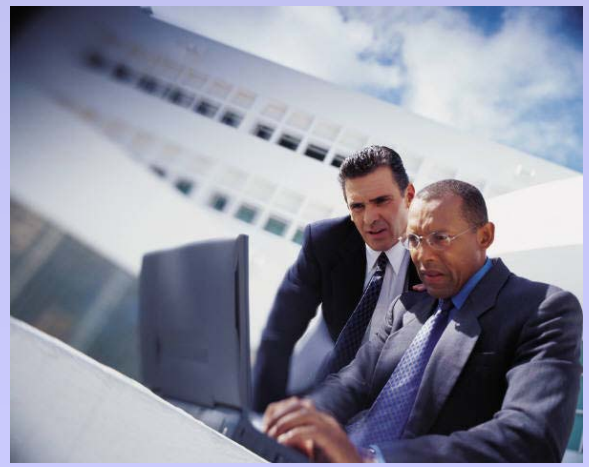
Fraude via e-mail por meio de Cavalos de Tróia e Clonagem de sites financeiros

Marcelo Lau
marcelo.lau@poli.usp.br



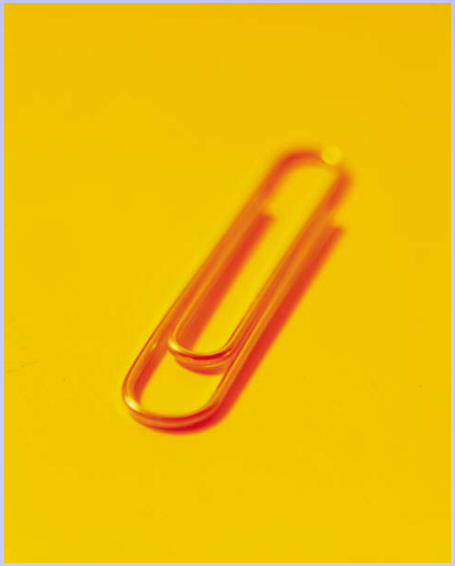
12/11/2004

SSI2004

Agenda

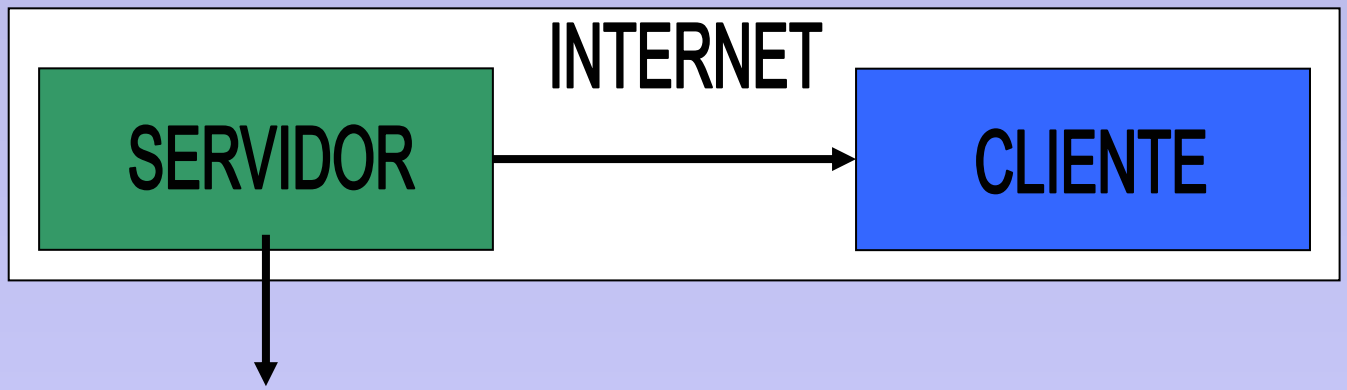
- Modelagem do problema
- Análise do SCAM
- Ferramentas de análise
- Análise do PHISHING
- Informações na Internet
- Considerações finais

Modelagem do problema



Modelagem do problema

Disponibilização do serviço

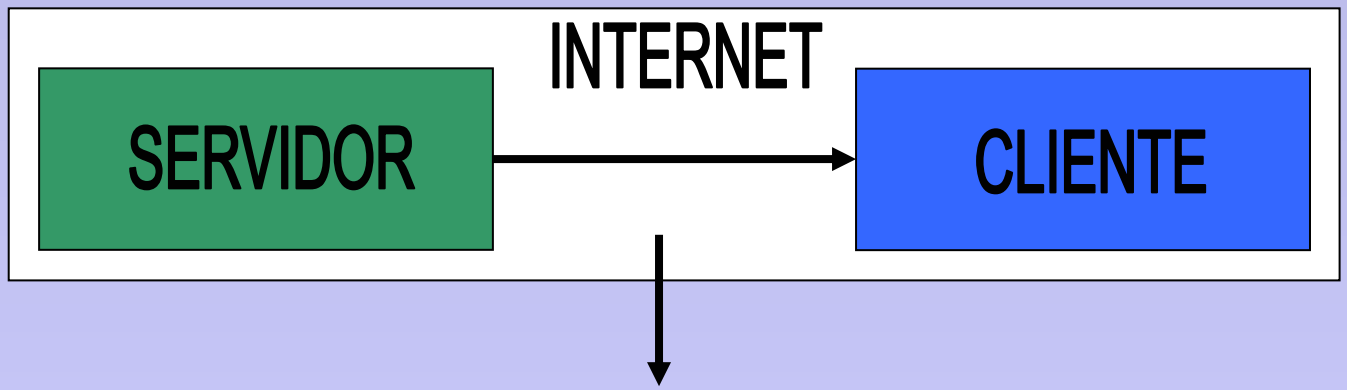


A porção Servidor disponibiliza o acesso ao serviço transacional (financeiro). Este ambiente em geral é uma interface de acesso a dados e transações que são armazenadas em outros ambientes ou sistemas.

Nível de proteção do ambiente : MÉDIO / ALTO

Modelagem do problema

Disponibilização do serviço



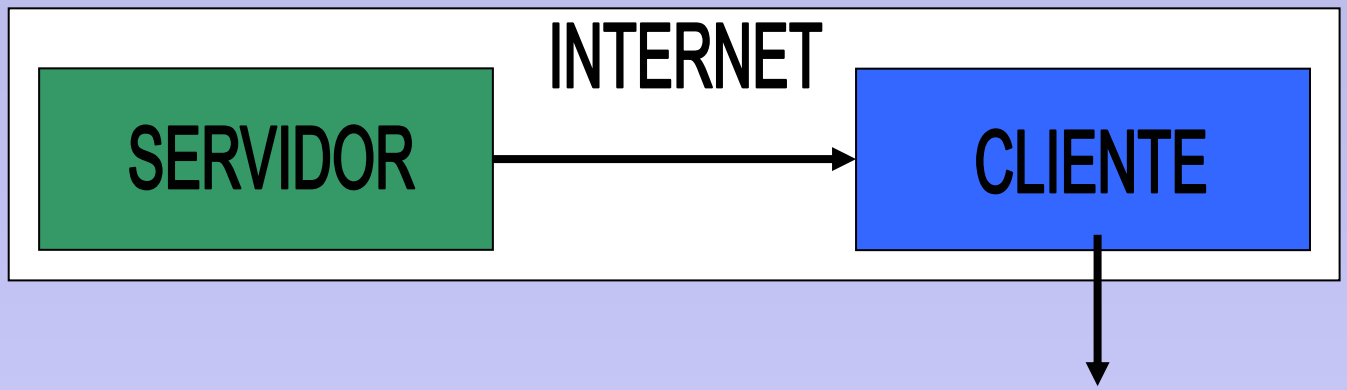
A linha de comunicação utiliza protocolo de comunicação HTTPS. A confidencialidade é garantida através de chaves assimétricas RSA de 1024 bits. (E chaves de sessão simétricas de 40 e 128 bits)

Nível de proteção do ambiente : MÉDIO* / ALTO

* Elementos de comunicação / Serviço de DNS

Modelagem do problema

Disponibilização do serviço

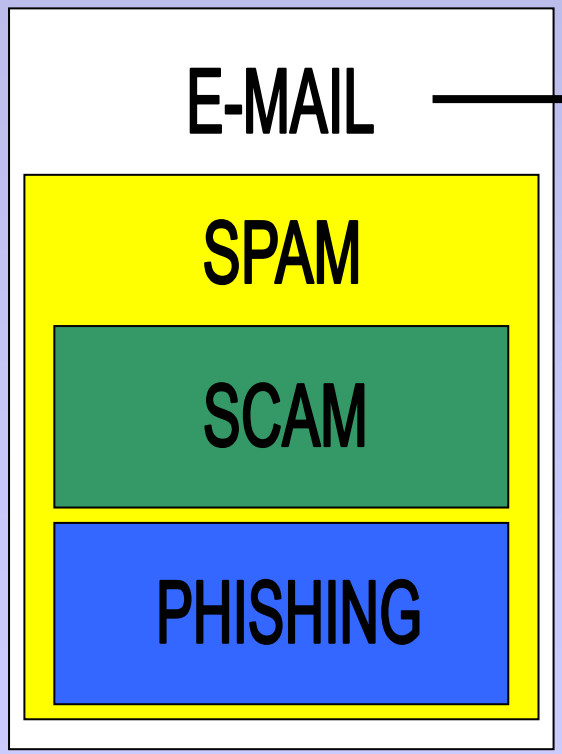


A porção Cliente é a interface utilizada para a realização de transações financeiras e acesso a outros serviços no ambiente Internet. Browser e Sistema Operacional são os principais itens do cliente.

