When Karma Comes Back

blog.group-ib.com/swarmshop

08.04.2021

The rise and fall of illicit cardshop breached twice in two years

Sergei Kokurin

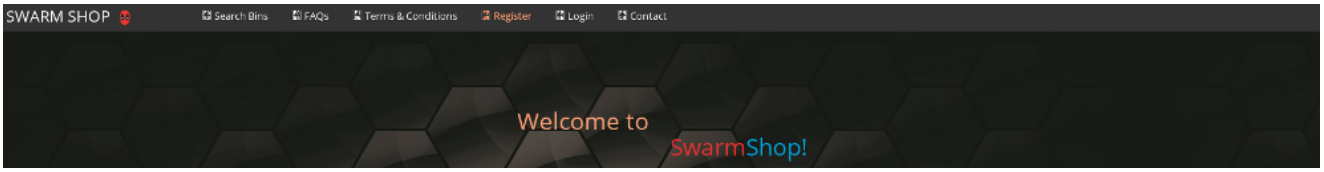
Threat Intelligence Analyst, Group-IB

Group-IB Threat Intelligence & Attribution system found that user data of the **Swarmshop** cardshop has been leaked online on March 17, 2021. The database was posted on a different underground forum and contained 12,344 records of the card shop admins, sellers and buyers including their nicknames, hashed passwords, contact details, history of activity, and current balance. In addition to user data, the database exposed all compromised data traded on the website, including 623,036 payment card records, 498 sets of online banking account credentials and 69,592 sets of US Social Security Numbers and Canadian Social Insurance Numbers.

While underground hacker forums get hacked from time to time, cardhsop breaches do not happen very often. In addition to buyers' and sellers' data, such breaches expose massive amounts of compromised payment and personal information of regular users. Although the source remains unknown, it must be one of those revenge hacks cases. This is a major reputation hit for the illicit cardshop as all the sellers lost their goods and personal data. The cardshop is unlikely to restore its status

Group-IB Threat Intelligence unit took a deep dive into the history of illicit cardshop, examined the driving forces behind its rise and fall, and discovered that the underground marketplace was breach twice in just two years by fellow cybercriminals.

Swarmshop profile



Swarmshop - is an underground mid-size "neighborhood" store for stolen personal and payment records. The cardshop has been operating since at least 2019, as the resource was first mentioned on underground forums in April 2019.

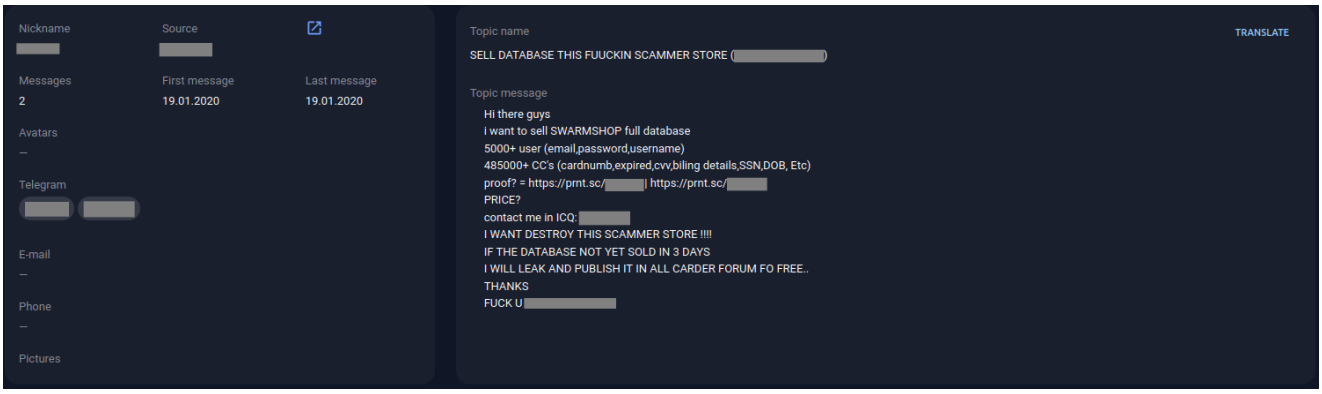
The user nicknamed "Swarmshop" is likely a cardshop administrator as they post information about updating databases and answers user questions on various forums under different nicknames. It is also known that cardshop admins are Russian-speaking.

By March 2021, it had more than 12K user base and over 600K payment card records on sale. The total amount deposited on all the accounts was at $18,145.73 – users of card shops do not store large amounts of money on their accounts and top up the balance to make payments if necessary.

This information was obtained from the data exposed in the March 2021 breach. Interestingly, it was not the first time Swarmshop has been targeted by fellow hackers. In January 2020, the cardshop's records were leaked on an underground forum.

