# A Journey To Protect Points Of Sale

**Nir Valtman, CISSP**
w : www.valtman.org
: @ValtmaNir

# Introduction

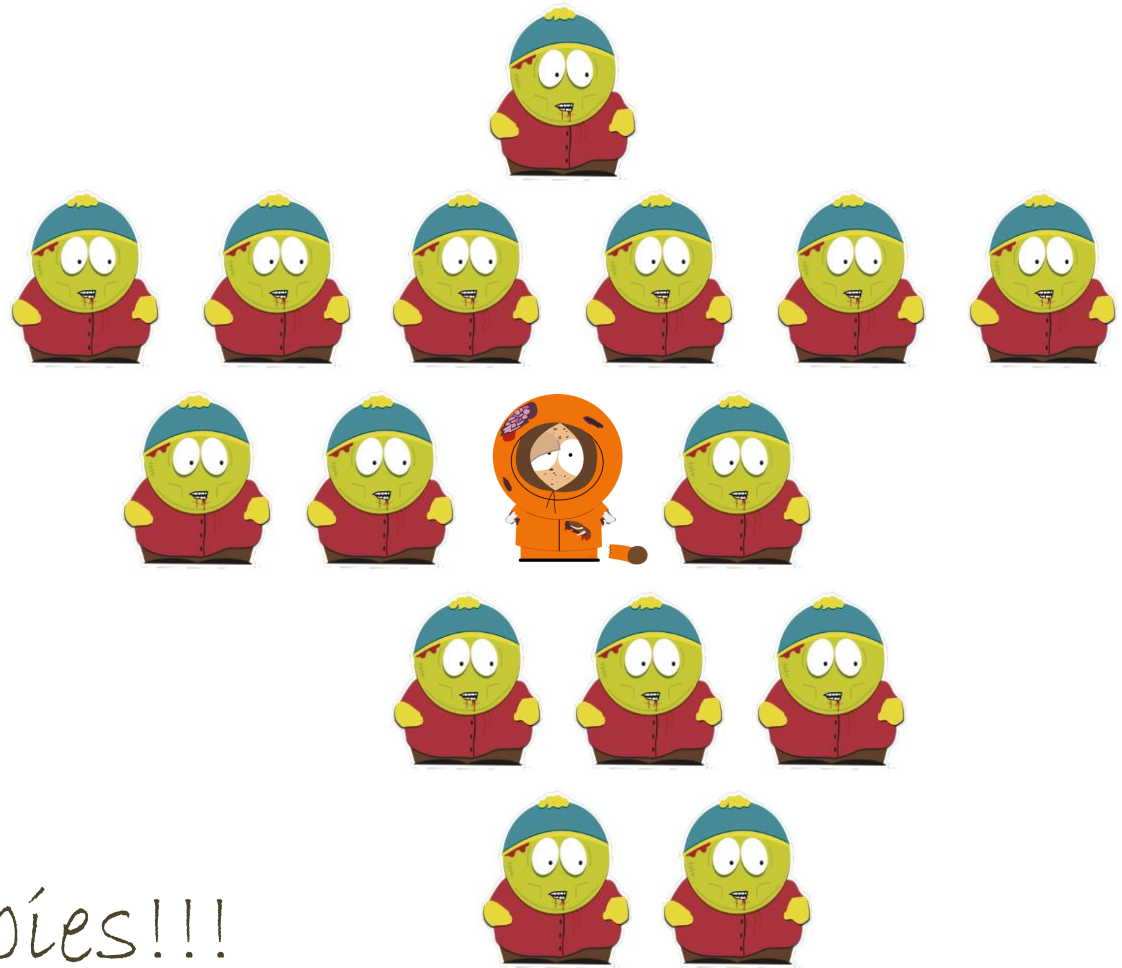


Photo by Bill Fraser


PUSH


Problems


NCR



Zombies!!!

# Defacement

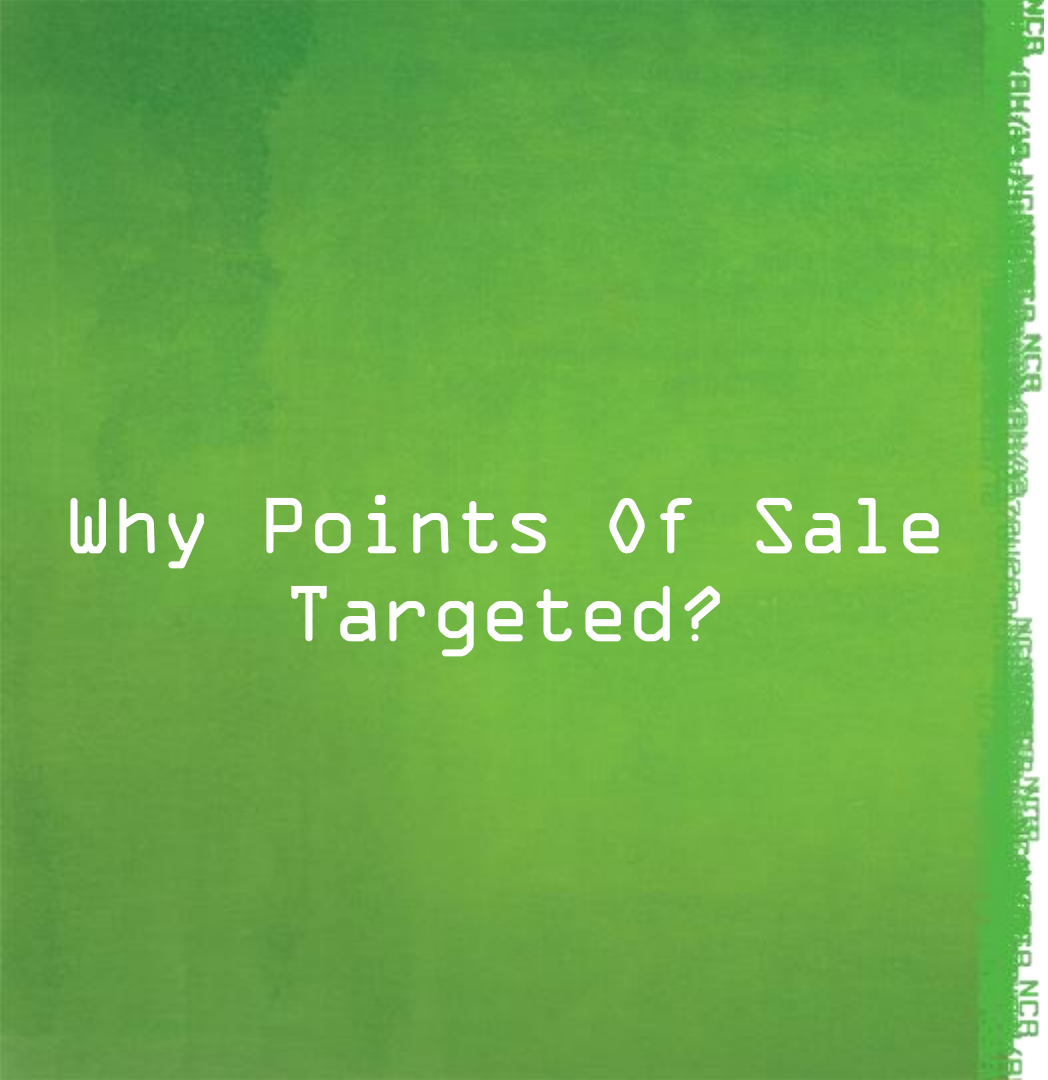
# OPEN SOURCE

AntiDef

Secure TDD

Memory Scraper

# Why Points Of Sale Targeted?



# CC's are delivered like this:

IBAN | CVV/CVV2 | EXP DATE | NAME | ADDRESS | CITY | STATE (USA) | ZIP | COUNTRY | MMN | DOB | SSN (USA) | PHONE | EMAIL |

---

**USA CC Fullz + tutorial**

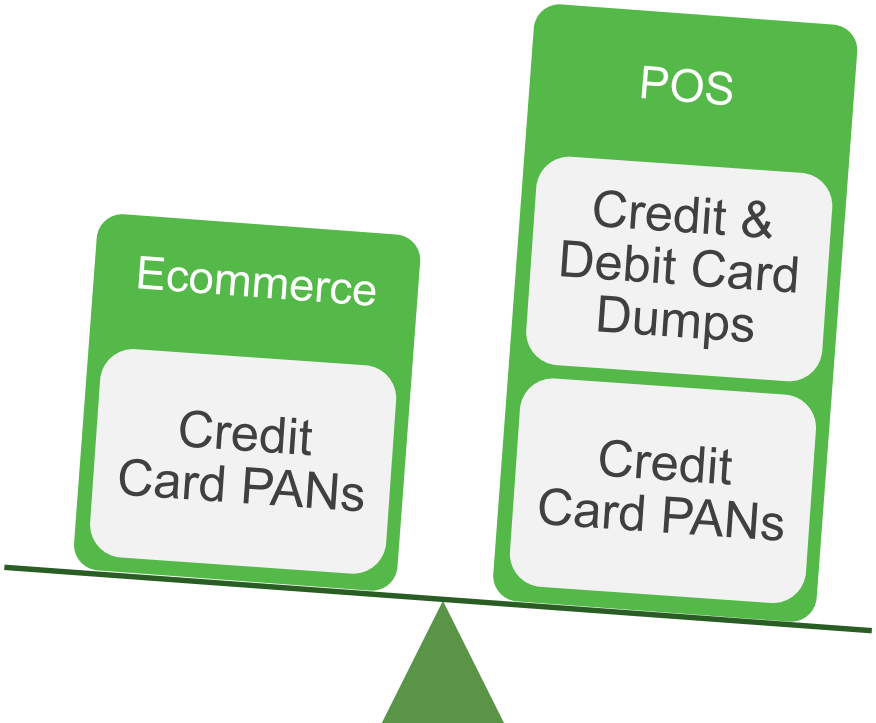
5 Full info CC USA – $40 /

Choose one or leave blank
5 Full info CC USA – $40 / 0.08BTC
10 Full info CC USA – $80 / 0.14BTC
20 Full info CC USA – $145 / 0.25BTC
Dumps USA + PIN – $100 / 0.17BTC

