Prilex modification now targeting contactless credit card transactions

By GReAT

Published: 2023-01-31 · Archived: 2026-04-05 13:17:49 UTC

Prilex is a singular threat actor that has evolved from ATM-focused malware into unique modular PoS malware—actually, the most advanced PoS threat we have seen so far, as described in a previous article. Forget about those old memory scrapers seen in PoS attacks. Prilex goes beyond these, and it has evolved very differently. This is highly advanced malware adopting a unique cryptographic scheme, doing real-time patching in target software, forcing protocol downgrades, manipulating cryptograms, doing GHOST transactions and performing credit card fraud—even on cards protected with the so-called unhackable CHIP and PIN technology. And now, Prilex has gone even further.

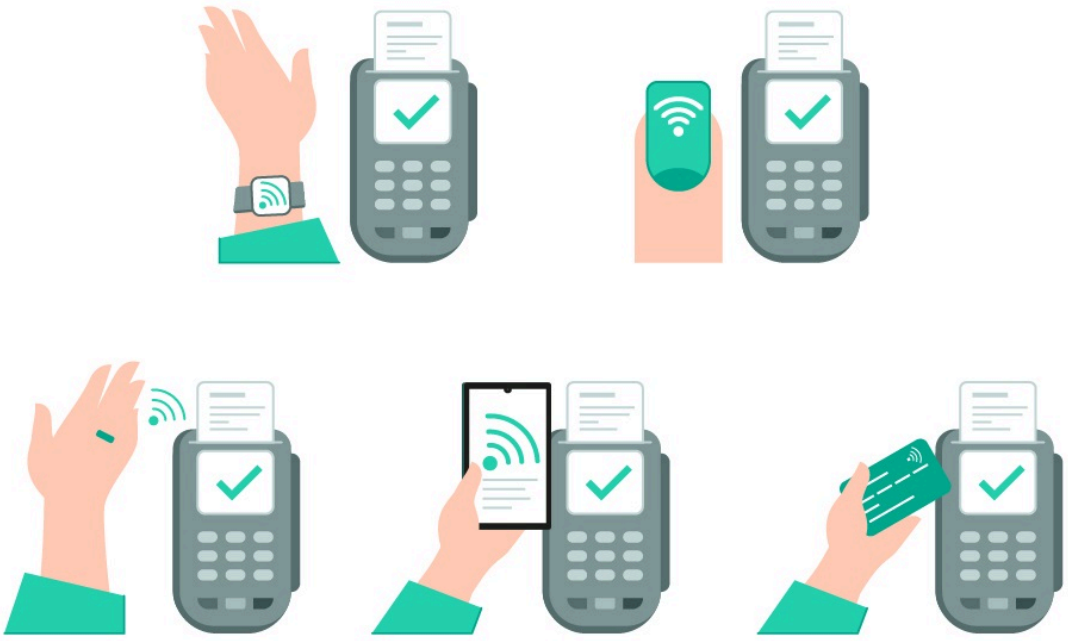
A frequent question asked about this threat was whether Prilex was able to capture data coming from NFC-enabled credit cards. During a recent Incident Response for a customer hit by Prilex, we were able to uncover **three new Prilex versions capable of blocking contactless payment transactions**, which became very popular in the pandemic times.

This blog post covers the NFC-related capabilities of recent Prilex modifications.

Tap-to-pay

Contactless payment systems are composed of credit and debit cards, key fobs, smart cards, or other devices, including smartphones and other mobile devices that use radio-frequency identification (RFID) or near-field communication (NFC, implemented in Samsung Pay, Apple Pay, Google Pay, Fitbit Pay, or any bank mobile application that supports contactless) for making secure payments.

The embedded integrated circuit chip and antenna enable consumers to pay by waving their card, fob, or handheld device over a reader at a point-of-sale terminal. Contactless payments are made in close physical proximity, unlike other types of mobile payments that use broad-area cellular or WiFi networks and do not require close physical proximity.



Different ways of tap-to-pay, but only one technology: NFC

Here is how they work:

- To make a payment with a contactless credit card, the cardholder simply holds the card close to the contactless-enabled payment terminal (usually within a few inches).
- The terminal sends a radio frequency (RF) signal to the card, activating the RFID chip embedded in the card.
- The RFID chip in the card sends a unique identification number (ID) and transaction information to the terminal. The transaction data is non-reusable, so even if it is stolen by cybercriminals, they cannot steal the money by using that. Neither can they access the RFID chip to tamper with the data generation processes.
- The terminal sends the transaction information to the card issuer's processing network for authorization.
- If the transaction is approved, the terminal usually displays a confirmation message, and the payment is processed.

