

A FRESH LOOK INTO THE UNDERGROUND CARD SHOP ECOSYSTEM

Beatriz Pimenta Klein

Lidia López Sanz



AGENDA

1. Introduction: underground card business models
 - a. Types of products offered, how these markets work
2. The card shop ecosystem
 - a. Methodology
 - b. Major card shops currently active
 - c. Closed and seized card shops
3. Fighting credit card fraud (advice and prevention)
4. Conclusive remarks

2021-01-15

Finale

END OF JOKER'S STASH

“we wish all young and mature ones cyber-gangsters not to lose themselves in the pursuit of easy money. Remember, that even all the money in the world will never make you happy”



---- ENG ----

Joker goes on a well-deserved retirement. Joker's Stash is closing.
When we opened years ago, nobody knew us. Today we are one of the largest cards/dumps marketplace.
Unfortunately, or fortunately - nothing lasts forever. It's time for us to leave forever.
We will leave the Stash opened for 30 more days, until 2021-02-15, so all Stash users can spend accounts balances.
On 2021-02-15 we will wipe all our servers and backups and Joker will fade to dark, forever.
And mark my word: WE WILL NEVER EVER OPEN AGAIN! Do NOT trust possible future imposters!
After 2021-02-15 there will be no more Joker and no more Joker's Stash.
Dear partners of Stash - you can be sure, that before we leave forever, you will get all payouts, contact me you know how.

We are also want to wish all young and mature ones cyber-gangsters not to lose themselves in the pursuit of easy money.
Remember, that even all the money in the world will never make you happy and that all the most truly valuable things in this life are free.

WHERE ARE CARDS SOLD?



AUTOMATED VENDING
CARTS (AVCS)



MARKETPLACES



SPECIALIZED FORUMS
AND CHATS

PRODUCTS – HOW ARE THESE OBTAINED?

- Dumps - payment card information
 - Point-of-Sales (PoS) malware: dump process memory, extract track data, exfiltrate stolen information
 - Skimmers



ATM skimmer

PRODUCTS – HOW ARE THESE OBTAINED?

- CVVs - also known as “cards”
 - Phishing pages;
 - Digital skimmers;
 - Leaked databases;
 - Information-stealing malware.



HOW BUYERS CASH OUT?

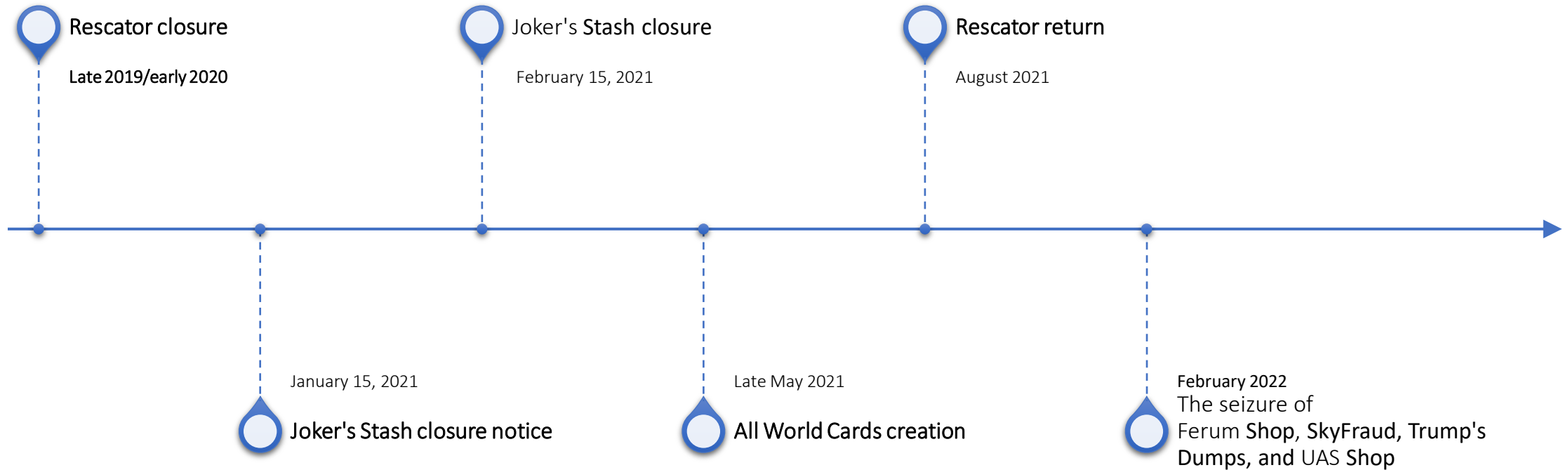
- Card-present fraud
 - Uses counterfeit cards created with dumps
- Card-not-present fraud
 - Employs CVVs data

