O mercado negro dos crimes cibernéticos no Brasil

Ronaldo Lima – Aline Bueno

Agenda

O mercado negro dos crimes cibernéticos no Brasil

- Cenário
- O mercado negro brasileiro
- Como eles trabalham
- Crimeware

Alguns números

- A Febraban estima que fraudes eletrônicas tenham causado prejuízos de cerca de **R$1.4 billhão** aos bancos em 2012.

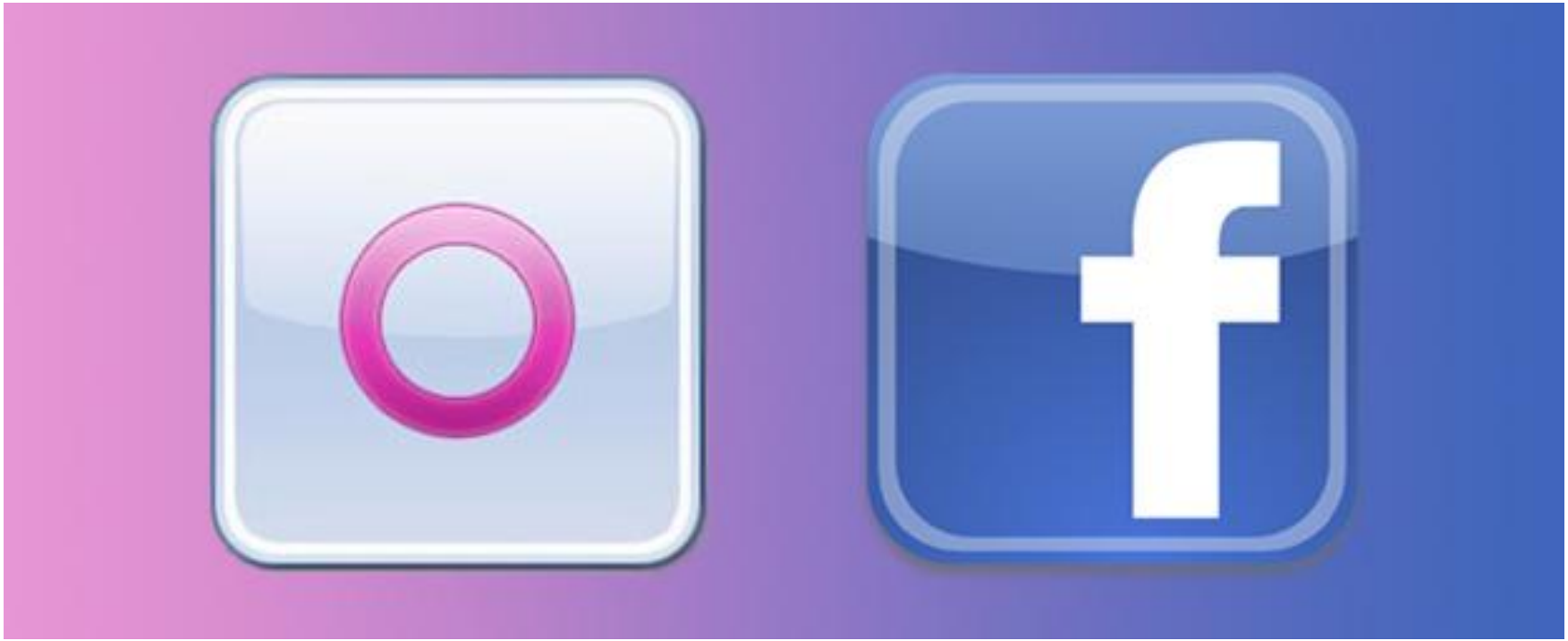
- O número de transações bancárias online (Internet Banking and Mobile Banking) ultrapassou o número de transações feitas em agências bancária.

- O Brasil já é o segundo maior mercado de cartões de crédito e débito do mundo.

Crimes cibérnéticos e bancos brasileiros

O Mercado Negro Brasileiro

Redes sociais



-=[+]=- S3R14L -K1LL3R -=[+]=-

add as friend | ignore | report

Infos CC | Milhas | Pontos Tam | Aprovações | Passagéns Aeréas // Com Fé Em Deus Eu Chego Lá...

location: São Paulo, Brazil

view full profile

Badges

About -=[+]=- S3R14L

© S3R14L - K1LL3R - OFICIAL ®
2012 - All Right Reserved* 1.7.1

Trabalho Com Todos Tipo De Serviços.

Infos CC (Visa , Master. Hiper) Em Unidades & Lote's De Infos CC

-

Novidade Milhas. TAM Consulte O Preço.

-

Novidade Documentos Digitalizados. RG.CPF.Card.Compr Res. Frente & Verso

-

Docs Editaveis, (Todos Os Tipos De Documentos Editaveis.

-

Senhas Consulta (Serasa,Intouch, Spc,Credd,Equifax,Bci

-

Kit Spam (Tudo Para Seu SPAM Carding Ou Banking.

-

Paginas Fakes, (Qualquer Tipo De Banco ou Bandeiras

-

Sources KL Pharming. Atualizados (Source E Compilado Delhpi VB

-

Modulos Banking (Bradesco,Caixa,Santander,Itau) Atualizados 2012

-

Enviadores Para Spam. (Ssh,Inbox, Smtp

-

Crypter's E Descripters (Otimos Crypter Hacking

-

Virus TEF (Virus C/ Descripter Negociavel

Trabalho Com Outros Tipos De Serviços Disponiveis No MSN

Contacto MSN Pessa Por Depoimento (Duvidas Envie Recado

-=[+]=- S3R14L -K1LL3R -=[+]=-

3 vibes

Infos CC | Milhas | Pontos...

his updates
profile
scraps
photos
videos
testimonials

Actions
Add as friend
Ignore user
Report abuse

friends (889)

search friends

Adriano | bruno | [MOD]

Upgrade Velox | $) Juuh | Dick Viganista

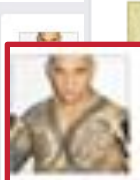
willian | $ jones | marcos

communities (198)

search communities

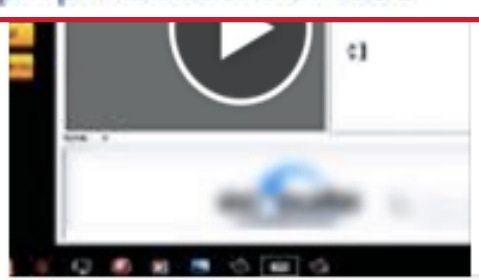
facebook.

iSIGHTPARTNERS℠



Yesterday at 2:33pm

Vendo e alugo kl proxy-banker top atualizada 25 telas nenhum avs pegando Promoção so essa semana o aluguel!!e diversas telas FAKES ... vendo testador universal de logins .. pegando pagseguro,casasbahia,uolhost,pontofrio,mercadolivre, e fast shop .. top !!! http://prntscr.com/37tu05



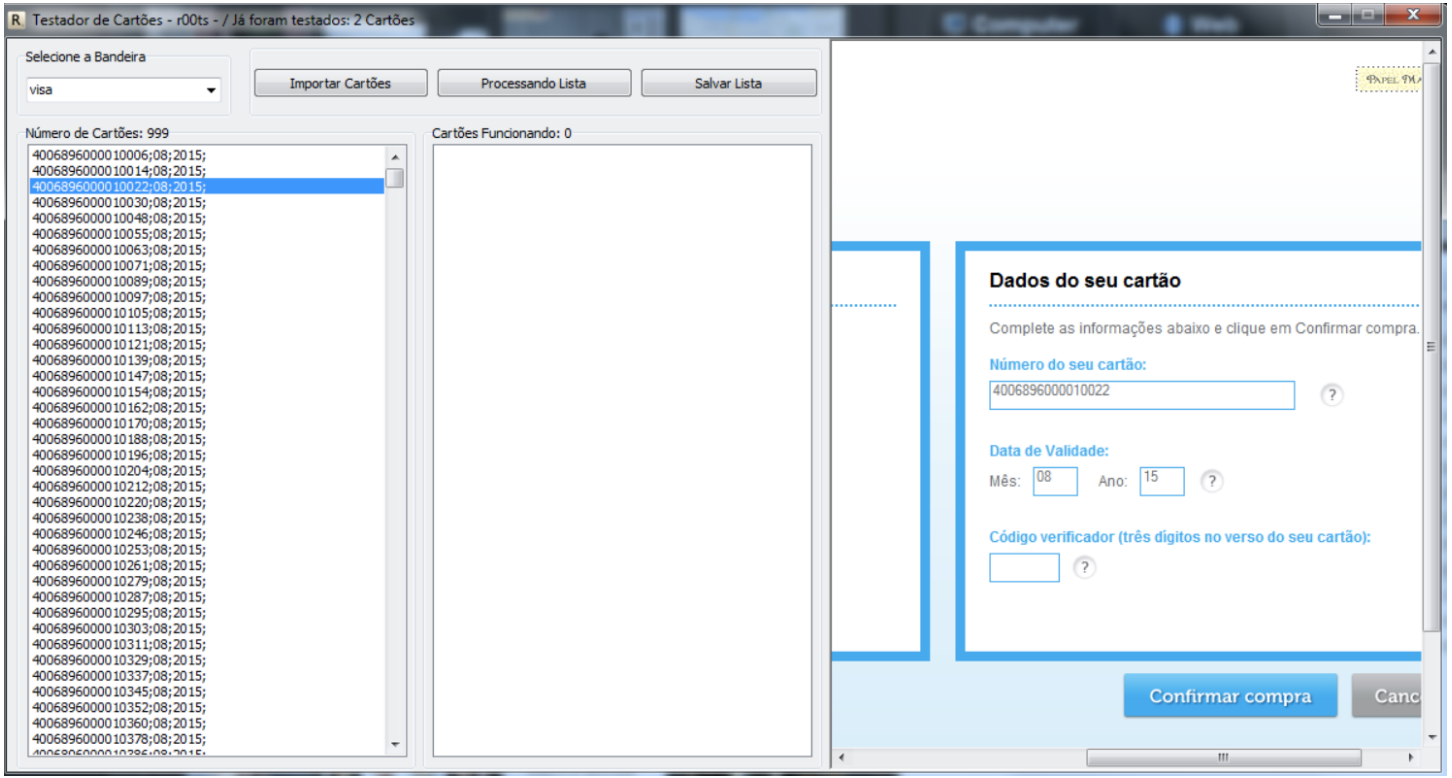
queima-las Chega de baixar programas cheios de virus . Nosso site testa suas infocc na hora http://o-rei-das-ap...