Nível de proteção do ambiente : BAIXO

Modelagem do problema

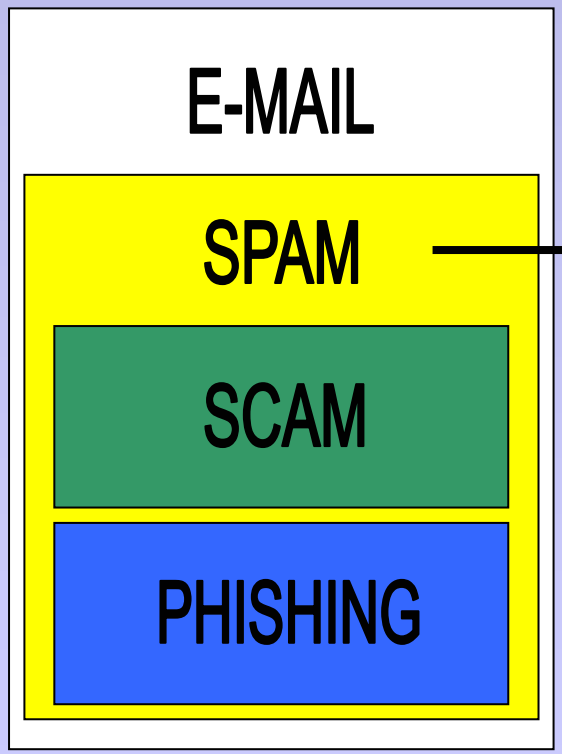
Vetor de Propagação



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



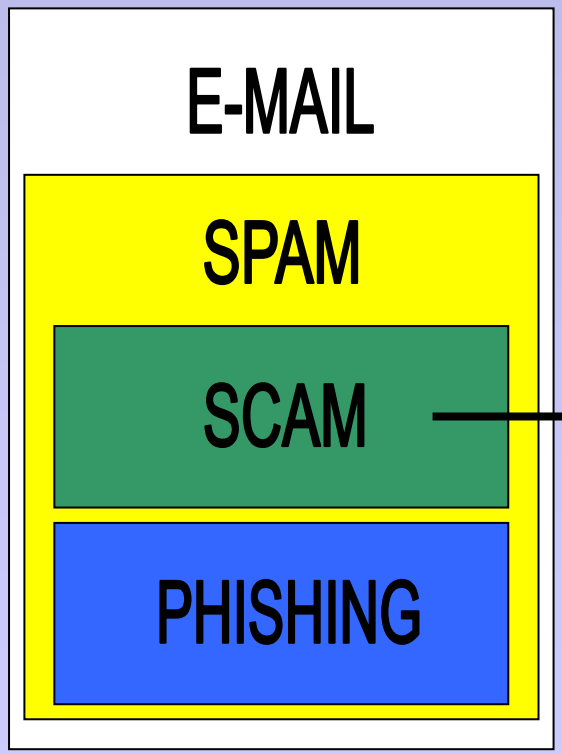
O SPAM é uma mensagem eletrônica não solicitada, enviada indiscriminadamente a múltiplas caixas postais eletrônicas, não permitindo aos usuários destas caixas postais a escolha de recebê-las.

É SPAM :

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

Modelagem do problema

Vetor de Propagação



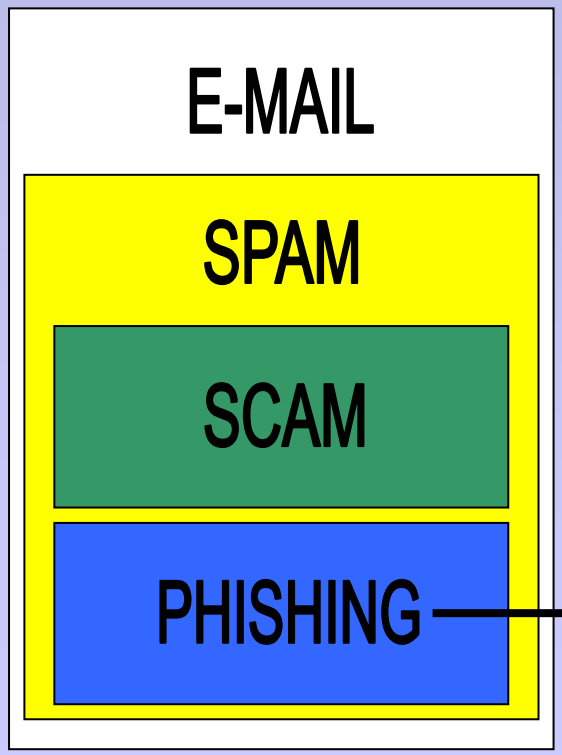
O SCAM é outro tipo de mensagem eletrônica repudiada pelos usuários, pois além de causar desconforto aos usuários de caixas postais, como o SPAM, eles apresentam natureza fraudulenta.

Exemplos de SCAMs:

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

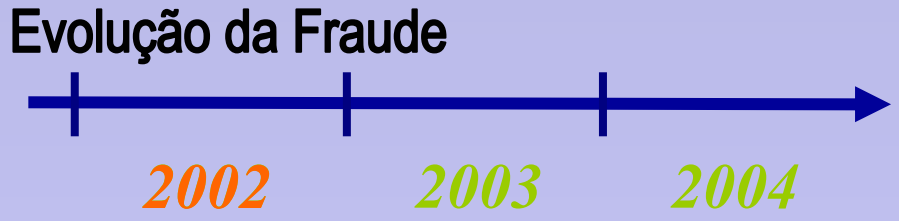
Modelagem do problema

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



• 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);

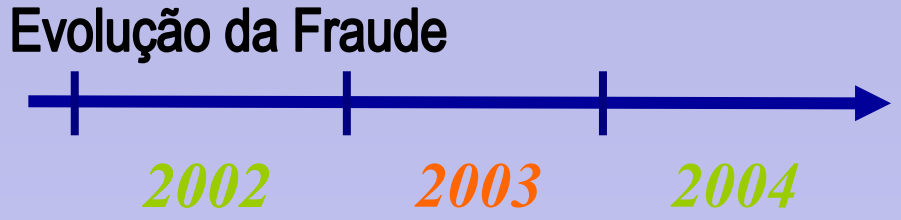
• Com o passar dos meses os Keyloggers permitem associação da identificação de tela da aplicação com o dado capturado;

• 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



• 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;

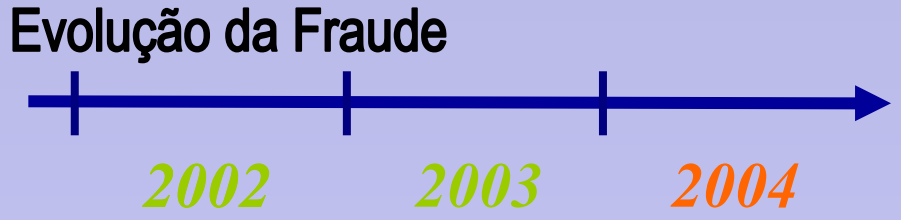
• Com o passar dos meses Keyloggers e Screenloggers são preparados para capturar dados de páginas específicas em browsers;

• 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



• 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.

