#westonhecker #skimbadsoftware

Goodbye Memory Scraping Malware

Hold Out Till "Chip And Pin”.
Weston Hecker Security Expert With KLJ

SKIMBAD

Systems Network Analyst/Penetrations Tester/President Of Computer Security Association Of North Dakota

Who Am I What Do I Do What's the Talk About,

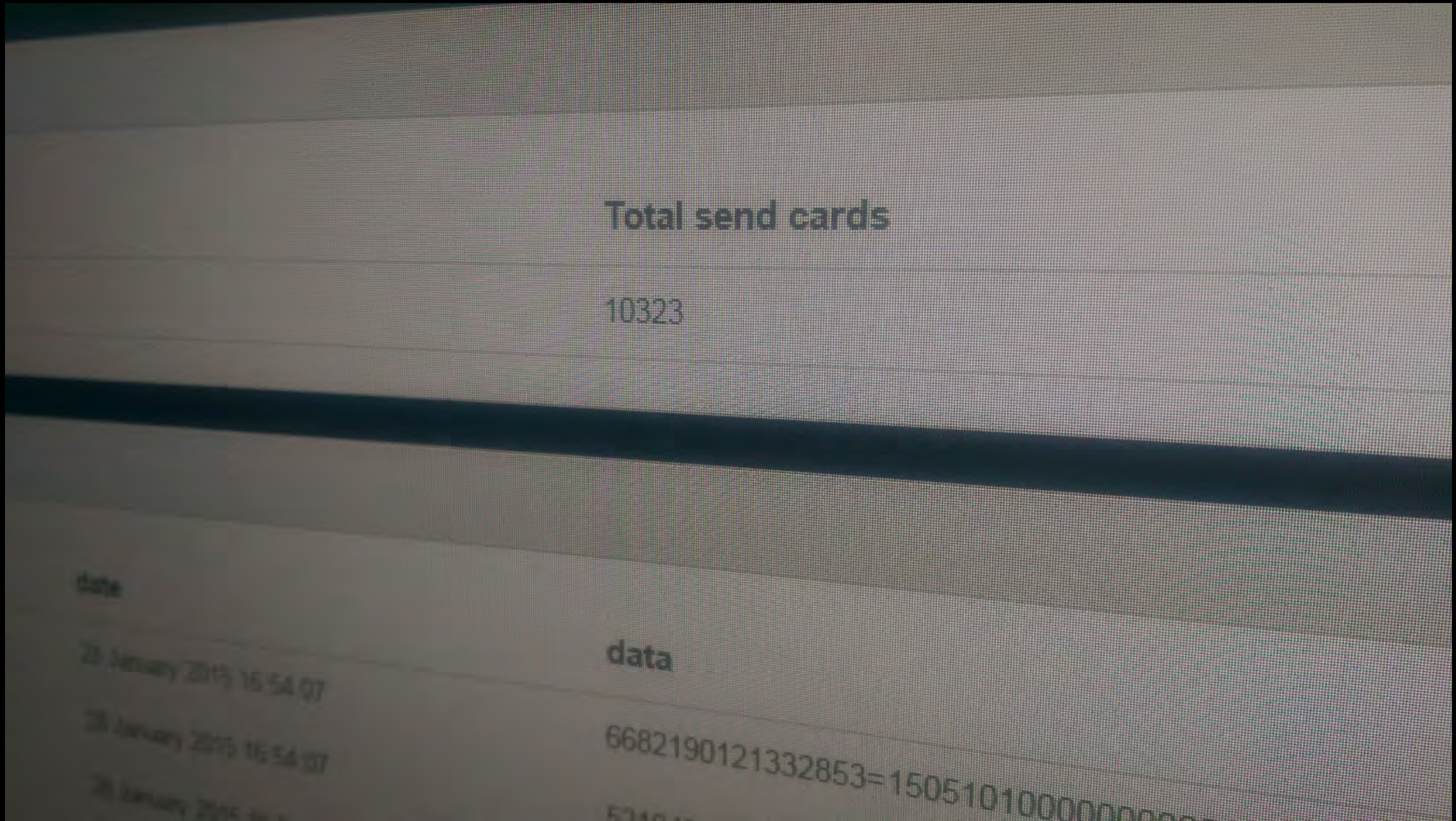
- About Me: Speaker at Defcon 22 Tons of Computer Certs, Computer Science/Geophysics
- About 11 years pen-testing, security research , Spoke at Defcon 22 Las Vegas on Burnerphone DDOS
- NERC, FFIEC, FISMA/NIST, ISO, GLBA and FDIC, Compliance audits HIPAA, Omnibus,
- Wrote custom exploits for obscure Internet service provider gear and PMS software.
- Tools of the trade “Fleet of Fake I phones” And now android variance.
- Co-writer of Skimbad Software Open source anti malware skimming software OPEN SOURCE. This talk today will be going of this new concept of protecting Data
- Pentesting for a living everything from banks, hospitals and ISP in the Mid-west. I live and work in North Dakota
- Security projects including Reverse engineering of malware and tracking software. Working on 911 Attack mitigation projects.

TEENSY 3.1 Container!!!

Build Your Own There Awesome !!!
Hit me up on Twitter or E-mail me.

START THE DEMO !!!

- This will Run while I speak
- We will check the number at the end of the Presentation
- The Graphical demonstration version is available on Skimbad.com
- Source Code and EXE are Available on GitHub



