Bold ad campaign

blog.group-ib.com/awc

06.08.2021

AWC joins illicit carding business by offering 1 Mln compromised cards for free

Sergey Kokurin

Underground Markets Analyst Group-IB

On August 2, Group-IB Threat Intelligence & Attribution system detected an unconventional post on several carding forums. A user, nicknamed AW_cards posted links to a file containing 1 million pieces of stolen payment records. The file offered for free contained

compromised card details from over 1 000 banks in more than 100 countries, including India, Mexico, the US, Australia, Brazil, and etc.

The post immediately sparked Group-IB researchers' interest, because cybercriminals in the carding community rarely offer so many cards for free. It's especially unusual for a previously unknown market player. The analysis of the file revealed that this huge batch of compromised cards had not appeared on other underground forums.

Further research revealed that the post was nothing but a very bold ad to scale up the user base of newly established card shop All World Cards, which joined the carding market in May 2021. Group-IB researchers found out that the alleged owners of the card shop had launched a massive promo campaign in the underground to advertise their new platform, which, in addition to a huge database giveaway, included a writing contest for other cybercriminals with a cash prize of USD 15,000.

This post analyzes the latest 1 mln stolen bank card record database as well as the short history of the All World Cards card shop and the activity of its alleged owners who are most likely not the newbies of the carding business.

"An extraordinary act of generosity"

On August 2, 2021, the same message was posted on two carding forums "crdclub" and "xss." The user nicknamed "AW_cards" in what they called "An extraordinary act of generosity" uploaded a database containing 1 million payment records, some of which included email addresses and phone numbers.

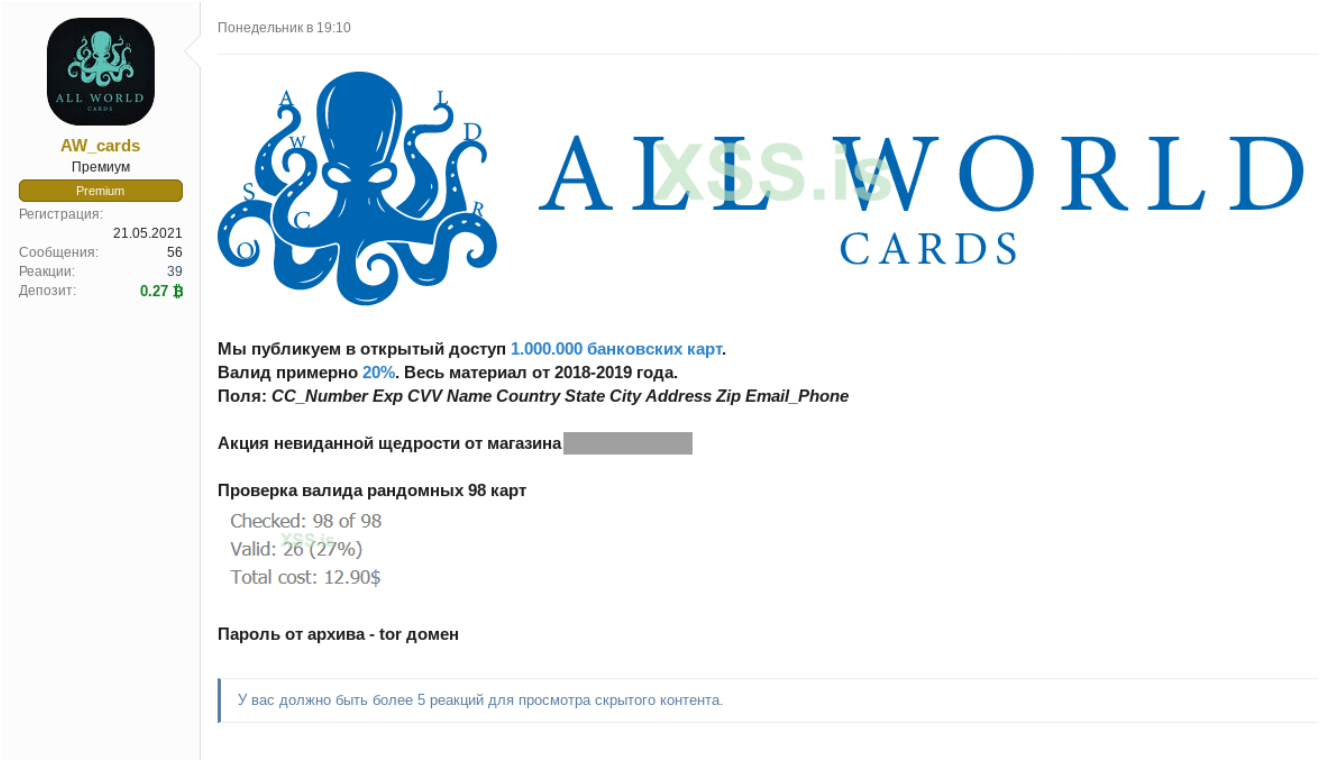


Figure 1 - Screenshot from "xss" forum (AW_cards: "We publish 1,000,000 bank cards to the public. Valid at 3%. All material from 2018-2019. Promotion of unprecedented generosity from the AllWorld.Cards store) Source: Group-IB Threat Intelligence & Attribution system

Figure 2 - Screenshot from Group-IB Threat Intelligence & Attribution system

It is noteworthy that a day after the publication, the post was edited. The "Valid parameter" (which stands for the share of valid bank cards that cybercriminals can monetize) was increased from 3% to 20% of cards in the entire batch.

