ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 5, Issue 22

B-2025-11-06b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

November 6, 2025

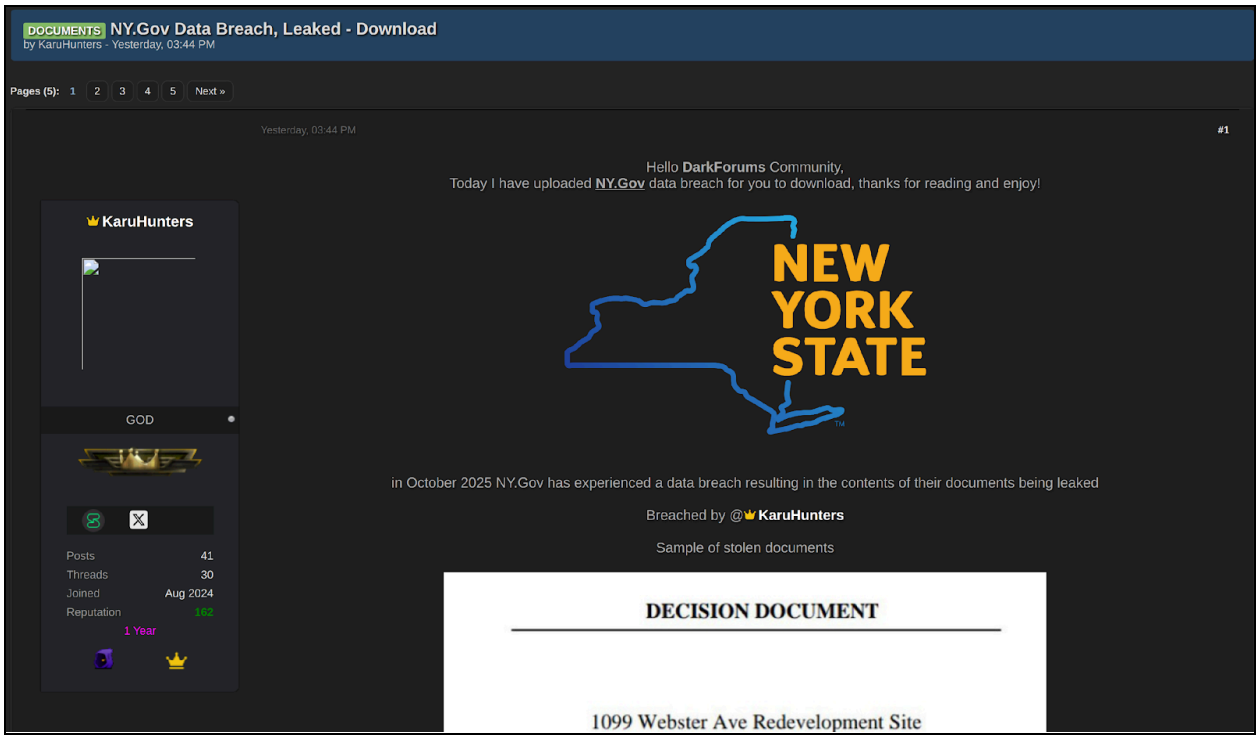
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot 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 10:30 AM (EST) on November 6, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | The Underground Economist: Volume 5, Issue 22

