DEPARTAMENTO DE POLÍCIA FEDERAL
SUP. DO ESTADO DE SANTA CATARINA
SETOR TÉCNICO-CIENTÍFICO

PERÍCIA E INFORMÁTICA FORENSE

PCF LUCIANO PETINATI FERREIRA
petinati.lpf@dpf.gov.br

RESUMO

- Apresentar os delitos praticados no espaço cibernético;
- Apresentar, brevemente, a estrutura do Departamento de Polícia Federal;
- Condução do processo investigativo;
- Atuação do PCF (área de informática);
- Ferramentas;
- Casos;
- Desafios;
- Perguntas;

INTRODUÇÃO

- Com a popularização da computação pessoal e do acesso a Internet, as atividades humanas passaram a contar com um ambiente de expressão e comunicação extremamente rico e dotado de possibilidades antes nunca vistas.
- Tal ambiente, realizado por sistemas de computador, também se tornou um espaço propício para a manifestação de condutas consideradas ilícitas por nosso ordenamento jurídico.

INTRODUÇÃO

- Vestígios em crimes relacionados a sistemas de computadores.
- Processamento de vestígios - técnicas especiais.
- A Polícia Federal vem se especializando:
  - recrutando mão-de-obra especializada,
  - adquirindo equipamentos de ponta
  - desenvolvendo abordagens e metodologias policiais mais inteligentes.

CRIMES RELACIONADOS A SISTEMAS DE COMPUTADORES

- Definição Crime Relacionado a Sistema de Computadores
  Atividade criminal, delituosa ou ilícita realizada por meio de, ou direcionada a, sistemas de computadores
- Várias denominações (inac
  - Crime virtual
  - Crime cibernético
  - Crime eletrônico
  - Crime digital
  - Crime por computador

CRIMES RELACIONADOS A SISTEMAS DE COMPUTADORES

- Modalidades
  - Crime praticado <u>por meio de</u> sistemas de computadores
    Ex.: estelionato, falsidade ideológica, violação de sigilo, incitação ao ódio racial e religioso, distribuição de pornografia infanto-juvenil, calúnia etc.
  - Crime praticado <u>contra</u> sistemas de computadores
    Ex.: acesso indevido a sistemas de computadores, indisponibilização criminosa de serviços, uso não-autorizado de recursos

CRIMES RELACIONADOS A SISTEMAS DE COMPUTADORES

- Crimes não-relacionados a sistemas de computadores também podem deixar vestígios "digitais", como
  - Arquivos em mídias/dispositivos de armazenamento

    Ex.: documentos, fotografias, "logs", listas de histórico etc.
  - Informações em bancos de dados
  - Comunicação via e-mail e Instant Messenger

    Ex.: MSN Messenger, Skype, Google
- Tais vestígios dão origem a evidências que exigem processamento específico para admissão em juízo

CRIMES RELACIONADOS A SISTEMAS DE COMPUTADORES

- Exemplos de práticas ilícitas bastante difundidas
  - Exploração não-autorizada de sistemas de computador

    Uso do sistema de computador de outrem para obter vantagem e/ou para causar danos a terceiros
  - "Spam"

    Propaganda não-solicitada enviada "em massa"
  - "Phishing Scam"

    Fraude visando induzir o usuário a realizar uma ação lesiva Ex.: fornecer informações sigilosas, instalar malwares

31/03/2008 - 17h14

Piratas virtuais picham suposto site da campanha de Obama

da **Folha Online**

PUBLICIDADE

Um site que supostamente pertence à campanha do candidato democrata às eleições dos Estados Unidos, Barack Obama, apareceu pichado nesta segunda-feira.

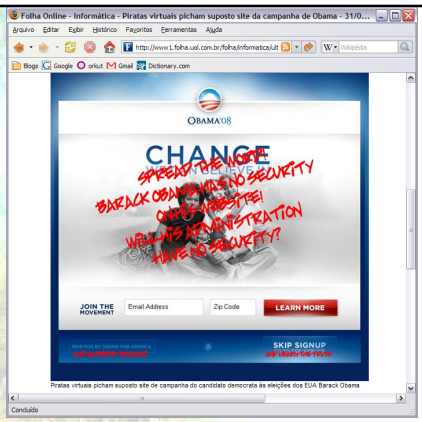
O Hope.net tem a mesma aparência do site oficial de Obama (que não foi invadido). A informação de que ele teria sido "hackeado" foi divulgada no Digg --mistura de blog, rede social e site de notícias.

