

A Journey To Protect Points Of Sale

Nir Valtman, CISSP

W : www.valtman.org

Twitter : @ValtmaNir



Introduction



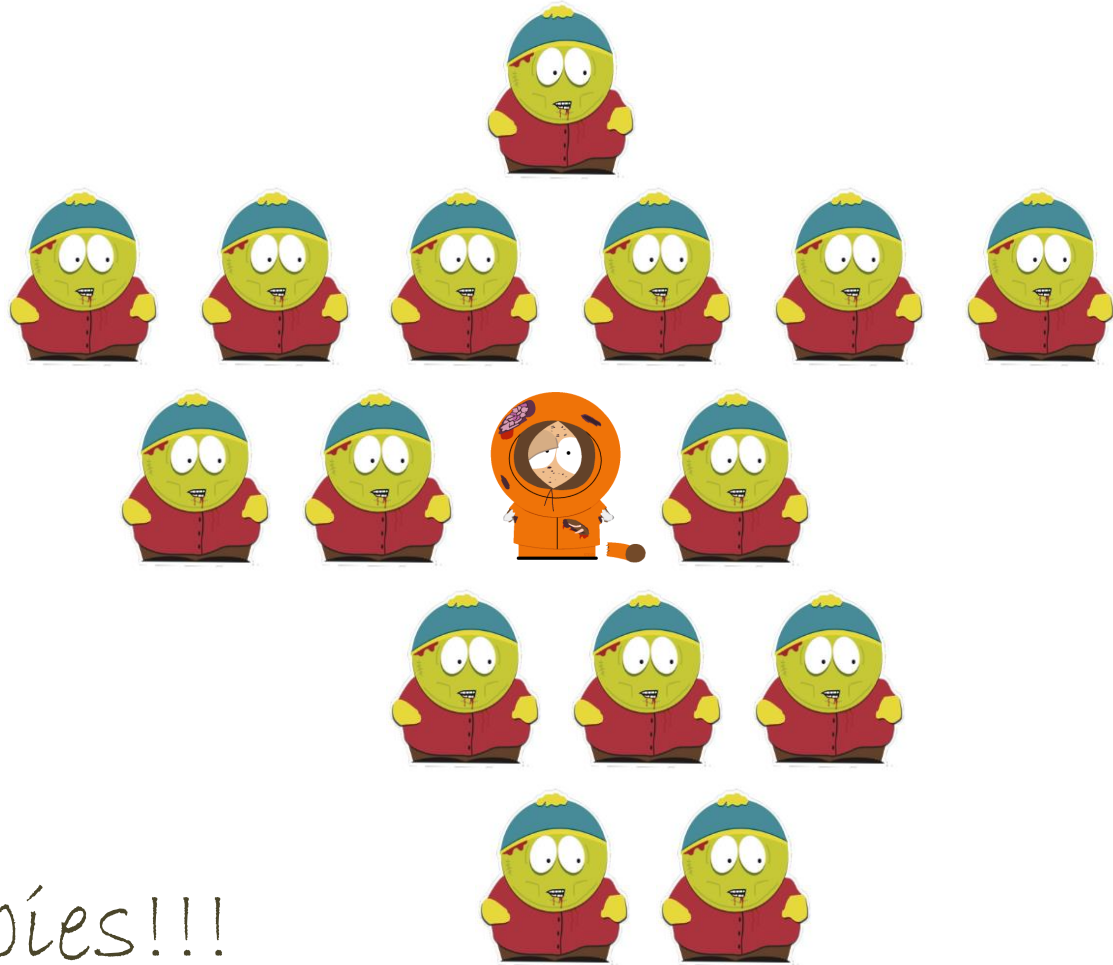


01/07/2014









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 |

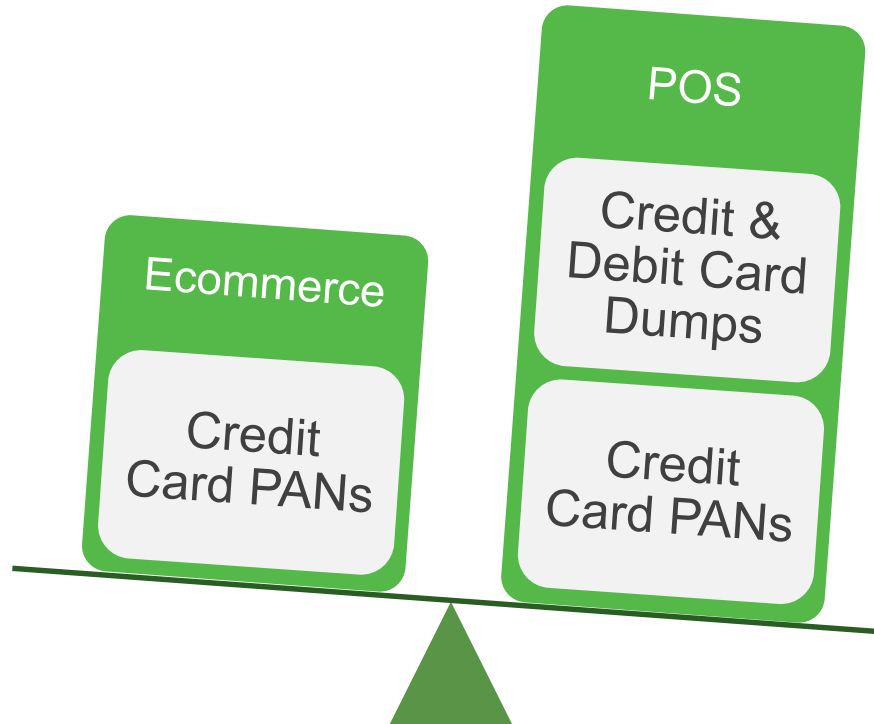
USA CC Fullz + tutorial

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

[BUY](#) (no javascript)