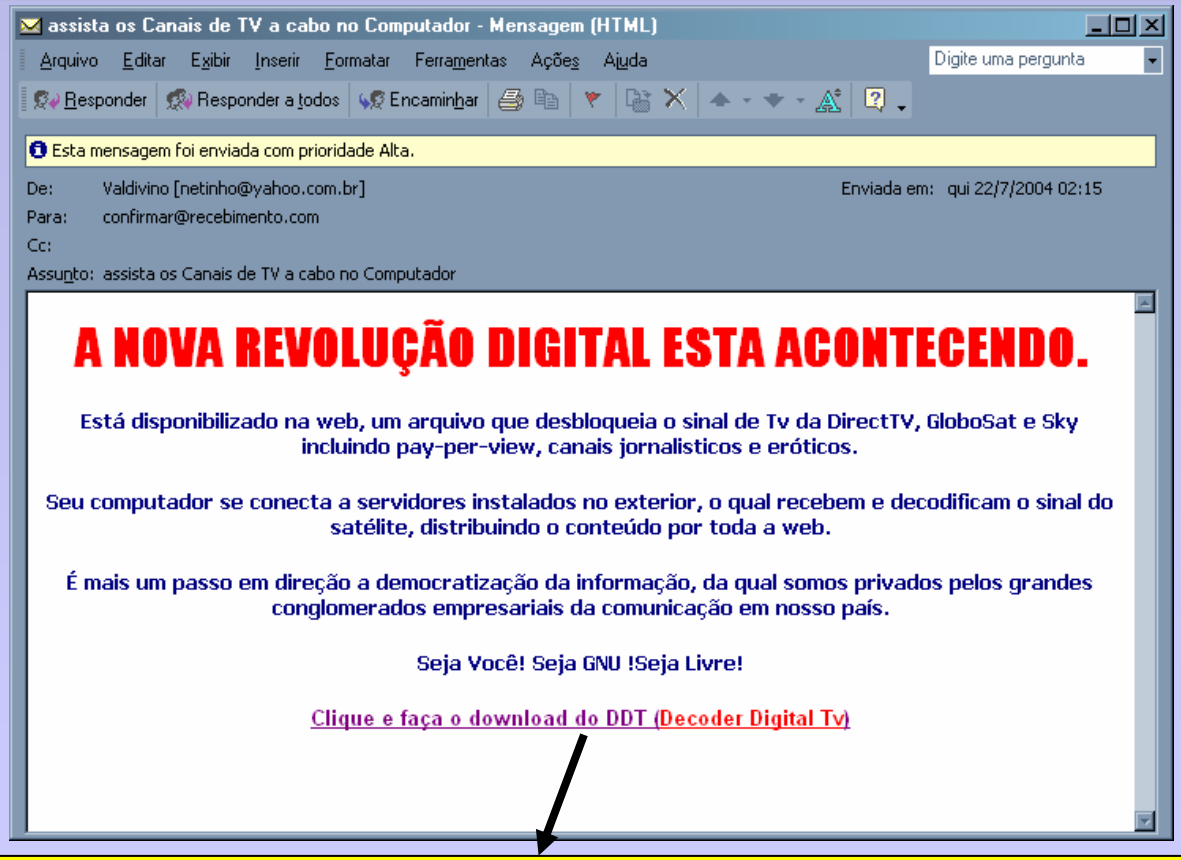
Modelagem do problema

Evolução da Autenticação

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

Análise do SCAM

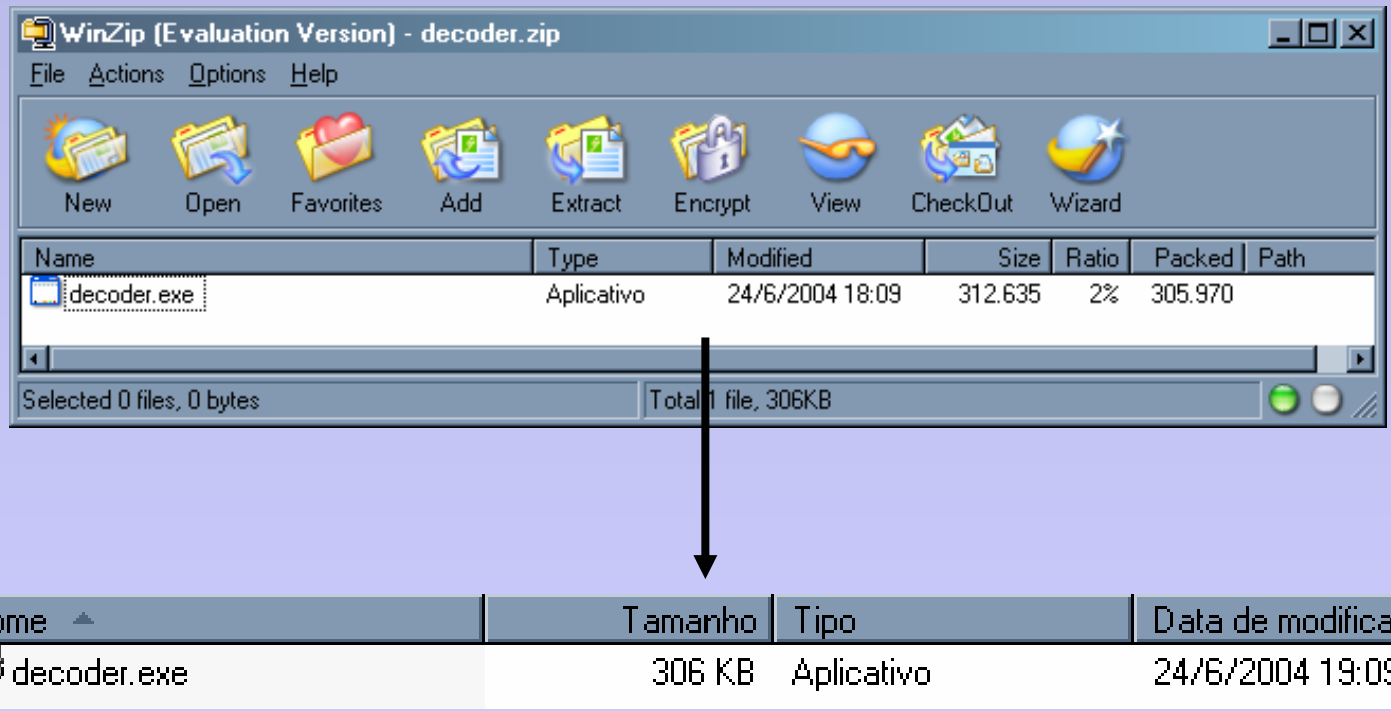
Análise do SCAM



****

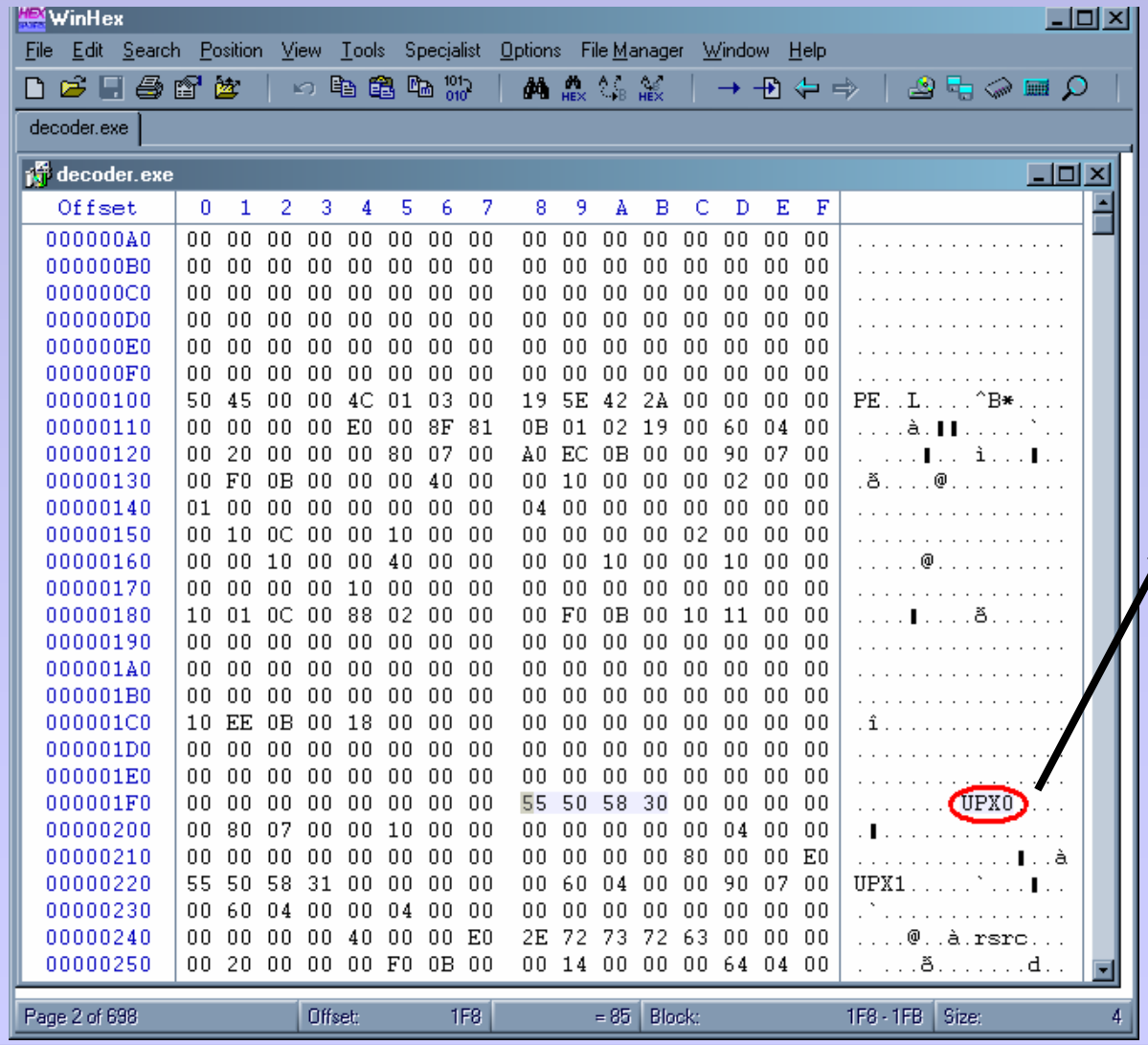
Clique e faça o download do DDT (Decoder Digital Tv)</p>

Análise do SCAM



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

Análise do SCAM



Característica de compactação

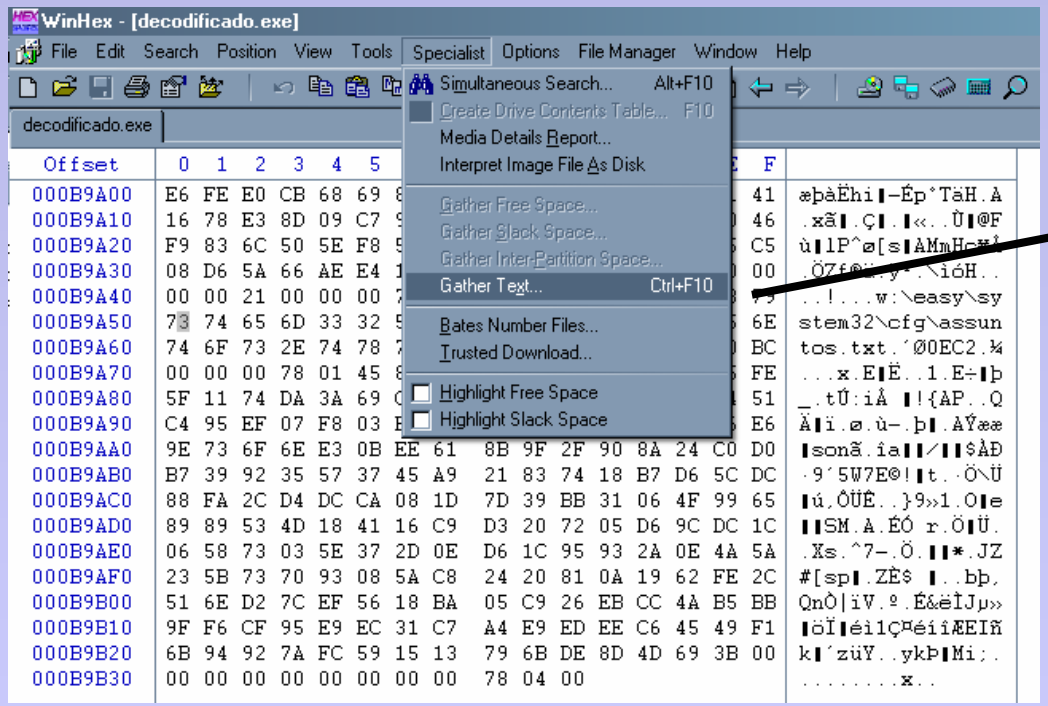
Ultimate Packer for eXecutables
http://upx.sourceforge.net

