



O mercado negro dos crimes cibernéticos no Brasil

Ronaldo Lima – Aline Bueno

O mercado negro dos crimes cibernéticos no Brasil

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

- A Febraban estima que fraudes eletrônicas tenham causado prejuízos de cerca de **R\$1.4 bilhão** 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 cibérneticos e bancos brasileiros









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

3 vibes

Infos CC | Milhas | Pontos...

his updates

- profile
- scraps
- photos
- videos
- testimonials

Actions

- Add as friend
- Ignore user
- Report abuse

-=[+]=- S3R14L -K1LL3R -=[+]=- [add as friend](#) [ignore](#) [report](#)

Infos CC | Milhas | Pontos Tam | Aprovações | Passagens Aéreas // Com Fê 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 Delphi VB

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

Enviadores Para Spam. (Ssh,Inbox,Smtp

Crypter's E Descriptors (Otimos Crypter Hacking

Virus TEF (Virus C/ Descriptor Negociavel

Trabalho Com Outros Tipos De Serviços Disponiveis No MSN

Contacto MSN Pessa Por Depoimento (Duvidas Envie Recado

advertisement

Microsoft

MANTENHA SUAS APLICAÇÕES SEMPRE FUNCIONANDO.

SAIBA MAIS >

Windows Server 2012

NASCIDO PARA NUVEM.

friends (889)

search friends

Adriano	bruno	[MOD]
Upgrade Velox	\$) Juuh	Dick Viganista
willian	\$ jones	marcos

communities (198)

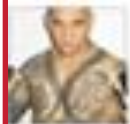
search communities

--	--	--



M
M
m
Li

35



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 infoce na hora <http://o-rei-das-ap...>




YOUTUBE.COM

Like · Comment · Share

Doação pela internet

Ajude a mudar a história de milhares de crianças e jovens brasileiros.
Faça sua doação.

Aqui no site você pode doar o ano inteiro. Escolha a melhor opção para você:

Cartão de crédito  Mastercard  Diners  VISA Visa

Cartão de débito  Visa Electron (apenas para cartões Bradesco)

Débito em conta  Banco do Brasil

Boleto bancário  Pagável em qualquer banco

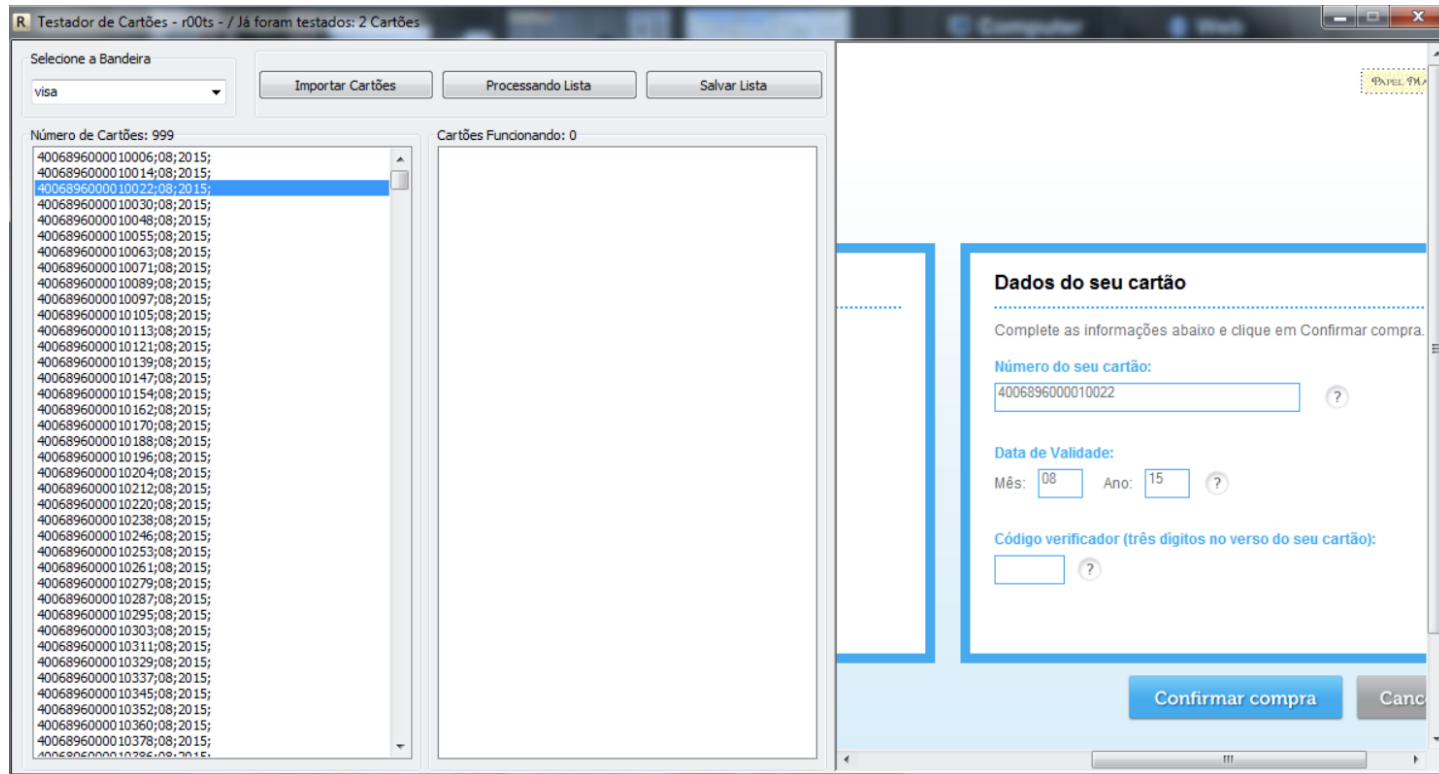
Preencha o formulário abaixo. Os campos com * são de preenchimento obrigatório.