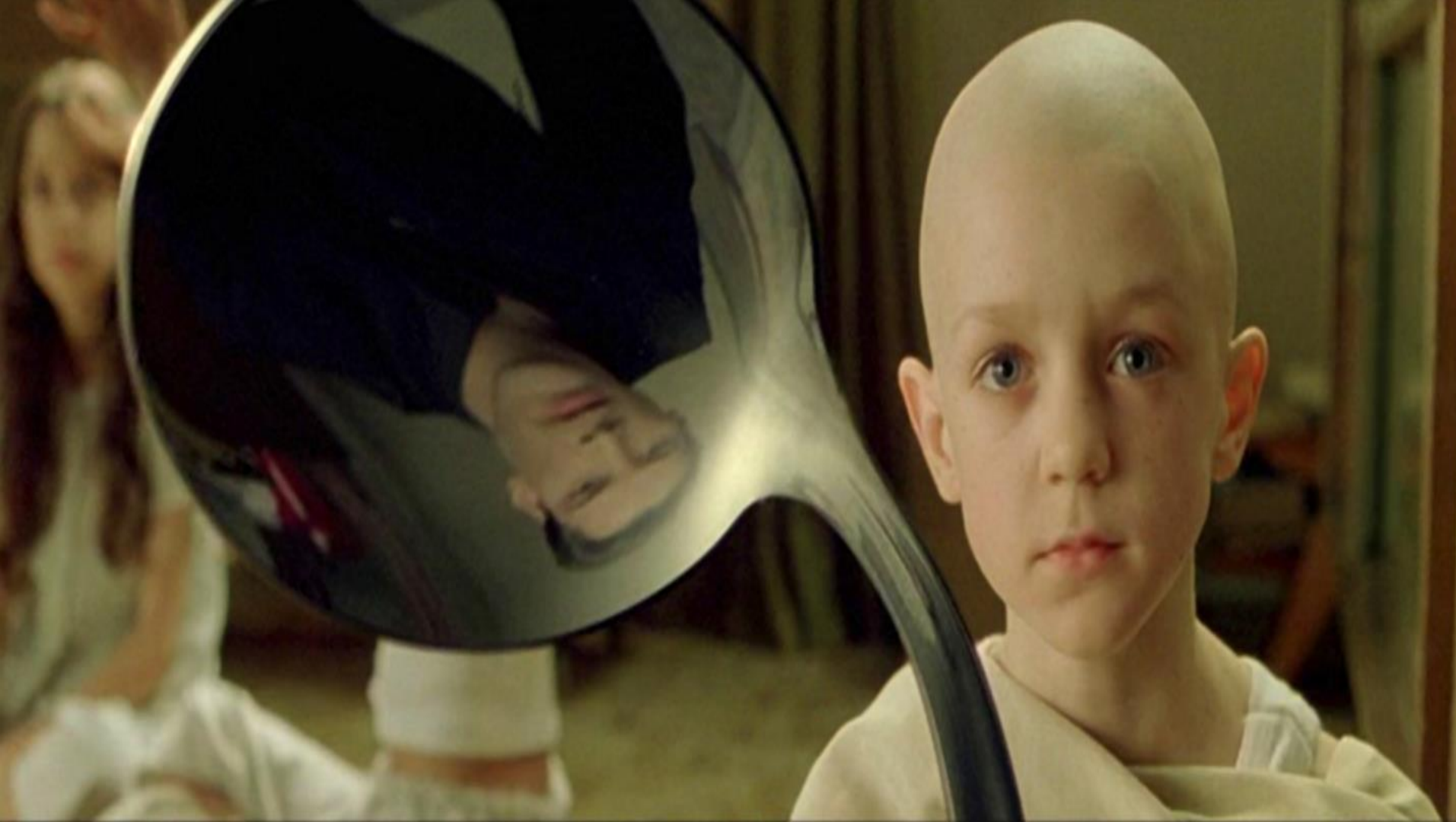


Deployment









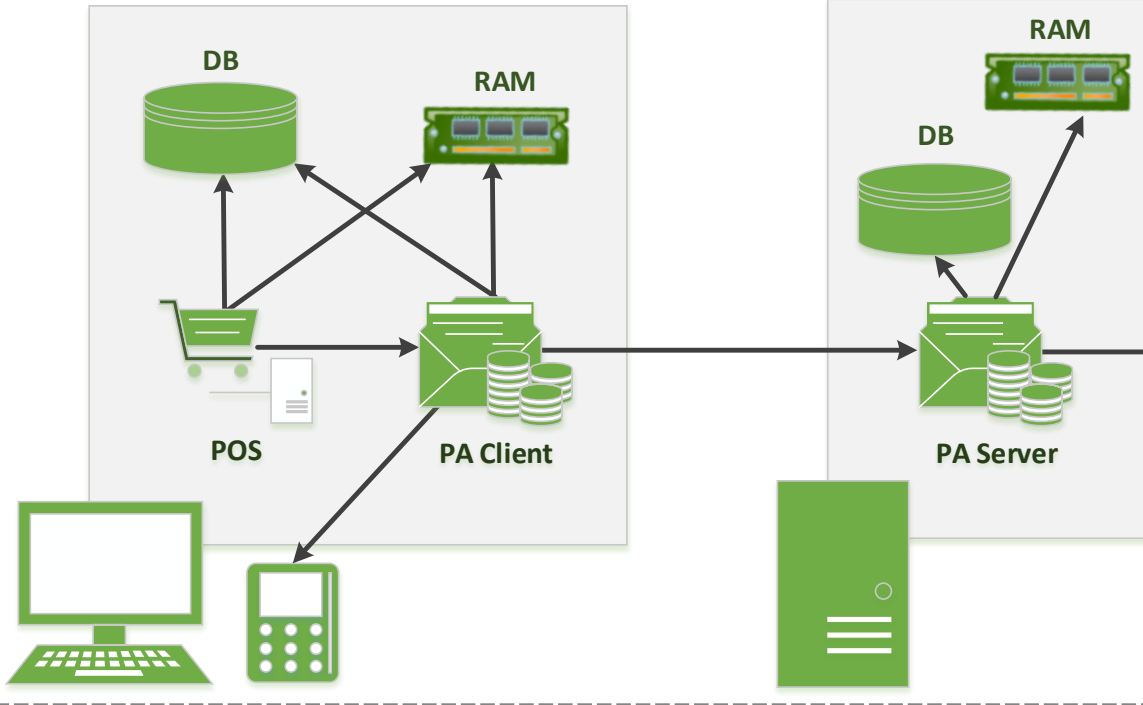
