

Fraude via e-mail por meio de Cavalos de Tróia e Clonagem de sites financeiros

Marcelo Lau
marcelo.lau@poli.usp.br



12/11/2004

Agenda

- Modelagem do problema
- Análise do SCAM
- Ferramentas de análise
- Análise do PHISHING
- Informações na Internet
- Considerações finais

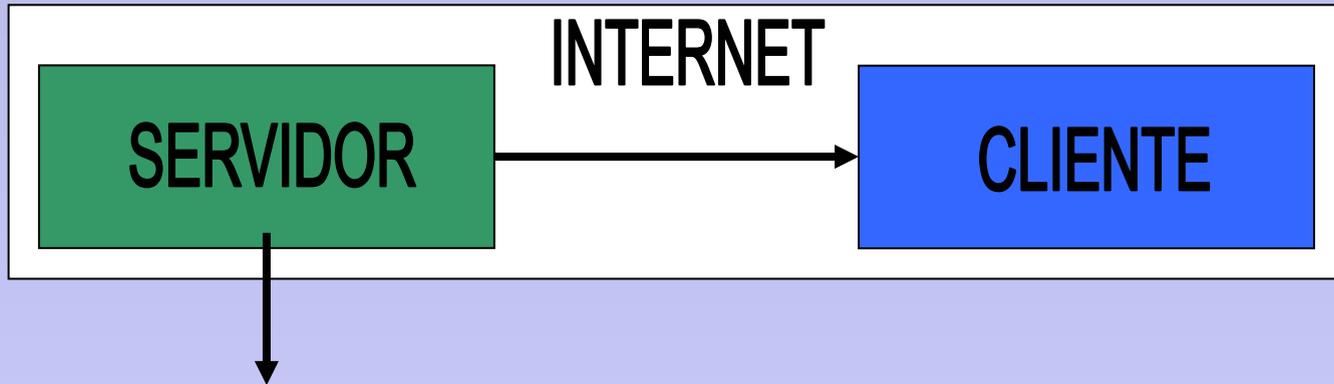


Modelagem do problema



Modelagem do problema

Disponibilização do serviço

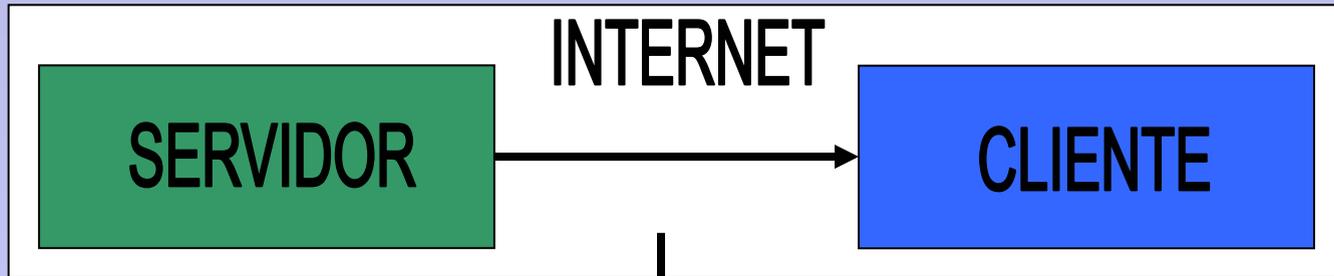


A porção Servidor disponibiliza o acesso ao serviço transacional (financeiro). Este ambiente em geral é uma interface de acesso a dados e transações que são armazenadas em outros ambientes ou sistemas.

Nível de proteção do ambiente : MÉDIO / ALTO

Modelagem do problema

Disponibilização do serviço



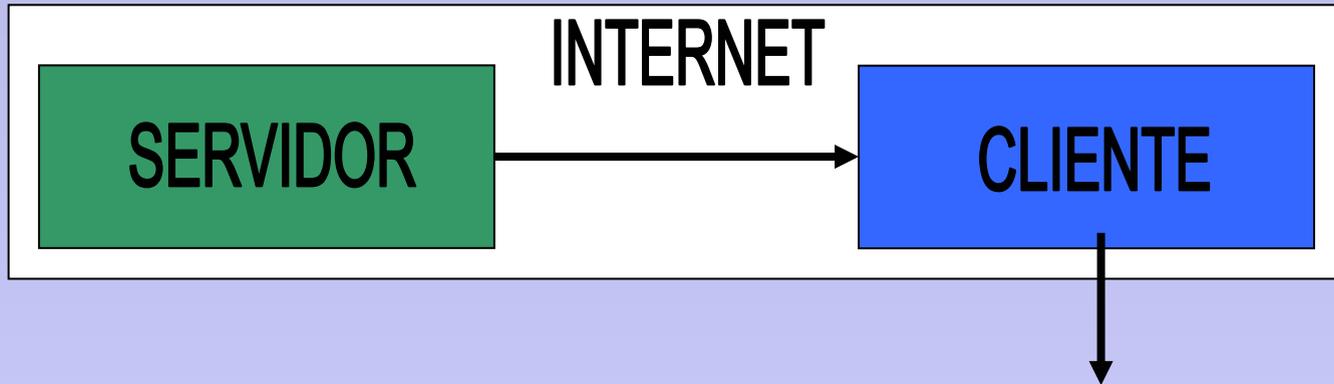
A linha de comunicação utiliza protocolo de comunicação HTTPS. A confidencialidade é garantida através de chaves assimétricas RSA de 1024 bits. (E chaves de sessão simétricas de 40 e 128 bits)

Nível de proteção do ambiente : MÉDIO* / ALTO

* Elementos de comunicação / Serviço de DNS

Modelagem do problema

Disponibilização do serviço

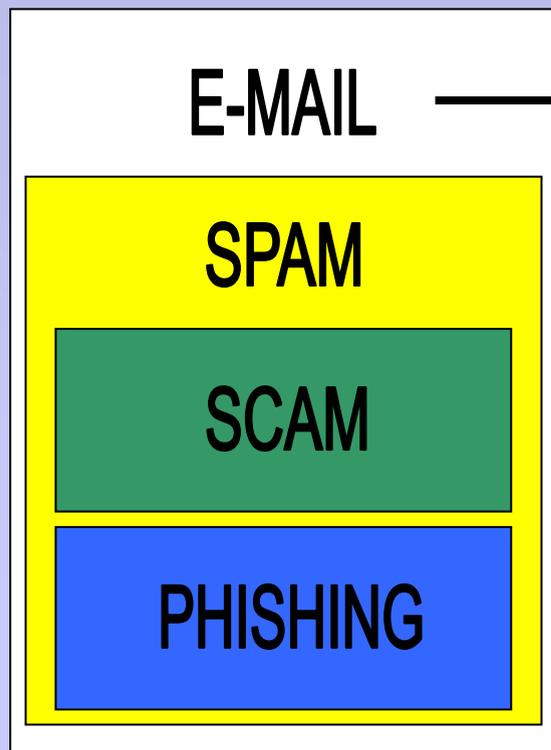


A porção Cliente é a interface utilizada para a realização de transações financeiras e acesso a outros serviços no ambiente Internet. Browser e Sistema Operacional são os principais itens do cliente.

Nível de proteção do ambiente : BAIXO

Modelagem do problema

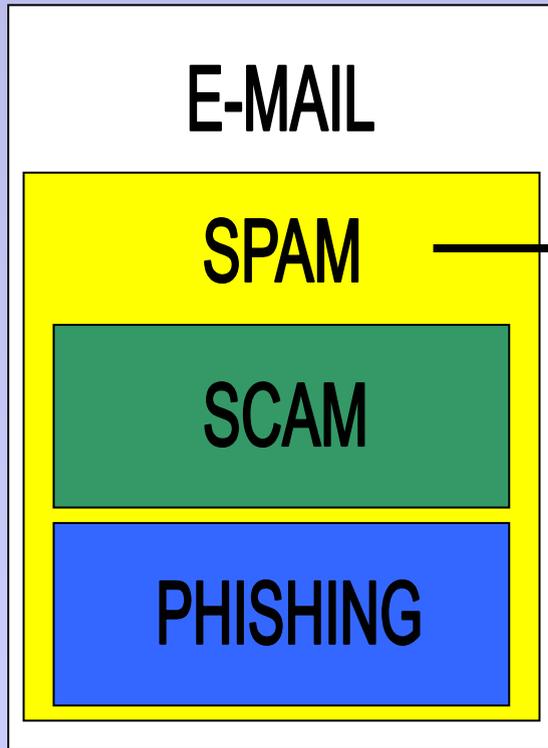
Vetor de Propagação



As fraudes que hoje atingem clientes de instituições financeiras apresentam como único vetor de propagação as mensagens eletrônicas. Não podemos descartar a utilização de outros meios para se vulnerabilizar a porção "CLIENT" do processo

Modelagem do problema

Vetor de Propagação



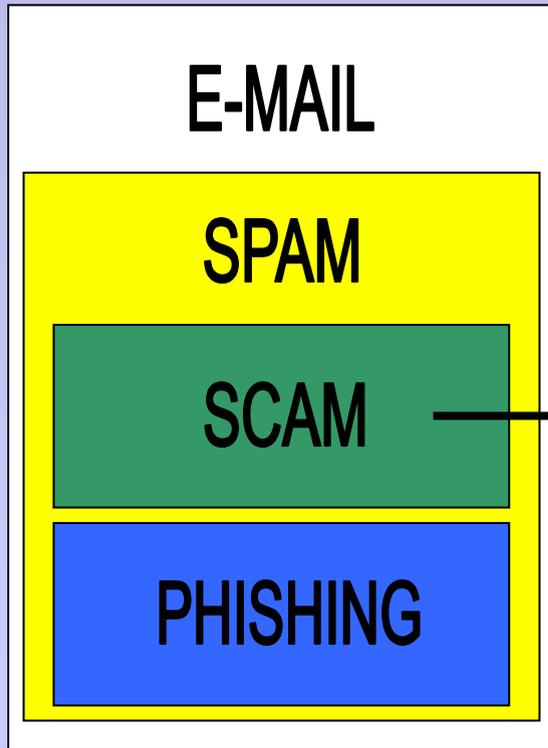
O SPAM é uma mensagem eletrônica não solicitada, enviada indiscriminadamente a múltiplas caixas postais eletrônicas, não permitindo aos usuários destas caixas postais a escolha de recebê-las.

É SPAM :

- Propaganda de produtos e serviços;
- Pedido de doações, correntes, etc.

Modelagem do problema

Vetor de Propagação



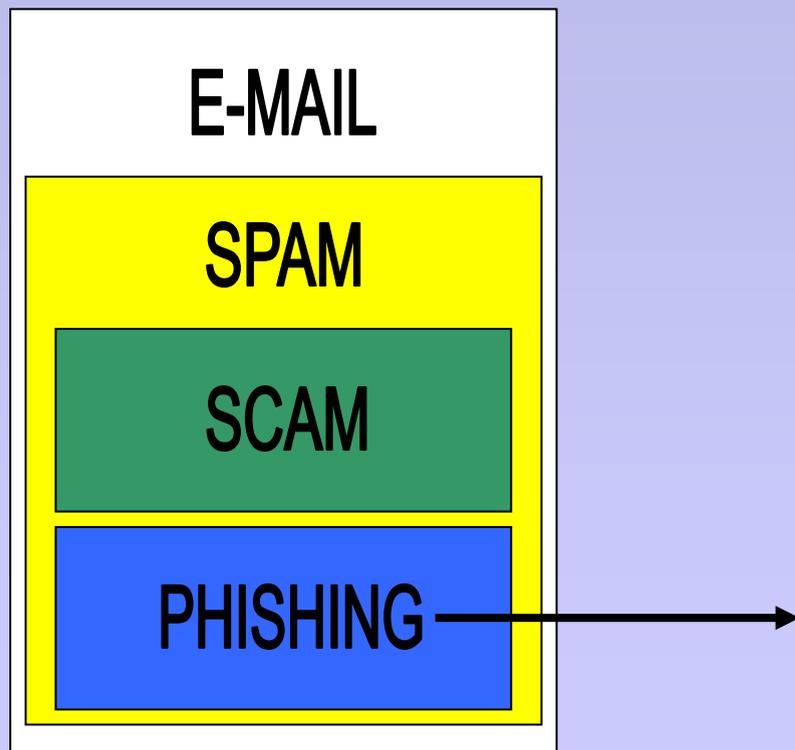
O SCAM é outro tipo de mensagem eletrônica repudiada pelos usuários, pois além de causar desconforto aos usuários de caixas postais, como o SPAM, eles apresentam natureza fraudulenta.