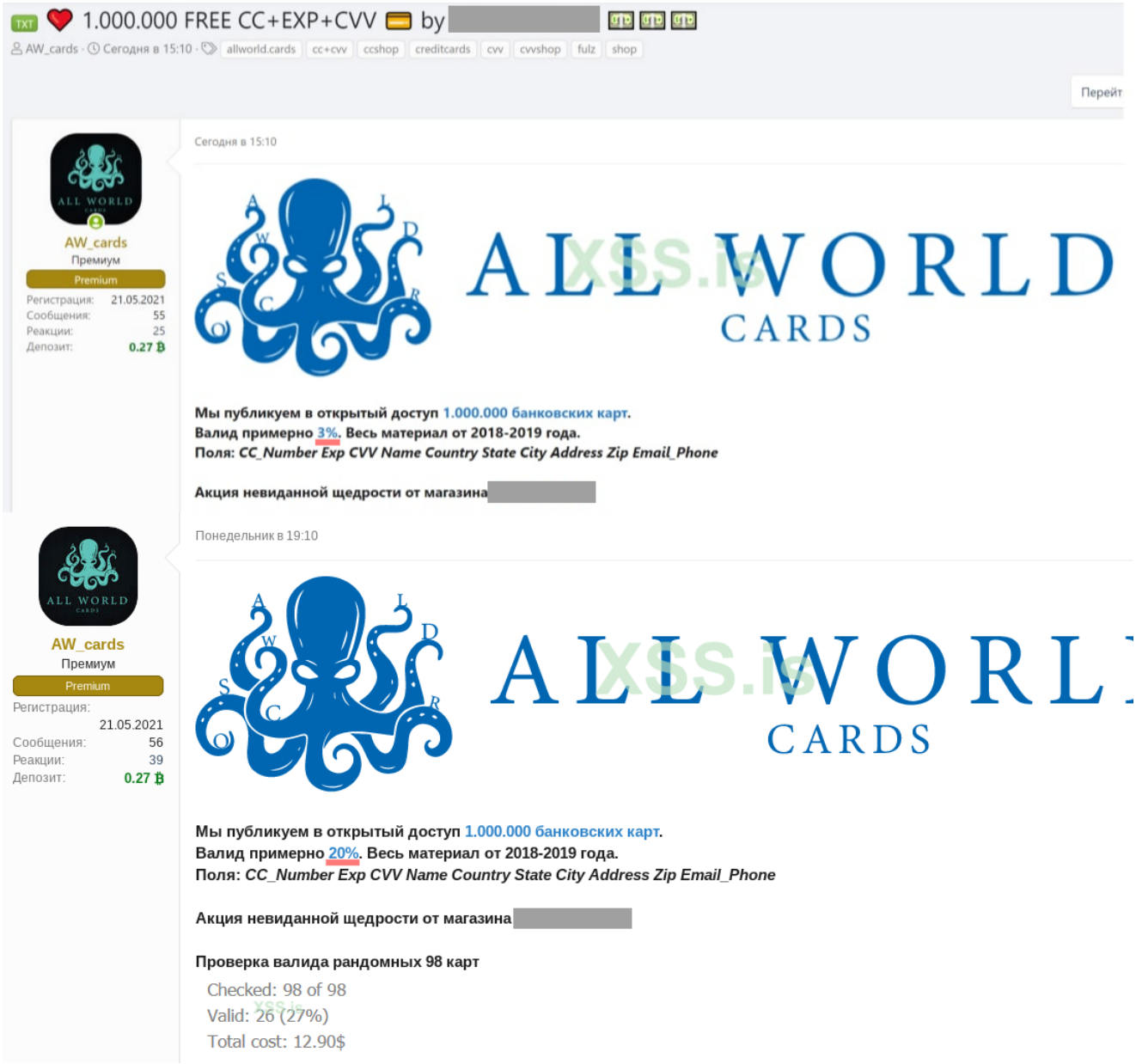


Figure 3 - Screenshot from "xss" forum

Figure 4 - Screenshot from "xss" forum (Xss forum user: "With only 3% validity, are these CCs generated?")

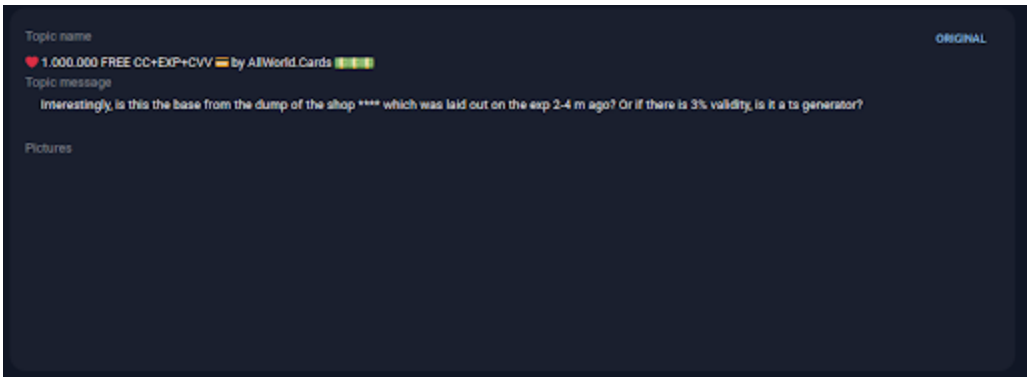


Figure 5 - Screenshot from Group-IB Threat Intelligence & Attribution system

Nevertheless, according to Group-IB's findings, despite the post author's claim that the cards were compromised from 2018-2019, 97% of the records in the database are still valid. In the entire batch Group-IB researchers found 810 expired cards, 30 of them expired in June 2021, 780 in July 2021. At least 27,112 cards are set to expire in August 2021. It can be assumed that most of the invalid cards have been removed from the database, or it is newer than declared by the author of the post.

Group-IB researchers established that the database's owner used several file sharing services to upload it. The database was contained in a password-protected zip archive with a text file containing 1 million lines with the following lines:

- Card number;
- Expiration date;
- CVV / CVC code;
- Name of the card holder;
- Country;
- State;
- City;
- The address;
- Zip code;
- Email and phone for some entries

However, not all of the above fields were available for every record in the database.

According to Group-IB's Threat Intelligence team, more than 200,000 (22%) of compromised payment cards were from the Indian banks, followed by Mexican (9%), US (9%), and Australian (8%) financial institutions. The distribution of cards in the batch by the country of the issuing bank is shown on Figure 6 below.

Group-IB continues the outreach campaign to inform the affected financial organizations so that they can take the necessary steps to mitigate potential impact of the compromised data.