IS NOT

Point Of Sale

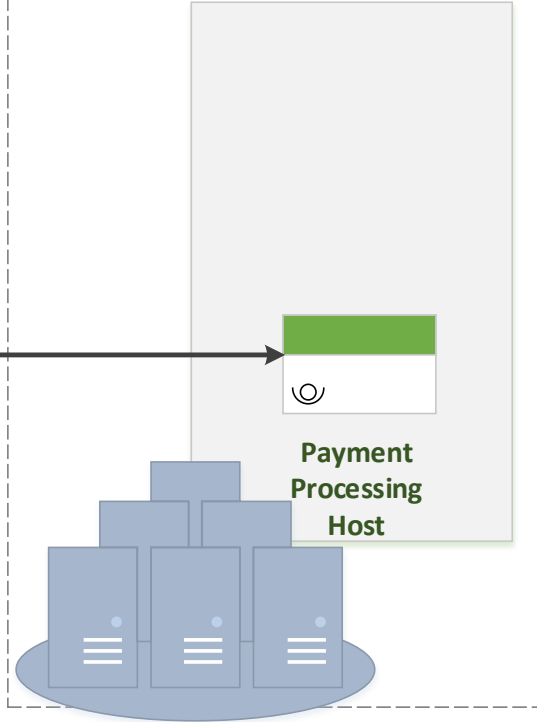


Payment Application

Store