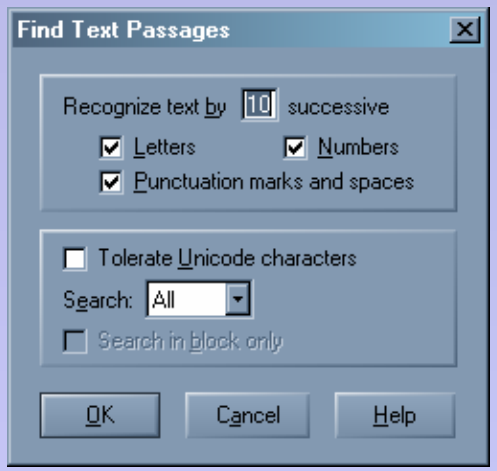
Análise do SCAM

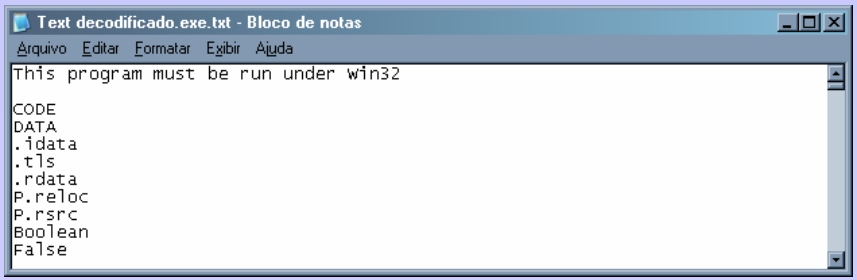
```
C:\upx>upx -d -o decodificado.exe decoder.exe
                       Ultimate Packer for eXecutables
          Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001, 2002
UPX 1.24w        Markus F.X.J. Oberhumer & Laszlo Molnar          Nov 7th 2002

        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

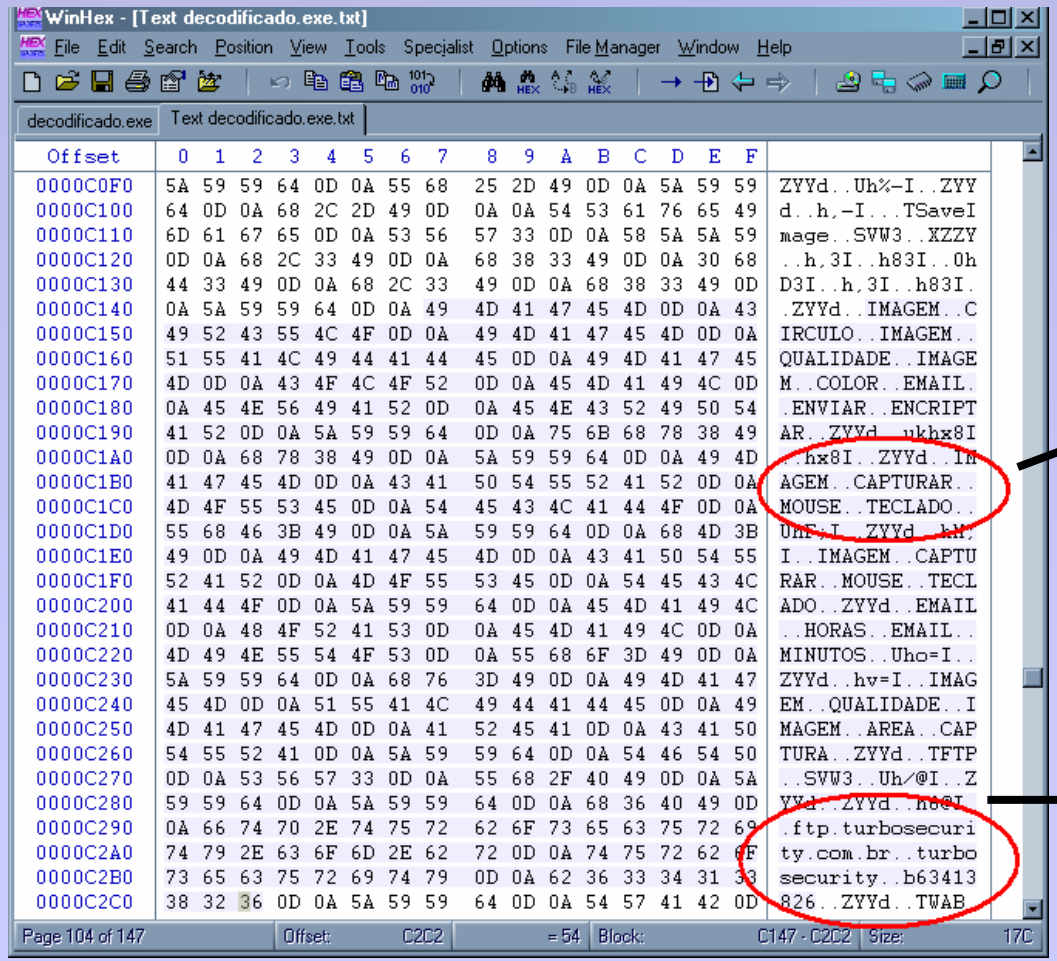
Análise do SCAM







Análise do SCAM



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;

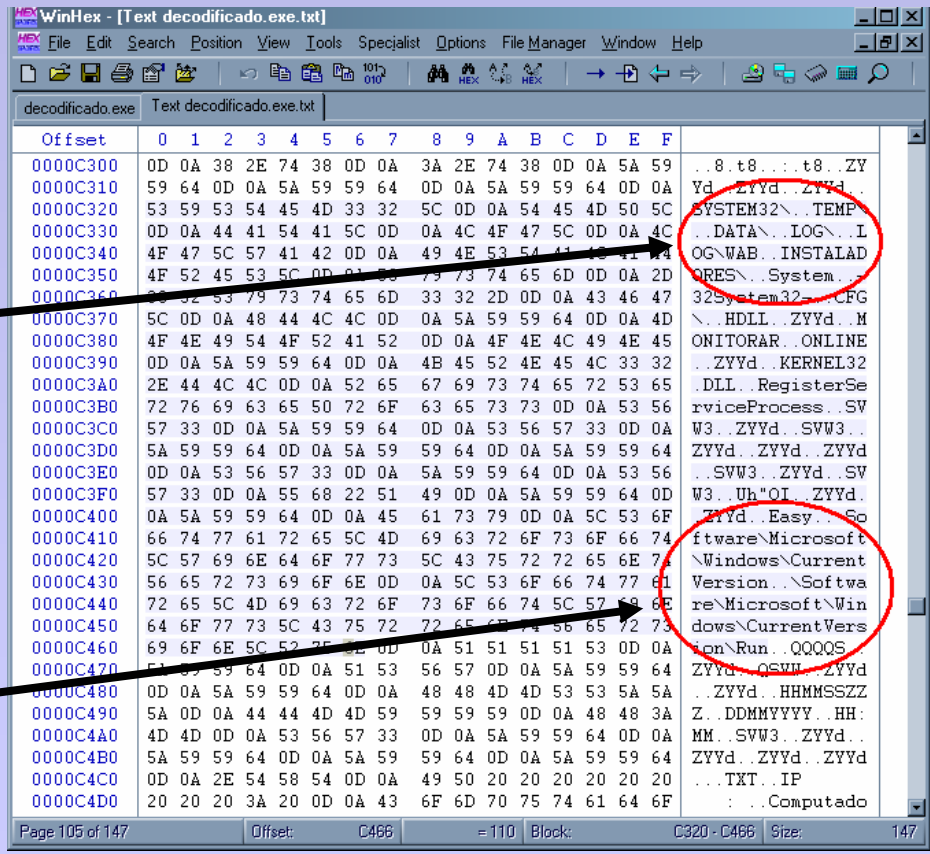
✓ c:\windows\system\system32\log;

✓ c:\windows\system\schost.exe.

- Alterações no sistema de registro:

✓ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN

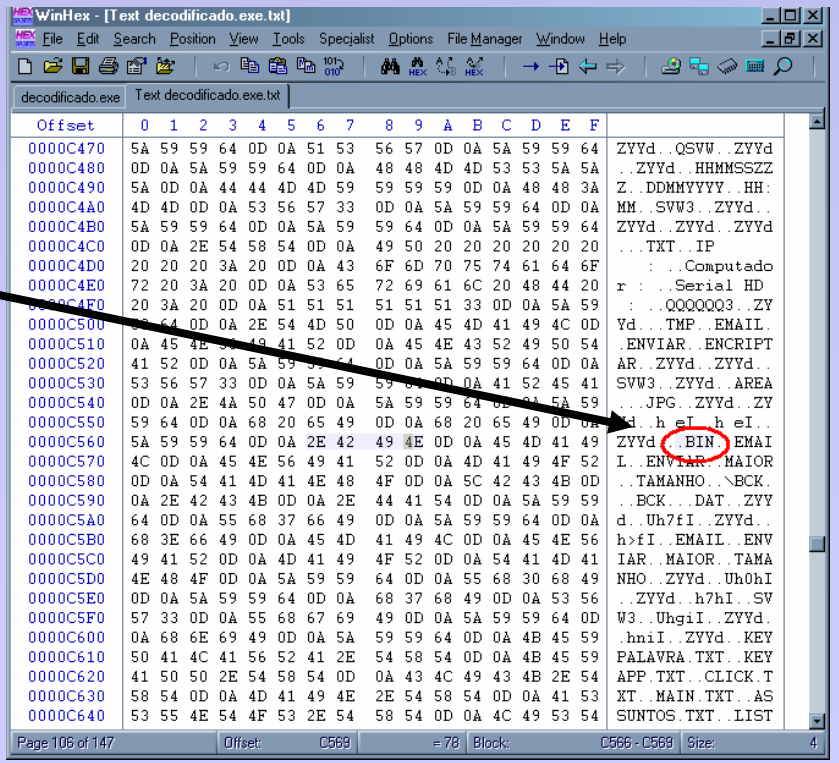
✓ Chave:
SYSTEM = "c:\windows\system\schost.exe"



Análise do SCAM

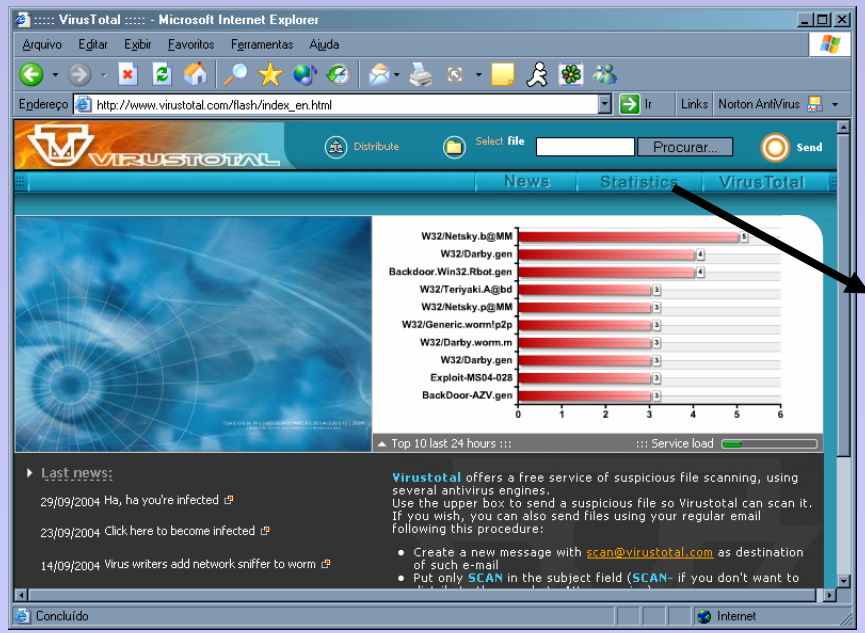
- Envio de e-mail usando protocolo POP3:
  - ✓ Servidor: "pop.vip.sc5.yahoo.com“;
  - ✓ User: "marcoalui“;
  - ✓ Senha: "988jlsgg“.

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



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);

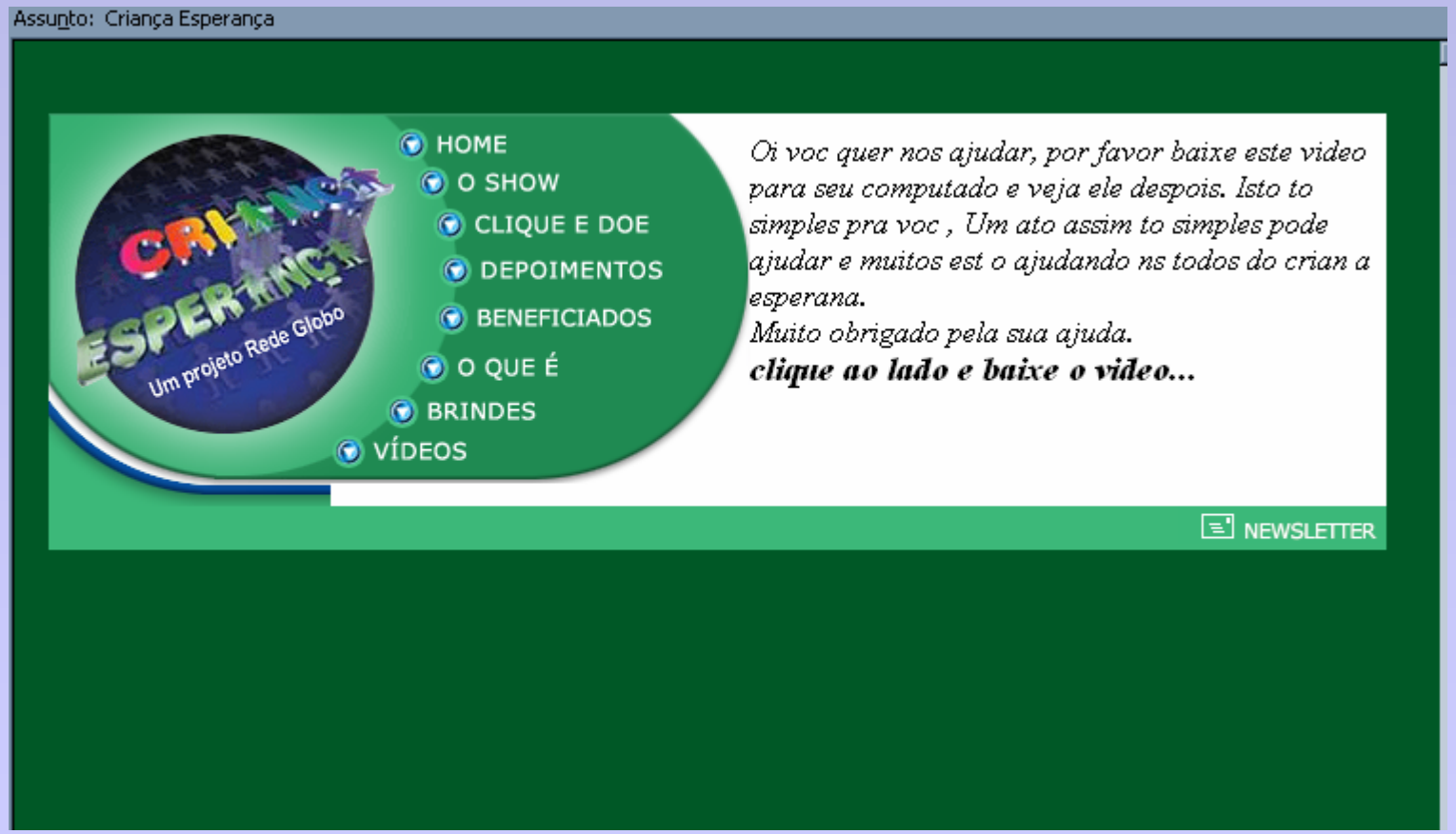
SCAM – Chaves de Registro

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\KnownDLLs
- HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\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

SCAM –Teclados Falsificados

SCAM - Exemplos



SCAM - Exemplos

Assunto: FW: Notificaçao de Pendencias financeitas!!

CDL Câmara de Dirigentes Lojistas

SPC 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 deseu computador.

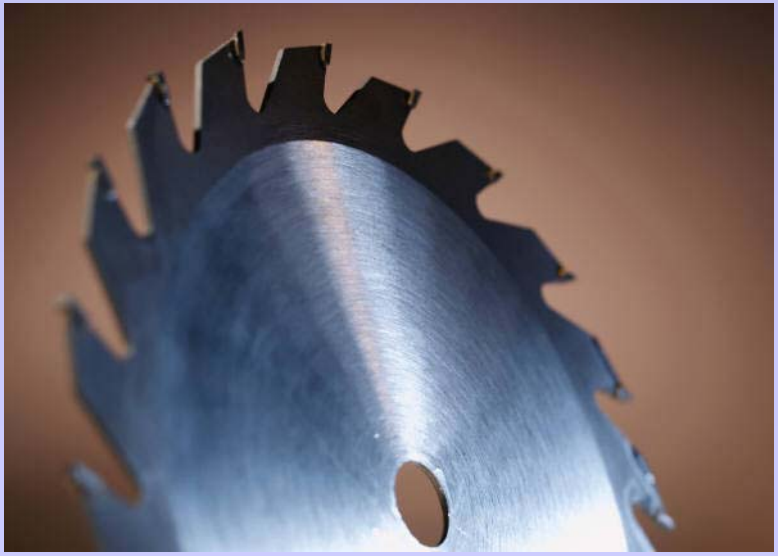
Microsoft

