

NCR ATM Security Alert

DATE: March 3, 2021

INCIDENT NO: 2021-02

REV: #1

Ploutus variation found in ATMs in Latin America

New guidance and recommendations from NCR

Metabase Q, a third-party IT company, has issued a [report](#) claiming that Itaotec ATMs may be affected by a variant of the Ploutus Malware. This malware can cause a full cash-out (“jackpot”) of the ATM.

This attack type is similar to malware attacks in the past. This report indicated a new version of the malware has been targeted to a specific manufacturer. All ATMs need to be protected from logical and physical attacks. NCR again advises that you ensure you have protected your ATMs from all forms of logical attacks by deploying the measures you can [find in this NCR whitepaper](#).

Contacts

- NCR ATM crime reporting: Global.Security@ncr.com
- NCR self-service security solutions and best practice: NCRSelf-Service.security@ncr.com

Best regards,

NCR Banking Team

NCR Corporation 864 Spring St. NW, Atlanta, GA 30308-1007

©2021 NCR Corporation. All rights reserved. ncr.com

NCR respects [your privacy](#).