Total send cards

10323

date

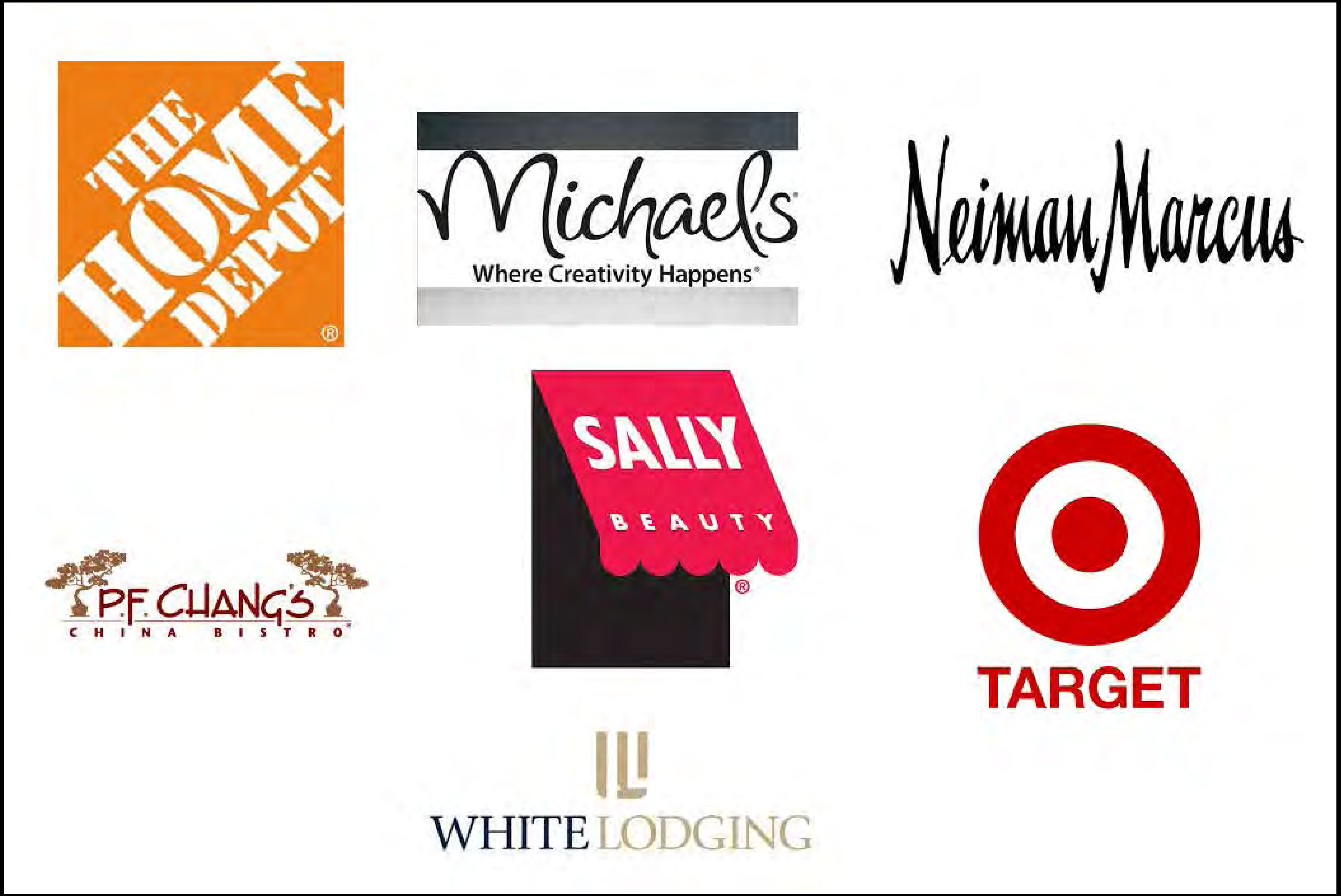
data

28 January 2015 16:54:07

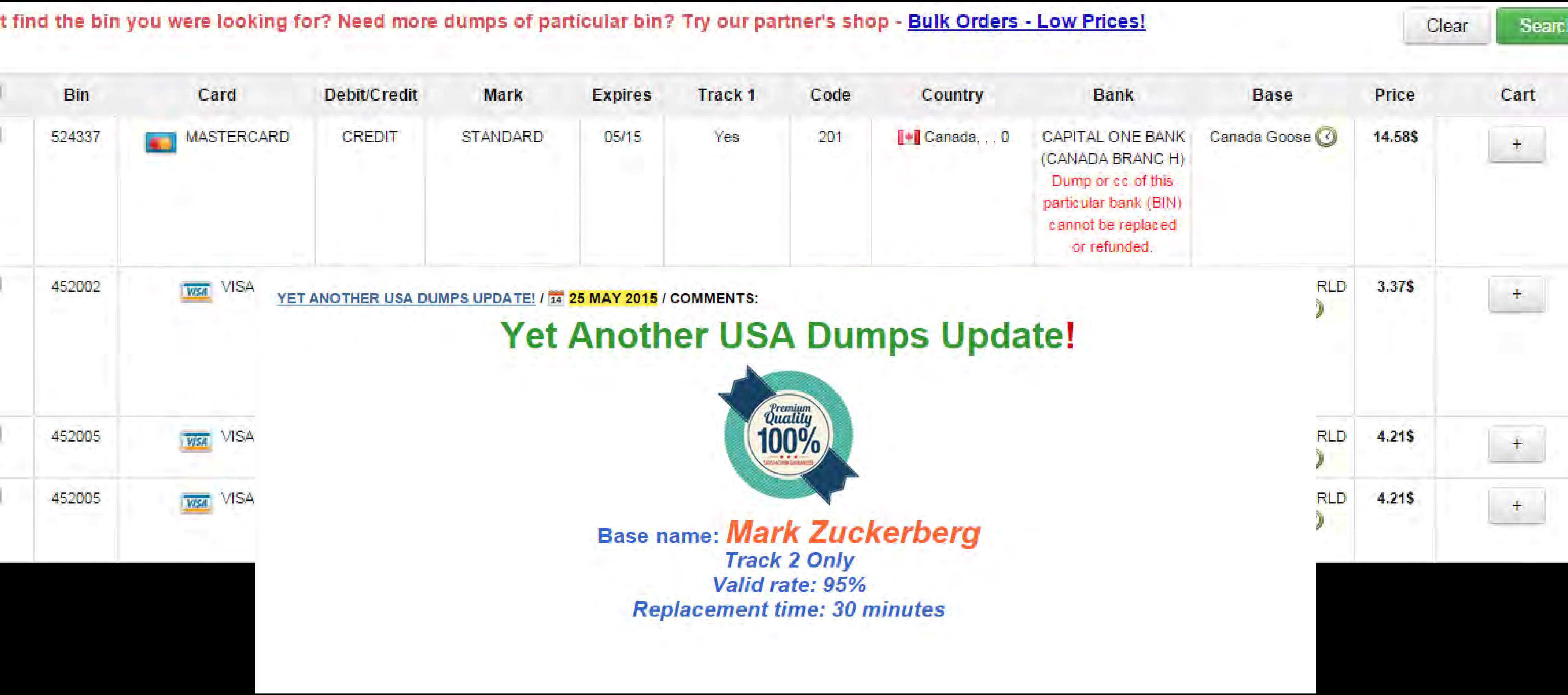
28 January 2015 16:54:07

6682190121332853=150510100000000

The problem of Data skimming malware/ Large Profile cases



Why do people skim data / how much does it cost



t find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - Bulk Orders - Low Prices!

Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
524337	MASTERCARD	CREDIT	STANDARD	05/15	Yes	201	Canada, , , 0	CAPITAL ONE BANK (CANADA BRANC H) Dump or cc of this particular bank (BIN) cannot be replaced or refunded.	Canada Goose	14.58$	+
452002	VISA								RLD	3.37$	+
452005	VISA								RLD	4.21$	+
452005	VISA								RLD	4.21$	+

YET ANOTHER USA DUMPS UPDATE! / 14 25 MAY 2015 / COMMENTS:

Yet Another USA Dumps Update!