Pais*

Valor da doação* valor mínimo: R\$ 15,00

Nome completo*

Email*



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 Adquirir a senha

Caso o login seja Efetuado com sucesso
Notas

Login
Password
Saldo Disponível
A receber
Bloqueado
Tipo de Conta / Verificada ou Não Verificada
Pontuação

OBS: No video mostra o Passo a Passo

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: antraxcoder@gmail.com

Skype: [antraxcoder](https://www.skype.com/people/antraxcoder)

ICQ:: [1004100000](https://www.icq.com/contacts/1004100000)

Segue o video abaixo :




Suggested Sites Web Slice Gallery

Venda de crypters


LOJA CARRINHO FINALIZAR COMPRA MINHA CONTA

LOJA
Mostrando todos 2 resultados

Ordenar por mais novos



Crypter 2.3
R\$15.00
[Comprar](#)



Crypter 2.2
R\$15.00
[Comprar](#)

Orgulhosamente mantido com WordPress

Compartilhar 0 mais Próximo blog»

INFO CC

[Início](#) [CONTATO](#) [QUEM SOMOS](#) [PRODUTOS](#)

PRODUTOS

Vendemos lotes com no minimo 10 pecas.

Lote com 10 platinum R\$1500,00 CONSULTADAS
Lote com 10 Gold R\$2000,00 CONSULTADAS
Lote com 10 mix R\$1000,00 (ccs variadas, não consultada, limite desconhecido)

Temos melhores valores para maiores quantidades, consulte-nos!
Consulte-nos por e-mail,
...@gmail.com

PVC

Cobramos 30% do valor disponivel em conta, para vender os dados da conta.
cobramos 40% para emitir o pvc e vc receber em seu endereco.
Consulte-nos por e-mail,
...@gmail.com

	Bronze	Silver	Gold	Platinum	Ultimate
Boot Maximo	300 segundos	450 segundos	600 segundos	1000 segundos	3600 segundos
Attacks	<i>ilimitado</i>	<i>ilimitado</i>	<i>ilimitado</i>	<i>ilimitado</i>	<i>ilimitado</i>
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	<i>ilimitado</i>	<i>ilimitado</i>	<i>ilimitado</i>	<i>ilimitado</i>	<i>ilimitado</i>
Suporte Fullt	✓	✓	✓	✓	✓
SSYN	✓	✓	✓	✓	✓
Ataque UDP	✓	✓	✓	✓	✓
	VALOR R\$40	VALOR R\$60	VALOR R\$85	VALOR R\$150	VALOR R\$250

```
Apr 02 10:49:54 < [redacted] > VENDO INFECT 0,80 CADA ENTRA NA MESMA HORA, INFECT DE QUALIDADE DIFERENCIADOS http://s8.postimg.org/suhkvrl51/hora.jpg
Apr 02 10:49:56 < [redacted] > LIMPO KL REMOTA, LOADER, BINARIOS ETC... DEIXO 100% INDETECTAVEL DE TODOS ANTIVIRUS https://www.youtube.com/wat [redacted] VA
Apr 02 10:50:58 < [redacted] > J0seC4rl0sVenancioJunior cde mano?
Apr 02 10:53:35 < [redacted] > Compro infos cef pago adiantado, agora só me venha no pvt se tiver OTIMAS Referencia.
Apr 02 10:54:12 < [redacted] > referência é meu pau duro.
Apr 02 10:54:27 < [redacted] > coloca no teu cú kkk
Apr 02 10:55:25 < [redacted] > VENDOOW OW NEGOCIOOO TELA BRADESCO 2014 E CIELO NEYMAR 2014..!!!!!!!.OUTRO POR SMTP VPS.

Apr 22 15:16:32 < [redacted] > VENDO REMOTA 500 SEMANAL
Apr 22 15:16:41 < [redacted] > se vc ta me ofendendo e eu nao te conheço é pq entra aki e ja deve ter trocado de nick umas 100 vezes
Apr 22 15:16:44 < [redacted] > kkkkkkkkkkkk
Apr 22 15:17:01 < [redacted] > O.o
Apr 22 15:17:06 < [redacted] > que comediação da porra
Apr 22 15:17:06 < [redacted] > VENDO ENG PRIV8 25,00

May 08 18:55:09 < [redacted] > vendo ssh enviando! 100,00! vendo scans! todo tipo, tenho todos =)
May 08 18:55:26 < [redacted] > Vendo infects - 2$/infect - Encomenda minima 500 infects - Pagamento adiantado.

May 09 12:29:23 < [redacted] > Card cef aqui pra trf doc interessados pvt
May 09 12:31:23 < [redacted] > Vendo: lista (wab ou hot), fakes (desco, cielo, americanas) por $$
May 09 12:31:48 < [redacted] > Vendo: lista (wab ou hot), fakes (desco, cielo, americanas todas com sistema anti-phishing 100% garantido por mim) por $$
May 09 12:31:53 < [redacted] > Vendo: lista (wab ou hot), fakes (desco, cielo, americanas todas com sistema anti-phishing 100% garantido por mim) = $$
May 09 12:31:55 < [redacted] > Vendo: lista (wab ou hot), fakes (desco, cielo, americanas todas com sistema anti-phishing 100% garantido por mim) = $$
```