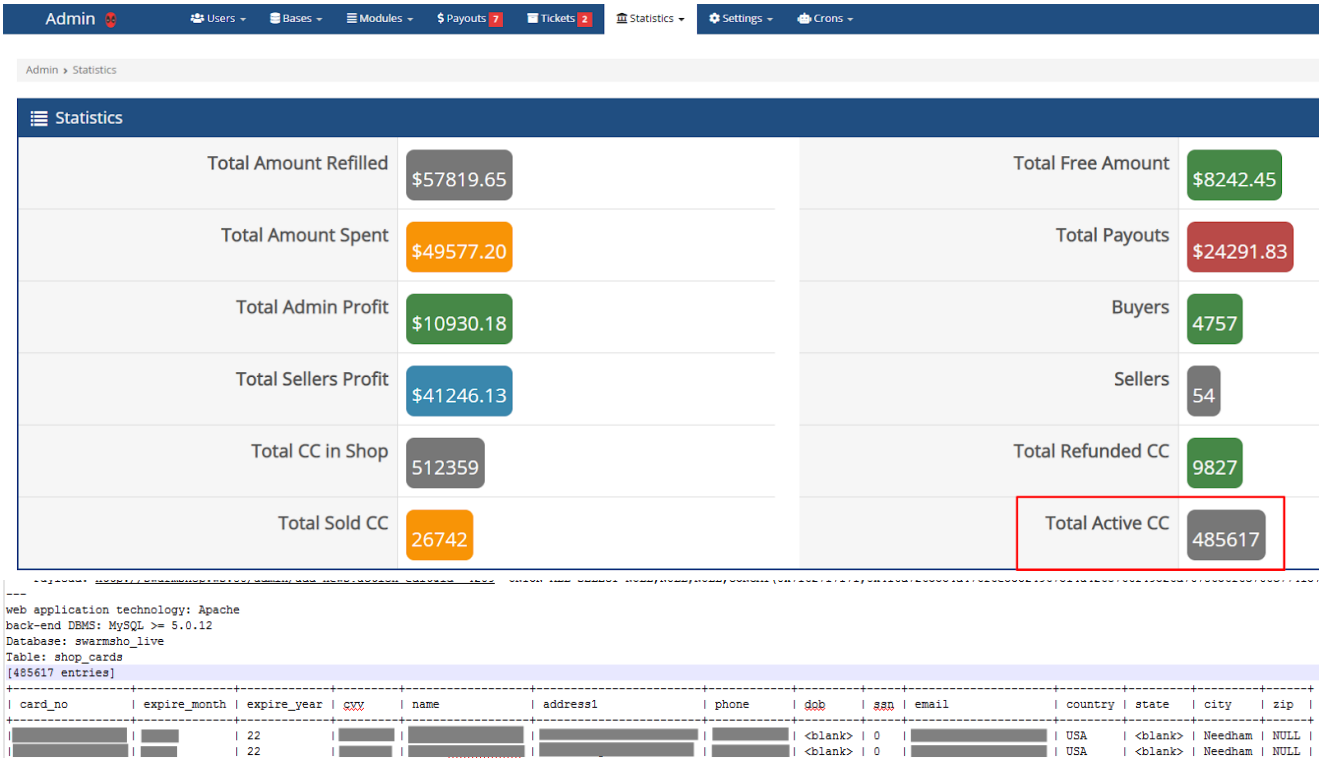
Swarmshop database leak in January 2020

On January 19, 2020, a user of the "procrd" forum, likely motivated by revenge, posted a message with an offer to sell the Swarmshop database.



Source: Group-IB Threat Intelligence & Attribution

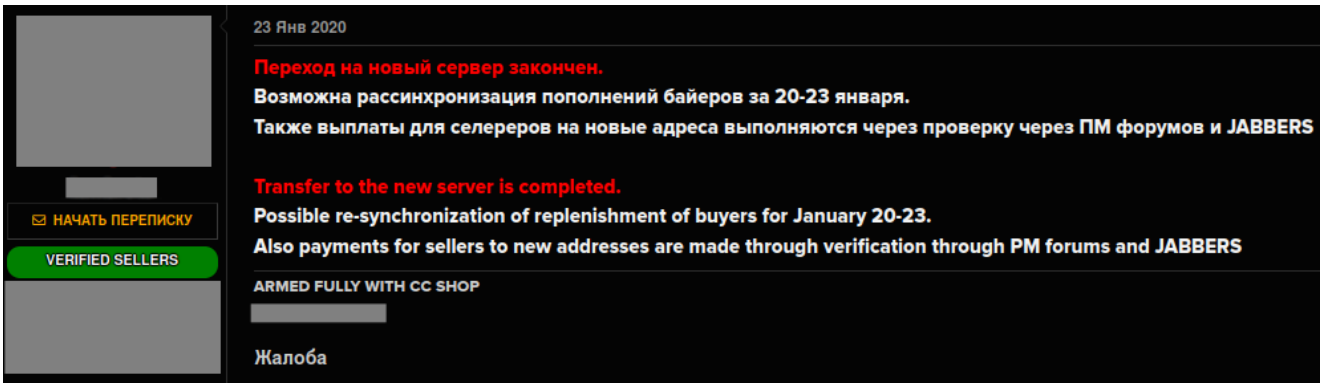
The user provided two screenshots as evidence, presumably taken from the admin panel of the Swarmshop.



Source: Group-IB Threat Intelligence & Attribution

The site administrators made no comment about the post, despite the fact that it was published in one of their advertising threads.

Four days later, an end-of-maintenance message appeared.



There were no other messages related to this database leak from neither the users nor the administrators.

Swarmshop database leak in March 2021

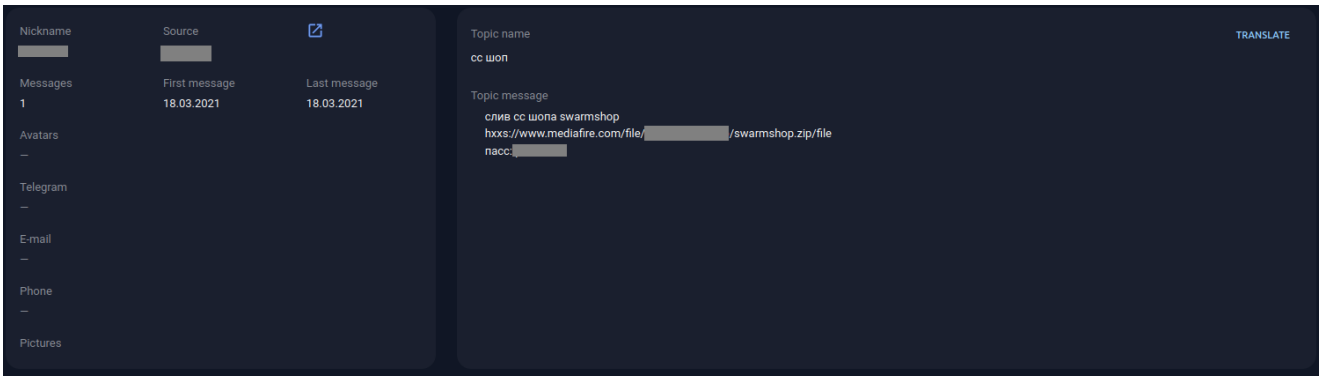
On March 17, 2021, a newly-registered user posted a link and password from the database of the "Swarmshop" market on the "crdclub" forum.

Screenshot from the "crdclub" forum

On March 18, 2021, a user with similar nicknames posted the same link and password on "tor" and "procrd" forums and added one sentence: "leak of cc shop swarmshop".

