ZEROFOX INTELLIGENCE

Brief

The Underground Economist: Volume 5, Issue 13

B-2025-07-04a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Ransomware

July 4, 2025

| Brief | The Underground Economist: Volume 5, Issue 13

B-2025-07-04a

TLP:CLEAR

ZEROFOX

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 7:00 AM (EDT) on July 4, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

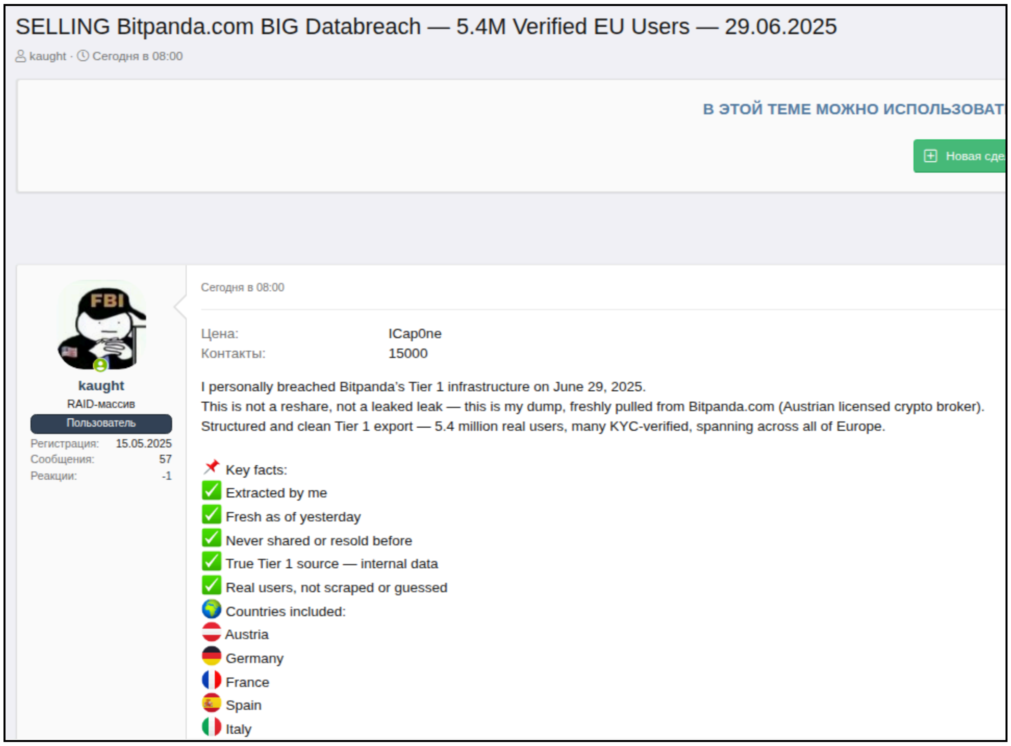
| Brief | The Underground Economist: Volume 5, Issue 13

| Alleged Bitpanda Breach Advertised in XSS

On June 30, 2025, actor "kaught" posted in the Russian-speaking dark web forum XSS, claiming to have breached the networks of cryptocurrency provider BitPanda, allegedly stealing data associated with approximately 5.4 million European Union (EU)-based users.

Kaught stated the breach occurred on June 29, 2025, assuring prospective buyers that the data is new and relevant. The advertised asking price is USD 15,000—approximately consistent with the volume and nature of exposed user data. The actor also shared 200 sample records that confirm the presence of the following exposed data fields:

- Country and country code
- First and last name
- Verified phone number
- Username and password hash
- Two factor authentication (2FA)
- Date of birth
- Address, city, and zipcode
- IP address
- Wallet address
- Know your customer (KYC) status—to confirm if users have verified their identity with a financial institution, which likely involves income verification



