A Journey To Protect Points Of Sale

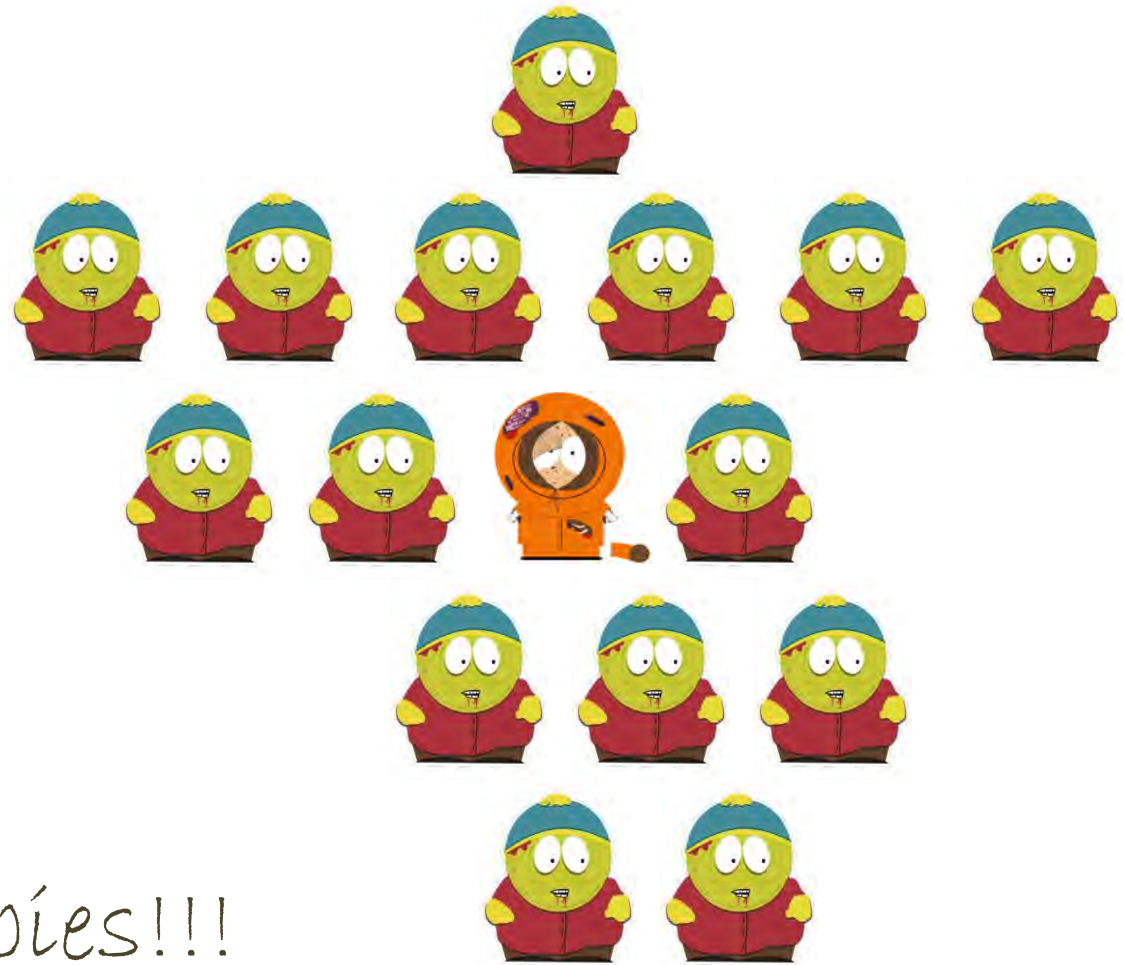
Nir Valtman, CISSP
w : www.valtman.org
: @ValtmaNir

Introduction

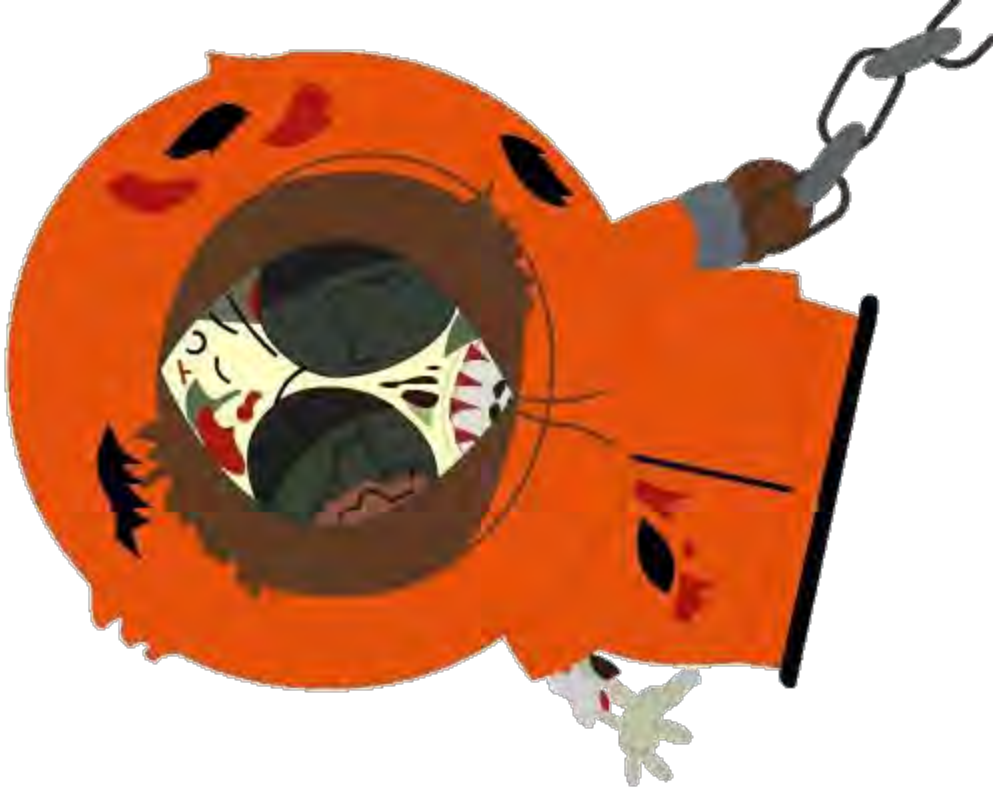
Photo by Bill Fraser


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

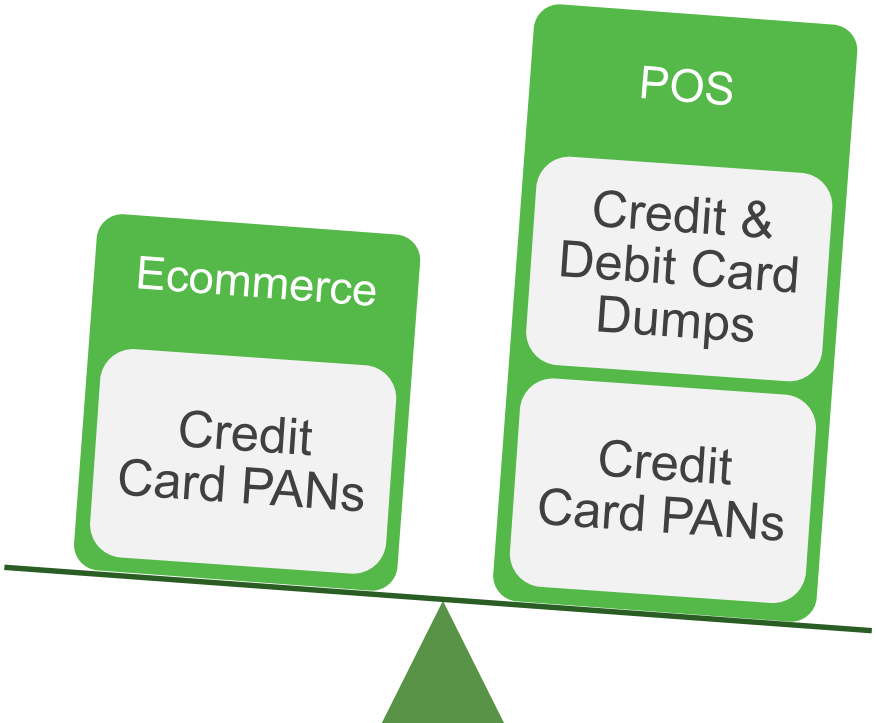
5 Full info CC USA – $40 /

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)