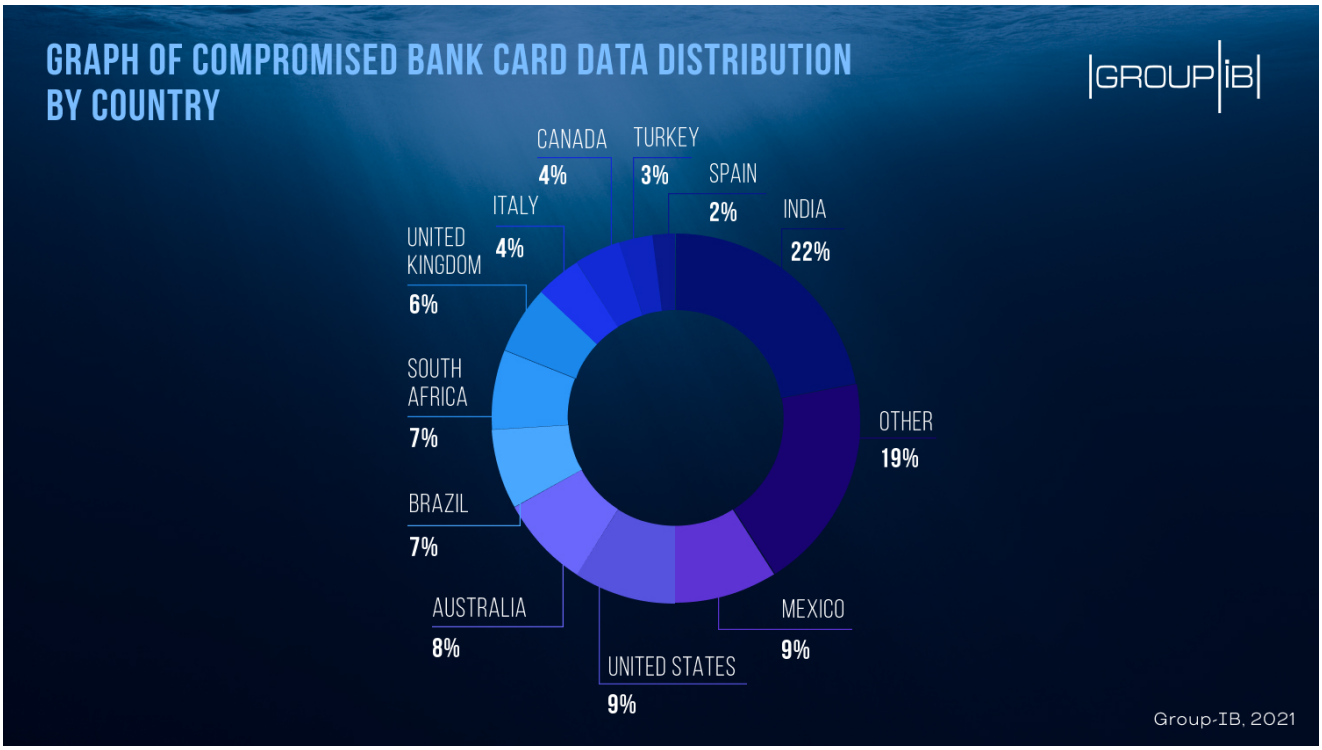


Figure 6 - Graph of compromised bank card data distribution by country

According to the findings, 77% of the cards in the batch were debit cards, 23% were credit cards, and the rest accounted for less than 1 percent.

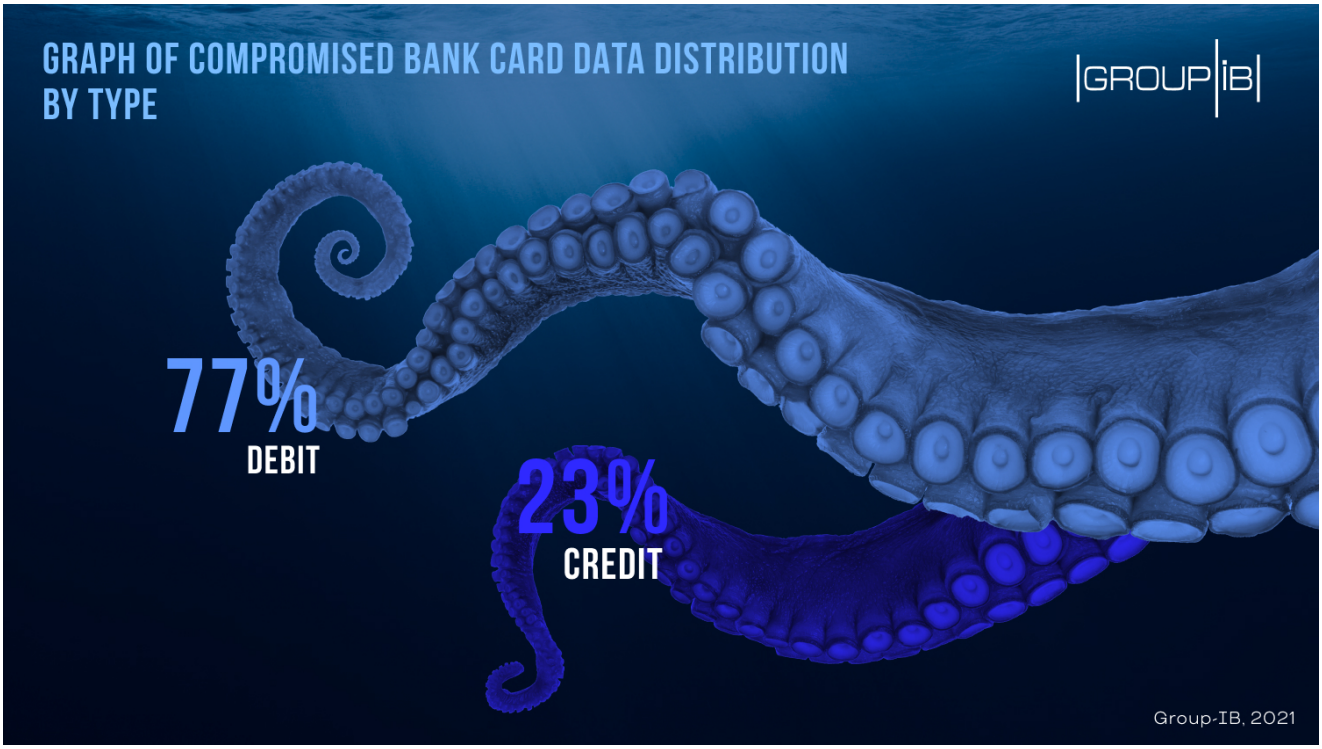


Figure 7 - Graph of compromised bank card data distribution by type

The distribution of compromised bank card data by the payment systems is roughly the same: Visa cards accounted for 48%, while Mastercard cards stood at 47%. At least 4% (more than 39,000 cards) belonged to "RuPay" — the national payment system of India.