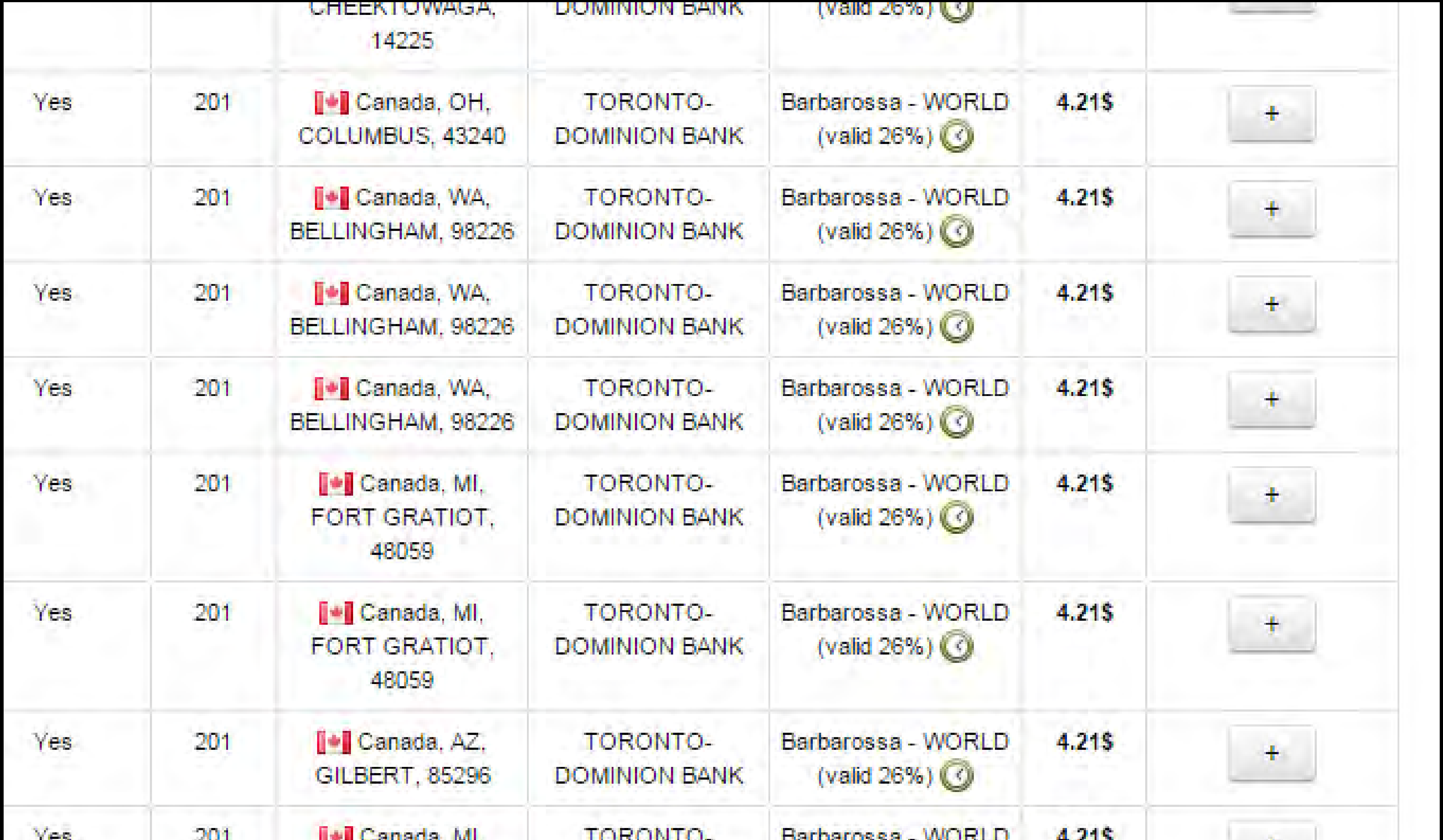
Base name: *Mark Zuckerberg*

Track 2 Only

Valid rate: 95%

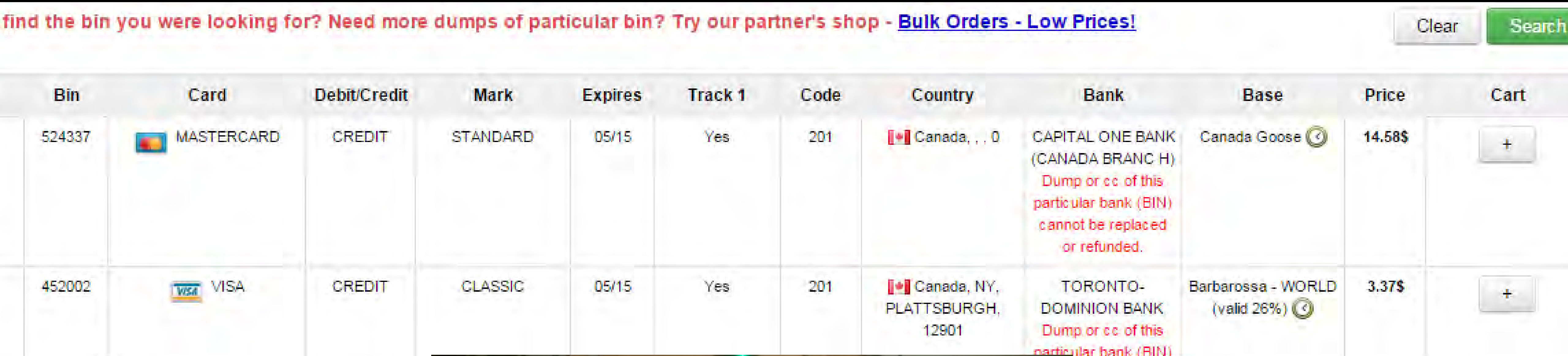
Replacement time: 30 minutes

Why do people skim data / how much does it cost



		CHEEKTOWAGA, 14225	DOMINION BANK	(valid 26%)		
Yes	201	🇨🇦 Canada, OH, COLUMBUS, 43240	TORONTO-DOMINION BANK	Barbarossa - WORLD (valid 26%)	4.21$	+
Yes	201	🇨🇦 Canada, WA, BELLINGHAM, 98226	TORONTO-DOMINION BANK	Barbarossa - WORLD (valid 26%)	4.21$	+
Yes	201	🇨🇦 Canada, WA, BELLINGHAM, 98226	TORONTO-DOMINION BANK	Barbarossa - WORLD (valid 26%)	4.21$	+
Yes	201	🇨🇦 Canada, WA, BELLINGHAM, 98226	TORONTO-DOMINION BANK	Barbarossa - WORLD (valid 26%)	4.21$	+
Yes	201	🇨🇦 Canada, MI, FORT GRATIOT, 48059	TORONTO-DOMINION BANK	Barbarossa - WORLD (valid 26%)	4.21$	+
Yes	201	🇨🇦 Canada, MI, FORT GRATIOT, 48059	TORONTO-DOMINION BANK	Barbarossa - WORLD (valid 26%)	4.21$	+
Yes	201	🇨🇦 Canada, AZ, GILBERT, 85296	TORONTO-DOMINION BANK	Barbarossa - WORLD (valid 26%)	4.21$	+
Yes	201	🇨🇦 Canada, MI,	TORONTO-	Barbarossa - WORLD	4.21$	

how its sold/used to defraud



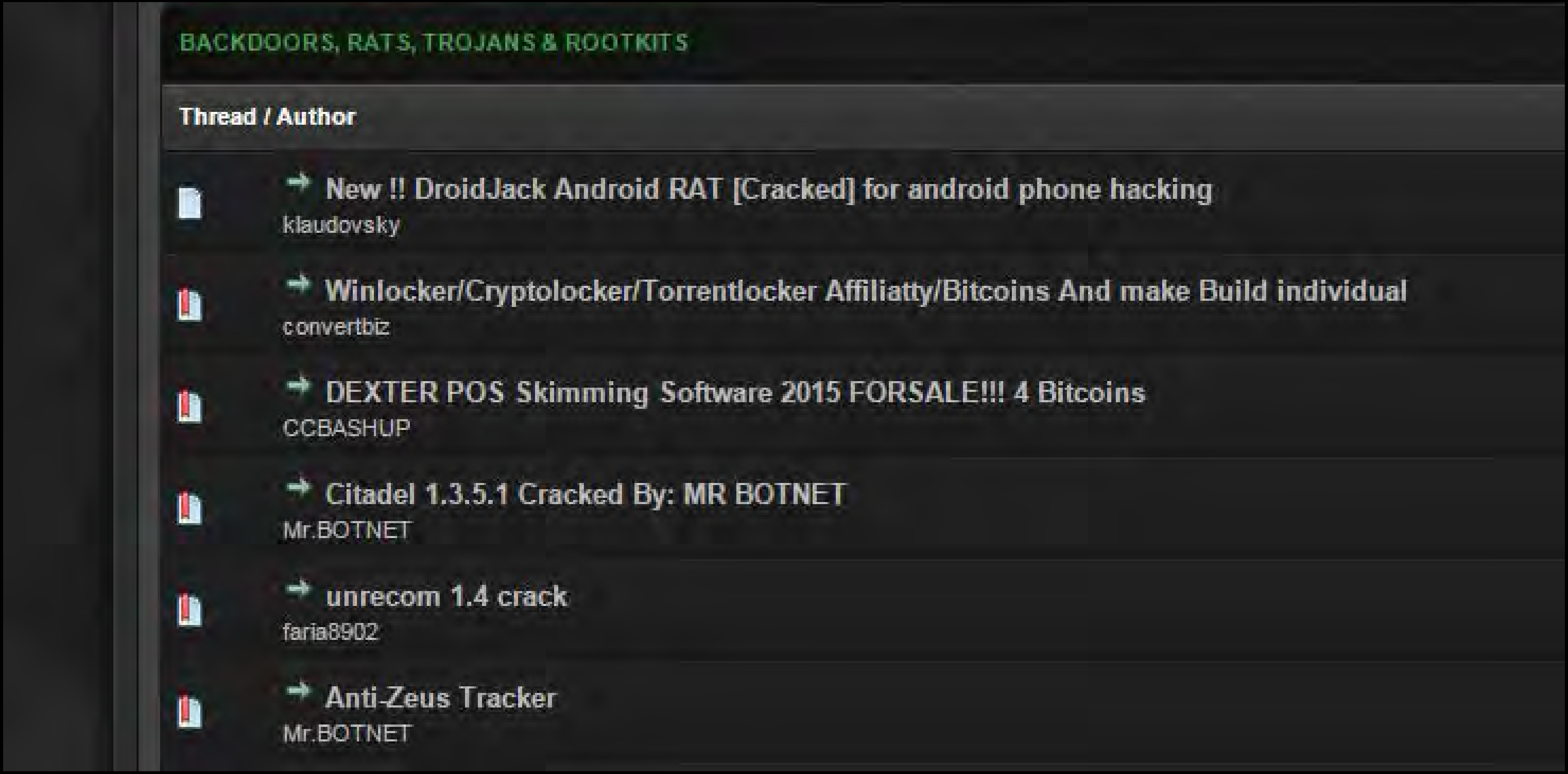
find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - Bulk Orders - Low Prices!

Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
524337	MASTERCARD	CREDIT	STANDARD	05/15	Yes	201	Canada, , , 0	CAPITAL ONE BANK (CANADA BRANC H) Dump or cc of this particular bank (BIN) cannot be replaced or refunded.	Canada Goose	14.58$	+
452002	VISA	CREDIT	CLASSIC	05/15	Yes	201	Canada, NY, PLATTSBURGH, 12901	TORONTO-DOMINION BANK Dump or cc of this articular bank (BIN) ot be replaced r refunded.	Barbarossa - WORLD (valid 26%)	3.37$	+
452005	VISA	CREDIT						ORONTO-MINION BANK	Barbarossa - WORLD (valid 26%)	4.21$	+
452005	VISA	CREDIT						ORONTO-MINION BANK	Barbarossa - WORLD (valid 26%)	4.21$	+

how its sold/used to defraud

- Carding/ Ordering things online
- Duplicating cards and using them in stores.
- ATM Cashout runs / Pin Skimmed Data.
- Theft of resources / Gas Food.
- Theft of online services or Licenced materials / Digital Movies /subscriptions to sites.
- Using Card data to transfer money WU runs.

How batches of data are ex-filtrated and sold



BACKDOORS, RATS, TROJANS & ROOTKITS

Thread / Author

New !! DroidJack Android RAT [Cracked] for android phone hacking
klaudovsky

Winlocker/Cryptolocker/Torrentlocker Affiliatty/Bitcoins And make Build individual
convertbiz