| New York State Website Breach and Leaked Documents

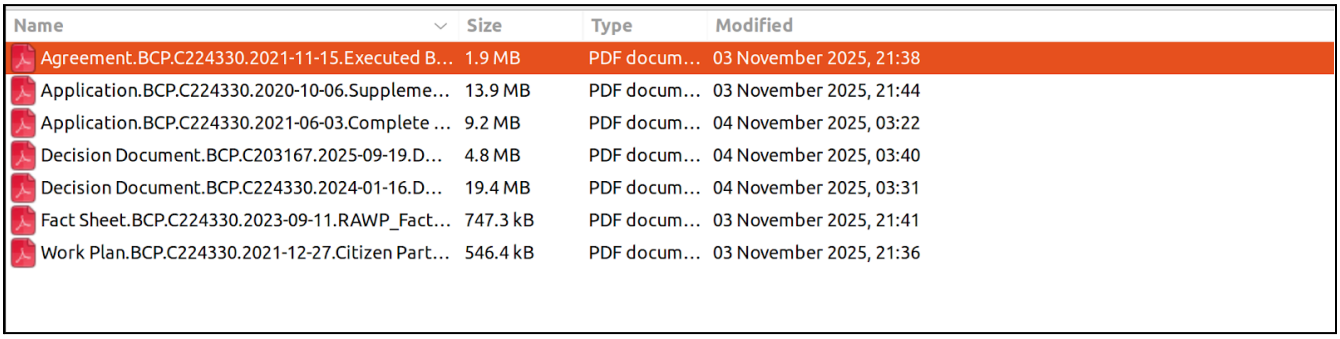
On November 4, 2025, an actor using the alias "KaruHunters" shared an allegedly recent breach that resulted in the actor gaining illicit access to and leaking several documents from New York state's website (ny[.]gov) on the deep web forum DarkForums. The actor included sample images of the stolen documents, one of which appeared to be a decision document prepared by the Division of Environmental Remediation of the New York State Department of Environmental Conservation.

- The leaked file list allegedly includes one agreement, two applications, one fact sheet, one work plan, and two decision documents.



KaruHunters' original DarkForums post

Source: ZeroFox Intelligence



Name	Size	Type	Modified
Agreement.BCP.C224330.2021-11-15.Executed B...	1.9 MB	PDF docum...	03 November 2025, 21:38
Application.BCP.C224330.2020-10-06.Suppleme...	13.9 MB	PDF docum...	03 November 2025, 21:44
Application.BCP.C224330.2021-06-03.Complete ...	9.2 MB	PDF docum...	04 November 2025, 03:22
Decision Document.BCP.C203167.2025-09-19.D...	4.8 MB	PDF docum...	04 November 2025, 03:40
Decision Document.BCP.C224330.2024-01-16.D...	19.4 MB	PDF docum...	04 November 2025, 03:31
Fact Sheet.BCP.C224330.2023-09-11.RAWP_Fact...	747.3 kB	PDF docum...	03 November 2025, 21:41
Work Plan.BCP.C224330.2021-12-27.Citizen Part...	546.4 kB	PDF docum...	03 November 2025, 21:36

KaruHunters' list of the alleged leaked documents on DarkForums

Source: ZeroFox Intelligence

KaruHunters joined DarkForums in August 2024 and has attained a high positive reputational score within the forum. On DarkForums, reputation is garnered through successful and legitimate transactions between sellers and buyers; considering the actor's more than 40 posts, it is very likely KaruHunters is viewed by users as credible. While reputation does not solely determine the actor's legitimacy, it is indicative of the actor's presence on the forum and their potential credibility.