Another 1% of the cards belonged to American Express, the rest of the systems accounted for less than a percent. At least 58% of records in the batch are "standard" or "classic" cards, 7% more are "gold" and 6% are "platinum" cards. It is interesting to note that 8,050 cards have a "corporate" postscript.

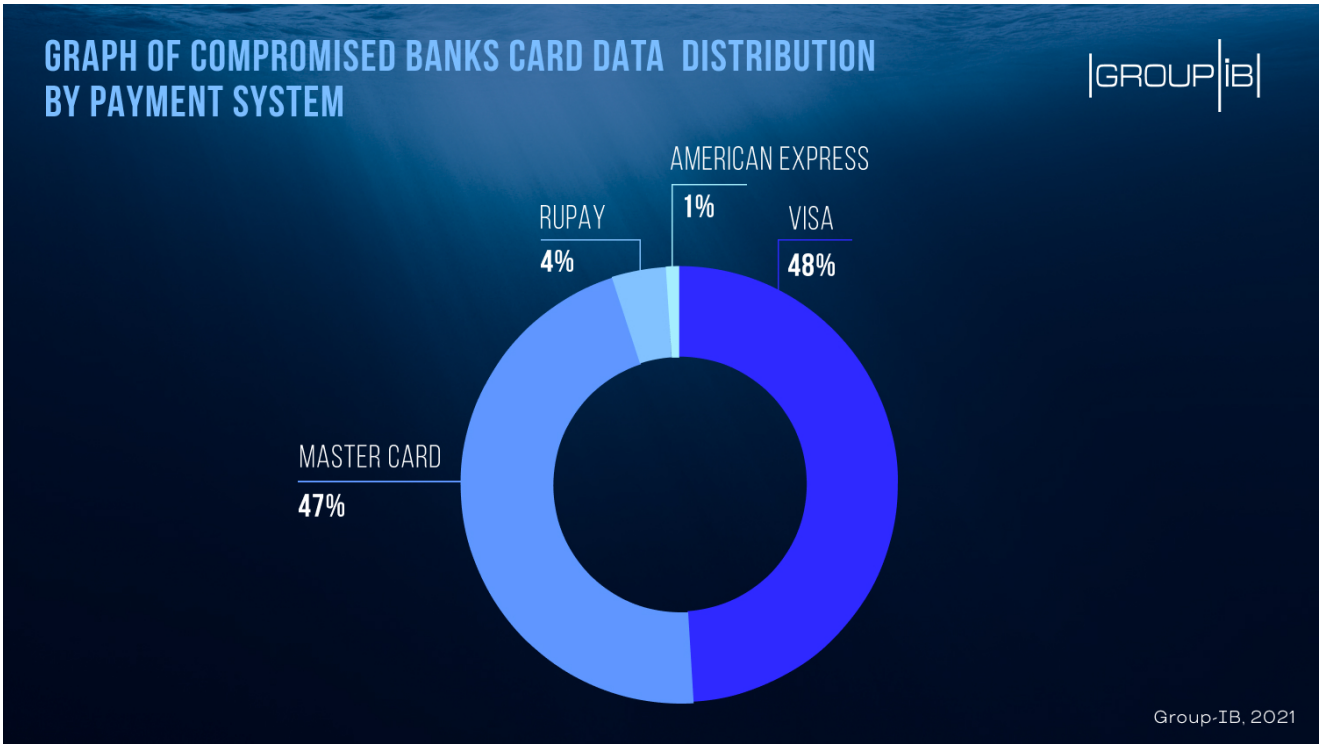


Figure 8 - Graph of compromised banks card data distribution by payment system

More than 600,000 lines with a correctly filled email address have been discovered. Among them, email addresses with the domain names of government organizations and banks were found.

Some of the compromised bank card records had IP addresses mentioned for them. Thus, at least 26,451 cards had IP addresses, but only 24,443 of them were unique.

A total of 77 cards from the entire list do not correspond to the Luhn algorithm (the algorithm for checking if the number on a plastic card is correct).

Judging by the analysis of Group-IB TI&A, less than 2% of the cards from the database overlap with the bank card data previously offered for sale on any underground resources, including cards from recent Swarmshop and BriansClub leaks. It should be also noted that some of the cards are related to malicious campaigns involving CoffeMokko JS-sniffers and other similar groups. But in any case, such a small percentage only suggests that the cards posted in this database were not previously published on other public sources.

Further analysis of the activity of the user kicknamed "AW_cards" revealed that they are the author of the newly established All World Cards card shop.

All World Cards

For the entire observation period, 3.8 million bank cards were offered for sale in this card shop. At least 2.6 million out of them are available for purchase at time of the publication.

It can be assumed that 1 mln cards offered for free were previously placed on the card shop itself. For a new card shop, this amount of sales in 2 months is too high.

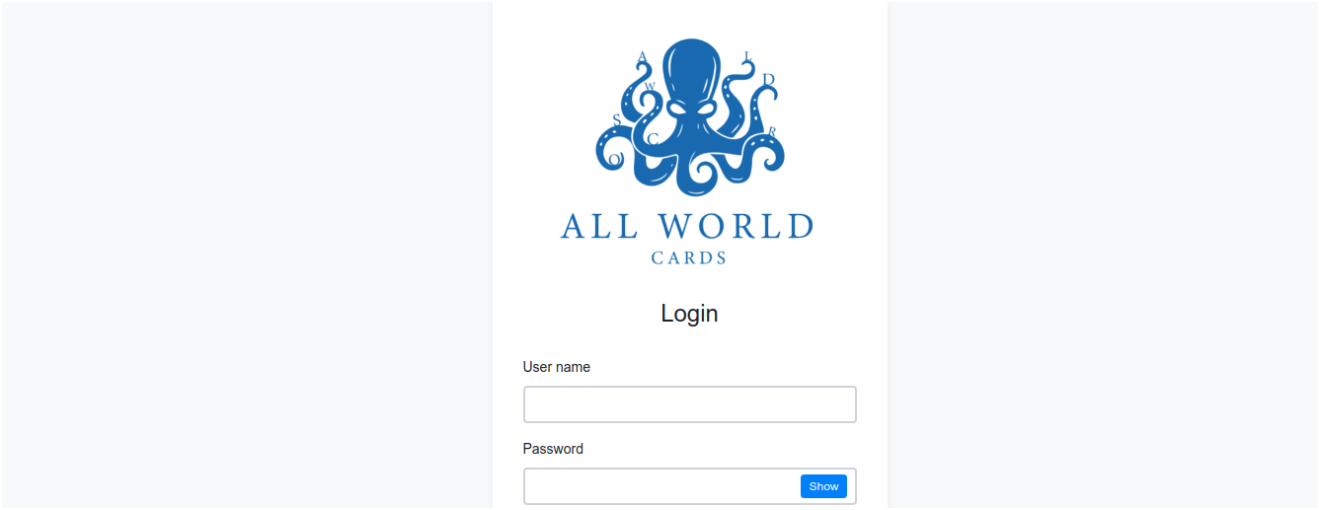


Figure 9 - *"All World Cards" card shop login page*

"All World Cards" is an underground credit card data marketplace. The first appearance of this card shop on the forums was recorded on May 31, 2021.