Exemplos de SCAMs:

- SCAMs de compras;
- SCAMs de investimento;
- "Nigerian Letters", etc

Modelagem do problema

Vetor de Propagação



PHISHING são mensagens eletrônicas enviadas aos usuários de caixas postais, convidando-os a acessar páginas fraudulentas na Internet, com a intenção de capturar informações pessoais e confidenciais, tais como números de cartões de crédito, contas e senhas de acesso bancário.

Modelagem do problema

Evolução da Fraude



- Surgimento dos primeiros SCAMs. E-mails contendo cavalos de tróia anexados à mensagens eletrônicas em nome de instituições financeiras;
- Cavalos de tróia com capacidade de captura de teclado (Keyloggers);
- Com o passar dos meses os Keyloggers permitem associação da identificação de tela da aplicação com o dado capturado;
- Criação das primeiras páginas falsas de instituições financeiras;
- Comprometimento do serviço de DNS de diversos provedores de acesso;
- Redirecionamento da vítima através de falhas no DNS e alterações do arquivo hosts pelo trojan.

Modelagem do problema

Evolução da Fraude



- Os SCAMs são mensagens que contém links à cavalos de tróia hospedados em provedores de conteúdo. As mensagens não estão mais associadas à instituições financeiras;
- Surgem os Keyloggers associados à Screenloggers;
- Com o passar dos meses Keyloggers e Screenloggers são preparados para capturar dados de páginas específicas em browsers;
- Surgem dos teclados virtuais falsos sobrepostos à sites de instituições financeiras;
- Cresce o comprometimento do serviço de DNS de diversos provedores de acesso;
- Aumentam as páginas falsas de instituições financeiras. Nasce o PHISHING.

Modelagem do problema

Evolução da Fraude



- Os SCAMs se aprimoram, utilizando uma diversidade maior de temas que atraem a curiosidade das vítimas. Alguns SCAMs contém links a páginas que hospedam o trojan;
- Surgem os cavalos de tróia que codificam os dados capturados;
- Com o passar dos meses, alguns cavalos de tróia desenvolvem a capacidade de análise do ambiente instalado com características de atualização automática do trojan.
- Surgem casos de comprometimento de computadores através de scripts ActiveX;
- Surgem os cavalos de tróia que sobrepõem telas ao browser, imitando o ambiente Web.

Modelagem do problema

Evolução da Autenticação

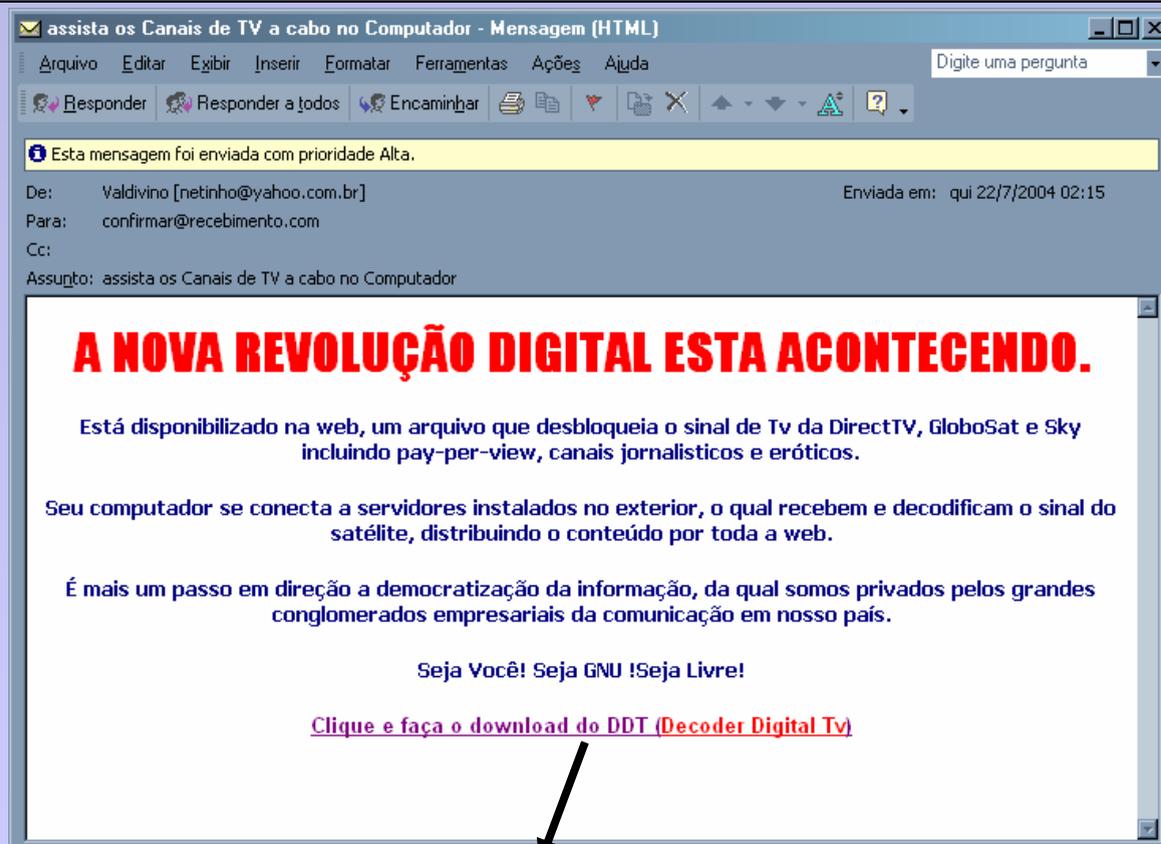


- Senha estática;
- Certificado Digital;
- Teclado virtual;
- Teclado virtual codificado;
- Dispositivos OTP (Token / SmartCard);
- Agentes anti-trojan;
- Cartão Matricial.

Análise do SCAM



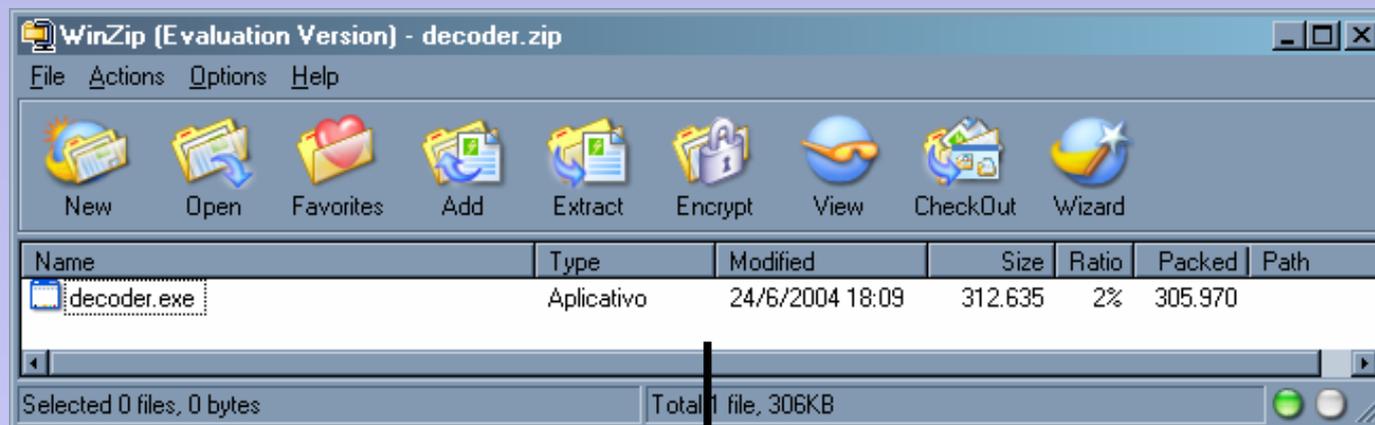
Análise do SCAM



``

`Clique e faça o download do DDT (Decoder
 Digital Tv)</p>`

Análise do SCAM



↓

Nome	Tamanho	Tipo	Data de modificação
decoder.exe	306 KB	Aplicativo	24/6/2004 19:09

Análise do SCAM

WinHex

decoder.exe

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	50	45	00	00	4C	01	03	00	19	5E	42	2A	00	00	00	00	PE..L...^B*
00000110	00	00	00	00	E0	00	8F	81	0B	01	02	19	00	60	04	00	...à.!!
00000120	00	20	00	00	00	80	07	00	A0	EC	0B	00	00	90	07	00	...i..!
00000130	00	F0	0B	00	00	00	40	00	00	10	00	00	00	02	00	00	...@..
00000140	01	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00
00000150	00	10	0C	00	00	10	00	00	00	00	00	00	02	00	00	00
00000160	00	00	10	00	00	40	00	00	00	00	10	00	00	10	00	00	...@.
00000170	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00
00000180	10	01	0C	00	88	02	00	00	00	F0	0B	00	10	11	00	00	...!...ä
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001C0	10	EE	0B	00	18	00	00	00	00	00	00	00	00	00	00	00	...i.....
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	55	50	58	30	00	00	00	00	...UPX0
00000200	00	80	07	00	00	10	00	00	00	00	00	00	00	04	00	00	...!.....
00000210	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	E0	...!..à
00000220	55	50	58	31	00	00	00	00	00	60	04	00	00	90	07	00	UPX1.....!
00000230	00	60	04	00	00	04	00	00	00	00	00	00	00	00	00	00
00000240	00	00	00	00	40	00	00	E0	2E	72	73	72	63	00	00	00	...@..à.rsrc...
00000250	00	20	00	00	00	F0	0B	00	00	14	00	00	00	64	04	00	...ä.....d..

Page 2 of 698 Offset: 1F8 = 85 Block: 1F8 - 1FB Size: 4

Característica de compactação

Ultimate Packer for eXecutables

<http://upx.sourceforge.net>

Análise do SCAM

```
C:\upx>upx -d -o decodificado.exe decoder.exe
          Ultimate Packer for eXecutables
    Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001, 2002
UPX 1.24w   Markus F.X.J. Oberhumer & Laszlo Molnar           Nov 7th 2002

-----
File size      Ratio      Format      Name
-----
760635 <-    312635    41.10%    win32/pe    decodificado.exe

Unpacked 1 file.
```



Nome	Tamanho	Tipo	Data de modificação
decoder.exe	306 KB	Aplicativo	24/6/2004 19:09
decodificado.exe	743 KB	Aplicativo	24/6/2004 19:09

Análise do SCAM

WinHex - [decodificado.exe]

File Edit Search Position View Tools Specialist Options File Manager Window Help

Simultaneous Search... Alt+F10
Create Drive Contents Table... F10
Media Details Report...
Interpret Image File As Disk
Gather Free Space...
Gather Slack Space...
Gather Inter-Partition Space...
Gather Text... Ctrl+F10
Bates Number Files...
Trusted Download...
Highlight Free Space
Highlight Slack Space

Offset	0	1	2	3	4	5
000B9A00	E6	FE	E0	CB	68	69
000B9A10	16	78	E3	8D	09	C7
000B9A20	F9	83	6C	50	5E	F8
000B9A30	08	D6	5A	66	AE	E4
000B9A40	00	00	21	00	00	00
000B9A50	73	74	65	6D	33	32
000B9A60	74	6F	73	2E	74	78
000B9A70	00	00	00	78	01	45
000B9A80	5F	11	74	DA	3A	69
000B9A90	C4	95	EF	07	F8	03
000B9AA0	9E	73	6F	6E	E3	0B
000B9AB0	B7	39	92	35	57	37
000B9AC0	88	FA	2C	D4	DC	CA
000B9AD0	89	89	53	4D	18	41
000B9AE0	06	58	73	03	5E	37
000B9AF0	23	5B	73	70	93	08
000B9B00	51	6E	D2	7C	EF	56
000B9B10	9F	F6	CF	95	E9	EC
000B9B20	6B	94	92	7A	FC	59
000B9B30	00	00	00	00	00	00