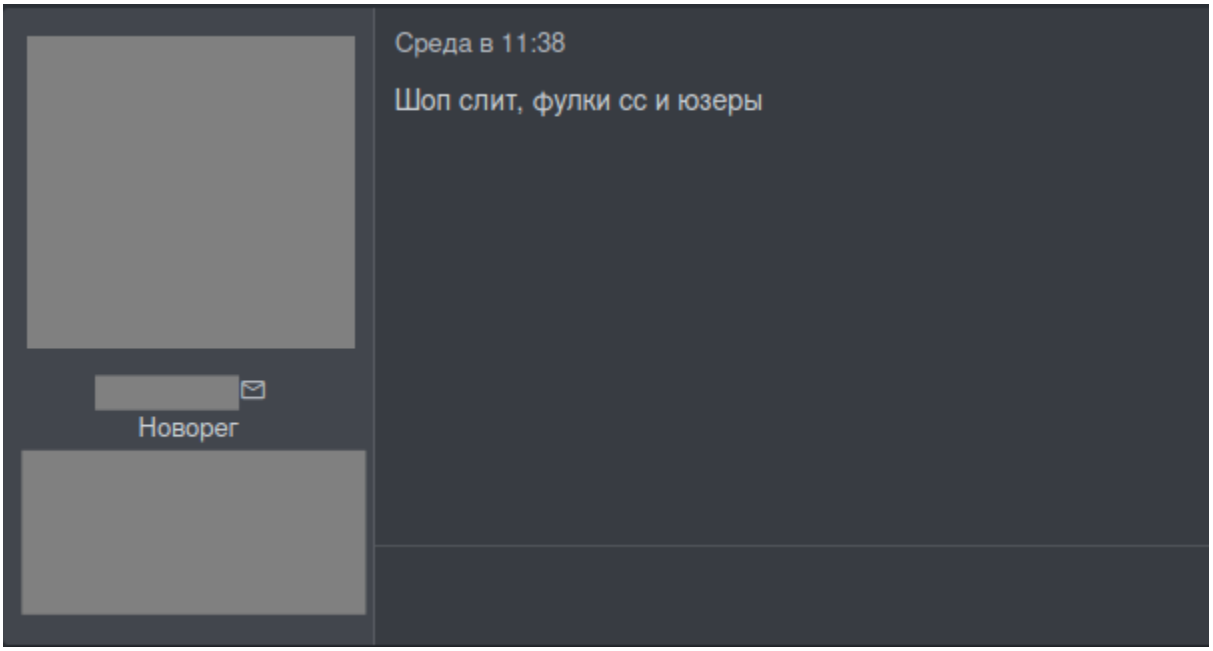
It should be noted that in the case of all three accounts that posted these messages, they were the user's first and only messages on the forums.

The post on procrd is currently deleted from the forum. Nevertheless, Group-IB Threat Intelligence & Attribution system was able to retrieve the original posts.



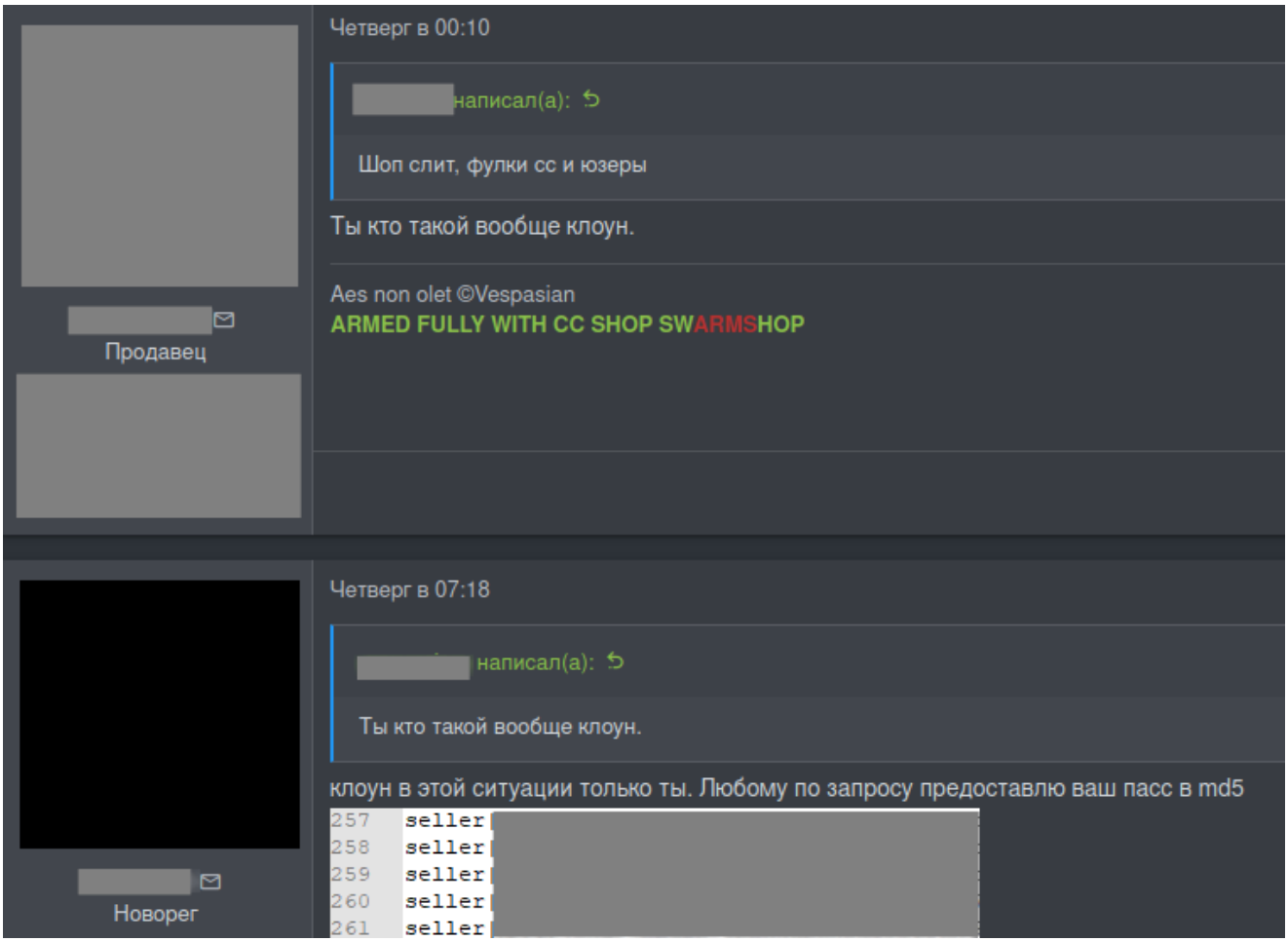
Source: Group-IB Threat Intelligence & Attribution

On March 17, twenty minutes after the first message about the Swarmshop database appeared. A different user posted a message about Swarmshop on the "bhf" forum in the topic dedicated to the market.