Na mensagem deixada no endereço Hope.net, os invasores questionam a segurança do site e de um possível governo de Obama. "Espalhem a palavra! Barack Obama não tem segurança em seu site? Sua administração não terá segurança?", diz o texto.

No campo do site que informa que o site foi pago pela campanha do democrata, a mensagem é de que o doador foi "hackeado" por alguém que assina como Zhuangzi.

Os links na página remetem ao site de campanha de Hillary Clinton, concorrente de Obama na escolha pelo candidato democrata à presidência.

No próprio Digg, onde a notícia foi publicada, internautas discutem a possibilidade de se tratar realmente de uma invasão ou ser um site criado para passar esta impressão.



28/09/2010 - 18h19 / Atualizada 28/09/2010 - 18h40

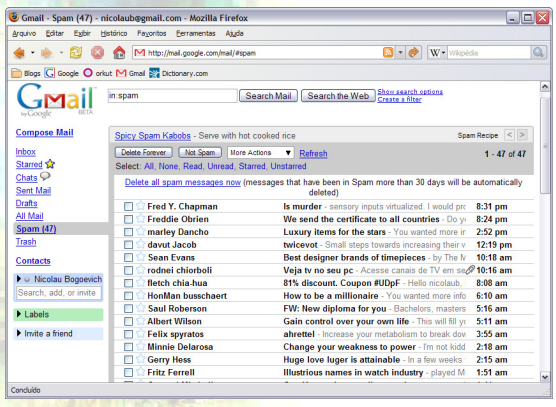
Site oficial de ex-candidato Joaquim Roriz sofre ataques via buscadores

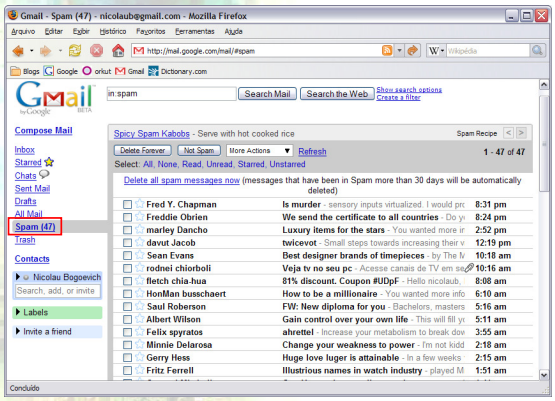
GUILHERME TAGIAROLI || Do UOL Tecnologia

Tweet 24 Recomendar Seja o primeiro de seus amigos a recomendar isso.

Ao tentar acessar site de Joaquim Roriz por serviços de busca, usuários lia para site falso acima

O site oficial de Joaquim Roriz, ex-candidato ao governo do Distrito Federal, sofreu uma série de ataques de hackers nesta semana. A partir de uma falha na página de Roriz, usuários que tentavam acessar o endereço por meio de serviços de busca, como Google e Bing, eram redirecionados para uma página fraudulenta com os dizeres "Ache solteiros Sexys em [área]!". Ao clicar na frase, o usuário era levado a um site de conteúdo adulto, voltado a usuários interessados em "sexo e swing".





13/70

11 de Fevereiro de 2008

Brasil já é o quarto no envio de spam

País sobe mais uma posição no ranking do lixo eletrônico e fica atrás apenas de EUA, Rússia e China

Segundo o último levantamento da empresa de segurança Sophos (que acaba de ser divulgado), o país subiu mais uma posição no ranking do spam e já ocupa o quarto lugar, com 4% de todo o volume enviado no último trimestre de 2007.

À frente do Brasil, apenas Estados Unidos, Rússia (que teve forte crescimento no período, saltando do quarto posto para o segundo) e China. Confira abaixo a lista dos 12 países que mais enviam mensagens indesejadas.