Find Text Passages

Recognize text by successive

Letters Numbers

Punctuation marks and spaces

Tolerate Unicode characters

Search:

Search in block only

OK Cancel Help

Text decodificado.exe.txt - Bloco de notas

Arquivo Editar Formatar Exibir Ajuda

```
This program must be run under win32  
  
CODE  
DATA  
.idata  
.tls  
.rdata  
P.reloc  
P.rsrc  
Boolean  
False
```

Análise do SCAM

WinHex - [Text decodificado.exe.txt]

File Edit Search Position View Tools Specialist Options File Manager Window Help

decodificado.exe Text decodificado.exe.txt

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000C0F0	5A	59	59	64	0D	0A	55	68	25	2D	49	0D	0A	5A	59	59	ZYYd..Uh%-I..ZYY
0000C100	64	0D	0A	68	2C	2D	49	0D	0A	0A	54	53	61	76	65	49	d..h.-I...TSaveI
0000C110	6D	61	67	65	0D	0A	53	56	57	33	0D	0A	58	5A	5A	59	mage..SVW3..XZZY
0000C120	0D	0A	68	2C	33	49	0D	0A	68	38	33	49	0D	0A	30	68	..h.3I..h83I..0h
0000C130	44	33	49	0D	0A	68	2C	33	49	0D	0A	68	38	33	49	0D	D3I..h.3I..h83I..
0000C140	0A	5A	59	59	64	0D	0A	49	4D	41	47	45	4D	0D	0A	43	..ZYYd..IMAGEM..C
0000C150	49	52	43	55	4C	4F	0D	0A	49	4D	41	47	45	4D	0D	0A	IRCULO..IMAGEM..
0000C160	51	55	41	4C	49	44	41	44	45	0D	0A	49	4D	41	47	45	QUALIDADE..IMAGE
0000C170	4D	0D	0A	43	4F	4C	4F	52	0D	0A	45	4D	41	49	4C	0D	M..COLOR..EMAIL..
0000C180	0A	45	4E	56	49	41	52	0D	0A	45	4E	43	52	49	50	54	..ENVIAR..ENCRYPT
0000C190	41	52	0D	0A	5A	59	59	64	0D	0A	75	6B	68	78	38	49	AR..ZYYd..ukhx8I
0000C1A0	0D	0A	68	78	38	49	0D	0A	5A	59	59	64	0D	0A	49	4D	..hx8I..ZYYd..IM
0000C1B0	41	47	45	4D	0D	0A	43	41	50	54	55	52	41	52	0D	0A	..AGEM..CAPTURAR..
0000C1C0	4D	4F	55	53	45	0D	0A	54	45	43	4C	41	44	4F	0D	0A	MOUSE..TECLADO..
0000C1D0	55	68	46	3B	49	0D	0A	5A	59	59	64	0D	0A	68	4D	3B	..UHF..I..ZYYd..kM;
0000C1E0	49	0D	0A	49	4D	41	47	45	4D	0D	0A	43	41	50	54	55	I..IMAGEM..CAPTU
0000C1F0	52	41	52	0D	0A	4D	4F	55	53	45	0D	0A	54	45	43	4C	RAR..MOUSE..TECL
0000C200	41	44	4F	0D	0A	5A	59	59	64	0D	0A	45	4D	41	49	4C	ADO..ZYYd..EMAIL
0000C210	0D	0A	48	4F	52	41	53	0D	0A	45	4D	41	49	4C	0D	0A	..HORAS..EMAIL..
0000C220	4D	49	4E	55	54	4F	53	0D	0A	55	68	6F	3D	49	0D	0A	MINUTOS..Uho=I..
0000C230	5A	59	59	64	0D	0A	68	76	3D	49	0D	0A	49	4D	41	47	ZYYd..hv=I..IMAG
0000C240	45	4D	0D	0A	51	55	41	4C	49	44	41	44	45	0D	0A	49	EM..QUALIDADE..I
0000C250	4D	41	47	45	4D	0D	0A	41	52	45	41	0D	0A	43	41	50	MAGEM..AREA..CAP
0000C260	54	55	52	41	0D	0A	5A	59	59	64	0D	0A	54	46	54	50	TURA..ZYYd..TFTP
0000C270	0D	0A	53	56	57	33	0D	0A	55	68	2F	40	49	0D	0A	5A	..SVW3..Uh/@I..Z
0000C280	59	59	64	0D	0A	5A	59	59	64	0D	0A	68	36	40	49	0D	YYd..ZYYd..no@I
0000C290	0A	66	74	70	2E	74	75	72	62	6F	73	65	63	75	72	69	..ftp.turbosecuri
0000C2A0	74	79	2E	63	6F	6D	2E	62	72	0D	0A	74	75	72	62	6F	ty.com.br..turbo
0000C2B0	73	65	63	75	72	69	74	79	0D	0A	62	36	33	34	31	33	security..b63413
0000C2C0	38	32	36	0D	0A	5A	59	59	64	0D	0A	54	57	41	42	0D	826..ZYYd..TWAB

Page 104 of 147 Offset: C2C2 = 54 Block: C147 - C2C2 Size: 17C

Indício de captura de teclado e de imagens associadas a ações realizadas pelo mouse

Referência a site de FTP que pode ser investigado

Análise do SCAM

➤ Alterações no sistema de arquivos:

- c:\windows\system\system32;
- ✓ c:\windows\system\system32\data;
- ✓ c:\windows\system\system32\temp;
- ✓ c:\windows\system\system32\cfg;
- ✓ c:\windows\system\system32\log;
- ✓ c:\windows\system\schost.exe.

➤ Alterações no sistema de registro:

- ✓ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
- ✓ Chave:
SYSTEM = "c:\windows\system\schost.exe"

WinHex - [Text decodificado.exe.txt]

decodificado.exe Text decodificado.exe.txt

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000C300	0D	0A	38	2E	74	38	0D	0A	3A	2E	74	38	0D	0A	5A	59	..8.t8...t8..ZY
0000C310	59	64	0D	0A	5A	59	59	64	0D	0A	5A	59	59	64	0D	0A	Yd..ZYD..ZYD..
0000C320	53	59	53	54	45	4D	33	32	5C	0D	0A	54	45	4D	50	5C	SYSTEM32\TEMP
0000C330	0D	0A	44	41	54	41	5C	0D	0A	4C	4F	47	5C	0D	0A	4C	..DATA\LOG..L
0000C340	4F	47	5C	57	41	42	0D	0A	49	4E	53	54	41	4C	41	44	OGNAB\INSTALAD
0000C350	4F	52	45	53	5C	0D	0A	58	79	73	74	65	6D	0D	0A	2D	RES\System...
0000C360	53	52	53	79	73	74	65	6D	33	32	2D	0D	0A	43	46	47	32\System32\CFG
0000C370	5C	0D	0A	48	44	4C	4C	0D	0A	5A	59	59	64	0D	0A	4D	..HDL\ZYD\M
0000C380	4F	4E	49	54	4F	52	41	52	0D	0A	4F	4E	4C	49	4E	45	ONITORAR\ONLINE
0000C390	0D	0A	5A	59	59	64	0D	0A	4B	45	52	4E	45	4C	33	32	..ZYD\KERNEL32
0000C3A0	2E	44	4C	4C	0D	0A	52	65	67	69	73	74	65	72	53	65	..DLL\RegisterSe
0000C3B0	72	76	69	63	65	50	72	6F	63	65	73	73	0D	0A	53	56	rviceProcess\SV
0000C3C0	57	33	0D	0A	5A	59	59	64	0D	0A	53	56	57	33	0D	0A	W3\ZYD\SVW3..
0000C3D0	5A	59	59	64	0D	0A	5A	59	59	64	0D	0A	5A	59	59	64	ZYD\ZYD\ZYD
0000C3E0	0D	0A	53	56	57	33	0D	0A	5A	59	59	64	0D	0A	53	56	..SVW3\ZYD\SV
0000C3F0	57	33	0D	0A	55	68	22	51	49	0D	0A	5A	59	59	64	0D	W3\Uh\OI\ZYD
0000C400	0A	5A	59	59	64	0D	0A	45	61	73	79	0D	0A	5C	53	6F	ZYD\Easy\So
0000C410	66	74	77	61	72	65	5C	4D	69	63	72	6F	73	6F	66	74	ftware\Microsoft
0000C420	5C	57	69	6E	64	6F	77	73	5C	43	75	72	72	65	6E	74	\Windows\Current
0000C430	56	65	72	73	69	6F	6E	0D	0A	5C	53	6F	66	74	77	61	Version\Softwa
0000C440	72	65	5C	4D	69	63	72	6F	73	6F	66	74	5C	57	59	6E	re\Microsoft\Win
0000C450	64	6F	77	73	5C	43	75	72	72	65	67	74	56	65	72	73	dows\CurrentVers
0000C460	69	6F	6E	5C	52	75	6E	0D	0A	51	51	51	51	53	0D	0A	ion\Run\QQQOS
0000C470	5A	59	59	64	0D	0A	51	53	56	57	0D	0A	5A	59	59	64	ZYD\QSW\ZYD
0000C480	0D	0A	5A	59	59	64	0D	0A	48	48	4D	4D	53	53	5A	5A	..ZYD\HHMSSZZ
0000C490	5A	0D	0A	44	44	4D	4D	59	59	59	59	0D	0A	48	48	3A	Z\DDMMYYYY\HH:
0000C4A0	4D	4D	0D	0A	53	56	57	33	0D	0A	5A	59	59	64	0D	0A	MM\SVW3\ZYD..
0000C4B0	5A	59	59	64	0D	0A	5A	59	59	64	0D	0A	5A	59	59	64	ZYD\ZYD\ZYD
0000C4C0	0D	0A	2E	54	58	54	0D	0A	49	50	20	20	20	20	20	20	..TXT\IP
0000C4D0	20	20	20	3A	20	0D	0A	43	6F	6D	70	75	74	61	64	6F	..Computado

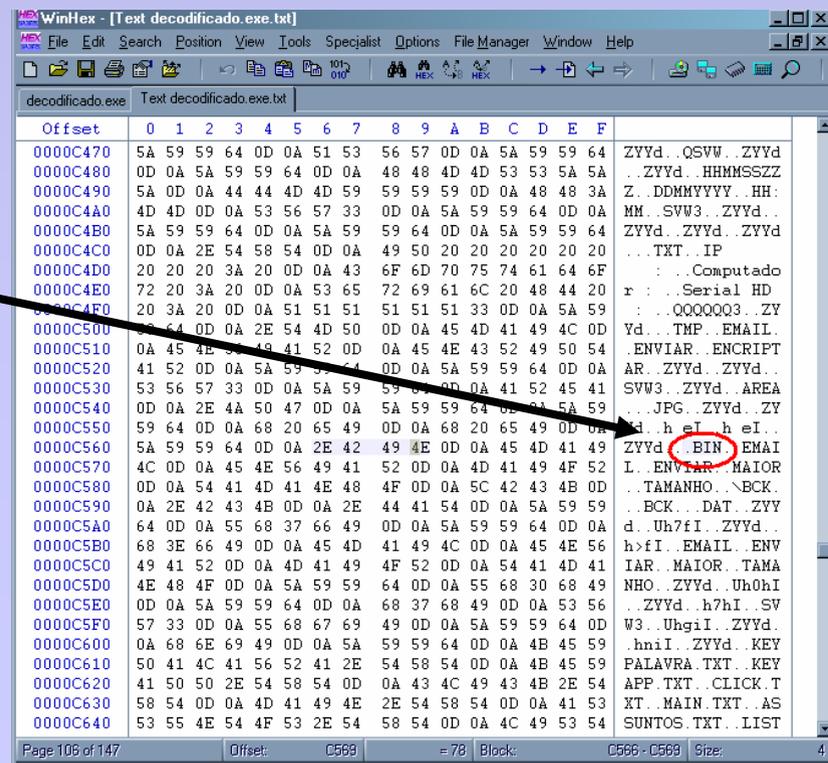
Page 105 of 147 Offset: C466 = 110 Block: C320 - C466 Size: 147

Análise do SCAM

➤ Envio de e-mail usando protocolo POP3:

- ✓ Servidor: "pop.vip.sc5.yahoo.com";
- ✓ User: "marcoalui";
- ✓ Senha: "988jlsgg".