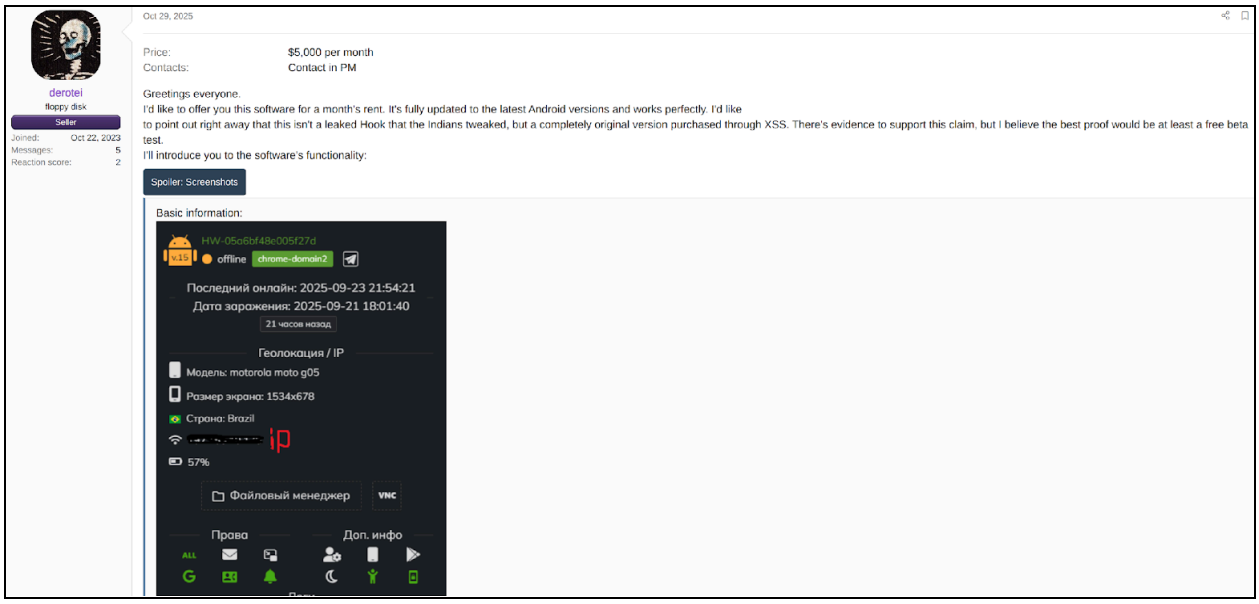
- Additionally, the contents of the alleged breach have been provided on DarkForums for free to download, likely indicating that the actor is either politically or ideologically motivated rather than financially driven.
- It is unlikely that KaruHunters is reusing or recycling previous breaches or leaks; however, since the documents are free to download, it remains a possibility the breach is not new data.

KaruHunters is known for multiple breaches targeting governments, corporations, and private targets worldwide. Notably, researchers did not detect any regional preference in the actor's choice of targets; however, Russia and China were allegedly not among their listed targets.

Android Hook Botnet for Rent on Dark Web Forum

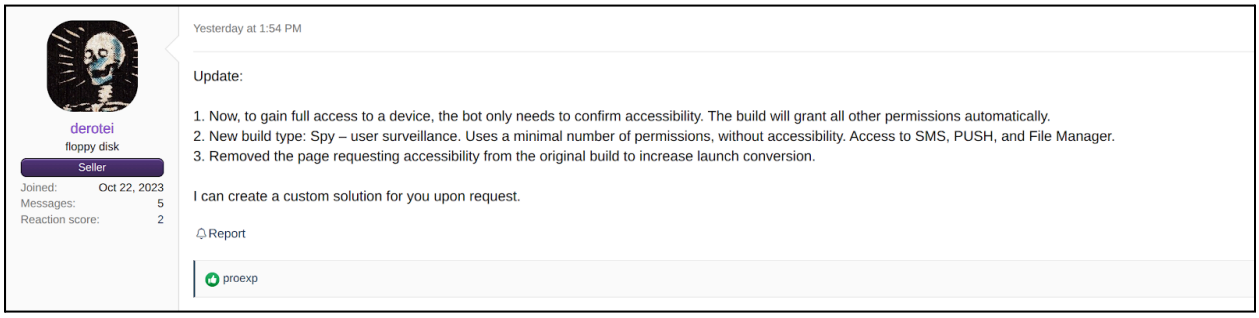
On October 29, 2025, a Russian-language actor using the alias "derotei" advertised an allegedly up-to-date Android hook botnet for rent on the dark web forum XSS. The actor specified that this hook botnet is an original product they purchased through the XSS forum and not a leaked hook version, claiming to have evidence to support this assertion.