Figure 10 -*Screenshot from "xss" forum (AW_cards: "Dear users, we present the All World Cards bank cardshop").*

It was a message promoting the opening of the card shop.

The card shop's owners are active on several forums using two nicknames "AW_cards" and "AW_support." From these two accounts, they post news about card database updates and answer users' questions.

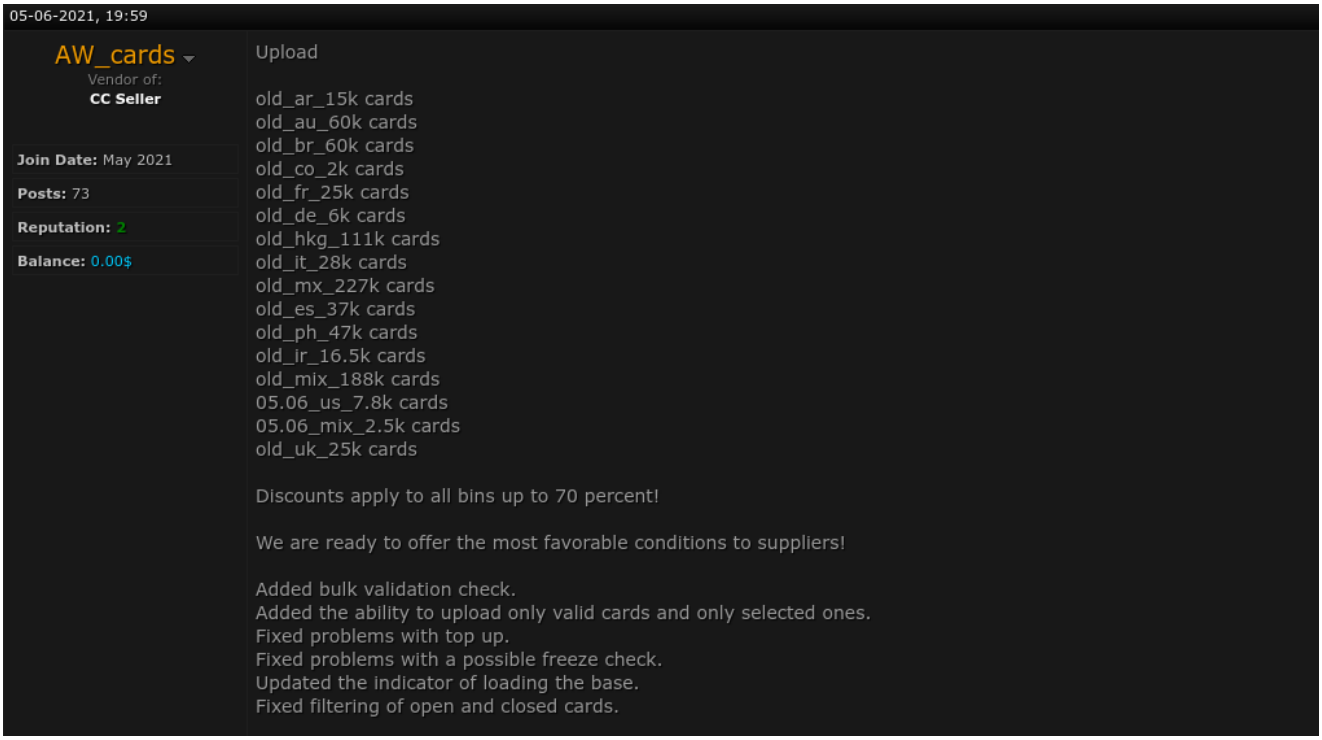
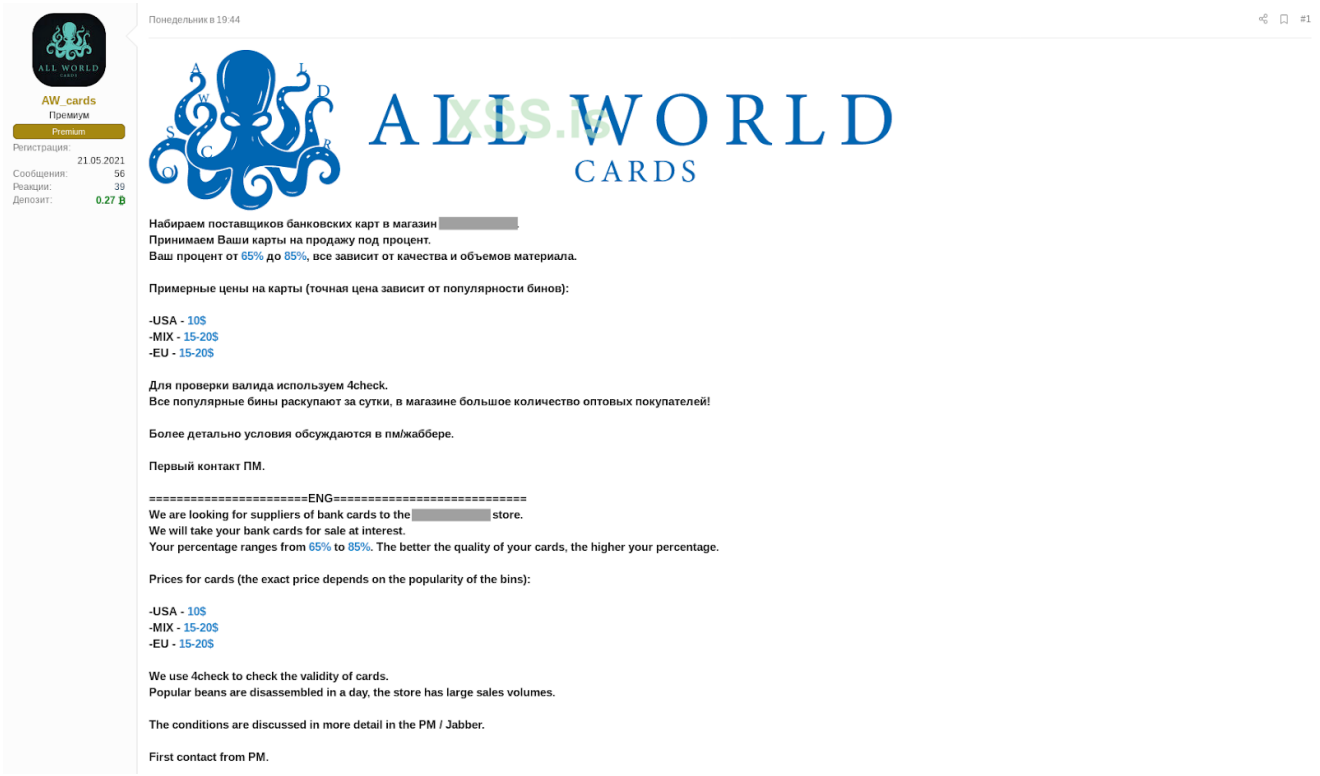