YOUTUBE.COM

Like · Comment · Share

Testador de Cartão de Crédito

Testador de Cartão de Crédito



Websites/Blogs

TESTADOR PAGSEGURO UOL

Testador de Logins Pagseguro UOL Para você que tem Lista De Emails Com senha Imensa e não tem oque fazer chegou a hora de Ad
senha

Caso o login seja Efetuado com
Notas

Login
Password
Saldo Disponivel
A receber
Bloqueado
Tipo de Conta / Verificada ou Nã
Pontuação

OBS: No video mostra o Passv

Testa 1 login a cada 3 segundos ...Super Rapido E não Bloqueia IP e não Queima Logins

Coding in : Delphi XE2

License : Commercial

Preço..: R$:800,00

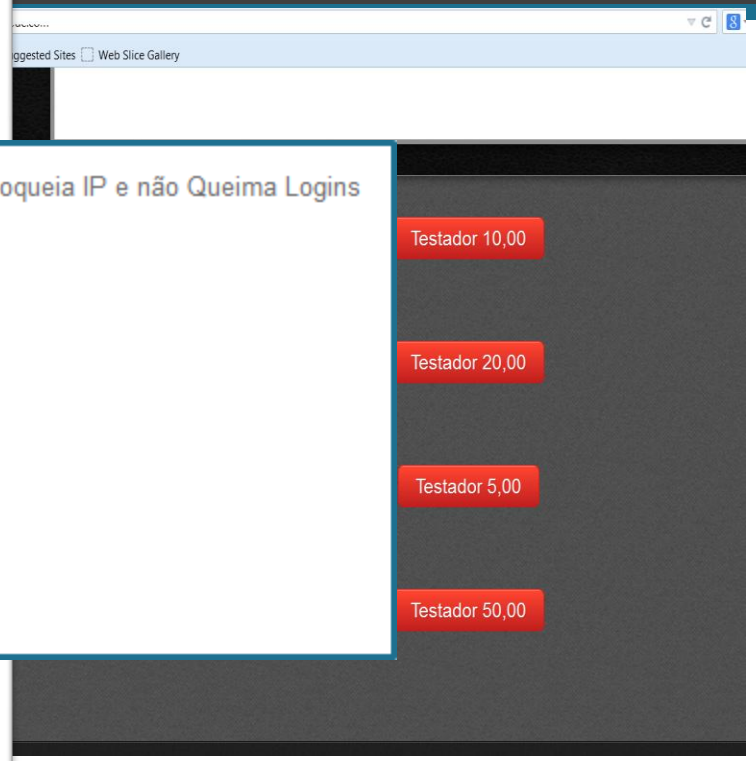
Para Maiores Informações Entre em Contato com alguma das formas Abaixo

E-mail:.

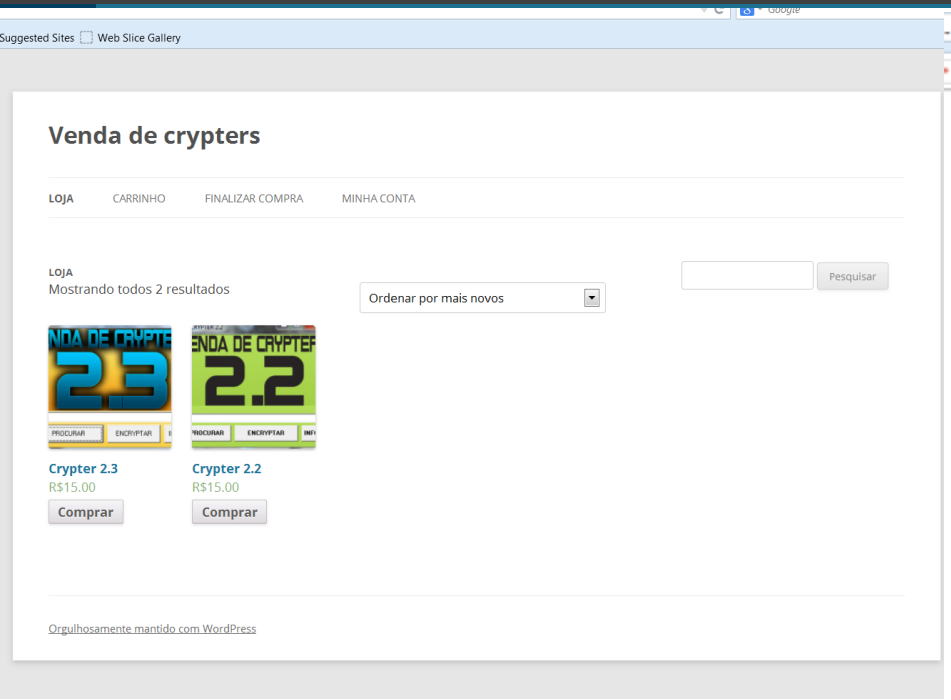
Skype:

ICQ::

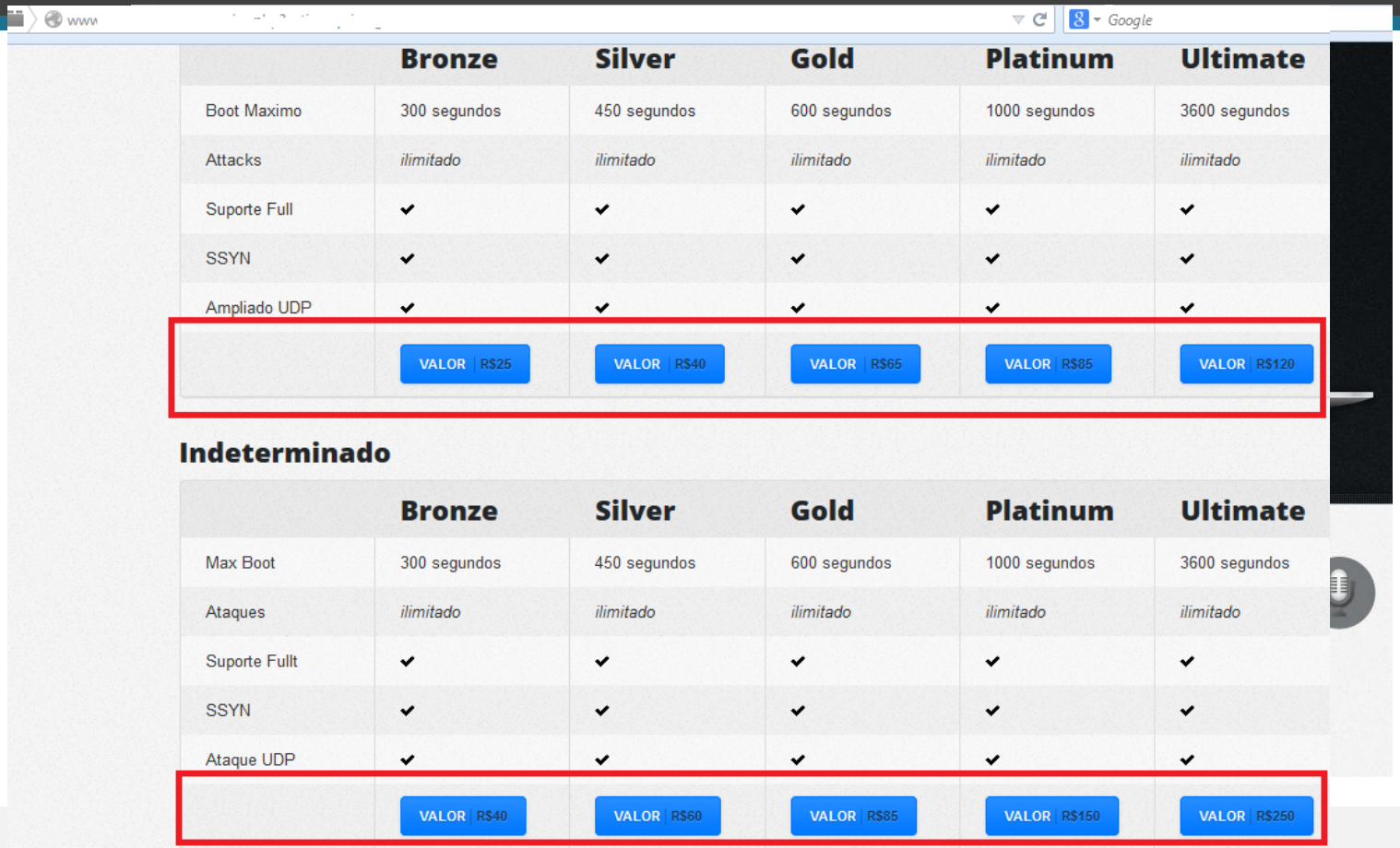
Segue o vídeo abaixa :