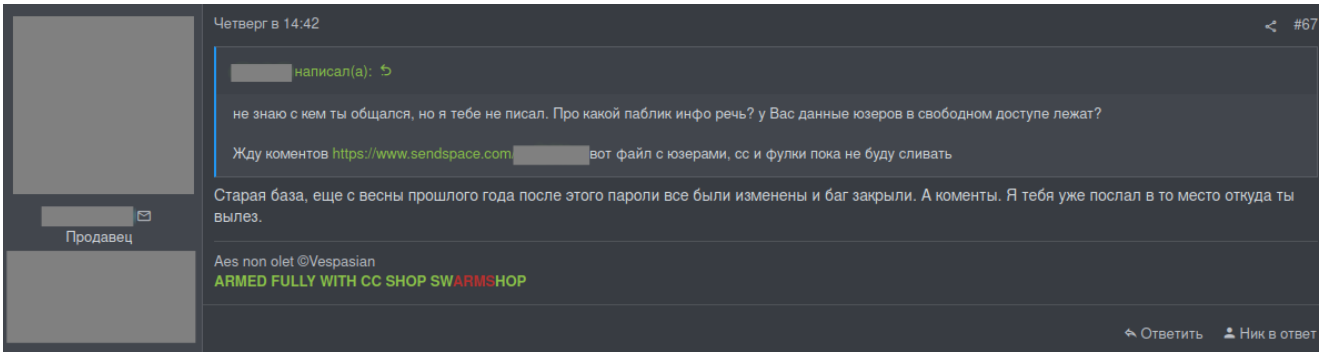
Screenshot from the "bhf" forum ("Shop leaked, full CC and users")

As is clear from subsequent messages, the website administrator was not aware that the database had been leaked.



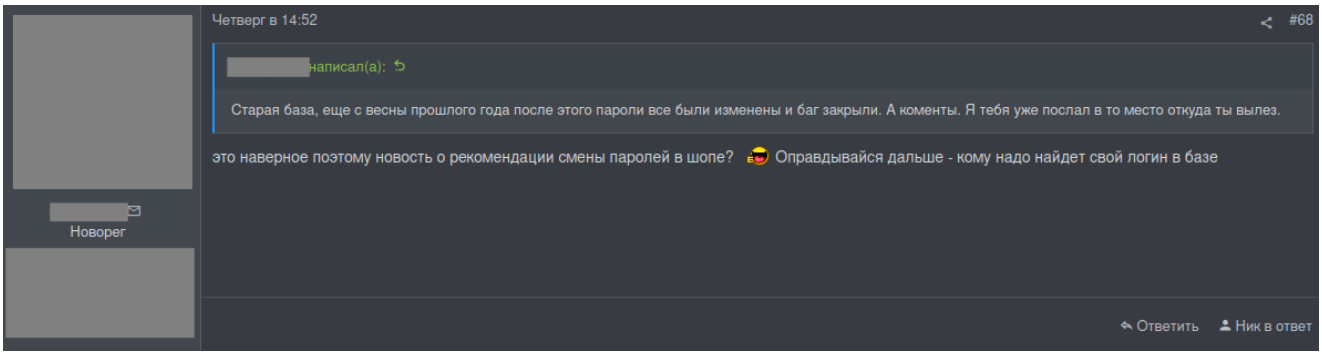
Screenshot from the "bhf" forum
(Swarmshop admin: "Who are you, clown?" bhf forum user: "You're the only clown in this situation. I will provide a pass in md5 at anyone's request")

In the last message, the administrator says that the data was leaked more than a year ago.



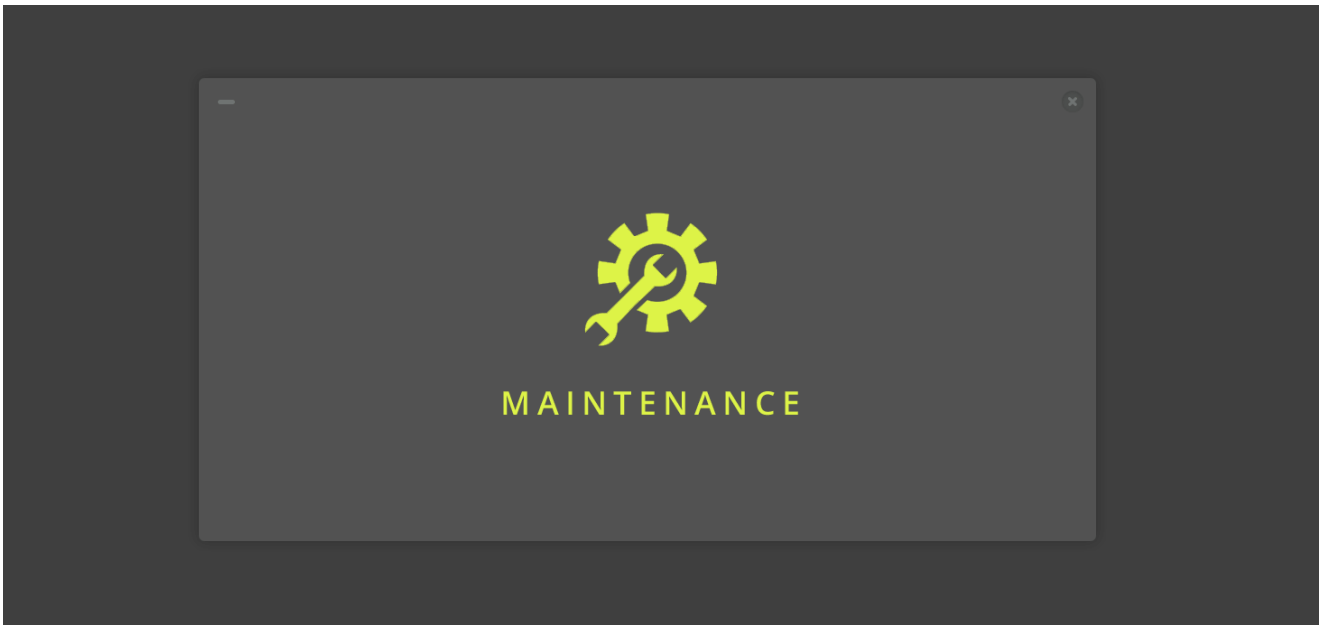
("The old database, since the spring of last year, after that, the passwords were all changed and the bug was closed. And the comments. I already sent you to the place where you came from.")

However, users reported that they received a recommendation to change their password on the website.