SELLING Bitpanda.com BIG Databreach — 5.4M Verified EU Users — 29.06.2025

kaught · Сегодня в 08:00

Регистрация: 15.05.2025
Сообщения: 57
Реакции: -1

Сегодня в 08:00

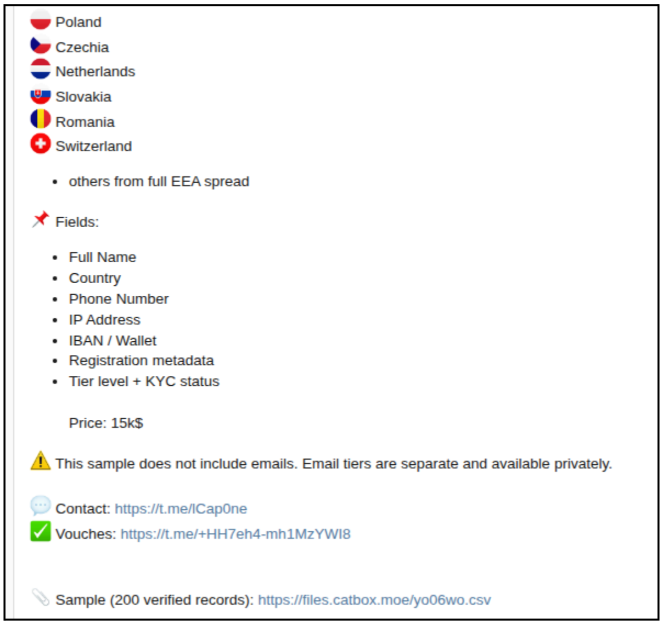
Цена: ICap0ne
Контакты: 15000

I personally breached Bitpanda's Tier 1 infrastructure on June 29, 2025.
This is not a reshare, not a leaked leak — this is my dump, freshly pulled from Bitpanda.com (Austrian licensed crypto broker).
Structured and clean Tier 1 export — 5.4 million real users, many KYC-verified, spanning across all of Europe.

📌 Key facts:
✓ Extracted by me
✓ Fresh as of yesterday
✓ Never shared or resold before
✓ True Tier 1 source — internal data
✓ Real users, not scraped or guessed
🌍 Countries included:
Austria
Germany
France
Spain
Italy

kaught's XSS post

Source: ZeroFox Intelligence



Poland
Czechia
Netherlands
Slovakia
Romania
Switzerland

- others from full EEA spread

📌 Fields:

- Full Name
- Country
- Phone Number
- IP Address
- IBAN / Wallet
- Registration metadata
- Tier level + KYC status

Price: 15k$

⚠ This sample does not include emails. Email tiers are separate and available privately.

💬 Contact: https://t.me/ICap0ne
✓ Vouches: https://t.me/+HH7eh4-mh1MzYWI8

📎 Sample (200 verified records): https://files.catbox.moe/yo06wo.csv

kaught's XSS post continued

Source: ZeroFox Intelligence

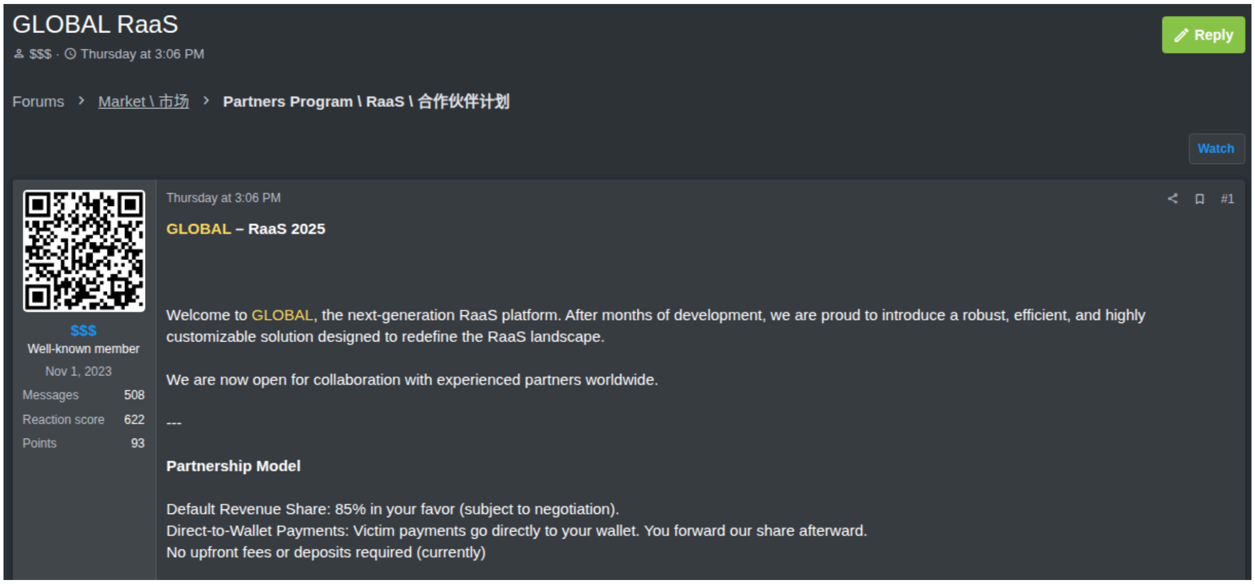
Kaught recently registered on XSS on May 15, 2025 and has already received a notable negative reputation from other forum users. While this negative scoring does not solely determine the legitimacy of the actor or the breach, it likely indicates that prospective buyers and forum users will consider the actor's reputation before engaging with this sale. The credibility of kaught's claim remains uncertain as of the writing of this report. Though the provision of data samples increases the likely legitimacy, BitPanda has reportedly stated that "these (kaught's) claims are false."[1]