Payment Processor's Data Center

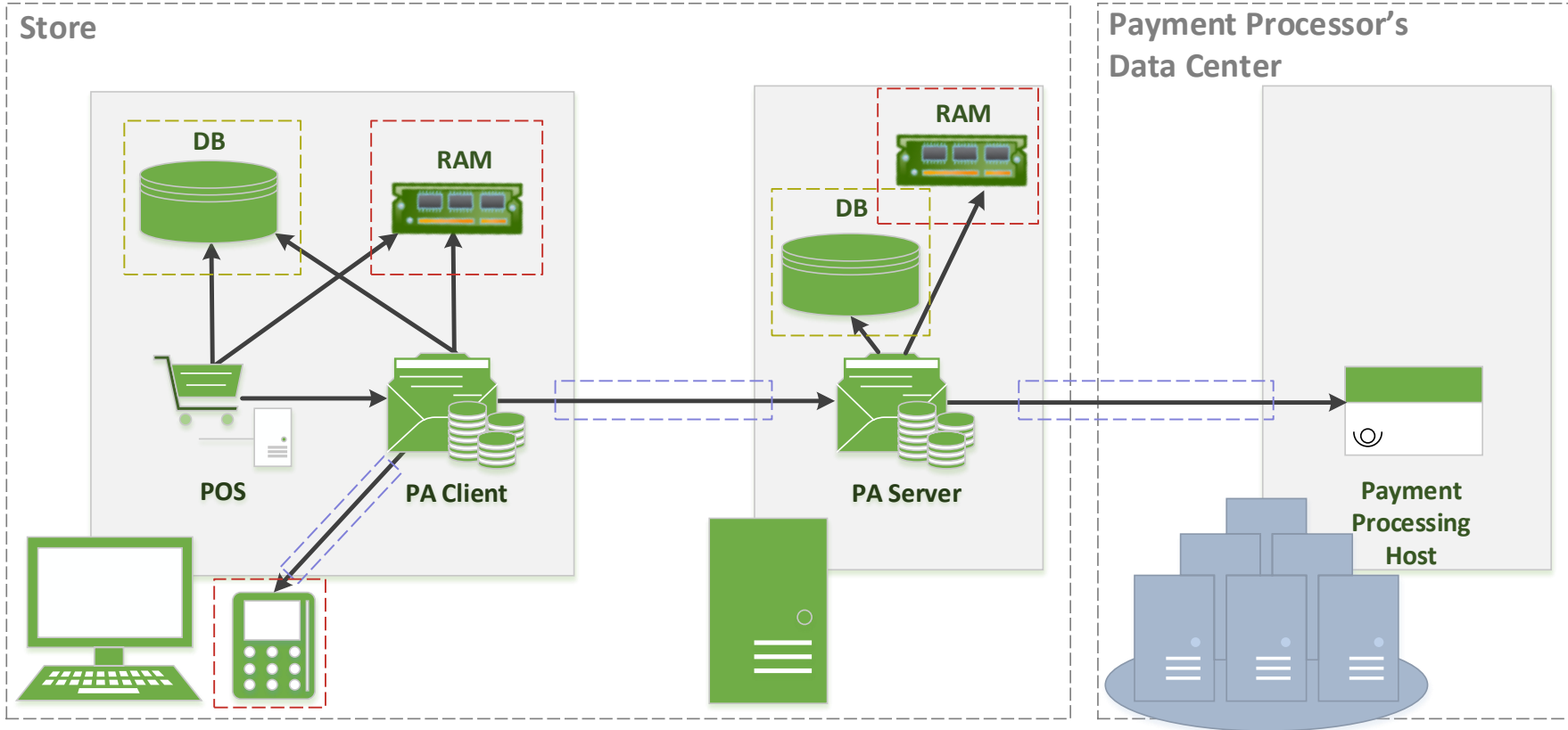


Where Are My Credit Cards?