Figure 11 - *Screenshot from "crdclub" forum*

The card shop's owners are very active in advertising their forum. For 2 months, more than 400 messages were posted from both accounts.

On August 2, 2021, a message about the recruitment of card sellers appeared on the "xss" forum.



Picture 12 - *Screenshot from "xss" forum (AW_cards: "We recruit suppliers of bank cards")*

Another unusual promotional move was the sponsorship of a contest for users who were asked to submit articles about penetration tests, the bypassing of security solutions, vulnerabilities and other hacking related topics. The organizers claimed to draw a $15,000 prize for users on the xss forum.

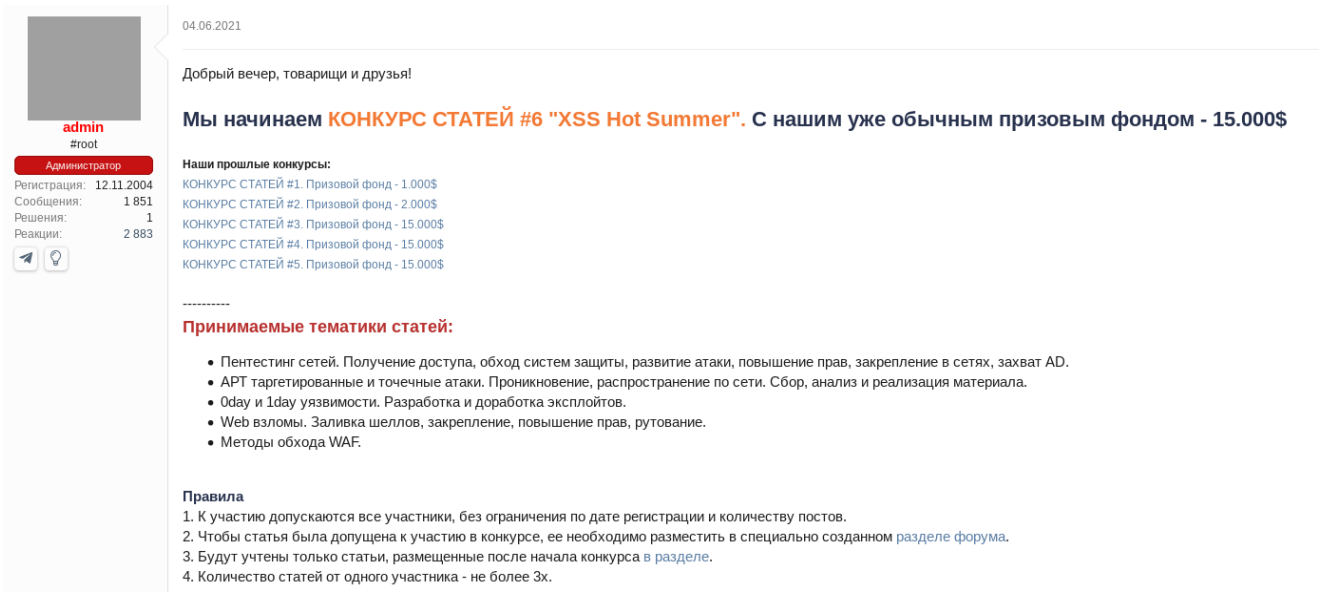


Figure 13 - *Screenshot from "xss" forum (Xss forum admin: "We are starting ARTICLES COMPETITION # 6 "XSS Hot Summer". With our already usual prize fund - $ 15,000. ")*

