (DDW) forums ZeroFox observed throughout the year. However, the competition

is still likely to result in the development and submission of new attack techniques and software, some of which may result in an increased threat to global organizations.

| Distributed-Denial-of-Service Offering Launches

On December 1, 2024, the actor “miyako” posted in the cybercrime forum BreachForums announcing the launch of a new Distributed-Denial-of-Service (DDoS) offering named DarkStresser, which will become available at darkstresser[.]net. Miyako, who has a positive reputation in the forum, claimed that the new service is privacy-focused and will offer buyers the capability to conduct disruptive attacks with “unmatched power and performance.” According to the advertisement, DarkStresser is able to deliver over “1 gbps” of malicious traffic to the target network.

- Despite appearing to be advertised as one gigabit per second (Gbps), Miyako very likely intends to advertise DarkStresser’s delivery capability as 1 gigabyte (GBps) per second. While this is not amongst the highest observed traffic volumes in DDoS attacks, its availability as a service by an actor that carries a positive reputation indicates a significantly increased threat.
- Miyako did not specify any privacy features associated with DarkStresser or how it delivers “unparalleled anonymity” as specified in the advertisement. There is a roughly even chance, however, that some potential buyers will be skeptical of the surface web [.]net domain.

A positive response was quickly posted in the thread by another actor with a positive reputation, “Venom”, who vouched for the service and wished miyako success with sales.



DarkStresser.net

Privacy-focused, powerful, and secure.

 Unparalleled anonymity and privacy.
Information encrypted & payment in most famous crypto-currencys accepted.

Unmatched power and performance, with more than +1gbps of power.

 Most low prices of the market for good quality.

 support@darkstresser.net  www.darkstresser.net

We open the 5th of December, 2024! join our telegram channel for more updates:
t.me/darkstressersu

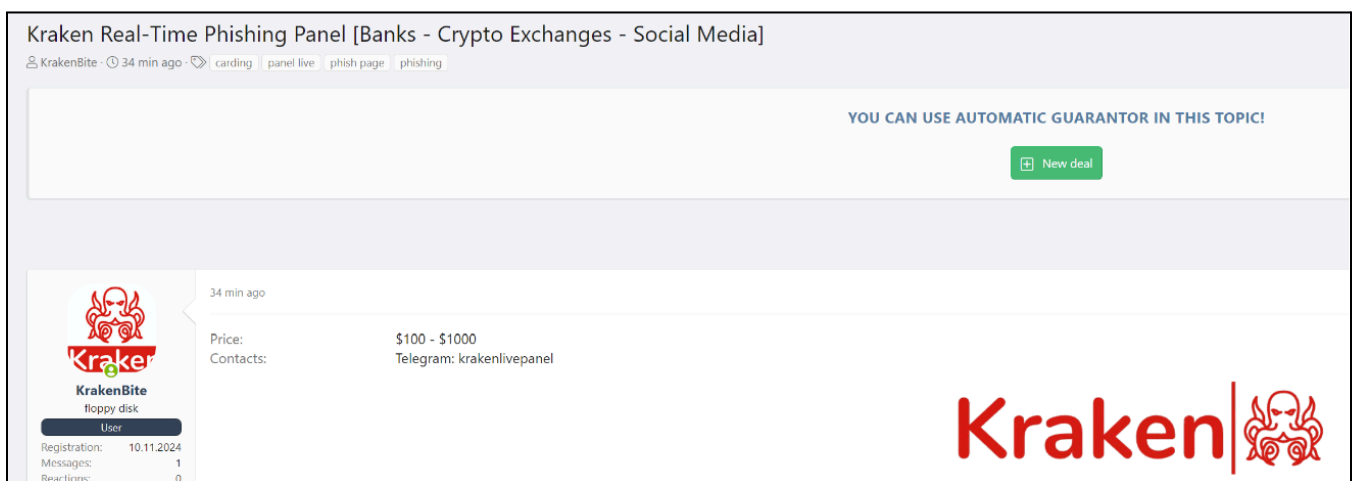
BreachForums post by miyako, advertising new DarkStresser DDoS service

Source: ZeroFox Intelligence

DDoS services are regularly advertised both in Russian-speaking DDW forums and encrypted instant messaging (IM) platforms such as Telegram. However, many of them are associated with actors perceived as not credible, and some appear to be attempts to scam potential customers. Given that DDoS attacks are a popular technique amongst a wide array of threat actors that are intent on causing disruption to their victims' networks, DarkStresser is very likely to generate interest amongst actors seeking reliable and privacy-focused services.

| New Phishing-as-a-Service Platform Announced

On November 24, 2024, actor “KrakenBite” posted in the Russian-speaking dark web forum xss, where they have an untested reputation. KrakenBite’s announcement unveiled a new web-based, live phishing panel that grants access to 75 malicious domains, which allegedly target organizations such as banks, cryptocurrency exchanges, and social media platforms. While exhaustive features were not specified, KrakenBite alleged that the service offers real-time customization capabilities.