- In the post, derotei advertises the botnet as a rental service available for USD 5,000 monthly that provides interested buyers with access to the official software.
- Derotei's post also includes several pictures allegedly showcasing the bot's functionality, such as basic information, its quick menu, and primary actions.
- The bot supposedly supports nine injections: booking[.]com, Gmail, Netflix, Snapchat, YouTube, Google Play, Instagram, Google Pay, and WhatsApp.



derotei's original XSS post
Source: ZeroFox Intelligence

On November 4, 2025, the actor provided updates to the botnet that include changes in how the botnet can gain full access to a device and an additional build type called "Spy" for user surveillance, which uses a minimal number of permissions to access SMS, PUSH, and File Manager. As part of the updated features, the actor removed the page requesting accessibility to increase launch conversion.



derotei's updated XSS post
Source: ZeroFox Intelligence

Derotei joined the XSS forum on October 22, 2023; despite a considerably long-standing account on the forum, the actor has garnered a low reaction score of two. However, this is likely positively received in the forum, as the reputational scoring metrics on primarily

Russian-language dark web forums such as XSS are distinctly more stringent than they are on other forums.

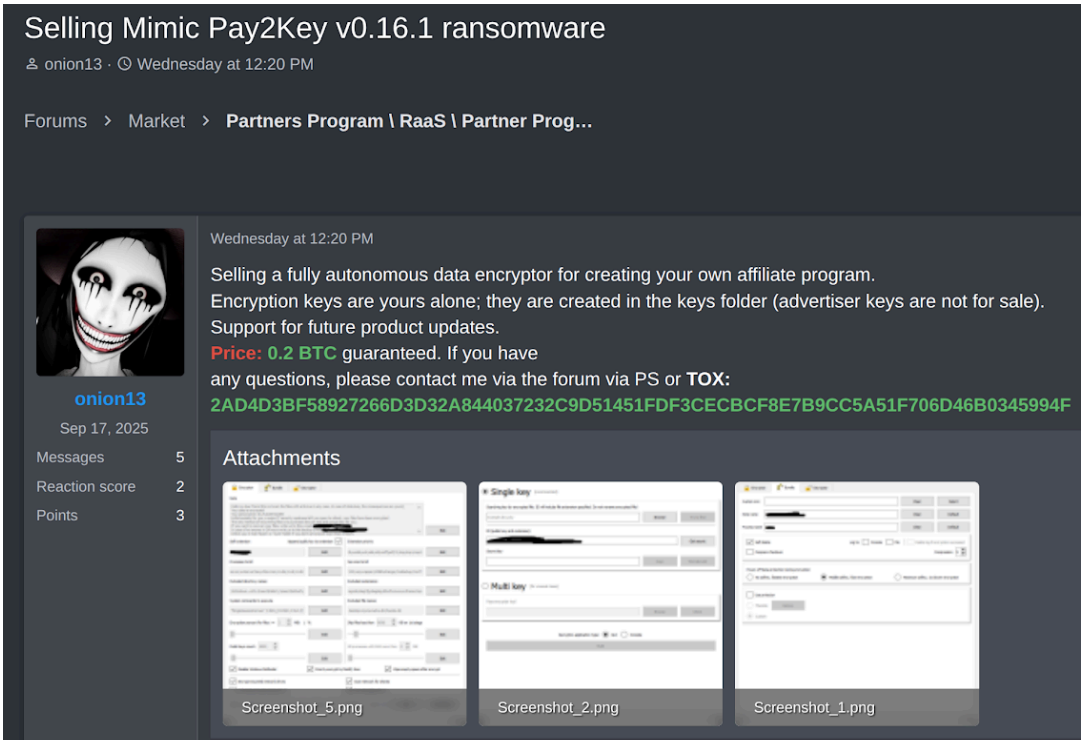
- The actor is likely considered reputable and potentially less experienced by potential buyers and peers in the forum. However, ZeroFox cannot verify the credibility of the actor or the efficacy of this botnet rental.

Notably, derotei's efforts to offer diverse build types for this hook botnet likely suggests that the actor is continuously customizing the already-weaponized Android hook bot; ZeroFox often observes Android bots supporting custom and private injections in deep and dark web (DDW) marketplaces. While the rental price of USD 5,000 per month is significantly higher than that of other bots, it would likely cause severe financial loss and compromise of personally identifiable information (PII) given the hook botnet's alleged capabilities.