Posição	País/região	Porcentagem
1	Estados Unidos	21,3%
2	Rússia	8,3%
3	China	4,2%
4	Brasil	4%
5	Coréia do Sul	3,9%
6	Turquia	3,8%
7	Itália	3,5%
8	Polônia	3,4%
9	Alemanha	3,2%
10	Espanha	3, 1%
10	México	3,1%
12	Reino Unido	2,5%
Outros		35,7%

Por Daniel dos Santos às 12h07

FONTE: http://pcworld.uol.com.br/especiais/secworld/archive/2008/02/11/brasil-j--o-quarto-no-envio-de-spam/

14/70

11 de Fevereiro de 2008

Brasil já é o quarto no envio de spam

País sobe mais uma posição no ranking do lixo eletrônico e fica atrás apenas de EUA, Rússia e China

Segundo o último levantamento da empresa de segurança Sophos (que acaba de ser divulgado), o país subiu mais uma posição no ranking do spam e já ocupa o quarto lugar, com 4% de todo o volume enviado no último trimestre de 2007.

À frente do Brasil, apenas Estados Unidos, Rússia (que teve forte crescimento no período, saltando do quarto posto para o segundo) e China. Confira abaixo a lista dos 12 países que mais enviam mensagens indesejadas.

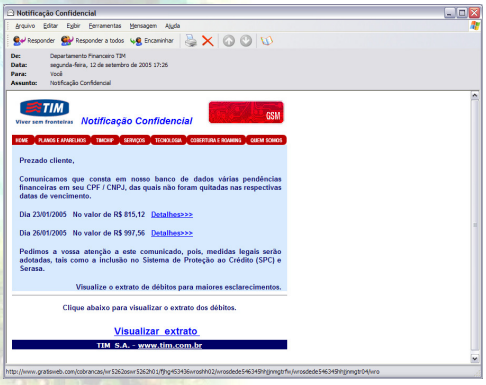
Posição	País/região	Porcentagem
1	Estados Unidos	21,3%
2	Rússia	8,3%
3	China	4,2%
4	Brasil	4%
5	Coréia do Sul	3,9%
6	Turquia	3,8%
7	Itália	3,5%
8	Polônia	3,4%
9	Alemanha	3,2%
10	Espanha	3, 1%
10	México	3,1%
12	Reino Unido	2,5%
Outros		35,7%

Por Daniel dos Santos às 12h07

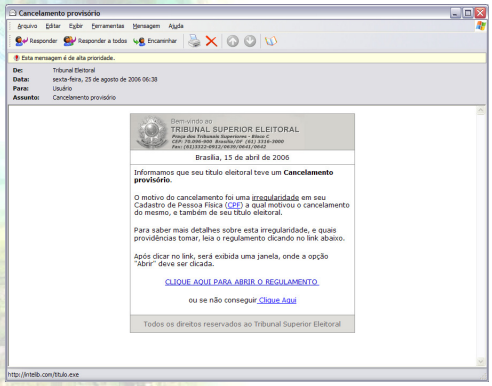
FONTE: http://pcworld.uol.com.br/especiais/secworld/archive/2008/02/11/brasil-j--o-quarto-no-envio-de-spam/