Rest

Transit

Memory

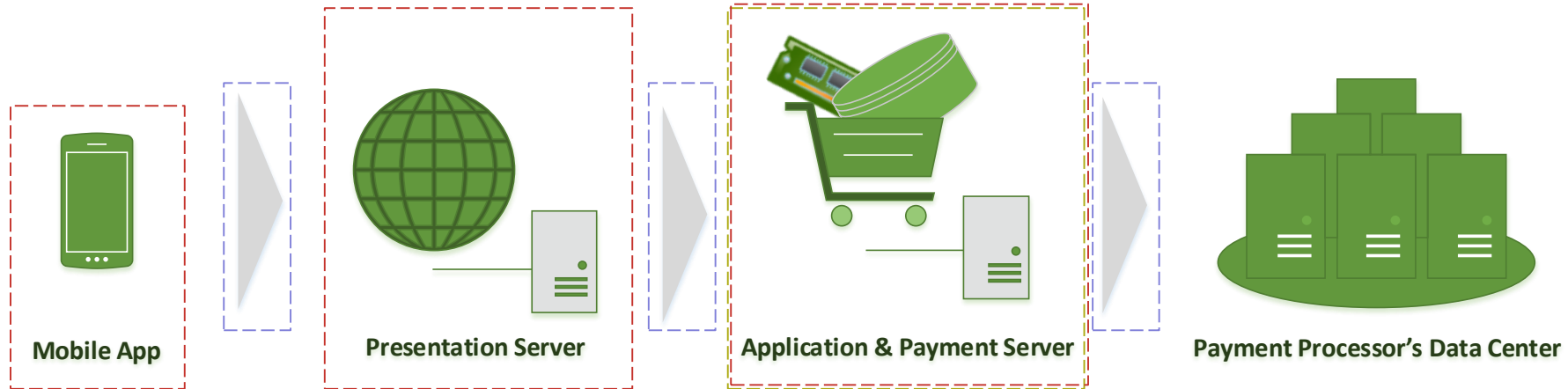


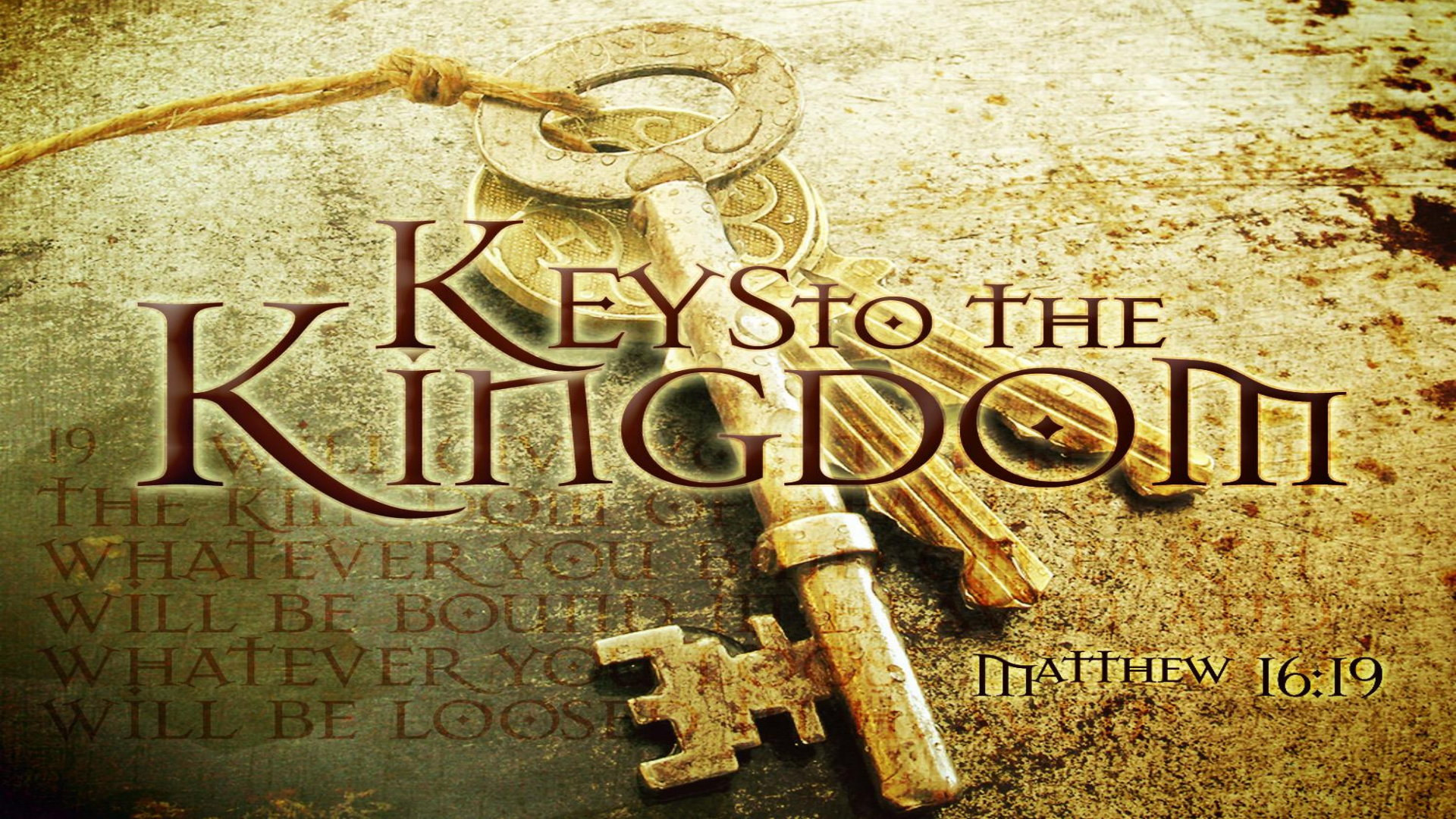
Where Are My Credit Cards?