DEXTER POS Skimming Software 2015 FORSALE!!! 4 Bitcoins
CCBASHUP

Citadel 1.3.5.1 Cracked By: MR BOTNET
Mr.BOTNET

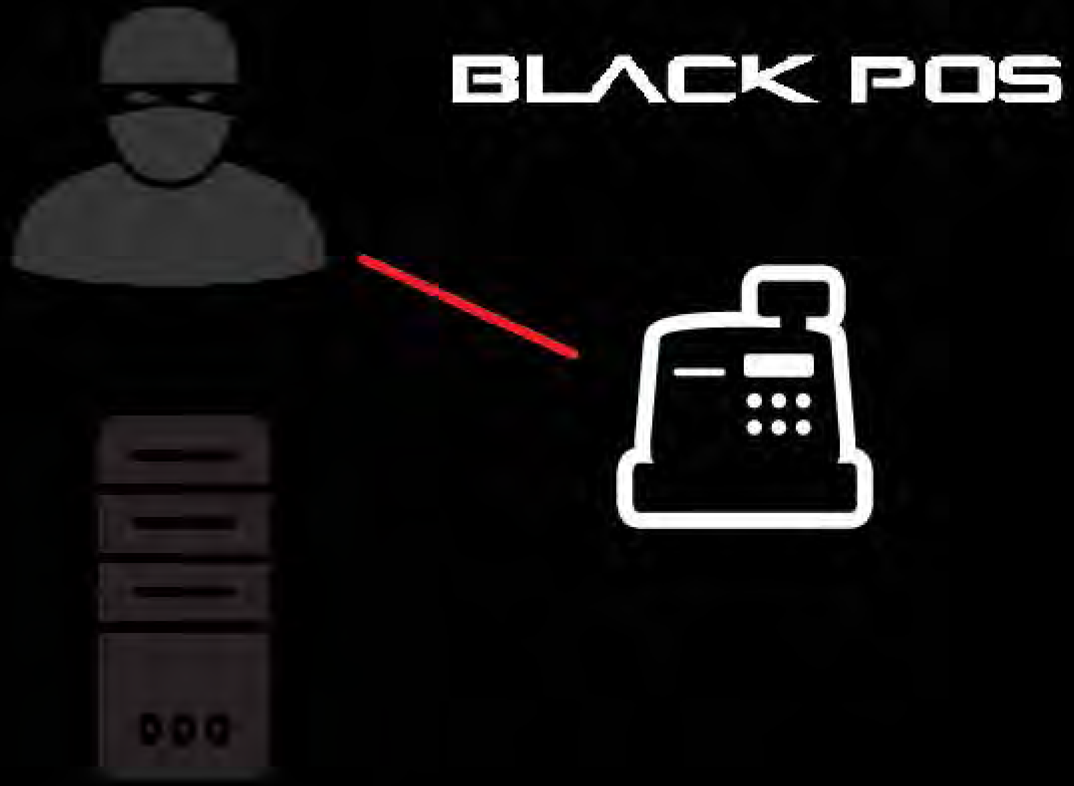
unrecom 1.4 crack
faria8902

Anti-Zeus Tracker
Mr.BOTNET

How batches of data are ex-filtrated and sold

- USB devices used to jump “Air” gapped or tighter security
- Use if spearfishing campaigns
- Software is loaded on to systems by classic hacking methods USB, HID.
- Batches are pull to servers most of the time using POST requests every time a card is found in memory the malware sends the data to a Dump
- Dumps are complied by BIN number and sold on carding pages price is determined by the banks usual Point of Sale and Debit limit.
- The validity rate is how many cards out of a 100 will work . Most batches sold on proper carding forums are 98% plus
- Two year old Target breach still has about a 10% validity Rate.

Initial POS terminal is breached and malware is loaded



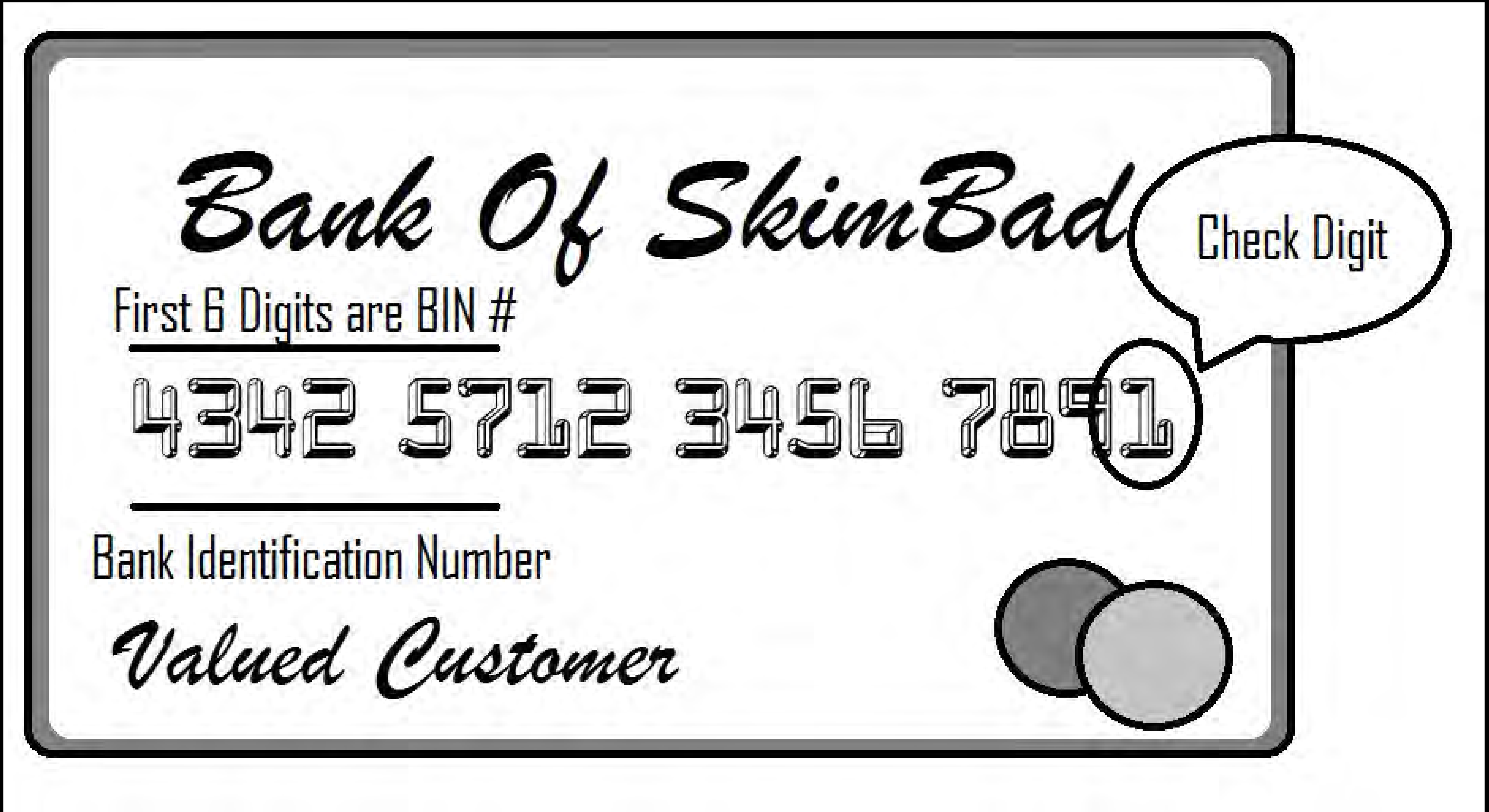
As cards are swiped they now are send to a Server where they will be sold online.

For the demonstration this all will be ran on one computer normally the POS is separate from the card catching Server.

How does malware tell credit card data from other data

Bank Of SkimBad
4342 5712 3456 7891
Valued Customer

Most Search Memory Using Custom Search Algorithms



It works against...

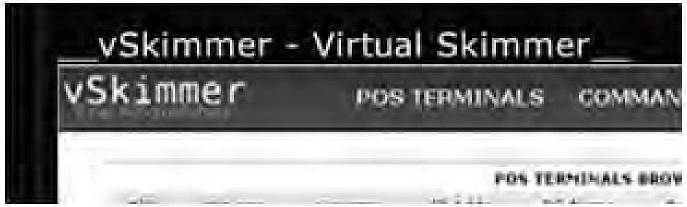
CHEWBACCA

BLACK POS

JackPos

DEXTER

BackOff



vSkimmer - Virtual Skimmer

vSkimmer

POS TERMINALS COMMAN

POS TERMINALS BROV

BrutPOS

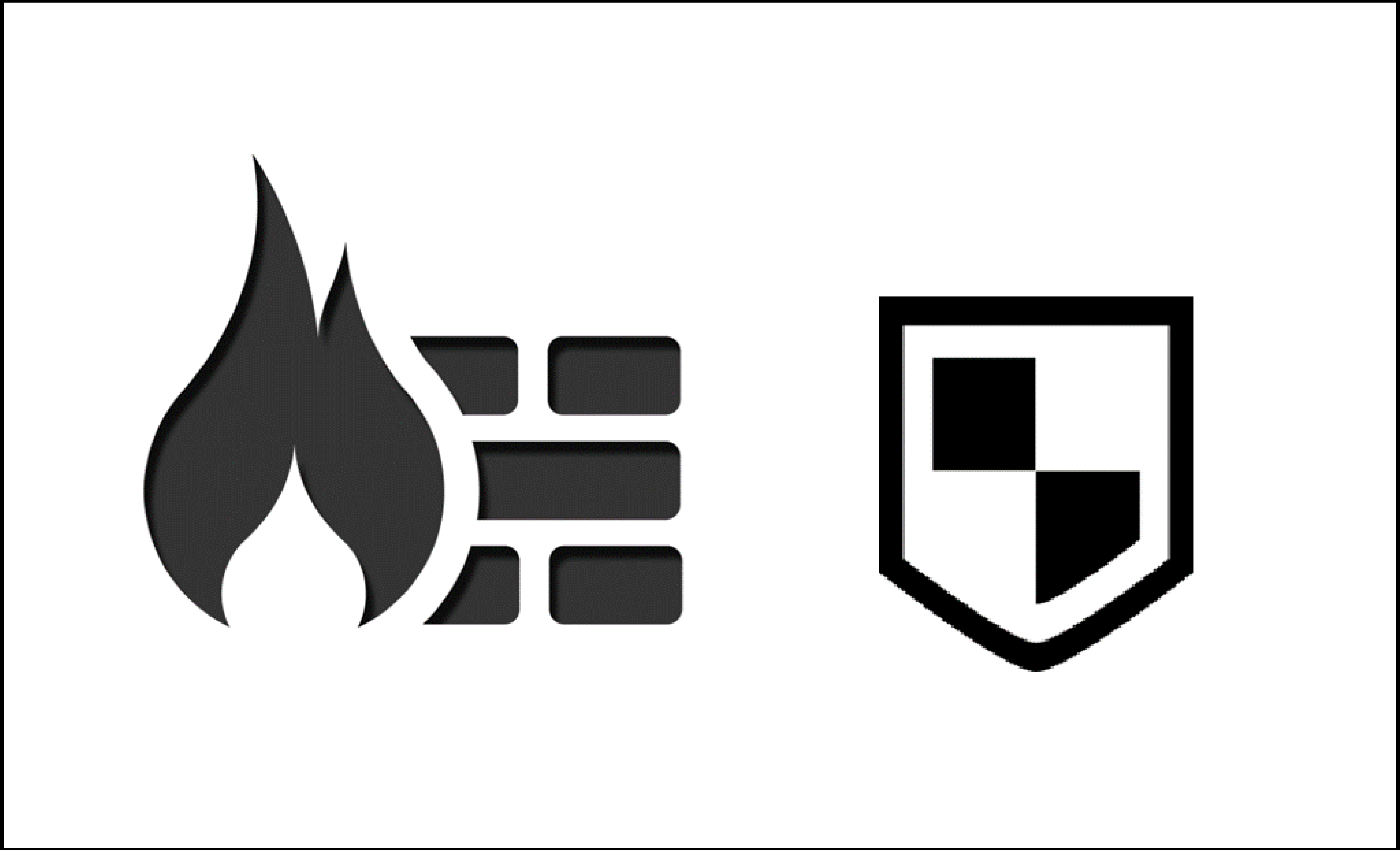
FREE

- Rdasrv
- Alina
- VSkimmer
- Dexter
- BlackPOS
- Decebal
- JackPOS
- Soraya
- ChewBacca
- BrutPOS
- Backof

