

2017-07-26 10:00:00



2017-07-26 10:00:00

A ARTE E O JEITINHO BRASILEIRO DA CLONAGEM DE CARTÃO

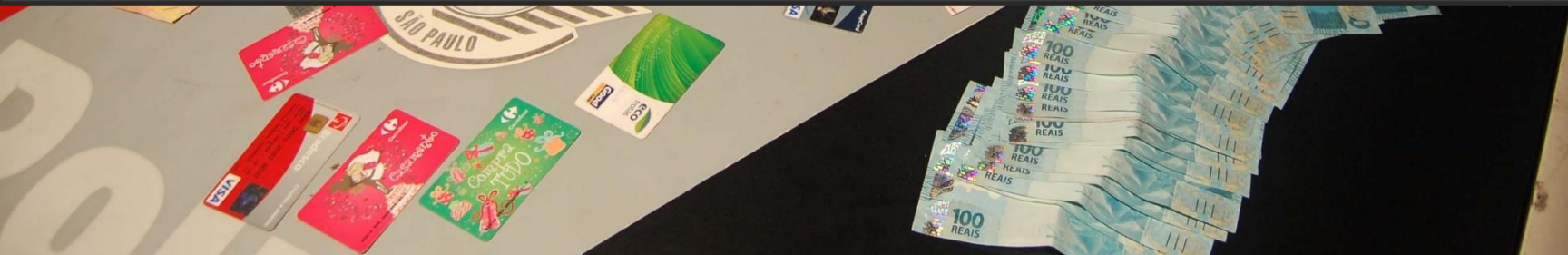
Thiago Marques, Kaspersky Lab

@thiagoolmarques

GO TO BRAZIL THEY SAID. IT WILL BE FUN THEY SAID.



Nos últimos cinco anos, metade da população Brasileira reportou ter sofrido fraude de cartão.



+55 48



+55 11

Venha montar seu próprio spam 🌟🌟🌟

Alugo sua tela BB ou Santa + Sistema de Envio Sms... Hospedo e configuro ela para você ! Tudo por um ótimo preço **semanal** 📧

Virando BB Sms todos os DDD
Virando BB Sms todos os DDD
Virando BB Sms todos os DDD

Resgato Chip do 71 ao 79 🌟

Tim 📞

Claro 📞

Oi 📞

Tenho card pra TED, DOC E TRF 🏦 !!

OBS: Se vc não entende do trampo nem venha me incomodar e encher o meu saco só venha se vc tiver e souber de tudo que eu mencionei no anúncio 🙌

09:33



ESQUEMAS MAQUINETAS

ESQUEMA BITCOIN ON

Curso BITCOIN ON TOP

ESQUEMA DE EMPRESTIMO

GRUPO FEXADO

15:01

+55 21

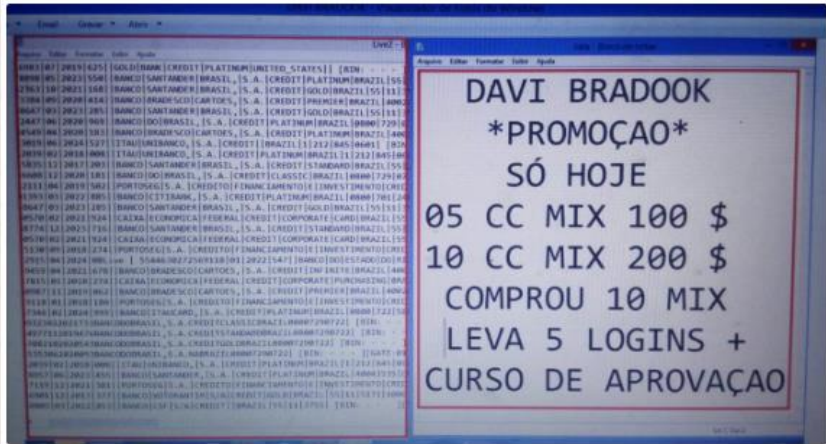
+55 21

Lotter kd o celular da minha filha?

????????