Autor

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

0 Membros e 1 Visitante estão vendo este tópico.

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 licença por mês: \$150 (dólares)

Custo da licença por ano: \$1000 (dólares)

Forma de pagamento aceita: BitCoin



CRYPTER
VENDAS DE INFOCC

INFINITE = 140
CORPORATE = 140
PURCHASING = 120
PLATINUM = 100
BUSINESS = 140
PREMIER = 80
GOLD = 60

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\$


```
[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
```

[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

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

ConnectionString

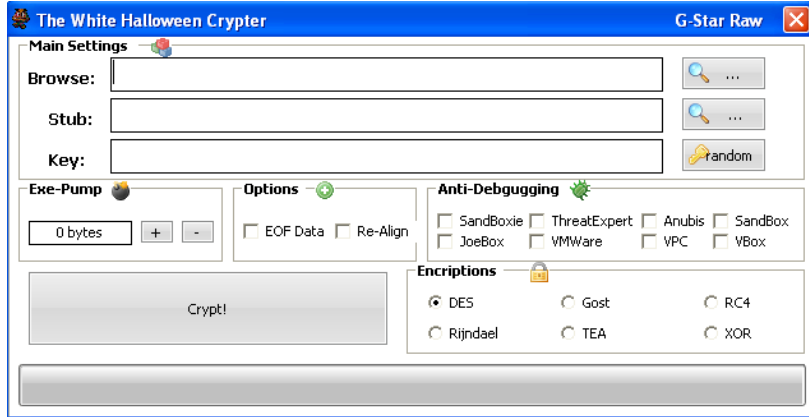
```
Provider=SQLOLEDB.1;Password=_____;Persist Security Info=True;User ID=_____;Initial Catalog=_____;Data Source=_____.com  
SQLOLEDB.1
```

- Linguagens:
 - + populares: Delphi, Visual Basic, PHP
 - usos específicos: Applet Java (drive by download), Autolt (crypters)

- FWC: Atenção, recadastramento de segurança Banco do Brasil. 11/12/2013 02:24:07

The screenshot shows a Mozilla Firefox browser window. The address bar displays the URL: <https://www.google.com.br/search?q=ares&oq=ares&aqs=chrome..69i57j5j0l2j69it>. The search results for 'skype' are visible, including a link to 'Baixe Skype6.0 - Download' and 'Baixe o Skype para o seu celular - Sua casa - T'. An 'Adobe Flash Player 11.5.502.16' download dialog is open, with buttons for 'Baixe agora' and 'Baixe depois'. The background shows the Lancenet website with a 'CAMPEONATO BRASILEIRO' banner and navigation links like 'HOME', 'FUTEBOL', and 'FUT: INTER'.





Sistema de envio de emails. Seleccione ao lado o sistema de envio, caso o sistema escolhido não funcione tente os outros.

	SMTP	<input checked="" type="radio"/>
	MAIL	<input type="radio"/>
	SENDMAIL	<input type="radio"/>

Estamos testando.

+BYSCR3ZY+

De / e-mail :

Assunto: Fw: Sr(a), %EMAIL% Seu Sistema de Segurança_BB esta De

Código HTML:

```
Digitos.</FONT><FONT size=2><BR>Remova ou crie sua  
senha da central de Atendimento no Link de atendimento  
abaixo.<BR></FONT><BR>  
<BR>  
<A href="http://www.events.com.sg/includes/_vji_cnf/Adesao.php#Recadastramento">  
[Recadastrando  
Cliente - BB]</A></SPAN></DIV>  
<DIV><SPAN  
style="FONT-FAMILY: Arial; COLOR: rgb(0,0,153); FONT-WEIGHT: bold"></SPAN><FONT
```

***Lembrete: texto em HTML**

Coloque o email de suas vítimas abaixo:

OBS: um e-mail em cima do outro

***Separado por quebra de linha**

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

The screenshot shows the Sugador application interface. On the left, a list of email addresses is displayed in a scrollable window. The main area shows a list of extracted data, including phone numbers and names. On the right, a Submarino login page is visible, featuring the company logo and a message indicating that the user's email has been blocked due to too many failed login attempts. The interface includes buttons for 'Load', 'Pegar CC', 'Next', 'Export', and 'End' at the bottom.

806	5		
easegantini@msn.com	lar123	5390290262343340	013;Joao Paul
eattizani@bol.com	271	4984017017808789	016;DAYAN S.
ebazarin@yahoo.com	sw1721	5274970126688847	015;Eduardo P
ebbarbosa@gmail.com	uProximus	5148953000367427	014;OTAVIO V
ebbmjr@gmail.com		5324730009588526	014;LUIS EDU.
eberfemando@gmail.com	n;e9190203		
eberk9@gmail.com	alk9		
ebemer@best.com	456e		
eberton.fagundes@terra.com.br	l.com.fagundes		
ebihl@terra.com.br	tica		
ebinhobike2@terra.com.br	ebinhobike		
ebordin@comp.br	n.br;celular		
ebrisa@terra.com.br	ne		
ebtrjr@yahoo.com	taeseis		
ebroering@gmail.com	ra		
ebuturi@uol.com.br	9eb		
ebx.entregas@gmail.com	1;12qwaszxc		
ecalixto@terra.com.br	1		
ecartunes2004@gmail.com	m.br;mindbike		
ecaporto@gmail.com	:80		
ecassinelli@riojaneiro.com.br	:ony1990		
eccf@hotmail.com			
ecdlopes@yahoo.com	159017		
ecelelem@uol.com.br	lani		
ecfnog@gmail.com	:9		
eclesiamesias@gmail.com	1;141100		
ecletica19@hotmail.com	ort9		

Principal

Site

Antigo Ingressos.com

Novo Ingressos.com

C:\Users\... Des...