Other uses EX. Malware research

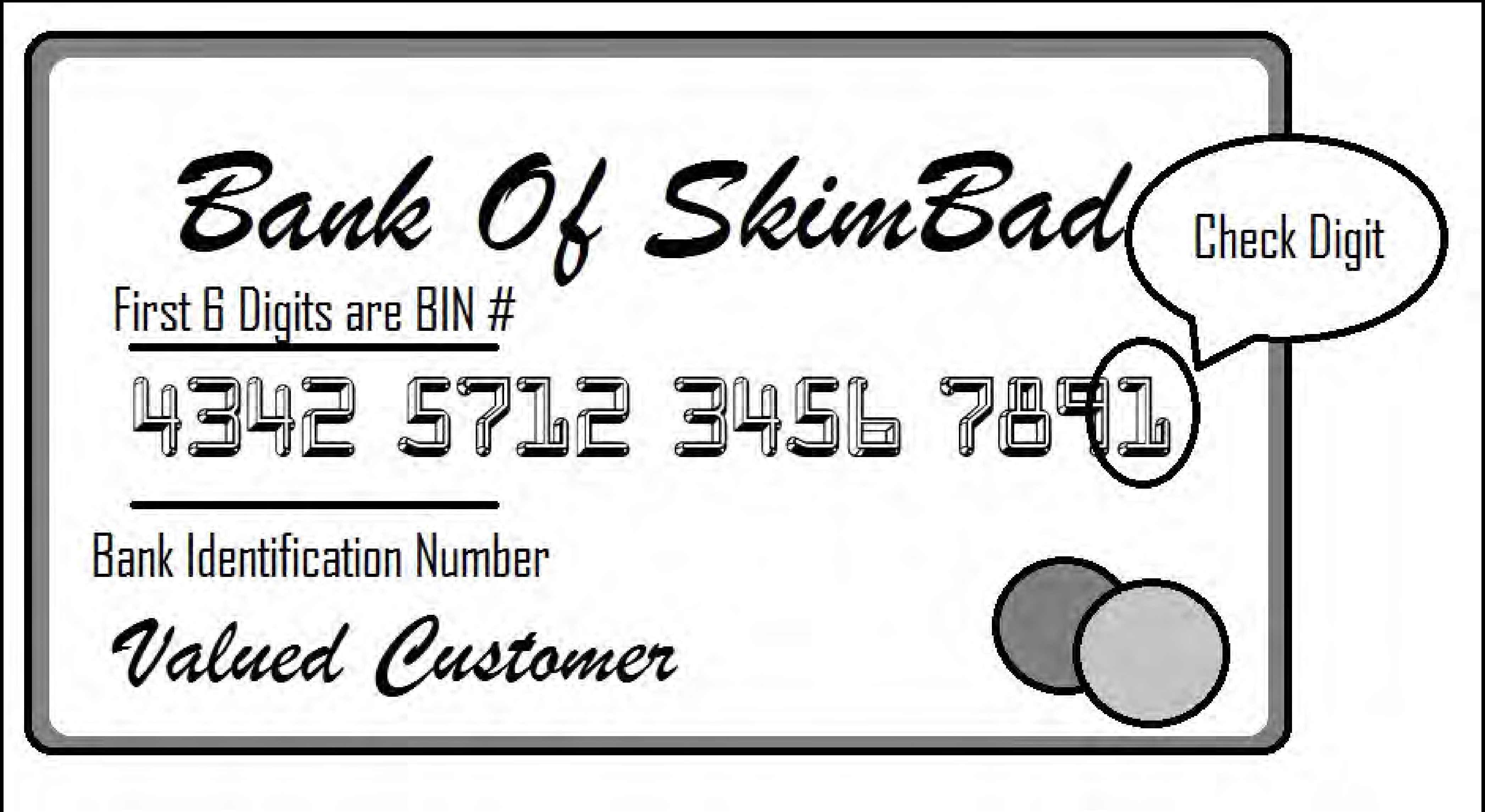
II. The approach to stopping Breaches / the tool