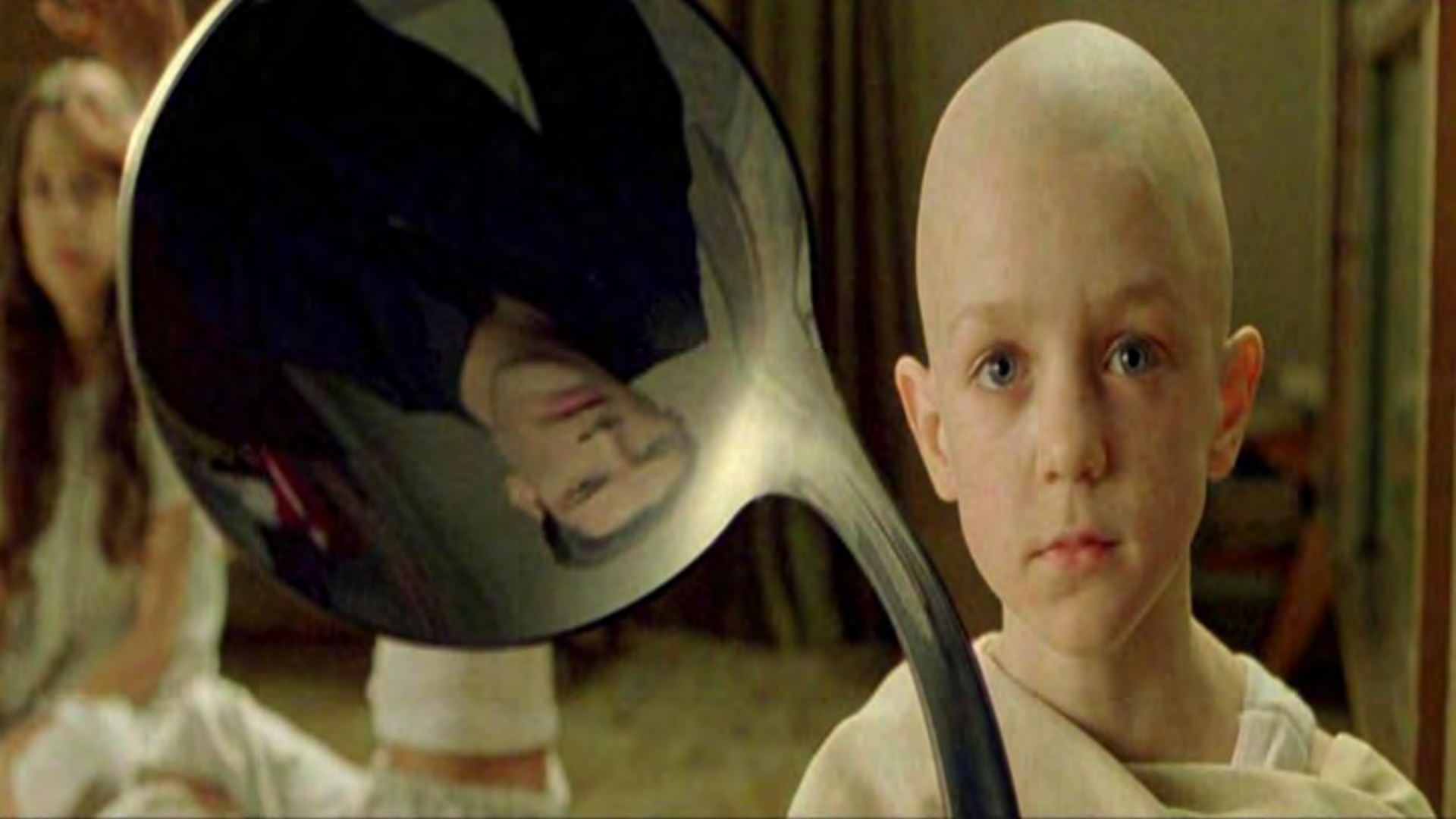
BUY (no javascript)