Latest Version of Iran-Linked Mimic Pay2Key Ransomware on Sale

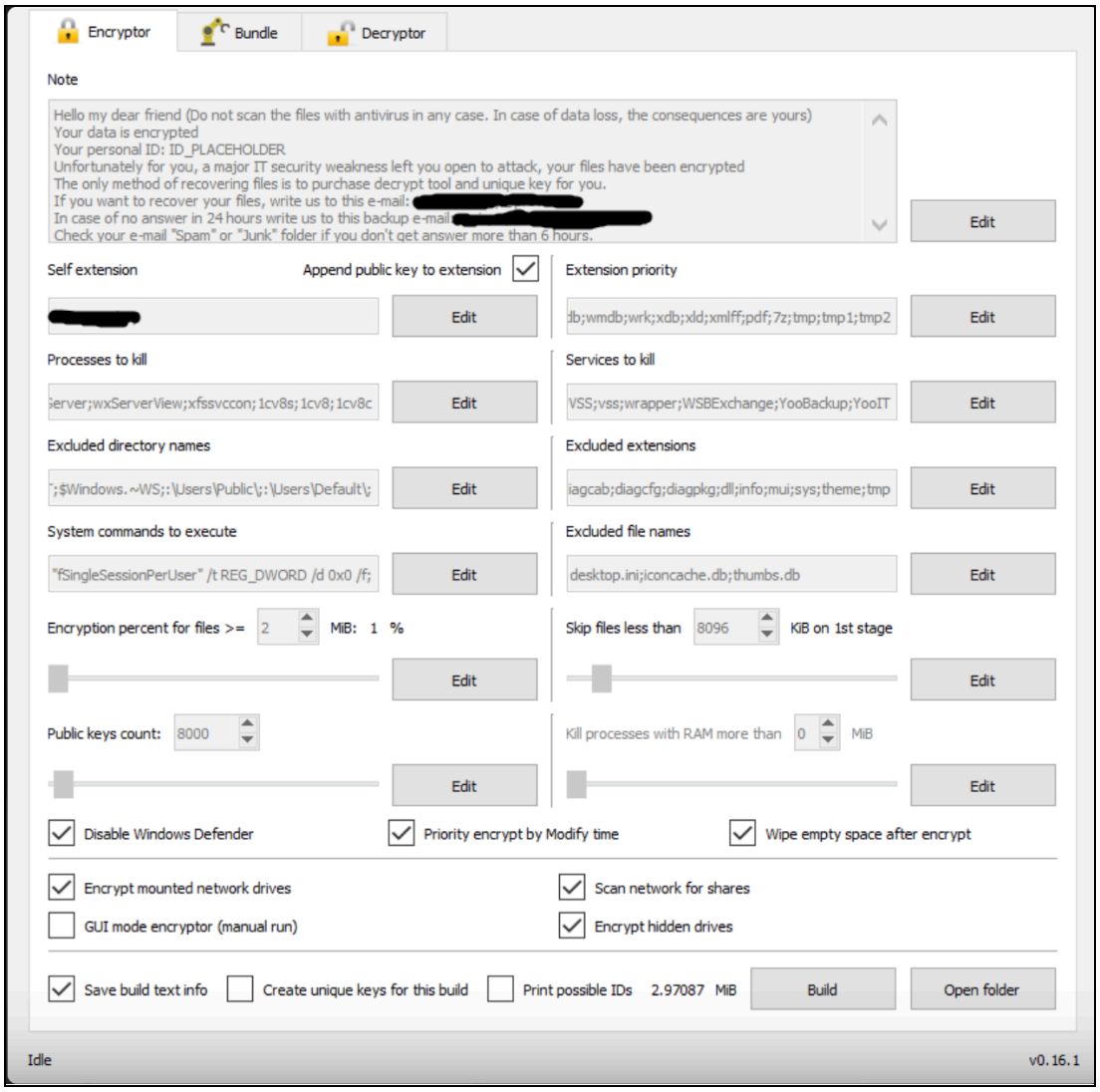
On October 22, 2025, untested threat actor "onion13" shared a post on dark web forum RAMP advertising the Mimic Pay2Key v0.16.1 ransomware. This ransomware-as-a-service (RaaS) product is priced at 0.2 BTC (or approximately USD 25,000). Onion13 claimed the ransomware is a fully autonomous data encryption malware strain suitable for creating an affiliate program, promising the buyer exclusive rights to manage the key.