Microsoft - Proteja seu PC

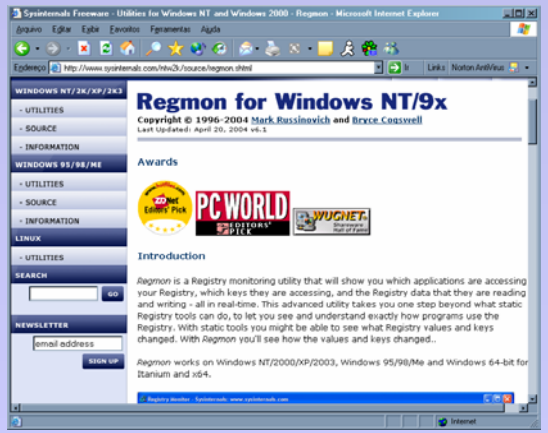
Nosso filtro de emails detectou em sua caixa postal arquivos maliciosos,
que podem causar danos a seu computador enviando mensagens indesejadas e comprometendo
sua segurança. Atualize seu computador usando nossa mais nova ferramenta de segurança e anti-spam
Email-scan

Microsoft Email-scan

Ferramentas de análise



Sysinternals : Registry Monitor



Registry Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

#	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

File Monitor - Sysinternals: www.sysinternals.com

File Edit Options Volumes Help

#	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

Process Explorer - Sysinternals: www.sysinternals.com

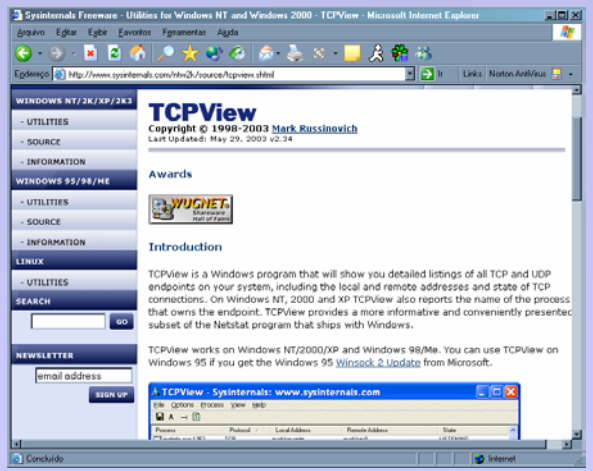
File Options View Process Find Handle Help

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
AGEN C:\WINDOWS\SYSTEM32\SERVICES.EXE			ent S...	Microsoft Corporation
SVCHOST.EXE	1316		Generic Host Pro...	Microsoft Corporation
S24EvMon.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\SvcctrlStartEvent_A3752DX
Event	\BaseNamedObjects\ScNetDrvMsg
Event	\BaseNamedObjects\WBEM_ESS_OPEN_FOR_BUSINESS
Event	\BaseNamedObjects\PnP_No_Pending_Install_Events
Event	\BaseNamedObjects\userenv: User Profile setup event
File	\Device\NamedPipe\ntsvcs
File	\Device\NamedPipe\ntsvcs
File	\Device\NamedPipe\ntsvcs
File	\Device\NamedPipe\ntsvcs
File	\Device\KsecDD

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

Sysinternals : TCPView

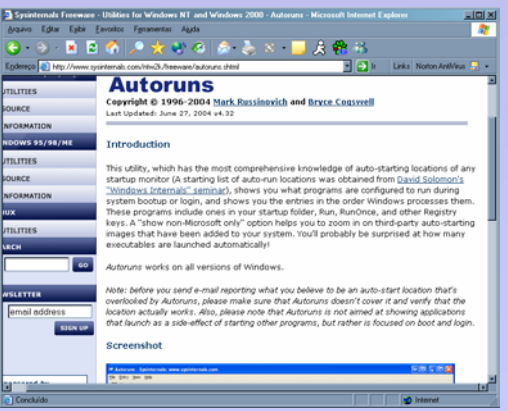


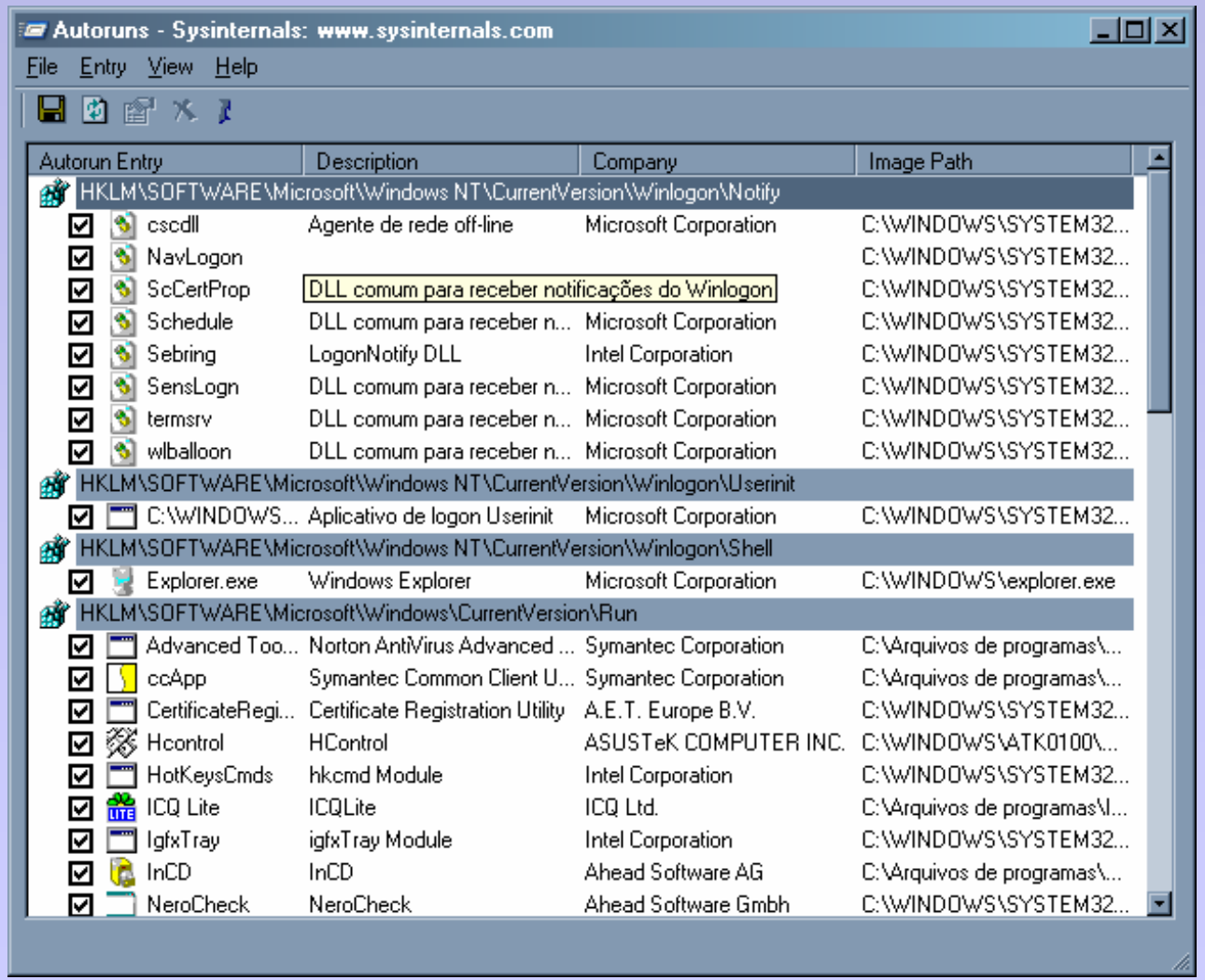
TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

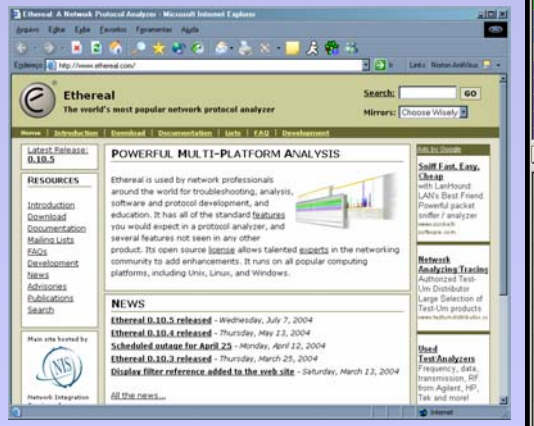