Obs: Cria arquivos com extensão ".BIN"
no diretório "c:\windows\system\data"
a cada clique do mouse.

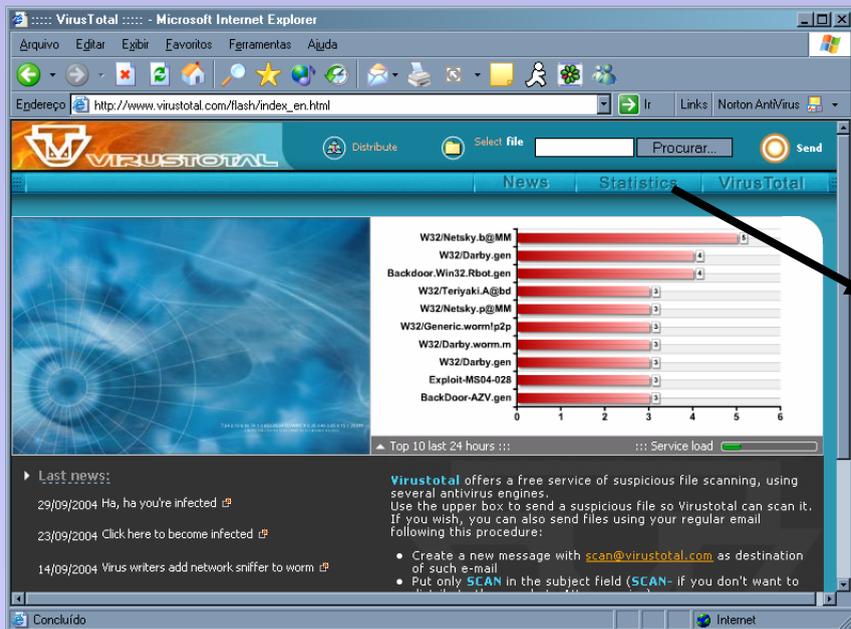


The screenshot shows a hex editor window titled "WinHex - [Text decodificado.exe.txt]". The main display area shows hex data in columns (0-15) and corresponding ASCII text on the right. A red circle highlights the ASCII string "..BIN" in the text column, which is circled in red. A black arrow points from the text "Obs: Cria arquivos com extensão ".BIN"..." to this red circle. The hex data is as follows:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Text	
0000C470	5A	59	59	64	0D	0A	51	53	56	57	0D	0A	5A	59	59	64	ZYYd..QSVW..ZYYd	
0000C480	0D	0A	5A	59	59	64	0D	0A	48	48	4D	4D	53	53	5A	5A	..ZYYd..HHMSSZZ	
0000C490	5A	0D	0A	44	44	4D	4D	59	59	59	59	0D	0A	48	48	3A	Z..DDMMYYYY..HH:	
0000C4A0	4D	4D	0D	0A	53	56	57	33	0D	0A	5A	59	59	64	0D	0A	MM..SVW3..ZYYd..	
0000C4B0	5A	59	59	64	0D	0A	5A	59	59	64	0D	0A	5A	59	59	64	ZYYd..ZYYd..ZYYd	
0000C4C0	0D	0A	2E	54	58	54	0D	0A	49	50	20	20	20	20	20	20	...TXT..IP	
0000C4D0	20	20	20	3A	20	0D	0A	43	6F	6D	70	75	74	61	64	6F	...Computado	
0000C4E0	72	20	3A	20	0D	0A	53	65	72	69	61	6C	20	48	44	20	r...Serial HD	
0000C4F0	20	3A	20	0D	0A	51	51	51	51	51	51	33	0D	0A	5A	59	...QQQQQ3..ZY	
0000C500	5A	59	64	0D	0A	2E	54	4D	50	0D	0A	45	4D	41	49	4C	0D	Yd...TMP..EMAIL.
0000C510	0A	45	4E	4A	49	41	52	0D	0A	45	4E	43	52	49	50	54	..ENVIAR..ENCRYPT	
0000C520	41	52	0D	0A	5A	59	59	64	0D	0A	5A	59	59	64	0D	0A	AR..ZYYd..ZYYd..	
0000C530	53	56	57	33	0D	0A	5A	59	59	64	0D	0A	41	52	45	41	SVW3..ZYYd..AREA	
0000C540	0D	0A	2E	4A	50	47	0D	0A	5A	59	59	64	0D	0A	5A	59	...JPG..ZYYd..ZY	
0000C550	59	64	0D	0A	68	20	65	49	0D	0A	68	20	65	49	0D	0A	d..heI..heI..	
0000C560	5A	59	59	64	0D	0A	2E	42	49	4E	0D	0A	45	4D	41	49	ZYYd..BIN..EMAI	
0000C570	4C	0D	0A	45	4E	56	49	41	52	0D	0A	4D	41	49	4F	52	L..ENVIAR..MAIOR	
0000C580	0D	0A	54	41	4D	41	4E	48	4F	0D	0A	5C	42	43	4B	0D	..TAMANHO..BCK.	
0000C590	0A	2E	42	43	4B	0D	0A	2E	44	41	54	0D	0A	5A	59	59	..BCK...DAT..ZYY	
0000C5A0	64	0D	0A	55	68	37	66	49	0D	0A	5A	59	59	64	0D	0A	d..Uh7fI..ZYYd..	
0000C5B0	68	3E	66	49	0D	0A	45	4D	41	49	4C	0D	0A	45	4E	56	h>fI..EMAIL..ENV	
0000C5C0	49	41	52	0D	0A	4D	41	49	4F	52	0D	0A	54	41	4D	41	IAR..MAIOR..TAMA	
0000C5D0	4E	48	4F	0D	0A	5A	59	59	64	0D	0A	55	68	30	68	49	NHO..ZYYd..UhOhI	
0000C5E0	0D	0A	5A	59	59	64	0D	0A	68	37	68	49	0D	0A	53	56	..ZYYd..h7hI..SV	
0000C5F0	57	33	0D	0A	55	68	67	69	49	0D	0A	5A	59	59	64	0D	W3..Uhgil..ZYYd.	
0000C600	0A	68	6E	69	49	0D	0A	5A	59	59	64	0D	0A	4B	45	59	..hniI..ZYYd..KEY	
0000C610	50	41	4C	41	56	52	41	2E	54	58	54	0D	0A	4B	45	59	PALAVRA.TXT..KEY	
0000C620	41	50	50	2E	54	58	54	0D	0A	43	4C	49	43	4B	2E	54	APP.TXT..CLICK.T	
0000C630	58	54	0D	0A	4D	41	49	4E	2E	54	58	54	0D	0A	41	53	XT..MAIN.TXT..AS	
0000C640	53	55	4E	54	4F	53	2E	54	58	54	0D	0A	4C	49	53	54	SUNTOS.TXT..LIST	

Análise do SCAM

➤ Detectado por antivírus:



SERVER RESPONSE

Results of a file scan

This is the report of the scanning done over "**decoder.zip**" file that VirusTotal processed on 07/22/2004 at 04:43:24.

Antivirus	Version	Up date	Result
BitDefender	7.0	07.21.2004	-
ClamWin	devel-20040719	07.21.2004	-
eTrustAV-Inoc	4641	07.21.2004	Win32/PWS.Bancos.343015.Trojan
F-Prot	3.15	07.19.2004	-
Kaspersky	4.0.2.23	07.22.2004	TrojanSpy.Win32.Delf.bi
* McAfee	4380	07.21.2004	PWS-Bancos
NOD32v2	1.818	07.20.2004	probably unknown NewHeur_PE
Norman	5.70.10	07.20.2004	-
Panda	7.02.00	07.21.2004	-
Sybari	7.5.1314	07.21.2004	PWS-Bancos
* Symantec	8.0	07.21.2004	PWSteal.Trojan
TrendMicro	7.000	07.19.2004	TROJ_BANCODOR.I

* Os antivírus marcados não fazem mais parte da avaliação do VirusTotal

SCAM – Tipos de arquivos

- Extensões utilizadas:

- *.exe;
- *.zip;
- *.scr;
- *.htm;
- *.html;

- Extensões suspeitas:

- *.vbe;
- *.js;
- *.jse;
- *.jpg;
- *.com;
- *.ocx;
- *.cpl;
- *.pif;
- *.pot;
- *.vbs;

SCAM – Locais de instalação

- %Windir%;
- C:\Windows (para Windows 95/98/ME/XP e Windows Server 2003/XP);
- C:\Winnt\ (para Windows NT/2000);

- %System%
- C:\Windows\System (para Windows 95/98/ME);
- C:\Winnt\System32 (para Windows NT/2000);
- C:\Windows\System32 (for Windows XP e Windows Server 2003/XP);

- %Temp%.
- C:\Windows\TEMP (para Windows 95/98/ME);
- C:\WINNT\Temp (para Windows NT/2000);
- C:\Document and Settings\<<Nome do Usuário>\Local Settings\Temp (para Windows XP e Windows Server 2003/XP);

SCAM – Chaves de Registro

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\KnownDLLs
- HKEY_LOCAL_MACHINE\System\ControlSet001\Control\SessionManager\KnownDLLs
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnceEx
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows (linha "run=")
- HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnceEx
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows (valor "run=")

SCAM – Teclados Falsificados

https://www2.bancobrasil.com.br/aapf/aai/login.pbk



Sua Conta **Banco do Brasil**

Agência Conta

Teclado Virtual

4	5	6	7	8	Senha de Auto-Atendimento
9	0	1	2	3	<input type="text"/>
					- ... contraste ... +
4	5	6	7	8	Senha do Cartão
9	0	1	2	3	<input type="text"/>
					- ... contraste ... +

[Informe sua Agencia](#)

Caixa Econômica Federal



Internet Banking CAIXA

Login

Tipo:
001-Cta. Corrente - P. Física

Agência:

Conta:

Senha Internet:

Senha Eletrônica:

"	!	@	#	\$	%	^	&	*	()	-	=	←
	Q	W	E	R	T	Y	U	I	O	P	,	{	
	caps lock	A	S	D	F	G	H	J	K	L	ç	^	}
	↑	i \	Z	X	C	V	B	N	M	<	>	? /	↑
	limpar											→	confirmar

 Internet

SCAM – Teclados Falsificados

Banco Itaú - Feito Para Você

Itaú **Itaú Bankline** AGÊNCIA: CONTA:

Teclado Virtual

Clique as senhas solicitadas nas teclas abaixo e confirme no botao OK.

Pessoa Física
 Pessoa Jurídica

Senha eletronica

Senha do Cartão

5 dígitos do Cartão

Informe aqui o número de 5 dígitos que fica do lado esquerdo do seu cartão magnético, acima do seu nome. Este é o número de confirmação

Digite os números que constam no seu cartão conforme exemplo ao lado.