Each CC limit > 2000USD + tutorial

il)

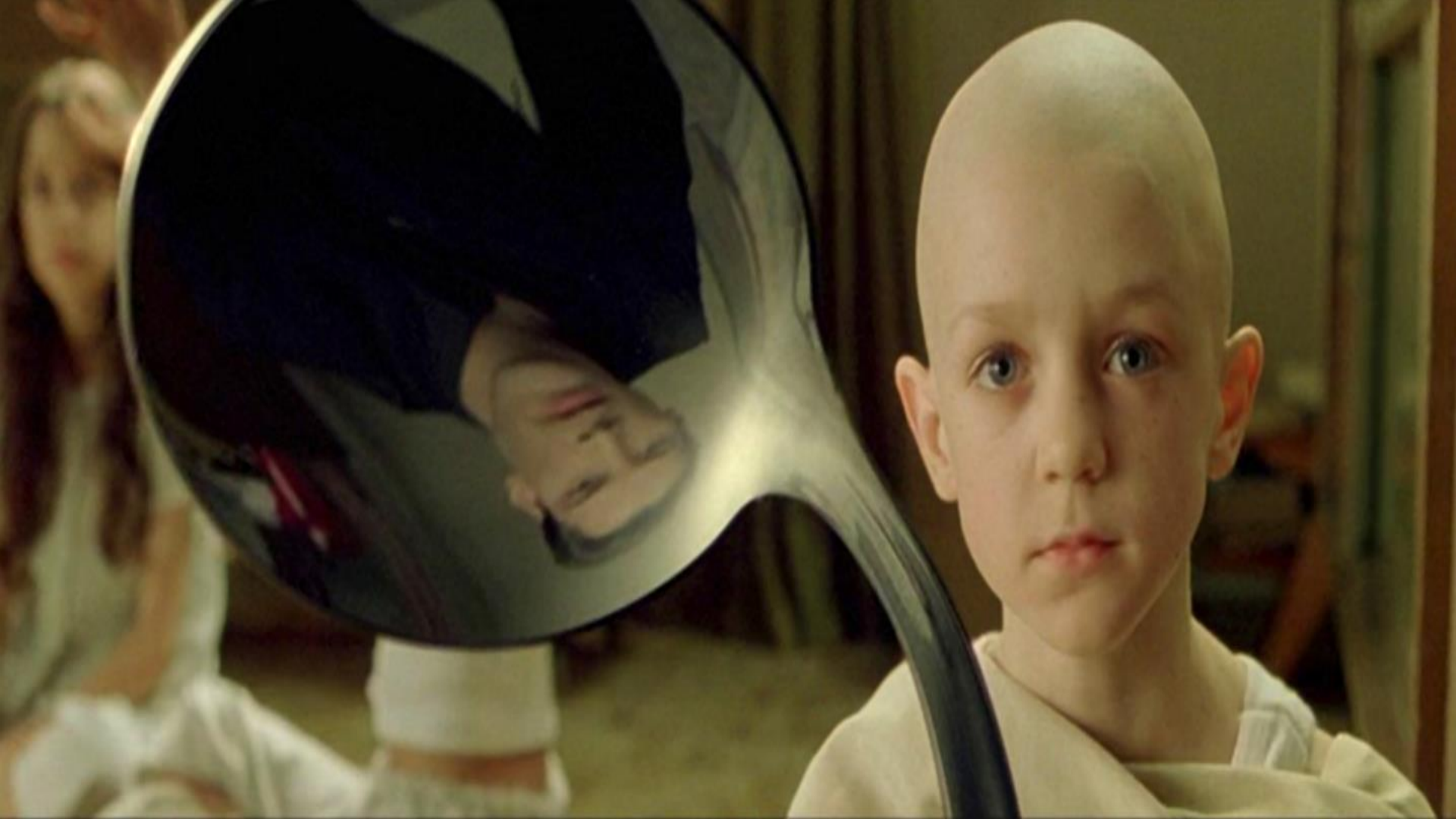
BUY (no javascript)