THE CARD SHOP ECOSYSTEM

METHODOLOGY

- How to identify and select important shops?
 - Advertisement in **forums** (threads and sponsorship);
 - Reactions and feedbacks;
 - **Telegram** channels + subscribers (plus);
 - **Marketing actions**;
 - Shop's **structure**.

TIMELINE: WHAT HAPPENED SINCE JS' CLOSURE?





- Bitcoin, Litecoin, Dash, and Cryptocheck;
- Free registration; add balance within 5 days.



- Checkers (\$0.5 per check).
- SSN / Date of Birth lookup service (offline).
- Free tools: bins lookup, zip lookup, track1 generator.
- Education Blog, Knowledge Base, Tutorials and Guides + FAQ + Rules



DUMPS

Prices: US\$3 - US\$269.6

CVVs

Prices: US\$8.4 - US\$84

☐ Off Live filtering. Warning! Slows down page loading.

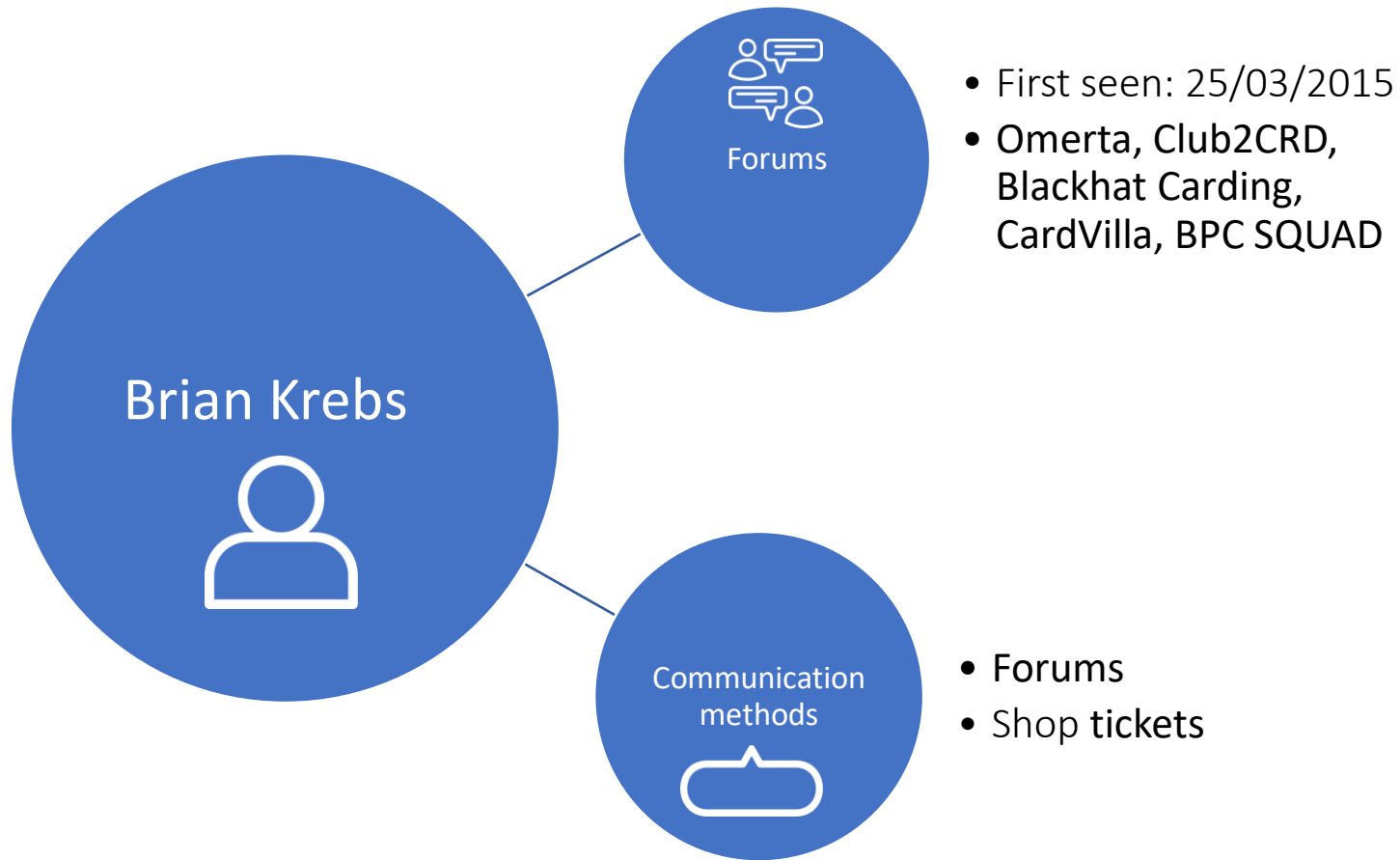
Bins:	<input type="text"/>	Country:	<input type="text" value="- all -"/>	Type:	<input type="text" value="- all -"/>	Base:	<input type="text" value="- all -"/>
Bins (8 digit):	Search by 8 digits is available for users with a rating of 5 crab and above. About rating	State:	<input type="text" value="- all -"/>	Credit/Debit:	<input type="text" value="- all -"/>	Exp Date:	<input type="text" value="03/22"/>
Bank:	<input type="text" value="- all -"/>	City:	<input type="text" value="- all -"/>	Subtype:	<input type="text" value="- all -"/>	Price Range:	<input type="text" value="- all -"/>