Rest

Transit

Memory





KEYS TO THE KINGDOM

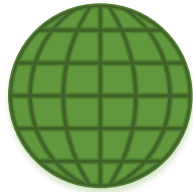
19
THE KINGDOM OF
WHATEVER YOU
WILL BE BOUND
WHATEVER YOU
WILL BE LOOSE

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



Not
vulnerable

Retail
Environment
Assumptions



Retail
Environment
Assumptions



Cashier \neq hacker

Retail
Environment
Assumptions



Big Brother

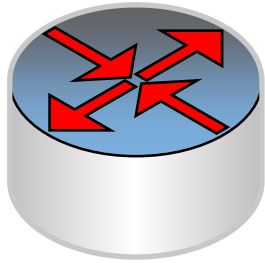
RATS



Achilles
Tendon

Remote
Administration
Tools

Achilles
Tendon



Routing

Achilles
Tendon



Achilles Tendon

Threats



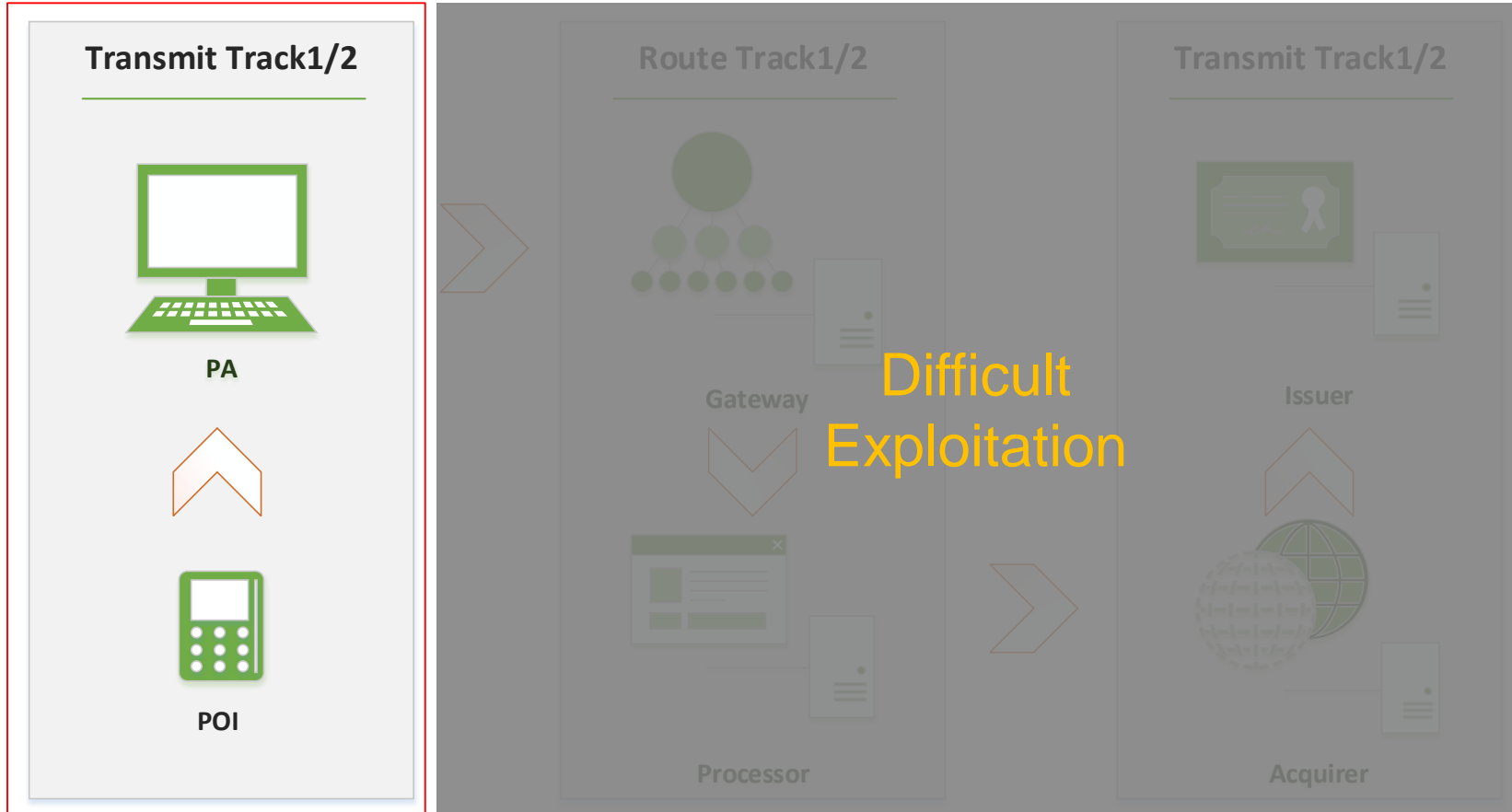
I AM BOB



ME TOO



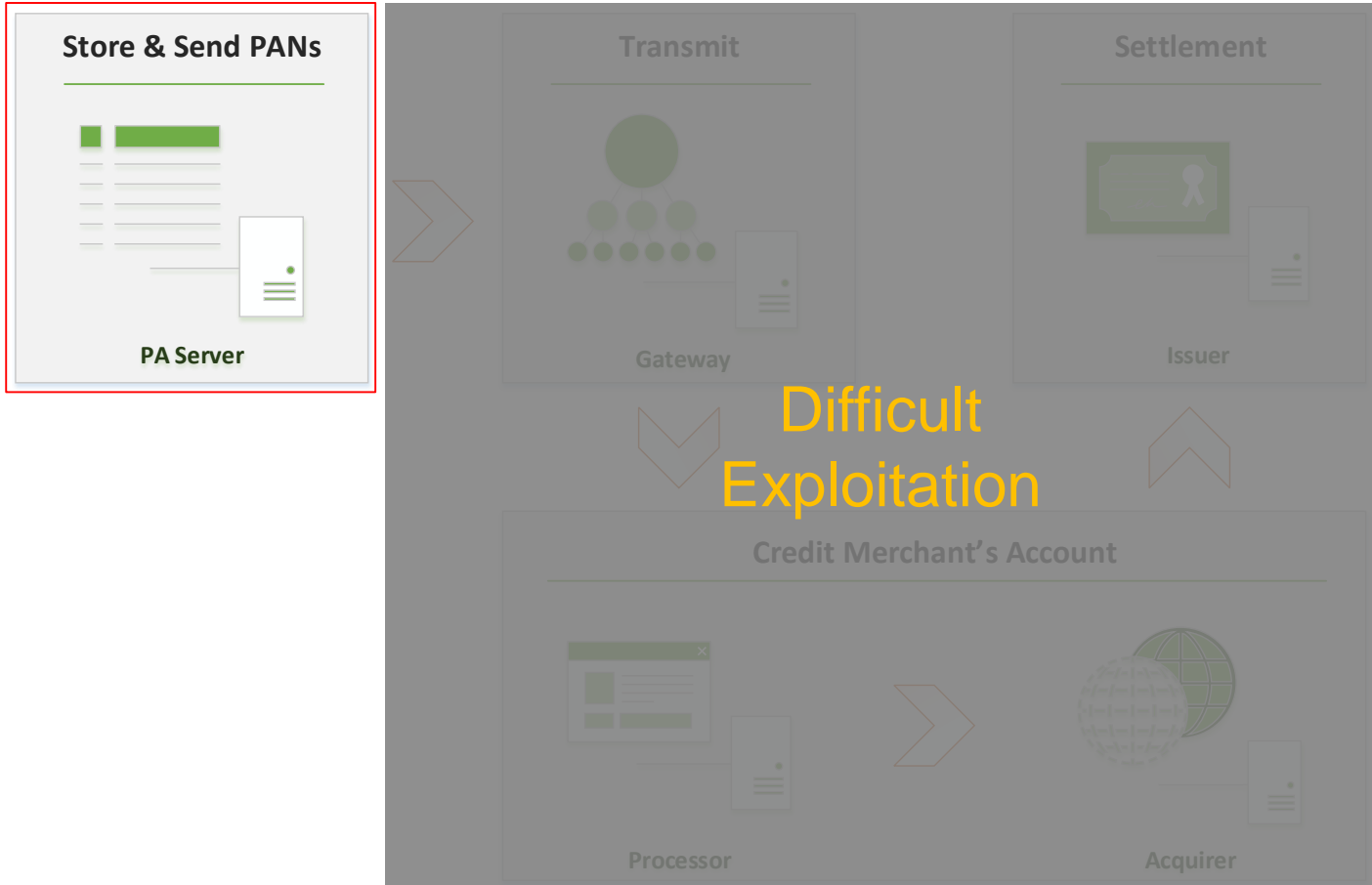
Payment Stages - Authorization



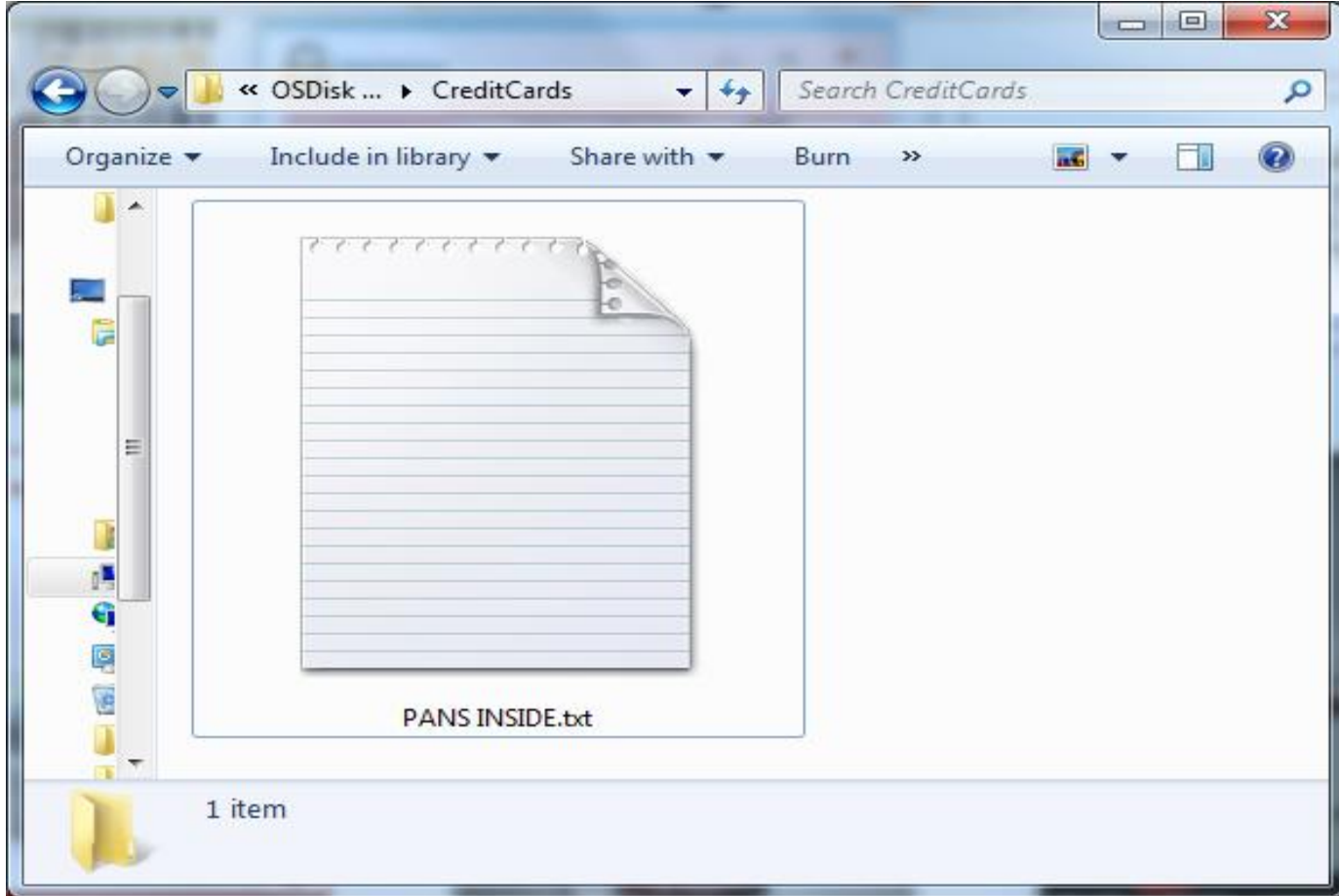
Payment Stages - Authorization



Payment Stages - Settlement



Payment Stages - Settlement





Memory Scraping

Demo

ve
nd
Login



Login



PRIVACY





Online

vs



Offline

Bypassed Solutions

SecureString Class

Demo



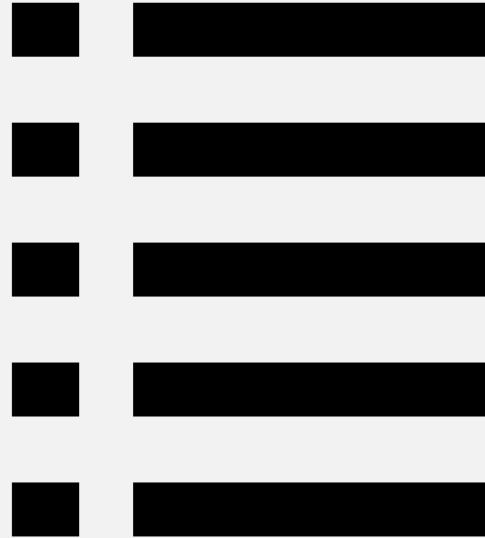
Next Next Next Generation Firewall

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

Любопытный


Группа: Пользователь
Сообщений: 11
Регистрация: 31.05.2014
Пользователь №: 55 605
Деятельность: [другой](#)