15/70

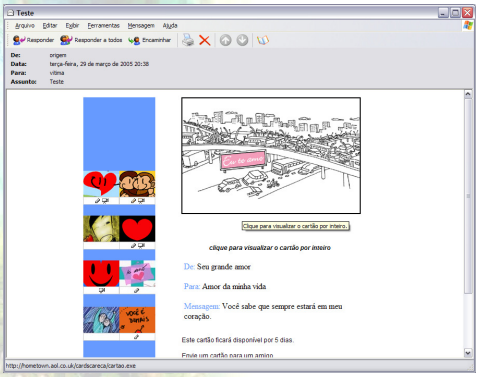
16/70



17/70

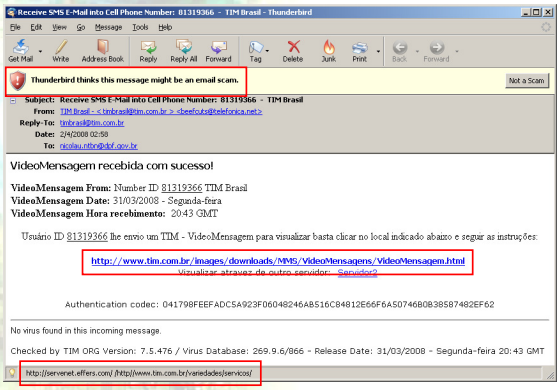


18/70

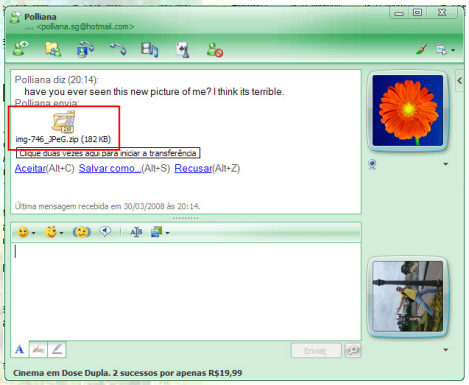


19/70

20/70



21/70



22/70

03 de Março de 2008

Novo vírus usa recados do Orkut

Praga virtual W32.Scrapkut envia mensagens para todos os contatos e promete vídeo sensual com Gyselle, do BBB8

A área de recados do Orkut pode ser uma fonte de dor de cabeça para seus usuários. Mais uma prova disso é a nova praga virtual W32.Scrapkut. Segundo pesquisadores da empresa de segurança Symantec, o processo de contaminação funciona da seguinte forma: o usuário do serviço entra em sua página de recados e encontra mensagens como "BBB8 Gyselle Muito Boa", com um vídeo de uma mulher nua (*imagem no final do texto*).

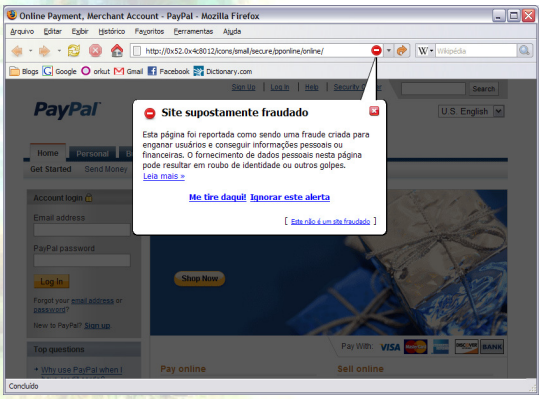
Ao clicar, a pessoa é redirecionada para um site que aciona o download do arquivo flashx_player_9.8.0.exe. Surge na tela a mensagem "Você não possui a ultima versão do Macromedia Flash Player instalado", com o botão "Instale agora". Quem acreditar na história e baixar o falso player, terá em seu computador vários arquivos nocivos.

Um deles faz com que, ao entrar no Orkut, o PC infectado passe a enviar os recados infectados para todos os contatos da conta atingida pelo W32.Scrapkut, ampliando o número de vítimas. Também podem ser executados softwares utilizados para roubar dados bancários. Se você encontrar um recado desse tipo em sua página, não clique.

FONTE: http://pcworld.uol.com.br/especiais/secworld/archive/2008/03/03/novo-vrus-usa-recados-do-orkut-/

23/70

24/70



25/70

PLANTÃO INFO / 04/2008 / TECNOLOGIA

Malware agora explora drives USB

Quarta-feira, 02 de abril de 2008 - 16h29

SÃO PAULO – Especialistas em segurança dizem que a nova onda de malware explora a popularidade dos pen drives.

Segundo a empresa de segurança ESET, fabricante do antivírus NOD32, 10,3% dos vírus e afins detectados em março continham informações sobre programas que devem rodar automaticamente quando um dispositivo removível é conectado ao PC.

Para a empresa, as contaminações via e-mail se tornaram tão comuns que as pessoas esquecem outras formas de invasão, ligadas diretamente ao desktop. No entanto, desde meados do ano passado, começaram a surgir ameaças concebidas para rodar em dispositivos como pen drives e HDs removíveis, conectáveis pela porta USB.

Carlos Machado, da INFO

FONTE: http://info.abril.com.br/aberto/infonews/042008/02042008-18.shl

26/70

28 de Janeiro de 2008

Tem vírus no porta-retrato

Equipamento digital da Insignia, que tem tela de 10,4 polegadas, inclui praga virtual destinada a PCs com Windows

Celulares, consoles de videogames, pendrives... As pragas virtuais não se limitam aos computadores e buscam novas plataformas. Afinal, vários equipamentos contam agora com recursos dignos de PCs.

A empresa Insignia publicou um alerta recentemente relacionado ao seu porta-retratos digital NS-DPF10A, que exibe fotos em uma tela de 10,4 polegadas. Ao conectar o dispositivo via porta USB, o computador pode ser infectado.