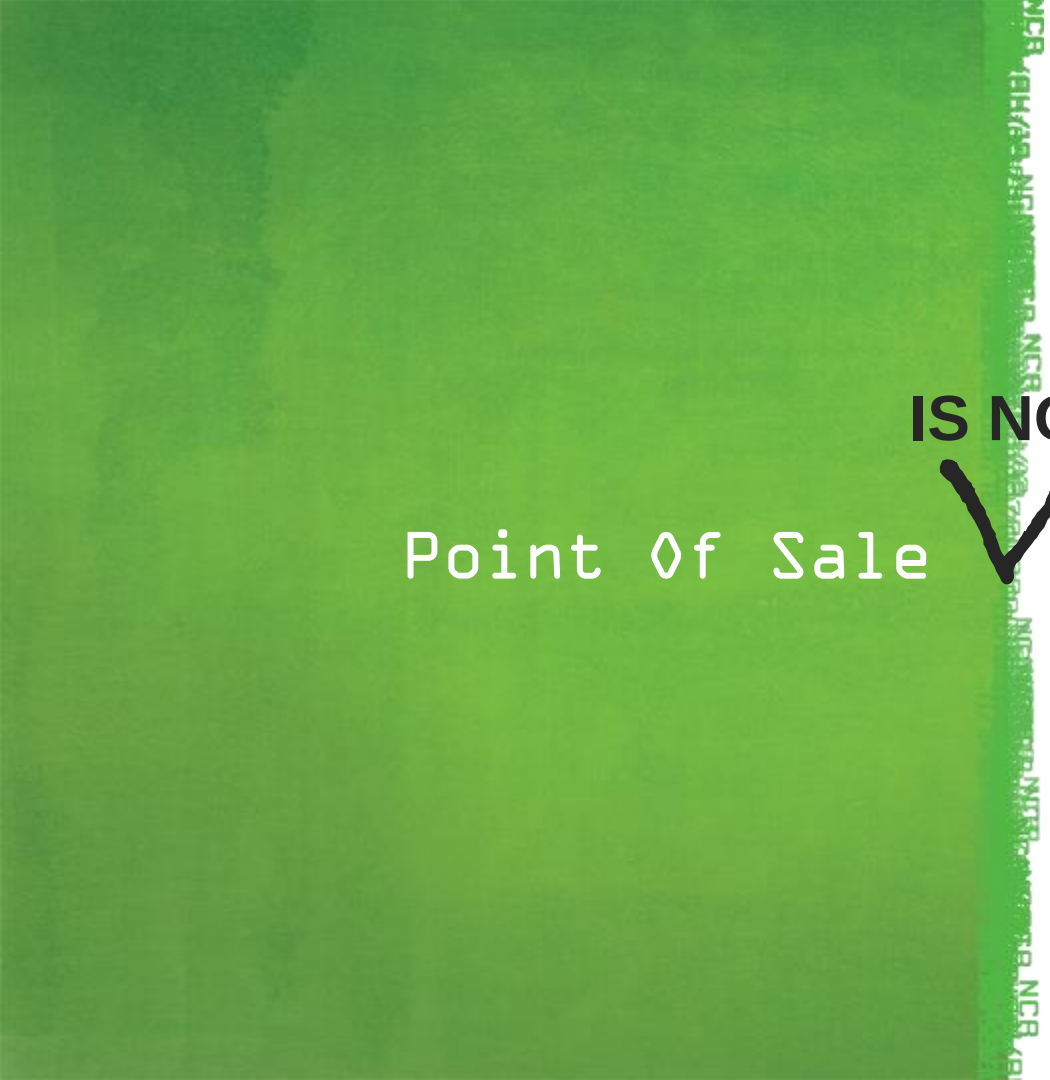

Ecommerce
Credit Card PANs
POS
Credit & Debit Card Dumps
Credit Card PANs

# Deployment

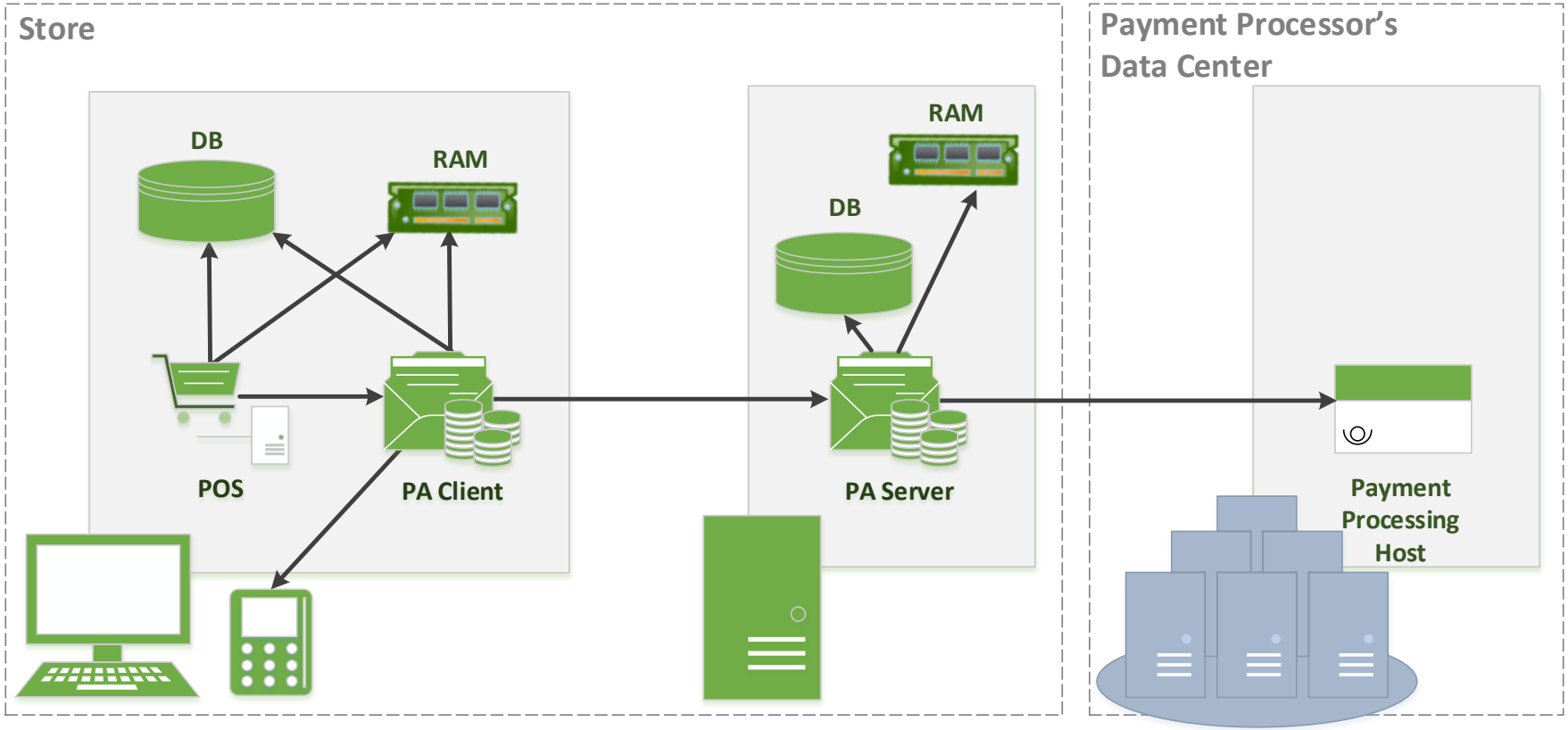

RealPOS


8:13 AM
connected
vantiv. Mobile Checkout
Powered by NCR Silver
Assign customer
Ticket
1 Goodnight Moon
Goodnight Moon
$5.99
1 The Great Gatsby
The Great Gatsby Hardcover
$15.64
1 Betty Crckr Cookbook
Betty Crocker Cookbook
$17.99
Lookup Item
Back to Items
Payment types
CASH
Cash
CHECK
Check
CREDIT
Credit Card
Gift
Non-integrated Gift...
PrePaid
PrePaid Coupons
$39.62
$3.19
Subtotal
Tax
Balance Due:
$42.81
Checkout
Hold
Void ticket
Ticket discount
Change tax
CARD
POWER
HAMLET
OTHELLO
ONE THING YOU CAN'T DO IN HEAVEN
David Allen
Getting Things DONE

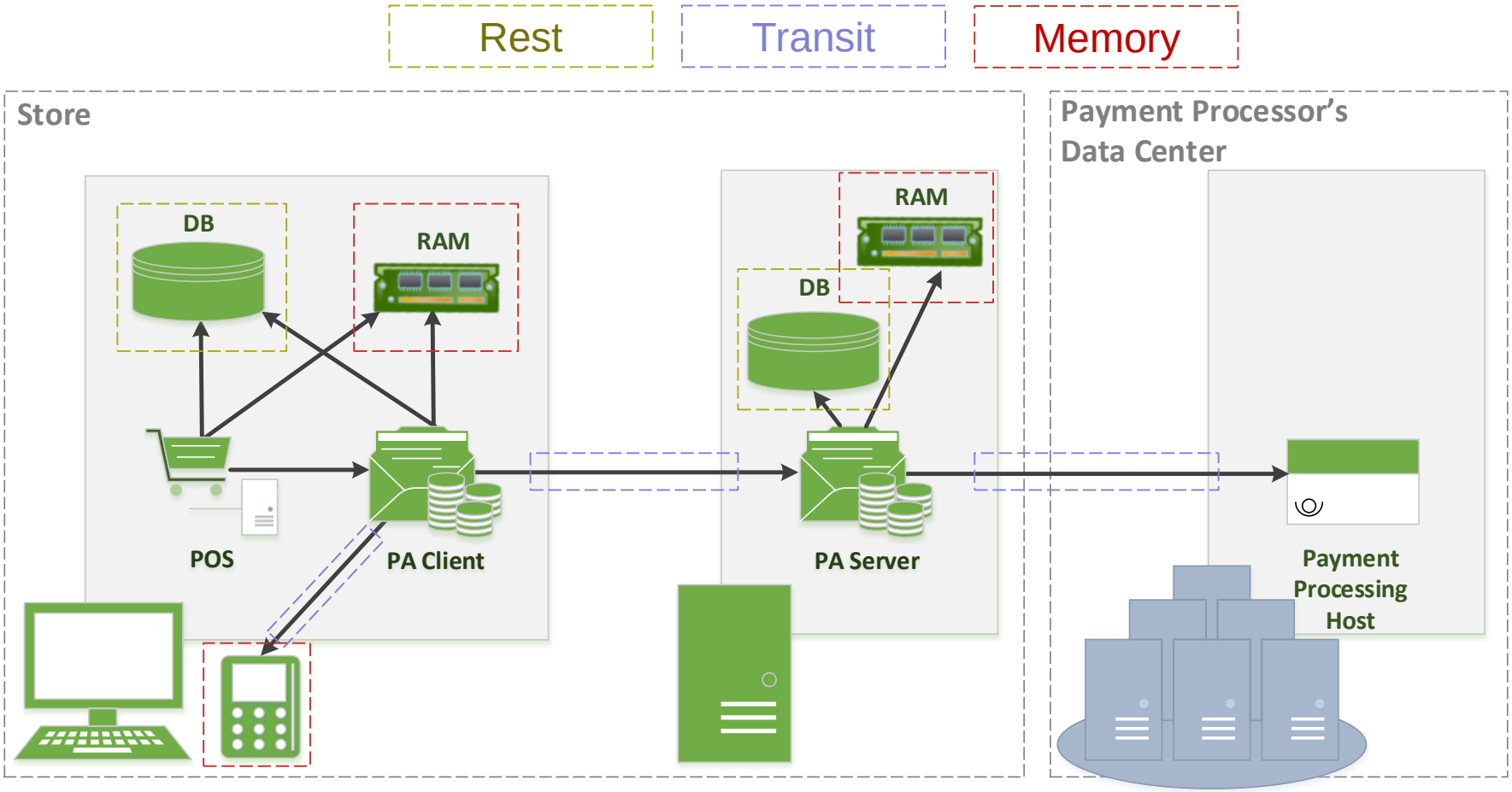




Point Of Sale IS NOT Payment Application

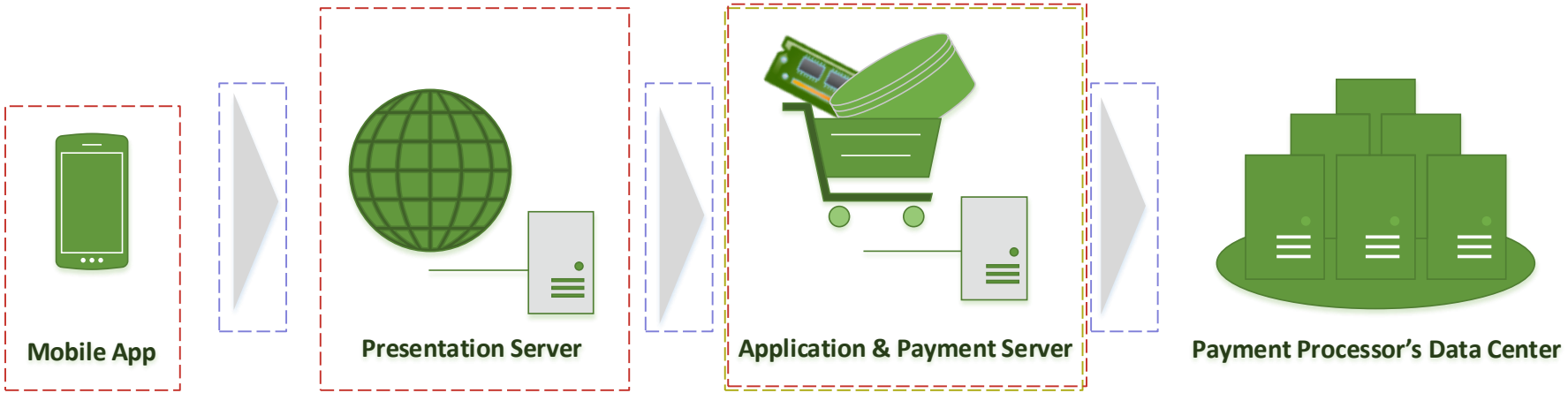

Store
DB
RAM
POS
PA Client
RAM
DB
PA Server
Payment Processor's Data Center
Payment Processing Host