what currently exists to stop skimming/data exfiltration

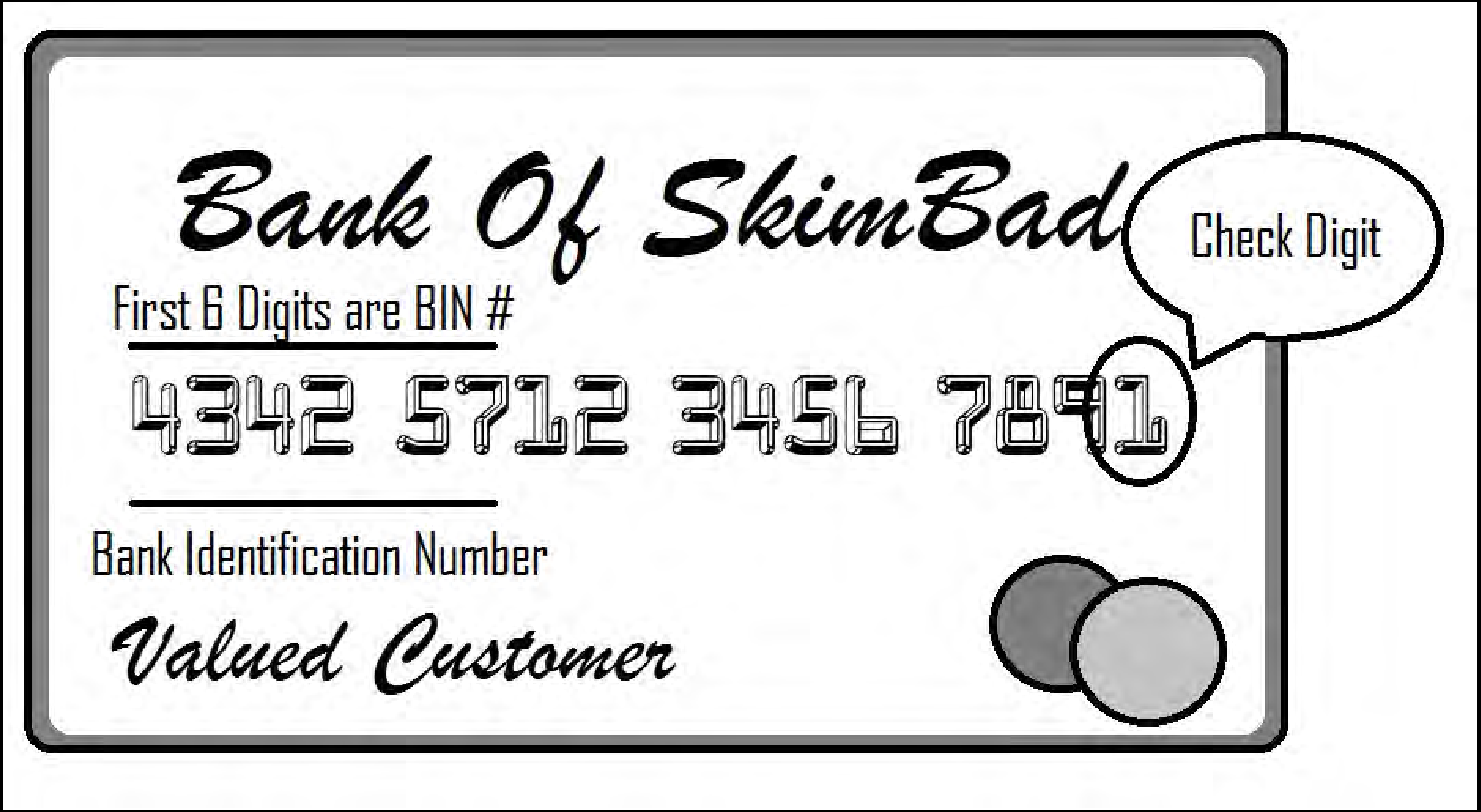


how this concept would make batches unusable

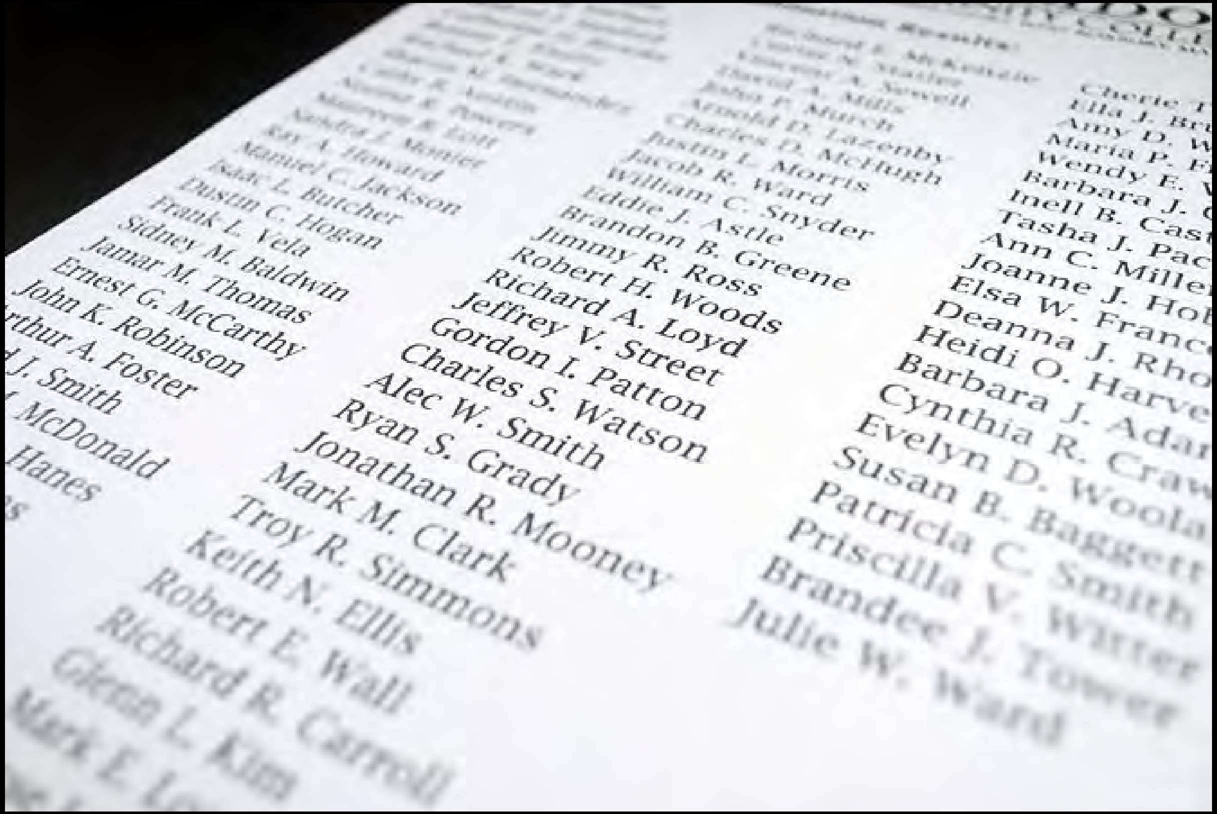
how are random credit cards made what are Bins



How random card numbers are made



How it makes random names.

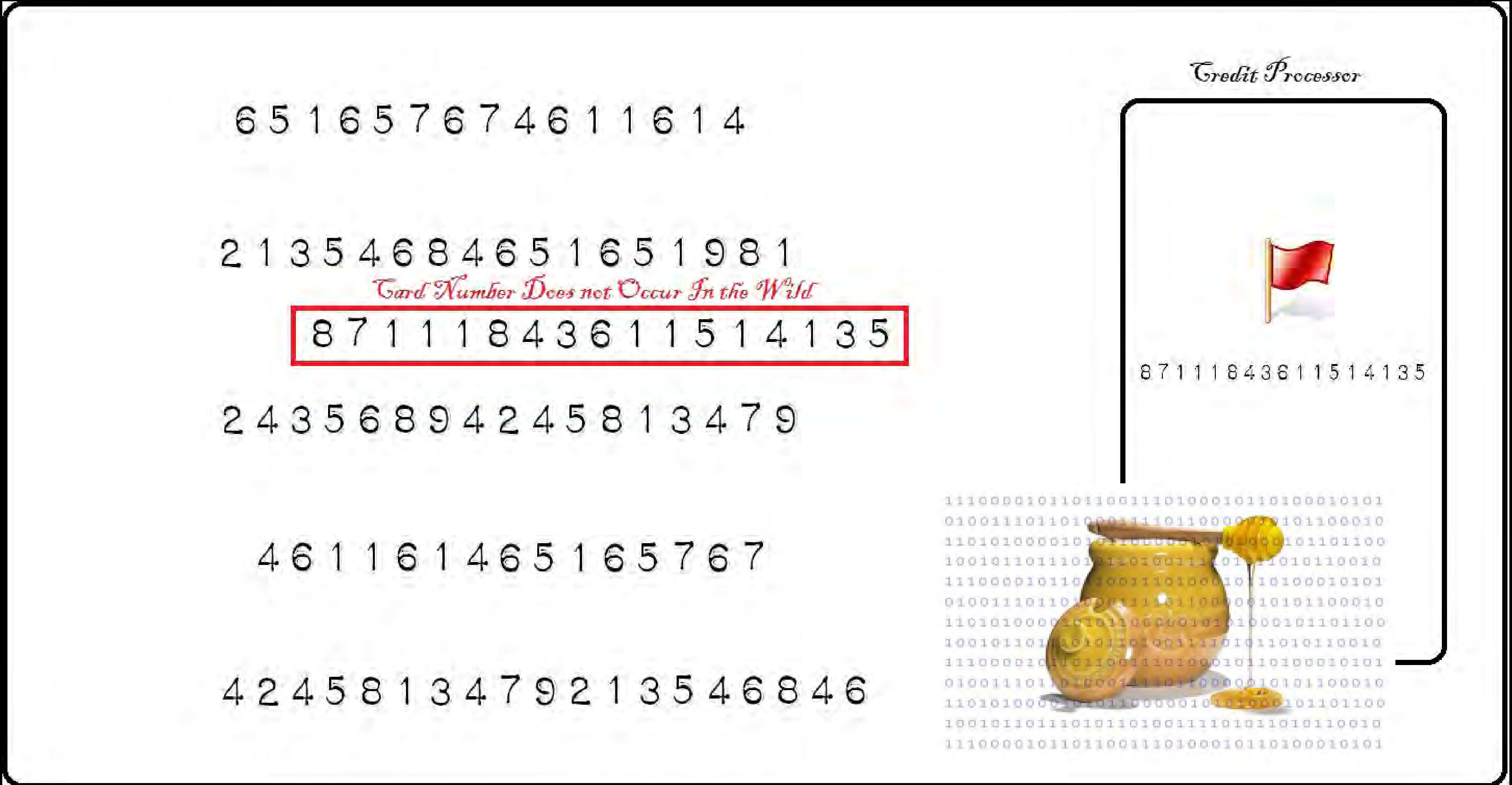


Ray A. Howard
Manuel C. Jackson
Isaac L. Butcher
Dustin C. Hogan
Frank L. Vela
Sidney M. Baldwin
Jamar M. Thomas
Ernest G. McCarthy
John K. Robinson
rthur A. Foster
d J. Smith
McDonald
Hanes
s

Results
Richard E. McKenzie
Vincent A. Newell
David A. Mills
John P. Murch
Arnold D. Lazenby
Charles D. McHugh
Justin L. Morris
Jacob R. Ward
William C. Snyder
Eddie J. Astle
Brandon B. Greene
Jimmy R. Ross
Robert H. Woods
Richard A. Loyd
Jeffrey V. Street
Gordon I. Patton
Charles S. Watson
Alec W. Smith
Ryan S. Grady
Jonathan R. Mooney
Mark M. Clark
Troy R. Simmons
Keith N. Ellis
Robert E. Wall
Richard R. Carroll
Glenn L. Kim
Mark E. L

Cherie T
Ella J. Br
Amy D. W
Maria P. F
Wendy E. V
Barbara J. C
Inell B. Cast
Tasha J. Pac
Ann C. Miller
Joanne J. Hol
Elsa W. Franc
Deanna J. Rho
Heidi O. Harve
Barbara J. Adar
Cynthia R. Craw
Evelyn D. Woola
Susan B. Baggett
Patricia C. Smith
Priscilla V. Witter
Brandee J. Tower
Julie W. Ward

Honeypot card numbers to let them know breach has occurred.