Bank Country:	<input type="text" value="- all -"/>	ZIPs:	<input type="text"/>	Code:	<input type="text" value="- all -"/>	Track1	<input type="checkbox"/>
Card Number:	Search by last 4 digits is available for users with a rating of 2 crab and above. About rating					PIN	<input type="checkbox"/>
						refundable only	<input type="checkbox"/>
						billing zip	<input type="checkbox"/>
						EDD+pin ⓘ	<input type="checkbox"/>

Clear

Search

<input type="checkbox"/>	Bin ↕	Type	Debit/Credit	Subtype	Exp Date	Track1	Billing zip	Code	Country	Address	Bank	Base	Price	Cart
<input type="checkbox"/>	527690		CREDIT	N/A	XX/24	-	-	201			N/A (); non refundable	Llama	16.80 \$	
<input type="checkbox"/>	424840		CREDIT	N/A	XX/26	-	-	201			N/A ()	Barge	53.66 \$	
<input type="checkbox"/>	527690		CREDIT	N/A	XX/24	-	-	201			N/A (); non refundable	Llama	16.80 \$	
<input type="checkbox"/>	528546		CREDIT	N/A	XX/24	✓	-	201		CO; Aurora	REGIONAL BANKS ASSOCIATION OF JAPAN (); non refundable	Doc	40.95 \$	

THREAT ACTOR PROFILE – *BRIAN KREBS* (NOT THE JOURNALIST)



BRIAN KREBS

02-02-2017, 13:32

Brian Krebs ▾

Vendor of:
Dumps

Join Date: Feb 2017

Posts: 1,605

Reputation: **21** [+/·]

Balance: **0.00\$**

Hello, cybercrooks!

Would you like to buy dumps and credit cards with cvv2 from the legendary Brian Krebs? In my shop you will find fresh firsthand dumps & cards at a great price!