Carregar Lista

Iniciar... 8

Status

Lendo 0 de 1560

Capturados: 0

ingresso.com

Life Essential Design

SALAS COMERCIAIS DE 34 A 75 M²

ÓTIMO INVESTIMENTO NA BARRA FUNDA

São Paulo ▾

Atendimento | Televentas 4003-2330 (Exceto Cinema)

Minha Conta | Meus Ingressos | Sair

Cinema | Teatro | Show | Circo | Promoção

Cadastro

Dados de Acesso:

Conectar com Facebook

Email* leonardoliporoni@yahoo.com.br

Developer by Kernel

Virus PLugin Chrome

Pessoal esta a venda um keylogger 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 infoc 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

Painel Retorno Plugin Google

BB Cef Logins Contador

Atualizar Backup 192.168.2.1 64.237.36.106 Exporta Somente Selecionado 1515 encontrados

IP	Data	Site	Login	Cont	Site	
179	8.157	Set 12 2013 12:59PM	www.facebook.com	gustavo...er@gmail.com	1	www8.tjmg.jus.br
179	8.157	Set 12 2013 12:59PM	www.facebook.com	gustavo...er@gmail.com	1	www8.receita.fazenda.gov.br
179	8.157	Set 12 2013 12:59PM	www.facebook.com	msndog...lva@hotmail.com	1	www3.prefeitura.sp.gov.br
200	3.62	Set 12 2013 12:53PM	detran.sp.gov.br	291.53	1	www3.catho.com.br
186	7.220	Set 12 2013 12:52PM	aprendiz.espro.org.br	365.11	1	www3.bcb.gov.br
186	1.78	Set 12 2013 12:51PM	www.xconto.com.br	maylan...il.com	3	www2.walmart.com.br
189	1.90	Set 12 2013 12:49PM	www.facebook.com	gustavo...tmail.com	1	www2.saude.ai.gov.br
189	7.225	Set 12 2013 12:43AM	www.facebook.com	marcioc...nior@gmail.com	9	www2.bancobrasil.com.br
189	03	Set 12 2013 12:39PM	www.facebook.com	alaide...hotmail.com	13	www2.bancobrasil.com.br
200	3.62	Set 12 2013 12:33PM	www.detran.sp.gov.br	291.53	1	www2.bancobrasil.com.br
187	12.160	Set 12 2013 12:33AM	www.facebook.com	cinthya...tmail.com	2	www17.senado.gov.br
200	3.62	Set 12 2013 12:32PM	www.detran.sp.gov.br	291.53	1	www.xconto.com.br
192	3.251	Set 12 2013 12:19AM	ref	user	1	www.xconto.com.br
200	3.62	Set 12 2013 12:18PM	detran.sp.gov.br	291.53	2	www.webcheats.com.br
189	1.228	Set 12 2013 12:06PM	www.facebook.com	clauder...@hotmail.com	2	www.wcm777.com
189	3.76	Set 12 2013 12:02PM	www.facebook.com	rafael...@gmail.com	1	www.wbstool.com
179	10.107	Set 12 2013 12:00PM	premier.ticketsforfun.com.br	rapozol...n.br	1	www.voceopina.com.br
189	1.120	Set 12 2013 11:53AM	www.aasn.com.br	116931	1	www.vitacnet.com.br