The pandemic gave a boost to NFC payments

The size of the global market for contactless payments was estimated at $34.55 billion in 2021 and is expected to continue growing at a compound rate of 19.1% from 2022 to 2030 annually, according to GrandView Research. The market was dominated by the retail segment, which accounted for more than 59.0% of global contactless revenue in 2021. Recent years saw an increase in the number of retail tap-and-go transactions: retailers can clearly see the benefits of contactless payments, which reduce transaction time, increase revenue, and improve

operational efficiency. As stated in a Mastercard global study covering the year 2020, 74.0% of retailers expressed the intention to continue using contactless payments beyond the pandemic.

According to the US Payments Forum, Visa reports that in the U.S., tap-to-pay accounts for 28% of all face-to-face transactions, five times the pre-pandemic levels, while Mastercard says that 82% of card-present transactions in the country are happening at contactless-enabled locations. In Australia, contactless payments were growing in popularity even before the pandemic, with four out of five point-of-sale purchases being contactless in 2019. In the coming years, the popularity of this payment method is expected to grow even more everywhere in the world.

Contactless credit cards offer a convenient and secure way to make payments without the need to physically insert or swipe the card. **But what happens if a threat can disable these payments in the EFT software running in the computer and force you to insert the card in the PINpad reader?**

Insert-to-get-robbed

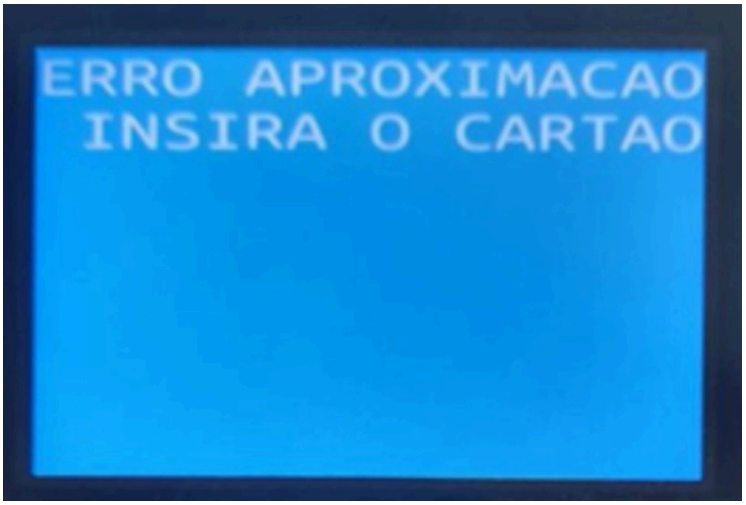
We have observed three new Prilex versions in the wild and managed to obtain the latest one (version 06.03.8080). The two others are 06.03.8070 and 06.03.8072.

The obtained version was discovered as **recently as November 2022** and appears to originate from a different codebase than the others we found at the beginning of that year. **Prilex now implements 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 a Prilex rules file referencing NFC blocking

This is due to the fact that NFC-based transactions often generate a unique ID or card number valid for only one transaction. If Prilex detects an NFC-based transaction and blocks it, the EFT software will program the PIN pad to show the following message:



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

Of course, the goal here is to force the victim to use their physical card by inserting it into the PIN pad reader, so the malware will be able to capture the data coming from the transaction by using all the techniques described in our previous publication, such as manipulating cryptograms and performing a GHOST attack. Another interesting new feature added in the latest Prilex samples is the possibility to filter credit cards according to segment and create different rules for each segment. For example, these rules can block NFC and capture card data only if the card is a Black/Infinite, Corporate or another tier with a high transaction limit, which is much more attractive than standard credit cards with a low balance/limit.

Malware adapting to the latest trends

With contactless cards growing in numbers and adoption increasing all over the world, the number of payments using this method has increased significantly and is expected to grow further in the years to come. Since transaction data generated during a contactless payment are useless from a cybercriminal's perspective, it is understandable that Prilex needs to force victims to insert the card into the infected PoS terminal. While the group is looking for a way to commit fraud with unique credit card numbers, this clever trick allows it to continue operating.

The Prilex family is detected by all Kaspersky products as **HEUR:Trojan.Win32.Prilex** and **HEUR:Trojan.Win64.Prilex**. More detailed analysis on the latest Prilex versions and a full analysis are available to customers of our private Threat Intelligence Reports. For any requests on this topic, please contact crimewareintel@kaspersky.com.