What you can buy:

- Dumps with Track 1 & Track 2 and billing zip code
- Credit Cards with CVV2
- Social Security Numbers and Date of Birth lookups

What makes me different:


- Auction that allows you to reserve, bid and outbid others who want to purchase exotic BINs
- Free gift/dump for everyday shoppers
- Social Security Number & Date of Birth lookup service to change PIN or approve large transactions for the dumps & cards you buy
- Dumps with billing zip codes
- Lottery where anyone can win large amount of money
- 3 crab rating is fixed for old school and high deposit customers
- Fully automated loan/credit request system

Shop domains:

- <https://briancrabs.at>
- <https://briancrabs.de>
- <https://briancrabs.cm>
- <https://briancrabs.vc>
- <https://briancrabs.mx>

- <https://briansclub.cm>
- <https://briansclub.mx>







BRIAN KREBS



Brian Krebs
(forum Heros)

Joined: 03-20-2020
D.O.B: Not Specified
Local Time: 03-15-2022 at 04:45 PM
Offline

Last Visitors

 (03-04-2022 - 07:36 PM),  (02-27-2022 - 04:51 AM),  **LegendaryRescator** (11-14-2021 - 10:59 AM),  (11-09-2021 - 11:01 PM),  (05-28-2021 - 02:37 PM),  (05-08-2020 - 02:21 AM)

LEGENDARY RESCATOR IS BACK



- Bitcoin only;
- Free registration.



- Checkers: dumps and CCs (\$0.5 per check);
- Wholesale – dump packages;
- For VIP customers updates available for 1 hour earlier.



DUMPS

Prices: US\$6.07 - US\$62.37

CVVs

Prices: US\$10 - US\$36

Country	CC type	CC mark	Debit/Credit
<div>All</div> All USA	<div>All</div> All Visa Master	<div>All</div> All Gold Platinum	<input checked="" type="checkbox"/> DEBIT <input checked="" type="checkbox"/> CREDIT
Zips & Bins	Bank & State & City	Base	Additional
<div>91111, HJ4111</div> <div>380282, 376282</div>	<div>Bank: All</div> <div>State: All</div> <div>City: All</div>	<div>All</div>	<input type="checkbox"/> Expiring 03/22 <input type="checkbox"/> Phone <input type="checkbox"/> VBV <input type="checkbox"/> Birthday <div>Exp. date (1312)</div>