[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

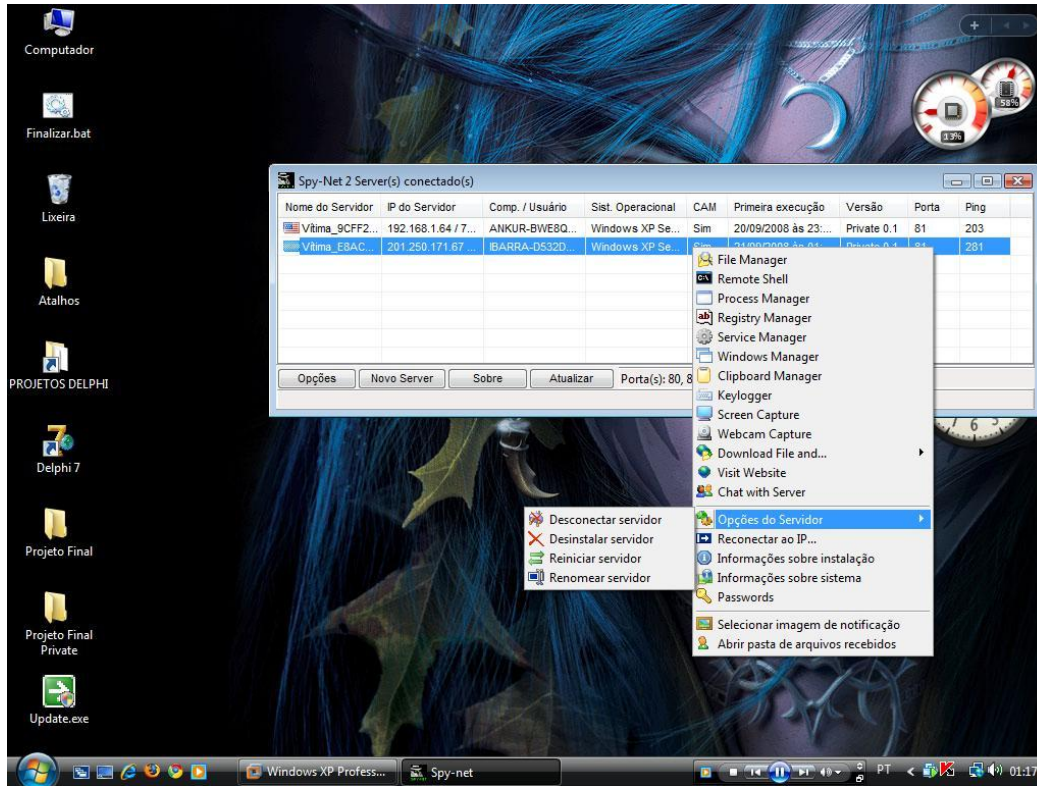
30.09.2008, 16:30

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



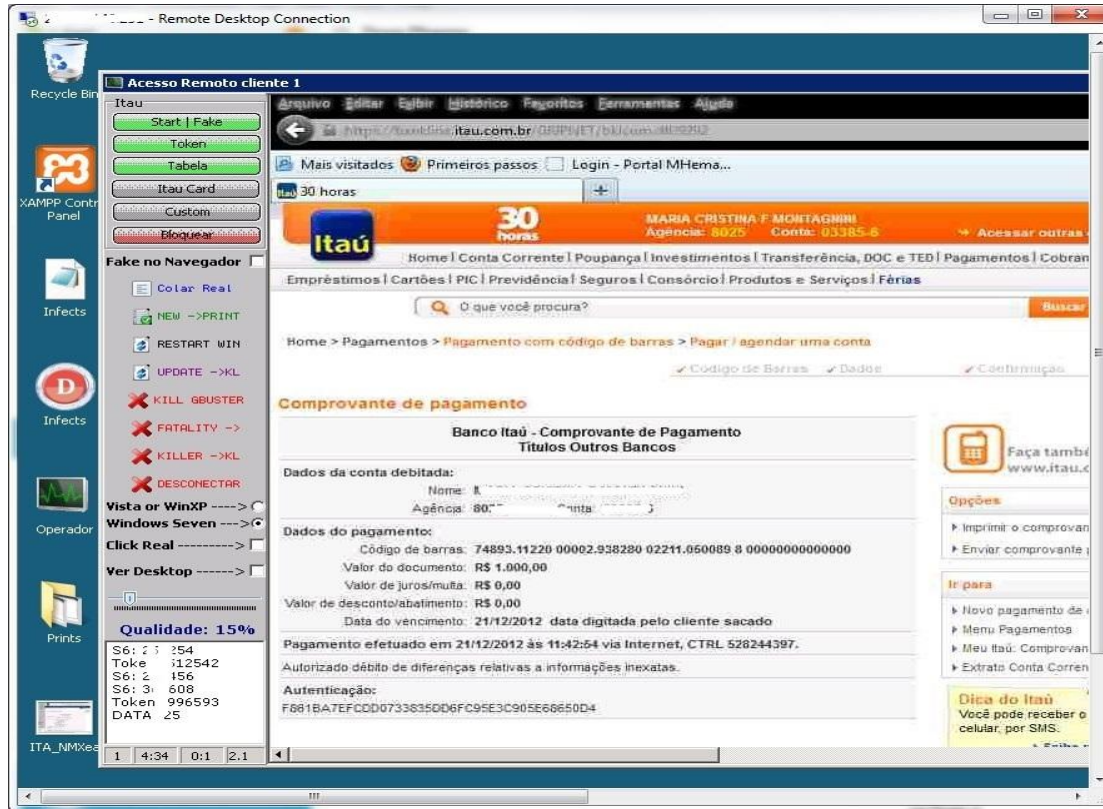
Spy Net RAT

The screenshot displays the Spy-Net 2.6 interface. The main window is titled "Spy-Net 2.6" and contains a table of infected computers. The table has columns for "ULKE" (Country), "ISIM" (Name), "COMPUTER / USER", "CAM", "OS", and "CPU". Below the table, it shows "ONLINE SAYISI: 29" and "ACIK OLAN PORTLAR: (80) (82)".