15:01

+55 21



PROMOÇÃO VALIDA SOMENTE HOJE

15:02

CPF: 833.89 [REDACTED]
NOME: INEZ [REDACTED]
MÃE: IOLAND [REDACTED]
PAI: IRINEU [REDACTED]
SEXO: FEMININO
RAÇA: SEM INFORMACAO
SIGNO: AQUÁRIO
DATA DE NASCIMENTO: 23/01/1962 - 56 ANOS
CIDADE DE NASCIMENTO: RIO DE JANEIRO - RJ
CIDADE ATUAL: RIO DE JANEIRO - RJ
BAIRRO: CPO GDE
RUA: DAS ANDORINHAS
NÚMERO: SEM INFORMAÇÃO [LT QD]
CEP: 23.015-200
TELEFONE: SEM INFORMAÇÃO
NACIONALIDADE: BRASILEIRA
ESTADO DA PESSOA: VIVA
TIPO SANGÜINEO: SEM INFORMAÇÃO
TITULO ELEITOR: SEM INFORMAÇÃO
RG: SEM INFORMAÇÃO

09:15

Caçado de Ppk

Caçado de Ppk:

Caçado de Ppk:



* 000000 TABELA 000000 *

* _____ *

* _ CC UNID _ *

* ① CLASSIC = R\$70,00 *

* ① STANDART = R\$80,00 *

* ① GOLD = R\$100,00 *

* ① PLATINUM = R\$150,00 *

* ① BLACK = R\$200,00 *

* ① INFINYT = R\$200,00 *

* _____ *

* _ CC MIX _ *

⑤ MIX = R\$240,00

⑩ MIX = R\$350,00

* ✓ MIX MAIOR PV! *