New RaaS Platform "GLOBAL" Announced on Dark Web Forum

On June 26, 2025, actor "$$$" posted on the predominantly Russian-speaking dark web forum Russian Anonymous Marketplace (RAMP), announcing the launch of a new ransomware-as-a-service (RaaS) platform coined "GLOBAL" and inviting prospective affiliates to join the project.

- ZeroFox has observed that actor $$$ advertised two other RaaS projects on RAMP: "Mamona RIP" in March 2025 and "BlackLock" in March 2024. ZeroFox has not observed any victims uploaded to the victim leak site of Mamona RIP since its launch in March 2025.
- There have been at least 52 ransomware and digital extortion (R&DE) BlackLock incidents since September 2024. North America was the most targeted region, accounting for 66% of all incidents; technology was the most targeted industry, accounting for 20% of all incidents.
- The provision of BlackLock has very likely garnered actor $$$ a reputation as a credible RaaS provider, and it is likely that their advertisement of GLOBAL will gain traction among potential ransomware affiliates.

[1] hXXps://cybernews[.]com/crypto/bitpanda-data-breach/


Reply
Forums › Market \ 市场 › Partners Program \ RaaS \ 合作伙伴计划
Watch
#1

GLOBAL RaaS

$$$ · Thursday at 3:06 PM

$$$
Well-known member
Nov 1, 2023
Messages 508
Reaction score 622
Points 93

Thursday at 3:06 PM

GLOBAL – RaaS 2025

Welcome to GLOBAL, the next-generation RaaS platform. After months of development, we are proud to introduce a robust, efficient, and highly customizable solution designed to redefine the RaaS landscape.

We are now open for collaboration with experienced partners worldwide.

Partnership Model

Default Revenue Share: 85% in your favor (subject to negotiation).
Direct-to-Wallet Payments: Victim payments go directly to your wallet. You forward our share afterward.
No upfront fees or deposits required (currently)

$$$'s RAMP post

Source: ZeroFox Intelligence

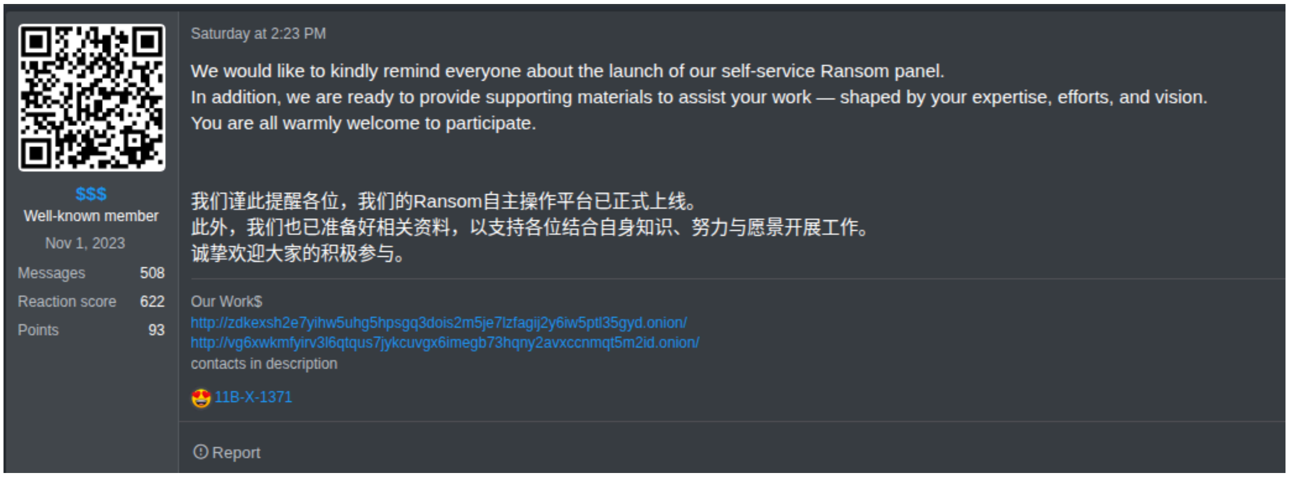
Many of the features and structures outlined in the advertisement are very likely to appeal to potential ransomware affiliates. GLOBAL reportedly features a default profit sharing ratio of 85:15—a ratio that favors the affiliate slightly more than many other RaaS operations, some of which pay as low as 70 percent. Additionally, according to actor $$$, following a successful compromise, GLOBAL pays affiliates first, with core operators being paid afterward. This is contrary to the majority of RaaS operations, wherein core operators receive prior payment—often leading to trust issues and enabling opportunistic exit scam-type activity. Lastly, also likely to garner affiliate interest, GLOBAL reportedly has no entry fees or deposit requirements.