ULKE	ISIM	COMPUTER / USER	CAM	OS	CPU
Turkey	deniz...	PC-BILGAYAR/Pc	<input checked="" type="checkbox"/>	Windows 7 Home Basic (Bul...	Intel(R) Co
Brazil	deniz...	TONYDOUGLAS-P...	<input checked="" type="checkbox"/>	Windows 7 Ultimate (Build: 7...	Pentum/R
Brazil	deniz...	TORRES-AFABSD3...	<input checked="" type="checkbox"/>	Windows XP Professional (...)	Intel(R) Pe
Turkey	deniz...	A-1ADD92D1A7DE...	<input checked="" type="checkbox"/>	Windows XP Home (Build: 2...	Intel(R) Pi
Turkey	deniz...	SAD/sajd	<input checked="" type="checkbox"/>	Windows XP Professional (...)	Intel(R) Pi
Brazil	deniz...	ELELSON-PC/Elel...	<input checked="" type="checkbox"/>	Windows 7 Ultimate (Build: 7...	Intel(R) Ce
Brazil	deniz...	CAIO-PC/Caio	<input checked="" type="checkbox"/>	Windows 7 Home Basic (Bul...	AMD Athlo
Turkey	deniz...	SANALADAM/Sanal	<input checked="" type="checkbox"/>	Windows 7 Ultimate (Build: 7...	AMD Athlo
Turkey	deniz...	PC-USER/puser	<input checked="" type="checkbox"/>	Windows XP Professional (...)	Pentium/R
Turkey	deniz...	MURATACMAZ/mur...	<input checked="" type="checkbox"/>	Windows XP Home (Build: 2...	Intel(R) Co
Turkey	deniz...	MUSTAFA-PC/Must...	<input checked="" type="checkbox"/>	Windows 7 Premium (Build: ...)	Intel(R) Co
Turkey	deniz...	ADIGE/saraha	<input checked="" type="checkbox"/>	Windows 7 Ultimate (Build: 7...	AMD Phen
France	deniz...	HP-PC/amal	<input checked="" type="checkbox"/>	Windows 7 Ultimate (Build: 7...	Pentium/R
Denmark	deniz...	JESPERPEDERSEN/...	<input checked="" type="checkbox"/>	Windows 7 Starter (Build: 7...	Intel(R) Ab
Denmark	deniz...	VLRAØGIVNING-P...	<input checked="" type="checkbox"/>	Windows Vista Premium (Bu...	AMD Turio
Turkey	deniz...	ASUS-142844734...	<input checked="" type="checkbox"/>	Windows XP Professional (...)	Intel(R) Co
Turkey	deniz...	RECEKÖSE-PC/RE...	<input checked="" type="checkbox"/>	Windows 7 Premium (Build: ...)	Intel(R) Co
Turkey	deniz...	SABRY-PC/SABRY	<input checked="" type="checkbox"/>	Windows Vista Home Basic (...)	Pentium/R

Below the table, it shows "ONLINE SAYISI: 29" and "ACIK OLAN PORTLAR: (80) (82)".

The interface also features several active camera feeds. The top right window shows a camera feed titled "deniz_000000DE --- KAMERA GORU...". Below it are two more camera feeds: "deniz_DA16813A --- KAMERA GORU..." and "deniz_9495B01D --- EKRAN GORUNT...". At the bottom, there are three more camera feeds: "deniz_8239205F --- KAMER...", "deniz_00000039 --- KAMER...", and "deniz_D8D135D6 --- KAMER...". Each camera feed includes controls for "BASLA" (Start), "DURDUR" (Stop), "SURE" (Sure), "KALITE" (Quality), and "KAYDET" (Record).



189.19.89.26 -> [BRADESCO] | by *****

BLOCKED: BLOCKEDBRD
TOKEN: 407051
CLIENTE TRAVADO

E-mail: valedov@bradesco.com.br
Perfil: Perfil Master
Último acesso: 07/10/2013 - 15h03
Nº de Acesso: 587

Autorizações

- > 0 Pendentes
- > 0 Pendentes para a Empresa
- > Recusões e Expirados
- > Autorizadas

Saldo Disponível (R\$)

Conta: CC

Total dos Saldos

Disponível

Limites

Cheque Flex Pessoa Jurídica

Limite Rotativo Flex Pessoa Jurídica

> Ver saldos de todas as contas

14/10 | 15:07:02 > Atualizar

Comprovante de Transação Bancária
Boletos de Cobrança
Data de operação: 14/10/2013 - 15h06
Nº de controle: 375.067.031.474.782.056 | Documento: 0001692

Bradesco
Net Empresa

Conta do débito: Agência: | Conta: | Tipo: Conta-Corrente

Empresa: | CNPJ: /0001-10

Código de barras: 34101 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

sT7dmVEX qhgNwWu3 7K0L0N3D 30Fbo2Y0 28J011Pg RuRdqgQv vT9x0*ea L0N0QR6R
 ZyYVYlg5 zh8RgTy5 eBSCfmL Hth47NDD aw45eH2g ogQu*rg9 C9jFoxPK Y*MB0wr*
 2k9n44eV qm0Lb0x ChoRb0p0 0JWfNt* gAPD5dax 9rUSIF0V 14911193 06790121

The screenshot displays a remote desktop environment. The main window is an Internet Explorer browser showing the Unimed website. The browser's address bar contains the URL `http://www2.unimedpponline.com.br/Default.aspx`. The website header includes the Unimed logo and the text "SISTEMA ON-LINE". Below the header, the user's login information is displayed: "Login: 302 - Nome: CENTRO PRUDENTINO DE IMAGEM S/C LTA" and "IP: 192.168.1.156".

The main content area of the website features a red banner with the text: "MÉDICOS COOPERADOS QUE SE ENCONTRAM DE FÉRIAS DE 18/11/2013 ATÉ O DIA 17/12/2013". Below this, a list of doctors is shown, including DR. ANTONIO FELICI, DR. AYRES J. CONCALVES PINELLI, DR. CESAR HEINRIQUE BATISTA FREDERICO, DR. DARCY NOVELLI JUNIOR, DR. EMERSON ITIKAWA, DR. EROS PUELIO SOARES HOGUEIRA, DR. EUIES CARLOS DE ALMEIDA, DR. FERNANDO SPINOZA SESTI, DR. FLAVIO PORTO FRANCO PIOLA, DRA. FLORA SUMIKO SAENARA YAMAZAKI, DR. HAROLDO PEDRINI, DR. JOAO CLAUDIO DA PAIXAO, DR. JOSE DIAS JUNIOR, DRA. MARY MARTINS HERY, DR. MASSAKAZU KAKITANI, DR. MILTON CAMILO RODRIGUES JUNIOR, and DRA. HEUSA JERONIMO P. FINGERHUT.