Segundo o fabricante, que pede desculpas pelo fato, unidades do equipamento foram comercializadas pela rede de lojas Best Buy nos Estados Unidos, antes da descoberta do vírus. Ao ser identificado o problema, a companhia afirma ter retirado o produto do mercado. A praga virtual é antiga e pode ser facilmente identificada com versões atualizadas de programas antivírus.

Depois dos porta-retratos digitais, qual será a próxima vítima dos vírus?

Por Daniel dos Santos às 16h35

FONTE: http://pcworld.uol.com.br/especiais/secworld/archive/2008/01/28/tem-vrus-no-porta-retrato/

27/70

01/04/2008 - 09h27

Nova Zelândia condena jovem de 18 anos por crimes na internet

da **France Presse**, em Welligton

Um jovem neozelandês foi condenado nesta terça-feira por liderar uma rede internacional de piratas virtuais que infectou pelo menos 1,3 milhão de computadores em todo o mundo, provocando um prejuízo de 20 milhões de dólares.

Owen Thor Walker, 18, declarou-se culpado de seis crimes em um tribunal de Thames, norte do país, e terá que se reapresentar à corte em 28 de maio.

FONTE: http://www1.folha.uol.com.br/folha/informatica/ult124u387750.shtml

28/70

Walker, que usa na internet o pseudônimo "Akill", começou a praticar os delitos pelos quais foi condenado quando ainda estava no colégio.

O jovem criou um vírus encriptado que não é detectado pelos programas de antivírus, segundo a polícia.

O vírus, que permitia o acesso aos nomes de usuário e às senhas dos internautas, assim como aos números de cartões de crédito, foi utilizado por outras pessoas que cometeram crimes.

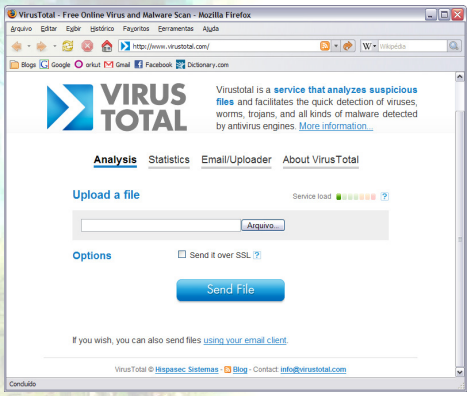
A polícia neozelandesa teve a cooperação do FBI (polícia federal norte-americana) e das autoridades holandesas para desmantelar a rede.

A investigação começou depois que um ataque contra 50.000 computadores bloqueou o servidor da Universidade da Pensilvânia, nos Estados Unidos, em 2006.

Walker morava com os pais quando cometeu os delitos, mas estes acreditavam que o filho se dedicava a criar programas de maneira legal, informou a polícia.

FONTE: http://www1.folha.uol.com.br/folha/informatica/ult124u387750.shtml

29/70



30/70

Complete scanning result of "Document_for_Case.doc", received in VirusTotal at 05.23.2007, 22:48:48 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AhnLab-V3	2007.5.24.0	05.23.2007	no virus found
AntiVir	7.4.0.27	05.23.2007	HEUR/Malware
Authentium	4.93.8	05.23.2007	no virus found
Avast	4.7.997.0	05.22.2007	no virus found
AVG	7.5.0.467	05.23.2007	no virus found
BitDefender	7.2	05.23.2007	BehavesLike:Win32.ExploreHijack
CAT-QuickHeal	9.00	05.23.2007	no virus found
ClamAV	devel-20070416	05.23.2007	no virus found
DrWeb	4.33	05.23.2007	DLOADER.Trojan
eSafe	7.0.15.0	05.21.2007	no virus found
eTrust-Vet	30.7.3655	05.23.2007	no virus found
Ewido	4.0	05.23.2007	no virus found
FileAdvisor	1	05.23.2007	no virus found
Fortinet	2.85.0.0	05.23.2007	no virus found
F-Prot	4.3.2.48	05.23.2007	no virus found
F-Secure	6.70.13030.0	05.23.2007	no virus found
Ikarus	T3.1.1.8	05.23.2007	no virus found
Kaspersky	4.0.2.24	05.23.2007	no virus found
McAfee	5037	05.23.2007	no virus found
Microsoft	1.2503	05.22.2007	no virus found
NOD32v2	2287	05.23.2007	no virus found
Norman	5.80.02	05.23.2007	no virus found
Panda	9.0.0.4	05.23.2007	Suspicious file
Prevx1	V2	05.23.2007	no virus found
Sophos	4.17.0	05.23.2007	Mal/Packer
Sunbelt	2.2.907.0	05.17.2007	no virus found
Symantec	10	05.23.2007	no virus found
TheHacker	6.1.6.121	05.23.2007	no virus found
VBA32	3.12.0	05.23.2007	no virus found
VirusBuster	4.3.23:9	05.23.2007	no virus found
Webwasher-Gateway	6.0.1	05.23.2007	Heuristic.Malware

