Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

ATM/ITM Transaction Reversal Fraud – New Variant

SUMMARY

We have recently become aware of a new variant of Transaction Reversal Fraud (TRF) incidents occurring in several Eastern European countries against RM3- and RM4-based terminals. In these cases, the fraudster physically damaged the ATM's shutter, then initiated a transaction during which they jammed the card reader to cause the transaction to abort. This created an error condition that led to an automatic reversal of the transaction, despite the fraudster having physical access to the cash.

The attacks caused visible damage to the ATM hardware, requiring a repair service visit. While the TRF attack method itself is not new, it can impact all ATM vendors and models.

KEY ATTACK METHOD

Transaction Reversal Fraud occurs when an attacker convinces the card issuer to reverse a transaction while still obtaining the cash. This attack targets the funds of the financial institution and not a legitimate cardholder, as the transaction is performed by the fraudster.

- The fraudster requires an active payment card and associated PIN (for an account with sufficient funds) to perform a cash withdrawal at an ATM. Often, attackers use foreign credit card accounts specifically created for fraudulent use.
- The attacker creates a hardware error on the terminal, usually by physically manipulating the card reader or cash dispenser during the transaction process.
- Regardless of the error, the fraudster ensures they retrieve all or part of the cash.

The error generated by this manipulation is sent by the ATM to the host network's transaction processor as a status message, allowing the attacker to obtain cash without being debited due to the transaction reversal.

MITIGATING THE RISK

Be proactive by contacting your vendor to identify and deploy available solutions if not already implemented. ITMs and ATMs are being attacked in many ways, so it is critical to maintain ongoing discussions with vendors to ensure all mitigation solutions are in place. Additionally, conduct regular inspections of terminals for signs of physical manipulation.

Check Terminal Software Stack and Hardware Configuration

- Ensure terminal settings limit the impact of TRF attacks. If a TRF attack is detected, the device should transition into an inoperative state, requiring an on-site visit with safe access to restore normal operation.
- ITMs/ATMs should have a sensor-based Anti-Cash Trapping Solution that includes drilling detection for the shutter.

Check Transaction Reversal Settings and Implement Transaction Monitoring at the Host

Implement additional authentication layers (beyond PIN alone) to use the ITM for transactions with higher risk, such as the following functions:

- Deposits
- Withdrawals over $500
- Check cashing
- Transfers
- Payments
- Non-member check cashing

Additional authentication options include:

- Monitor for repeated or unusually high numbers of transaction reversals on the same card or cards with the same Bank Identification Number (BIN). Combine this with factors such as geography, amount, or time of day. When these patterns are detected, block the transactions to prevent potential fraud.
- Monitor security-related hardware and software events in real time, including suspicious activity such as repeated card reader jams.
- Configure the host to debit cash directly with the dispense command, independent of follow-up commands. This should only be used in environments with highly reliable hardware, as failures during the dispense operation could lead to legitimate customer complaints. Alternatively, delay sending the final host message of the transaction until all cash device commands are executed and error/platform statuses have been evaluated for fraud indicators.
- Consider implementing a “cash-before-card” transaction flow to reduce the likelihood that a fraudster can trigger a relevant error using the card reader.
- Ensure network hosts evaluate all available information in status messages. Detailed status data can help determine whether to post or reverse a transaction. Verify that protocol sequences comply with specifications and are correctly handled by the host.
- Configure the host so that if an error related to a hardware issue is reported, the account is still debited and only reversed after the ITM/ATM has been reconciled.

RISK MITIGATION RESOURCES

- Read more
  - ATM Protection (White Paper PDF)
  - ATM Jackpotting Attacks on the Rise (Risk Alert PDF)
- News: New Trends in ATM Fraud
- Sign up for our **Let's Talk Fraud** quarterly webinars
- View additional risk resources

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net

LinkedIn