651657674611614

21354684651651981

Card Number Does not Occur In the Wild

87111843611514135

24356894245813479

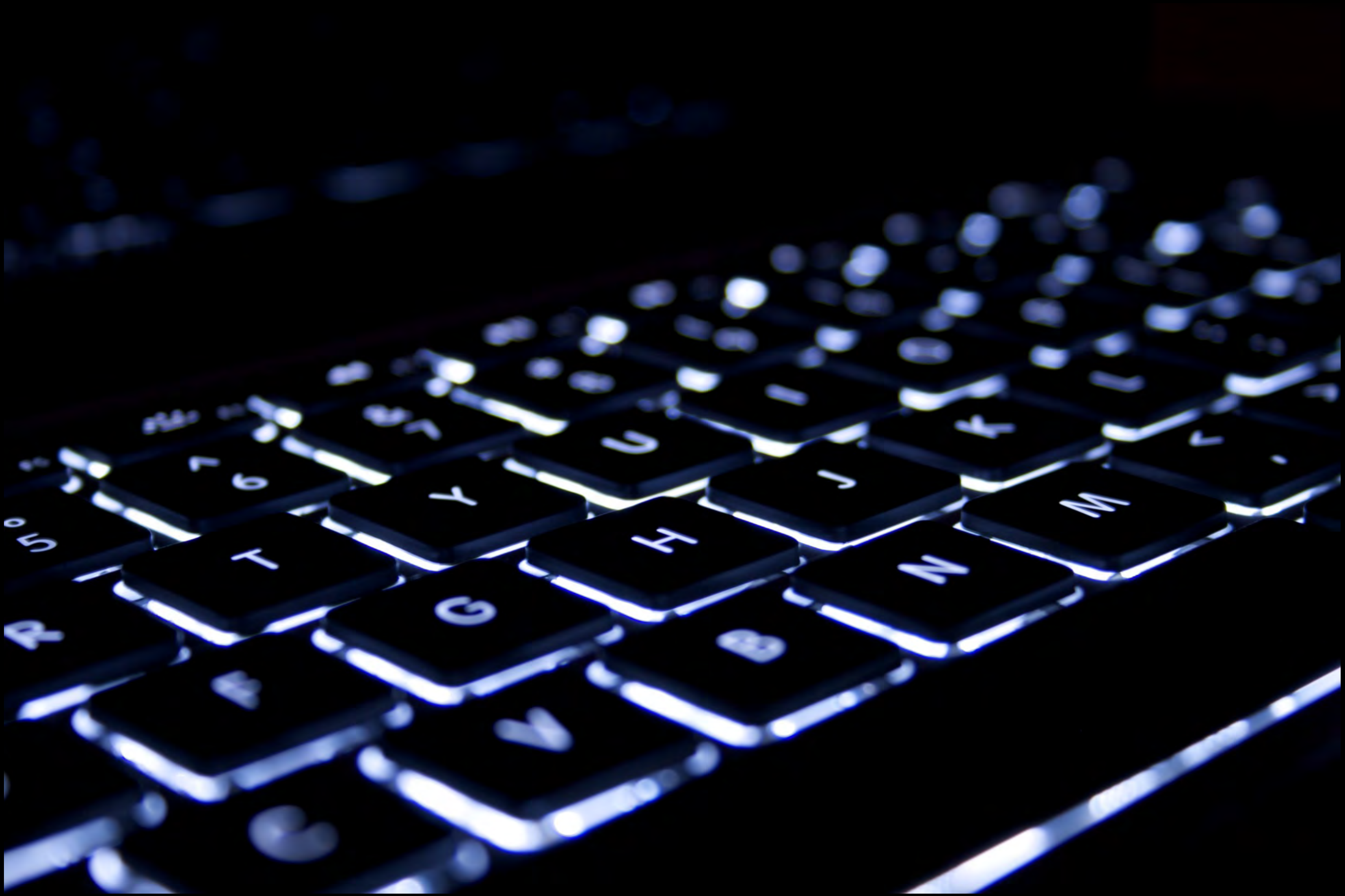
461161465165767

4245813479213546846

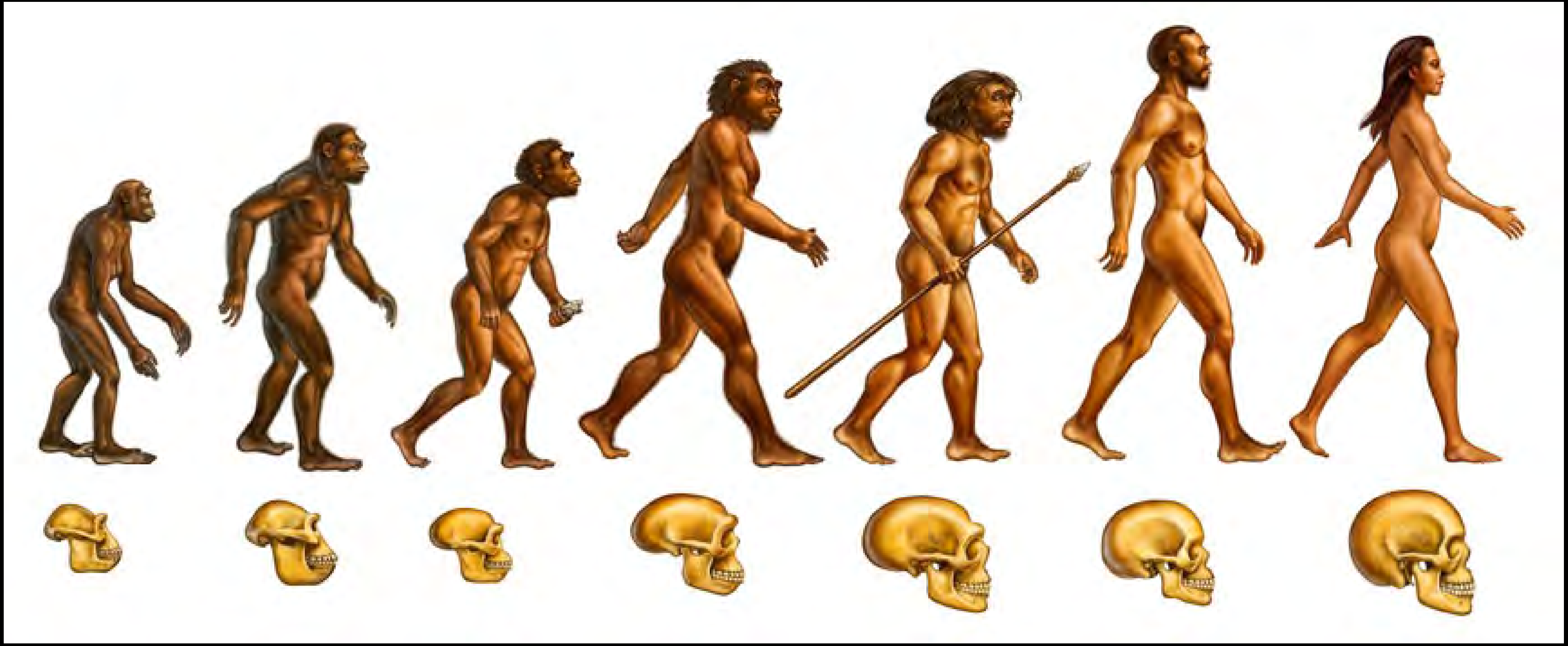
Credit Processor

87111843611514135

Anti-keystroke Catching



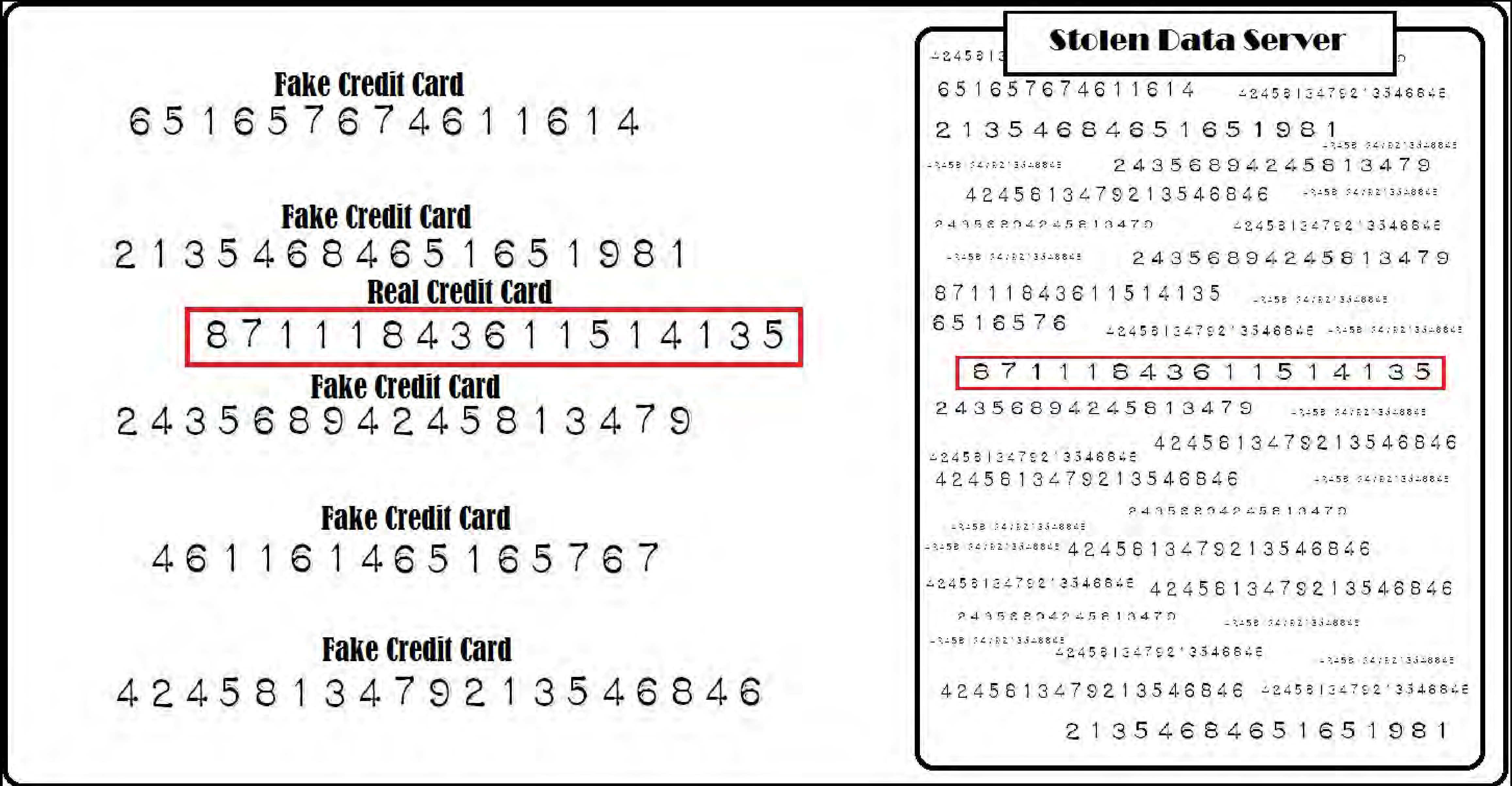
III. How will malware evolve and how we will stay on top of it