Process	Protocol	Local Address	Remote Address	State
aim.exe:568	TCP	A1A:3198	A1A:0	LISTENING
aim.exe:568	TCP	A1A:3222	A1A:0	LISTENING
aim.exe:568	TCP	A1A:5180	A1A:0	LISTENING
aim.exe:568	TCP	a1a:3198	205.188.8.179:5190	ESTABLISHED
aim.exe:568	TCP	a1a:3222	205.188.10.216:5...	ESTABLISHED
ALG.EXE:1388	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





Ethereal



few packets.cap - Ethereal

File Edit View Capture Analyze Help

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=65
14	14.817689	0.000119	192.168.0.2	192.168.0.10	TCP	80 > 1242 [SYN, ACK] Seq=3661615104 Ack=1404
15	14.818178	0.000489	192.168.0.10	192.168.0.2	TCP	1242 > 80 [ACK] Seq=1404510824 Ack=366161510
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=140451123
23	19.382555	4.406740	192.168.0.10	192.168.0.2	TCP	1242 > 80 [FIN, ACK] Seq=1404511234 Ack=3661
24	19.382634	0.000079	192.168.0.2	192.168.0.10	TCP	80 > 1242 [ACK] Seq=3661615105 Ack=140451123
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=65
55	58.137176	0.000113	192.168.0.2	192.168.0.10	TCP	135 > 1244 [SYN, ACK] Seq=3672465192 Ack=141
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 AddToSet=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 AddToSet=0 DelFromSet=1[

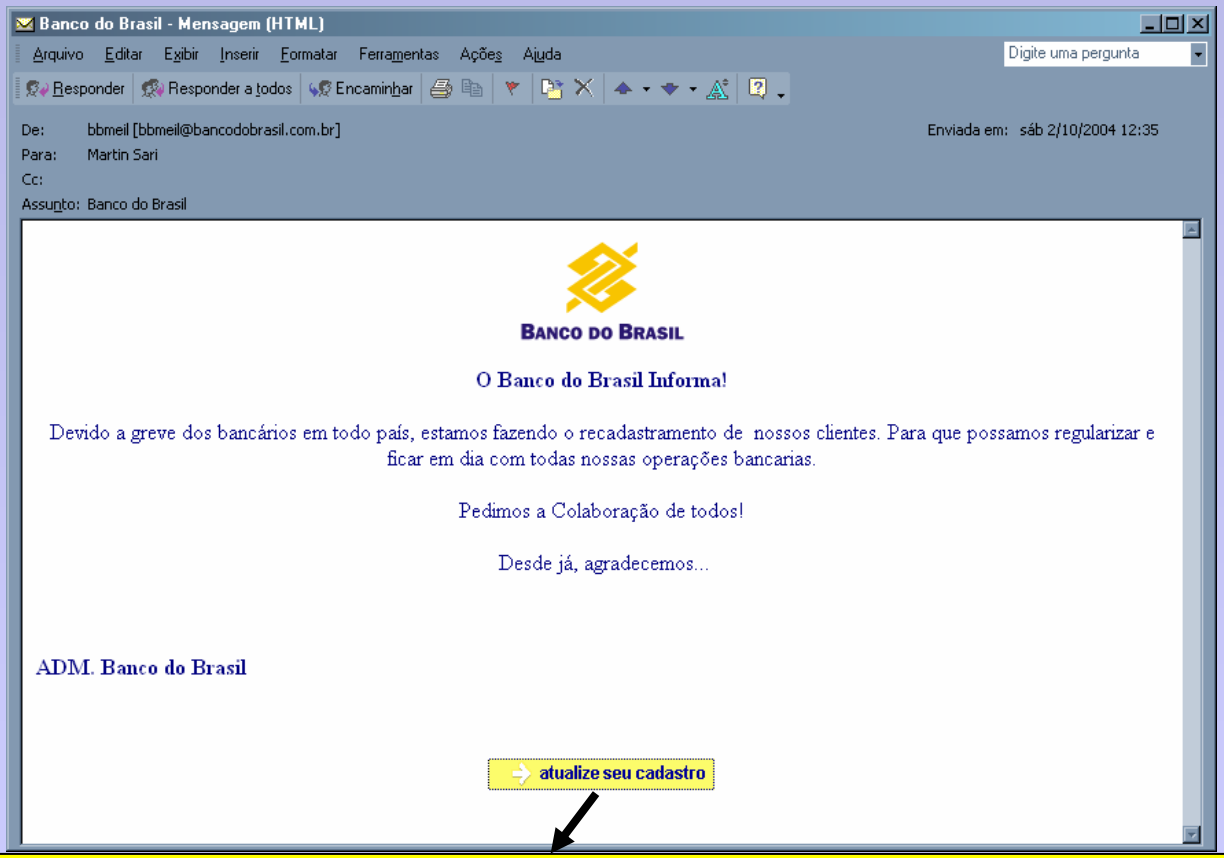
```
▷ Frame 16 (464 bytes on wire, 464 bytes captured)
▷ Ethernet II, Src: 00:04:61:4a:1e:95, Dst: 00:0b:5d:20:cd:02
▷ Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: 192.168.0.2 (192.168.0.2)
▷ Transmission Control Protocol, Src Port: 1242 (1242), Dst Port: 80 (80), Seq: 1404510824, 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=
    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
```

