Hackers say they stole millions of credit cards from Banco BCR

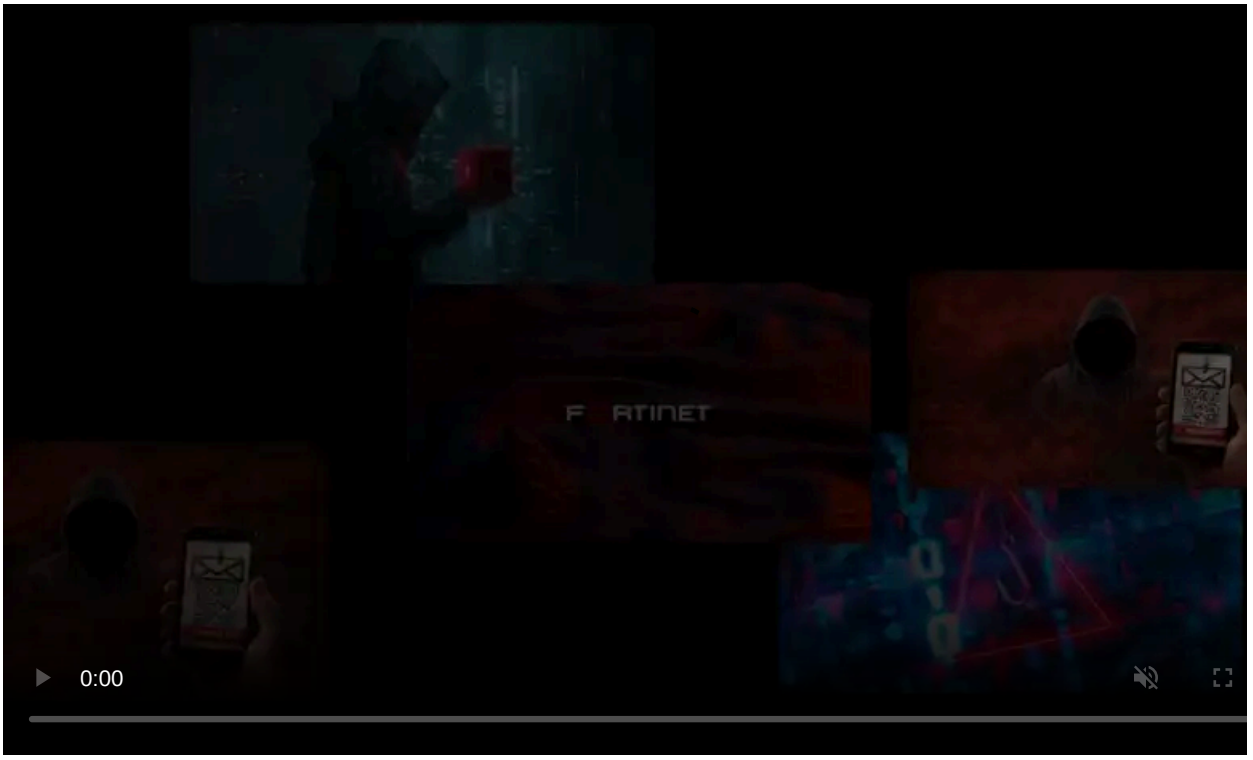
By Lawrence Abrams

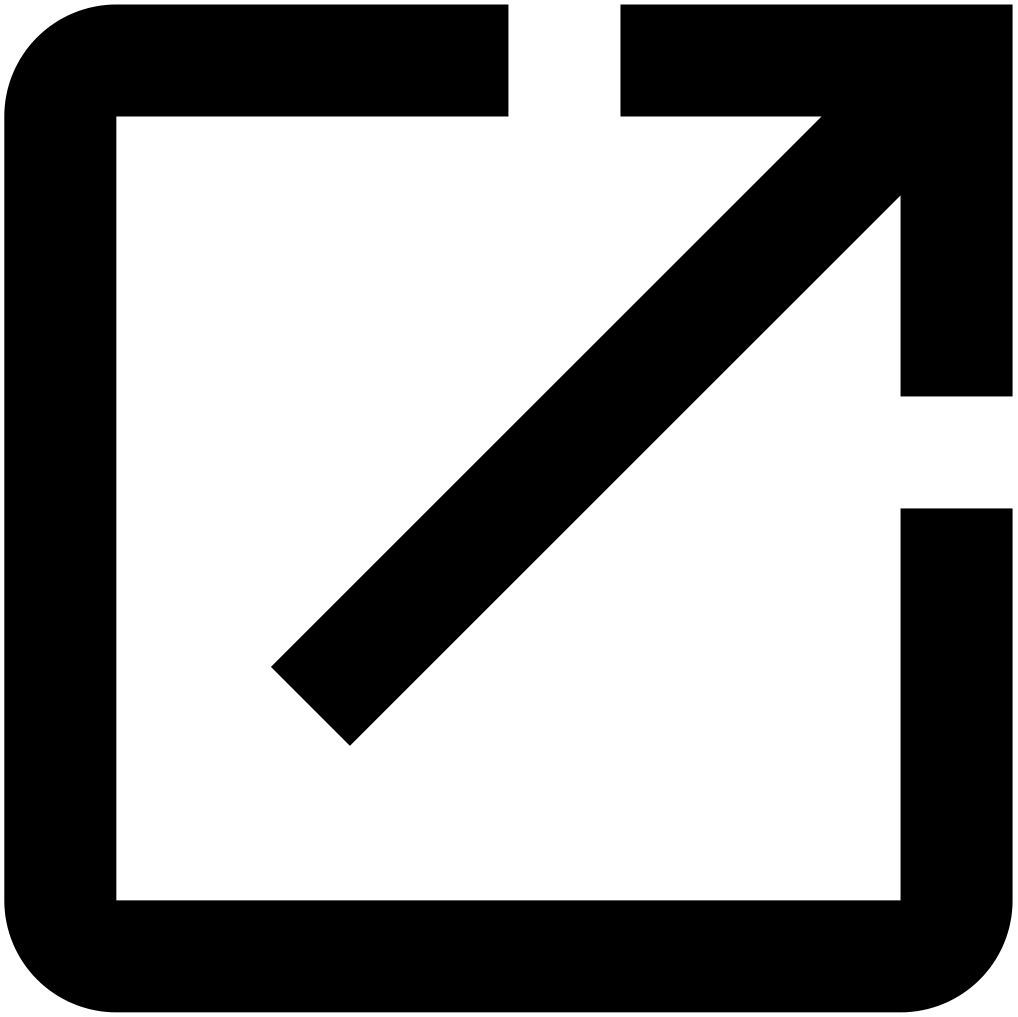
Published: 2020-05-01 · Archived: 2026-04-05 21:14:12 UTC