Websites/Blogs



Websites/Blogs

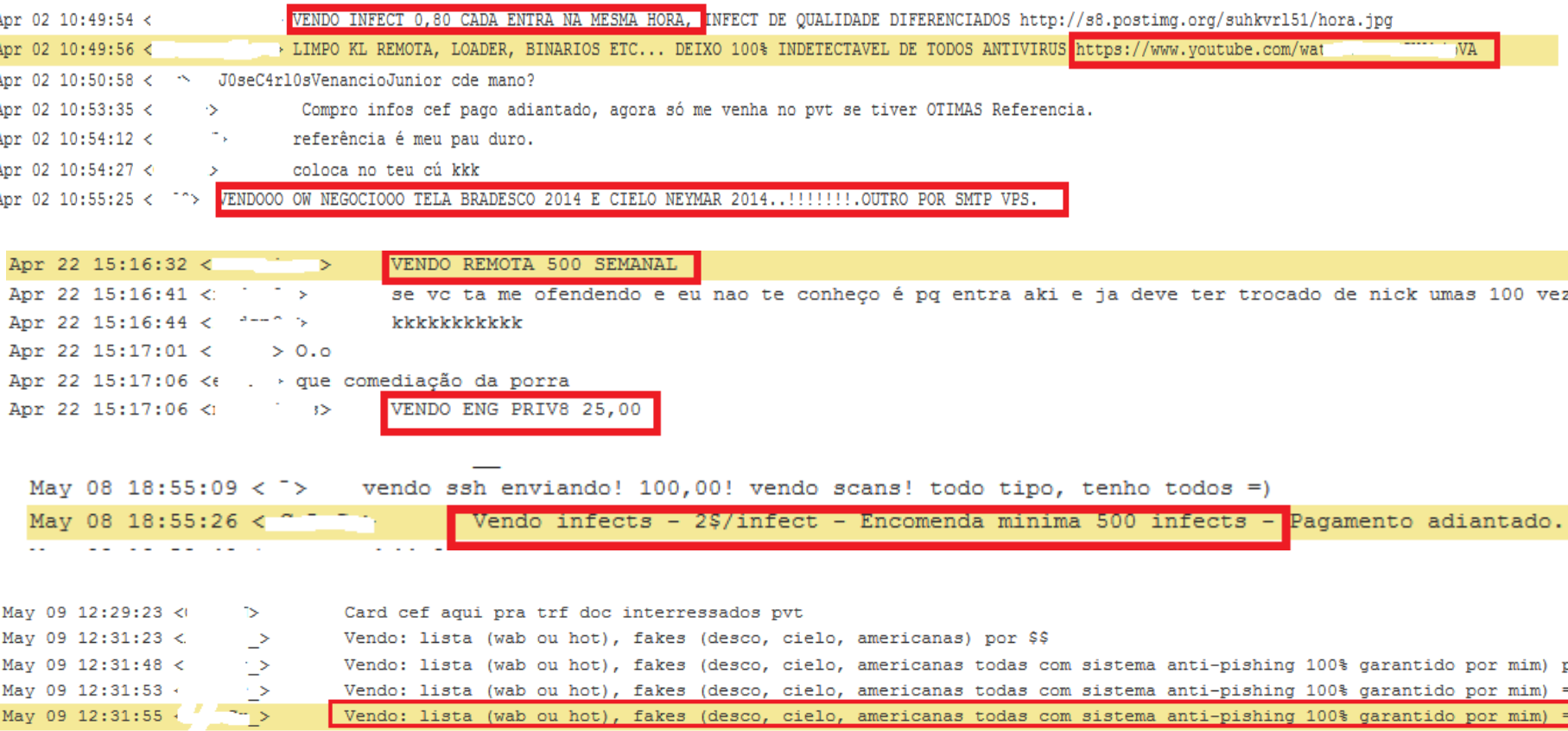


	Bronze	Silver	Gold	Platinum	Ultimate
Boot Maximo	300 segundos	450 segundos	600 segundos	1000 segundos	3600 segundos
Attacks	*ilimitado*	*ilimitado*	*ilimitado*	*ilimitado*	*ilimitado*
Suporte Full	✔	✔	✔	✔	✔
SSYN	✔	✔	✔	✔	✔
Ampliado UDP	✔	✔	✔	✔	✔
	VALOR R$25	VALOR R$40	VALOR R$65	VALOR R$85	VALOR R$120

Indeterminado

	Bronze	Silver	Gold	Platinum	Ultimate
Max Boot	300 segundos	450 segundos	600 segundos	1000 segundos	3600 segundos
Ataques	*ilimitado*	*ilimitado*	*ilimitado*	*ilimitado*	*ilimitado*
Suporte Fullt	✔	✔	✔	✔	✔
SSYN	✔	✔	✔	✔	✔
Ataque UDP	✔	✔	✔	✔	✔
	VALOR R$40	VALOR R$60	VALOR R$85	VALOR R$150	VALOR R$250

Canais de IRC



Fórums

Autor | **Tópico: DedoDuro v0.1.0 (seu bot funcionando via Tor)**

0 Membros e 1 Visitante estão vendo este tópico.

[redacted]
Novato

VX
4 ever

Mensagens: 5
Avaliações: +1/-0

DedoDuro v0.1.0 (seu bot funcionando via Tor)
« **Online:** 10 de Abril de 2014, 13:12 »

Agora seu bot HTTP pode ser controlado via Tor (suporta GET e POST)

Agora você não tem que se preocupar da sua botnet ser tirada do ar.

Agora você não precisa comprar hosting a prova de balas.

Hospede seu painel de controle em qualquer país, sem se preocupar.

Custo da licensa por mês: $150 (dólares)

Custo da licensa por ano: $1000 (dólares)

Forma de pagamento aceita: BitCoin

Fórums

Autor | Tópico: AppCloud Android botnet for Banking (BANK ALL INJ BOT)

estão vendo este tópico.

AppCloud Android botnet for Banking (BANK ALL INJ BOT)

« **Online:** 15 de Abril de 2014, 05:01 »

2. In included bot as well as one in the admin application goes with it "Drop APP"

Price :

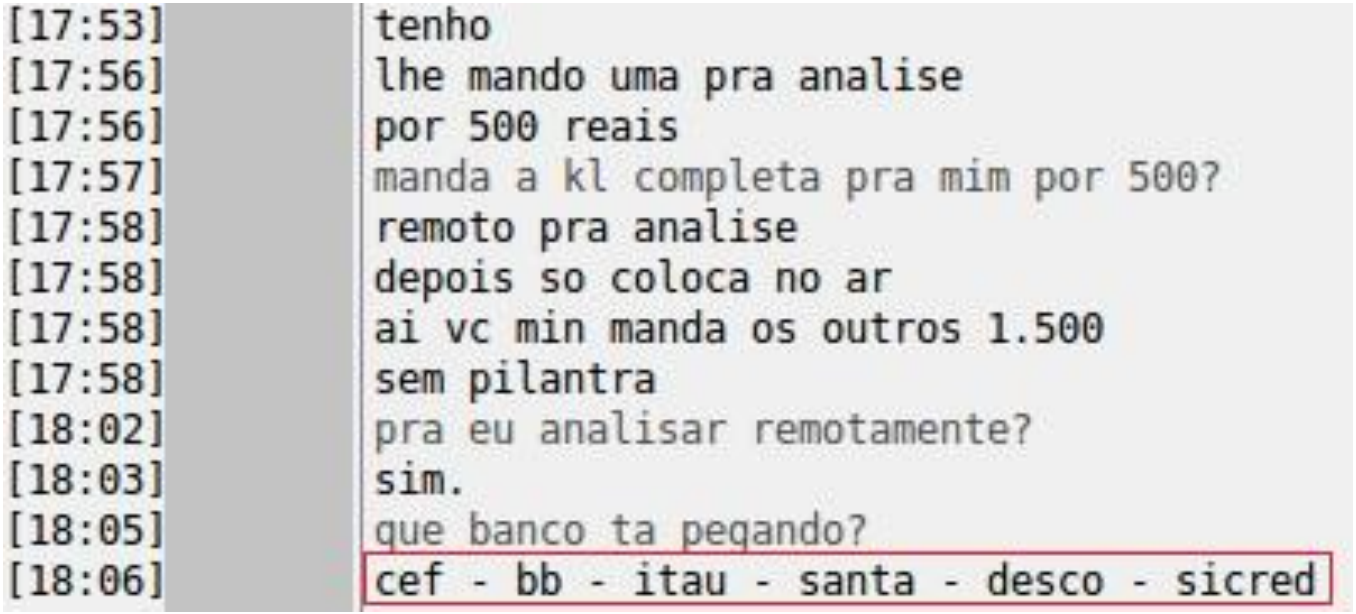
Payment via BTC / PM

AppCloud apk + panel and installation = 299$

AppCloud source code (panel +builder + src) = 1999$

AppCloud apk + panel and installation = 299$
AppCloud source code (panel +builder + src) = 1999$