* _____ *

* _ LOGINS _ *

* _05 LOGINS POR R\$10,00_ *

* _10 LOGINS POR R\$20,00_ *

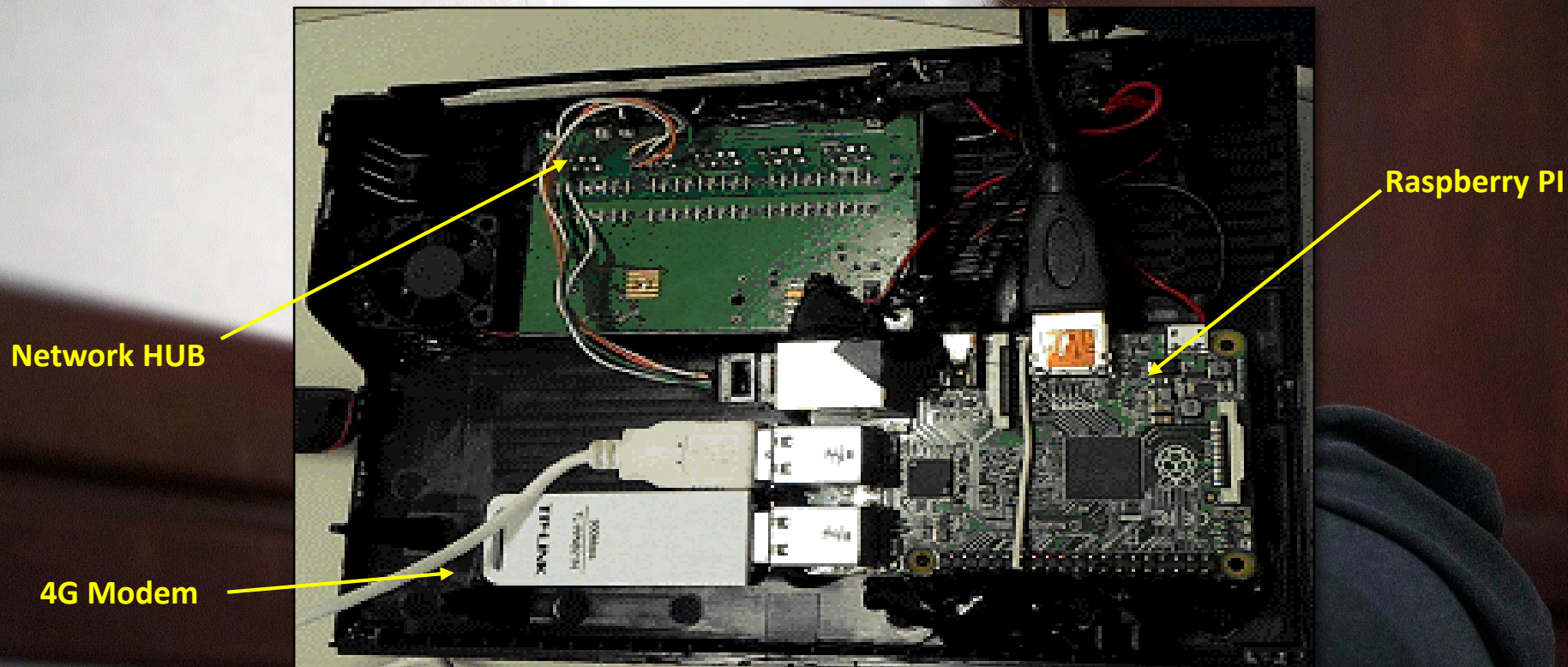
* _15 LOGINS POR R\$30,00_ *

* _CASAS BAHIA _ *

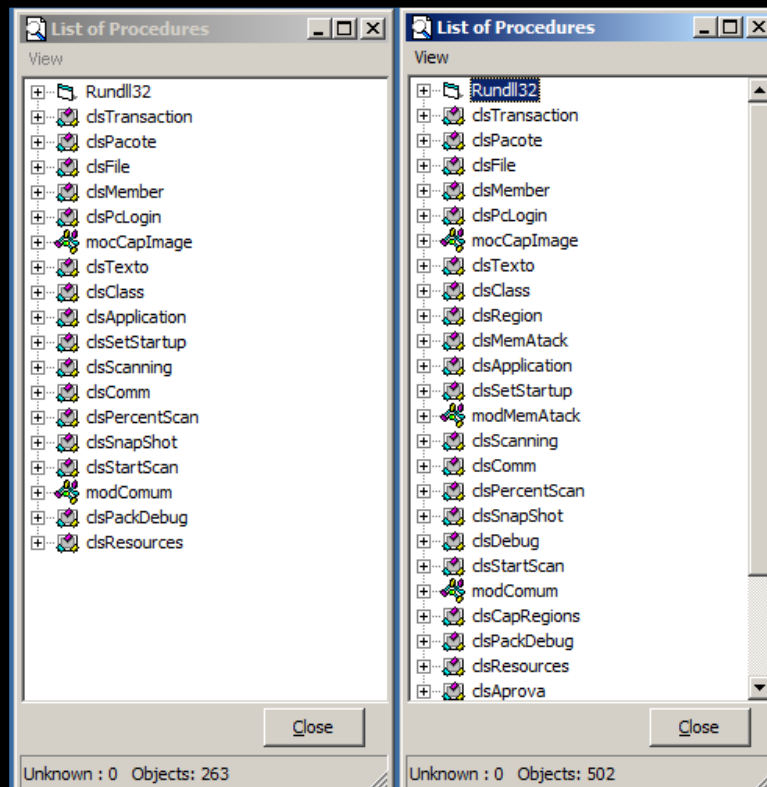
* _AMERICANAS _ *

* _PONTO FRIJO _ *

MR. ROBOT E OS ATAQUES A ATM



NÃO, ISSO NÃO É OUTRO MALWARE DE ATM



```
; DATA XREF: .text:0041268D  
; .text:004127E8↓  
0, <hkcmd>, 0  
  
; DATA XREF: .text:00412677  
; .text:004127D2↓  
0, <\\hkcmd.exe>, 0  
  
0, <D>, 0  
  
; DATA XREF: .text:004128BD  
; .text:004128EC↓  
0, <c:\\windows\\sysconfig\\sysconfig.exe>, 0  
  
0, <F>, 0  
  
; DATA XREF: .text:004128F9  
0, <c:\\clisitef\\sysconfig\\sysconfig.exe>, 0
```


O PROBLEMA



ATENÇÃO AVISO FALSO DE ATUALIZAÇÃO

Alguns clientes estão recebendo um telegrama a respeito de uma suposta atualização de módulos do Sitef, a ser feita pela Software Express no local.