As well as containing many of the usual features offered by modern ransomware strains, such as advanced Command and Control (C2) capabilities, panel customization, and lateral movement, GLOBAL is also said to have an AI-assisted chatbot. While the specific features and intent of this are not outlined, actor $$$ claimed that it can assist in "dynamic and realistic communication" while analyzing victim data.

- ZeroFox has not observed this feature being offered by RaaS platforms before. Potential affiliates will very likely perceive it as novel, though its effectiveness in conducting negotiation and extortion cannot be determined.

According to the post, GLOBAL affiliates are not permitted to target entities located within the Commonwealth of Independent States (CIS)—a restriction fairly typical of Russian-speaking digital extortion collectives. A further restriction is placed upon the targeting of critical infrastructure and non-profit organizations, which very likely reflects the collective's intent to reduce exposure to media publicity and law enforcement operations.

On June 28, 2025, actor $$$ updated the thread to remind interested parties about the launch of their "self-service Ransom panel." Notably, the post was duplicated in Chinese rather than Russian—almost certainly reflecting an attempt to garner interest from the growing Chinese-speaking presence within deep and dark web (DDW) marketplaces.



$$$
Well-known member
Nov 1, 2023

Messages	508
Reaction score	622
Points	93

Saturday at 2:23 PM

We would like to kindly remind everyone about the launch of our self-service Ransom panel.
In addition, we are ready to provide supporting materials to assist your work — shaped by your expertise, efforts, and vision.
You are all warmly welcome to participate.

我们谨此提醒各位，我们的Ransom自主操作平台已正式上线。
此外，我们也已准备好相关资料，以支持各位结合自身知识、努力与愿景开展工作。
诚挚欢迎大家的积极参与。

Our Work$
http://zdkexsh2e7yihw5uhg5hpsgq3dois2m5je7lzfagij2y6iw5ptl35gyd.onion/
http://vg6xwkmfyirv3l6qtqus7jykcuvgx6imegb73hqny2avxccnmqt5m2id.onion/
contacts in description