Malware gets smarter and detects BINs from area and other methods

watch dog portions (protection from malware)

How to make batches look real



Fake Credit Card

651657674611614

Fake Credit Card

21354684651651981

Real Credit Card

87111843611514135

Fake Credit Card

24356894245813479

Fake Credit Card

461161465165767

Fake Credit Card

4245813479213546846

Stolen Data Server

651657674611614

21354684651651981

24356894245813479

4245813479213546846

24356894245813479

87111843611514135

6516576

87111843611514135

24356894245813479

4245813479213546846

4245813479213546846

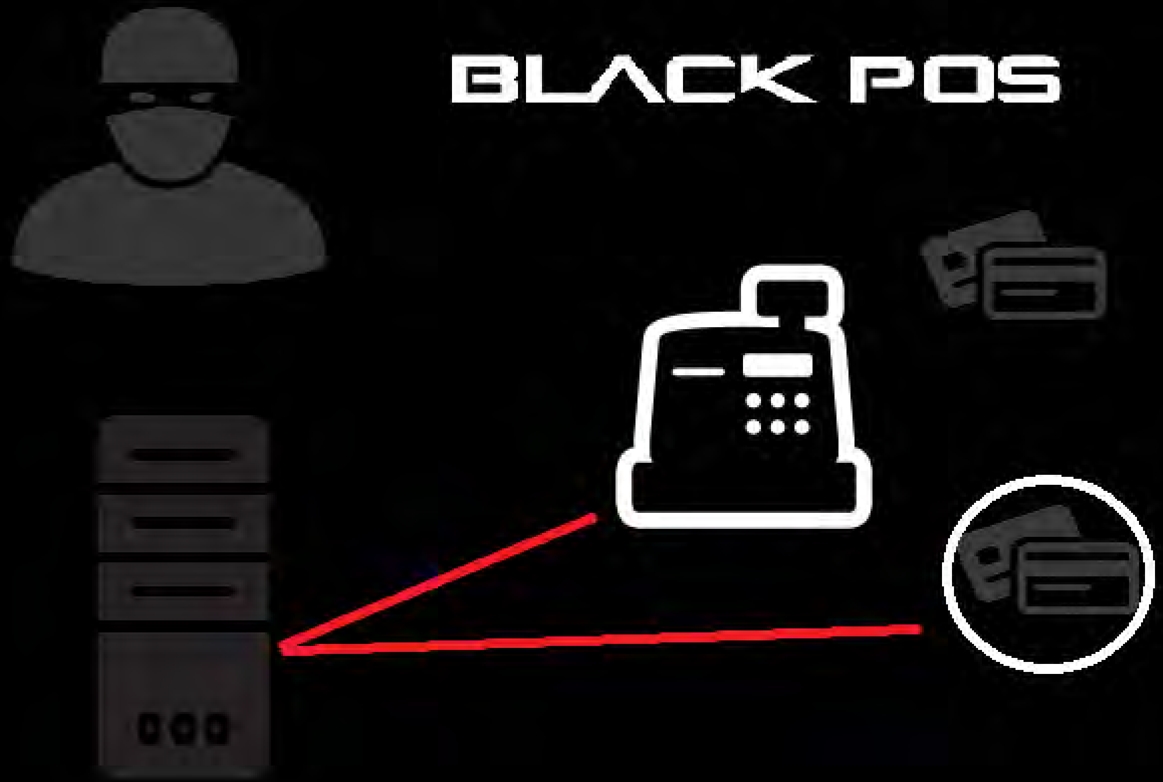
4245813479213546846

4245813479213546846

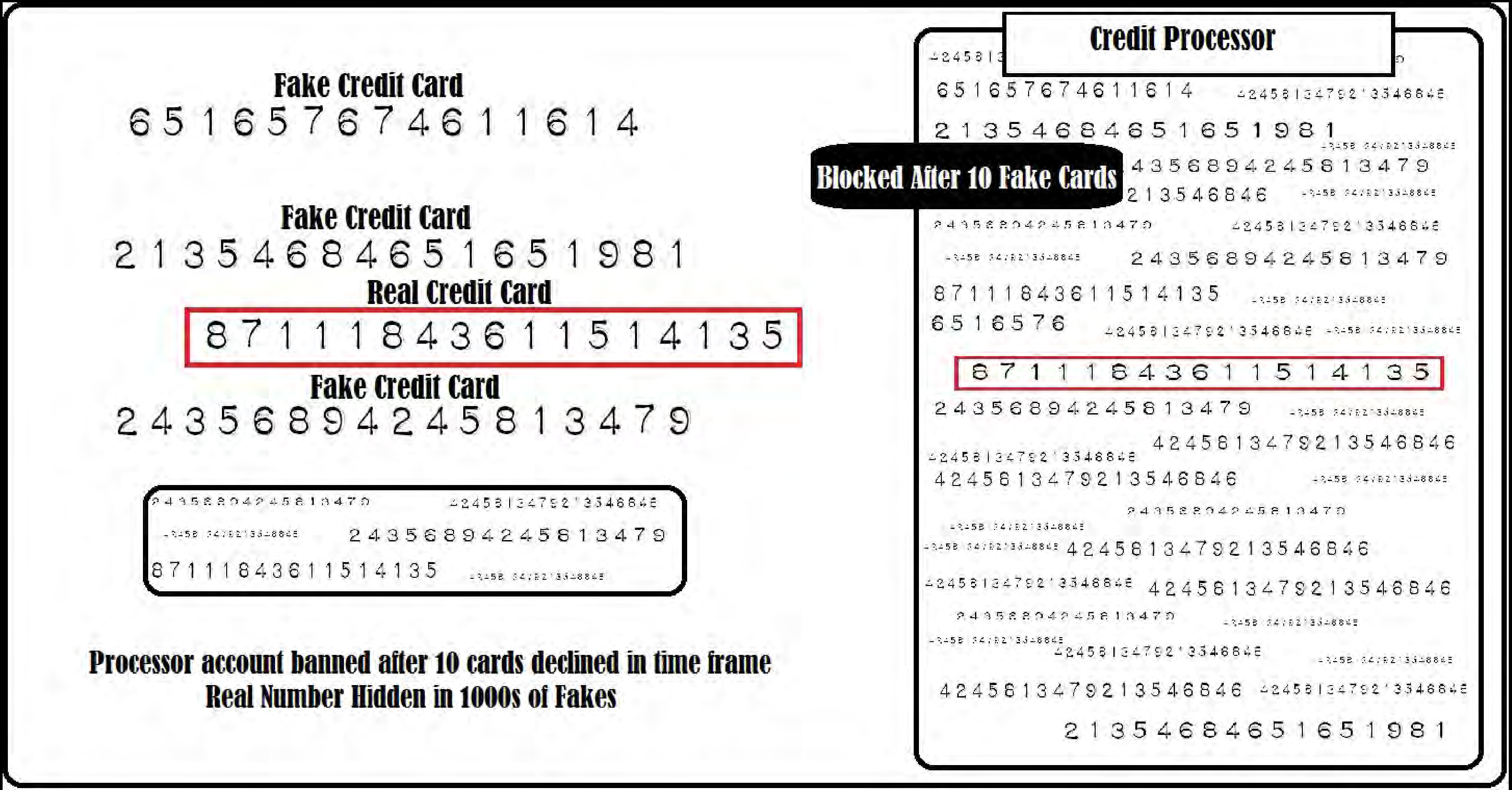
4245813479213546846

21354684651651981

The Legitimate Credit Cards are Covered with Fakes



How to make fake batches (unscrubable no reversing of process)



Fake Credit Card

6516576746116 14

Fake Credit Card

2135468465165 1981

Real Credit Card

8711184361151 4135

Fake Credit Card

2435689424581 3479

2435689424581 3479

8711184361151 4135

Processor account banned after 10 cards declined in time frame

Real Number Hidden in 1000s of Fakes

Credit Processor

6516576746116 14

2135468465165 1981

Blocked After 10 Fake Cards

435689424581 3479

213546846

2435689424581 3479

8711184361151 4135

6516576

8711184361151 4135

2435689424581 3479

424581347921 3546846

424581347921 3546846

424581347921 3546846

424581347921 3546846

424581347921 3546846

2135468465165 1981

Will Chip/Pin stop skimming ?

Software is Open Source Free
Help make it better

There is no reason that this concept should not be built into every POS system

Conclusions:

Thanks for Listening

Questions Concerns?

Special Thanks to: Tim Swartz, My Family, My Work Defcon Crew for approving my topic.

Contact Information

- ***Weston Hecker***
- **Weston@skimbad.com**
- **www.skimbad.com**
- **Twitter @westonhecker @skimbadsoftware.**