Esse telegrama é FALSO.

A Software Express não realiza acessos diretos aos ambientes de Estabelecimentos Comerciais.

Favor informar à sua equipe para ignorar qualquer solicitação nesse sentido.

ATENÇÃO AVISOS IMPORTANTES PARA A SEGURANÇA DE SEU AMBIENTE SITEF

Detectamos a presença de vírus Malware em alguns terminais de venda. O Malware é de origem desconhecida capaz de afetar algumas funções das transações TEF e ocasionar a parada do sistema e, por conseguinte, eventuais transtornos e perdas nas vendas.

[Leia mais aqui...](#)

Baixe a VacinaSE (versão 1.00 atualizada em 24/01/2017), [clique aqui](#).

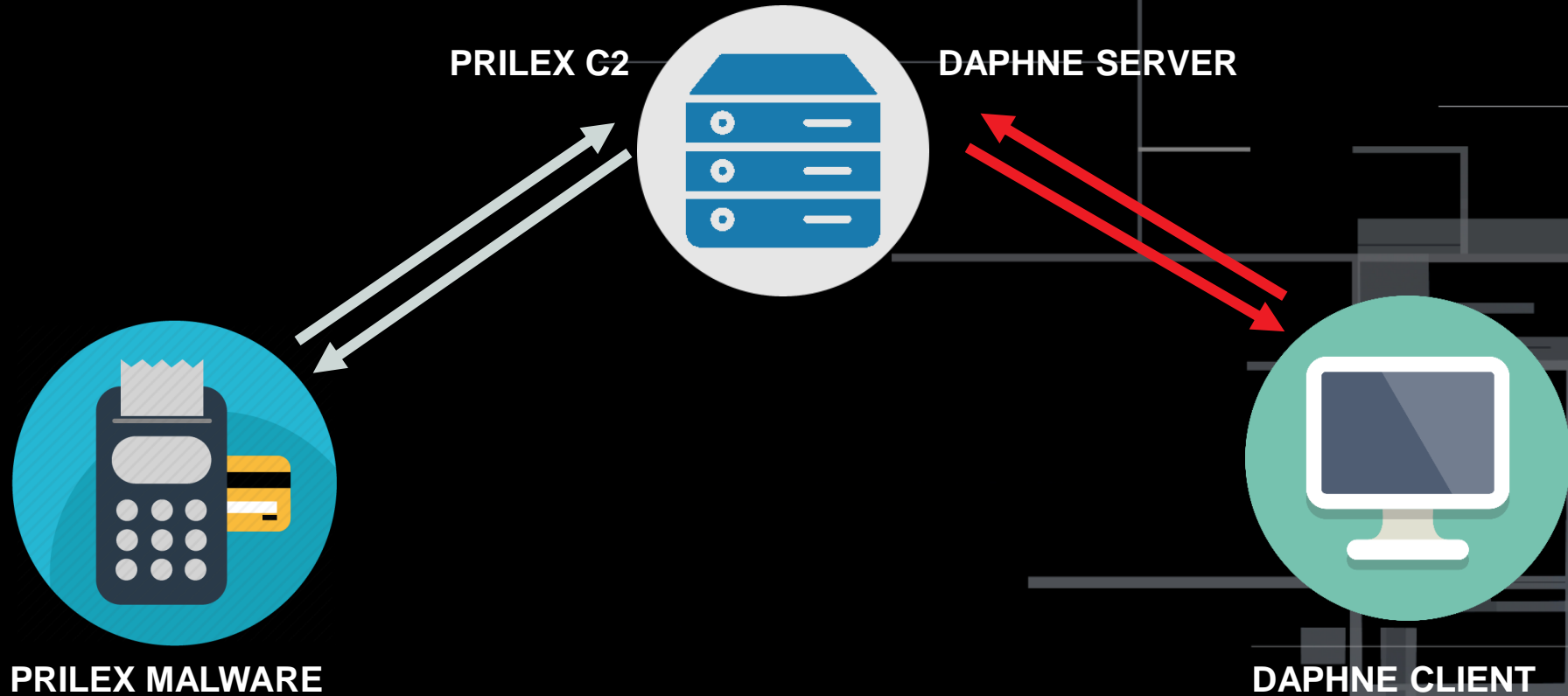
Assinaturas digitais do arquivo VacinaSE.rar:

MD5: c06c359950ef5f27ce7f2efd9f51283

SHA1: 78070383ed0c1b479657374d2574d31d3017ca2d

Para maiores informações: contate nosso suporte via email [REDACTED] ou pelos telefones (11) 4766-8000/3170-5353.

CONHEÇA O **PRILEX**



BUSCANDO OS BYTES E REALIZANDO PATCH

```

; .text
unicode 0, <ScanProcessStart>,0
align 10h
dd 0B4DC5A97h, 4BEDCE3Fh, 0C1674
dword_409690 dd 0E158870h, 4E553955h, 0A84F0
; DATA
; .text
aRegion_0 db 'Region',0
; DATA
; .text
align 4
aAppdebug_0 db 'AppDebug',0
; DATA
; .text
align 4
aProcess_0 db 'Process',0
; DATA
; .text
aMematack_0 db 'MemAtack',0
; DATA
; .text
align 4
aChangescreen_0 db 'ChangeScreen',0
; DATA
; .text
align 4
aKeys_0 db 'Keys',0
; DATA
; .text
align 10h
aSavedata_0 db 'SaveData',0
; DATA
```

CLISITEF32.DLL

```

DLL BASE:
(0X
)
(0X
)
&h
25 FF FF 00 00 81 E2 FF FF 00 00 51 50 89 15
&h
1PosByteDeCrypt 1 nao encontrado
83 C4 04 2B C8 6A 00 8D 44 10 02 51 50 FF 15 E4
&h
1PosByteDeCrypt 2 nao encontrado
52 03 CE 50 51 56 8D 54 24 30
&h
1PosByteDeCrypt 3 nao encontrado
51 FF D5 83 C4 10 8D 54 24 1C 52 68
&h
1PosByteDeCrypt:
83 C9 FF 33 C0 F2 AE F7 D1 49 85 C9 7E
&h
PosNome:
DLL BASE
(0X
)
&h
FindApp - Sem Aplicacao
Erro tnrGetHandle_Timer:
Inject Out Transacao Finalizada
```

MOSTRE O QUE TEM

00415437	MOV DWORD PTR [EBP-BC],5aba9e54.00404E14	GETAMMY
00415471	MOV EDX,5aba9e54.00404CCC	AMMY
004154B9	PUSH 5aba9e54.00404398	AMMY
004154FA	PUSH 5aba9e54.00404E2C	GETFILE
004155A1	MOV DWORD PTR [EBP-BC],5aba9e54.00404E44	AMMYON
0041565D	MOV EDX,5aba9e54.00403474	amy.exe
00415696	PUSH 5aba9e54.00404E58	cmd /c start
0041569B	PUSH 5aba9e54.00403474	amy.exe
004156DC	MOV DWORD PTR [EBP-BC],5aba9e54.00404E78	AMMYOFF
004157B3	MOV DWORD PTR [EBP-BC],5aba9e54.00404E90	GETLOG
004159A6	MOV DWORD PTR [EBP-BC],5aba9e54.00404EA4	SHELL
00415AC3	PUSH 5aba9e54.00404500	
00415B20	PUSH 5aba9e54.00404EB4	Executar
00415C49	PUSH 5aba9e54.00404ECC	Executar cmd /c
00415C98	PUSH 5aba9e54.00404D64	cmd /c
00415CF1	MOV EDX,5aba9e54.00404EF4	Ok

DAPHNE ENTERPRISE



[Enviar Cargas](#)
[Infos](#)
[Extras](#)