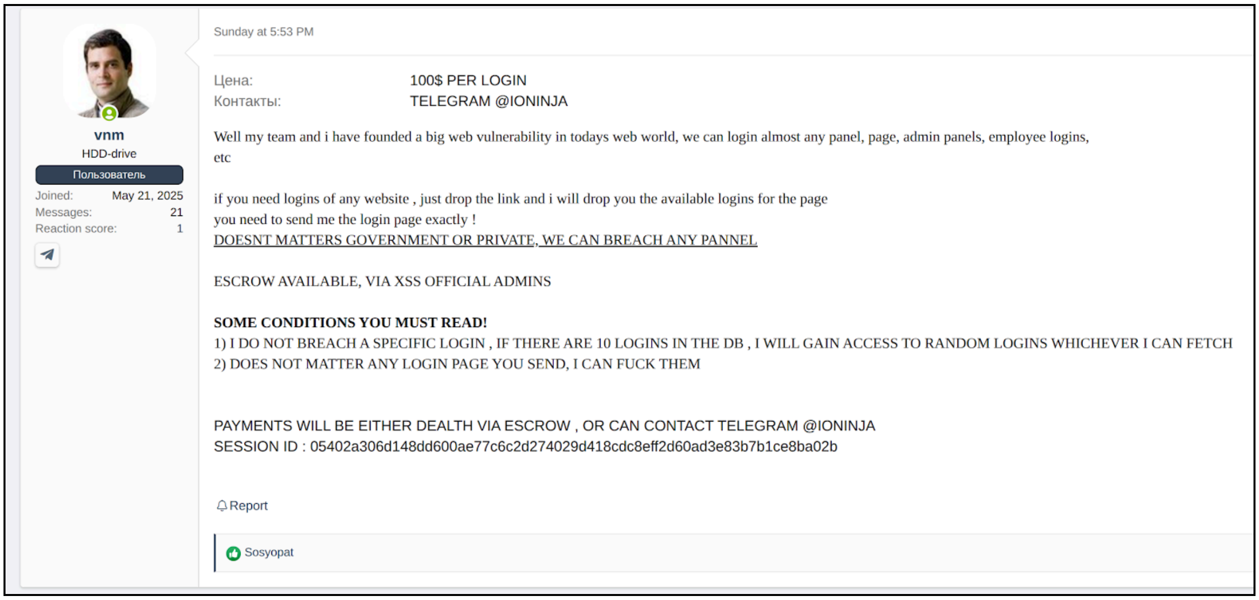
😍 11B-X-1371

$$$'s updated RAMP post

Source: ZeroFox Intelligence

Zero-Day Vulnerability with Access to "Any Website" Advertised

On June 22, 2025, the actor "vnm" posted on XSS, claiming to have discovered a zero-day vulnerability which allows them to retrieve valid login credentials for "any website," including those associated with both public and private entities. The actor detailed that the service does not involve the targeting of any individual account. Instead, all logins found that are associated with a given platform can be provided to the buyer. The service was advertised at a price of USD 100 per set of credentials retrieved, with the use of XSS escrow services also offered.



vnm
HDD-drive
Пользователь
Joined: May 21, 2025
Messages: 21
Reaction score: 1

Sunday at 5:53 PM

Цена: 100$ PER LOGIN
Контакты: TELEGRAM @IONINJA

Well my team and i have founded a big web vulnerability in todays web world, we can login almost any panel, page, admin panels, employee logins, etc

if you need logins of any website , just drop the link and i will drop you the available logins for the page
you need to send me the login page exactly !
DOESNT MATTERS GOVERNMENT OR PRIVATE, WE CAN BREACH ANY PANNEL

ESCROW AVAILABLE, VIA XSS OFFICIAL ADMINS

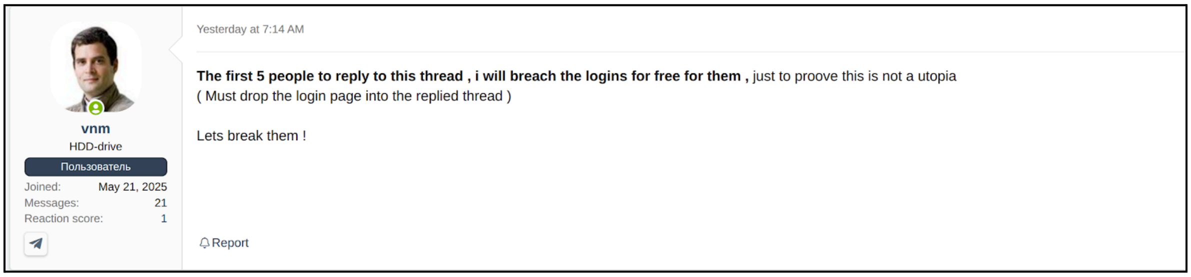
SOME CONDITIONS YOU MUST READ!
1) I DO NOT BREACH A SPECIFIC LOGIN , IF THERE ARE 10 LOGINS IN THE DB , I WILL GAIN ACCESS TO RANDOM LOGINS WHICHEVER I CAN FETCH
2) DOES NOT MATTER ANY LOGIN PAGE YOU SEND, I CAN FUCK THEM

PAYMENTS WILL BE EITHER DEALTH VIA ESCROW , OR CAN CONTACT TELEGRAM @IONINJA
SESSION ID : 05402a306d148dd600ae77c6c2d274029d418cdc8eff2d60ad3e83b7b1ce8ba02b

vnm's XSS advertisement
Source: ZeroFox Intelligence

In response to some skeptical XSS users, vnm stated that the first five forum members to respond will receive a free trial, whereby they may request valid login credentials from a specific platform, which will reportedly be delivered within 24 hours. ZeroFox observed several users expressing interest in this offering. While the results were not publicly observable, vnm admitted failure in one instance, stating that they could not retrieve credentials for a localhost/auth/login[.]php page. The actor also conceded that multi-factor authentication (MFA) implemented within victim platforms had hindered the service.