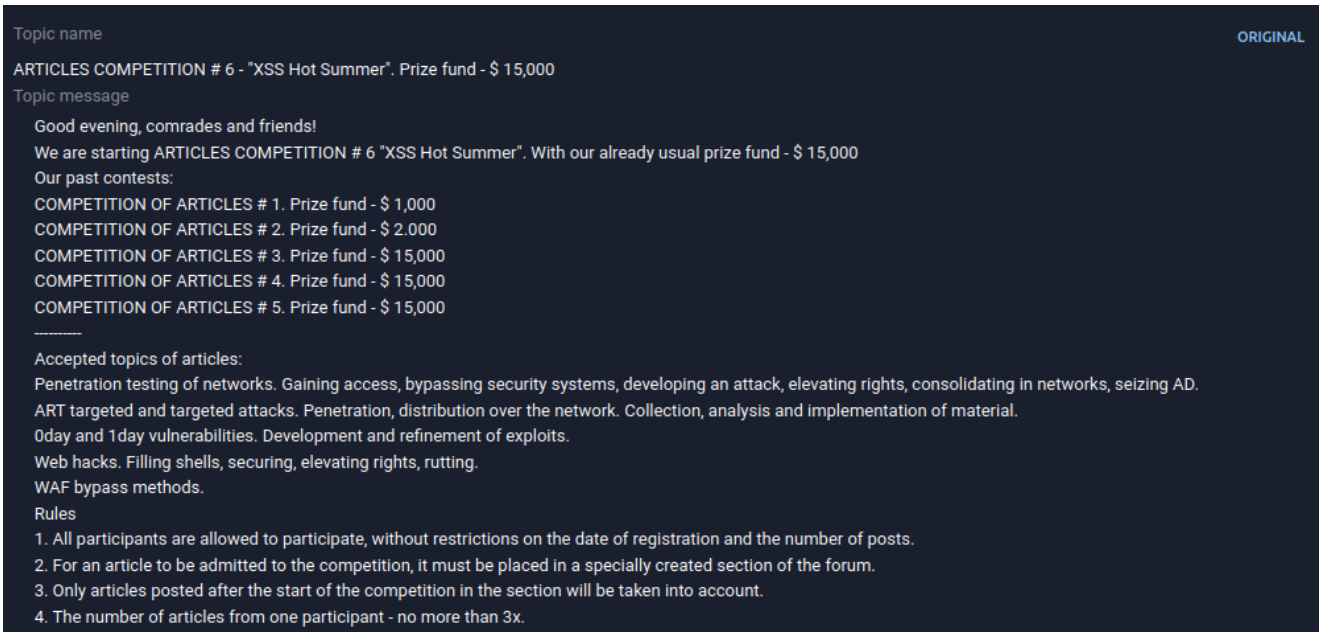


Figure 14 - Screenshot from Group-IB Threat Intelligence & Attribution system

This topic on the forum appeared 5 days after the first message from the owner of the card shop. Most likely, "AW_cards" talked about this contest with the "xss" administrator even before the card shop was launched.

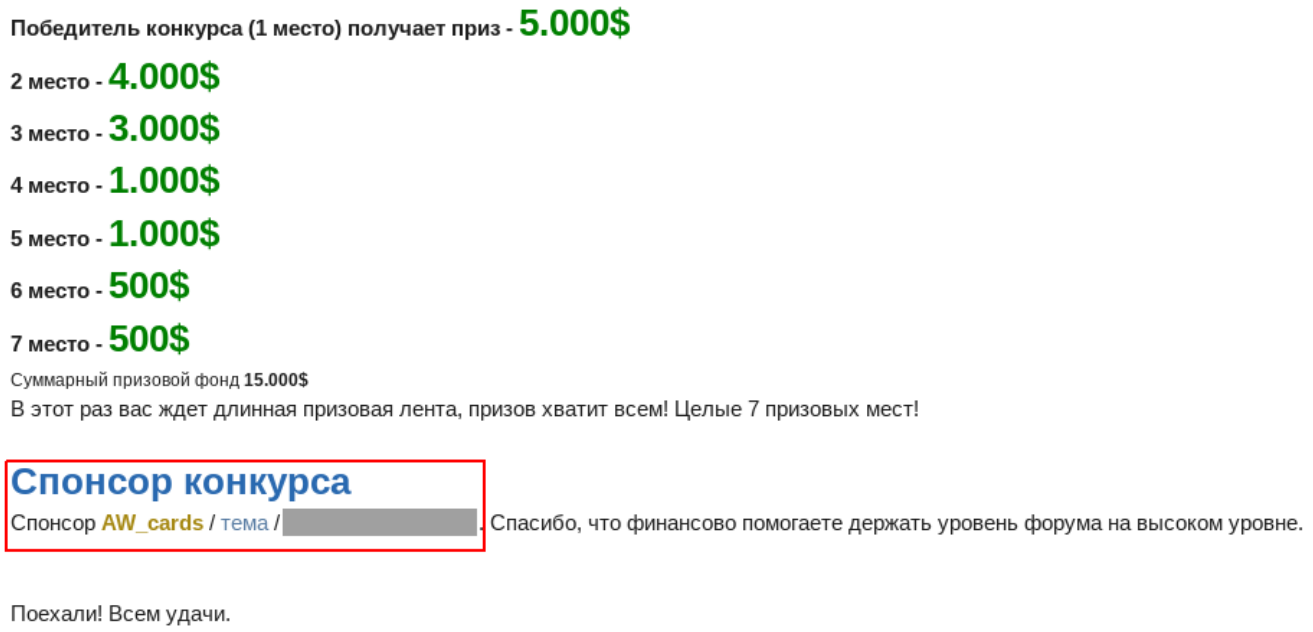


Figure 15 - *Screenshot from "xss" forum (Xss forum admin: "Competition sponsor Sponsor AW_cards."*

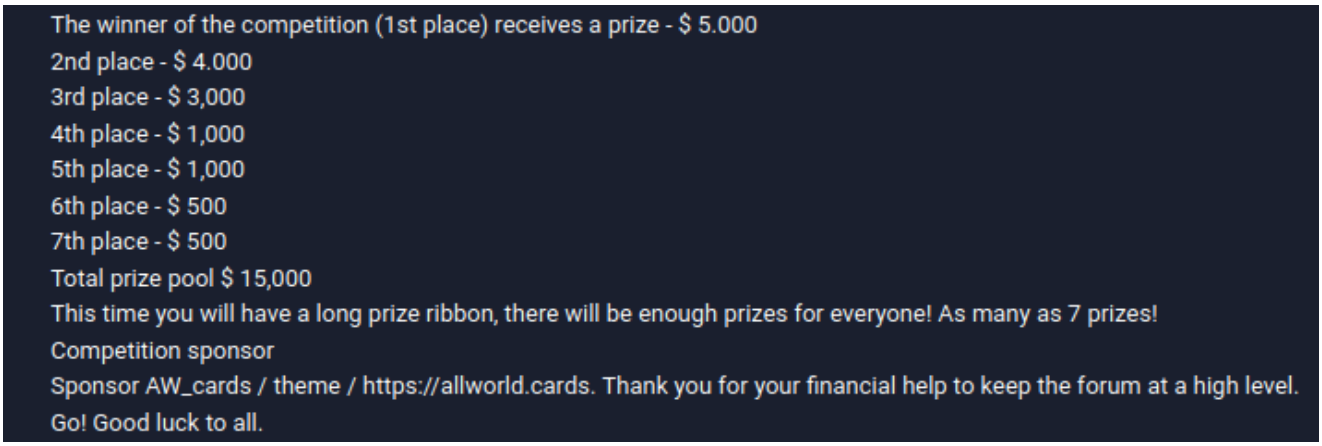


Figure 14 - Screenshot from Group-IB Threat Intelligence & Attribution system

Despite the fact that "All World Cards" is a new name among card shops, its owner is not new to the business of selling cards and administering such resources.

AW_cards has also written reviews in several threads with already published articles.