Negociações



[17:53]	tenho
[17:56]	lhe mando uma pra analise
[17:56]	por 500 reais
[17:57]	manda a kl completa pra mim por 500?
[17:58]	remoto pra analise
[17:58]	depois so coloca no ar
[17:58]	ai vc min manda os outros 1.500
[17:58]	sem pilantra
[18:02]	pra eu analisar remotamente?
[18:03]	sim.
[18:05]	que banco ta pegando?
[18:06]	cef - bb - itau - santa - desco - sicred

Negociações

[redacted]	nao sei oque tem acontecido aqui mano	14:55
	to sem envio nem 1	14:55
	e nao cai desco	14:55
	pensei em me matar ontem	14:55
	juro por deus	14:55
[redacted]	como q vai cair se vc nao tem envio ?	14:58
[redacted]	mano ontem eu tinha	14:58
	mas nao dava click	14:58
	qd u tava spam desco tava caindo mto ?	15:00
	pq parou desco ?	15:04
[redacted]	veio	15:08
	ja falei	15:08

Como eles trabalham

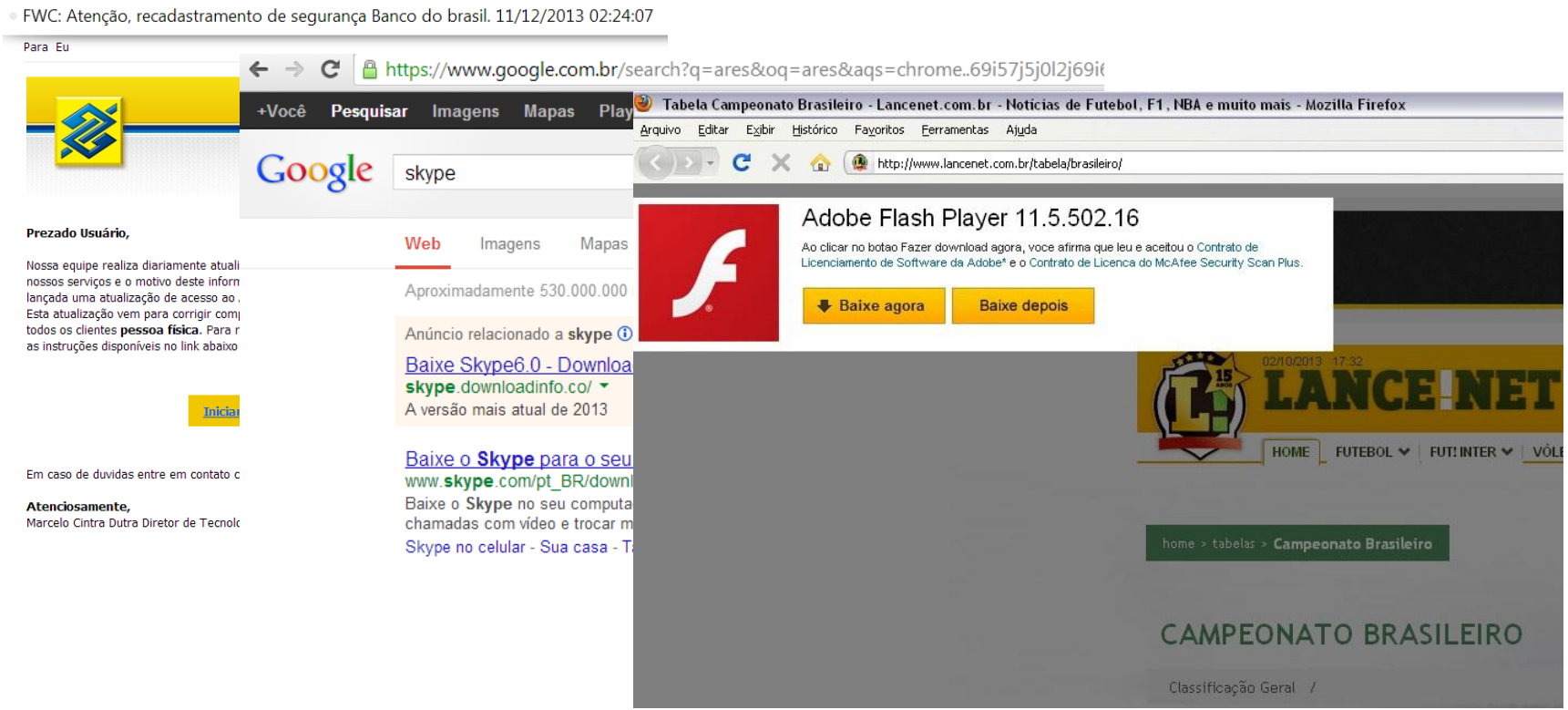
- Não gostam de pagar por hosting
- Free, invadido, dropbox, google code, google drive...
- Pouco uso de servidores dedicados – UOL HOST + DB

- Linguagens:

  + populares: Delphi, Visual Basic, PHP

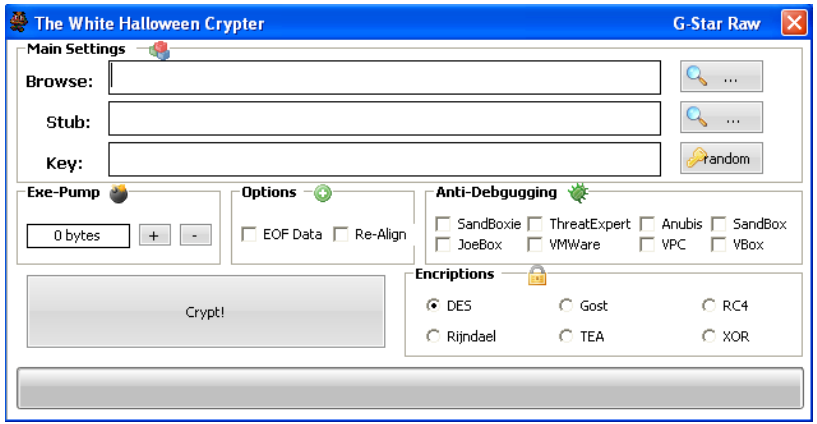
  usos específicos: Applet Java (drive by download), AutoIt (crypters)

