PCI Security Standards Council

# Prilex Malware

## Evolution and Prevention Techniques

# Agenda

- About Cielo
- What this presentation is not about
- Complexity of the Brazilian payment ecosystem
- POS Malware history
- Working with the community
- Key Takeaways

# Who I Am

Fernando Bucelli

- Graduated in Network Computers and Post Graduated in Information Security
- Internal Security Assessor – ISA
- PCI Professional – PCIP
- Since 2008 paving the way in payment security
- Since 2013 working for Cielo

PCI Security Standards Council

# About Cielo


- Leader in electronic payments in Latin America:
- +1 million merchants.

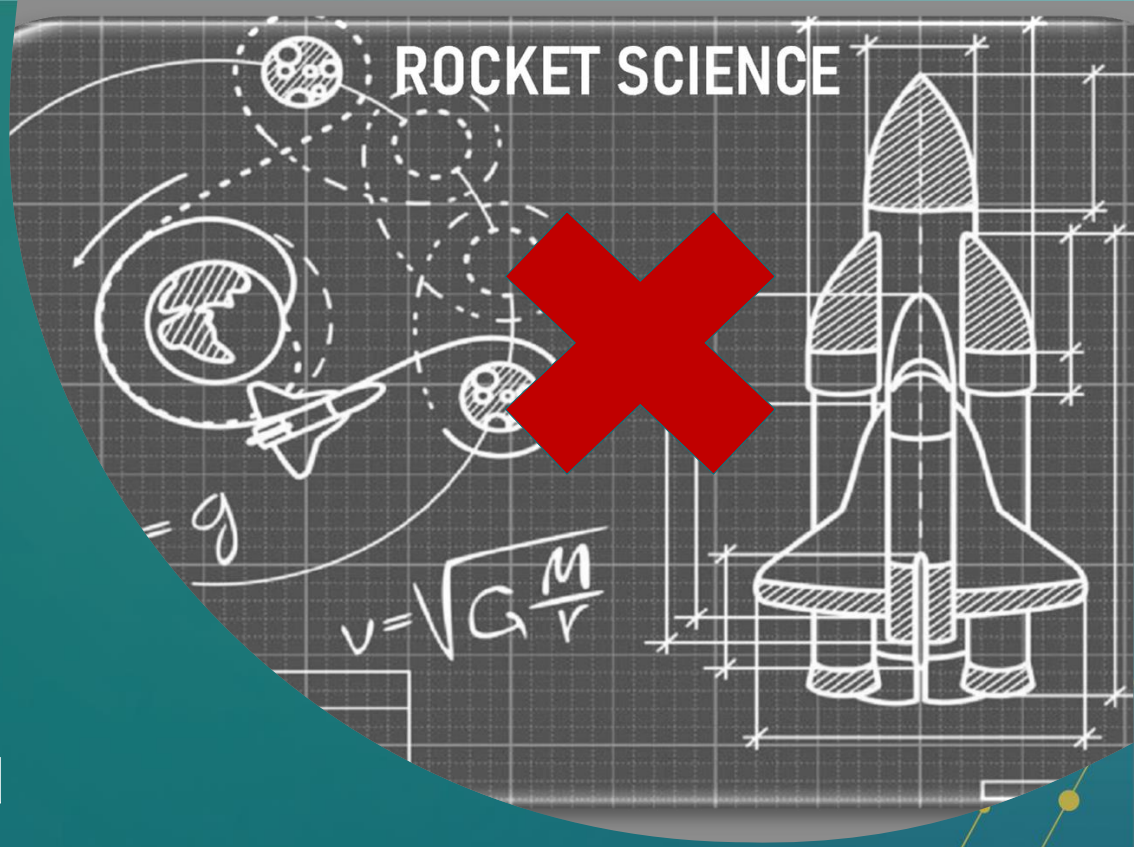
- 8 billion transactions processed:
  - 10% of Brazil's GDP are processed by Cielo.
  - 80 Brands are accepted at Cielo terminals.

- PPO | BoA | REB | RRG | TAB:
  +46,000 hours helping Merchants and Service Providers to be more secure.

PCI Security Standards Council

# What This Presentation is Not About

- This presentation is not a deep technical discussion about Prilex.
- This is about how the ecosystem has been suffering from malware and how we should organize ourselves to solve the problem.