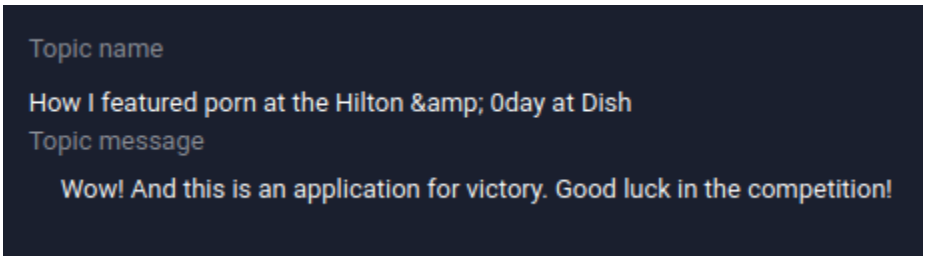


Figure 16 - Screenshot from Group-IB Threat Intelligence & Attribution system

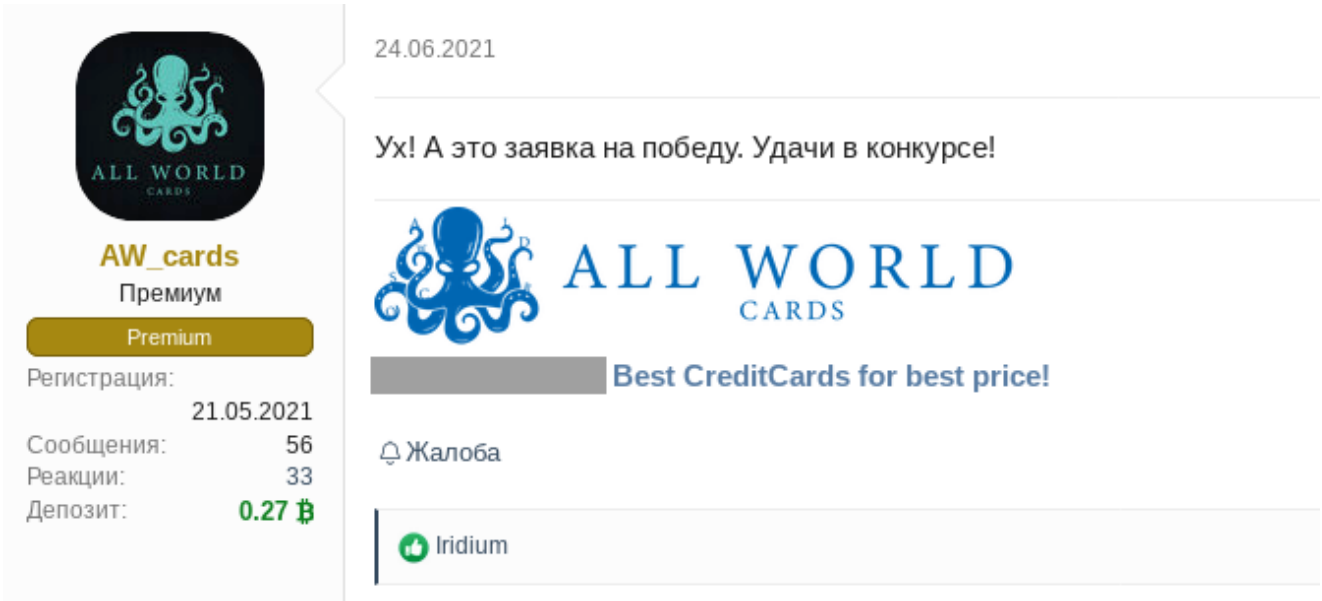


Figure 17 - *Screenshot from "xss" forum (AW_cards: "It looks like a winner. Good luck in the competition!")*

It is also worth noting that the "AW_cards" account on the "xxs" forum has a deposit of 0.27 Bitcoin ($ 8,500 at the August 2021 exchange).

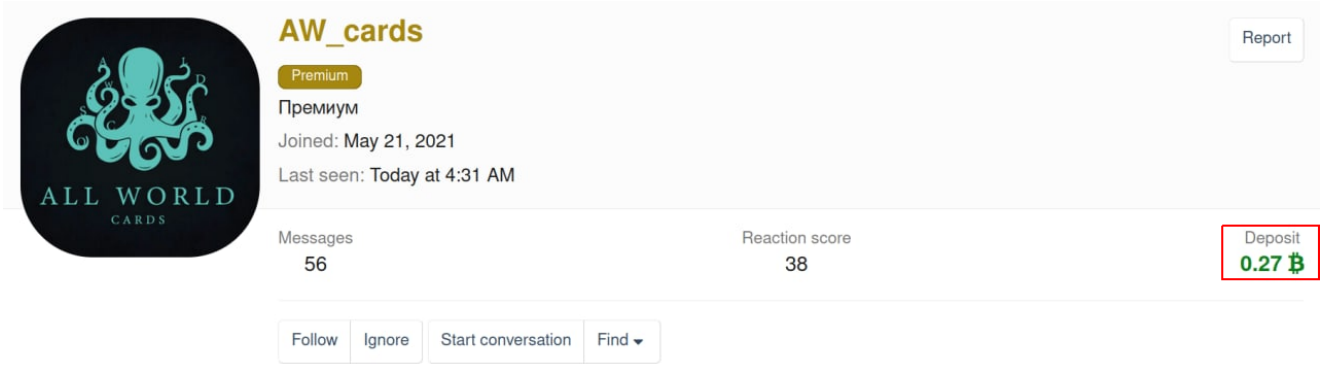


Figure 18 - *User page form "xss" forum*

This deposit can be spent on various transactions on the forum, but it can also serve as insurance and used to pay damages in case the deposit owner cheats on someone.

Making a deposit is most likely also some kind of advertisement, as forum users are more likely to trust accounts with deposit.

Conclusion

This is a unique case in which a new name for the marketplace business is using such a large financial investment to advertise its own cardshop. A total of 1 million cards offered for free is a unique case.

Despite the new name, the actions of the owners of the card shop to promote the new platform indicate that they are likely to be no strangers to this business. Since the creation of the market 2 months ago, more than 3.8 million cards have been placed on a card shop and more than 2.6 million are now on sale. Not all of the currently existing card shops can provide such an amount of compromised data.

Such a generous offer may indicate that "All World Cards" came into this business seriously and for a long time. This is most likely not the last time we hear about this card shop.