Tap-to-pay, insert-to-rob: cybercriminals can now block contactless payments

Kaspersky ⋮ 7-9 minutes ⋮ 2/1/2023

If Prilex detects an NFC-based transaction and blocks it, the EFT software will program the PIN pad to show the following message:

Prilex is a notorious threat actor, that gradually evolved from Automated Teller Machines (ATMs)-focused malware into a unique modular Point of Sales (PoS) malware — the most advanced PoS threat discovered so far. As described by Kaspersky previously in 2022, Prilex threat actor conducts so-called “GHOST” attacks, allowing them to perform credit card fraud — even on cards protected with the purported unhackable CHIP and PIN technology. Now, Prilex has gone even further.

Security experts wondered whether Prilex was able to capture data coming from NFC enabled credit cards. Recently, during an incident response for a customer affected by Prilex, Kaspersky researchers uncovered three new modifications with the power to block contactless payment transactions, that become extremely popular during and after pandemics.

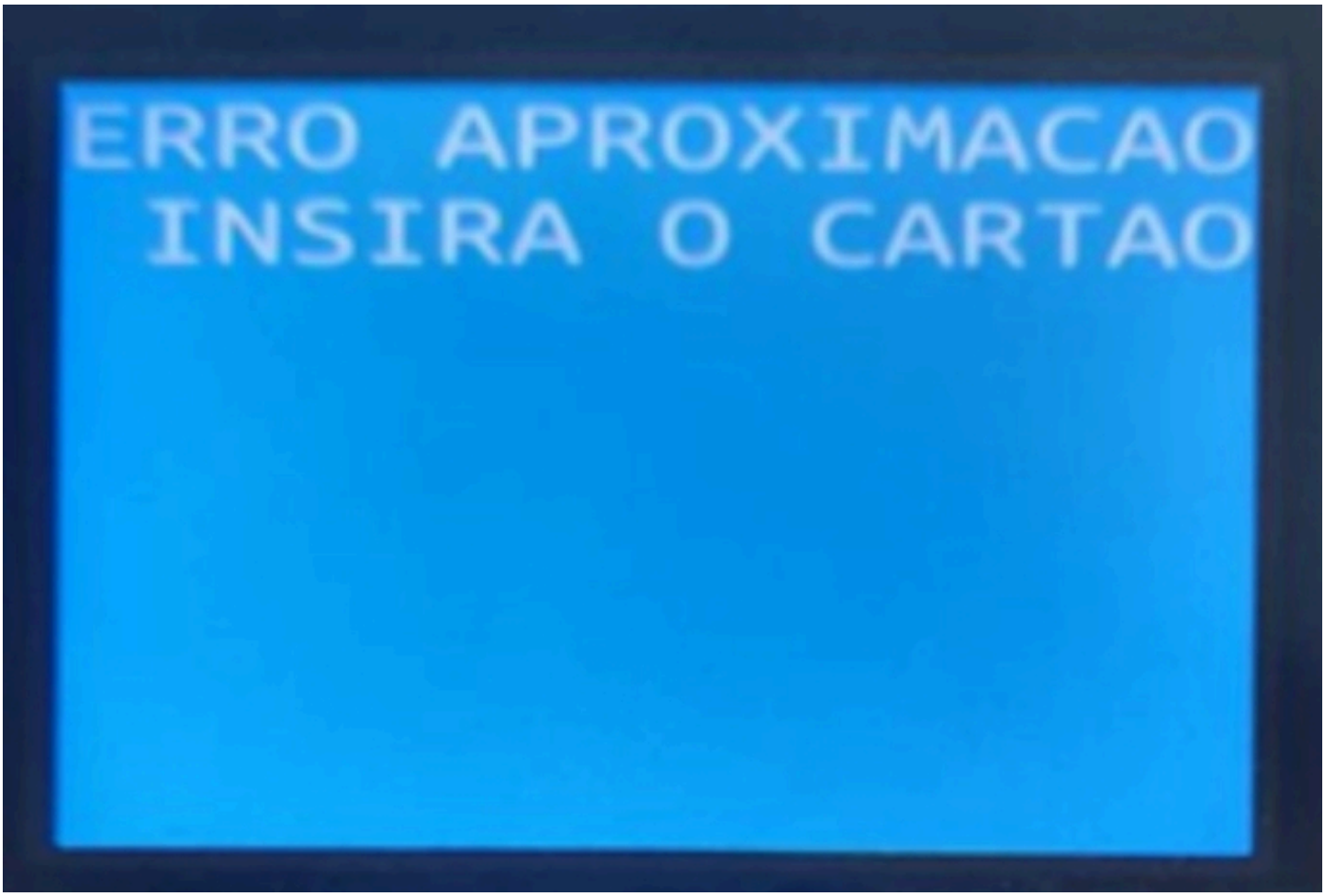
Contactless payment systems such as credit and debit cards, key fobs, and other smart devices, including mobile devices have traditionally featured radio-frequency identification (RFID). More recently, Samsung Pay, Apple Pay, Google Pay, Fitbit Pay and mobile bank applications have implemented near-field communication (NFC) technologies to support secure contactless transactions.