Número do Portador:

Internet

https://wwwss.bradesco.com.br/scripts/ib2k1.dll/LOGIN

Bradesco Internet Banking

Cadeado de Segurança
Esse é um incativo de segurança do site
Para sua segurança informe novamente os dados da sua conta

Agência Conta

Senha de 4 Dígitos

Senha do meu Cartão



Para sua segurança, o teclado do computador não deve ser utilizado na digitação das senhas. Por favor utilize o Teclado Virtual

Indicação Positiva
Minha Resposta Secreta e:

ISQ 9001 Copy

SCAM - Exemplos

Assunto: Criança Esperança



- HOME
- O SHOW
- CLIQUE E DOE
- DEPOIMENTOS
- BENEFICIADOS
- O QUE É
- BRINDES
- VÍDEOS

Oi voc quer nos ajudar, por favor baixe este video para seu computador e veja ele depois. Isto to simples pra voc , Um ato assim to simples pode ajudar e muitos est o ajudando ns todos do crian a esperana.

*Muito obrigado pela sua ajuda.
clique ao lado e baixe o video...*

 NEWSLETTER

SCAM - Exemplos

Assunto: FW: Notificação de Pendências financeiras!!



Serviço de Proteção ao Crédito
SUPORTE DE ATENDIMENTO AO LOJISTA DO ESTADO DA BAHIA
Tel.: 0xx (71) 320-4000

Notificação

Comunicamos que seu (CPF/CNPJ) consta em nossos cadastros por motivo de pendências financeiras, com a instituição abaixo relacionada.

*Akiyoshi Executivo Central de Cobranças - Total de Pendências: **R\$ 3.754,74.***

Para sua segurança e praticidade e necessário baixar o arquivo do relatório de pendências.

Relatório de Pendências Financeiras [**Abrir Relatório**](#)

Se você efetuou a regularização, favor desconsiderar.

*Manoel Rocha Akiyoshi
Diretor*

SCAM - Exemplos

Assunto: Foram detectados emails que podem comprometer a segurança de seu computador.

Microsoft



Proteja seu PC

3 etapas para garantir que seu PC esteja protegido.

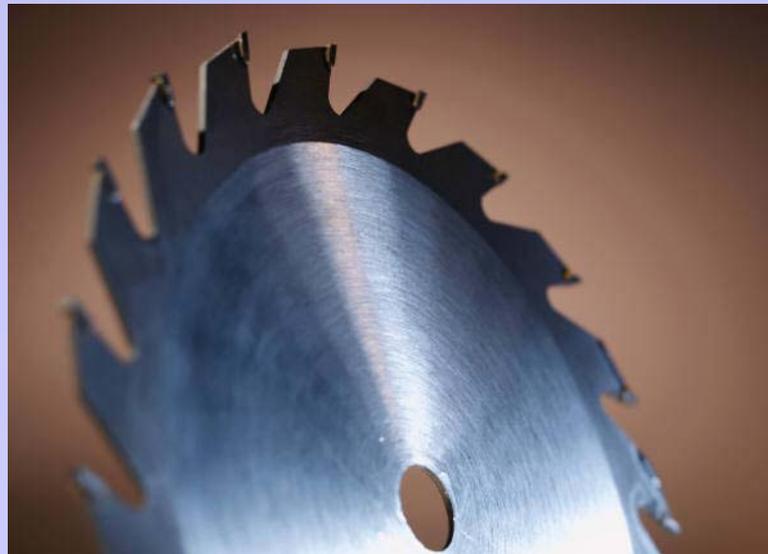
- 1 Usar um firewall de Internet
- 2 Obter atualizações para o computador
- 3 Usar um software antivírus atualizado

Microsoft - Proteja seu PC

Nosso filtro de emails detectou em sua caixa postal arquivos maliciosos, que podem causar danos a seu computador enviando mensagens indesejadas e comprometendo sua segurança. Atualize seu computador usando nossa mais nova ferramenta de segurança e anti-spam *Email-scan*

[Microsoft Email-scan](#)

Ferramentas de análise



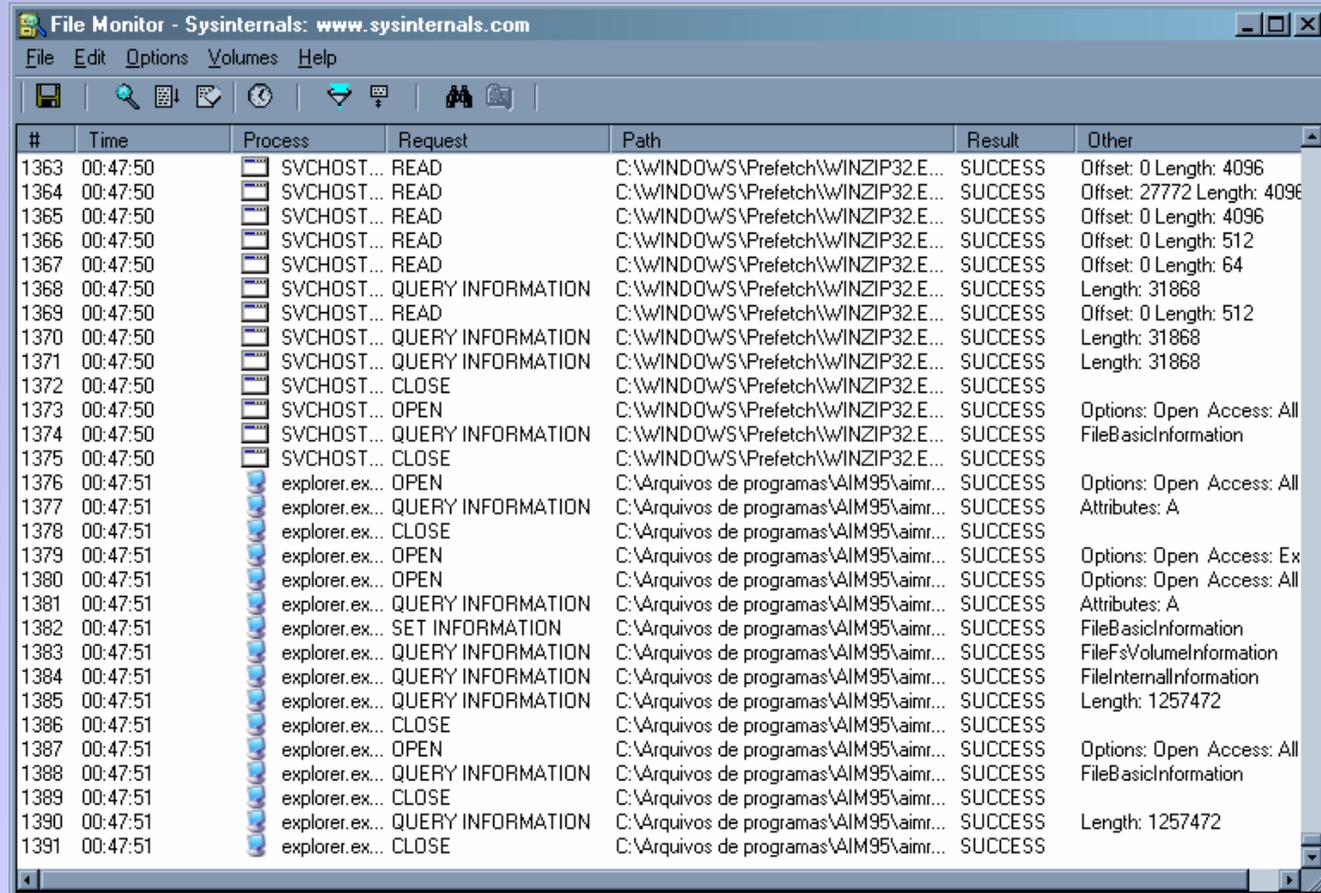
Sysinternals : Registry Monitor



The screenshot shows the Registry Monitor application window. The title bar reads "Registry Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Options", and "Help". The toolbar contains icons for file operations, search, and help. The main area displays a table of registry operations.

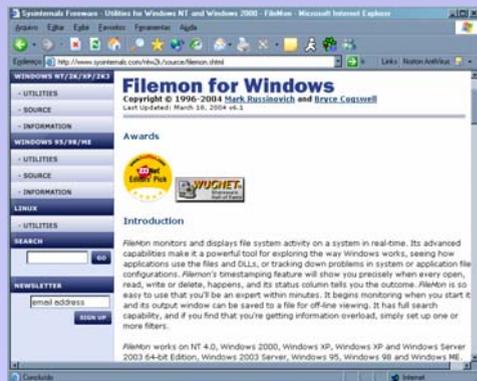
#	Time	Process	Request	Path	Result	Other
19653	14.34906839	explor...	OpenKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	Access: 0x...
19654	14.34910582	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	0x1
19655	14.34914801	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	0x40F44A63
19656	14.34919103	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	0x40F83EE3
19657	14.34922483	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	"10.48.4.16"
19658	14.34925891	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	"10.48.4.16"
19659	14.34930222	explor...	CloseKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	
19660	14.34948771	explor...	OpenKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	Access: 0x...
19661	14.34952263	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	0x0
19662	14.34955811	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	NOTFO...	
19663	14.34959667	explor...	CloseKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	
19664	14.34983552	explor...	QueryValue	HKLM\SYSTEM\ControlSet001\Servic...	BUFOV...	
19665	14.34986933	explor...	QueryValue	HKLM\SYSTEM\ControlSet001\Servic...	BUFOV...	
19666	14.34991794	explor...	QueryValue	HKLM\SYSTEM\ControlSet001\Servic...	SUCCE...	"\Device{\...
19667	14.35045851	explor...	OpenKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	Access: 0x...
19668	14.35050013	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	0x1
19669	14.35054232	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	0x40F44A63
19670	14.35057919	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	0x40F83EE3
19671	14.35061356	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	"10.48.4.16"
19672	14.35065295	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	"10.48.4.16"
19673	14.35068843	explor...	CloseKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	
19674	14.35084403	explor...	OpenKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	Access: 0x...
19675	14.35088258	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	0x0
19676	14.35091583	explor...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	NOTFO...	
19677	14.35094907	explor...	CloseKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	
19678	14.85547130	discad...	QueryValue	HKLM\SOFTWARE\Microsoft\Windo...	NOTFO...	
19679	14.90707087	ICQLit...	CreateKey	HKLM\Software\Mirabilis\ICQ\ICQLite	SUCCE...	Access: 0x...
19680	14.90712730	ICQLit...	SetValue	HKLM\Software\Mirabilis\ICQ\ICQLite\...	SUCCE...	"No"
19681	14.90715384	ICQLit...	CloseKey	HKLM\Software\Mirabilis\ICQ\ICQLite	SUCCE...	

Sysinternals : File Monitor



The screenshot shows the Sysinternals File Monitor application window. The title bar reads "File Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Options", "Volumes", and "Help". The toolbar contains icons for file operations and monitoring. The main display area is a table with the following columns: #, Time, Process, Request, Path, Result, and Other. The table lists various file system operations performed by the system (SVCHOST) and the user (explorer.exe).