1.06.2014, 20:43 Отправлено #2

 BlackPOS?


[ПРОФИЛЬ](#) [ПМ](#) [ЖАЛОБА](#) [ВВЕРХ](#) [ЦИТАТА](#) [ОТВЕТ](#)

1.06.2014, 21:16 Отправлено #2

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

[ПРОФИЛЬ](#) [ПМ](#) [ЖАЛОБА](#) [ВВЕРХ](#) [ЦИТАТА](#) [ОТВЕТ](#)

1.06.2014, 22:11 Отправлено #3

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

Firefox нас нае%ал))) (с)

ККККККК
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 <#>



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)

Под этим сообщением задротиндикатор.



Отдан за 700\$, гарант.

Группа: Пользователь

Сообщений: 135

Регистрация: 12.08.2008

Пользователь №: 12 966

Деятельность: [другое](#)

Контакты в ПМ. Мозготрахи 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 [Invictus](#) 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

Уточню, дабы не было лишних вопросов в ПМ. Пос - фейк **verifone** 670. При первой арице залог -400 вкз, потом

RFI: Change terminal configuration to require PIN for all cards.

Cause: Get only 101 data, but wants PINs

Member:



Помогите по делу

Возможно ли настроить **pos** Ingenico на 100 % запрос пинкода? Стоит в достаточно тяжелом месте, приходится работать с онлайном и проблема при смене 101, пин он не запрашивает. Косяк второй, место прибыльное и в то же время дико неудобное, накладку на клавишу тяжело ставить, что можно придумать по выдерживанию пина?

Кто что может сказать на счет инфракрасного тепловизора, по нему с помощью остатков тепла после нажатия на кнопки возможно определить нажатые клавиши и последовательность набора. Дабы не сбиваться после каждого ввода, можно протирать клавишу влажной салфеткой. Рассматриваю варианты спрея.

У кого какие оригинальные мысли? Так же стукните ко мне с накладками на инженерки. Благодарствую.

Proposed Solution:
Thermal Imager



Sandbox





**Network-based
Anomaly Detection**



Operating System Anomaly Detection

Runtime Obfuscation

Not only products required !

Security Architecture

Performance

Security

Security Architecture

Assembly
Signing



Security Architecture



Assembly Obfuscation

PROCESS

ISOLATION



?

?

?

?

?

?

?

What Next

?

?

?

?

?

?

?

?

?

What Would You Steal?







cashier = hacker



Summary

Security by Obscurity

Simple Exploitation

Hard to Protect



You're Insured

Thank You

Nir Valtman

W : www.valtman.org

🐦 : @ValtmaNir