Contactless credit cards offer a convenient and secure way to make payments without the need to physically touch, insert or swipe the card. However, Prilex has learned to block such transactions by implementing a rule-based file that specifies whether or not to capture credit card information, and an option to block NFC-based transactions.

```
REGRA=modo=nfc;level=BLACK/INFINITE/CORPORATE/NANQUIM|nfcblock;ntm 1;error 2;chip
REGRA=modo=nfc;bandeira=AMEX|nfcblock;ntm 1;error 2;chip
REGRA=modo=nfc;issuer=[redacted];level=PLATINUM|nfcblock;ntm 1;error 2;chip
REGRA=modo=nfc;issuer=[redacted];level=[redacted]|nfcblock;ntm 1;error 2;chip
REGRA=modo=nfc;issuer=BANCO [redacted];level=PLATINUM|nfcblock;ntm 1;error 2;chip
```

Excerpt from Prilex rules file referencing to NFC blocking

Because NFC-based transactions generate a unique card number valid for only one transaction, if Prilex detects an NFC-based transaction and blocks it, the PIN pad will show the following message:



Prilex fake error displayed in the PIN pad reader that says "Contactless error, insert your card"

The cybercriminal's goal is to force the victim to use his/her physical card by inserting it into the PIN pad reader, so the malware can capture data coming from the transaction, using every way available for Prilex, such as manipulating cryptograms to perform GHOST attacks. Another new feature added to the latest Prilex samples is the possibility to filter credit cards according to their segment, and create different rules for different segments. For example, they can block NFC and capture card data, only if the card is Black/Infinite, Corporate or other with high transaction limit, which is much more attractive than standard credit cards, with low balance/limit.

Prilex has been operating in LatAm region since 2014 and is allegedly behind one of the largest attacks in the region. During the Rio carnival in 2016, the actor cloned more than 28,000 credit cards and drained more than 1,000 ATMs in Brazilian banks. Now, it has expanded its attacks globally. It was spotted in Germany in 2019 when a criminal gang cloned Mastercard debit cards issued by German bank OLB and withdrew more than €1.5 million from around 2,000 customers. As for the recently discovered modifications, they have been detected in Brazil – however, they may spread to other countries and regions as well.

"Contactless payments are now a part of our everyday life and the statistics shows the retail segment dominated the market with more than 59 percent share of the global contactless revenue in 2021. Such transactions are extremely convenient and particularly safe, so it's logical for cybercriminals to create malware that blocks NFC-related systems. As the transaction data generated during contactless payment is useless from a cybercriminal's perspective, it's understandable that Prilex needs to prevent contactless payment to force victims to insert the card into the infected PoS terminal," comments Fabio Assolini, head of the Latin American Global Research and Analysis Team (GReAT) at Kaspersky.

Read more about new Prilex PoS malware modifications on Securelist.

To protect yourself from Prilex, Kaspersky recommends:

- **Use a multi-layered solution**, offering an optimal selection of protective layers to provide the best security level possible for devices of differing power and implementation scenarios
- **Implement** Kaspersky SDK into PoS modules to prevent malicious code from tampering with the transactions managed by those modules.
- **Secure older systems with up-to-date protection** so they are optimized to run older versions of Windows and the latest Microsoft suite with full-functionality. This ensures your business will be provided with total support for the older MS families for the foreseeable future, and gives it an opportunity to upgrade anytime it is needed.
- **Install a security solution** that protects devices from different attack vectors, such as Kaspersky Embedded Systems Security. If the device has extremely low system specifications, the Kaspersky solution would still protect it with a Default Deny scenario.
- For financial institutions that are victims of this kind of fraud, Kaspersky recommends the Threat Attribution Engine to help IR teams to **find and detect Prilex files** in attacked environments.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 240,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

Tap-to-pay, insert-to-rob: cybercriminals can now block contactless payments

Kaspersky uncovered three new variants of Prilex malware, made by a group of cybercriminals, that was named after the most advanced Point-of-Sales (PoS) malware back in 2022. The discovered Prilex modifications can now block contactless near-field communication (NFC) transactions on infected devices, forcing customers to use their physical credit cards, enabling cybercriminals to steal money.

kaspersky