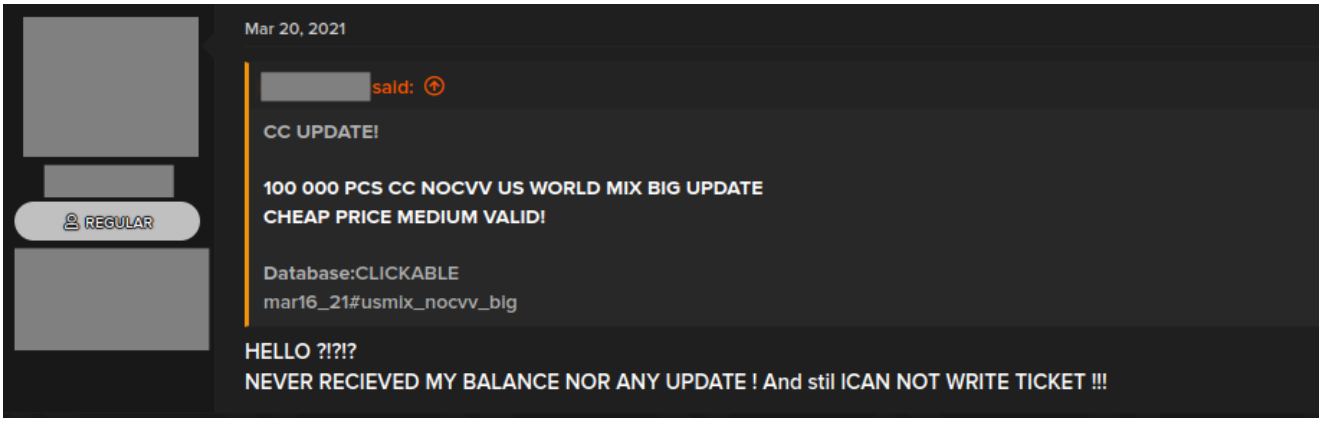


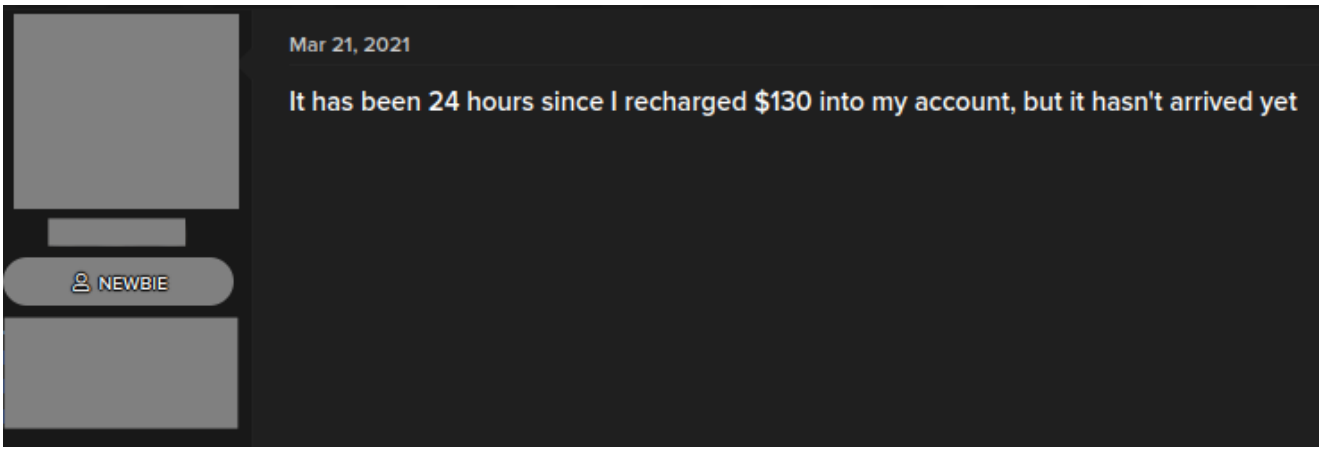
("This is probably the reason for the news about the recommendation of changing passwords in the shop? Keep justifying yourself - anyone who needs to will find their username in the database")

Within a week of the leak, if someone tried to enter the website, occasionally a message was displayed: "Maintenance".

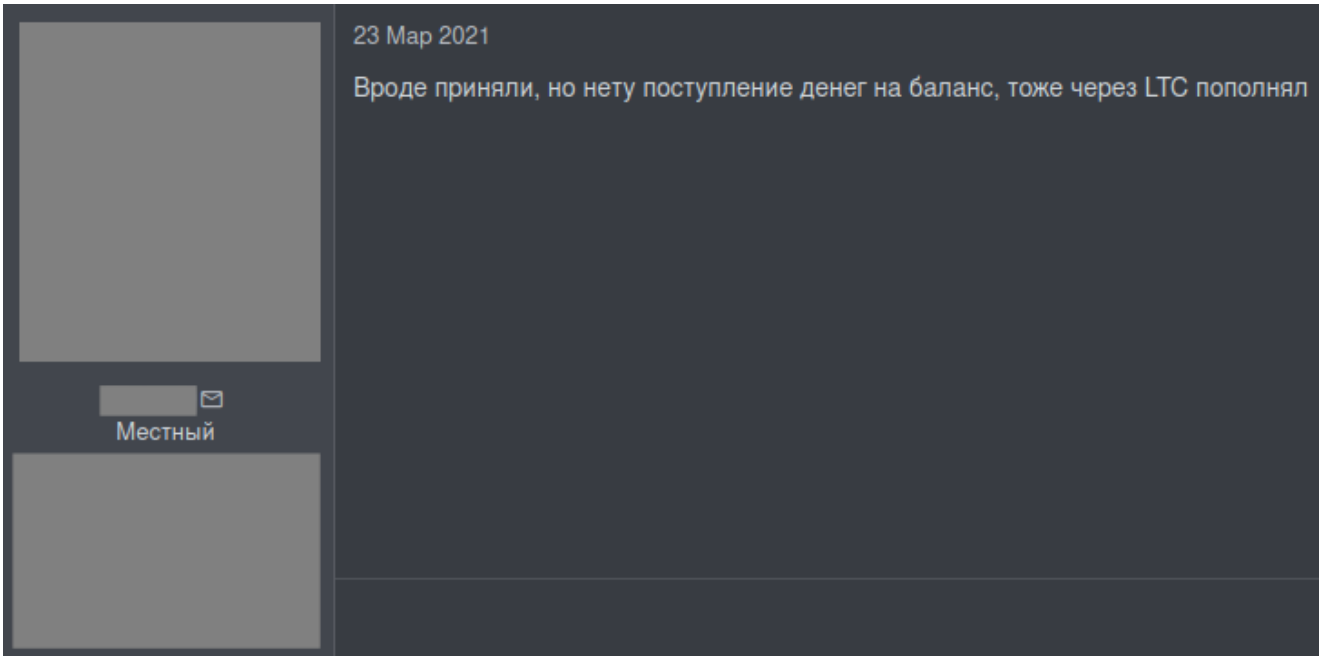


At the same time, users experienced problems with their balance, the ticket system, and trying to communicate with the website administrator.