Below the doctor list, there is a section titled "Concurso Hospital Estadual" and a red banner that says "MENSAGENS IMPORTANTES". A date "13/09/2013" is visible, along with a message addressed to "Prezada secretaria(o)" stating that medical services at Unimed de Paranaíba are suspended and that urgent/emergency cases will be attended to.

The desktop environment includes a taskbar with the "Iniciar" button and several open applications, including "SisClínica 2000". The system tray shows the time as 15:28 and the language set to PT. On the right side of the desktop, there is a vertical panel with various utility icons, including "Abrir HSBC", "Abrir Itaú", "Abrir Desco", "Abrir SICREDI", "LIBERA NAV", "KILLA ALL NAV", "Reinstala DLL", "Limpa Info", "Instala Java", "Patch Remoto", "Killa Link", "Restaura GB", "Ativa Link", "Desativa CH+Alt+Del", "Conectar", "Reinicia Remoto", "Ativa CH+Alt+Del", "Desconectar", "Desativar Remoto", "Desativa UAC", and "Parar Som".

[»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



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

#		Version	Country	IP	SO
21	Learning-0xac49b6c845368c5c9e582792bfc7959	v0.0.1	Brasil	156.35	Windows 7
23	bardela-0x5df3fefe612781850a1e662ff0a5020f	v0.0.1	Brasil	109.139	Windows V
29	seme-0x4e6472e9ecc04828af21dd12d6ca520a	v0.0.1	Brasil	5.106.250	Windows 7
32	Ver_JoseRaimundo-0xb894a1938525171abf768ee8ce6536c5	v0.0.1	Brasil	3.254.206	Windows X
38	ANNI-PC-0x7f6ffedd94cf2512b9a12ab1059d096e	v0.0.1	Brasil	2.104.6	Windows 7
44	win 7-0x73c3235594d169b6ed6b474cdfaf73f	v0.0.1	Brasil	102.209	Windows 7
46	USUARIO-0x4a29173752e53938e2ba6d90a92bf052	v0.0.1	Brasil	3.253.16	Windows X
103	mmmmmmmmmmmmmmmmmmmm-0xe76501c994a9602927d0f7af2648e4e8	v0.0.1	Brasil	23.28	Windows 7
108	FEFE-0xd9ddd1c00a3841e314c62901f065036d	v0.0.1	Hungary	94.65	Windows 7
121	Consigliere-0x5cfe7ebedd97f08bca2c6311371c7971	v0.0.1	Brasil	9.171.172	Windows V
144	Pedro Henrique-0x8fd9b095dbb09cfab88a7fe1512b35c6	v0.0.1	Brasil	3.103.171	Windows 7
149	ADAILTON-0xa74847e8d3f57355f85265c8c8ebf95f	v0.0.1	Brasil	1.217.25	Windows X
164	cadu-0x7dea362b3fac8e00956a4952a3d4f474	v0.0.1	Brasil	7.199.50	Windows 7
171	Khalifa-0x146fcb709b0820f23d9b62d039181537	v0.0.1	Brasil	9.41.227	Windows 7
179	Familia-0xf8115ba1515049c9a3d8c4d81a4c00c4	v0.0.1	Brasil	243.49	Windows 7
202	Ivanildo-0xd10679dc80caacdb36aacbef600a3556	v0.0.1	Brasil	1.91.121	Windows 7

Information	
	Learning-0xac49b6c845368c5c9e582792bfc7959
Version	 v0.0.1
Country	 Brasil
Public IP / First access	189.50. 
Public IP / Last access	189.50. 
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”

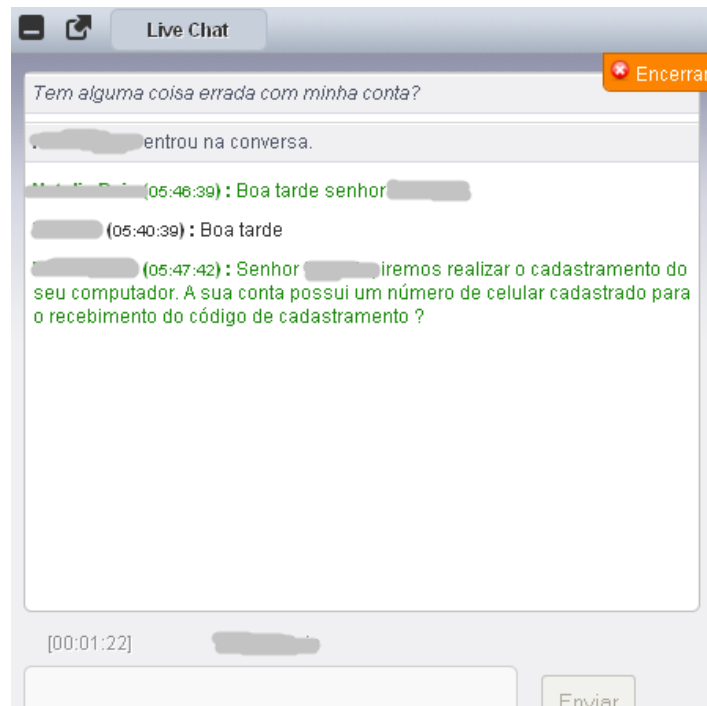
> CÓDIGO DE CADASTRAMENTO:

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 à Sexta-Feira - 09h:00 às 22h:30.