```
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  31 36 38 2e 30 2e 32 0d  0a 55 73 65 72 2d 41 67   168.0.2. .User-Ag
```

Filter: tcp | Expression... | Clear | Apply | File: few packets.cap 24 KB 00:0 | P: 104 D: 19 M: 0

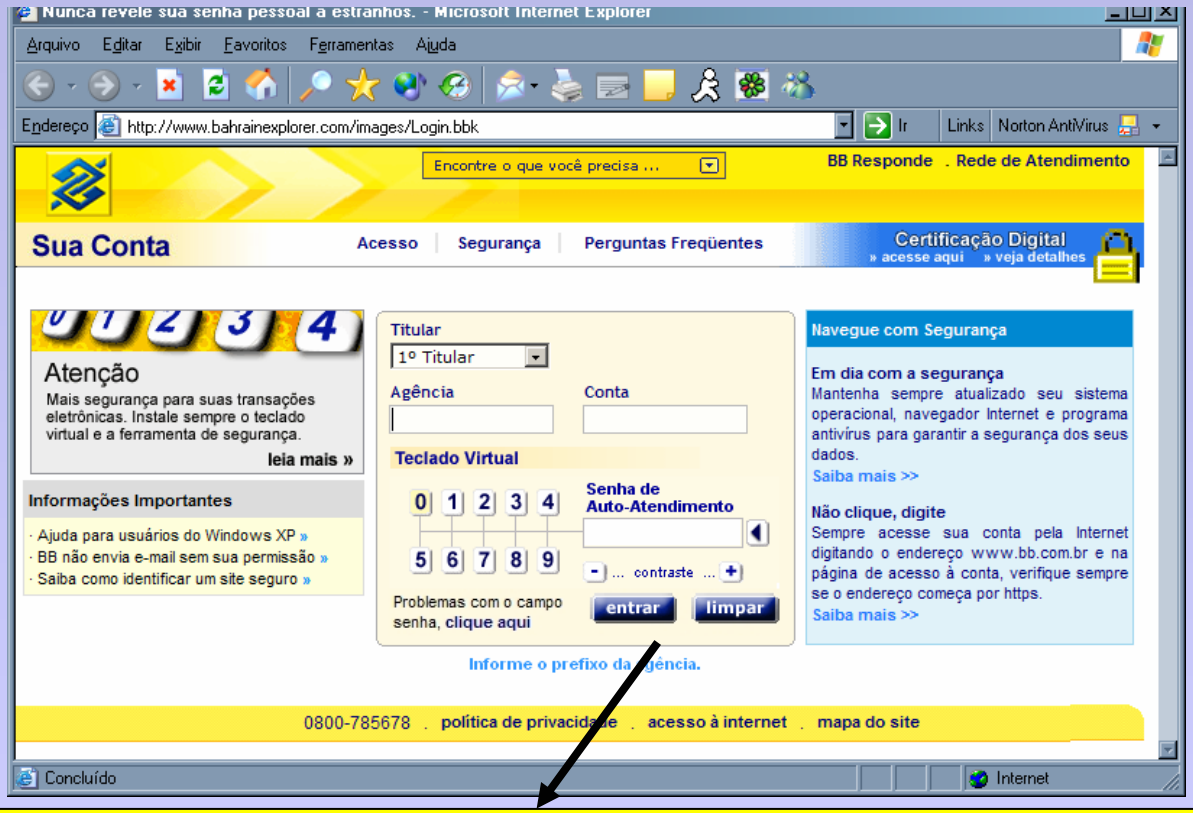
Análise do PHISHING

Análise do PHISHING