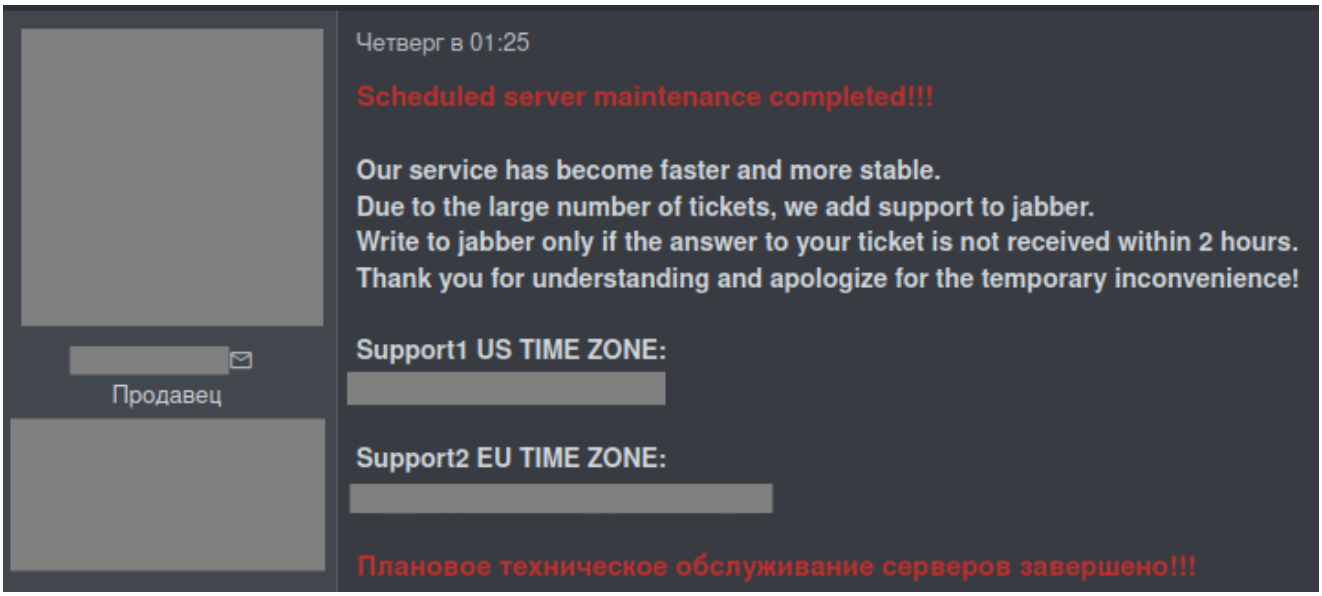


Screenshots from the "ascarding" forum



Screenshot from the "bhf" forum ("It seems to have been accepted, but the money has not been transferred to the balance, I also replenished it through LTC")

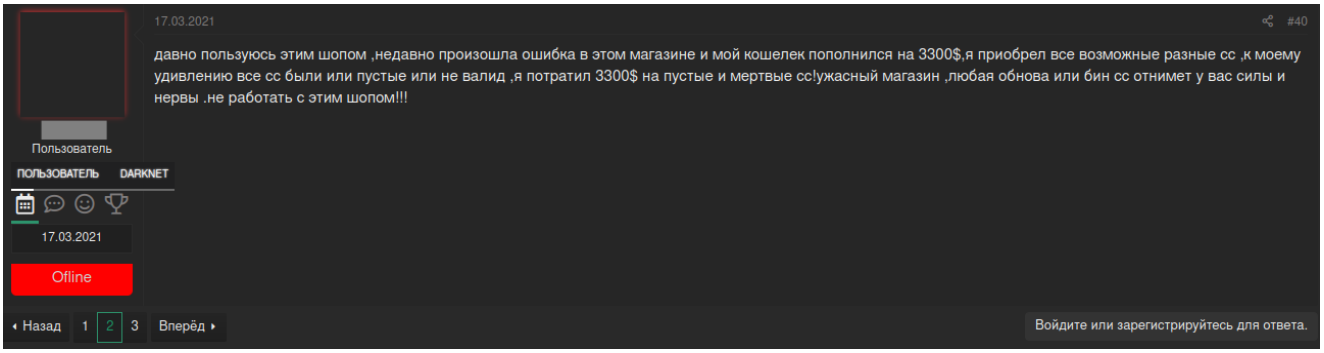
On March 25, the Swarmshop administrator posted a message about server maintenance ending. The message also mentioned the high number of tickets received.



Screenshot from the "bhf" forum

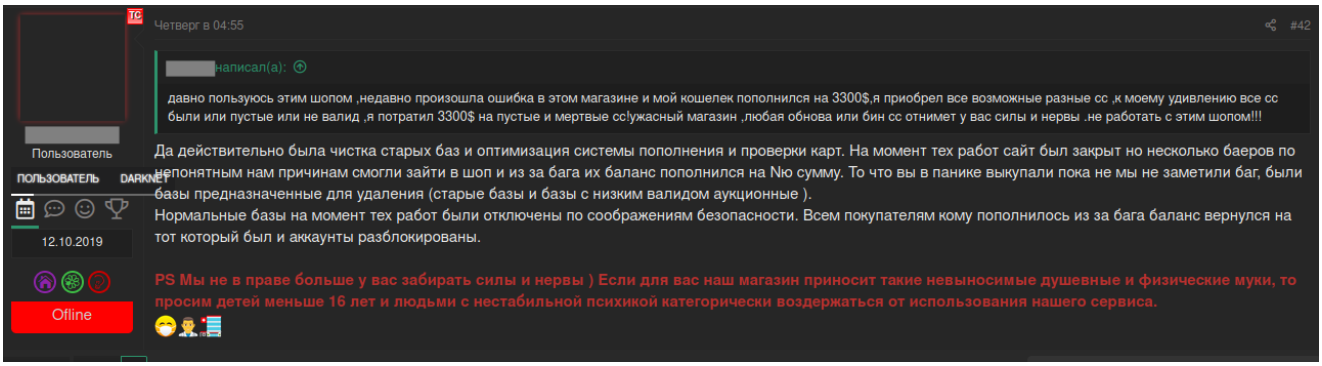
The messages appeared on various forums in all topics related to the Swarmshop market.