Visualizar
Infos

Infos Em
Aberto

Mensagens

Verificar
Card

Admin Off-Line

 Infos

Exibir Infos Filtradas

Carga

4

Id	Número	Nome
1	99999999999999999999	CARDHOLDER NAME




Esta tela pode ser usada para enviar mensagens de texto para o administrador (APENAS O ADMINISTRADOR). Os outros usuários não terão acesso as suas mensagens!

```
<<2017-05-31 12:37:14>>
ola
```


GPSHELL E JAVA SMART CARDS

<



>

Novo - 109 vendidos

Novo - 534 vendidos

Leitor Certificado Digital II Smart Card Gemalto - Usb

★★★★★ 11 opiniões

R\$ 47¹⁸

6x R\$ 7⁸⁶ sem juros

VISA Mastercard Boleto

Mais informações

Envio para todo o país

Saiba os prazos de entrega e as formas de envio.

Calculador de frete

Devolução grátis por 7 dias

A partir da data que receber o produto

Quantidade:

1 ^ v

Comprar agora

Adicionar ao carrinho

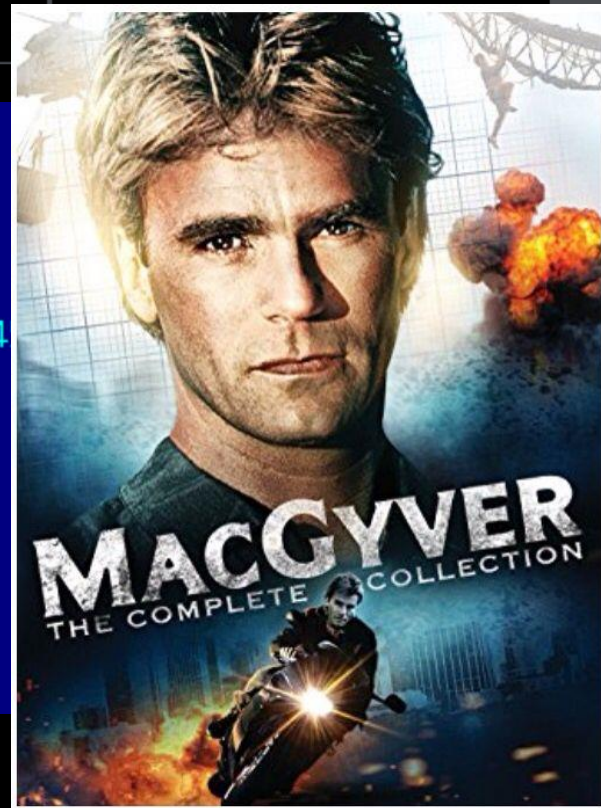
MACGYVER

```
#select CardManager
select -AID a000000003000000

#open security channel to be able to write to the card
open_sc -security 1 -keyind 0 -keyver 0 -mac_key 40414243444

#cleanup existing Payment System Environment - 1PAY.SYS.DDF
delete -AID 315041592E5359532E444446303101
delete -AID 315041592E5359532E4444463031

#install malicious CAP file
install -file OS.dat -priv 4
```



Select PSE 1PAY.SYS.DDF

AID Mastercard

Application Label: MasterCard

Track 2

Cardholder Name: THESAS 2018

APPLICATION INTERCHANGE PROFILE

4000 (BYTE 1 BIT 7) SDA SUPPORTED

1000 (BYTE 1 BIT 5) CARDHOLDER VERIFICATION IS SUPPORTED

0800 (BYTE 1 BIT 4) TERMINAL RISK MANAGEMENT IS TO BE PERFORMED

0000 (BYTE 2 BIT 8) ONLY MAGSTRIPE MODE SUPPORTED

STATIC DATA AUTHENTICATION



**SIGNED STATIC APPLICATION DATA
(SSAD)
HASHED DATA**



**NÃO PODE EVITAR CLONAGEM DE
CARTÃO**



O QUE PODEMOS ESPERAR ...