Distribuição de malware

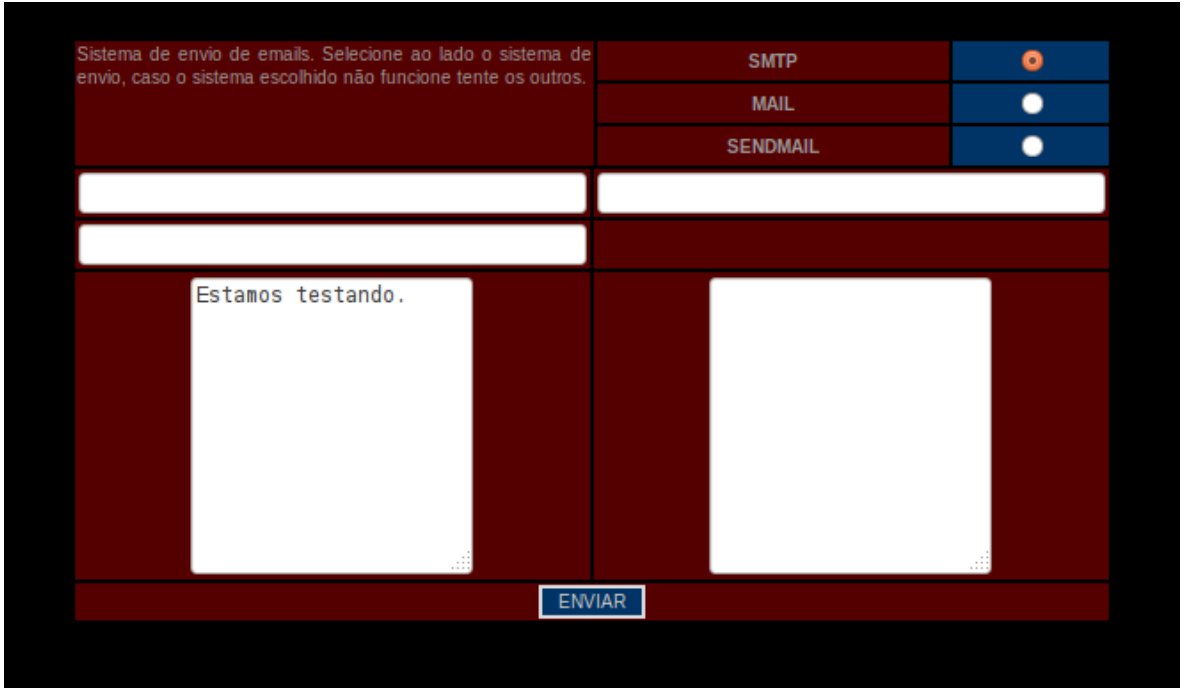


Ferramentas / Crimeware

Crypter



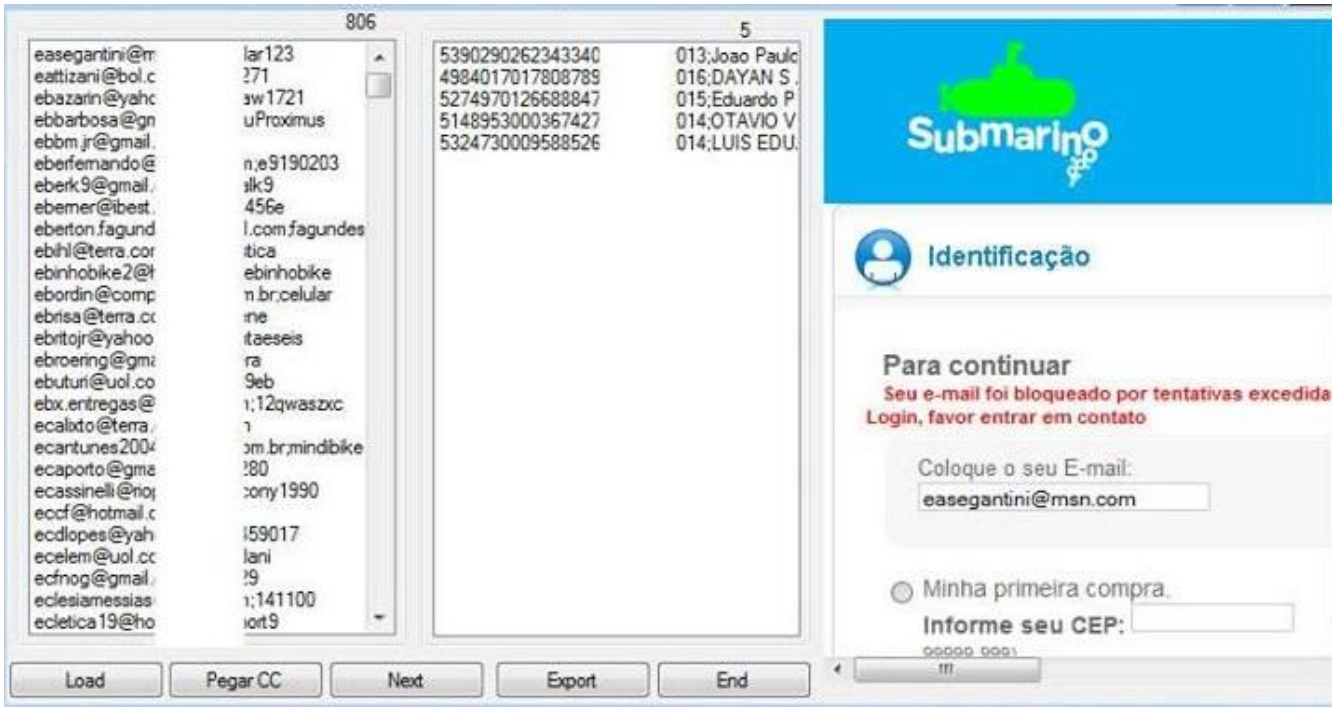
Envio de SPAM



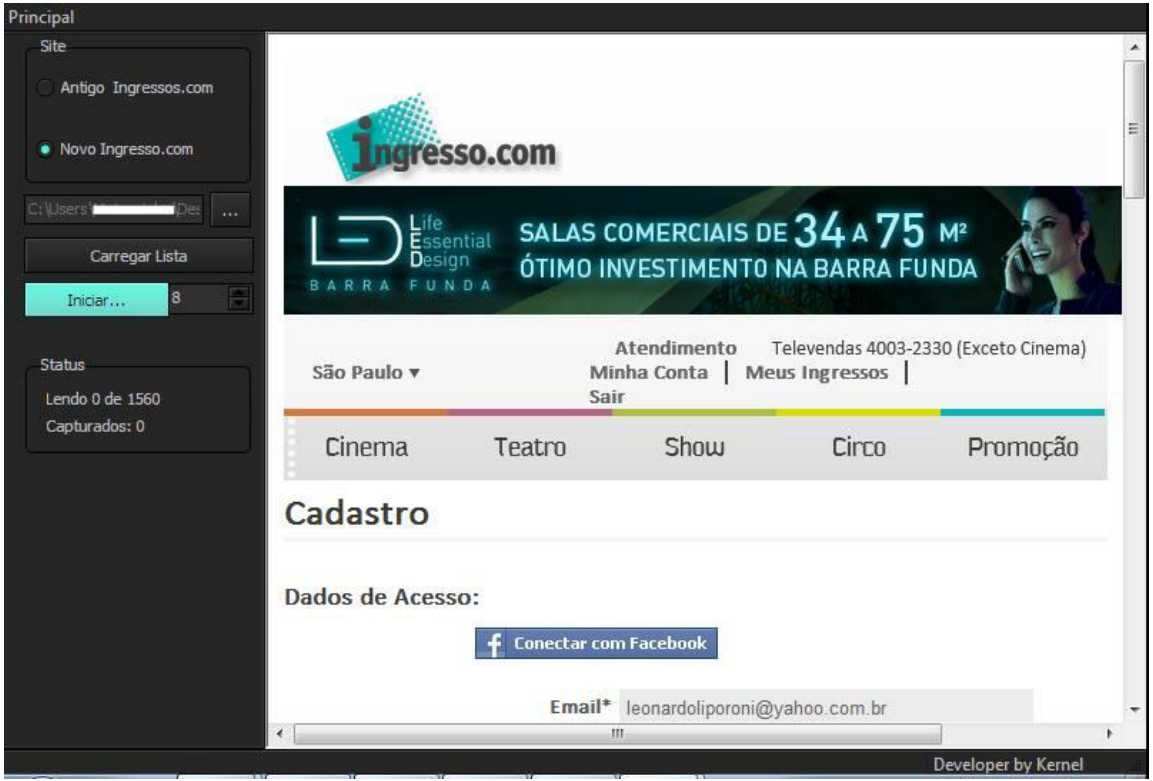
Envio de SPAM

Sugador

```
Vendo novo sugador de cc da www.submarino.com pegando CC,VALIDADE,CVV,NOME,CPF,RG coisa top mostro pelo teamview funcionando
Vendo novo sugador de cc da www.submarino.com pegando CC,VALIDADE,CVV,NOME,CPF,RG coisa top mostro pelo teamview funcionando
```



Sugador



Extensão Maliciosa Google Chrome

Virus PLugin Chrome

Pessoal esta a venda um keyloger que roda como plugin no Chrome.

O mesmo captura:

Login e senha em qualquer site que tenha dois campos textos mais um input

Pega os dados de infocc na hora do pagamento nso gateway moip, cielo, redcard, pagseguro

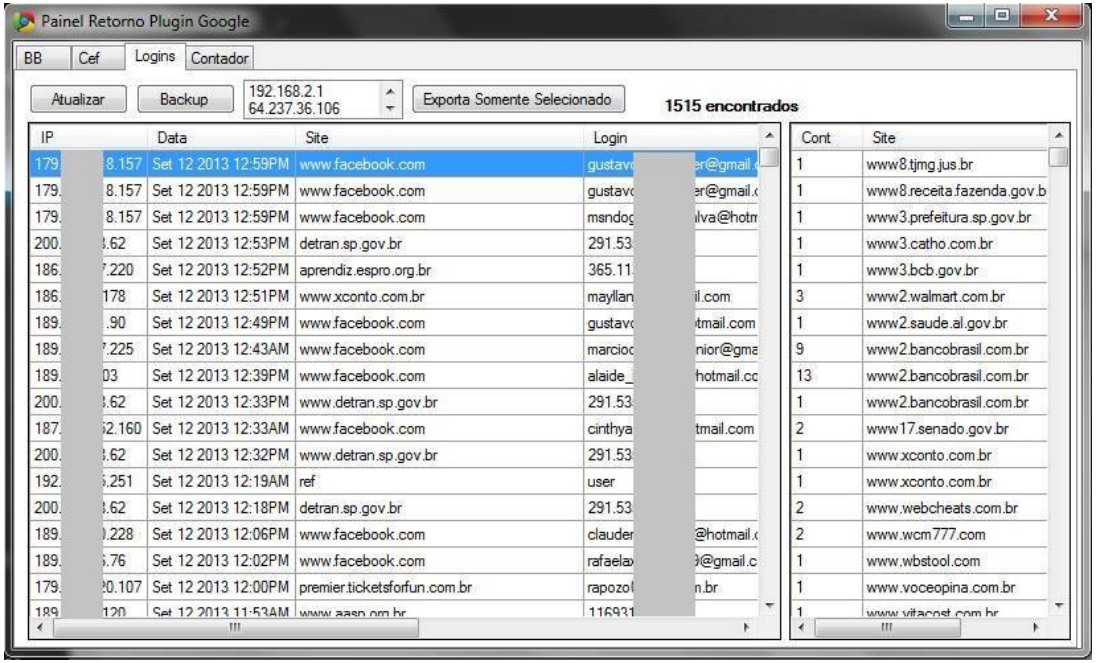
pega infobank cef e bb

Como o mesmo fica no navegador

Se você já tem algum kl posso montar o load para baixar os dois assim pegara infos bank pelo kl e logins pelo chrome

O valor do mesmo é 1000 reais por mês. e primeiro mês 1500 para cobrir a instalação dos servidores.