On one of the forums, on March 17, a few hours after the first message with the Swarmshop database was posted, one of the users complained about problems with the site. They said that a large balance was suddenly credited to his account, but all the purchased cards were invalid.



("I have been using this shop for a long time, recently there was an error in this store and my wallet was replenished with $3,300, I purchased all possible cc, to my surprise all cc were either empty orinvalid, I spent $3,300 on empty and dead cc! awful store , any update or bin cc will take away yourstrength and nerves. do not work with this shop !!!")

The response from the administrator did not come until March 25, after the maintenance report. According to the response, an error occurred in connection with updating databases and removing old, "non-working" cards.



("Yes, old databases really were cleaned out and the system for replenishing and checking cards was optimized. At the time when this was being done, the site was closed, but for some unknown reasonseveral buyers were able to enter the shop and, due to a bug, their balances were replenished by N amount. What you bought in a panic before we noticed the bug were databases intended for deletion (old bases and bases with a low validity auction). At the time that work was being carried out, normal bases were shut down for security reasons. For all buyers who replenished due to the bug,we returned their balance to what it was before and the accounts have been unlocked.")

Analysis of information exposed in March breach

The analysis of the database found the structured data files subdivided into two categories:

- Detailed compromised payment and personal records traded on the cardhsop
- Information about cardshop admins, sellers, and buyers.

Swarmshop users in the database are divided into three groups: "Admin" (website administrators and moderators),"Seller" (accounts belonging to sellers who post data for sale), and "Buyer" (accounts belonging to regular users).

Each account is assigned one of four statuses. "Active" (valid account without restrictions) on the one hand, and "Archive", "Blocked", and "Suspended" on the other (presumably accounts with various kinds of restrictions to access the site).

The analysis of the freshly exposed database found that the information was new as it indicated the latest user activity timestamps. Considering that the most recent date in the database is March 10, 2021 08:18:36, it can be assumed that the data was downloaded between 8:18 and 9:00 on March 10. However, the time zone cannot be deduced from the files.

In total, the databased revealed the records of **4** cardshop admins, **90** sellers, and **12,250** buyers of stolen data, including their nicknames, hashed passwords, account balance, and contact details for some entries. The share of various statuses are shown in the table below.

In the case of Buyer accounts, the amount of funds deposited into the account was also indicated: $18,145.73. Users of card shops do not store large amounts of money on their accounts and top up the balance to make payments if necessary.

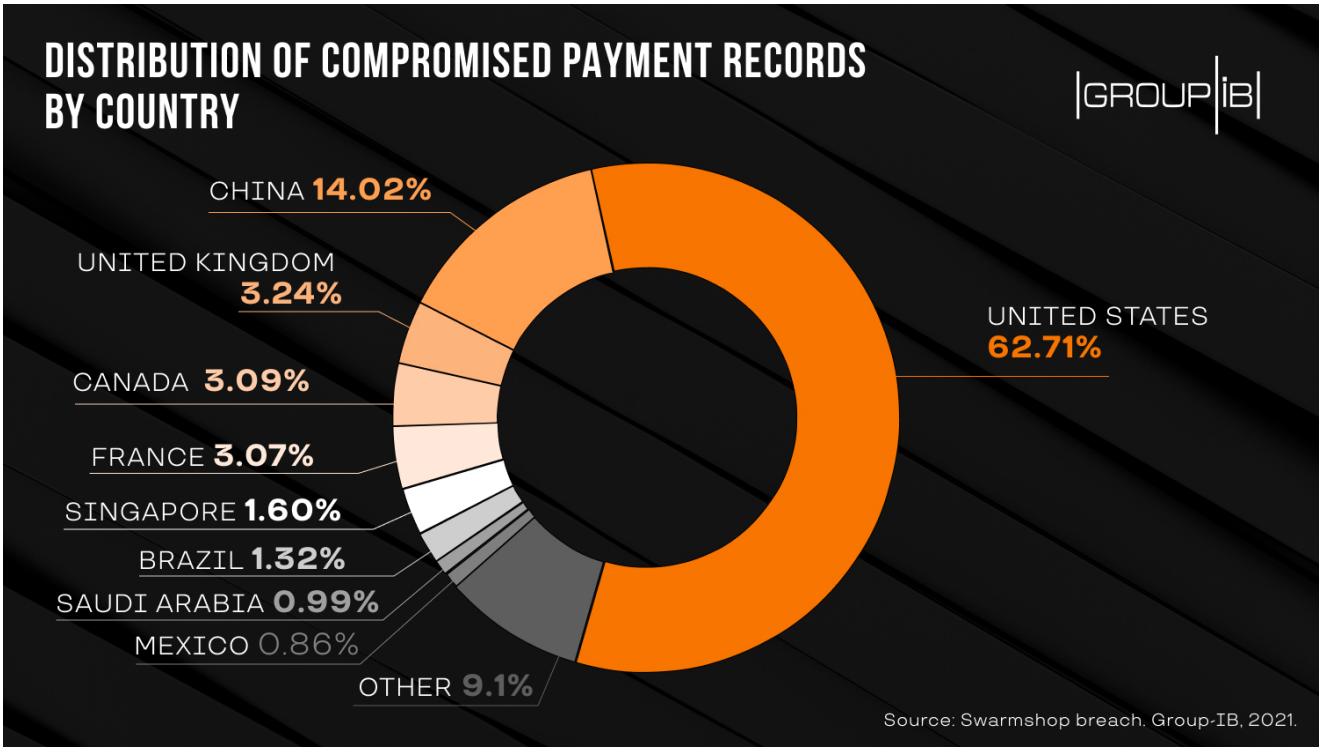
While the source of the breach remains unclear, the exposed records show that two card shop users attempted to inject a malicious script searching for website vulnerabilities in the contact information field. It's impossible to determine if the two events are connected to the breach.

```
ctive|2021-02-15 14:59:17
|archive|2019-06-19 21:08:56
3ef|0.46| |active|2020-12-02 08:31:13
ef|0.00| |archive|2019-08-15 22:21:47
archive|2019-08-03 06:47:00
8| |active|2020-09-28 09:00:27
00|&amp;amp;amp;amp;amp;amp;amp;gt;&amp;amp;amp;amp;amp;amp;amp;lt; src=https://[redacted]lo.xss.[redacted]&|active|2021-01-26 05:40:08
.00| |archive|2019-06-05 16:19:02
rchive|2020-01-26 11:30:21
 |active|2020-12-27 21:37:40
|archive|2019-06-05 15:51:03
00| |archive|2019-05-02 18:53:25
00| |archive|2020-12-02 08:31:23
 |archive|2020-03-07 04:25:47
|active|2021-03-10 05:13:44
active|2021-01-25 11:47:10
```