Additional Information

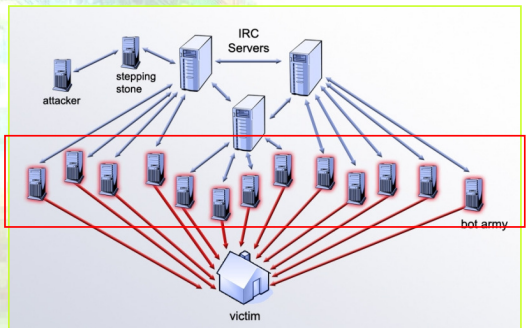
File size: 40498 bytes

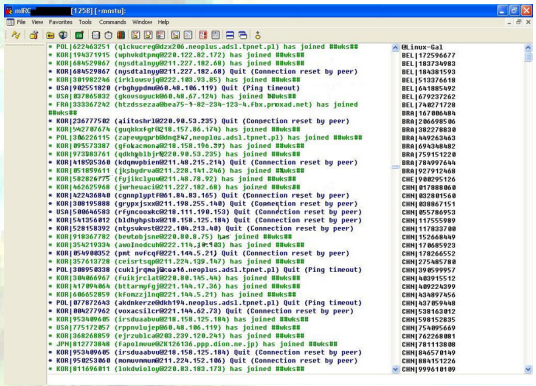
MD5: 5e297f759286207f46f82e6445917147

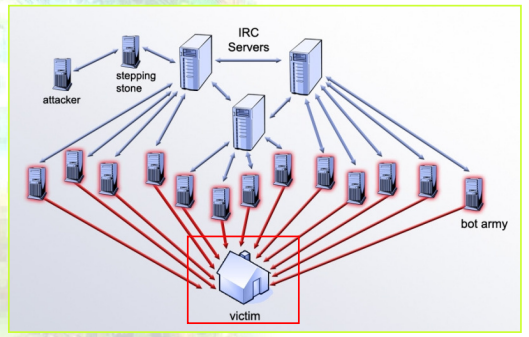
SHA1: 3b794a025cc5a8873fe0b9c7143c3eb8237cd8cc

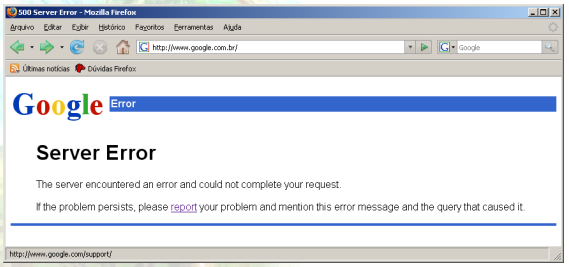
packers: FSG, BINARYRES

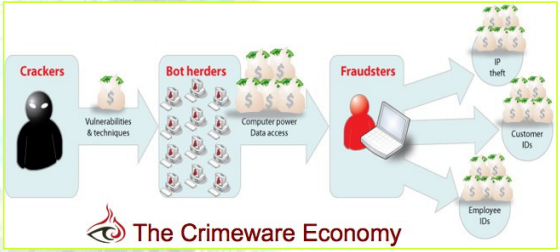
packers: FSG

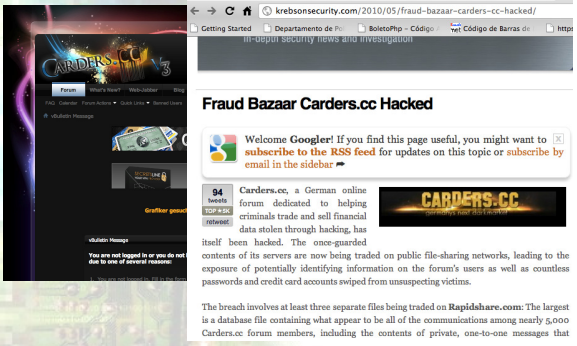












Ladrão que rouba ladrão;
Carders – Alemanha
Fraude bancária: banker

SEGURANÇA PÚBLICA

- ART. 144 da Constituição Federal de 1988

A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, por meio dos seguintes órgãos:

I – Polícia Federal;

I – Polícia Rodoviária Federal;

I – Polícia Ferroviária Federal;

I – Polícias Civis; e

I – Polícias Militares e Corpos de Bombeiros Militares.

POLÍCIA FEDERAL

Unidades centrais:

Gabinete;
Diretoria-Executiva;
Diretoria de Combate ao Crime Organizado;
Corregedoria-Geral de Polícia Federal;
Diretoria de Inteligência Policial;
Diretoria Técnico-Científica;
Diretoria de Gestão de Pessoal; e
Diretoria de Administração e Logística Policial;

Unidades Descentralizadas:

SRs, DPFs, Del. Especializadas e adidâncias policiais (ARG, COL, PRY);

CRH: Carreira policial (DPF, PCF, APF, EPF e PPF) e Adm;

POLÍCIA FEDERAL

- Missão: manter a lei e a ordem, cumprir a[s] [leis] contidas na CF e as infraconstitucionais);
- Visão: referência mundial em segurança pública...
- Atividades de combate sistemático:

ao crime organizado; aos crimes de colarinho branco; à lavagem de dinheiro;
ao trabalho escravo; ao contrabando e descaminho; ao terrorismo;
aos crimes cibernéticos;
à biopirataria; ao narcotráfico; e
aos crimes concernentes à atuação da Interpol, bem como casos de sequestro, cárcere privado e extorsão mediante sequestro.
Atividades de Proteção (MA, patrimônio, res. Indígenas e vítimas ameaçadas); e
Atividades de controle (imigração, passaporte, Prod.químicos, seg. privada e porte de arma);

POLÍCIA FEDERAL

- Atuação:

Procedimento investigativo (IPL):

Levantamento, investigação, oitiva, planejamento,

logística, operações, busca e apreensão;

Formação de provas:

Exames de locais, informática, laboratoriais, engenharia, contábeis, audiovisuais e eletrônicos;

Ministério Público;

Processo Judicial;

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO)

- Cargo provido mediante concurso público com exigência de formação específica em Computação, Informática ou SI

Atribuições Policiais

- Planejamento e coordenação das atividades policiais envolvendo sistemas de computadores
- Elaboração e aplicação de procedimentos técnico-científicos em computação criminal

Atuação Criminal

- Exames Periciais

≈ 150 Área 3 no Território Nacional

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO)

- Investigação Criminal: Atividade Técnico-Científica

  Reunir indícios e vestígios sobre a prática criminosa
  - Processamento de local de crime
  - Processamento de mídias e dispositivos de armazenamento

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO)

- Perícia Criminal: Atividades Técnico-Científicas

  Processar indícios e vestígios da prática criminosa
  - Assessoramento técnico-científico forense
  - Exames e procedimentos laboratoriais
  - Pesquisa e desenvolvimento de métodos e ferramentas

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO)

- Ferramentas

  Uso de soluções comerciais e desenvolvimento “in-house”
  - Equipamentos especiais:
    - Bloqueio de escrita, Hash, buscas;
  - Ferramentas forenses proprietárias
  - Ferramentas open-source e “free s

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO) tirar

- Equipamentos

Talon

Dossier

Solo

MPFS

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO)

- Software

  Espelhamento
  - Dd, dcfldd, dd_rhelp, FTK Imager;

  Recuperação de Dados
  - FTK (Registry Viewer, PRTK), Encase, Easy Recovery, GetdataBack;

  Tráfego de Dados
  - Wireshark, NetResident

  Dispositivos móveis
  - Paraben Device Sizure, XRY

  Engenharia Reversa:
  - IDA PRO, OllyDbg;

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO)