Extensão Maliciosa Google Chrome



Spy Net RAT (Remote Access Tool)

Portal of Russian Hackers > Хакинг & Безопасность > Социальная инженерия & Трояны > RAT Spy-Net

PDA

Просмотр полной версии : RAT Spy-Net

Noctambulaar 24.09.2008, 01:19

http://noctambulaar.ru/ad.jpg

описания нет.
Скрин с функциями (http://img89.imageshack.us/img89/4429/1832d1222011417spynettreu9.jpg)

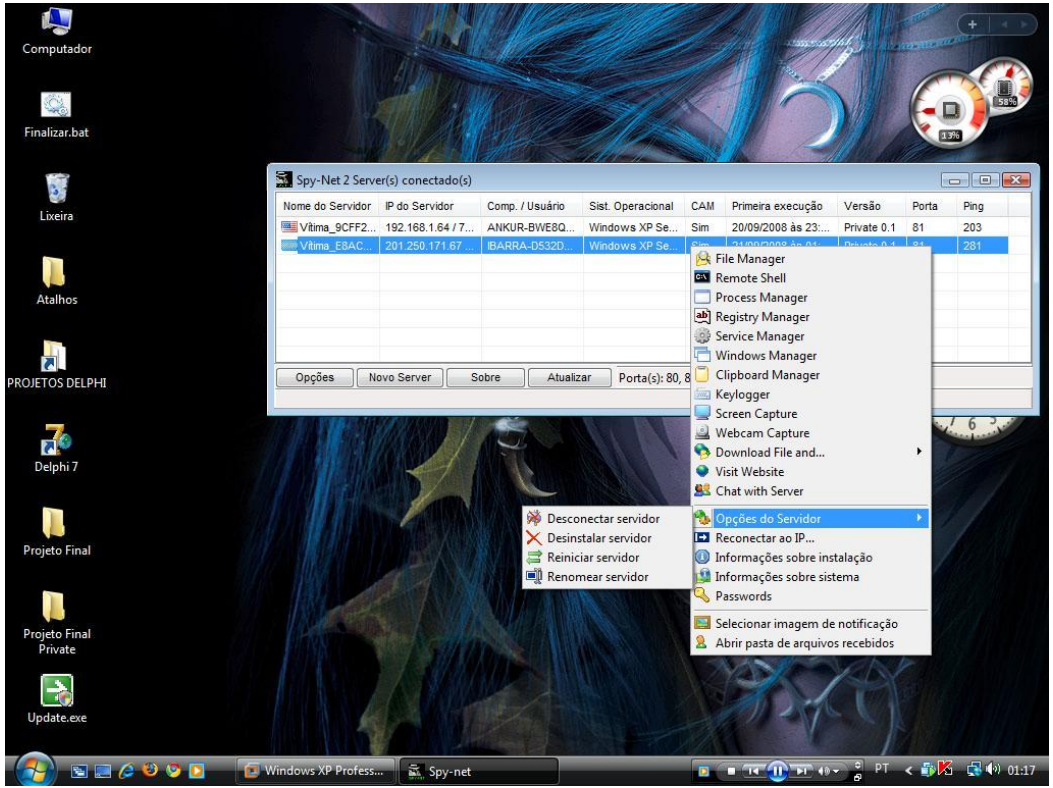
Скачать | Download (http://www.sendspace.com/file/1mz02k) (pass: n0)

Noctambulaar 30.09.2008, 16:30

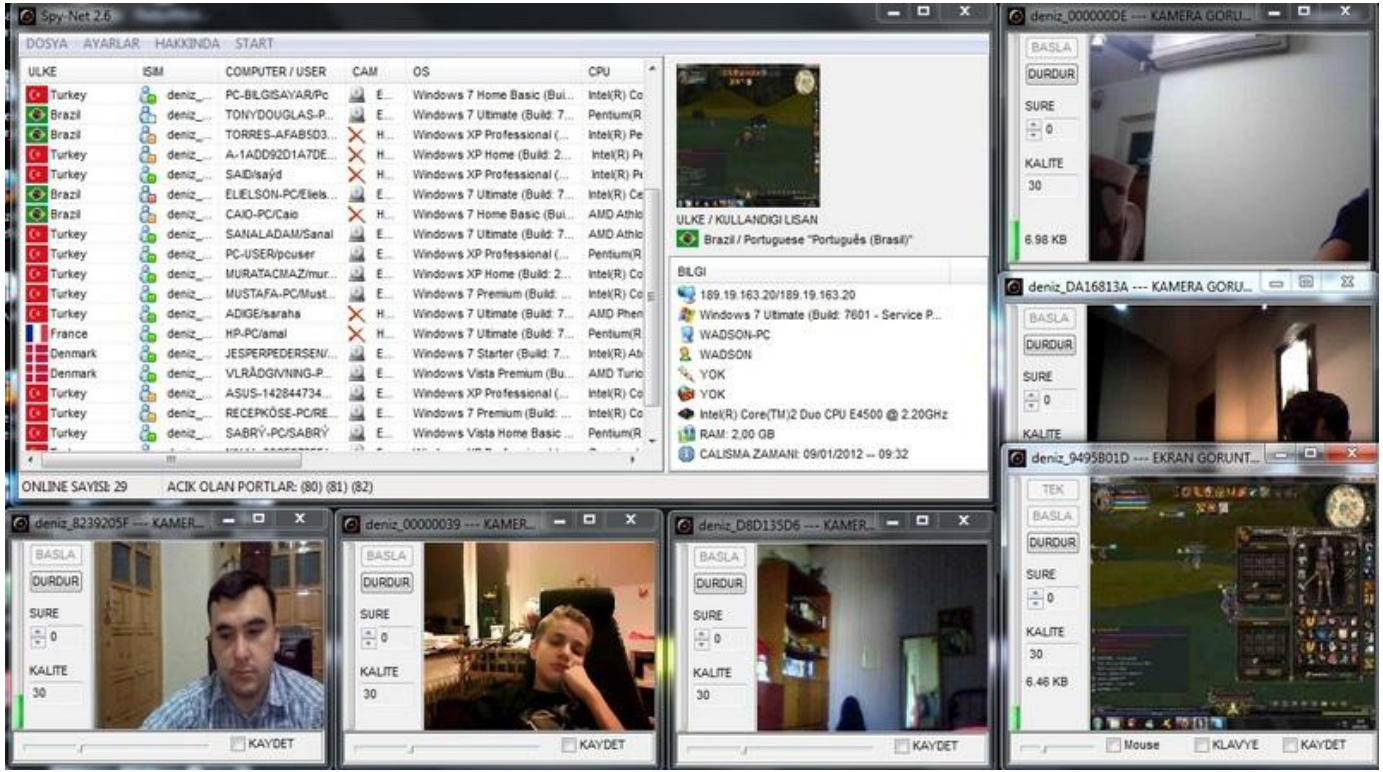
Новая версия. Spy-Net 0.4
скрин (http://img215.imageshack.us/my.php?image=principalpx2.jpg)

скачать (http://rapidshare.com/files/149480587/Spy-Net.zip.html)
password: Spy-Net