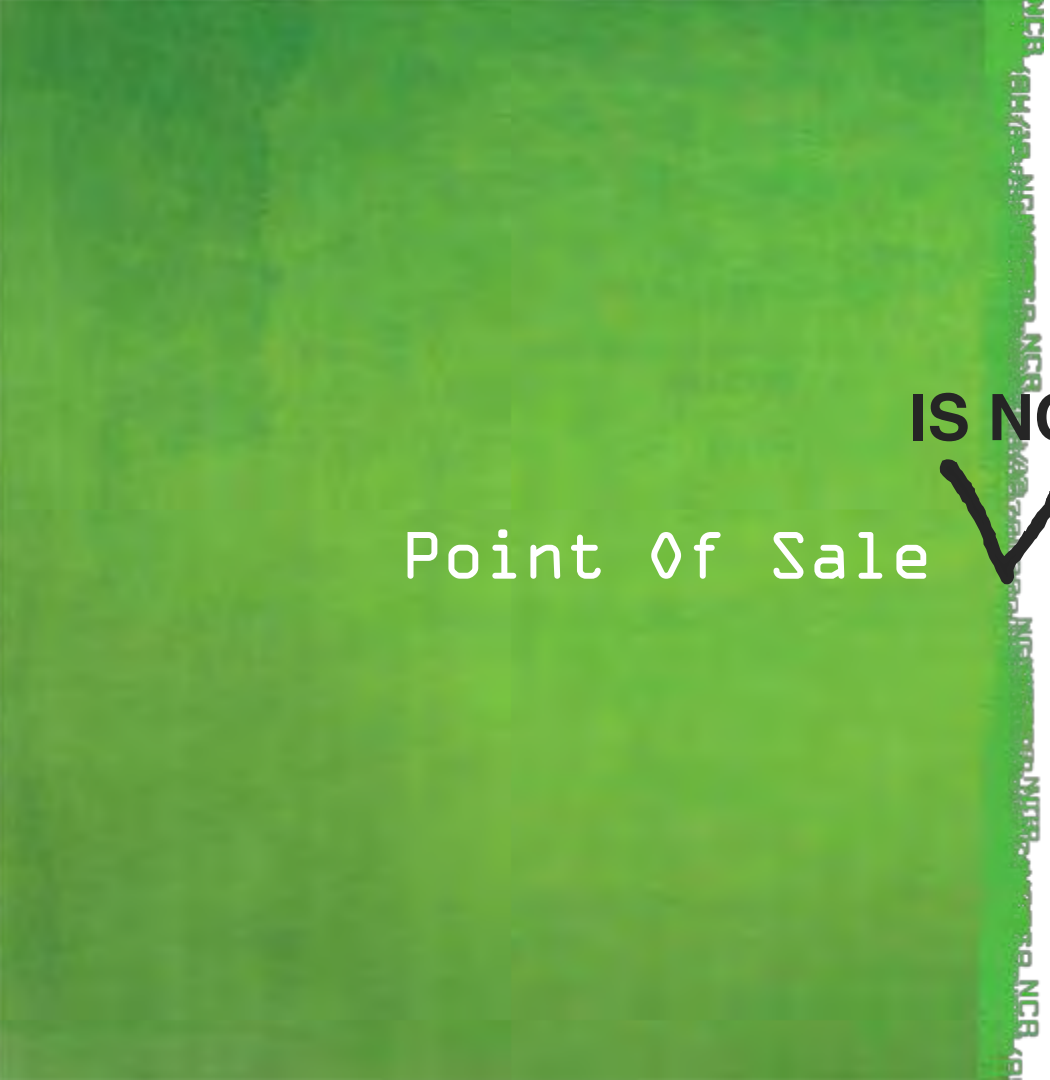

Ecommerce
Credit Card PANs
POS
Credit & Debit Card Dumps
Credit Card PANs

Deployment


RealPOS

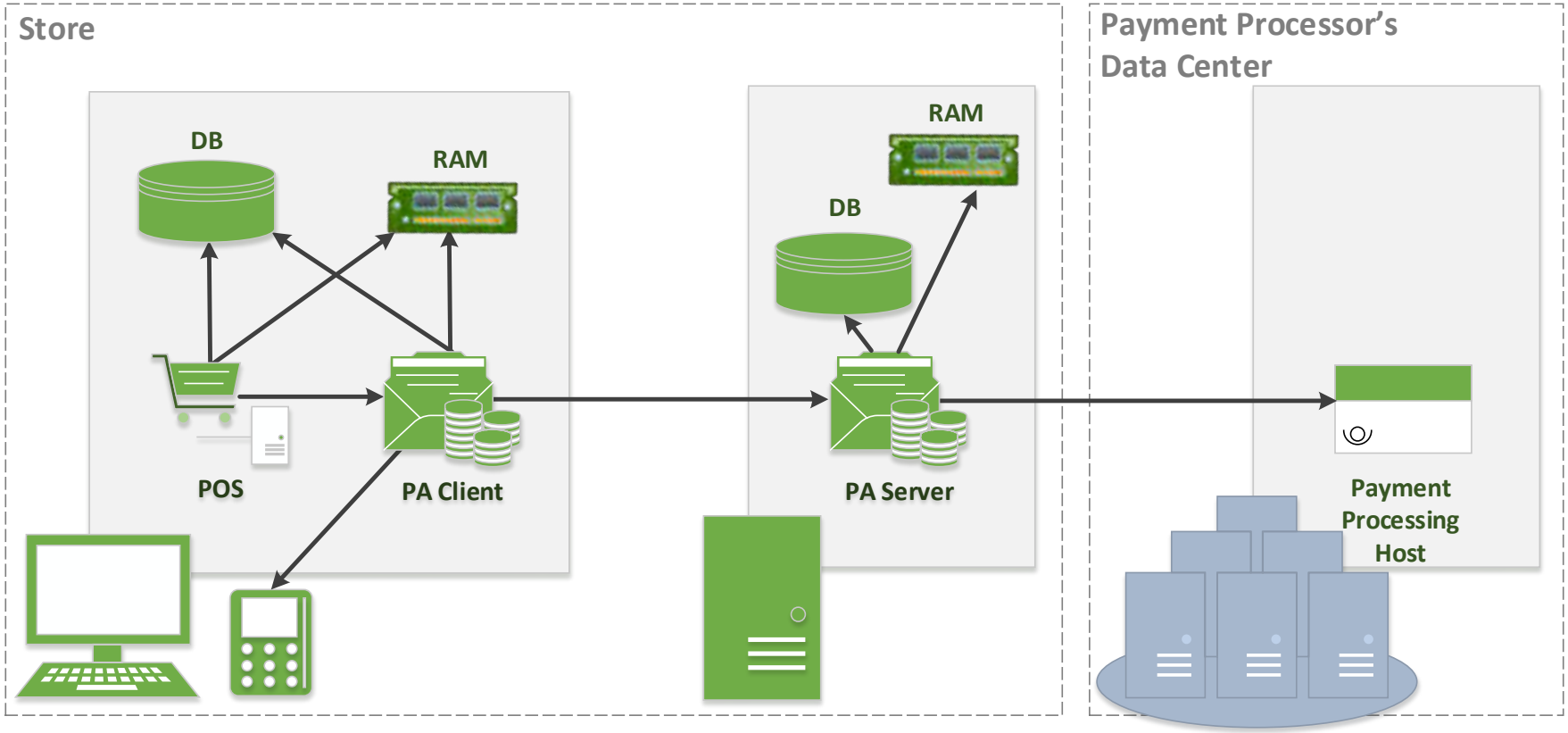

8:13 AM
connected
vantiv
Mobile Checkout
Payment types
Back to Items
CASH
Cash
CHECK
Check
CREDIT
Credit Card
Gift
Non-integrated Gift...
PrePaid
PrePaid Coupons
Ticket
1
Goodnight Moon
Goodnight Moon
$5.99
1
The Great Gatsby
The Great Gatsby Hardcover
$15.64
1
Betty Crckr Cookbook
Betty Crocker Cookbook
$17.99
Lookup Item
$39.62
$3.19
Subtotal
Tax
Balance Due:
$42.81
Checkout
Hold
Void ticket
Ticket discount
Change tax
CARD
HAMLET
OTHELLO