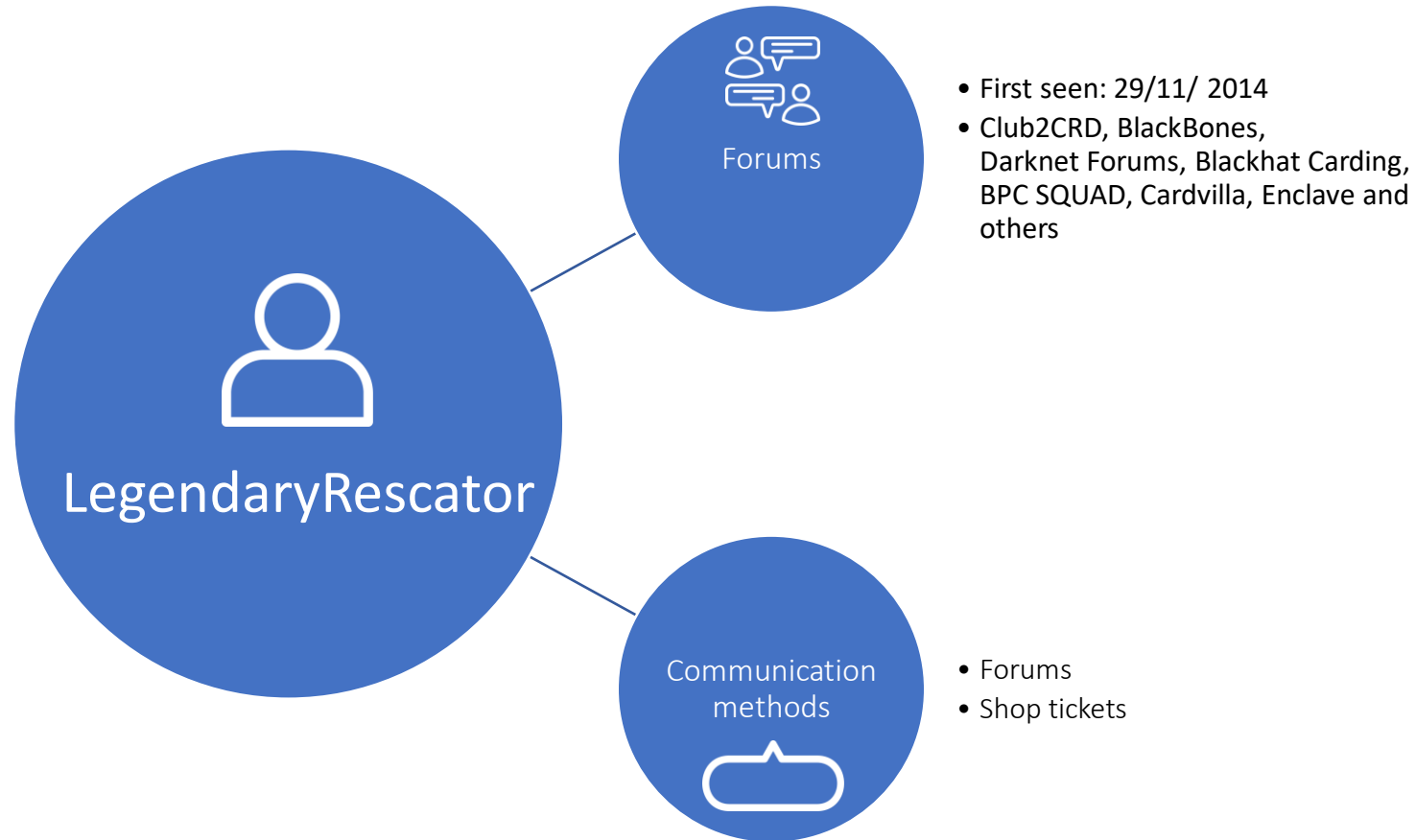
Save money and buy packs at wholesale prices. Pay less - get more. Go to [Wholesale section](#) of the shop!

Clear

Search

<input type="checkbox"/>	Bin	Card	Debit/Credit	Mark	Expires	Country	State	City	Zip	Phone	VBV	Birthday	Base	Price	Cart
<input type="checkbox"/>	431947	 VISA ALLIED IRISH BANKS PLC	DEBIT	CLASSIC	07/2023	 Ireland	Dublin16	DUBLIN 16	D16X2W4				AirASIA 	24\$	<div>+</div>
<input type="checkbox"/>	533621	 MASTERCARD PEOPLES TRUST COMPANY	DEBIT	PREPAID	07/2023	 Canada	QC	Montreal	H3B 2M3	Yes			USA_JK4 	24\$	<div>+</div>

THREAT ACTOR PROFILE - *LEGENDARYRESCATOR*



INACTIVE CARD SHOPS

- Organized closure: early warnings, justification;
- Seized by law enforcement;
- Exit scam.

FERUM

- English-language card shop active since 2013;
- It used to include a banner ad for competitor Trump's Dumps, possibly indicating a link between the two shops;
- Seized by the Russian Ministry of Internal Affairs in early February 2022.

FERUM CVVS SECTION

Filter:

BINs:

Country:

(3) ▾

State:

City:

Zip:

Type:

Any ▾

Base:

Any ▾

Search

Reset

Cards found: **4445757**

Card number	Expire	Name	City	State	Zip	Country	Base	Check time	Price	<input type="checkbox"/>
5596010*****	05/21	GOODWILL	City	state	zipcode	INDIA	OLD BASES 2017		\$6.90	<input type="checkbox"/>
6521831*****	12/24		City	state	zipcode	INDIA	OLD BASES 2017		\$6.90	<input type="checkbox"/>
4838123*****	11/24		City	state	zipcode	INDIA	OLD BASES 2017		\$6.90	<input type="checkbox"/>
6071239*****	01/23	K	City	state	zipcode	INDIA	OLD BASES 2017		\$6.90	<input type="checkbox"/>
6073864*****	02/24	PUSHPA	City	state	zipcode	INDIA	OLD BASES 2017		\$6.90	<input type="checkbox"/>
4363030*****	01/22		City	state	zipcode	INDIA	OLD BASES 2017		\$6.90	<input type="checkbox"/>



ALLWORLD CARDS

We publish **1,000,000 bank cards for public access.**

The validity is about **20%**. All material from 2018-2019.