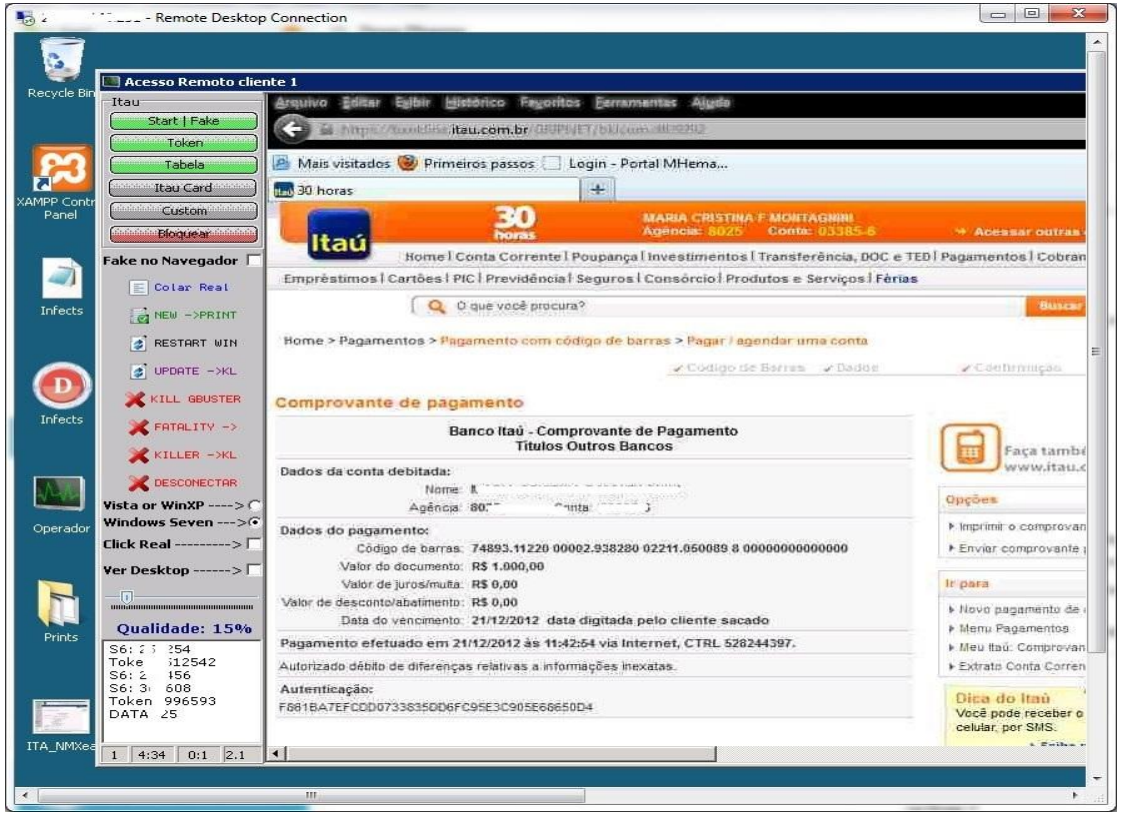
Spy Net RAT



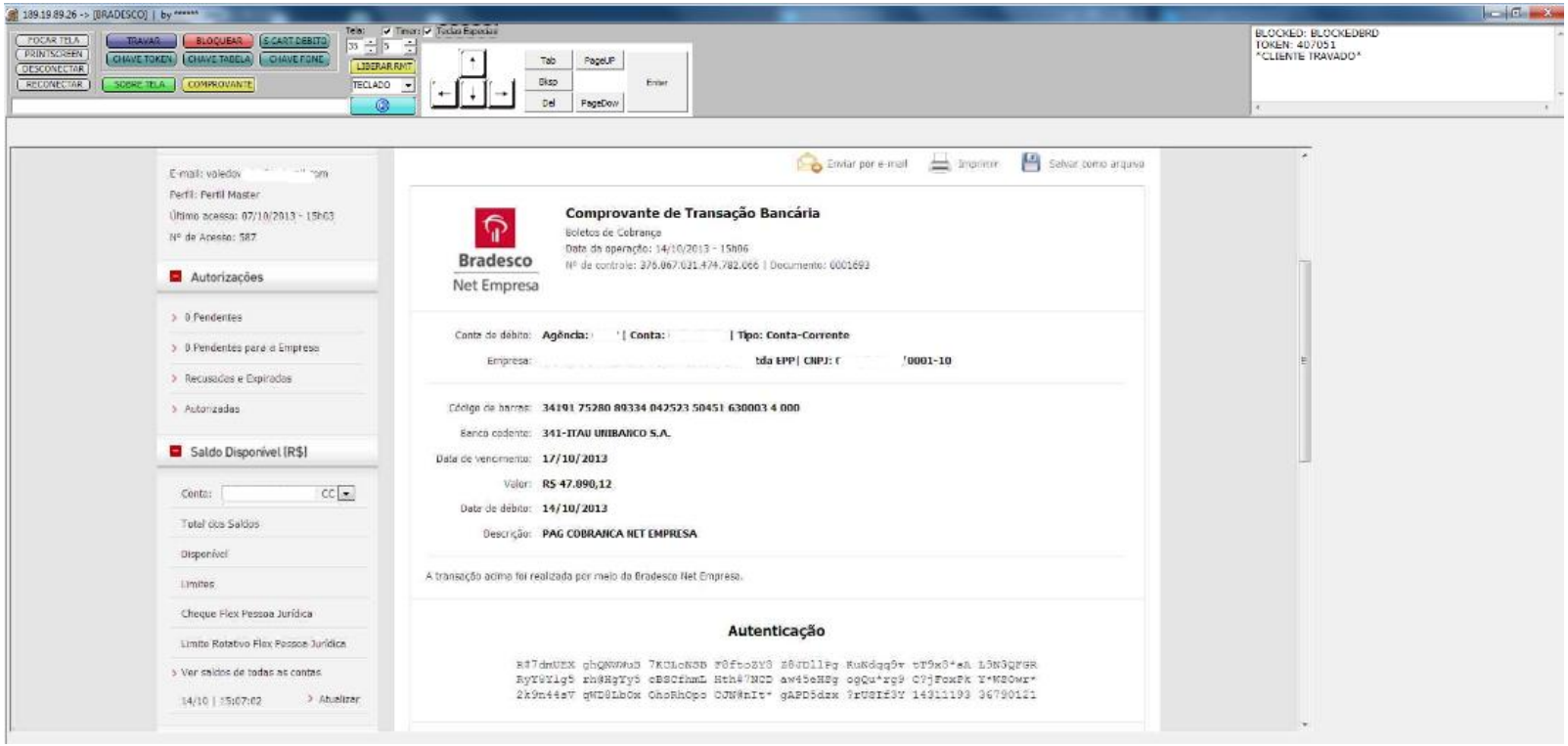
Spy Net RAT



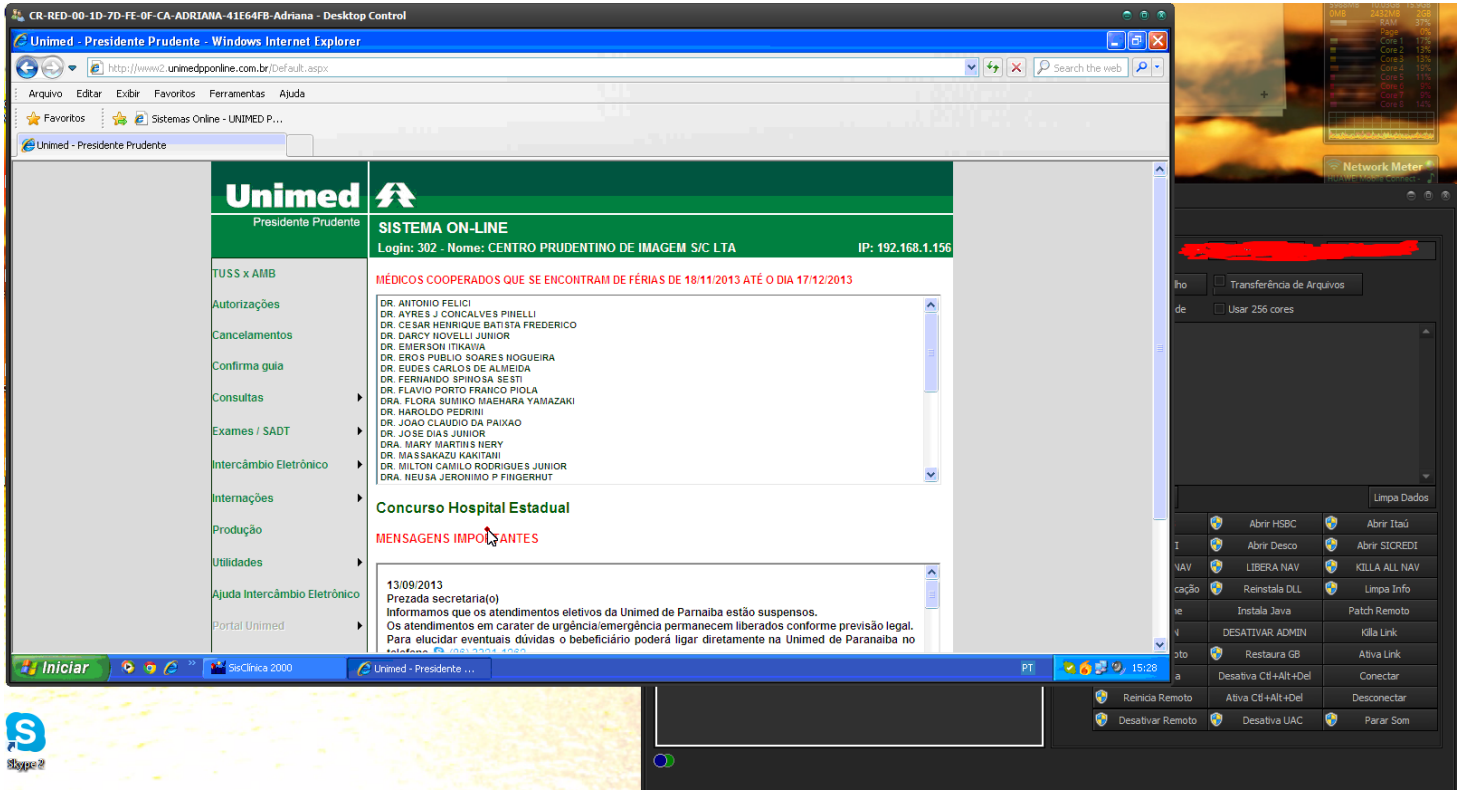
KL Remota



KL Remota


FOCAR TELA
PRINTSCREEN
DESCONECTAR
RECONECTAR
TRAVAR
BLOQUEAR
S CART DEBITO
CHAVE TOKEN
CHAVE TABELA
CHAVE FONE
SOBRE TELA
COMPROVANTE
LIBERAR RMT
TECLADO
Tab
PageUP
Del
PageDow
Enter
BLOCKED: BLOCKEDBRD
TOKEN: 407051
CLIENTE TRAVADO
Enviar por e-mail
Imprimir
Salvar como arquivo
Perfil: Perfil Master
Último acesso: 07/10/2013 - 15h03
Nº de Acesso: 587
Autorizações
0 Pendentes
0 Pendentes para a Empresa
Recusadas e Expiradas
Autorizadas
Saldo Disponível (R$)
Conta:
Total dos Saldos
Disponível
Limites
Cheque Flex Pessoa Jurídica
Limite Rotativo Flex Pessoa Jurídica
Ver saldos de todas as contas
Atualizar
Bradesco
Net Empresa
Comprovante de Transação Bancária
Boletos de Cobrança
Data da operação: 14/10/2013 - 15h06
Nº de controle: 376.067.031.474.782.066 | Documento: 0001693
Conta de débito: Agência: | Conta: | Tipo: Conta-Corrente
Empresa: | CNPJ:
Código de barras: 34191 75280 80334 042523 50451 630003 4 000
Banco cedente: 341-ITAU UNIBANCO S.A.
Data de vencimento: 17/10/2013
Valor: R$ 47.090,12
Data de débito: 14/10/2013
Descrição: PAG COBRANCA NET EMPRESA
A transação acima foi realizada por meio do Bradesco Net Empresa.
Autenticação

KL Remota



Botnet

»Home »Bots »Monitor »Upgrade »Logs

Statistics by system

Windows 7	6.487
Windows 8	3.022
Windows Vista	34
Windows XP	131
Windows 2000/2003	0
Windows Unknown	0
Linux	0
FreeBSD	0
Unknown	0

Statistics Bots

Total	10.676
Online	10.258
Offline	6.418
Favorite	6.113

Statistics by country

Botnet

Statistics of online bots :: Manage offline bots :: Manage favorite bots :: Reset online bots