★★ KIT COMPLETO PRONTO PARA TRABALHAR ★★

✓ GRAVADORA DE CARTÃO MCR 200 CHIP E TARJA

✓ SOFTWARE GRAVAÇÃO

✓ FORNECEDOR DE TRILHAS

✓ 10 CARTÕES PVC

✓ COLHEDOR DE TRILHA

R\$ 1200 💰 >>TEMPO LIMITADO<<

*ENVIAMOS PARA TODO BRASIL COM CÓDIGO DE RASTREIO

PRAZO DE ENTREGA: 20 A 30 DIAS

APÓS PAGAMENTO CÓDIGO DE RASTREIO ENVIADO EM ATÉ 5 DIAS ÚTEIS.

CONTATOS 100% POR E-MAIL.



magnata 22 de janeiro de 2018 20:54

5 CLONE CARD PVC 5

WHATHSAPP 77 999019232

Com senha -> FORMATO DE PVC CLONE ATUALIZADOS, NÃO TRABALHO COM VELHARIA

LOTES:

05 Unidades PREÇO -R\$ 500,00

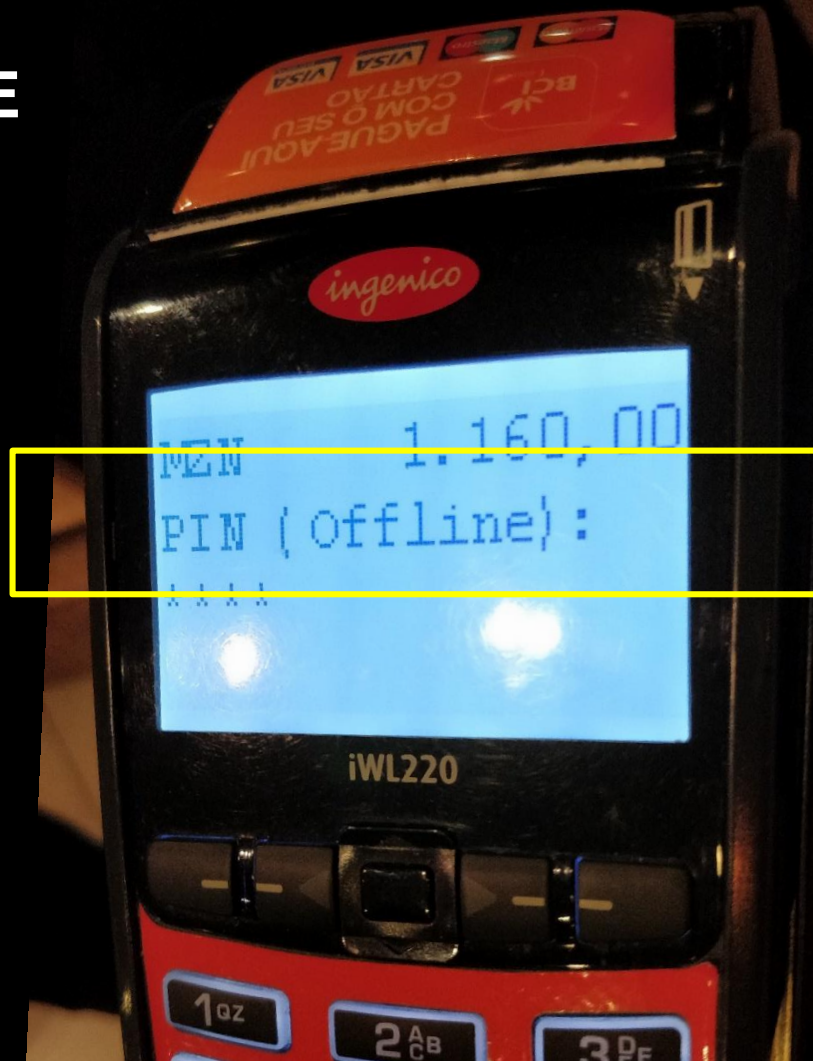
20 Unidades PREÇO -R\$ 1500,00

40 Unidades PREÇO -R\$ 2500,00

50 Unidades PREÇO -R\$ 4000,00

NÃO VENDO "BARATO" PORQUE SEI O POTENCIAL DE GANHO DO MEU PRODUTO
PVC FÍSICO, IMPRESSO, COM RELEVO E 3D

MOÇAMBIQUE





OBRIGADO

Thiago Marques, Kaspersky Lab

@thiagoolmarques