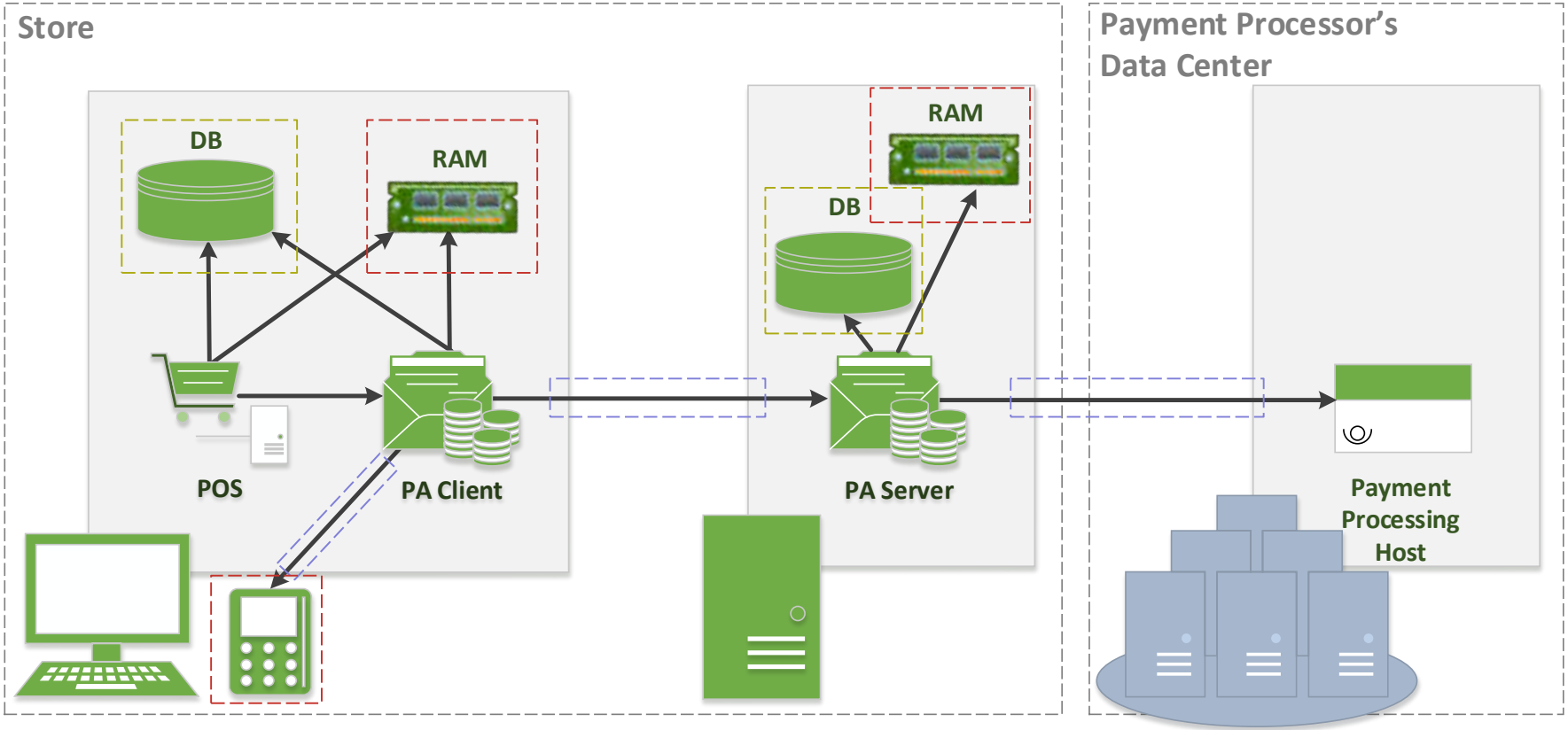
IS NOT

Point Of Sale V Payment Application


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

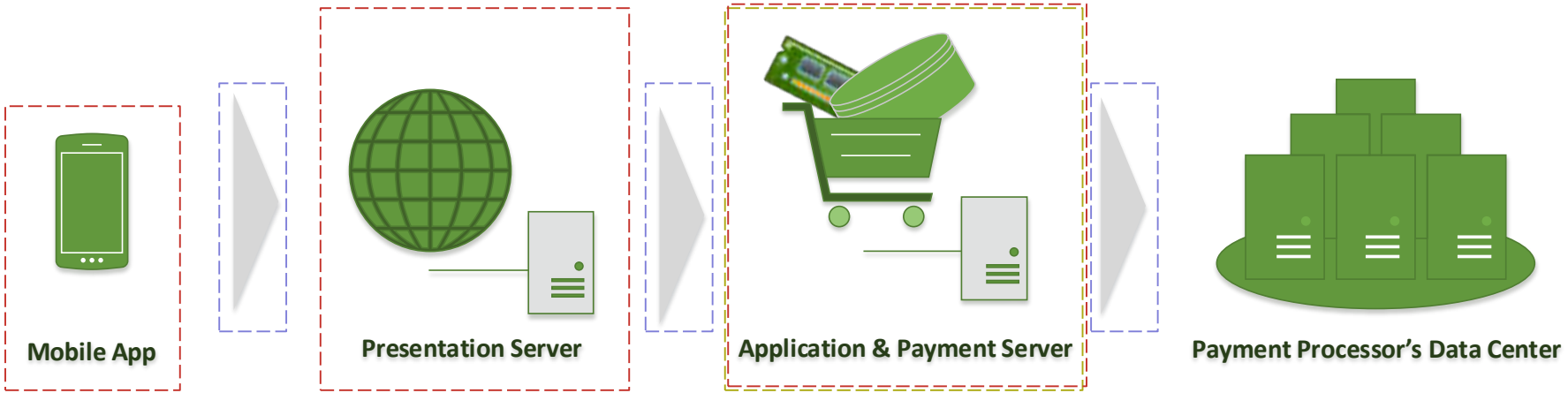
Where Are My Credit Cards?

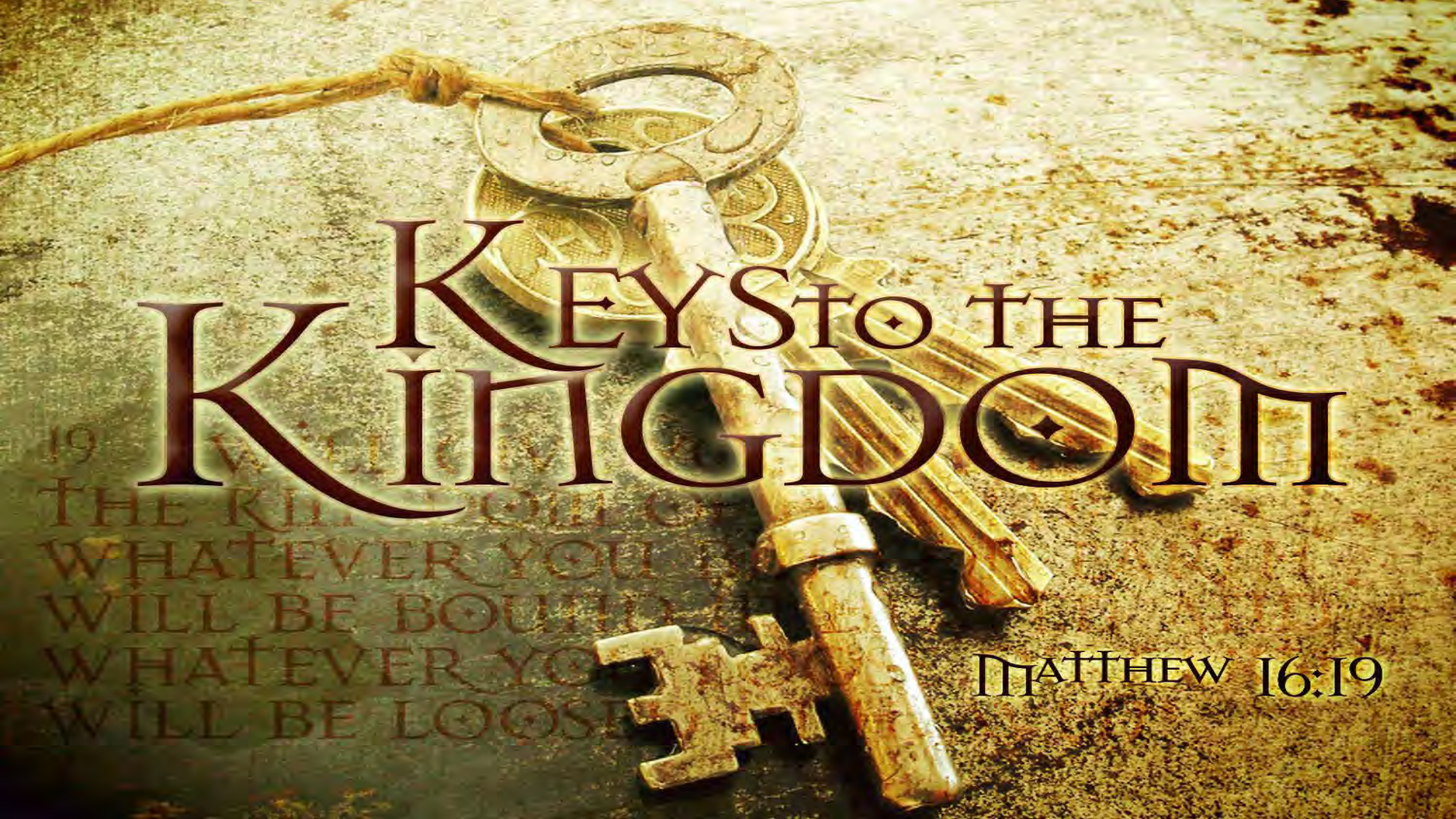
Rest | Transit | Memory

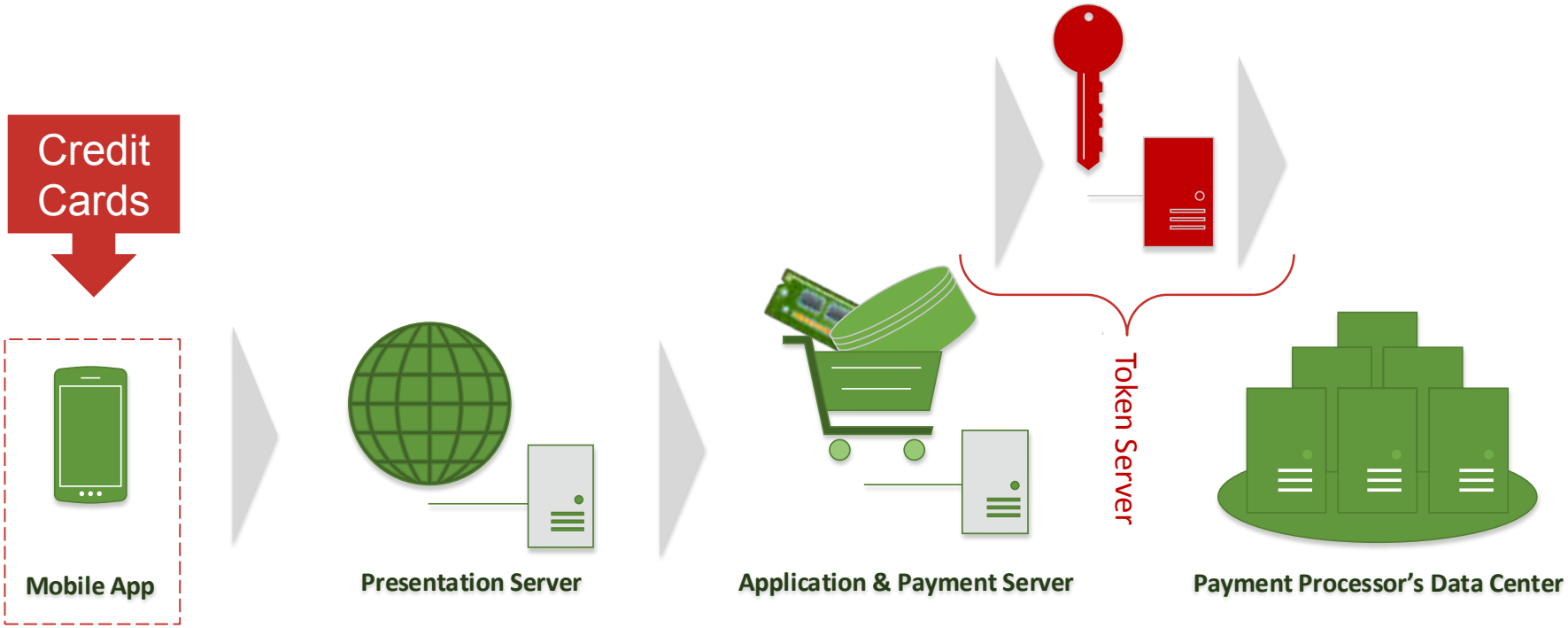


Where Are My Credit Cards?