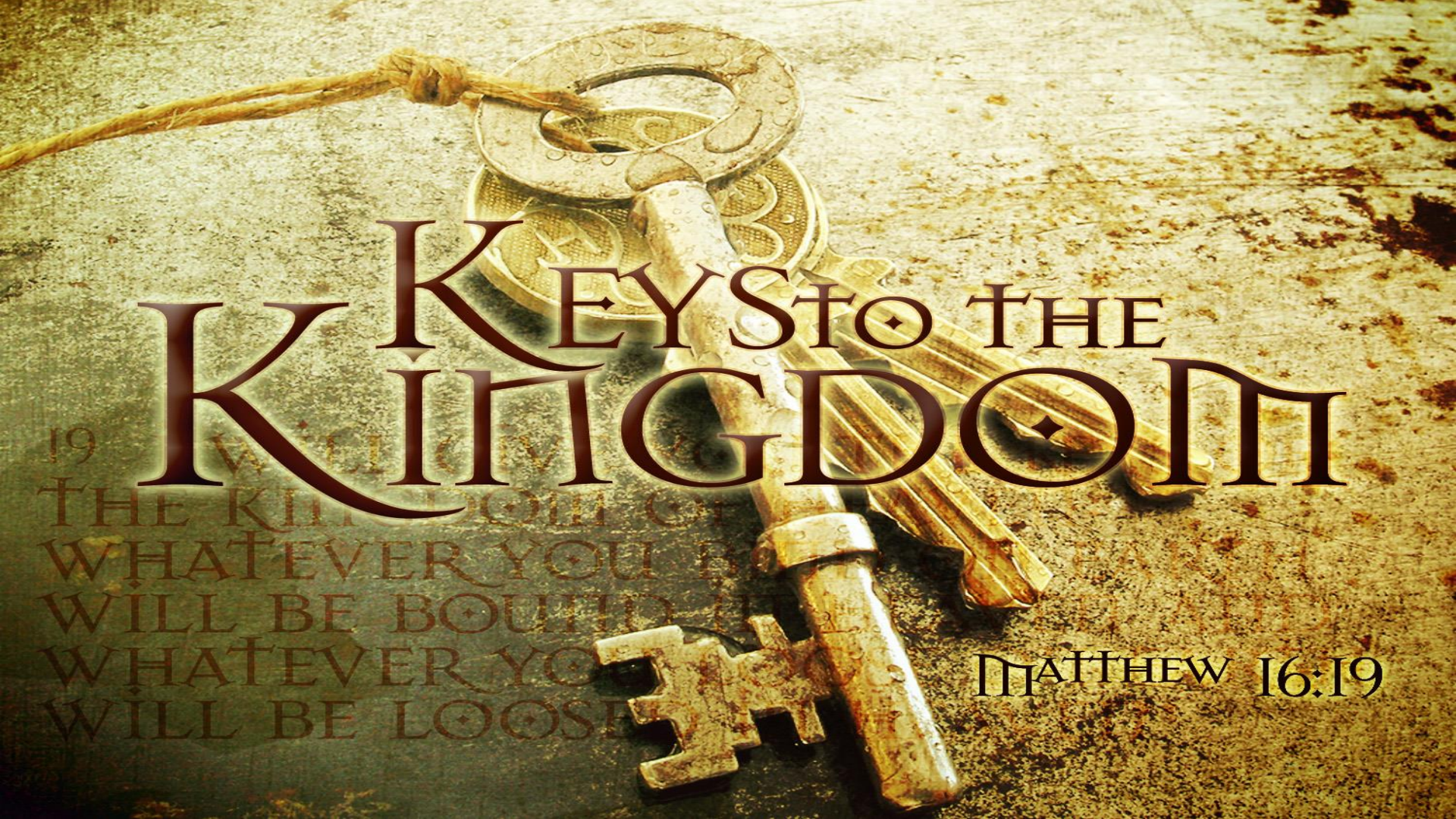
# Where Are My Credit Cards?

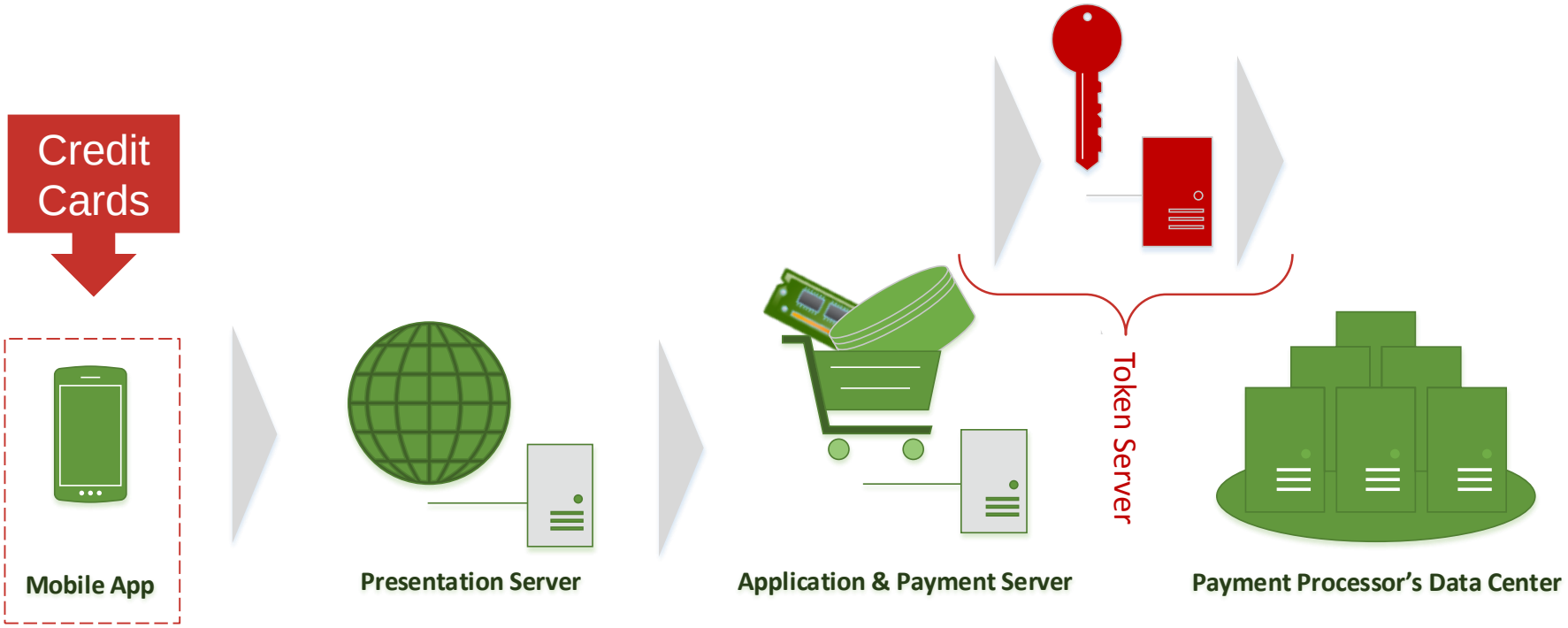


# Where Are My Credit Cards?

Rest | Transit | Memory




KEYS TO THE KINGDOM
MATTHEW 16:19


Credit Cards
Mobile App
Presentation Server
Application & Payment Server
Token Server
Payment Processor's Data Center