Compromised payment and personal records in the database were divided into three types:

- CC - full bank card details (number, expiration date, owner name, etc.)
- VBA - login and password for online bank accounts or payment systems
- SSN - Social Security Number (also contained SIN – Social Insurance Numbers in Canada)

The dump contained **623,036** payment card records, **62.7 percent** of which were issued by the US banks. Other records were issued by the financial institutions from China (14.02%), the UK (3.24%), Canada (3.09%), France (3.07%), Singapore (1.6%), Brazil (1.32%), Saudi Arabia (0.99%), and Mexico (0.86%). Group-IB notified the national CERTs in the abovementioned countries about the breach so they could take the necessary steps to mitigate the threat.



In addition to stolen bank cards, the database revealed **498** sets of online banking account credentials and **68,995** sets of US Social Security Numbers and **597** pieces of Canadian Social Insurance Numbers.

Companies that process user personal and payment information need to ensure the integrity and security of customer data by putting in place advanced Threat Intelligence & Attribution solutions which allow to monitor for leaked credentials. Constant underground monitoring for compromised personal and payment customer records, gives banks and financial organisations the ability to mitigate risks and further damage by quickly blocking stolen cards.

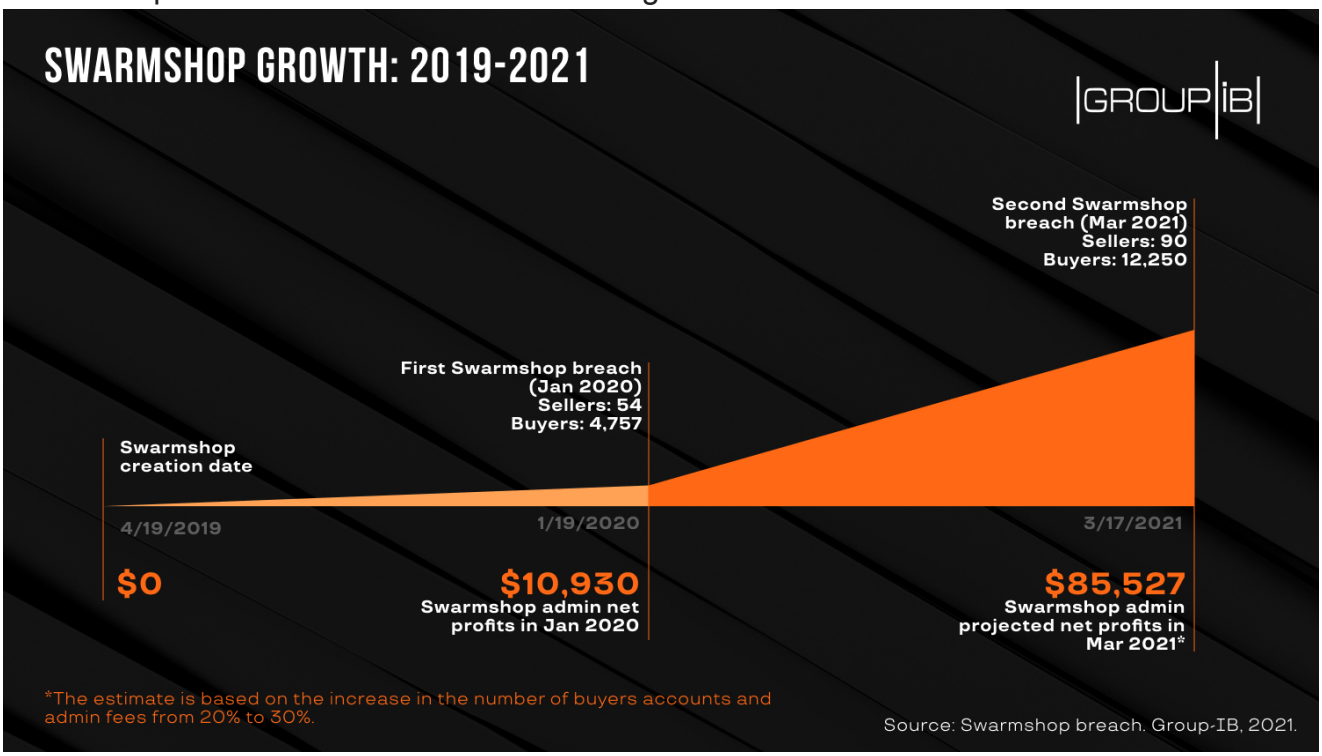
Swarmshop growth: 2019 - 2021

Based on the data obtained from the leaks that occurred in 2020 and 2021, it is possible to analyze how the market developed over the years.

For example, "Seller" accounts increased by 36 (90 in total compared to 54 at the time of the first leak). The number of "Buyer" accounts grew more than 2.5 times (from 4,757 to 12,250). It is worth clarifying, however, that the number of discovered accounts is only a total number and does not reflect the number of users who were active on the resource. Another parameter using which we were able to compare the two leaks is the unspent funds on "Buyer" accounts: $8,242 during the leak in 2020 and as much as $18,145 during the data breach in March, 2021.

The net profit of the Swarmshop administrators at the time of the first leak was about $1,300 per month, while in 2021 it is fair to assume that it was as much as $5,300 per month. The

change is due to an increase in the total number of "Buyer" accounts and fees for Swarmshop administration services increasing from 20% to 30%.



Recommendations for financial organisations

● Notify users of possible risks in the online payment process when using bank cards.

● If payment cards related to your bank have been compromised, block these cards and notify the users as soon as possible.

● Receive first-hand reports about compromised payment and personal records sales on the Dark web. Check for the cards issued by the bank in the DBs for sale.

To access unique closed sources, and improve your visibility into the underground card shops you may use **Group-IB Threat Intelligence & Attribution.**

Share

Receive insights on the latest cybercrime trends