Hackers claim to have gained access to the network of Banco BCR, the state-owned Bank of Costa Rica, and stolen 11 million credit card credentials along with other data.

This attack was allegedly conducted by the operators of the Maze Ransomware, who have been behind numerous cyberattacks against high-profile victims such as IT services giant Cognizant, cyber insurer Chubb, and drug testing facility Hammersmith Medicines Research LTD.

On their data leak site, the hackers claim to have gained access to Banco BCR's network in August 2019, but did not proceed with encrypting the devices as "the possible damage was too high."


F RTINET
0:00



Visit Advertiser websiteGO TO PAGE

Maze claims that the bank never secured their network and once again gained access to the bank's network in February 2020.

They state that they did not encrypt the bank during the second attack because it "was at least incorrect during the world pandemic," but claim to have stolen a few years of data, including 11 million credit cards.

Of these credit cards, 4 million are stated to be unique and 140,000 allegedly belong to people from the USA.

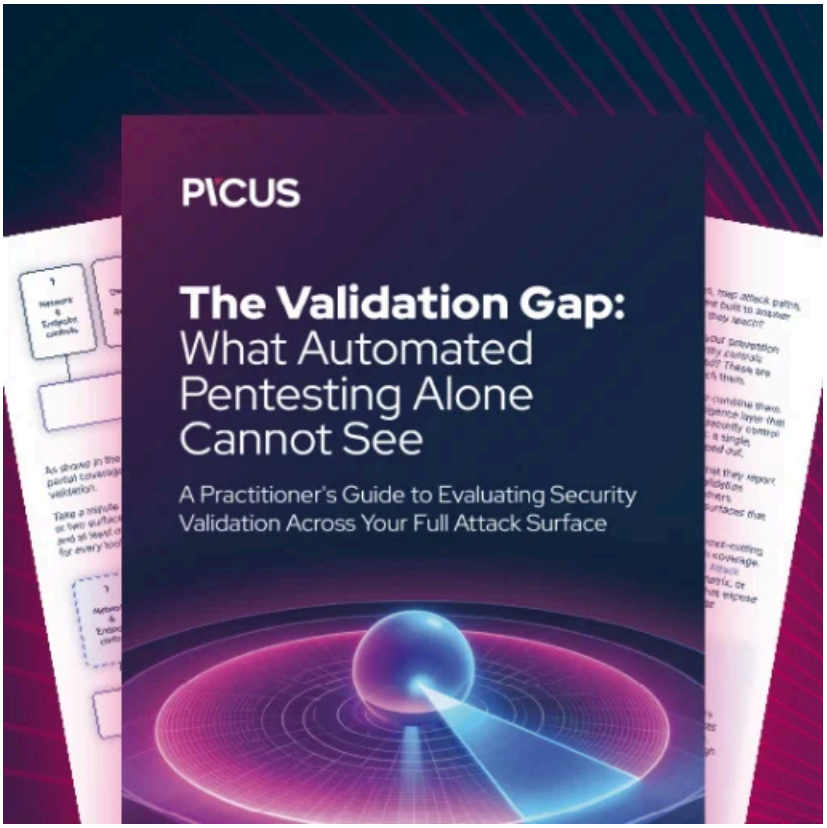
As proof of this theft, Maze posted what they say are 240 credit card numbers, with the last four digits removed, along with expiration dates and credit card verification codes (CVC).

The ransomware operators told BleepingComputer that they have tried to contact the bank multiple times with a ransom demand and may sell the data on the dark web.

Maze states that this ransom is their "reward for pointing out problems in the security system through which half a bank could be pulled out".

If you are a credit card customer of Banco BCR, it is suggested that you contact the bank to confirm that your account is not at risk and to monitor your credit card activity for fraudulent charges.

BleepingComputer has contacted Banco BCR to confirm the attack but has not received a response as of yet.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/hackers-say-they-stole-millions-of-credit-cards-from-banco-bcr/