Retail
Environment
Assumptions


100% PCI Compliant

# Retail Environment Assumptions

Windows® Embedded POSReady 7

# Retail Environment Assumptions

Retail
Environment
Assumptions

# Retail Environment Assumptions

# Retail Environment Assumptions


Cashier ≠ hacker

# Retail Environment Assumptions

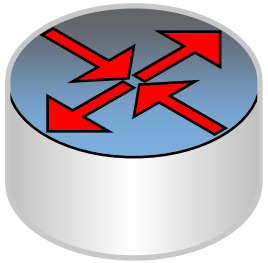
Big Brother

# RATs

Achilles Tendon

Remote Administration Tools

Achilles Tendon



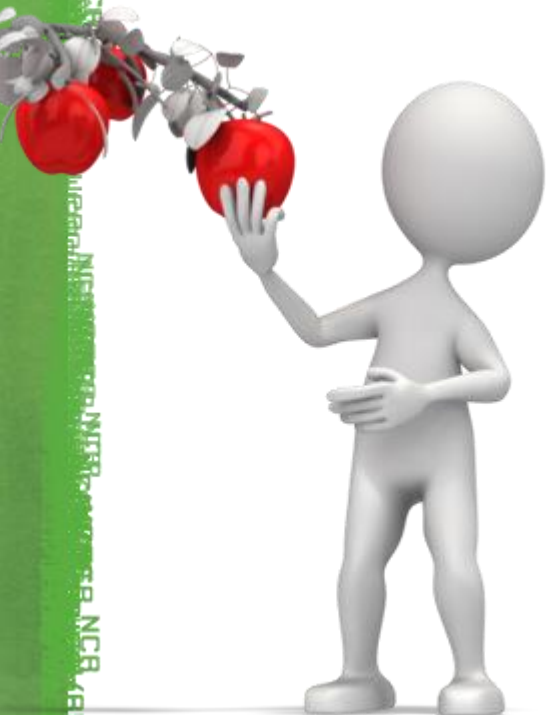
Routing

Achilles

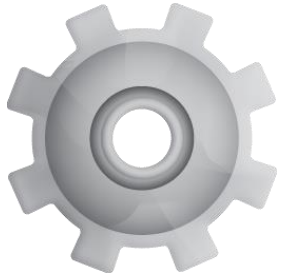
Tendon

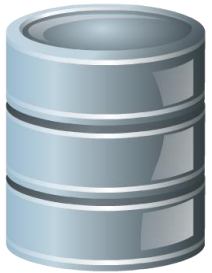

# Achilles Tendon

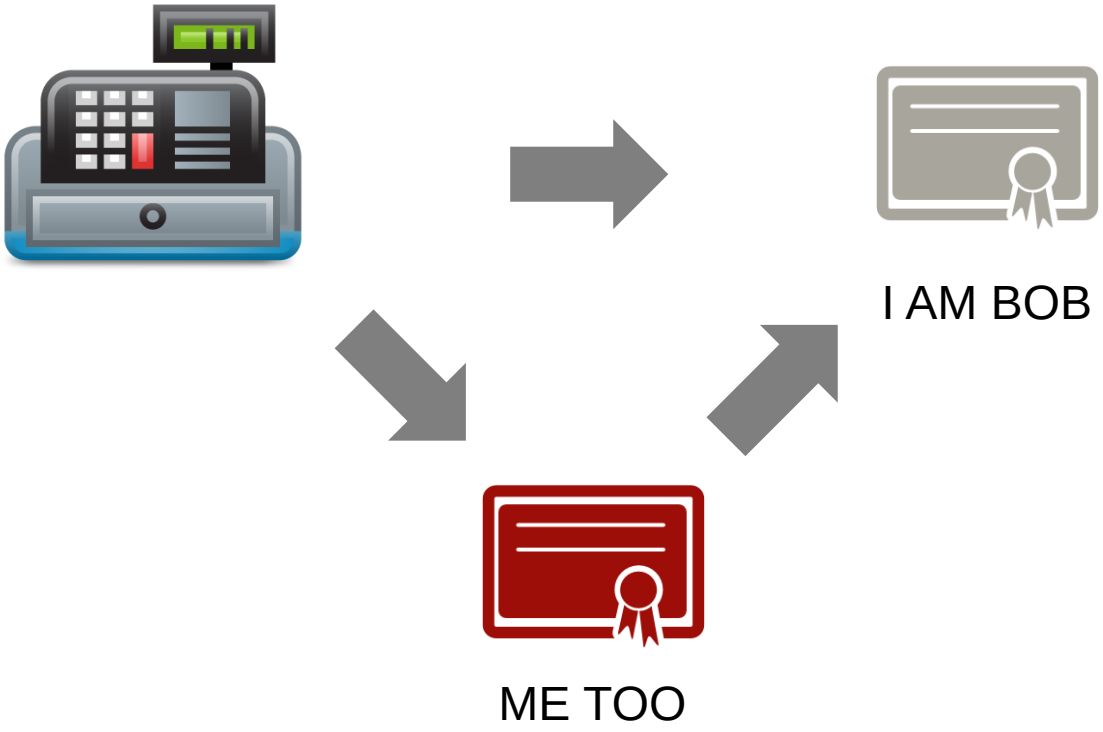
# Threats



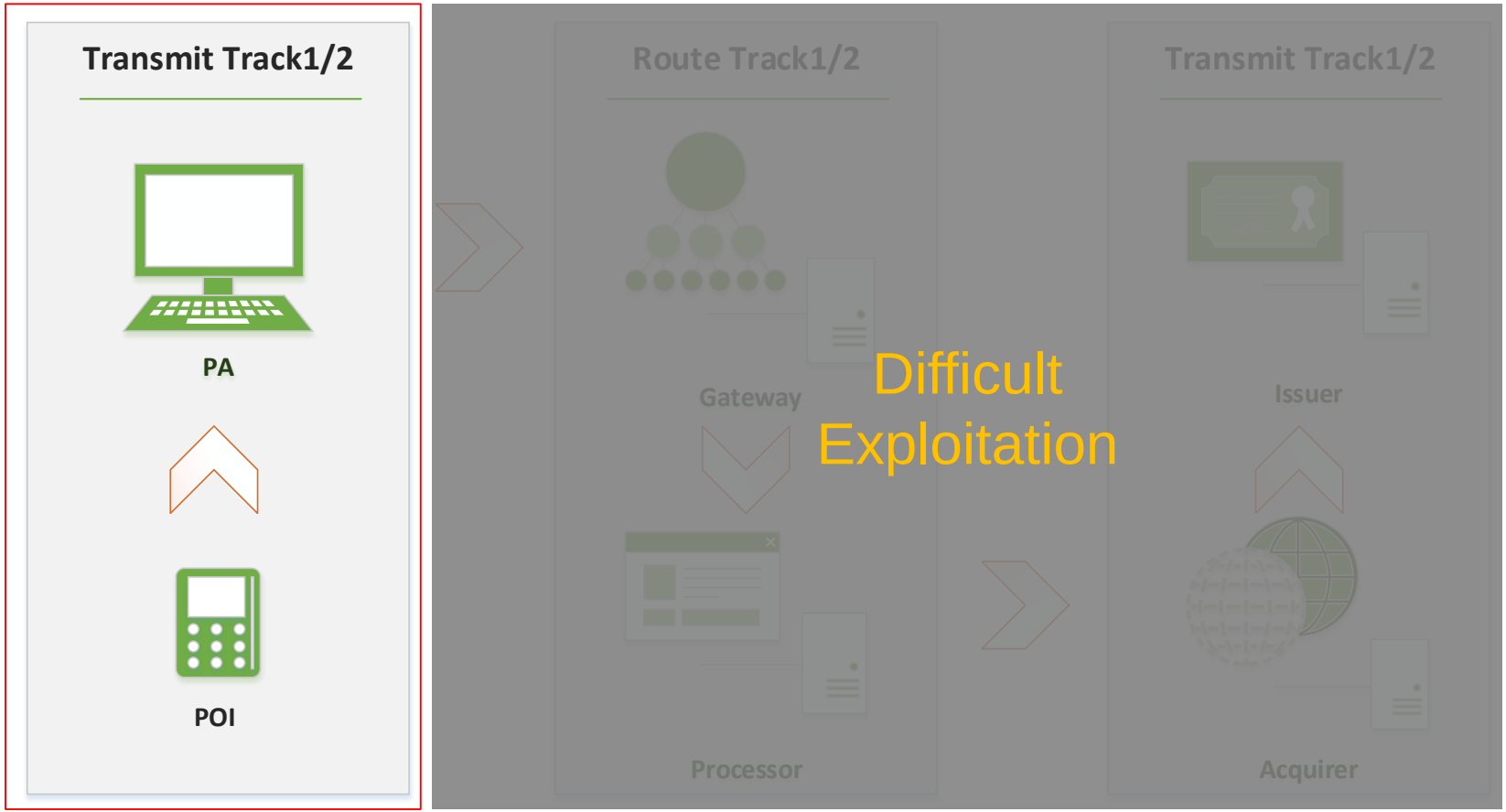

READ&WRITE





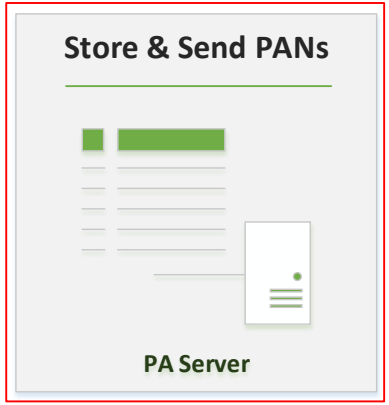

I AM BOB
ME TOO

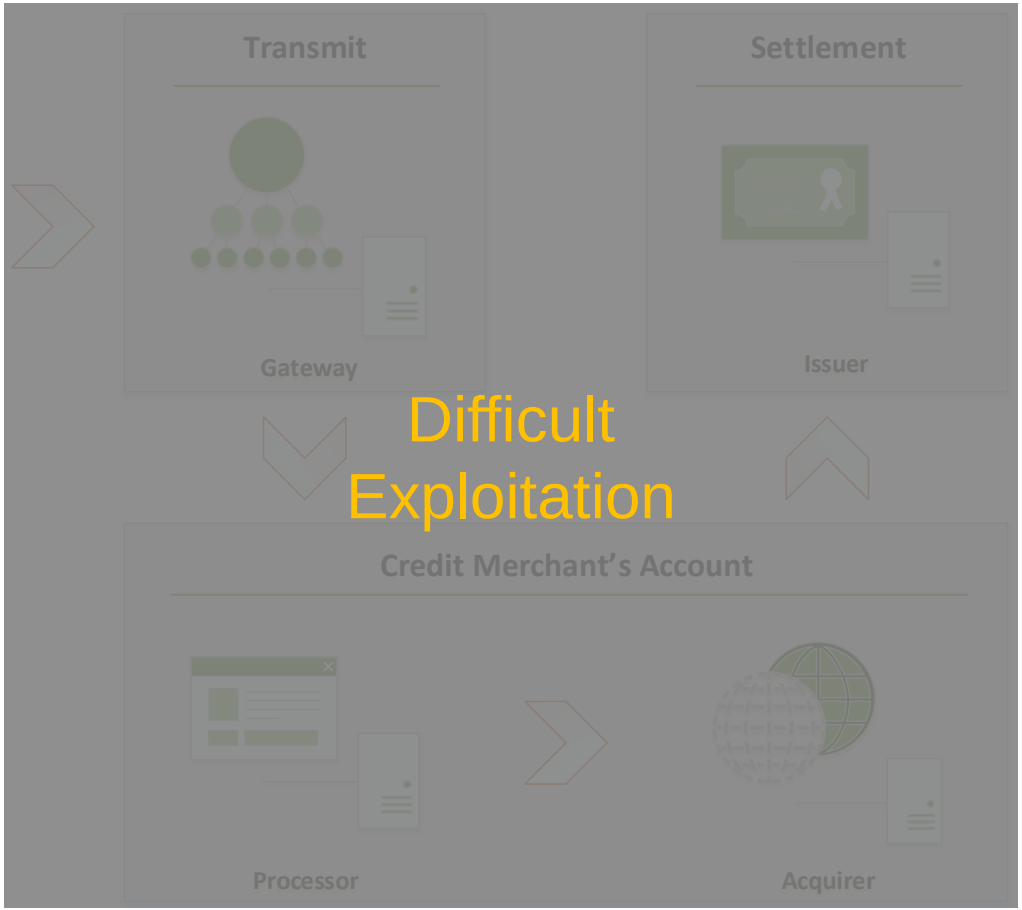
# Payment Stages - Authorization



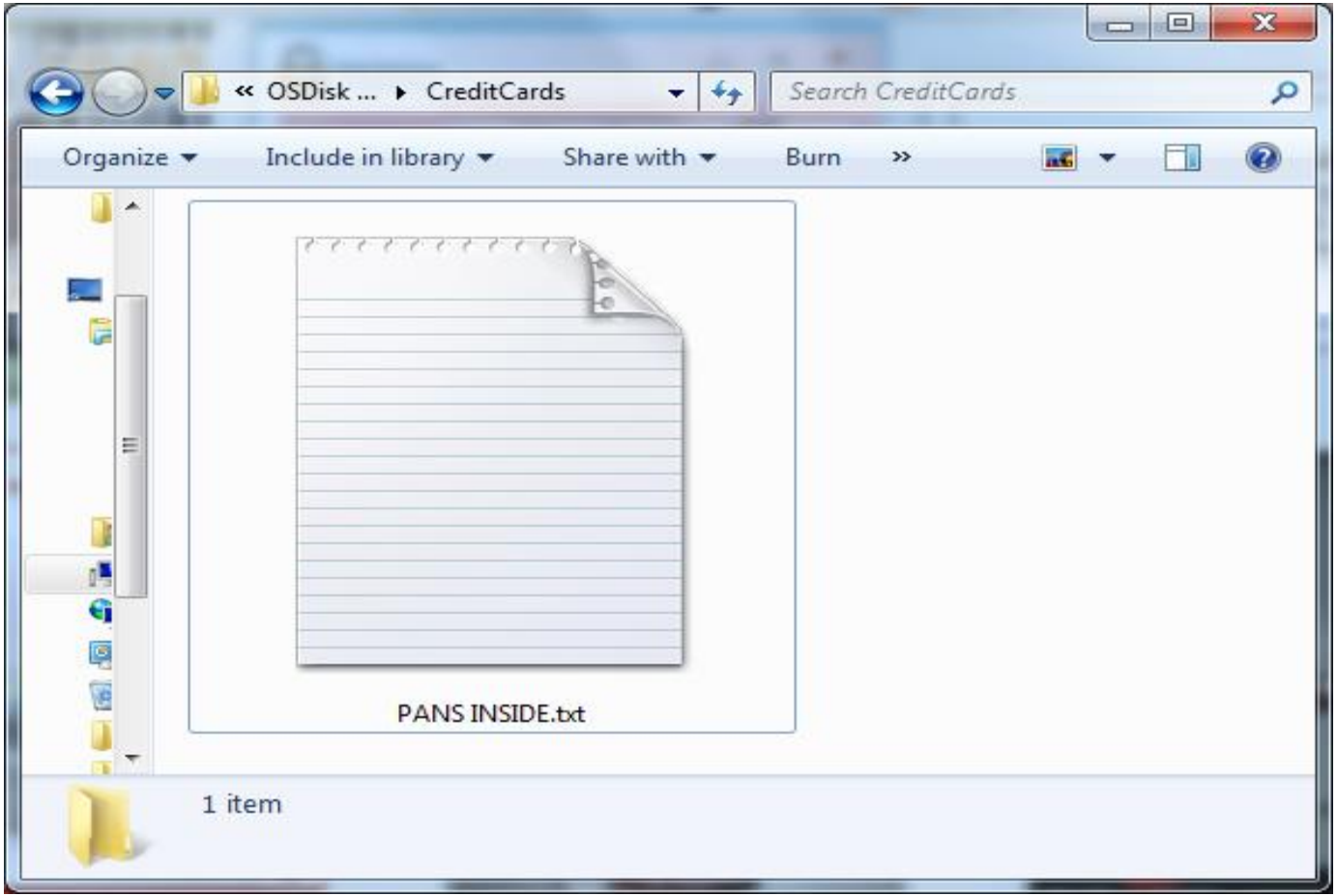