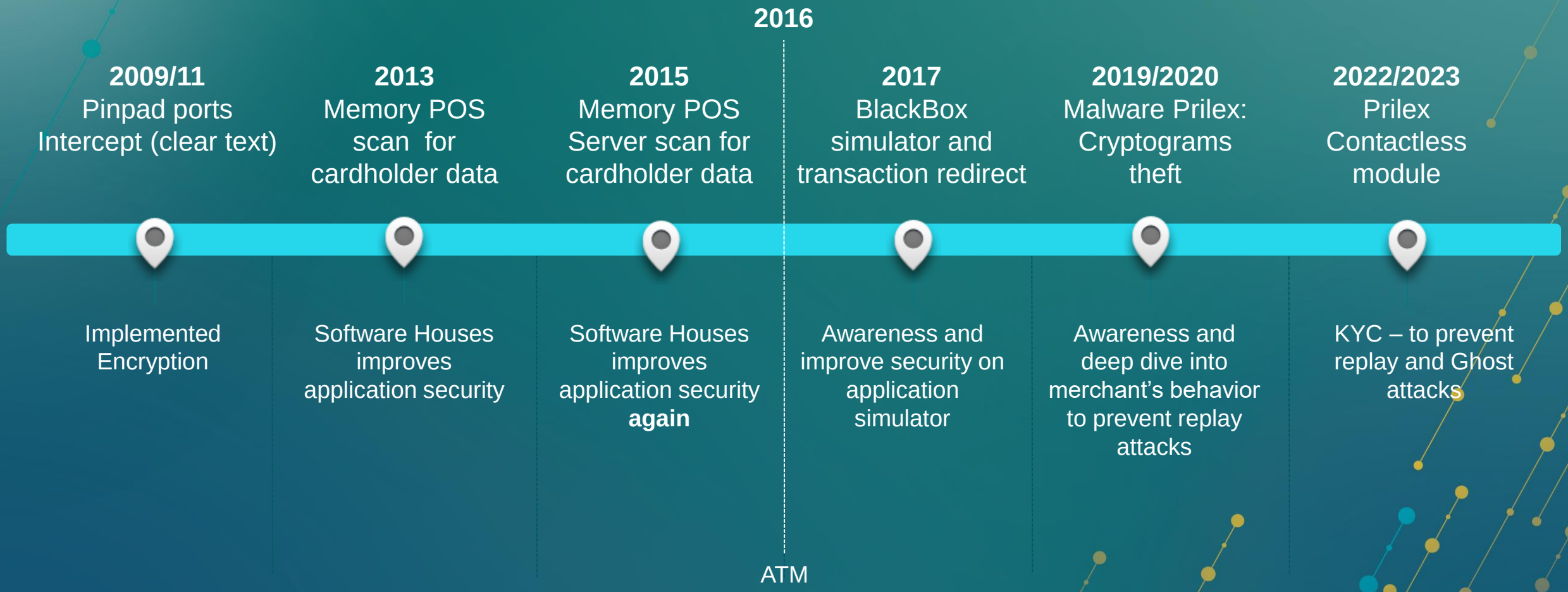

PCI Security Standards Council

# Complexity of The Brazilian Payment Ecosystem

1. Automation companies: Build the POS and provide integration with peripherals.
2. Software Houses – Develop the Payment Application – PA-DSS and SSF standards.
3. Domestic Brands that may have different rules for authorizes transactions.
4. Central Bank and Abecs to regulate how the ecosystem should work.


Different actors providing services.

# POS Malware History in Brazil



# Are we on The Same Page? – Some Concepts to Guide Us

- KYC – Know Your Customer  (Screening).

- ATC and Cryptogram on EMV Chip (*Fraud Identifiers*).
  - ATC: The Counter of transactions.
  - Cryptogram – Generation of a unique code.


- KSI – Transaction Counter on KSI (TC)

PCI Security Standards Council

# Working With The Community – What Are We Doing to Contain Replay Attacks

- KYC - Know Your Customer is the key to identifying and preventing cardholder theft and replay attacks!

- Fraud and prevention services support: a team working 24x7 to identify fraudulent registration and behavior of fraudsters.


PCI Security Standards Council

## Working With The Community – What Are We Doing to Contain Replay Attacks

KYC Analysis

- 50% of Cielo merchants use Standalone GPRS/Dial terminals. They have to worry about non-sophisticated attacks.

- The other 50% of Cielo merchants uses Point of Sales. Infrastructure sophisticated attacks.

PCI Security Standards Council

## Working With The Community – What Are We Doing to Contain Replay Attacks

## Fraud and Prevention Tools

- Custom rules to identify replay attacks originating from fraudsters merchants. The key of the work – ATC & Cryptograms are verified.

1. ATC Are the counters very different when compared to our database?
2. Cryptograms are the same already used on transactions?

# Working With The Community – What Are We Doing to Contain Replay Attacks

## Payment Community Task force

- Cross-work between acquirers, issuers and brands for quick action when new cases are identified.

PCI Security Standards Council

# Key Takeaways

- KYC – Know your customer
- ATC and Cryptograms
- Teamwork with community

Thank you!

fernando.bucelli@cielo.com.br