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

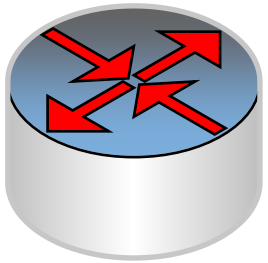
RATs

Achilles

Tendon

Remote Administration Tools

Achilles Tendon



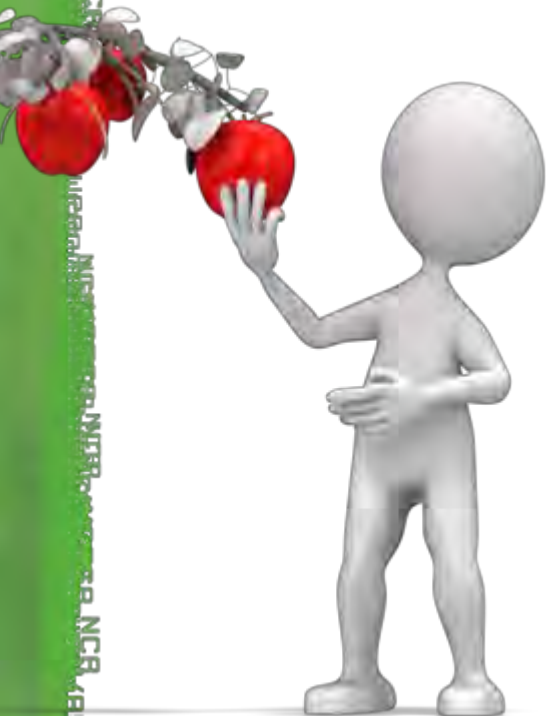
Routing

Achilles

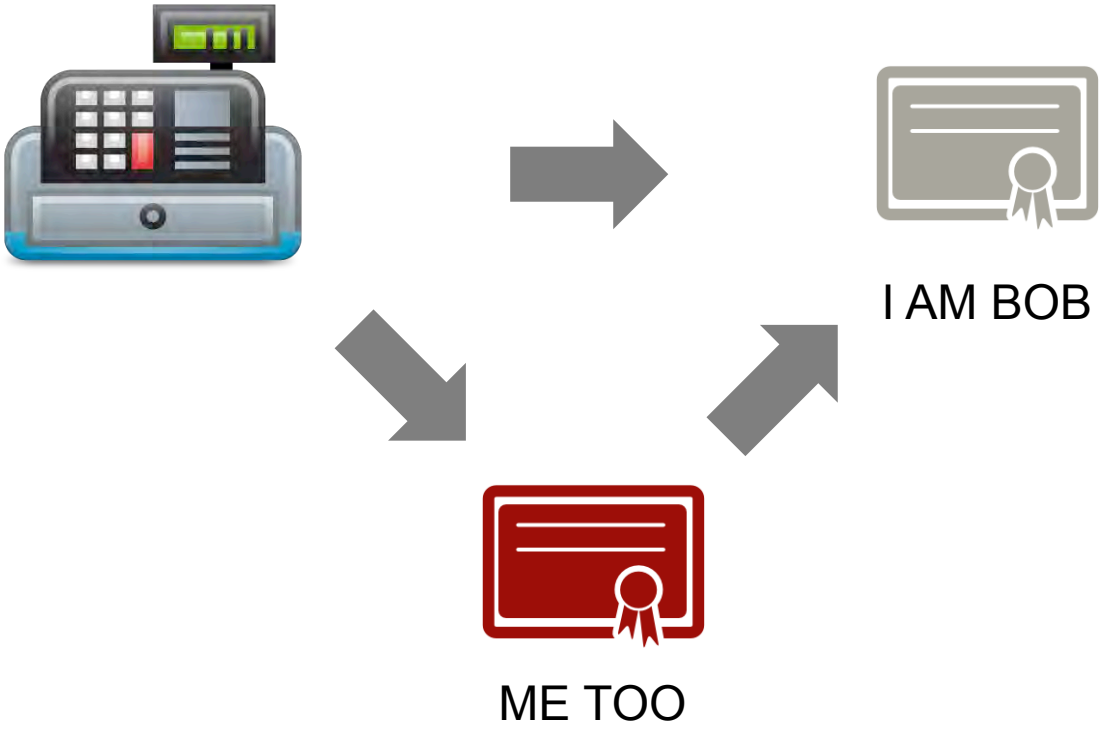
Tendon

Achilles Tendon

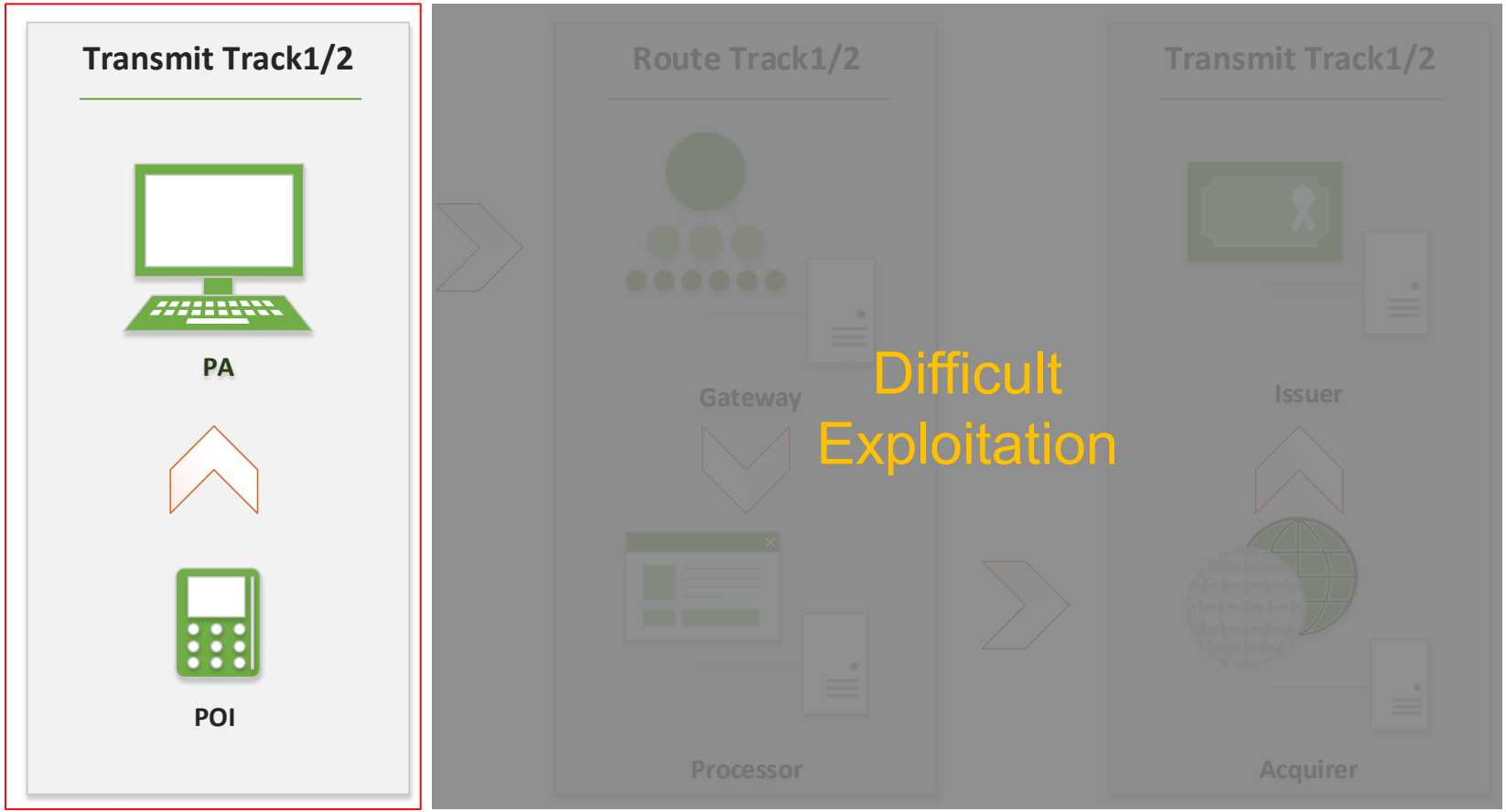
Threats



READ&WRITE

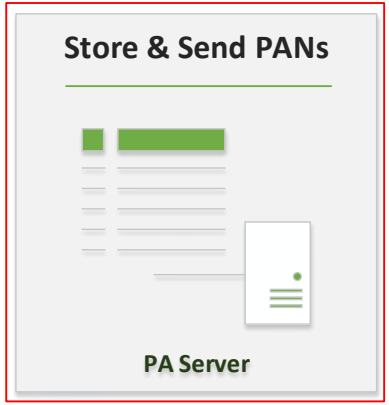

I AM BOB
ME TOO

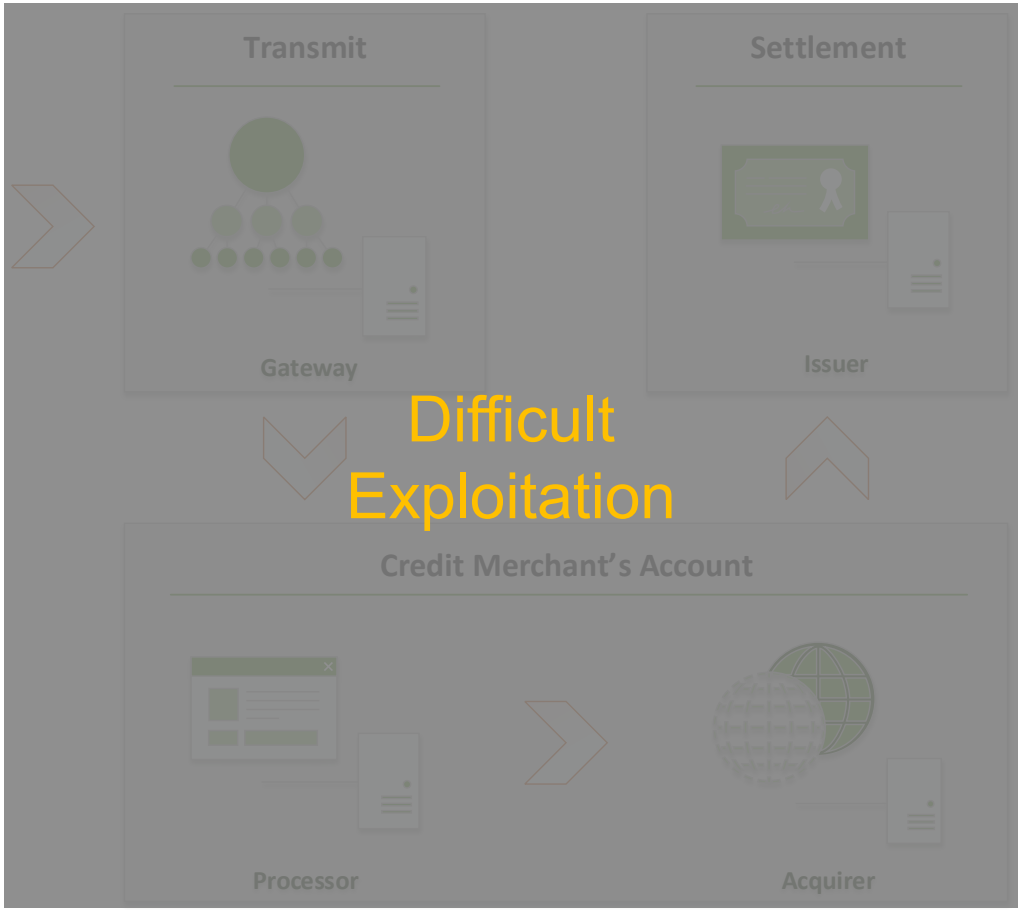
Payment Stages - Authorization



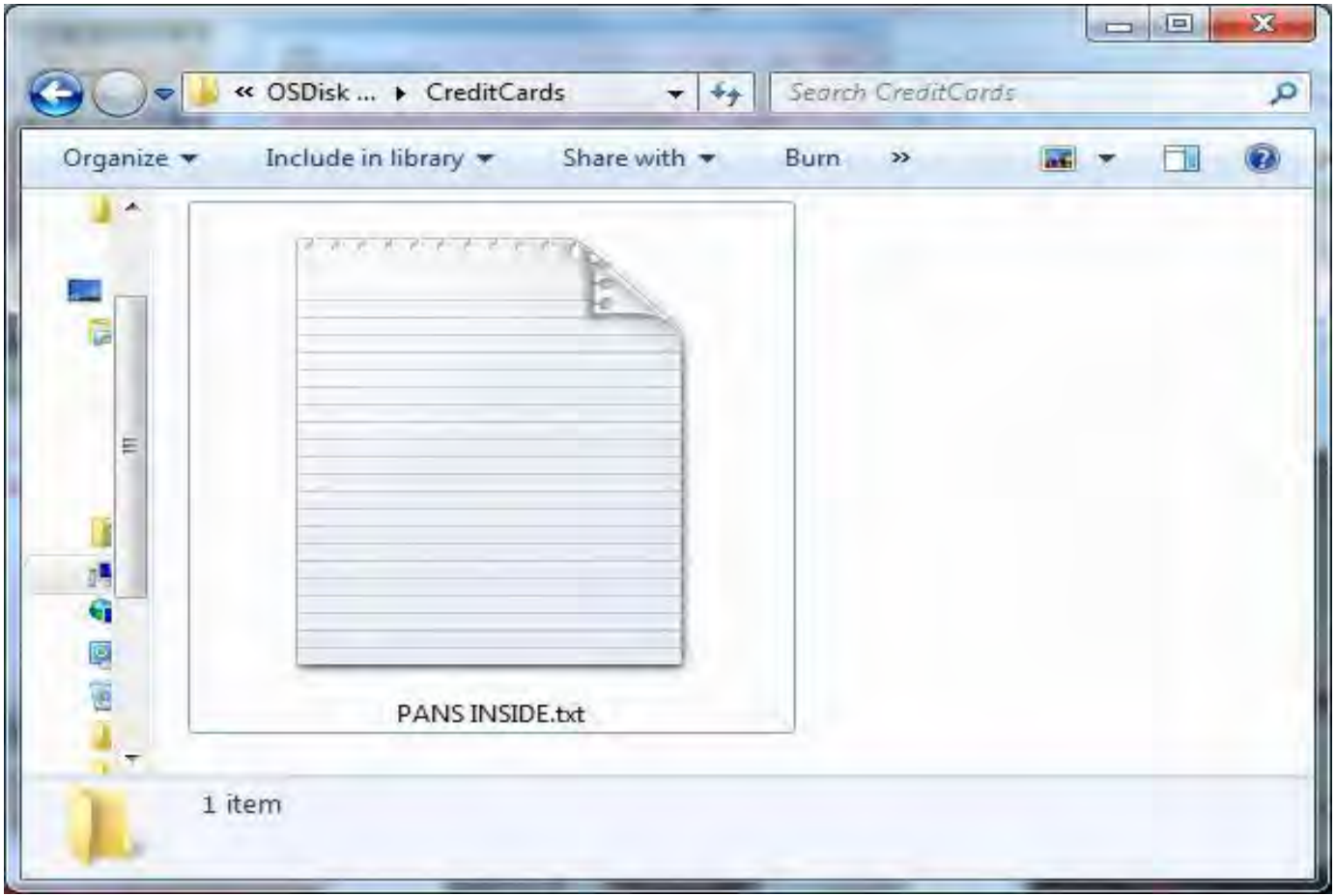
Payment Stages - Authorization