- In a separate XSS post observed by ZeroFox, vnm stated that they are seeking collaborators who can assist in bypassing MFA protocols.



vnm
HDD-drive
Пользователь
Joined: May 21, 2025
Messages: 21
Reaction score: 1

Yesterday at 7:14 AM

The first 5 people to reply to this thread , i will breach the logins for free for them , just to proove this is not a utopia
(Must drop the login page into the replied thread)

Lets break them !

vnm offers a free trial of its service
Source: ZeroFox Intelligence

Though actor vnm claimed to be in possession of an unspecified web zero-day vulnerability, this is very unlikely to be the case. Any such vulnerability is very unlikely to facilitate the compromise of login platforms indiscriminately, considering that they are based on different frameworks and leverage different authentication protocols. Even upon initial compromise, any extracted passwords are unlikely to be cleartext, requiring successful decryption before use. Furthermore, buyers would be met with an array of MFA challenges for which vnm provides no solution, rendering the services significantly less useful for subsequent malicious exploitation.

There is a more likely chance that vnm possesses a large quantity of unknown login pairs parsed from various stealer logs—which are tested against the platforms requested by buyers. The likely exaggerations in vnm’s advertisement coincide with its lack of a significant reputation within the XSS forum, which is very likely to deter potential buyers.

Nova RaaS Partnership Program

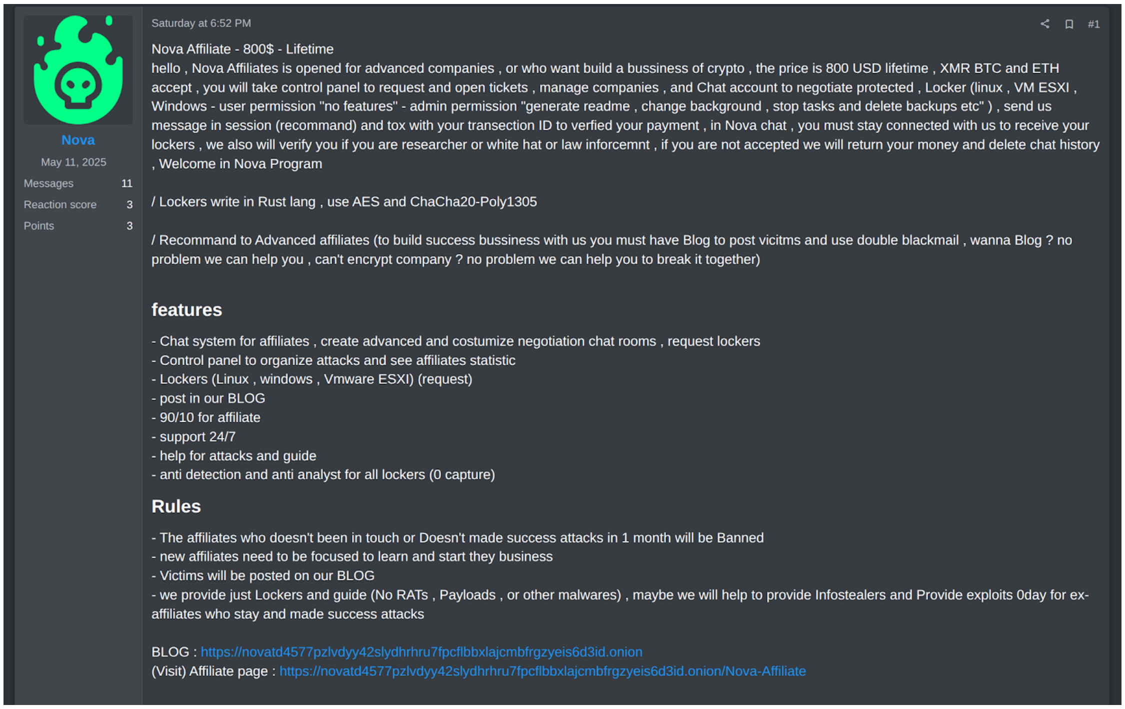
On June 21, 2025, an actor using the alias “Nova” posted on RAMP, advertising their recently-emerged RaaS platform named “(Partners program) Nova RaaS,” which claims to be a full-service platform with features designed to support prospective digital extortion affiliates. Lifetime access to the program is offered for USD 800. The program reportedly offers features and services such as a customised chat system for secure negotiation communication and payment locker services between affiliates and victims. Other features specified include:

- Lockers for Linux, Windows, and VMware ESXi (available upon request)
- Control panel to organize attacks, view affiliate statistics, and open support tickets
- Ability to post on Nova’s blog and an option for assistance with creating blog posts for double extortion to blackmail victims
- Revenue split of 90 percent to the affiliate and 10 percent to Nova
- 24/7 support
- Assistance with and guidance on attacks
- Anti-detection and anti-analysis features for all lockers

Nova ransomware was first observed by ZeroFox in April 2025, and since then, it has uploaded at least 13 different entities to its victim leak site. Victims appear to have been from different industries, though Nova seems to target Europe-based organizations disproportionately highly. Its recent advertisement likely reflects a renewed effort to advertise the programme and attract new affiliates.

According to Nova, unlike the majority of other RaaS platforms, new affiliates will be subject to a verification process conducted to ensure that the buyer is not a security or white hat researcher or from law enforcement. Nova claims that any rejected buyers will have their payment refunded and activity history deleted. The following further rules are specified for verifed affiliates:

- Affiliates who do not maintain contact or fail to conduct successful attacks within one month will be banned.
- New affiliates are expected to focus on learning and building their business.
- Victim details will be posted on the group's blog.
- The group provides only lockers and guidance, rather than Remote Access Trojans (RATs), payloads, or other malware.
- However, the group may offer infostealers or zero-day exploits to long-term and successful affiliates.



Saturday at 6:52 PM

Nova Affiliate - 800$ - Lifetime
hello , Nova Affiliates is opened for advanced companies , or who want build a bussiness of crypto , the price is 800 USD lifetime , XMR BTC and ETH accept , you will take control panel to request and open tickets , manage companies , and Chat account to negotiate protected , Locker (linux , VM ESXI , Windows - user permission "no features" - admin permission "generate readme , change background , stop tasks and delete backups etc") , send us message in session (recommand) and tox with your transection ID to verfied your payment , in Nova chat , you must stay connected with us to receive your lockers , we also will verify you if you are researcher or white hat or law inforcemnt , if you are not accepted we will return your money and delete chat history , Welcome in Nova Program

/ Lockers write in Rust lang , use AES and ChaCha20-Poly1305

/ Recommand to Advanced affiliates (to build success bussiness with us you must have Blog to post vicitms and use double blackmail , wanna Blog ? no problem we can help you , can't encrypt company ? no problem we can help you to break it together)

features

- Chat system for affiliates , create advanced and costumize negotiation chat rooms , request lockers
- Control panel to organize attacks and see affiliates statistic
- Lockers (Linux , windows , Vmware ESXI) (request)
- post in our BLOG
- 90/10 for affiliate
- support 24/7
- help for attacks and guide
- anti detection and anti analyst for all lockers (0 capture)

Rules

- The affiliates who doesn't been in touch or Doesn't made success attacks in 1 month will be Banned
- new affiliates need to be focused to learn and start they business
- Victims will be posted on our BLOG
- we provide just Lockers and guide (No RATs , Payloads , or other malwares) , maybe we will help to provide Infostealers and Provide exploits 0day for ex-affiliates who stay and made success attacks

BLOG : https://novatd4577pzlvdyy42slydhrhru7fpcflbbxlajcmbfrgzyeis6d3id.onion
(Visit) Affiliate page : https://novatd4577pzlvdyy42slydhrhru7fpcflbbxlajcmbfrgzyeis6d3id.onion/Nova-Affiliate