#	Time	Process	Request	Path	Result	Other
1363	00:47:50	SVCHOST...	READ	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Offset: 0 Length: 4096
1364	00:47:50	SVCHOST...	READ	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Offset: 27772 Length: 4096
1365	00:47:50	SVCHOST...	READ	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Offset: 0 Length: 4096
1366	00:47:50	SVCHOST...	READ	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Offset: 0 Length: 512
1367	00:47:50	SVCHOST...	READ	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Offset: 0 Length: 64
1368	00:47:50	SVCHOST...	QUERY INFORMATION	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Length: 31868
1369	00:47:50	SVCHOST...	READ	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Offset: 0 Length: 512
1370	00:47:50	SVCHOST...	QUERY INFORMATION	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Length: 31868
1371	00:47:50	SVCHOST...	QUERY INFORMATION	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Length: 31868
1372	00:47:50	SVCHOST...	CLOSE	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	
1373	00:47:50	SVCHOST...	OPEN	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	Options: Open Access: All
1374	00:47:50	SVCHOST...	QUERY INFORMATION	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	FileBasicInformation
1375	00:47:50	SVCHOST...	CLOSE	C:\WINDOWS\Prefetch\WINZIP32.E...	SUCCESS	
1376	00:47:51	explorer.ex...	OPEN	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	Options: Open Access: All
1377	00:47:51	explorer.ex...	QUERY INFORMATION	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	Attributes: A
1378	00:47:51	explorer.ex...	CLOSE	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	
1379	00:47:51	explorer.ex...	OPEN	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	Options: Open Access: Ex
1380	00:47:51	explorer.ex...	OPEN	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	Options: Open Access: All
1381	00:47:51	explorer.ex...	QUERY INFORMATION	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	Attributes: A
1382	00:47:51	explorer.ex...	SET INFORMATION	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	FileBasicInformation
1383	00:47:51	explorer.ex...	QUERY INFORMATION	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	FileFsVolumeInformation
1384	00:47:51	explorer.ex...	QUERY INFORMATION	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	FileInternalInformation
1385	00:47:51	explorer.ex...	QUERY INFORMATION	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	Length: 1257472
1386	00:47:51	explorer.ex...	CLOSE	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	
1387	00:47:51	explorer.ex...	OPEN	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	Options: Open Access: All
1388	00:47:51	explorer.ex...	QUERY INFORMATION	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	FileBasicInformation
1389	00:47:51	explorer.ex...	CLOSE	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	
1390	00:47:51	explorer.ex...	QUERY INFORMATION	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	Length: 1257472
1391	00:47:51	explorer.ex...	CLOSE	C:\Arquivos de programas\AIM95\aimr...	SUCCESS	



Sysinternals : Process Explorer

The screenshot displays the Process Explorer application window. The main window shows a list of processes with columns for Process, PID, CPU, Description, and Company Name. The system tree on the left is expanded to show the 'SERVICES.EXE' process, which is highlighted in blue. Below the process list, a detailed view shows the system tree structure, including the 'AGENC:\WINDOWS\SYSTEM32\SERVICES.EXE' process. The status bar at the bottom indicates CPU Usage: 20%, Commit Charge: 24.41%, and Processes: 56.

Process	PID	CPU	Description	Company Name
System Idle Process	0	80		
Interrupts	n/a	6	Hardware Interrupts	
DPCs	n/a		Deferred Procedu...	
System	4			
SMSS.EXE	896		Windows NT Ses...	Microsoft Corporation
CSRSS.EXE	964		Client Server Run...	Microsoft Corporation
WINLOGON.EXE	992		Aplicativo de logo...	Microsoft Corporation
SERVICES.EXE	1040	7	Aplicativo de serv...	Microsoft Corporation
SVCHOST.EXE	1236		Generic Host Pro...	Microsoft Corporation
AGENC:\WINDOWS\SYSTEM32\SERVICES.EXE			Agent S...	Microsoft Corporation
SVCHOST.EXE	1316		Generic Host Pro...	Microsoft Corporation
S24E\Mon.exe	1440		Event Monitor - S...	Intel Corporation
SVCHOST.EXE	1532		Generic Host Pro...	Microsoft Corporation

Type	Name
Desktop	\Default
Directory	\Windows
Directory	\BaseNamedObjects
Directory	\KnownDlls
Event	\BaseNamedObjects\SC_AutoStartComplete
Event	\BaseNamedObjects\svcsctlStartEvent_A3752DX
Event	\BaseNamedObjects\svcsNetDrvMsg
Event	\BaseNamedObjects\WBEM_ESS_OPEN_FOR_BUSINESS
Event	\BaseNamedObjects\PhP_No_Pending_Install_Events
Event	\BaseNamedObjects\userenv: User Profile setup event
File	\Device\NamedPipe\ntsvcs
File	\Device\KsecDD

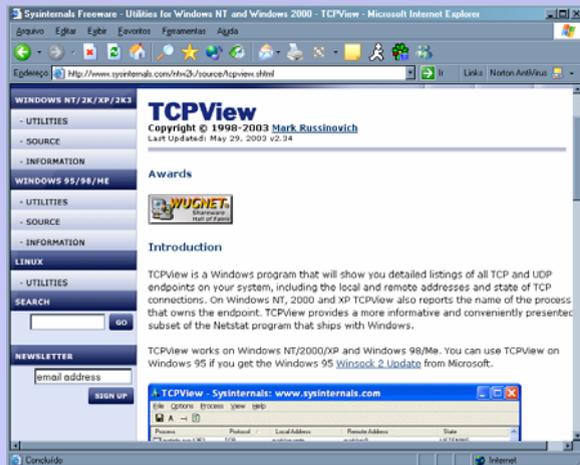
CPU Usage: 20% Commit Charge: 24.41% Processes: 56

The screenshot shows the Sysinternals Process Explorer website. The page features a navigation menu with links for Utilities, Source, Information, Awards, and Introduction. The main content area displays the 'Process Explorer' logo and a brief introduction to the tool. A search bar is located at the bottom of the page.

Process Explorer
Copyright © 1998-2004 Mark Russinovich
Last updated: June 27, 2004 v8.43

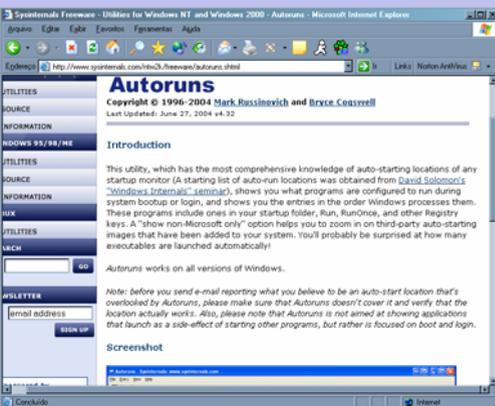
Introduction
Ever wondered which program has a particular file or directory open? Now you can find out. Process Explorer shows you information about which handles and DLLs processes have opened or loaded.

Sysinternals : TCPView



Process	Protocol	Local Address	Remote Address	State
aim.exe:568	TCP	A1A:3198	A1A:0	LISTENING
aim.exe:568	TCP	A1A:3222	A1A:0	LISTENING
aim.exe:568	TCP	A1A:5180	A1A:0	LISTENING
aim.exe:568	TCP	a1a:3198	205.188.8.179:5190	ESTABLISHED
aim.exe:568	TCP	a1a:3222	205.188.10.216:5...	ESTABLISHED
ALG.EXE:1388	TCP	A1A:3001	A1A:0	LISTENING
ccApp.exe:1504	TCP	A1A:1028	A1A:0	LISTENING
IEXPLORE.EXE:4...	TCP	A1A:3606	A1A:0	LISTENING
IEXPLORE.EXE:4...	TCP	A1A:3625	A1A:0	LISTENING
IEXPLORE.EXE:4...	TCP	a1a:3606	66-193-254-46.ge...	LAST_ACK
IEXPLORE.EXE:4...	TCP	a1a:3625	66-193-254-46.ge...	ESTABLISHED
IEXPLORE.EXE:4...	UDP	A1A:3189	**	
LSASS.EXE:1052	UDP	A1A:isakmp	**	
msmsgs.exe:1872	TCP	A1A:3184	A1A:0	LISTENING
msmsgs.exe:1872	TCP	A1A:3218	A1A:0	LISTENING
msmsgs.exe:1872	TCP	a1a:3184	baym-cs75.msgr.h...	ESTABLISHED
msmsgs.exe:1872	TCP	a1a:7068	A1A:0	LISTENING
msmsgs.exe:1872	UDP	A1A:1027	**	
msmsgs.exe:1872	UDP	A1A:3187	**	
msmsgs.exe:1872	UDP	a1a:13155	**	
msmsgs.exe:1872	UDP	a1a:42317	**	
persfw.exe:440	TCP	A1A:44334	A1A:0	LISTENING
persfw.exe:440	UDP	A1A:44334	**	
POWERPNT.EXE...	UDP	A1A:3277	**	
SVCHOST.EXE:1...	TCP	A1A:epmap	A1A:0	LISTENING
SVCHOST.EXE:1...	TCP	A1A:1025	A1A:0	LISTENING
SVCHOST.EXE:1...	TCP	A1A:3002	A1A:0	LISTENING
SVCHOST.EXE:1...	TCP	A1A:3003	A1A:0	LISTENING
SVCHOST.EXE:1...	UDP	A1A:ntp	**	

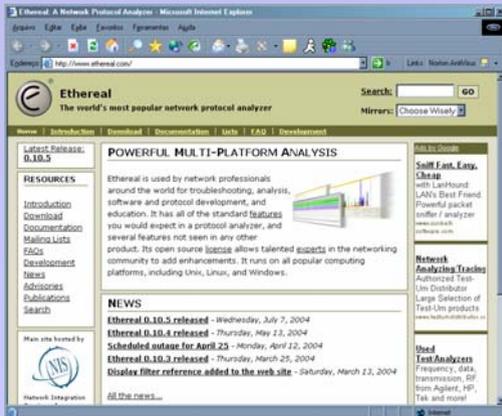
Sysinternals : Autoruns



The screenshot shows the Autoruns utility interface. The title bar reads "Autoruns - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Entry", "View", and "Help". The toolbar contains icons for file operations. The main area displays a table of auto-starting programs with columns for "Autorun Entry", "Description", "Company", and "Image Path".

Autorun Entry	Description	Company	Image Path	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify				
<input checked="" type="checkbox"/>	csodll	Agente de rede off-line	Microsoft Corporation	C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	NavLogon			C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	ScCertProp	DLL comum para receber notificações do Winlogon		C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	Schedule	DLL comum para receber n...	Microsoft Corporation	C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	Sebring	LogonNotify DLL	Intel Corporation	C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	SensLogn	DLL comum para receber n...	Microsoft Corporation	C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	termsrv	DLL comum para receber n...	Microsoft Corporation	C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	wlballoon	DLL comum para receber n...	Microsoft Corporation	C:\WINDOWS\SYSTEM32...
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit				
<input checked="" type="checkbox"/>	C:\WINDOWS...	Aplicativo de logon Userinit	Microsoft Corporation	C:\WINDOWS\SYSTEM32...
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell				
<input checked="" type="checkbox"/>	Explorer.exe	Windows Explorer	Microsoft Corporation	C:\WINDOWS\explorer.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
<input checked="" type="checkbox"/>	Advanced Too...	Norton AntiVirus Advanced ...	Symantec Corporation	C:\Arquivos de programas\...
<input checked="" type="checkbox"/>	ccApp	Symantec Common Client U...	Symantec Corporation	C:\Arquivos de programas\...
<input checked="" type="checkbox"/>	CertificateRegi...	Certificate Registration Utility	A.E.T. Europe B.V.	C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	Hcontrol	HControl	ASUSTeK COMPUTER INC.	C:\WINDOWS\ATK0100\...
<input checked="" type="checkbox"/>	HotKeysCmds	hkcmd Module	Intel Corporation	C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	ICQ Lite	ICQLite	ICQ Ltd.	C:\Arquivos de programas\I...
<input checked="" type="checkbox"/>	IgfxTray	igfxTray Module	Intel Corporation	C:\WINDOWS\SYSTEM32...
<input checked="" type="checkbox"/>	InCD	InCD	Ahead Software AG	C:\Arquivos de programas\...
<input checked="" type="checkbox"/>	NeroCheck	NeroCheck	Ahead Software Gmbh	C:\WINDOWS\SYSTEM32...