- Pay2Key is an Iran-backed RaaS operation first observed in 2020 that is known for using Mimic ransomware.
- ZeroFox researchers observed that onion13 has also posted the same RaaS for sale on another Russian-language cybercrime forum called forum.Gerki[.]ws. This post indicated there was a price hike to BTC 0.3 (or approximately USD 31,000) on November 1, 2025. The threat actor gave instructions to contact them either via personal message or through TOX.
- In March 2025, RAMP user "TheShadowHacker" posted about a RaaS dubbed "Pay2Key" with features such as bypassing Windows protection and hosting an affiliate panel on the I2P network.



onion13's RAMP post

Source: ZeroFox Intelligence



Screenshot of Mimic encryptor GUI shared by onion13

Source: ZeroFox Intelligence

The lack of opportunistic posting also likely indicates that the threat actor's posts and the sale of the Mimic encryptor are legitimate. The post has garnered one reaction from user "$$$" (who is among the most reputed users on RAMP) inquiring about an update on its readiness, to which onion13 responded positively.

- Notably, onion13 joined on September 17, 2025, and has only two positive reactions, making it too early to determine their reputation.
- The sale is likely to generate more interest from reputable members of the forum.

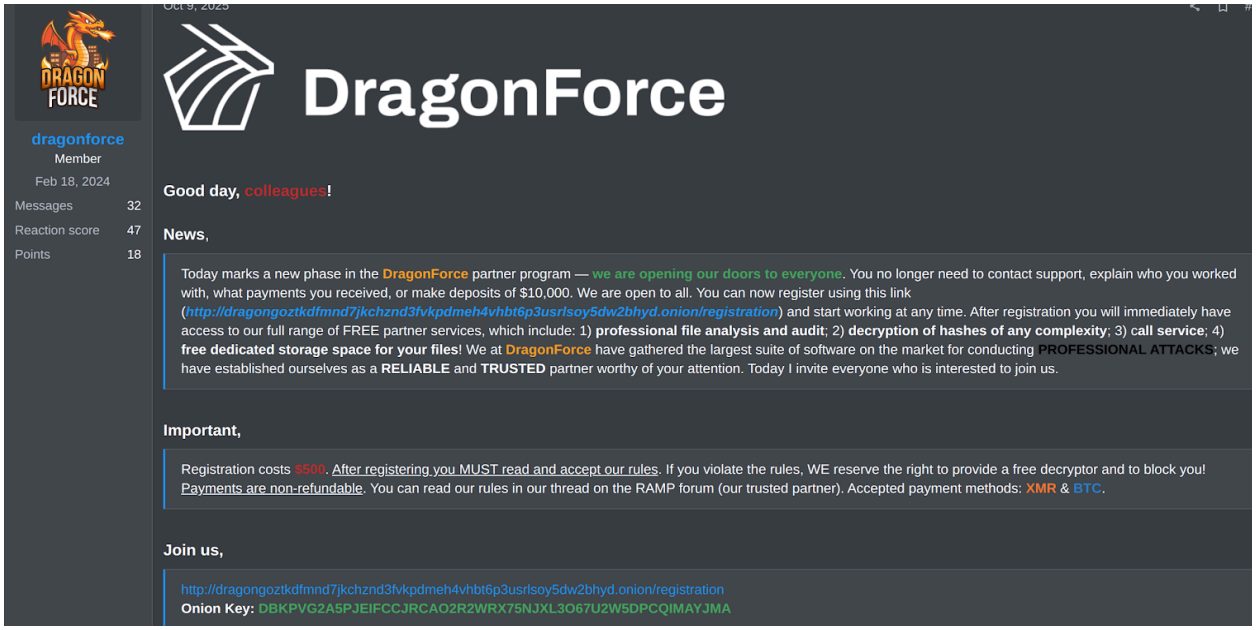
Mimic Pay2Key v0.16.1 is likely a new version of the ransomware, with little details available publicly. Historically, Pay2Key is known in DDW marketplaces for offering better prices to pro-Iranian affiliates to incentivize political and ideological targeting of Western organizations—especially those in the United States and Israel. In addition, ZeroFox has often observed Pay2Key strategically positioning its ransomware on primarily Russian and Chinese dark web platforms. As a result, it is likely that this supposed update of Pay2Key will continue to be leveraged against Western organizations and other politically aligned countries.