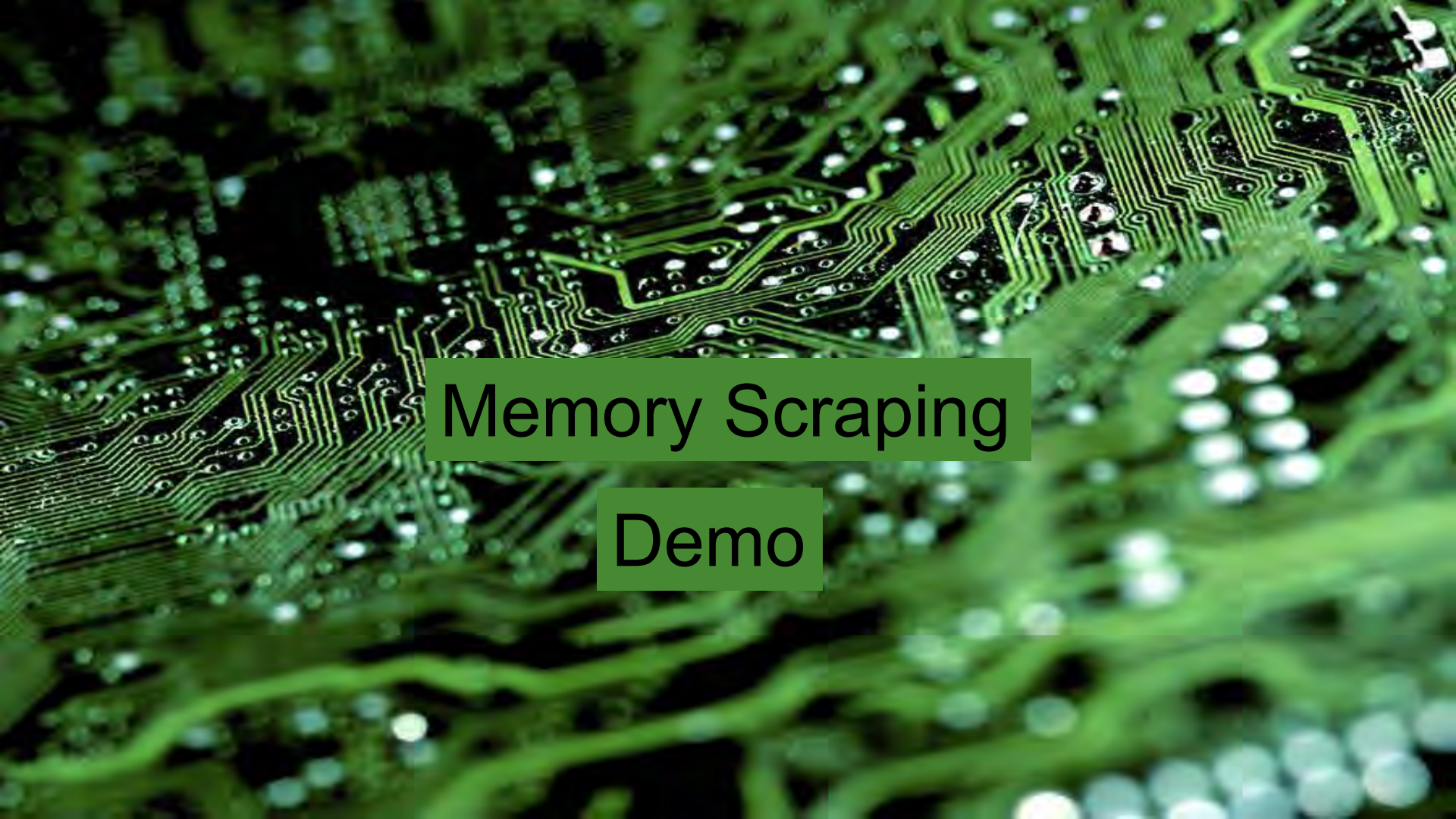
Payment Stages - Settlement





Payment Stages - Settlement




Memory Scraping
Demo


Login
Login


PRIVACY


FBD


Online
VS
Offline

Bypassed Solutions

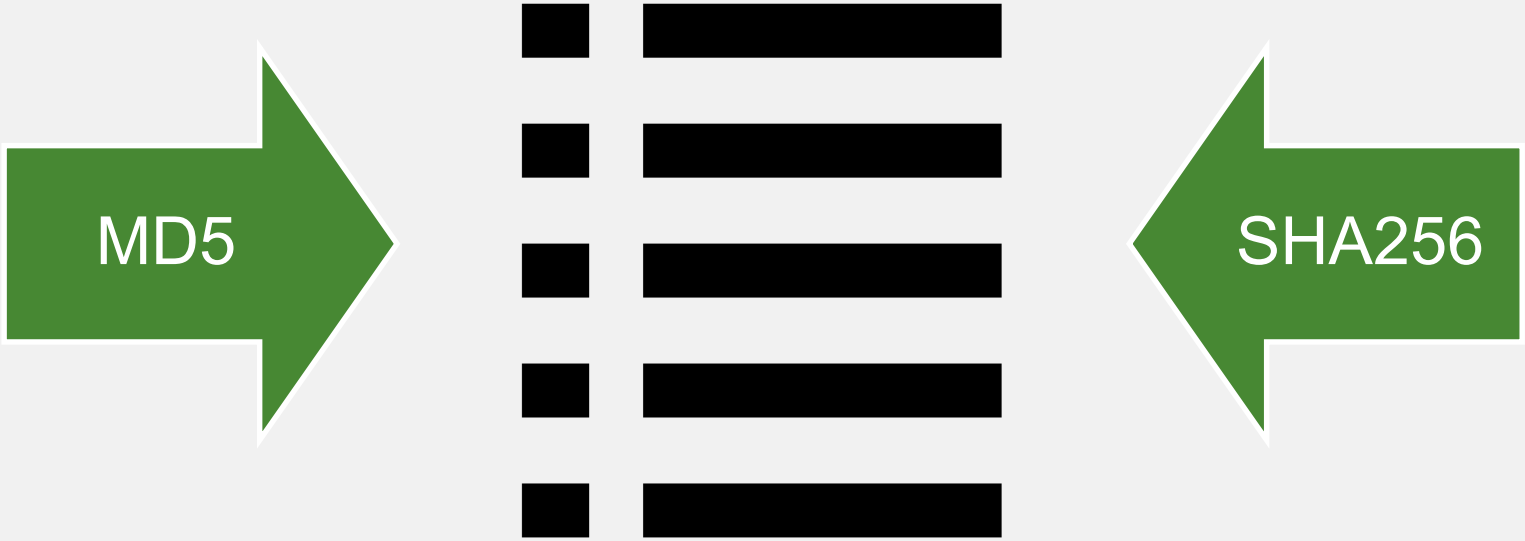

SecureString Class
Demo

Next Next Next Generation Firewall

ANTI *


Data loss

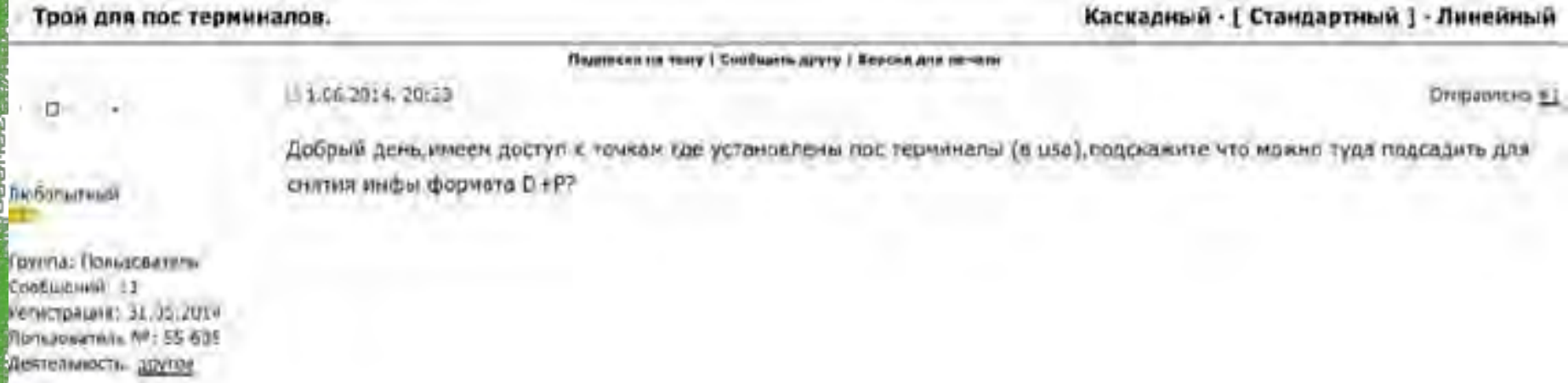
Whitelist



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

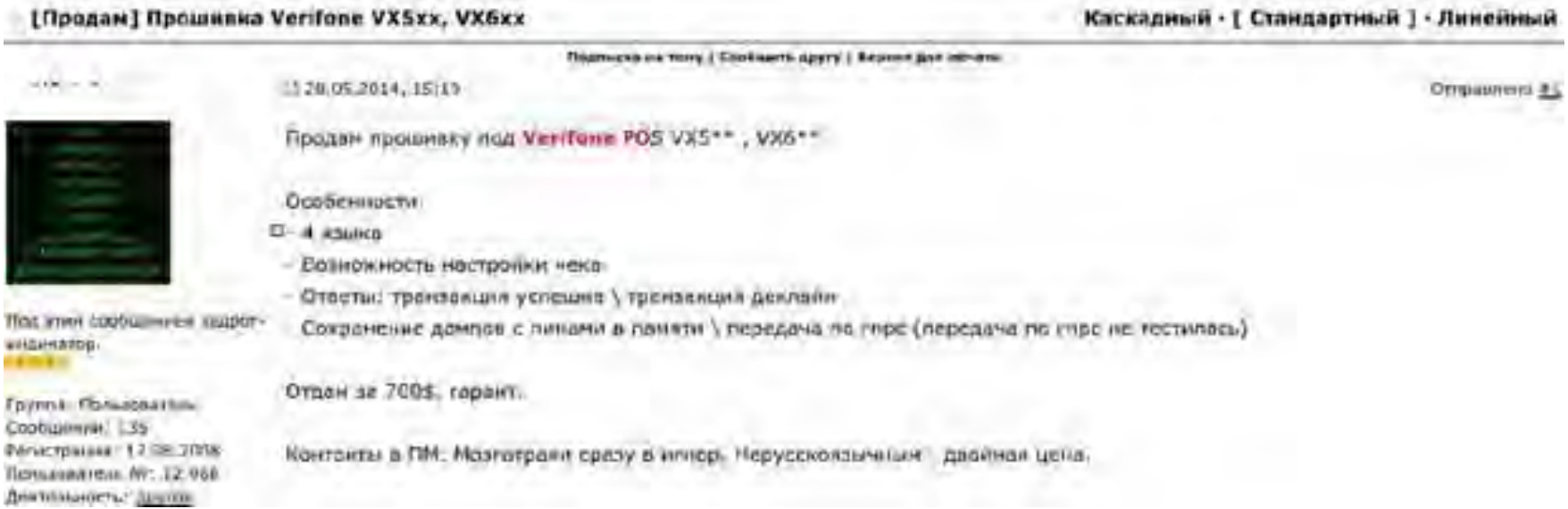
Добрый день,имеем доступ к точкам где установлены пос терминалы (в usa),подскажите что можно туда подсадить для снятия инфы формата D+P?