Fields: *CC_Number Exp CVV Name Country State City Address Zip Email_Phone*

An action of unprecedented generosity from [AllWorld.Cards](#)

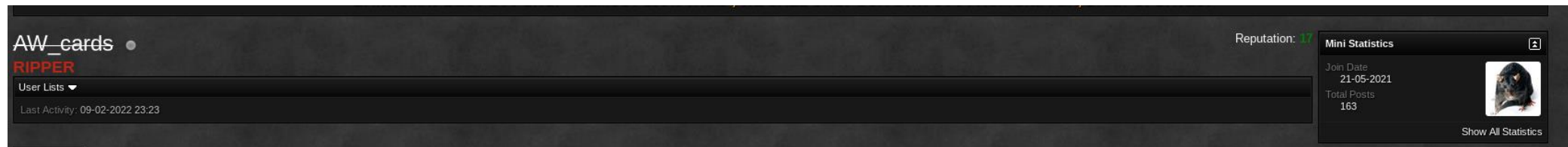
Checking the validity of 98 random cards

Checked: 98 of 98

Valid: 26 (27%)

Total cost: 12.90\$

The password for the archive is the Tor domain.



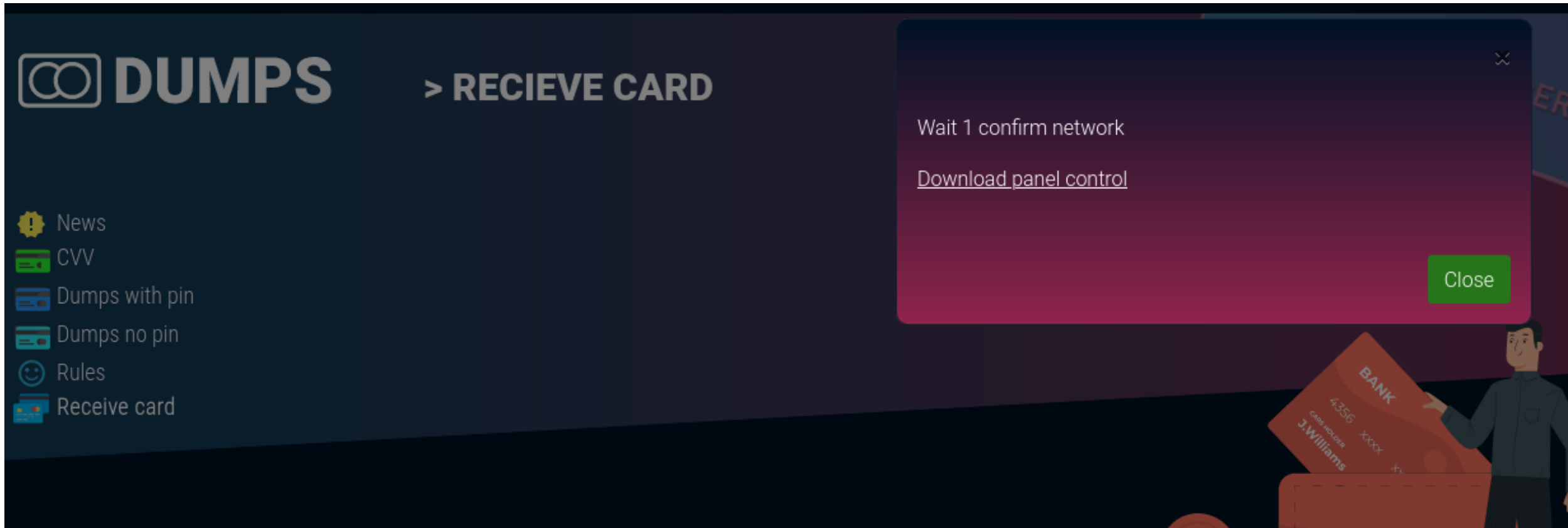
CARD SHOPS SCAM

- Thousands of phishing cards shops with typosquatting domains similar to popular card shops.
- Whois registry ~March 2022.
- All phishing card shops have listed the same fake cards.
- "Receive card" section downloads clipboard hijacker malware.

