October 21, 2020

BULLETIN: THE THREAT OF ACCOUNT TESTING TO PAYMENT SECURITY

The PCI Security Standards Council (PCI SSC) and the National Cyber-Forensics and Training Alliance (NCFTA) want to highlight an ongoing threat that requires urgent attention.

What is the threat?

Account testing attacks – also referred to as payment account enumeration, card testing, and BIN attacks involve a cybercriminal testing payment account numbers in order to validate cardholder information to perpetrate fraud. The two main testing techniques involve testing a full card number or brute forcing an incomplete card dataset. Once an account number is validated, it can then be monetized by being sold on the Dark Web or immediately utilized to commit fraudulent transactions.

How do these attacks work?

There are different methods that criminals can use to undertake account testing, and each has a different impact on merchants and other entities in the payment lifecycle. The cardholder data in these types of attacks are obtained through two primary techniques – a Point of Interaction (POI) malware or system intrusion data breach within the cardholder data environment or by account number enumeration for fraudulent purposes. An overwhelming majority of attacks today utilize automated software to simply enable account testing to be undertaken on a massive scale in a very short timeframe.

The assumption for all of these attacks is that the criminal has obtained a very large number of Primary Account Numbers, along with Expiry dates and the Card Verification Code or Value. Where these types of Sensitive Authentication Data (SAD) are not known, then certain account tests can be undertaken to identify and validate this data.

Card testing tools, also known as credit card number checkers, are often referred by the abbreviations CC checker, CVV checker, or CCN checker. These tools are usually hosted on Clearnet websites (publicly accessible, non-darknet websites) and allow attackers to enter bulk amounts of card numbers, typically with expiration dates and CVV codes, and identify which card numbers are valid. Some of these tools require registration and a fee for use while others do not require registration and are free to use. Additionally, attackers can pay for and gain access to “commercial” card testing tools on underground and dark web markets and forums.

In instances where attackers do not have complete card numbers, they can conduct a BIN attack. A BIN attack involves attackers taking identified BIN numbers and using card number generation tools to generate the remaining card numbers to form a complete card number that needs to be validated. Card number generation tools are also often hosted on Clearnet websites and may be free to use without registration. These tools may be referred to as “credit card

generators." It should be noted these tools typically only generate a potentially legitimate card number and do not validate the card number is active.

Merchant ID Takeover

In this attack the criminals obtain the Merchant ID and credentials. These credentials are obtained due to poor installation or management of the payment process, or other means that lead to access of the merchants' systems. Most often for either scenario, poor network security coupled with poor password selection or not changing default passwords enables the criminals to gain access and control. In some instances, fraudsters have introduced fake terminals where weak security practices and predictable terminal ID's allow for their insertion onto the network.

The criminals will then effectively pose as the merchant requesting authorization for significant volumes of low value credit card purchases. Where expiry date and Card Verification Value or Code numbers are known, this is a fast and simple process. Authorized card details are then added to a "Validated List" of cards for the criminals to sell. Where those numbers are not known, it is a relatively easy task to run through the limited number of options until a valid number is reached.

Carding or Card Stuffing

Carding or Card stuffing is an attempt to steal and validate credit cards through automated web injections. If only the Primary Account Number, (PAN) is known, automated software (e.g. bots) can be used to attempt multiple online transactions for low value purchases through multiple merchants, inserting the PAN and options for the expiry date, postal code, and Card Verification Code or Value of the card. When a card is accepted, the attacker knows the correct value has been entered.

By undertaking attempts in parallel the cybercriminal can defeat transaction attempt frequency limits. Given cards are generally valid for three to five years, the valid expiry date can be generated in effectively 60 attempts, assuming a maximum of 5 attempts per site across 12 sites in parallel.

There are still many websites that do not require the Card Verification Code or Value or do not validate that the code has been correctly entered. Where a three-digit Card Verification Code or Value is required on a website, 1,000 attempts would be required to generate the correct value. Assuming 5 attempts per site, this requires 200 sites to be targeted in parallel to generate a valid number.

Again, successful data is then combined into a list of validated card data to be monetized. Card stuffing is dangerous to both consumers and enterprises because of the ripple effects of these breaches.

Card validation services have been recognized as an important part of the carding market. The underlying process behind checkers varies from service to service. Because charity sites often receive large batches of small donations and have simple payment processes, fraud is often hard to detect and easy to automate. Small payments made to charity websites often range from $1.00 to $5.00. Threat actors actively target small merchant sites that are vulnerable and could be used to check large batches of compromised cards

Blind brute force attack

A Brute Force attack is when a criminal systematically works to initiate transactions to obtain valid credentials like a card verification code or value and/or expiration date by testing a large volume of potential combinations.

In this attack, the criminal does not know any details of the cardholder data but uses a software program to test card numbers by repeating the transaction sequential card numbers until a valid number is achieved. Even if 98% or more of submitted numbers are rejected this still has several major impacts on all of those involved.

For example, a criminal undertaking 10,000 attempted transactions per hour with only a 2% success rate, generates 200 valid card details per hour and 4,800 per day, particularly if using automated tools to do so.

Who is most at risk?

Account testing attacks pose risks to issuers, acquirers and merchants, and the threat exists across many acceptance channels. The consumer also could become the victim of financial/identity theft as a result of a successful attack. Everyone involved in the payment chain is potentially a source of exposure and it is the responsibility of all involved to be vigilant and, on the look-out for this type of attack. Good payment security practices need to be a priority for the merchant, the payment processors as well as issuers and the acquirers. Defeating this ever-growing attack requires a team effort from all involved parties.