любопытный

Группа: Пользователь
Сообщений: 13
Регистрация: 31.05.2014
Пользователь №: 55 609
Деятельность: другое

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

28.05.2014, 15:19

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 gprs (передача по gprs не тестилась)

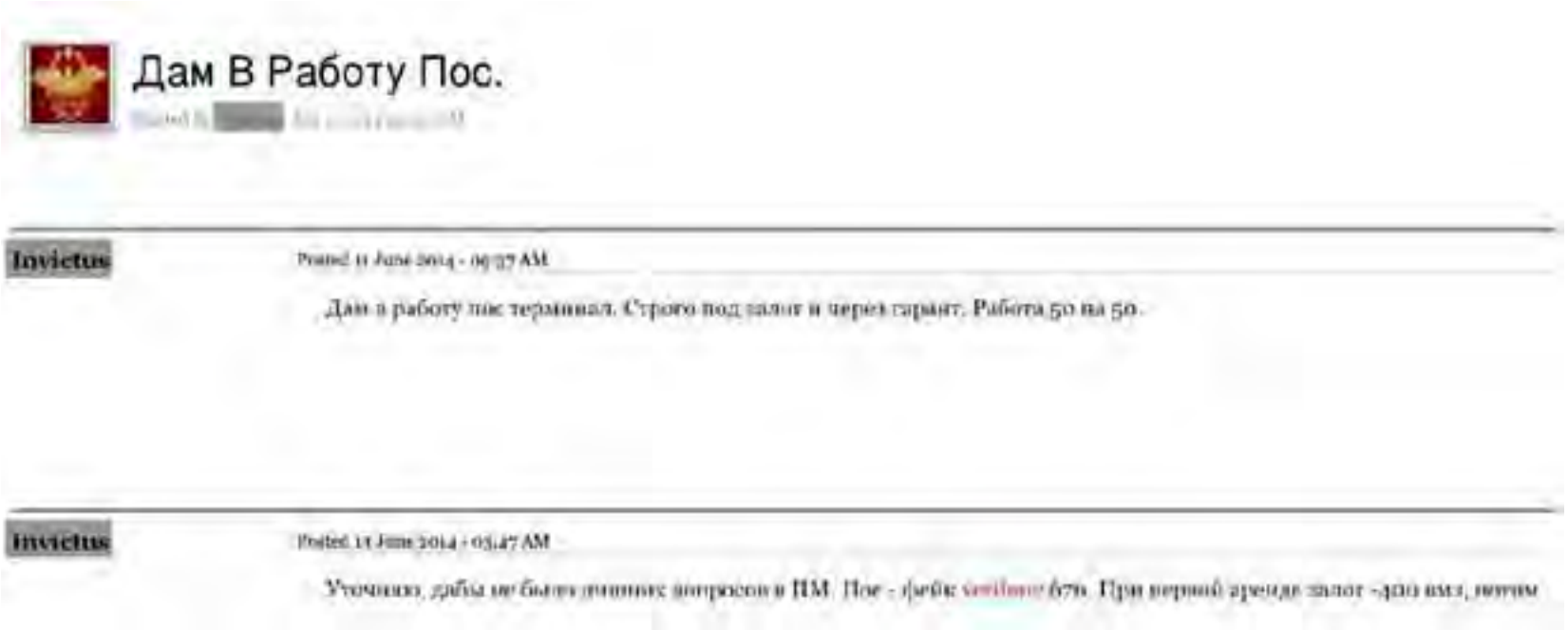
Отдам за 700$, гарант.

Контакты в ПМ. Мозготрахи сразу в минус. Нерусскоязычным двойная цена.

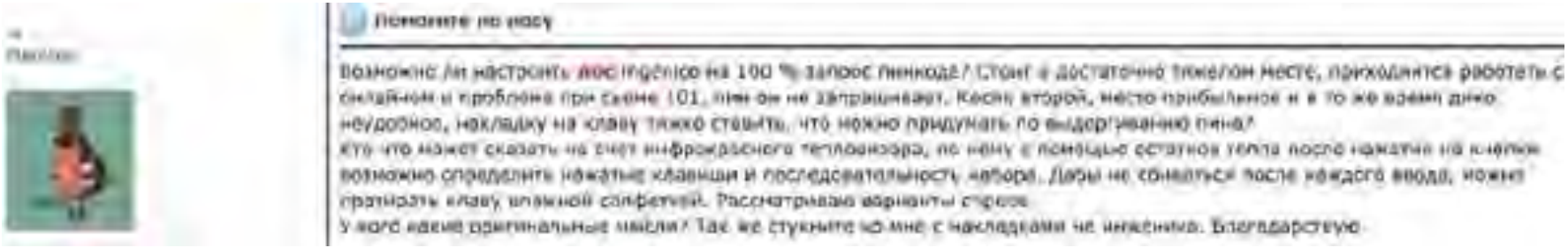
Business Development Offer

Owner of a fake POS sells his terminal.

Price: 50% from revenue sharing.



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



Proposed Solution:
Thermal Imager


Sandbox

Network-based Anomaly Detection

Operating System Anomaly Detection

Runtime Obfuscation

Not only products required !

Security Architecture

Security Architecture

Assembly Signing

Assembly Obfuscation

PROCESS ISOLATION

What Next ?

What Would You Steal?


Memory
Scraping

Cashier = hacker

Summary

Security by Obscurity

Simple Exploitation

Hard to Protect

You’re Insured

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