#	[redacted]	Version	Country	IP	SO
21	Learning-0xac49b6c845368c5c9e582792bfcb7959	v0.0.1	Brasil	[redacted]156.35	Windows 7
23	bardela-0x5cf3fefe612781850a1e662ff0a5020f	v0.0.1	Brasil	[redacted]109.139	Windows V
29	seme-0x4e6472e9ecc04828af21dd12d6ca520a	v0.0.1	Brasil	[redacted].106.250	Windows 7
32	Ver_JoseRaimundo-0xb894a1938525171abf768ee8ce6536c5	v0.0.1	Brasil	[redacted].254.206	Windows X
38	ANNI-PC-0x7f6ffedd94cf2512b9a12ab1059d096e	v0.0.1	Brasil	[redacted].104.6	Windows 7
44	win 7-0x73c3235594d169b6ed6b474cdffaf73f	v0.0.1	Brasil	[redacted]102.209	Windows 7
46	USUARIO-0x4a29173752e53938e2ba6d90a92bf052	v0.0.1	Brasil	[redacted].253.16	Windows X
103	mmmmmmmmmmmmmmmmmmmmm-0xe76501c994a9602927d0f7af2648e4e8	v0.0.1	Brasil	[redacted]23.28	Windows 7
108	FEFE-0xd9ddd1c00a3841e314c62901f065036d	v0.0.1	Hungary	[redacted]94.65	Windows 7
121	Consigliere-0x5cfe7ebedd97f08bca2c6311371c7971	v0.0.1	Brasil	[redacted].171.172	Windows V
144	Pedro Henrique-0x8fd9b095dbb09cfab88a7fe1512b35c6	v0.0.1	Brasil	[redacted].103.171	Windows 7
149	ADAILTON-0xa74847e8d3f57355f85265c8c6ebf95f	v0.0.1	Brasil	[redacted].217.25	Windows X
164	cadu-0x7dea362b3fac8e00956a4952a3d4f474	v0.0.1	Brasil	[redacted].199.50	Windows 7
171	Khalifa-0x146fcb709b0820f23d9b62d039181537	v0.0.1	Brasil	[redacted].41.227	Windows 7
179	Familia-0xf8115ba1515049c9a3d8c4d81a4c00c4	v0.0.1	Brasil	[redacted]243.49	Windows 7
202	Ivanildo-0xd10679dc80caacdb36aacbef600a3556	v0.0.1	Brasil	[redacted].91.121	Windows 7

Botnet

Information	
[redacted]	Learning-0xac49b6c845368c5c9e582792bfcb7959
Version	[redacted]v0.0.1
Country	Brasil
Public IP / First access	189.50.[redacted]
Public IP / Last access	189.50.[redacted]
Internal IP	192.168.0.100
Subnet Mask	[255.255.255.0]
Install date	18-02-2014 15:22:548
Last access	18/02/2014 19:22:12
User name	Learning
System	Windows 7
Status	Online
Favorite	Add to favorites

Information about bank plugins		
Caixa Econômica Federal	Not installed	Mozilla Firefox
Banco do Brasil	Not installed	Google Chrome
Itaú	Not installed	Opera Browser
Others / ABN / UNI / Scopus	Not installed	Internet Explorer

Management
Remote Desktop (Print Screen / Remote Browser Control)
User Utilities (DLL Run / Download File / Upload File / Execute File)

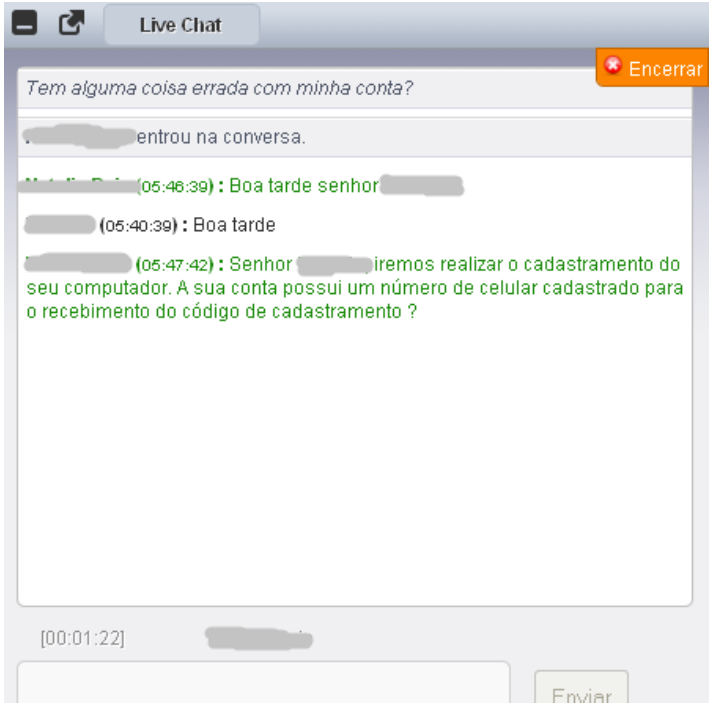
Atendimento ao vivo para os “clientes”

› CÓDIGO DE CADASTRAMENTO:

CADASTRAR

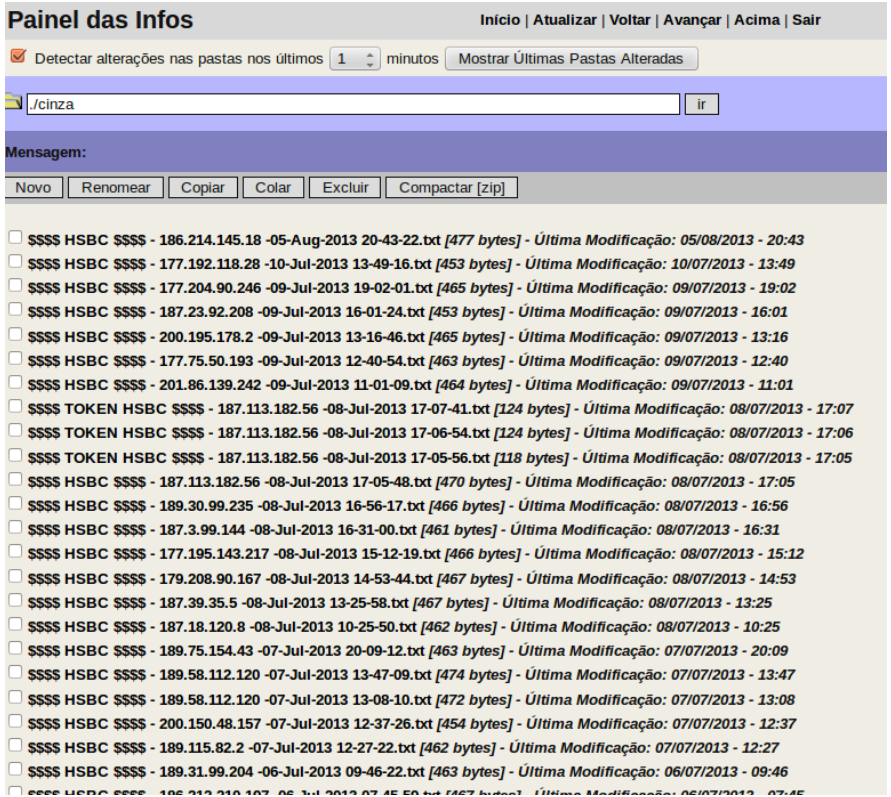
Nosso novo sistema de atendimento ao vivo, poderá sofrer alterações no horário de funcionamento, devido ao grande número de atendimentos decorridos durante o dia. Entretanto caso isso ocorra, um de nossos funcionários poderá ligar para finalizar o cadastramento.

Dia e Horário de Funcionamento: Segunda-Feira á Sexta-Feira - 09h:00 ás 22h:30.



Painel de Administração

Painel de Administração



Painel de Administração

Relatórios para análises

Dia : 2013-10-26 CMD-TV: G114 CMD-MV: N172 Gerar

Down_M - último refresh ás 04:56:21

Hora	Total / media	Versao	BR %	Outros %	Win 7 %	Vista %	Win XP %	ie6 %	ie7 %	ie8 %	ie9 %	Total/+3600/media
4:00	800/200	0	508 63%	292 36%	411 51%	24 03%	302 37%	56 07%	35 04%	363 45%	346 43%	0
3:00	1047/262	0	672 64%	375 35%	570 54%	33 03%	367 35%	77 07%	44 04%	438 41%	487 46%	0
2:00	1410/353	0	924 65%	486 34%	827 58%	49 03%	450 31%	94 06%	54 03%	561 39%	700 49%	0
1:00	1746/437	0	1179 67%	567 32%	1014 58%	52 02%	577 33%	122 06%	67 03%	704 40%	852 48%	0
0:00	2051/513	0	1411 68%	640 31%	1215 59%	62 03%	675 32%	142 06%	73 03%	828 40%	1007 49%	0

Conclusões e Projeções

- Impunidade = criminosos agem sem medo
- Uso de ferramentas personalizadas (criatividade)
- Reuso de código disponível na web
- Tendências: automatização, profissionalização, mercados estrangeiros
- Ainda há espaço para o crescimento de Internet Banking...

Vamos trocar informações técnicas!

Obrigado!

Ronaldo Lima

rplima.br@gmail.com

@crimescibernet

www.crimescicberneticos.com

Aline Bueno

alibueno@gmail.com

@alibueno