```
href="http://www.bahrainexplorer.com/images/Login.bbk">
<img height="23" alt="Atualize seu cadastro"
     src="http://www.bb.com.br/portal/img/btAtualizeCadastro.gif"
```

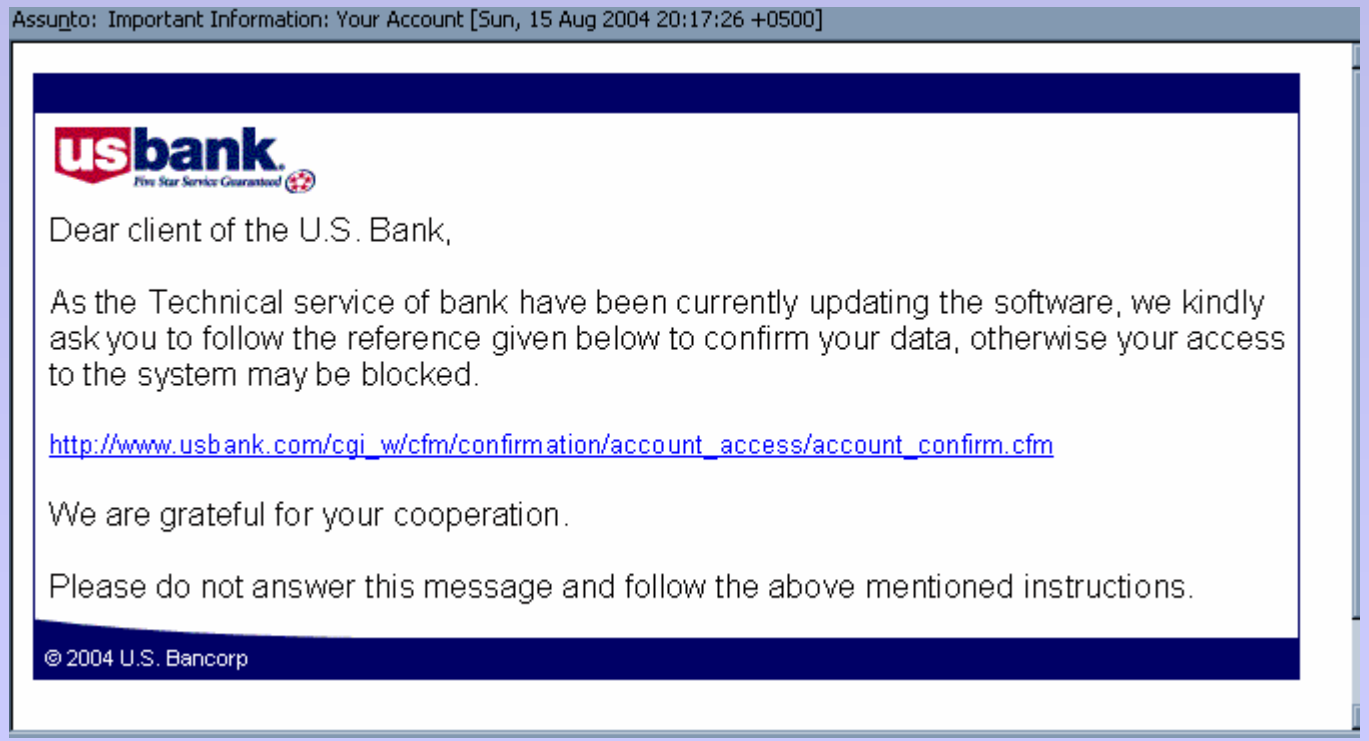
Análise do PHISHING



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

PHISHING - Exemplos

PHISHING - Exemplos



PHISHING - Exemplos

BANCO CENTRAL DO BRASIL

De acordo com a LEI Nº 10.216, DE 8 DE DEZEMBRO DE 2003 , as contas de depósito (correntes ou poupanças), cujo titulares não efetuarem o recadastramento eletrônico serão bloqueadas a partir de 20 DE FEVEREIRO DE 2004. Visando agilizar o processo de recadastramento, o Banco Central está disponibilizando através deste e-mail os links dos bancos que possuem a maior incidência de fraudes, para os correntistas efetuarem o recadastramento dos dados, esta medida visa combater a corrupção e eliminar a existência de contas fantasmas em nosso País. O processo é simples e rápido, para tanto, basta acessar o seu Banco através de um dos links abaixo, e preencher as informações que forem solicitadas.

Banco do Brasil - http://www.bb.com.br

Caixa Econômica Federal - http://www.caixa.gov.br

Bradesco - http://www.bradesco.com.br

Santander - http://www.santander.com.br

Cordialmente,

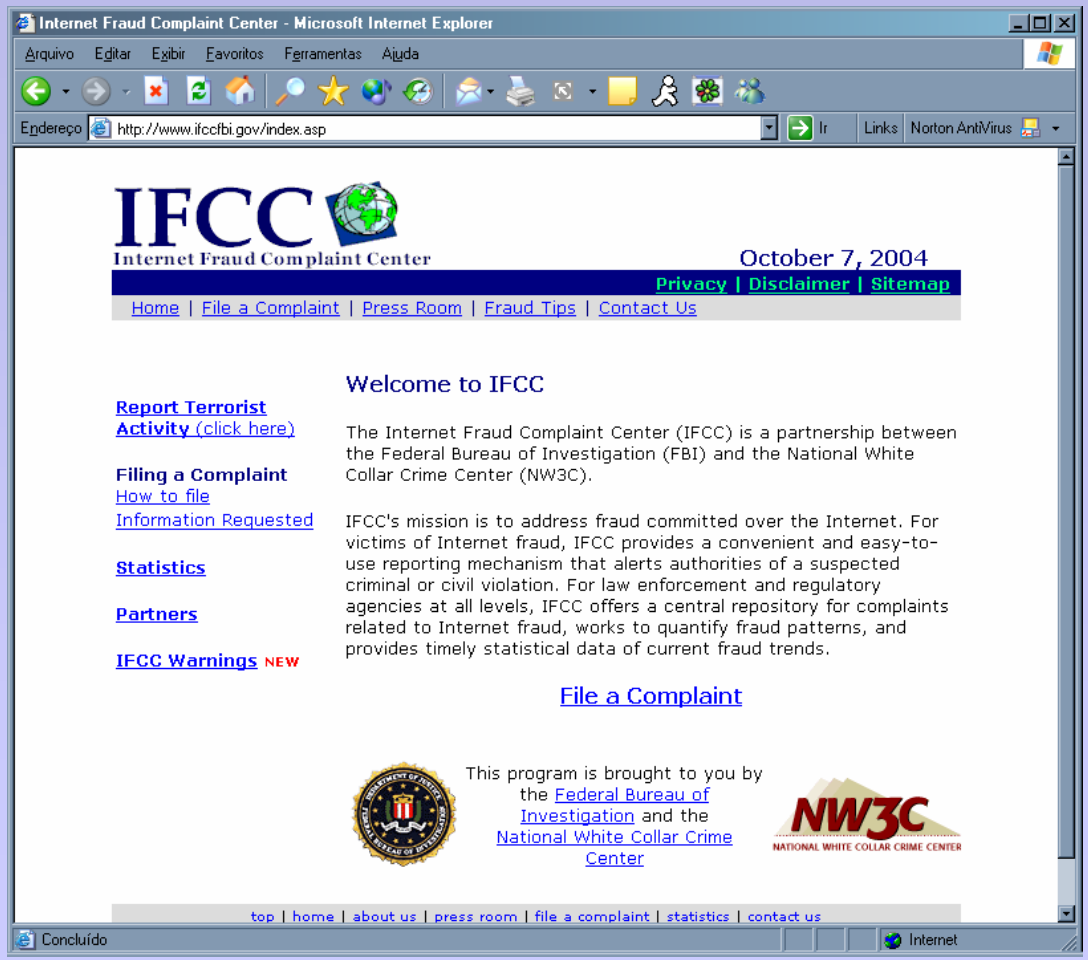
Henrique de Campos Meirelles
Presidente

Informações na Internet

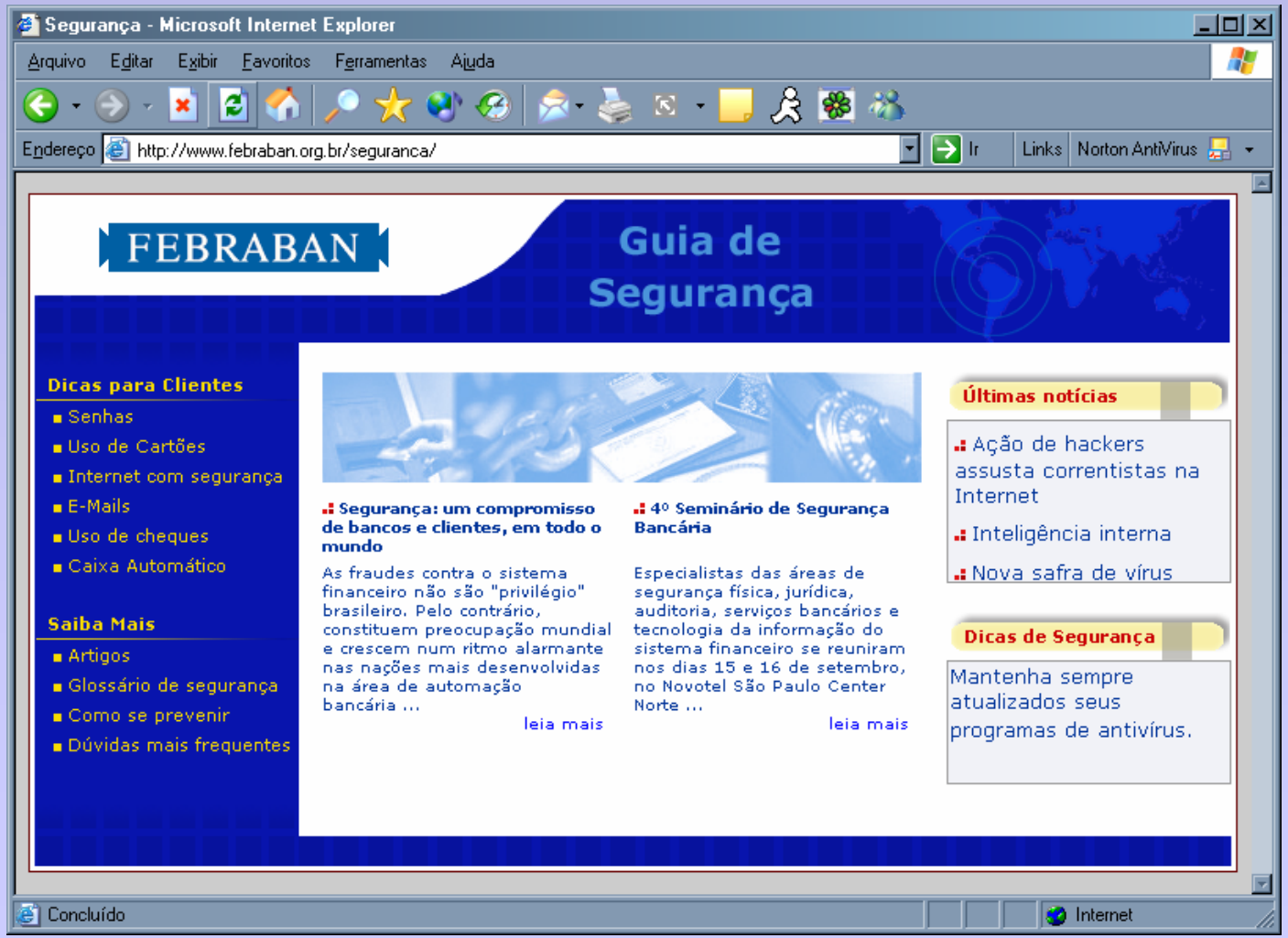
SCAM / PHISHING

Anti-Phishing Working Group

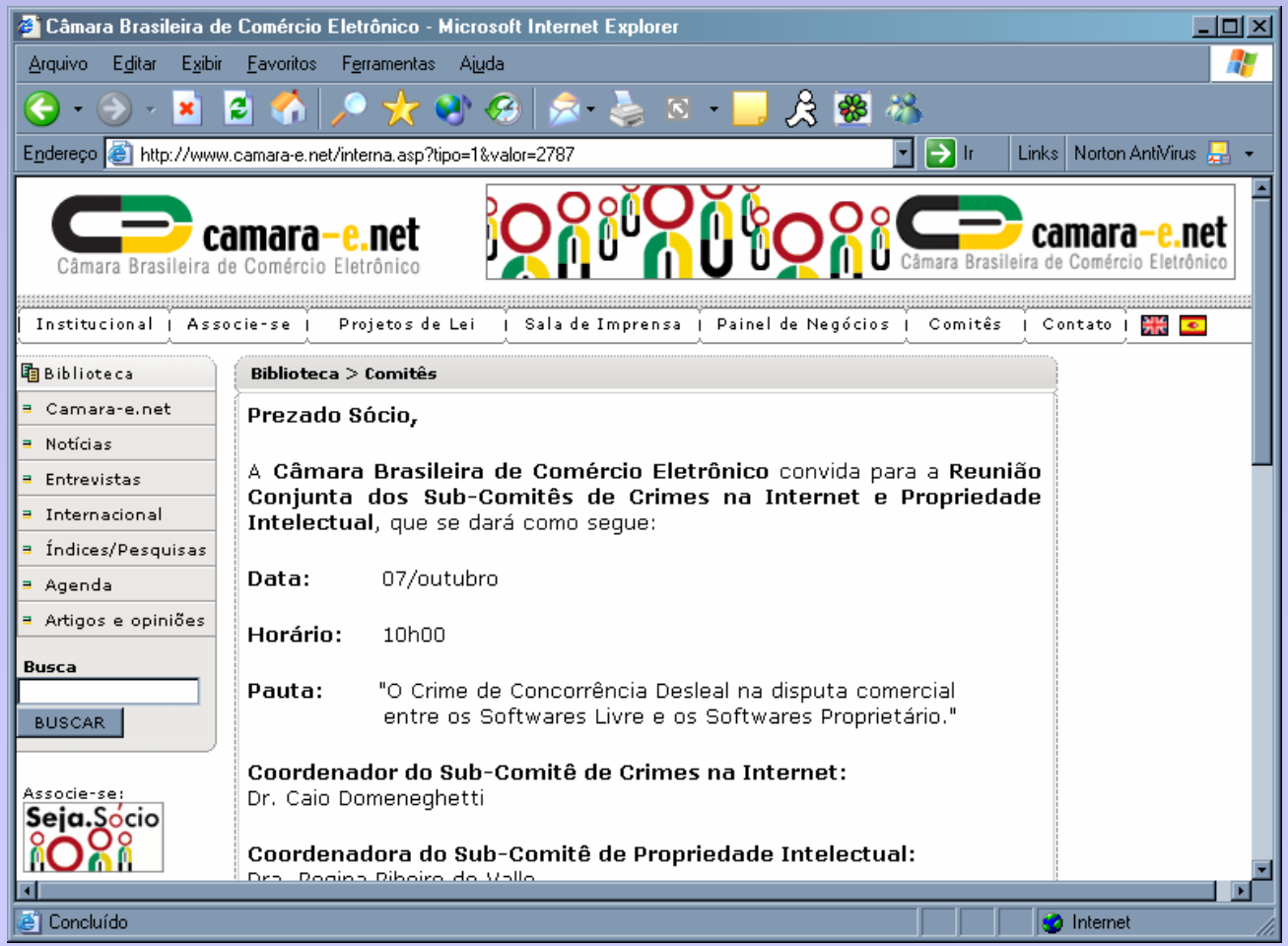
Internet Fraud Complaint Center



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

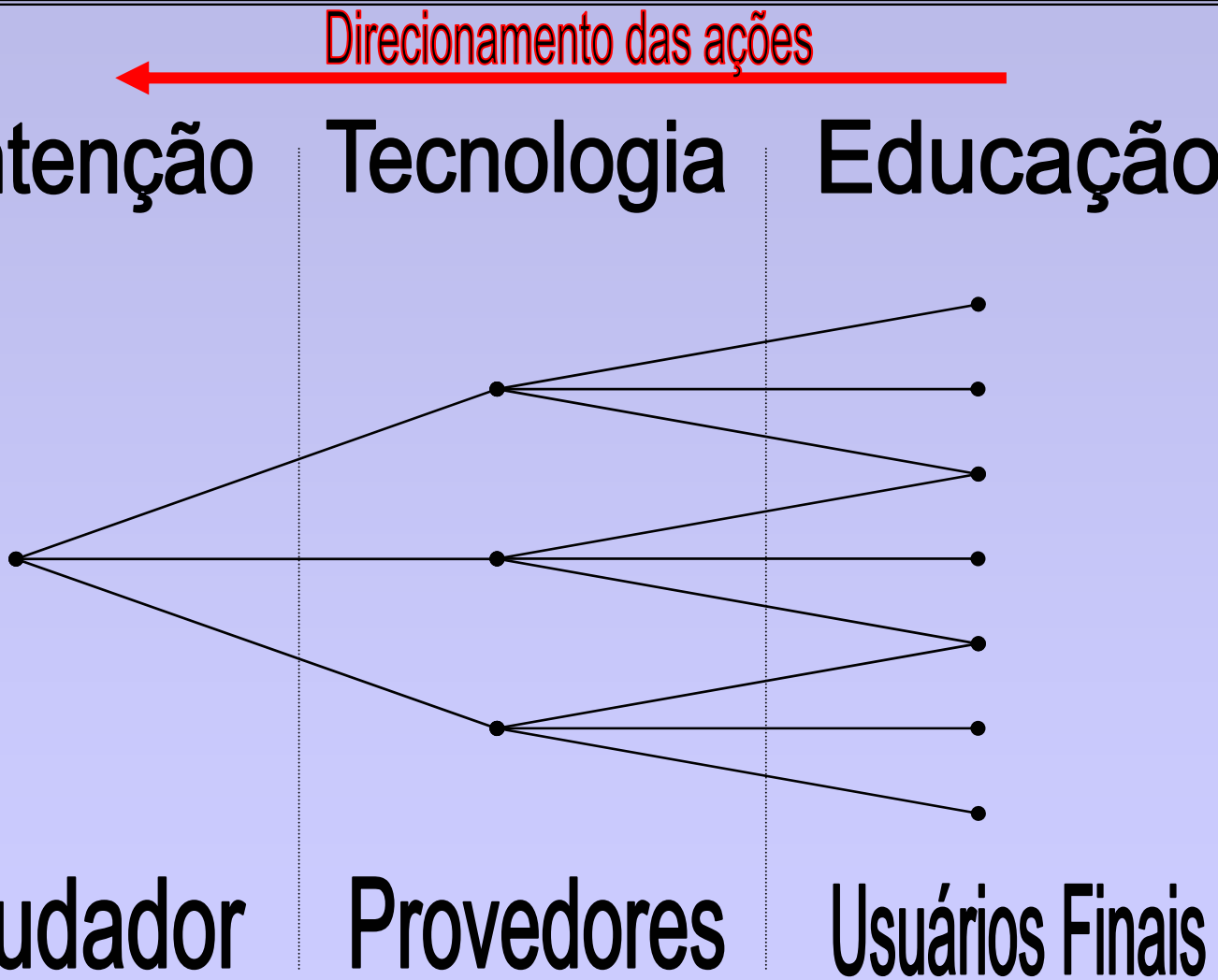

Câmara Brasileira de Comércio Eletrônico - Microsoft Internet Explorer
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço http://www.camara-e.net/interna.asp?tipo=1&valor=2787
Ir Links Norton AntiVirus
camara-e.net
Câmara Brasileira de Comércio Eletrônico
Institucional | Associe-se | Projetos de Lei | Sala de Imprensa | Painel de Negócios | Comitês | Contato
Biblioteca
Camara-e.net
Notícias
Entrevistas
Internacional
Índices/Pesquisas
Agenda
Artigos e opiniões
Busca
BUSCAR
Associe-se:
Seja.Sócio
Biblioteca > Comitês
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:
Concluído
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