# Payment Stages - Authorization

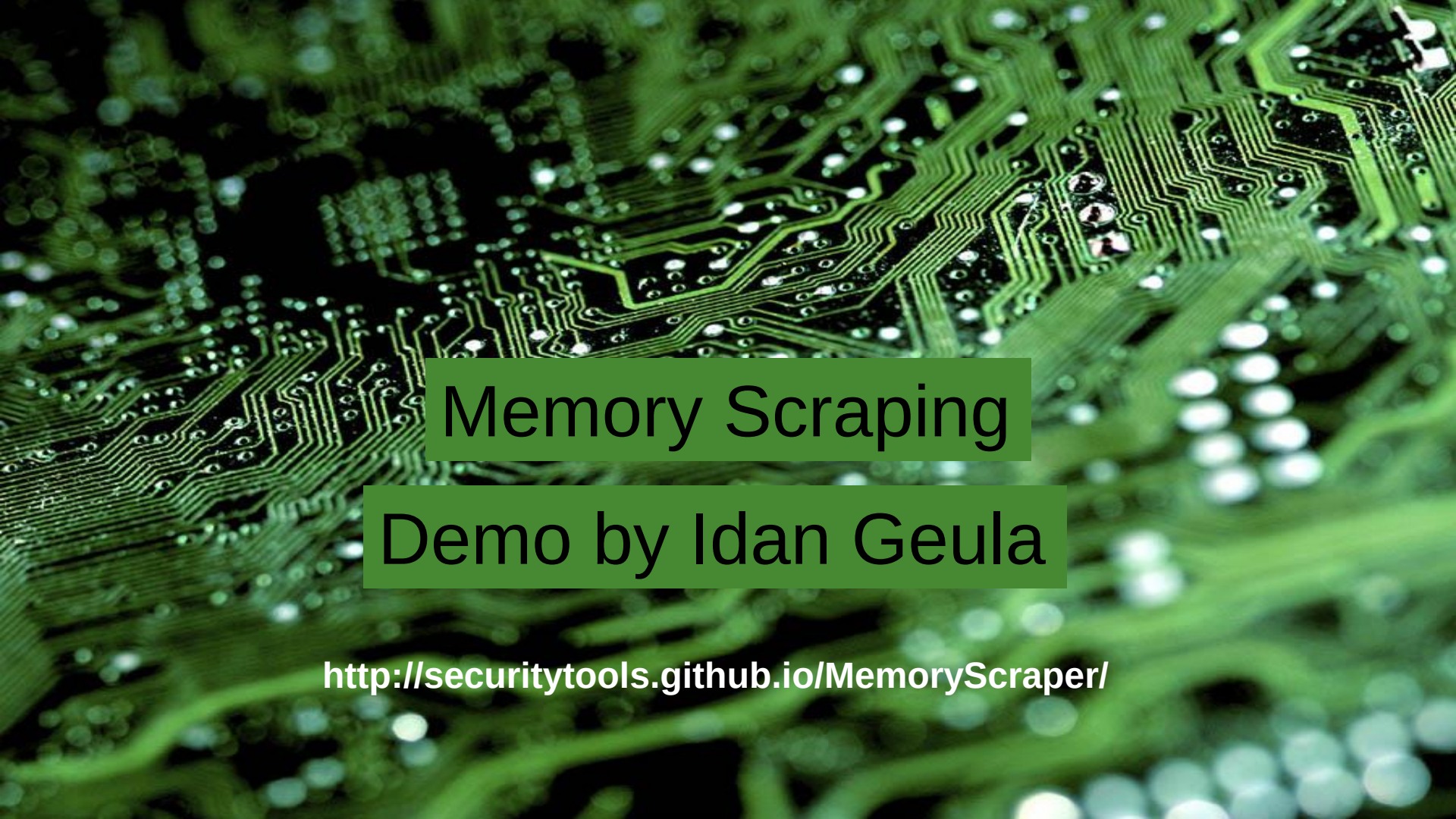
# Payment Stages - Settlement

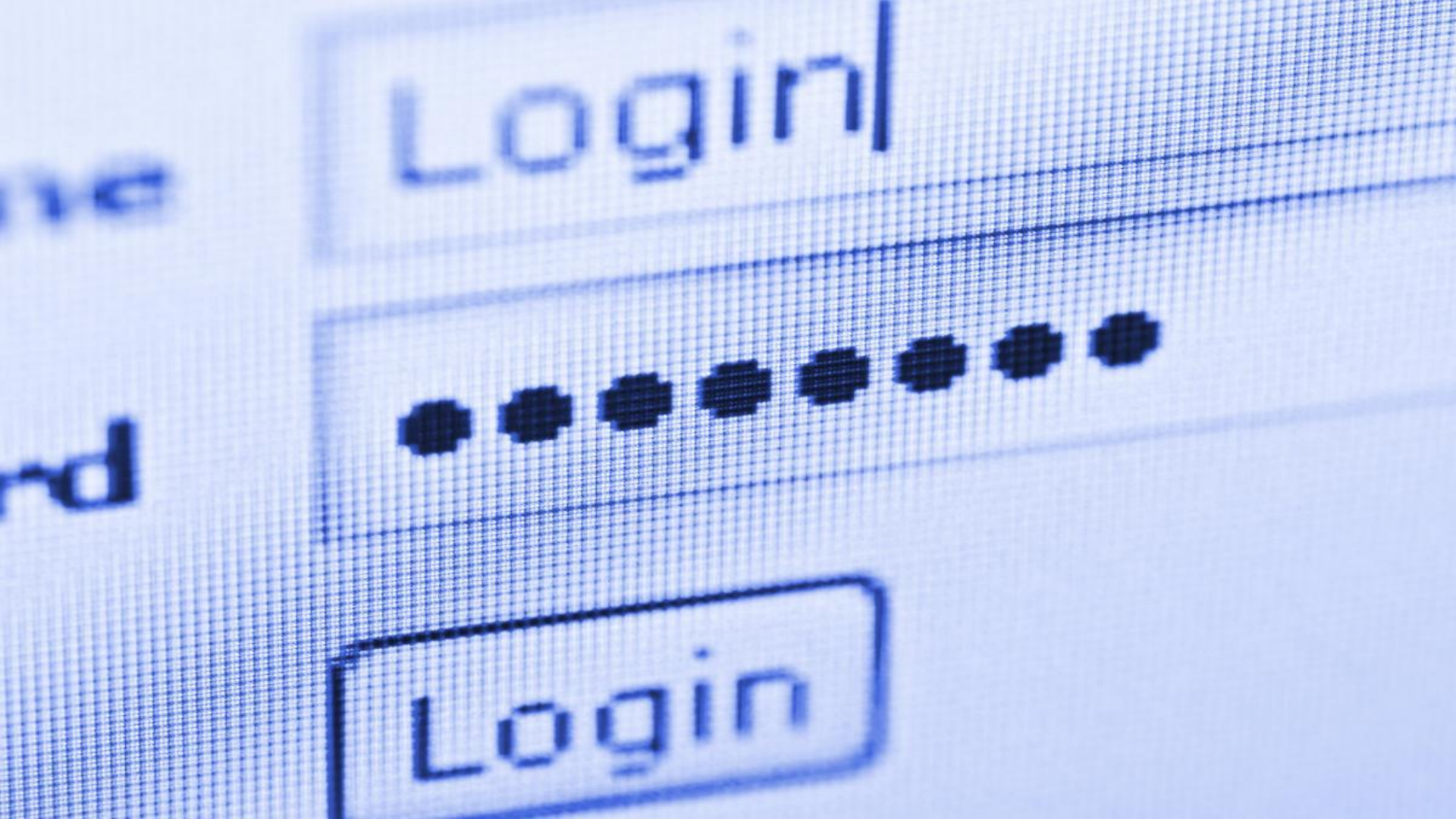


# Payment Stages - Settlement




Memory Scraping
Demo by Idan Geula
http://securitytools.github.io/MemoryScraper/


Login
Login


PRIVACY

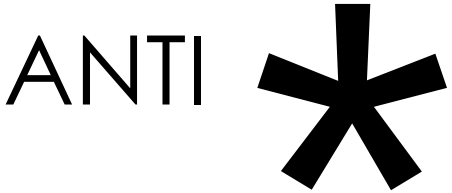

FBD


Online
VS
Offline

# Bypassed Solutions

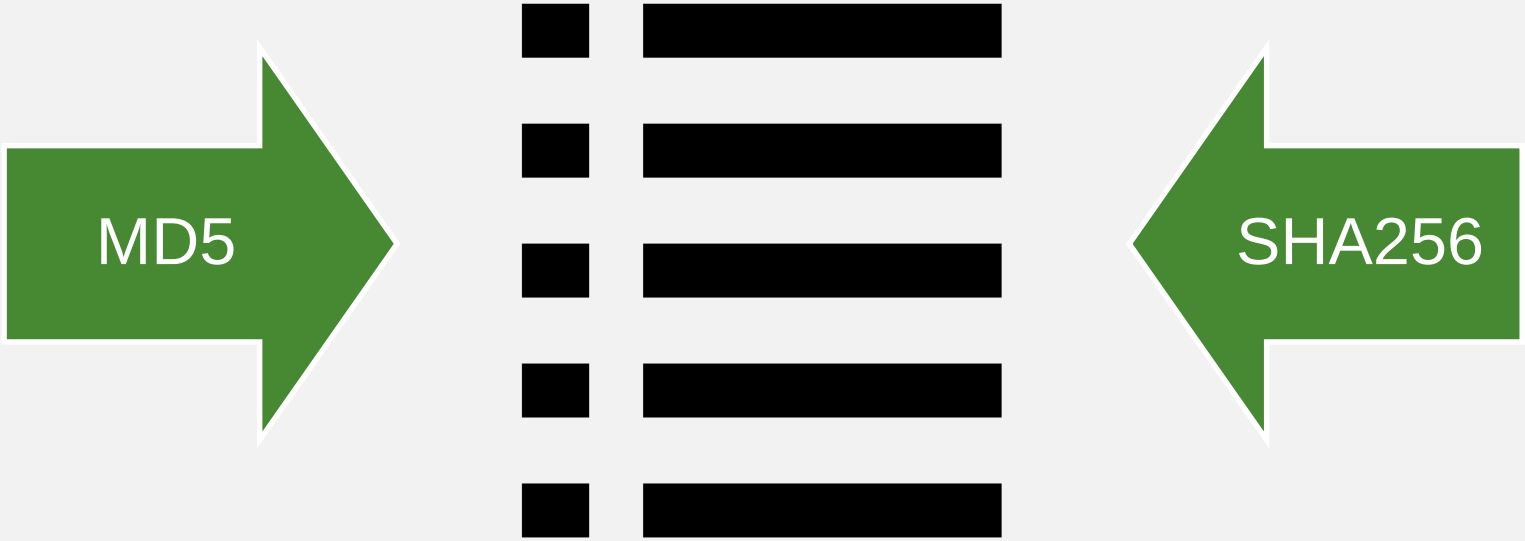

SecureString Class
Demo

# Next Next Next Generation Firewall


ANTI


Data loss

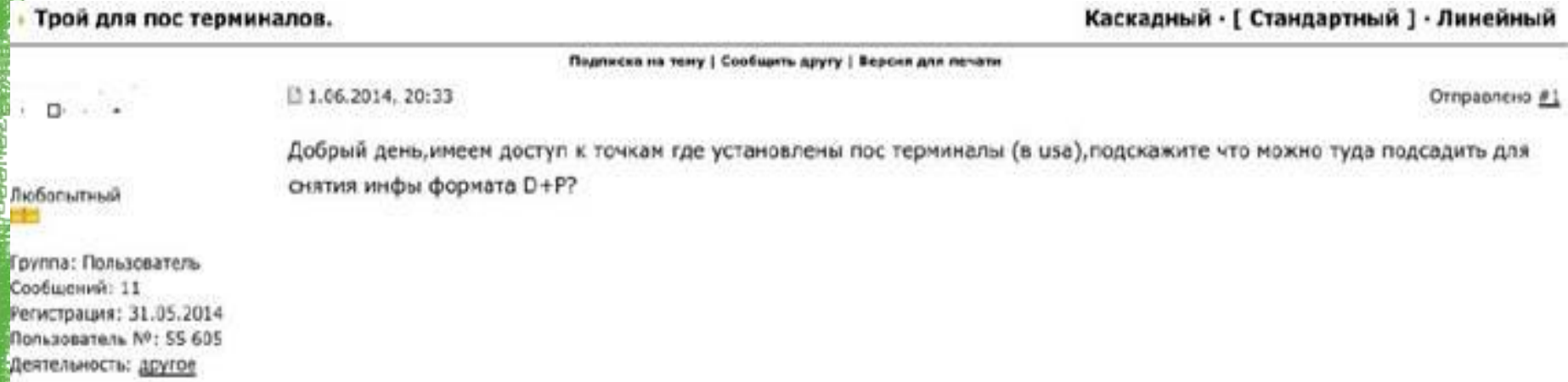
# Whitelist



# Correct Solutions

# Cyber Intelligence

# I have access to POS terminals in the US, what is the best malware I should use?



Трой для пос терминалов.

Каскадный · [ Стандартный ] · Линейный

Подписка на тему | Сообщить другу | Версия для печати

1.06.2014, 20:33

Отправлено #1

Добрый день,имеем доступ к точкам где установлены пос терминалы (в usa),подскажите что можно туда подсадить для снятия инфы формата D+P?

Любопытный

Группа: Пользователь
Сообщений: 11
Регистрация: 31.05.2014
Пользователь №: 55 605
Деятельность: другое

1.06.2014, 20:43 Отправлено #2

BlackPOS?

ПРОФИЛЬ ЛМ ЖАЛОБА ВВЕРХ +ЦИТАТА ОТВЕТ

1.06.2014, 21:16 Отправлено #3

Your best looking for this soft from carding communitys. Alina is best costs 5k but i think the seller's jabber was hacked.

ПРОФИЛЬ ЛМ ЖАЛОБА ВВЕРХ +ЦИТАТА ОТВЕТ

1.06.2014, 22:11 Отправлено #3

polyk прав, пос надо шить , чтоб можно было собирать д+п, если малварь пихать удаленно, то конеш можно словить будет трек1 трек 2, но пин будет идти в виде хэша, в большинстве случаев.А так, в падлике дохрена софта, помимо лек поса лежит , ищи лучше

---

Firefox нас нае%ал))] (c)

K♥K♦K♣K♠

Группа: Пользователь

You need to infect the firmware of the terminal.
By doing that, you can get full track 1 + 2,
but the PIN will be hashed.