DragonForce Alters Partner Program to Abolish Prerequisites

On October 9, 2025, an account associated with the ransomware and digital extortion (R&DE) collective DragonForce posted on the dark web forum RAMP, announcing the beginning of a new phase in its partner program. The post stated that there are no longer prerequisites that aspiring affiliates must fulfill before joining; they can now simply register on DragonForce's onion website[1] for a fee of USD 500.

- Previous prerequisites to use DragonForce's service included contact support, work history, payment history, and financial deposits.
- On October 27, 2025, DragonForce updated the post, announcing the introduction of an automated payment system. This system enables clients and partners to automatically withdraw 80 percent of the ransom payments, with the remaining 20 percent transferred directly to the DragonForce wallet.

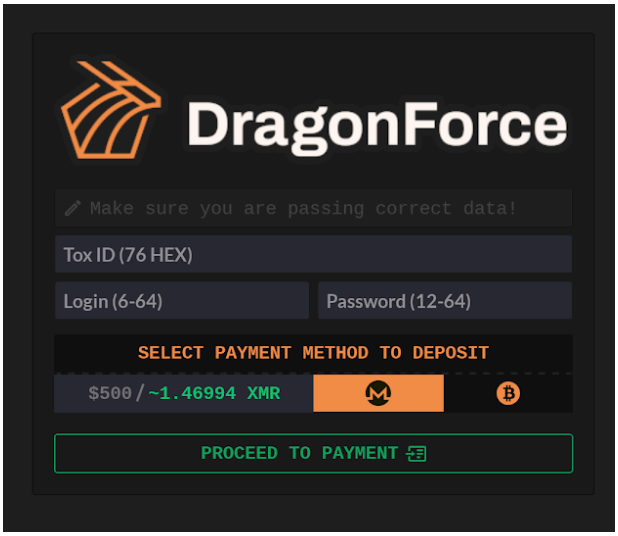
[1] hXXp://dragongoztkdfmnd7jkchznd3fvkpdmeh4vhbt6p3usrlsoy5dw2bhyd[.]onion/registration



DragonForce's initial RAMP post
Source: ZeroFox Intelligence

DragonForce claims to possess the largest suite of software on the market for conducting professional attacks—a claim that is likely an exaggeration to garner attention and promote the DragonForce brand in the cybercrime underground. According to the post, newly registered partners will gain access to the group's full suite of partner services, which include:

- Professional file analysis and audit
- Hash decryption of any complexity
- Call service
- Free, dedicated file storage



DragonForce's partner registration form
Source: ZeroFox Intelligence

This represents an unprecedented development in the R&DE marketplace. Combined with DragonForce's existing, open business model, opening the partner program to the wider public will likely have a significant impact on the ransomware ecosystem in the near future, allowing for less skilled threat actors to conduct high-capability attacks.

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 multi-factor authentication (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 tactics, techniques, and procedures (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%