Brought to you by: SettleMINT EFT AuditLink

BRUTE FORCE BIN ATTACK CHECKLIST

WHAT IS A BRUTE FORCE BIN ATTACK?

A brute force attack is a trial and error method used by fraudsters to obtain, within seconds, payment card information such as an account number, card expiration date, PIN or Card Verification Value 2 (CVV2).

In a brute force attack, an automated software commonly known as a "botnet" is used as a downloader or credential collection tool that generates a large volume of consecutive guesses of account data.

For a complete understanding of what these attacks are, check out our whitepaper: auditlinksuite.com/wp-content/uploads/brute-force-bin-attacks-whitepaper-May2020.pdf

HOW DO BIN ATTACKS OCCUR?

Most of the time the attack comes from a single merchant whose payment system has been hacked. The attacks often occur on federal holidays when the credit union is closed, and therefore staff are not on site to monitor transaction activity.

The attacks are usually discovered when members contact the credit union complaining about unauthorized activity on their accounts.

It is imperative that your credit union react immediately to a BIN attack

BE READY BEFORE A BIN ATTACK HAPPENS

Review data at the vendor switch level

Most of a fraudster's BIN testing occurs at the vendor switch level before reaching the credit union. Reviewing data at the vendor will help identify possible attacks before they affect the credit union's core data.

We recommend running queries from your EFT vendor site (for example, for FIS/COOP, use Data Navigator) to look for the following:

- ✓ Denials for invalid card numbers that are sequenced the same number of digits apart
- ✓ Denials based upon CVV or expiration date on valid cards
- ✓ Authorizations or denials from the same vendor within seconds of each other

Be proactive with your fraud partner

- ☐ Get to know your vendor's fraud team, how you can contact them, and how to initiate a rapid response to a possible attack.
- ☐ Review your credit union's fraud system configuration at least once a year and make sure you understand the fraud recognition patterns in place.
- ☐ Contact your fraud partner multiple times during the year (at a minimum, quarterly) to review emerging fraud schemes and determine if additional fraud recognition parameters should be added to your system configuration.
- ☐ Review the blocked countries list and follow the fraud partner's recommendations on which countries should be on the list. Understand if you can issue travel letters for members traveling abroad or whether the entire membership is blocked if you block a country.
- ☐ Review offline transaction limits and in what instances they apply. If CU*Answers and your vendor are not communicating, the offline limits at your vendor will be used. But what happens if VISA/MasterCard or other networks are not communicating with your vendor? Do they have stand-in limits that would be used? If so, what are they?

IF YOU DETECT SUSPICIOUS TRANSACTIONS

If you think that you may have experienced a brute-force BIN attack, contact:

AuditLink: Jim Vilker	SettleMINT: Heather French	AFTER HOURS
•jvilker@cuanswers.com •800.327.3478 x167	•hfrench@cuanswers.com •800.327.3478 x253	•Contact Operations •800.327.3478 (opt 4)

Steps to take right away

- ☐ **Contact your vendor and its fraud team immediately**, and be prepared to contact them multiple times if needed. Ask that they develop a rule to stop the attacks immediately. Do not wait for them, as delays can be costly. Ask for a specific ETA on implementing the rule and push hard to make it happen as soon as possible.
- ☐ **Contact your Board Chairperson immediately** and explain the circumstances. These attacks can and do create large losses and your board should be involved from the very beginning.

- ☐ Don't just look for attacks involving dollars leaving member accounts. Also **look at zero-dollar authorizations**. Zero-dollar authorizations are used to uncover the numbering schema or simply to validate the card which could then be sold on the black market.

- ☐ **Provide examples to the team at CU*Answers** so that that we can review the data that has reached the core and determine if patterns suggest an attack is underway. Remember that most of the time these attacks do not hit the core, which is why it is important to query the data at the vendor switch level.

Data you can review in CU*BASE

Starting in 2021, a new table called **ISOCUDTA** has been added to your credit union's FILExx library and can be used with the CU*BASE Report Builder. It is compiled at the end of each day (so the most recent data is as of yesterday), and contains a rolling 30 days of EFT transaction data, including merchant name, Merchant Category Code (MCC), and more.

- ☐ **Query the ISOCUDTA table** to find any transactions that may have passed your fraud detection parameters and made it to member accounts.

NEED DATA HELP?

Contact the Asterisk Intelligence team and ask about our canned Queries over the ISOCUDTA table:

- ✓ Transactions per MCC
- ✓ Denied transactions
- ✓ Card-not-present activity
- ✓ …and more!

Actions you can take in CU*BASE

- ☐ **Freeze** the affected accounts, either manually or programmatically.

- ☐ Initiate a **mass card reissue**.

- ☐ **Consider requesting a new BIN**. This is not a requirement, and there are expenses associated with this process. A new BIN request can take 3 weeks, and if your vendor requires certification that adds even more time. Then you will need to do a mass reissue of cards from the old BIN to the new BIN.

- ☐ **Request a BIN extension** (changes the 8th-10th positions). The vendor will evaluate potential issues with CU*Answers building an extension. If your vendor needs to create the extension too, then certification may be required. Once these options are determined, we would then look to do a mass reissue.

- ☐ **Work directly with your vendor's fraud team**. If a specific merchant was identified, queries can be run over your history files (TRANS1, TRANS2, HTRANS1, HTRANS2) to determine if transactions were posted to member accounts. If transactions did post, your credit union can review the best course of action with the fraud team.

- ☐ **Watch your settlement accounts**. If the settlement amounts are larger than previous days or even the previous week, that could be another reason to raise an alarm. Remember that holidays, spring breaks, etc., can also cause settlement amounts to be larger than normal.

CU*ANSWERS
A Credit Union Service Organization

cuanswers.com