Painel das Infos Início | Atualizar | Voltar | Avançar | Acima | Sair

Detectar alterações nas pastas nos últimos minutos

Mensagem:

- \$\$\$\$ HSBC \$\$\$\$ - 186.214.145.18 -05-Aug-2013 20-43-22.txt [477 bytes] - Última Modificação: 05/08/2013 - 20:43
- \$\$\$\$ HSBC \$\$\$\$ - 177.192.118.28 -10-Jul-2013 13-49-16.txt [453 bytes] - Última Modificação: 10/07/2013 - 13:49
- \$\$\$\$ HSBC \$\$\$\$ - 177.204.90.246 -09-Jul-2013 19-02-01.txt [465 bytes] - Última Modificação: 09/07/2013 - 19:02
- \$\$\$\$ HSBC \$\$\$\$ - 187.23.92.208 -09-Jul-2013 16-01-24.txt [453 bytes] - Última Modificação: 09/07/2013 - 16:01
- \$\$\$\$ HSBC \$\$\$\$ - 200.195.178.2 -09-Jul-2013 13-16-46.txt [465 bytes] - Última Modificação: 09/07/2013 - 13:16
- \$\$\$\$ HSBC \$\$\$\$ - 177.75.50.193 -09-Jul-2013 12-40-54.txt [463 bytes] - Última Modificação: 09/07/2013 - 12:40
- \$\$\$\$ HSBC \$\$\$\$ - 201.86.139.242 -09-Jul-2013 11-01-09.txt [464 bytes] - Última Modificação: 09/07/2013 - 11:01
- \$\$\$\$ TOKEN HSBC \$\$\$\$ - 187.113.182.56 -08-Jul-2013 17-07-41.txt [124 bytes] - Última Modificação: 08/07/2013 - 17:07
- \$\$\$\$ TOKEN HSBC \$\$\$\$ - 187.113.182.56 -08-Jul-2013 17-06-54.txt [124 bytes] - Última Modificação: 08/07/2013 - 17:06
- \$\$\$\$ TOKEN HSBC \$\$\$\$ - 187.113.182.56 -08-Jul-2013 17-05-56.txt [118 bytes] - Última Modificação: 08/07/2013 - 17:05
- \$\$\$\$ HSBC \$\$\$\$ - 187.113.182.56 -08-Jul-2013 17-05-48.txt [470 bytes] - Última Modificação: 08/07/2013 - 17:05
- \$\$\$\$ HSBC \$\$\$\$ - 189.30.99.235 -08-Jul-2013 16-56-17.txt [466 bytes] - Última Modificação: 08/07/2013 - 16:56
- \$\$\$\$ HSBC \$\$\$\$ - 187.3.99.144 -08-Jul-2013 16-31-00.txt [461 bytes] - Última Modificação: 08/07/2013 - 16:31
- \$\$\$\$ HSBC \$\$\$\$ - 177.195.143.217 -08-Jul-2013 15-12-19.txt [466 bytes] - Última Modificação: 08/07/2013 - 15:12
- \$\$\$\$ HSBC \$\$\$\$ - 179.208.90.167 -08-Jul-2013 14-53-44.txt [467 bytes] - Última Modificação: 08/07/2013 - 14:53
- \$\$\$\$ HSBC \$\$\$\$ - 187.39.35.5 -08-Jul-2013 13-25-58.txt [467 bytes] - Última Modificação: 08/07/2013 - 13:25
- \$\$\$\$ HSBC \$\$\$\$ - 187.18.120.8 -08-Jul-2013 10-25-50.txt [462 bytes] - Última Modificação: 08/07/2013 - 10:25
- \$\$\$\$ HSBC \$\$\$\$ - 189.75.154.43 -07-Jul-2013 20-09-12.txt [463 bytes] - Última Modificação: 07/07/2013 - 20:09
- \$\$\$\$ HSBC \$\$\$\$ - 189.58.112.120 -07-Jul-2013 13-47-09.txt [474 bytes] - Última Modificação: 07/07/2013 - 13:47
- \$\$\$\$ HSBC \$\$\$\$ - 189.58.112.120 -07-Jul-2013 13-08-10.txt [472 bytes] - Última Modificação: 07/07/2013 - 13:08
- \$\$\$\$ HSBC \$\$\$\$ - 200.150.48.157 -07-Jul-2013 12-37-26.txt [454 bytes] - Última Modificação: 07/07/2013 - 12:37
- \$\$\$\$ HSBC \$\$\$\$ - 189.115.82.2 -07-Jul-2013 12-27-22.txt [462 bytes] - Última Modificação: 07/07/2013 - 12:27
- \$\$\$\$ HSBC \$\$\$\$ - 189.31.99.204 -06-Jul-2013 09-46-22.txt [463 bytes] - Última Modificação: 06/07/2013 - 09:46
- \$\$\$\$ HSBC \$\$\$\$ - 185.213.213.107 -06-Jul-2013 07-45-50.txt [467 bytes] - Última Modificação: 06/07/2013 - 07:45

Relatórios para análises

Dia : 2013-10-26

CMD-TV: G114

CMD-MV: N172

Gerar

Down_M - último refresh às 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

- 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.crimesciberneticos.com

Aline Bueno

alibueno@gmail.com

@alibueno