Ethereal



The screenshot shows the Ethereal network protocol analyzer interface. The title bar reads 'few packets.cap - Ethereal'. The menu bar includes File, Edit, View, Capture, Analyze, and Help. The toolbar contains various icons for file operations and analysis. The main display area is divided into three panes:

- Packet List:** A table showing captured packets. The selected packet (No. 16) is highlighted in green.
- Packet Bytes:** A hex dump of the selected packet's raw bytes.
- Packet Details:** A tree view showing the protocol stack for the selected packet, including Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Delta	Source	Destination	Protocol	Info
13	14.817570	14.817570	192.168.0.10	192.168.0.2	TCP	1242 > 80 [SYN] Seq=1404510823 Ack=0 win=65535
14	14.817689	0.000119	192.168.0.2	192.168.0.10	TCP	80 > 1242 [SYN, ACK] Seq=3661615104 Ack=1404510823
15	14.818178	0.000489	192.168.0.10	192.168.0.2	TCP	1242 > 80 [ACK] Seq=1404510824 Ack=3661615105
16	14.819035	0.000857	192.168.0.10	192.168.0.2	HTTP	GET / HTTP/1.1
17	14.975815	0.156780	192.168.0.2	192.168.0.10	TCP	80 > 1242 [ACK] Seq=3661615105 Ack=1404511235
23	19.382555	4.406740	192.168.0.10	192.168.0.2	TCP	1242 > 80 [FIN, ACK] Seq=1404511234 Ack=3661615105
24	19.382634	0.000079	192.168.0.2	192.168.0.10	TCP	80 > 1242 [ACK] Seq=3661615105 Ack=1404511235
52	54.234482	34.851848	192.168.0.2	192.168.0.10	HTTP	HTTP/1.1 403 Forbidden (text/html)
53	54.235272	0.000790	192.168.0.10	192.168.0.2	TCP	1242 > 80 [RST] Seq=1404511235 Ack=366044707
54	58.137063	3.901791	192.168.0.10	192.168.0.2	TCP	1244 > 135 [SYN] Seq=1414452237 Ack=0 win=65535
55	58.137176	0.000113	192.168.0.2	192.168.0.10	TCP	135 > 1244 [SYN, ACK] Seq=3672465192 Ack=1414452237
56	58.137527	0.000351	192.168.0.10	192.168.0.2	TCP	1244 > 135 [ACK] Seq=1414452238 Ack=36724651
57	58.137992	0.000465	192.168.0.10	192.168.0.2	DCERPC	Bind: call_id: 57 UUID: IOXIDResolver
58	58.188933	0.050941	192.168.0.2	192.168.0.10	DCERPC	Bind_ack: call_id: 57 accept_max_xmit: 5840
59	58.189601	0.000668	192.168.0.10	192.168.0.2	IOXIDR	ComplexPing request AddrToSet=0 DelFromSet=1
60	58.202631	0.013030	192.168.0.2	192.168.0.10	IOXIDR	ComplexPing response -> Unknown (0x00000778)
61	58.203457	0.000826	192.168.0.10	192.168.0.2	IOXIDR	ComplexPing request AddrToSet=0 DelFromSet=1

Packet Details for Frame 16 (464 bytes on wire, 464 bytes captured):

- Ethernet II, Src: 00:04:61:4a:1e:95, Dst: 00:0b:5d:20:cd:02
- Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: 192.168.0.2 (192.168.0.2)
- Transmission Control Protocol, Src Port: 1242 (1242), Dst Port: 80 (80), Seq: 1404510824, Ack: 3661615105, Len: 410
- Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Host: 192.168.0.2\r\n
 - User-Agent: Mozilla/5.0 (windows; u; windows NT 5.0; en-US; rv:1.5) Gecko/20031007\r\n
 - Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.7,*/*;q=0.5\r\n
 - Accept-Language: en-us,en;q=0.5\r\n
 - Accept-Encoding: gzip,deflate\r\n
 - Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
 - Keep-Alive: 300\r\n
 - Connection: keep-alive\r\n

Packet Bytes:

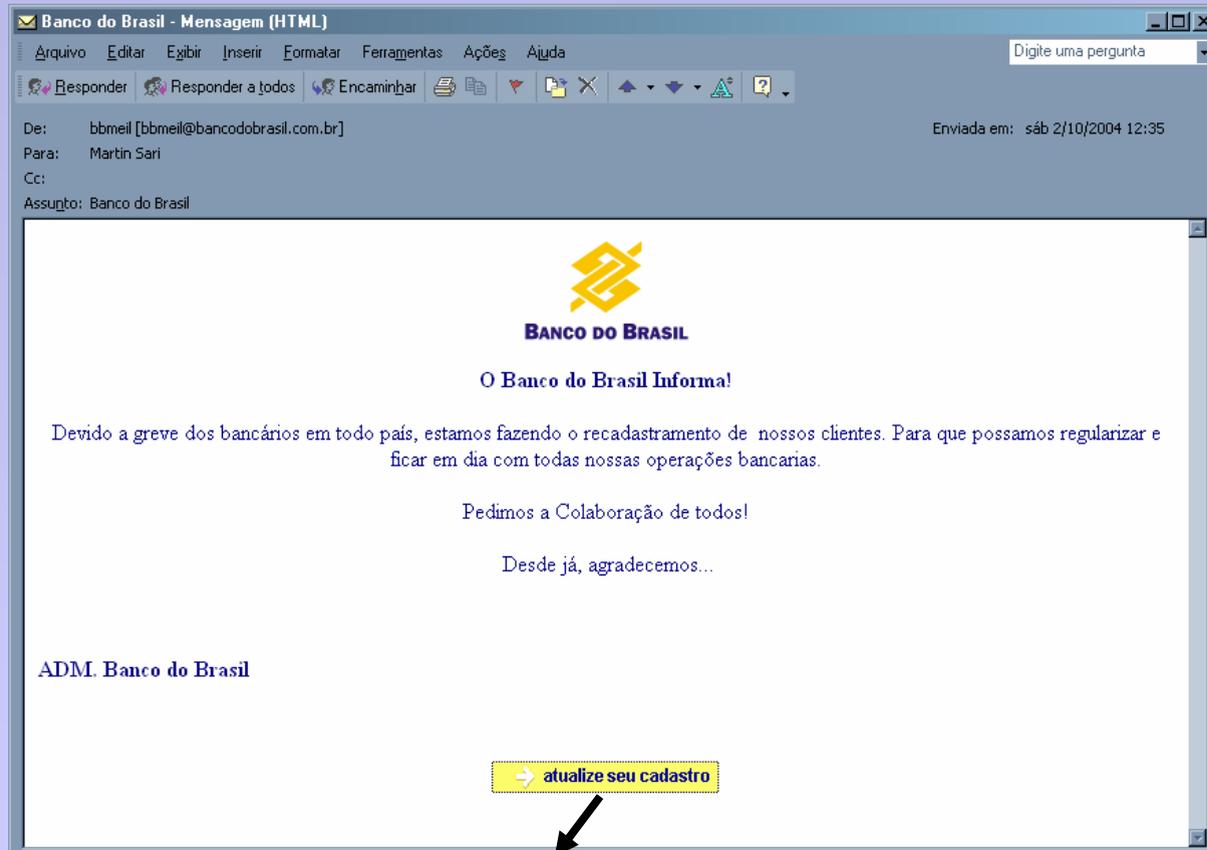
```
0000 00 0b 5d 20 cd 02 00 04 61 4a 1e 95 08 00 45 00 ..]...aJ...E.
0010 01 c2 d1 6d 40 00 80 06 a6 6b c0 a8 00 0a c0 a8 ...m@...k.....
0020 00 02 04 da 00 50 53 b7 22 68 da 3f d0 01 50 18 ....PS."h?.P.
0030 ff ff 46 26 00 00 47 45 54 20 2f 20 48 54 54 50 ..F&..GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e /1.1..HO st: 192.
0050 21 26 28 20 20 22 0d 03 55 72 65 72 2d 41 67 168.0.2 HTTP/1.1
```

Filter: tcp

Análise do PHISHING



Análise do PHISHING



```
href="http://www.bahrainexplorer.com/images/Login.bbk">  


Encontre o que você precisa ... BB Responde . Rede de Atendimento

**Sua Conta** Acesso | Segurança | Perguntas Frequentes Certificação Digital  
» acesse aqui » veja detalhes

**Atenção**  
Mais segurança para suas transações eletrônicas. Instale sempre o teclado virtual e a ferramenta de segurança.  
[leia mais »](#)

**Informações Importantes**

- Ajuda para usuários do Windows XP »
- BB não envia e-mail sem sua permissão »
- Saiba como identificar um site seguro »

Titular  
1º Titular

Agência

Conta

**Teclado Virtual**

0 1 2 3 4  
5 6 7 8 9

Senha de Auto-Atendimento

... contraste ...

Problemas com o campo senha, clique aqui

[Informe o prefixo da agência.](#)

**Navegue com Segurança**

**Em dia com a segurança**  
Mantenha sempre atualizado seu sistema operacional, navegador Internet e programa antivírus para garantir a segurança dos seus dados.  
[Saiba mais >>](#)

**Não clique, digite**  
Sempre acesse sua conta pela Internet digitando o endereço [www.bb.com.br](http://www.bb.com.br) e na página de acesso à conta, verifique sempre se o endereço começa por https.  
[Saiba mais >>](#)

0800-785678 . política de privacidade . acesso à internet . mapa do site

Concluído Internet