# Selling malicious firmware for Verifone's POS terminals. Leaks dumps + PINs through GPRS. Price: Only 700$

[Продам] Прошивка Verifone VX5xx, VX6xx

Каскадный · [ Стандартный ] · Линейный

Подписка на тему | Сообщить другу | Версия для печати

28.05.2014, 15:19

Отправлено #1

Под этим сообщением задрот-индикатор.

Группа: Пользователь
Сообщений: 135
Регистрация: 12.08.2008
Пользователь №: 12 966
Деятельность: другое

Продам прошивку под Verifone POS VX5** , VX6** .

Особенности:

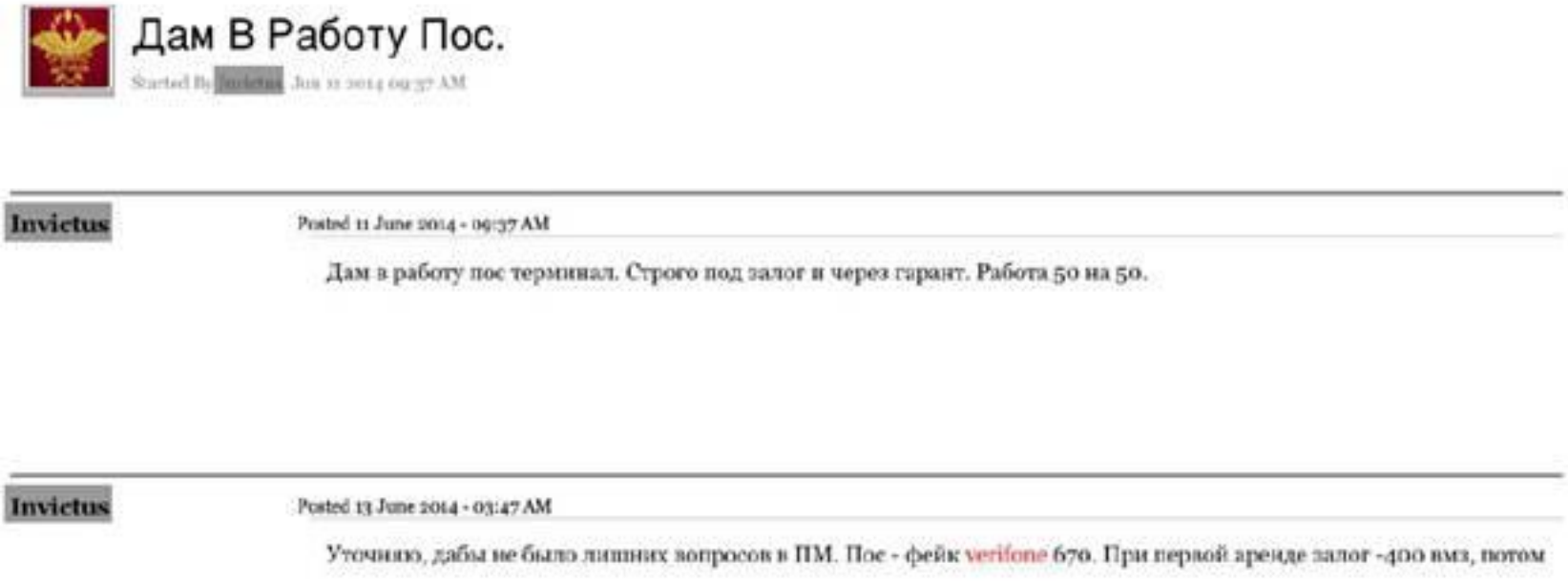
- 4 языка
- Возможность настройки чека
- Ответы: транзакция успешна \ транзакция деклайн
- Сохранение дампов с пинами в памяти \ передача по гпрс (передача по гпрс не тестилась)

Отдам за 700$, гарант.

Контакты в ПМ. Мозготраки сразу в игнор. Нерусскоязычным - двойная цена.

# Business Development Offer

## Owner of a fake POS sells his terminal.
## Price: 50% from revenue sharing.



Дам В Работу Пос.

Started By [redacted] Jun 11 2014 09:37 AM

**Invictus** Posted 11 June 2014 - 09:37 AM

Дам в работу пос терминал. Строго под залог и через гарант. Работа 50 на 50.

**Invictus** Posted 13 June 2014 - 03:47 AM

Уточняю, дабы не было лишних вопросов в ПМ. Пос - фейк verifone 670. При первой аренде залог -400 вмз, потом

# RFI: Change terminal configuration to require PIN for all cards.
# Cause: Get only 101 data, but wants PINs

Member

**Помогите по посу**

Возможно ли настроить **пос** ingenico на 100 % запрос пинкода? Стоит в достаточно тяжелом месте, приходятся работать с онлайном и проблема при съеме 101, пин он не запрашивает. Косяк второй, место прибыльное и в то же время дико неудобное, накладку на клаву тяжко ставить, что можно придумать по выдергиванию пина?
Кто что может сказать на счет инфракрасного тепловизора, по нему с помощью остатков тепла после нажатия на кнопки возможно определить нажатые клавиши и последсвательность набора. Дабы не сбиваться после каждого ввода, можно протирать клаву влажной салфеткой. Рассматриваю варианты спосов.
У кого какие оригинальные мысли? Так же стукните ко мне с накладками на инженико. Благодарствую.

## Proposed Solution:
## Thermal Imager


Sandbox

# Network-based Anomaly Detection

# Operating System Anomaly Detection

# Runtime Obfuscation

# Not only products required !

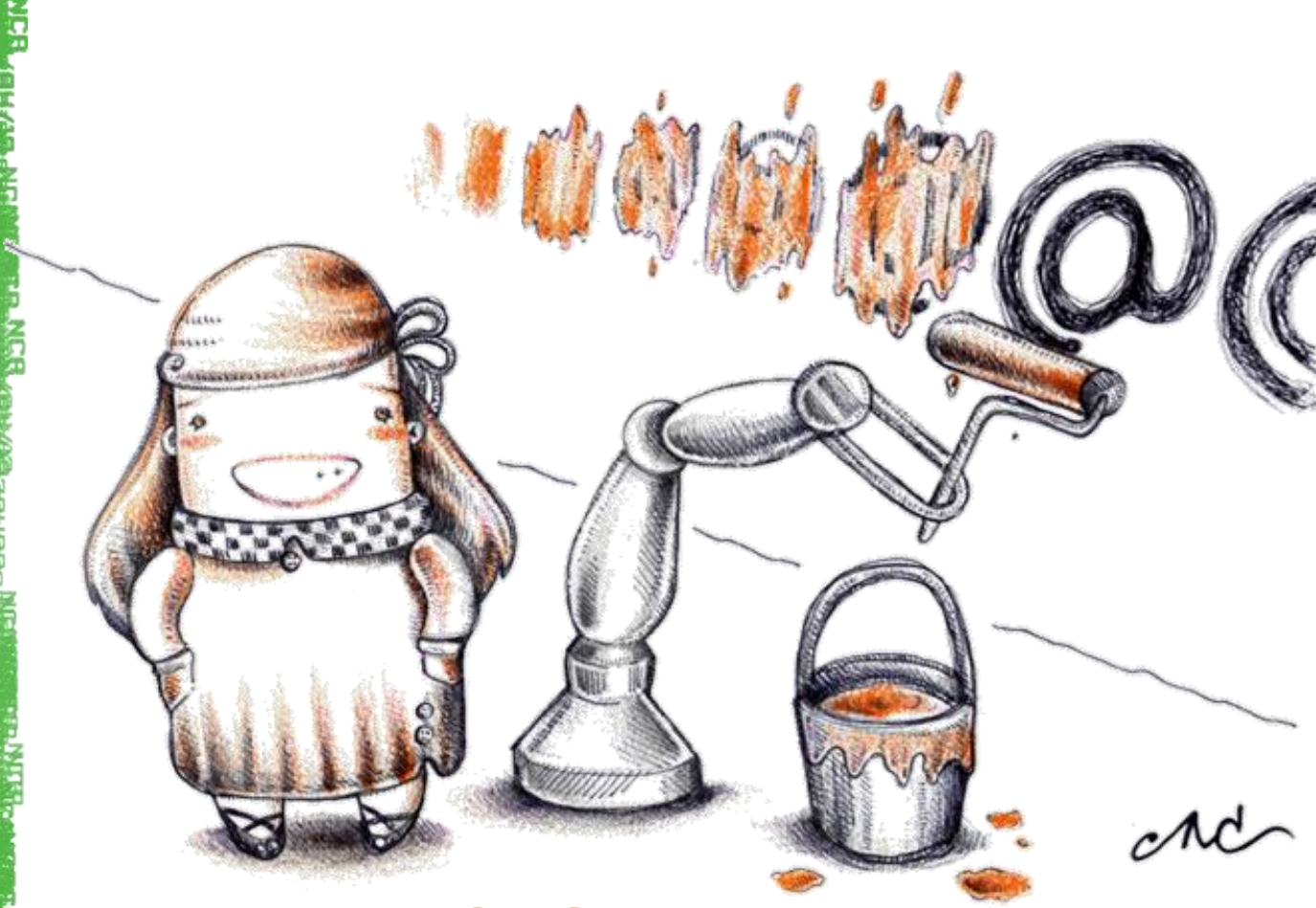
# Security Architecture

# Security Architecture

# Security Architecture

Assembly Signing

Security Architecture



# Assembly Obfuscation

# PROCESS ISOLATION

# What Next ?

# What Would You Steal?



Memory
Scraping


Cashier = hacker


ATMEL

# Summary

# Security by Obscurity

# Simple Exploitation

# Hard to Protect


# You’re Insured

# Thank You

**Nir Valtman**
w : www.valtman.org
: @ValtmaNir