- Software

  Caseiros:
  - NuDetective: Ferramenta de detecção automática de nudez para uso em operações de combate à pedofilia
  - FTK Script: Ferramenta para geração automática de bookmarks utilizando SQL
  - ff3hr - Firefox 3 History Recovery: Ferramenta para recuperação de registros de histórico (SQLite) apagados do Firefox 3
  - GmailCacheParser: Ferramenta para recuperação de e-mails do Google Mail (Gmail) a partir do cache do Internet Explorer

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO)

- Software
  Caseiros:
  - WMM: Uma ferramenta de recuperação de vestígios do Windows Live Messenger 8.X
  - EspiaMule: Ferramenta para monitoramento das redes utilizadas pelo eMule
  - jMsnSniffer: Ferramenta para extração de conversas MSN em arquivos pcap (interceptação telemática)
  - PcaptoWeb.exe extrai os streams dos pcaps e deles extrai emails (POP e SMTP), objetos web (htmls, imagens, etc.), MSN (chat, trasnf de arquivos, conversas com e conversas voz), VOIP

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO)

- CASOS
  PEDOFILIA;
  REDES PONTO A PONTO;
  FALSIFICAÇÃO DE DOCUMENTOS;
  FALSIFICAÇÃO DE MOEDAS (REAL E DÓLAR);
  FALSIFICAÇÃO DE MÍDIAS;
  PRODUÇÃO DE DOCUMENTOS PÚBLICOS;
  CELULAR;
  MENSAGENS DE E-MAIL (RACISMO, TERRORISMO)

Funcionamento

PERITO CRIMINAL FEDERAL - ÁREA 3 (COMPUTAÇÃO)

- Comércio Eletrônico
- 5- Confirmação vem para o navegador do usuário
- 6- Do navegador ela vai para site da loja
  - <form name="Input" method="POST" action="http://sitedaloja.com/receb.asp">
  - <input type="hidden" name="NOMECOMPRADOR" value="Teste Santos">
  - <input type="hidden" name="CODRETORNO" value="">
  - <input type="hidden" name="VENDAID" value="56658572">
  - <input type="hidden" name="VALOR" value="100">
  - <input type="hidden" name="CODAUTORIZACAO" value="08E1BA28825">
  - <input type="hidden" name="CODPAGAMENTO" value="1">
  - .....
  - document.frmInput.submit();

DESAFIOS

- Avanço tecnológico x capacitação continua
  Crimes cada vez mais sofisticados;
  Produtividade x desenvolvimento técnico;
- Modernização x Burocracia
  Inquérito extremamente ritualístico, justiça lenta;
- Cooperação entre instituições
  Google, Skype, Microsoft, outras polícias etc.
- Cooperação com a iniciativa privada
  Provedores, instituições bancárias, etc

DESAFIOS

- Desafios tecnológicos
  Escassez de fornecedores;
  Necessidade de ferramentas forenses:
  Ferramentas para classificação de imagens;
  Criptografia e esteganografia;
- Cooperação entre instituições
  Convênios com instituições de ensino;

FINALIZANDO

- Cada vez mais os criminosos utilizam práticas mais modernas;
- Trabalho árduo, minucioso;
- Nã

Prática

- Exemplo FTK:
  - Análise de caso (imagens, arquivos apagados, criptografados, busca por palavras-chaves, etc);
  - Recuperação de imagens;
  - Recuperação de bate-papos;
  - Recuperação de e-mails (google/gmail);
  - Malware (banker);

POLÍCIA FEDERAL

- Combate a Crimes Relacionados a Computadores:
  - Unidade Repressão a Crimes Cibernéticos (URCC)
    - http://www.dpf.gov.br
    - http://denuncia.dpf.gov.br
    - crime.internet@dpf.gov.br
    - urcc.cgpfaz@dpf.gov.br
  - Diretoria Técnico-Científica (DITEC
    - Fantástico, 07/01/2007 [02:02]

DEPARTAMENTO DE POLÍCIA FEDERAL
SUP. DO ESTADO DE SANTA CATARINA
SETOR TÉCNICO-CIENTÍFICO

Obrigado!

PCF LUCIANO PETINATI FERREIRA
petinati.lpf@dpf.gov.br

DEPARTAMENTO DE POLÍCIA FEDERAL
SUP. DO ESTADO DE SANTA CATARINA
SETOR TÉCNICO-CIENTÍFICO

Obrigado!

PCF LUCIANO PETINATI FERREIRA
petinati.lpf@dpf.gov.br