```
<FORM Method="post" Action="principal/default.asp" Name="Form">
```

# PHISHING - Exemplos

Assunto:



## É Dia de Ganhar com o Itaú

**A promoção continua.**

**Agora são 92 prêmios de R\$ 6.000,00.**

Entre 1º de agosto e 31 de outubro, a premiação é dobrada. Em vez de R\$ 3.000,00, você concorre a R\$ 6.000,00

São 92 prêmios de R\$ 6.000,00, um para cada dia da promoção!  
Se você ainda não se cadastrou, não perca tempo!

Cadastre hoje mesmo no Itaú Bankline Internet.

# PHISHING - Exemplos

Assunto: Important Information: Your Account [Sun, 15 Aug 2004 20:17:26 +0500]



Dear client of the U.S. Bank,

As the Technical service of bank have been currently updating the software, we kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

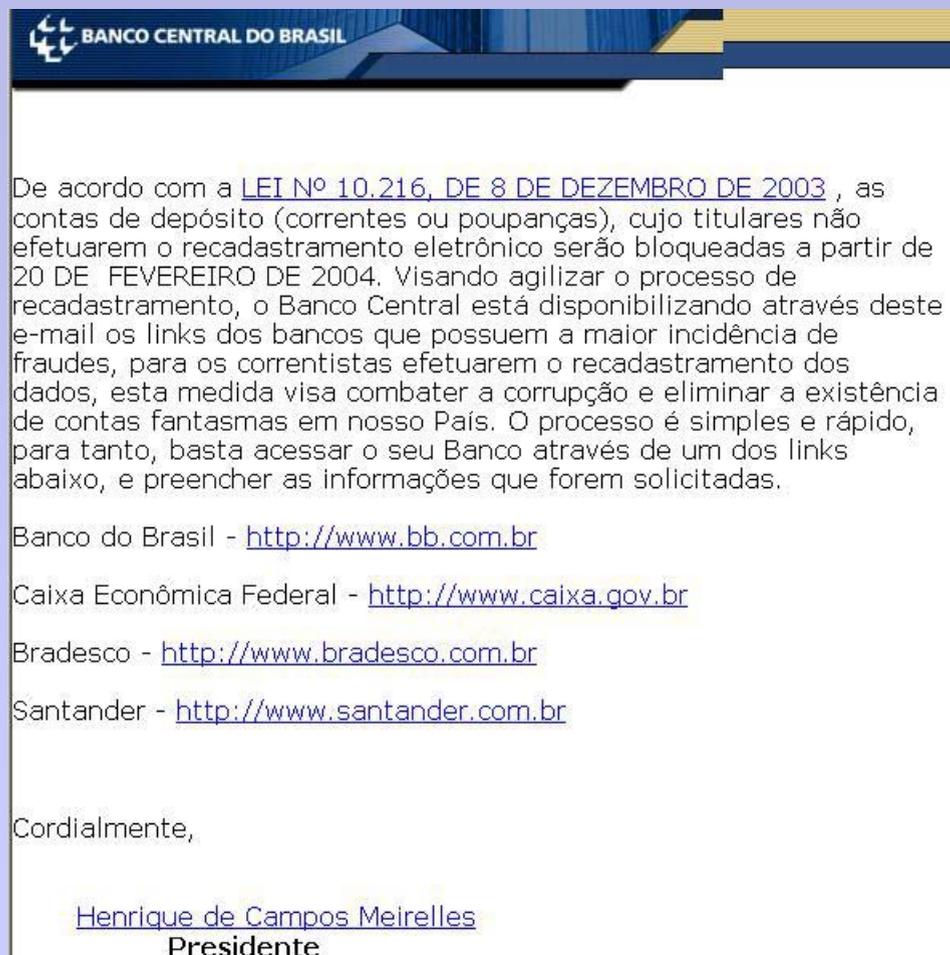
[http://www.usbank.com/cgi\\_w/cfm/confirmation/account\\_access/account\\_confirm.cfm](http://www.usbank.com/cgi_w/cfm/confirmation/account_access/account_confirm.cfm)

We are grateful for your cooperation.

Please do not answer this message and follow the above mentioned instructions.

© 2004 U.S. Bancorp

# PHISHING - Exemplos



# Informações na Internet

SCAM / PHISHING



# Anti-Phishing Working Group

Anti-Phishing Working Group - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço <http://www.antiphishing.org/>

Anti-Phishing Working Group **APWG** **Anti-Phishing Working Group** [register](#)  
Committed to wiping out Internet scams and fraud

[report phishing - click here](#)

- Home
- Phishing Archive
- Report Phishing
- Events
- APWG News
- Resources
- Membership
- APWG Member Site
- Contact Us
- JOIN THE APWG

**PARTNER EVENT:**

Spam Archiving Compliance Delivery

**EAST inBOX THE EMAIL EVENT**

**What is Phishing?**

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

**Unique Phishing Attack Trends**  
May 2004 - July 2004

Date	Cumulative Phishing Attacks	Weekly Phishing Attacks
5/1/2004	216	216
5/8/2004	279	279
5/15/2004	341	341
5/22/2004	374	374
5/29/2004	405	405
6/5/2004	424	424
6/12/2004	455	455
6/19/2004	487	487
6/26/2004	504	504
7/3/2004	504	504
7/10/2004	504	504
7/17/2004	504	504
7/24/2004	504	504
7/31/2004	504	504

**Anti-Phishing Working Group**  
The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing.

**APWG Members**

- Over 636 members
- Over 407 companies
- 8 of the top 10 US banks
- 4 of the top 5 US ISPs
- Over 100 technology vendors
- Law enforcement from Australia, Canada, UK, USA

**APWG Working Groups**

- Best Practices
- Education
- Future Threat Models
- Phishing Repository
- Sizing the Problem
- Solution Evaluation/Trial
- Law Enforcement

**APWG SPONSORS:**

VISA

Microsoft

**News and Events:**

- 30-Aug-04 - New Phishing Trends Report Available!  
[Phishing Attack Trends Report - July 2004](#)
- APWG September Meeting and Workshop in Washington DC

LATEST NEWS IN THE FIELD

[http://www.antiphishing.org/APWG\\_Phishing\\_Attack\\_ReportJul2004.pdf](http://www.antiphishing.org/APWG_Phishing_Attack_ReportJul2004.pdf)

Zona desconhecida

# Internet Fraud Complaint Center

The screenshot shows a Microsoft Internet Explorer browser window displaying the Internet Fraud Complaint Center (IFCC) website. The browser's address bar shows the URL <http://www.ifccfbi.gov/index.asp>. The website header features the IFCC logo, the date "October 7, 2004", and navigation links for "Privacy", "Disclaimer", and "Sitemap". A secondary navigation bar includes "Home", "File a Complaint", "Press Room", "Fraud Tips", and "Contact Us".

The main content area is titled "Welcome to IFCC" and contains the following text:

**Report Terrorist Activity** ([click here](#))

**Filing a Complaint**  
[How to file](#)  
[Information Requested](#)

**Statistics**

**Partners**

**IFCC Warnings** NEW

The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

IFCC's mission is to address fraud committed over the Internet. For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation. For law enforcement and regulatory agencies at all levels, IFCC offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.

[File a Complaint](#)

This program is brought to you by the [Federal Bureau of Investigation](#) and the [National White Collar Crime Center](#).

The FBI logo is on the left, and the NW3C logo is on the right. The footer contains a navigation bar with links: [top](#) | [home](#) | [about us](#) | [press room](#) | [file a complaint](#) | [statistics](#) | [contact us](#). The status bar at the bottom shows "Concluído" and "Internet".

# Febraban

Segurança - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço <http://www.febraban.org.br/seguranca/> Ir Links Norton AntiVirus

## FEBRABAN

### Guia de Segurança



#### Dicas para Clientes

- Senhas
- Uso de Cartões
- Internet com segurança
- E-Mails
- Uso de cheques
- Caixa Automático

#### Saiba Mais

- Artigos
- Glossário de segurança
- Como se prevenir
- Dúvidas mais frequentes



#### Segurança: um compromisso de bancos e clientes, em todo o mundo

As fraudes contra o sistema financeiro não são "privilégio" brasileiro. Pelo contrário, constituem preocupação mundial e crescem num ritmo alarmante nas nações mais desenvolvidas na área de automação bancária ...

[leia mais](#)

#### 4º Seminário de Segurança Bancária

Especialistas das áreas de segurança física, jurídica, auditoria, serviços bancários e tecnologia da informação do sistema financeiro se reuniram nos dias 15 e 16 de setembro, no Novotel São Paulo Center Norte ...

[leia mais](#)

#### Últimas notícias

- Ação de hackers assusta correntistas na Internet
- Inteligência interna
- Nova safra de vírus

#### Dicas de Segurança

Mantenha sempre atualizados seus programas de antivírus.

Concluído Internet

# Camara e-net

The screenshot shows a Microsoft Internet Explorer browser window displaying the website of the Câmara Brasileira de Comércio Eletrônico (Câmara e-net). The browser's address bar shows the URL: <http://www.camara-e.net/interna.asp?tipo=1&valor=2787>. The website header features the logo of the Câmara Brasileira de Comércio Eletrônico and a navigation menu with links to: Institucional, Associe-se, Projetos de Lei, Sala de Imprensa, Painel de Negócios, Comitês, and Contato. A sidebar on the left contains a 'Biblioteca' section with links to Camara-e.net, Notícias, Entrevistas, Internacional, Índices/Pesquisas, Agenda, and Artigos e opiniões. Below this is a search box labeled 'Busca' with a 'BUSCAR' button. The main content area is titled 'Biblioteca > Comitês' and contains the following text:

**Prezado Sócio,**

A **Câmara Brasileira de Comércio Eletrônico** convida para a **Reunião Conjunta dos Sub-Comitês de Crimes na Internet e Propriedade Intelectual**, que se dará como segue:

**Data:** 07/outubro

**Horário:** 10h00

**Pauta:** "O Crime de Concorrência Desleal na disputa comercial entre os Softwares Livre e os Softwares Proprietário."

**Coordenador do Sub-Comitê de Crimes na Internet:**  
Dr. Caio Domeneghetti

**Coordenadora do Sub-Comitê de Propriedade Intelectual:**  
Dra. Regina Ribeiro de Valle

At the bottom of the browser window, the status bar shows 'Concluído' and 'Internet'.

# Considerações finais

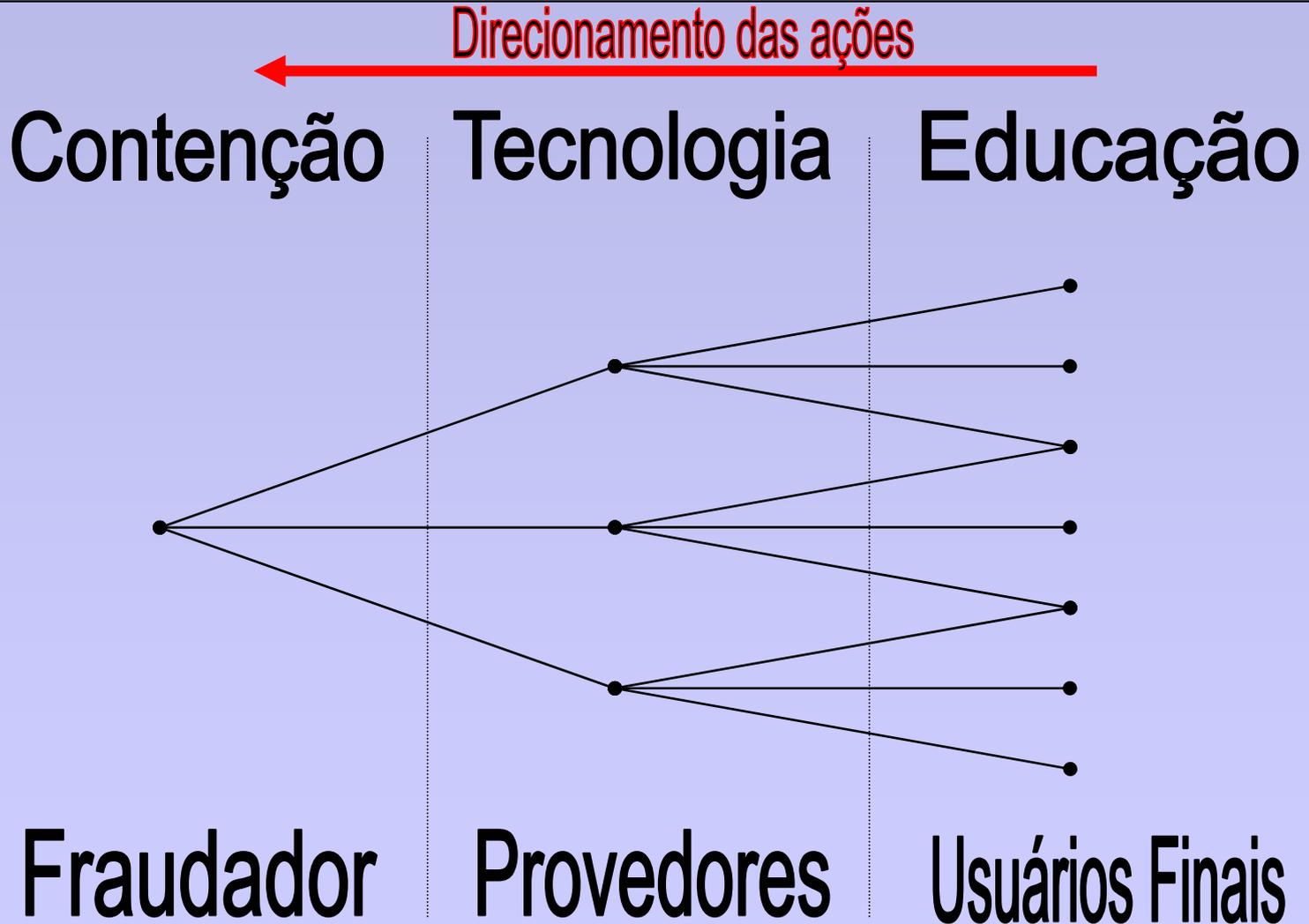


# Possíveis evoluções das ameaças

---

- Implementação de programas não detectáveis através de antivírus / anti-trojans;
- Fortificação na codificação dos dados capturados;
- Segmentação dos ataques SCAM e PHISHING;
- Utilização de outros vetores para o ataque e outros protocolos para o envio de informações capturadas;
- Realização de transações automatizadas pelo trojan no momento da captura da autenticação (Man-In-The-Middle pré-programado).

# Modelo de mitigação



# Modelo de mitigação

---

- Criação de mecanismos de proteção podem encarecer a implementação de trojans e envio de SPAMs, tornando inviável esta modalidade de fraude;
- Conscientização do usuário final é essencial para que ele participe no processo de proteção contra este tipo de ameaça;
- Tornando visível e frequente a punição jurídica. O crime decresce ao passo que a punição é factível (presente) e severa.

# Recomendações Finais

---

- Mantenha atualizado o sistema operacional e browser por meio de patches;
- Instale um antivírus e o mantenha atualizado;
- Instale um firewall e o mantenha bem configurado\*;
- Não acesse links de e-mails suspeitos. Elimine estas mensagens de sua caixa de entrada.

Lembre-se: “Tenha um computador para o trabalho e outro para o lazer”

---

# Perguntas



**Marcelo Lau**  
**marcelo.lau@poli.usp.br**