- News
- CVV
- Dumps with pin
- Dumps no pin
- Rules
- Receive card

Bin + Zip	Type	Subtype	EXP	Name	Country	State	Bank	Base	Email	DOB	SSN	MMN	Price	Buy
438955 N/A	VISA	CLASSIC	07/23	N/A	ROMANIA	N/A	RAIFFEISEN BANK, S.A.	fresh-cvv	0	0	0	0	\$ 5	ADD
533155 N/A	MASTERCARD	STANDARD	10/23	N/A	ROMANIA	N/A	RAIFFEISEN BANK S.A.	fresh-cvv	0	0	0	0	\$ 5	ADD
529913 N/A	MASTERCARD	STANDARD	03/23	N/A	ROMANIA	N/A	BANCA TRANSILVANIA S.A.	fresh-cvv	0	0	0	0	\$ 5	ADD
535230 N/A	MASTERCARD	STANDARD	12/23	N/A	POLAND	N/A	BANK POLSKA KASA OPIEKI S.A. - (BANK PEKAO S.A.)	fresh-cvv	0	0	0	0	\$ 5	ADD
535470 N/A	MASTERCARD	STANDARD	10/23	N/A	POLAND	N/A	POWSZECHNA KASA OSZCZEDNOSCI BANK POLSKI S.A. (PKO BANK POLSKI S.A.)	fresh-cvv	0	0	0	0	\$ 5	ADD
557511 N/A	MASTERCARD	STANDARD	02/23	N/A	POLAND	N/A	MBANK S.A.	fresh-cvv	0	0	0	0	\$ 5	ADD
516931 N/A	MASTERCARD	STANDARD	09/23	N/A	POLAND	N/A	POWSZECHNA KASA OSZCZEDNOSCI BANK POLSKI S.A. (PKO BANK POLSKI S.A.)	fresh-cvv	0	0	0	0	\$ 5	ADD
421352 N/A	VISA	CLASSIC	05/23	N/A	POLAND	N/A	BANK ZACHODNI WBK, S.A.	fresh-cvv	0	0	0	0	\$ 5	ADD
535693 N/A	MASTERCARD	N/A	04/24	N/A	POLAND	N/A	N/A	fresh-cvv	0	0	0	0	\$ 5	ADD
557524 N/A	MASTERCARD	STANDARD	09/24	N/A	POLAND	N/A	BANK POLSKA KASA OPIEKI S.A. - (BANK PEKAO S.A.)	fresh-cvv	0	0	0	0	\$ 5	ADD
424671 N/A	VISA	CLASSIC	04/24	N/A	POLAND	N/A	ING BANK SLASKI, S.A.	fresh-cvv	0	0	0	0	\$ 5	ADD
557511 N/A	MASTERCARD	STANDARD	04/25	N/A	POLAND	N/A	MBANK S.A.	fresh-cvv	0	0	0	0	\$ 5	ADD

CLIPPER MALWARE DOWNLOAD LINK



FIGHTING CARD FRAUD

- Implement EMV 3-D Secure (3DS2) protocol;
- Stay on top of the latest standards (e.g. PCI DSS v4.0);
- Keep all hardware and software up to date;
- Active scanning for skimming equipment and devices at ATM.

CONCLUSIONS

- The card shops landscape is highly fluctuating, as it is impacted by momentum.
- The importance of continuously monitoring the status of the landscape.
 - Future trends: card-not-present > card present.
- Scamming is a part of the ecosystem, taking advantage of the fluctuating scenario.

QUESTIONS?



beatriz.pimenta@blueliv.com



Beatriz Pimenta Klein



lidia.lopez@blueliv.com



Lidia López Sanz