Impact to the Merchant

Account testing can have a wide range of impacts on a merchant depending on how the attack is undertaken. If a merchant is charged per transaction whether it is successful or not, then being subjected to an account testing attack can cost the merchant thousands of dollars in processing charges. A high rate of rejected transactions can also affect the merchants rating with Brands, Issuers and Acquirers being less inclined to accept legitimate transactions. The merchant also will receive significant numbers of charge backs from the legitimate cardholders, again having a financial and reputational impact upon the merchant.

Impact on the Issuer

Issuers will see the massive number of low value transactions coming through their systems along with the high reject rate. This will make it difficult for the Issuer to determine legitimate transactions from attempted fraudulent transactions. Issuers might also be forced to absorb the eventual costs when legitimate cards are stolen and used to commit fraud. Issuers are also subjected to fees associated with these transactions which can have a large financial impact especially for small issuing banks.

Impact on Acquirers

For Acquirers, the volume and scale of Account testing attacks can lead to service level impacts to the Acquirers network. It can also lead to an increase in fee disputes and transaction reversals. Time consuming service calls and a decrease in merchant confidence and

satisfaction in an Acquirers ability to provide safe and secure payment processing can also have a detrimental impact on an Acquirers reputation. This could lead to merchant attrition in the long run.

What are some DETECTION red flags?

The ability to detect these threats before they can cause damage is critically important. Security needs to be a 24/7 priority with security monitoring that looks for and identifies unusual behavior and irregular patterns.

The following characteristics are some common indications of authorization/account testing:

- Account numbers being used do not exist, e.g., a card number from an un-issued BIN range.
- Account numbers being used repeatedly with variations in the security features (expiration date, CVV2/CID, cardholder's postal code).
- Increase in account numbers attempted within a BIN range, particularly when used at the same merchant for small amounts. Testing may occur with sequential account numbers, or certain digits within the account number may be incremented in regular intervals.
- Increase in AVS checks (e.g. Condition Code)
- An increase in the percent of declines for a merchant or BIN range. Authorization testing will generate higher numbers of declines as fraudsters attempt to find the correct combination of account number, expiration date and security codes (e.g. CVV2/CID).
- An increase in the percent of approved authorizations that do not settle for a merchant.
- An increase in transaction velocity / volume at a new merchant or merchant with low settlement rates.
- A rapid increase in transaction velocity / volume at a merchant that has been inactive.
- An increase in the number of different names being submitted on transactions for a merchant when historically that merchant has submitted only a few legitimate names

What are some PREVENTION best practices?

The best protection to mitigate against account testing attacks is to adopt a layered defense that includes secure authentication protocols, patching operating systems and software with the latest security updates, vigilant intrusion detection practices and the proper installation of payment systems. Also, being PCI DSS compliant provides a strong security foundation that can help to address this threat by creating a culture that prioritizes outstanding security standards and practices. Some recommendations and guidance to thwart account testing attacks for Issuers, Acquirers and Merchants include:

Issuers:

- Avoid issuing PANs sequentially
- Use random expiration dates within BIN ranges
- Block unused BIN ranges
- Monitor BINs for anomalies

- Validate security codes (e.g. CVV2/CID) on all transactions where it is present and consider declining all invalid CVV2/CID
- Calibrate rules to detect and decline transactions during these attacks

Acquirers:

- Work with merchants to secure websites (i.e. captcha, 3DSecure, etc.)
- Consider botnet detection at the acquirer level
- Work with your gateway to ensure crucial data elements are monitored and shared with acquirer (such as IP address)
- Implement velocity checks (spikes in transaction attempts, approvals, declines, speed of transactions from a specific BIN range)
- Consider utilizing a negative file for known bad IP addresses
- Validate POS devices connected to host systems so that no unauthorized or cloned POS devices can connect to a live merchant ID.
- Create reporting based on "Invalid Account Number" fraud detection attempts at the issuer BIN level or account number or merchant doing business as (DBA) name level
- Conduct due diligence – verify information associated with prospective merchants
- Randomize terminal IDs – sequential terminal IDs are easier for criminals to exploit
- Protect merchant credentials by issuing strong user IDs and passwords for payment gateway portals

Merchants:

- Maintain strict inventory of POS terminals
- Work with your acquirer to secure your website and prevent automated attacks (i.e. captcha, 3DSecure, etc.)
- Discuss botnet detection with acquirer
- Consider injecting random pauses when checking cards to slow down a brute-force attack
- Discuss implementing a negative file for known bad IP addresses with your acquirer
- Review logins with suspicious commonly used passwords
- Lock out an account after a select number of incorrect username/password guesses
- Look for logins for a single card account coming from many IP addresses

###

About the PCI Security Standards Council

The PCI Security Standards Council (PCI SSC) leads a global, cross-industry effort to increase payment security by providing industry-driven, flexible and effective data security standards and programs that help businesses detect, mitigate and prevent cyberattacks and breaches. Connect with the PCI SSC on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.

About NCFTA

The National Cyber-Forensics and Training Alliance is a nonprofit corporation founded in 2002, focused on identifying, mitigating, and disrupting cybercrime threats globally. The NCFTA was created by industry, academia, and law enforcement for the sole purpose of establishing a neutral, trusted environment that enables two-way information sharing with the ultimate goal to identify, mitigate, disrupt, and neutralize cyber threats. https://www.ncfta.net/