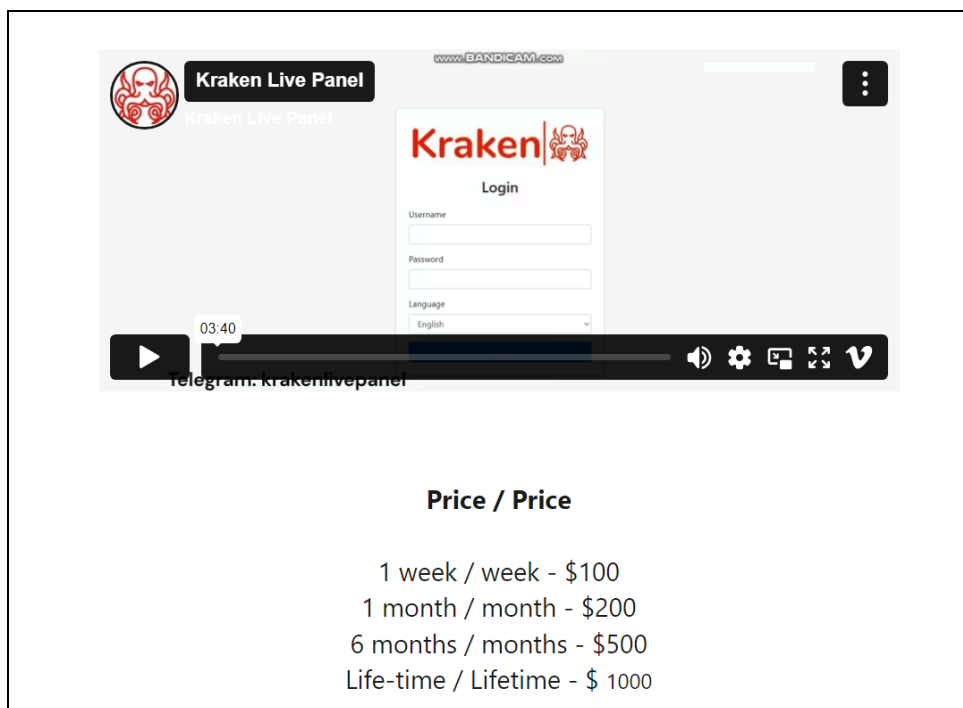


KrakenBite’s post on xss advertising new phishing panel

Source: ZeroFox Intelligence

- The ability to customize phishing pages in real time can enable an attacker to dynamically alter the page in response to victim behavior. This can increase the domain’s perceived legitimacy by reacting to inputs and facilitate further compromise via the bypassing of security protocols. While this feature is not unique amongst phishing kits offered in DDW marketplaces, it remains uncommon.

The advertised price for the service ranged from USD 100 for one week to USD 1,000 for lifetime access, with prices allegedly inclusive of hosting and domain maintenance costs. After purchasing, a customer is required only to distribute malicious phishing links, which are shortened by a built-in tool to increase legitimacy and decrease the chances of being obstructed by security features.

**KrakenBite's embedded demonstration video and pricing structure***Source: ZeroFox Intelligence*

In the thread, KrakenBite embedded a video file providing a brief demonstration of the phishing panel in use, alongside a list of financial organizations against which ready-to-use malicious domains can be deployed. KrakenBite claims that they are willing to receive payment via escrow services and also offers “tests” for certain customers. While it is unclear how the tests would take place, both the offer to provide proof of functionality and the acceptance of payments via escrow are indicative of increased threat actor and service reliability.

KrakenBite's phishing kit is very likely reflective of the evolving phishing-as-a-service (PhaaS) threat landscape. As individuals and organizations continue to exhibit increased cyber hygiene and threat awareness, and deploy effective defenses such as multi-factor authentication (MFA) and know-your-customer (KYC) protocols, threat actors seeking to monetize malicious social engineering services are required to continuously offer capabilities able to maintain attack success rates deemed high-payoff.

| Alleged Zero-Day Vulnerabilities Announced for Sale

On November 24, 2024, untested actor “n4pster” announced in the Russian-speaking dark web forum Exploit that they have three zero-day vulnerabilities for sale. N4pster claimed that these are newly developed, have been tested, and have not been previously sold; they also emphasized that transactions would be conducted through an escrow service.

- A zero-day vulnerability refers to a security flaw that is unknown to the manufacturer or vendor. Such vulnerabilities pose a significantly elevated threat to users of the affected software or hardware, as no mitigation yet exists. This leads to an increased chance of successful compromise by malicious threat actors.

N4pster included a page displaying results from vulnerability scans, which supposedly highlight the number of vulnerable endpoints. Some details were also provided on the alleged vulnerabilities:

- A Preauthentication Remote Code Execution (RCE) that grants root access to Control-WebPanel (CWP). N4pster specified an asking price of USD 150,000.
- A Preauthentication RCE that grants root access to Uniview DVR. N4pster specified an asking price of USD 80,000 and claimed a target base of approximately 1.7 million devices.
- A Preauthentication RCE that targets Raisecom products. N4pster specified an asking price of USD 45,000 and claimed a target base of approximately 197,000 devices.



New 0days up for sale

By n4pster, 3 hours ago in [Software] - malware, exploits, bundles, crypts

Post by n4pster advertising alleged zero-day vulnerabilities

Source: ZeroFox Intelligence

There is a likely chance that this advertisement is a scam attempt, as zero-day vulnerabilities are often leveraged in such activity and are typically targeted at inexperienced actors frequenting DDW marketplaces. While the offer to transact via escrow slightly increases the credibility of both n4pster and the sale, sales involving uncommon goods such as zero-day vulnerabilities often result in dispute—and in some cases, a buyer not receiving the intended product. If the actor is credible, however, the finding is very likely reflective of an increased threat to the highlighted software.

| Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant MFA, and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

| Appendix A: 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.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%