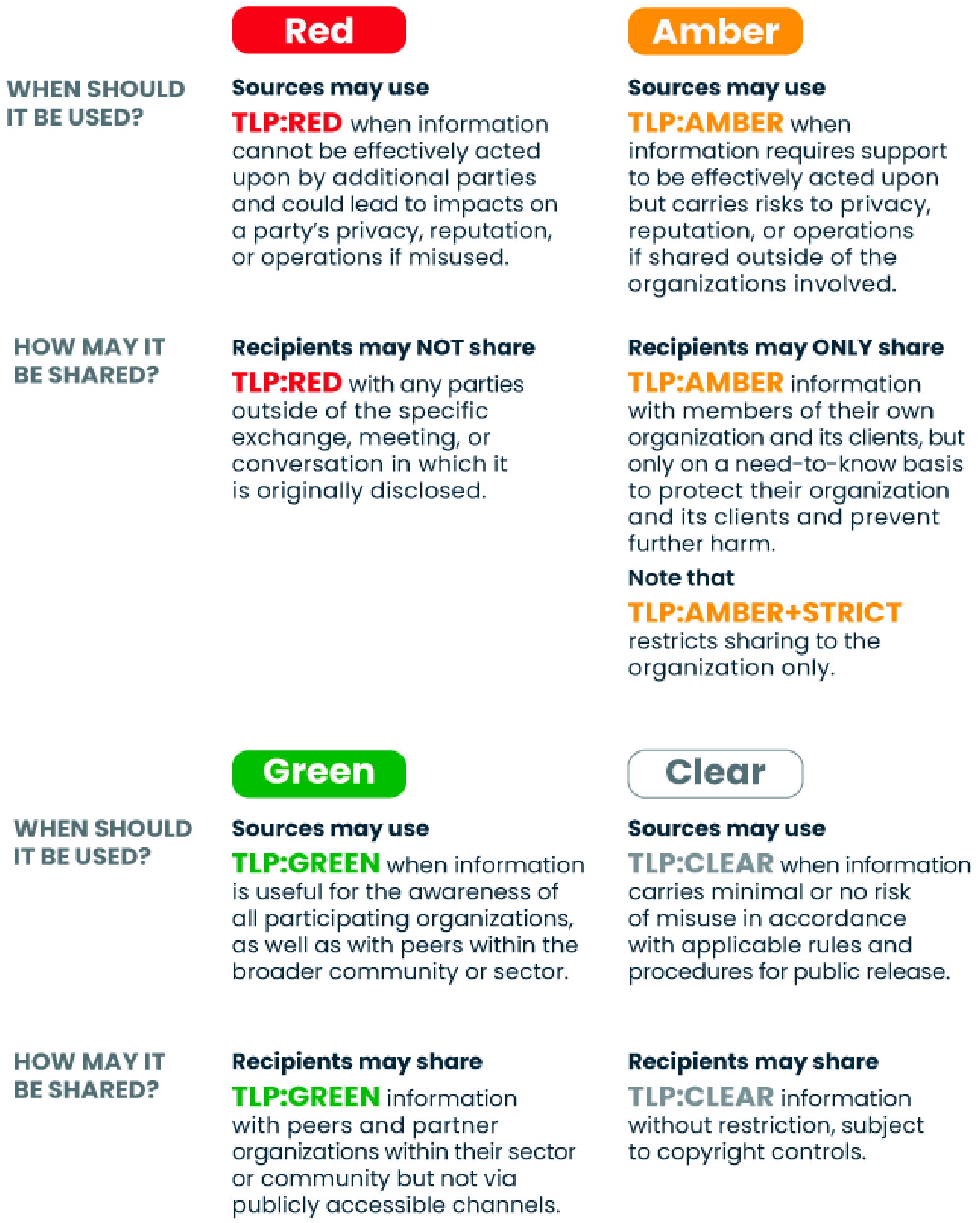
Nova's RAMP post

Source: ZeroFox Intelligence

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 tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

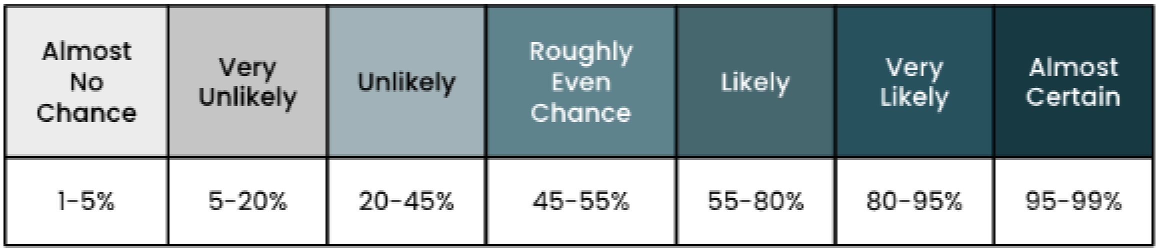


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively 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%