CENTRO PAULA SOUZA
COMPETÊNCIA EM EDUCAÇÃO PÚBLICA PROFISSIONAL

CENTRO TECNOLÓGICO DA ZONA LESTE
FACULDADE DE TECNOLOGIA DA ZONA LESTE

DANIEL PEDROSA AGUIAR

ESTUDO SOBRE CRIMES PRATICADOS NA INTERNET COM O USO DO COMPUTADOR

São Paulo

2009

CENTRO TECNOLÓGICO DA ZONA LESTE
FACULDADE DE TECNOLOGIA DA ZONA LESTE

DANIEL PEDROSA AGUIAR

ESTUDO SOBRE CRIMES PRATICADOS NA INTERNET COM O USO DO COMPUTADOR

Monografia apresentada no curso de Tecnologia em Informática com ênfase em gestão de negócio na FATEC ZL como requisito parcial para obter o Título de Tecnólogo em Informática com ênfase para a gestão de negócio.

Orientador: Prof. MS. Joilson de Souza Cardoso

São Paulo

2009

CENTRO PAULA SOUZA
COMPETÊNCIA EM EDUCAÇÃO PÚBLICA PROFISSIONAL
CENTRO TECNOLÓGICO DA ZONA LESTE
FACULDADE DE TECNOLOGIA DA ZONA LESTE

DANIEL PEDROSA AGUIAR

ESTUDO SOBRE CRIMES PRATICADOS NA INTERNET COM O USO DO COMPUTADOR

Monografia apresentada no curso de Tecnologia em Informática com ênfase em gestão de negócio na FATEC ZL como requisito parcial para obter o Título de Tecnólogo em Informática com ênfase para a Gestão de Negócios.

COMISSÃO EXAMINADORA

_____
Prof. Me. Joilson de Souza Cardoso
Faculdade de Tecnologia da Zona Leste

_____
Prof. Me. Manoel Teixeira
Faculdade de Tecnologia da Zona Leste

_____
Prof. Me. Edson Roberto Barbosa Ceroni
Faculdade de Tecnologia de São Paulo

São Paulo, 10 de dezembro de 2009.

A Deus, minha filha e pessoas que já não se encontram aqui...

Mas que contribuíram muito para o que eu sou hoje...

AGRADECIMENTOS

As pessoas que convivem e trabalham comigo no dia-a-dia, que de uma forma ou de outra me auxiliaram na elaboração deste trabalho.

Especial agradecimento ao meu orientador e mestre Joilson que, com sua experiência me guiou na elaboração deste Trabalho.

Agradeço também a minha família, em especial minha pequena filha, que é a fonte de todas as minhas motivações para que sempre possa estar buscando novos desafios.

"O êxito da vida não se mede pelo caminho que você conquistou,
mas sim pelas dificuldades que superou no caminho."

Abraham Lincoln

AGUIAR, Daniel Pedrosa. **Estudo sobre os crimes praticados na Internet com o uso do Computador**. 2009. 68f. Monografia (Graduação em Tecnologia em Informática com Ênfase para a Gestão de Negócios) – Faculdade de tecnologia da Zona Leste.

RESUMO

Os crimes cometidos na internet com o uso do computador vêm sendo gradativamente mais constantes e habituais. A mídia em geral vem dando grande importância a estes fatos que surgem juntamente com o desenvolvimento social e com a inclusão digital. Embora não seja uma modalidade nova de delito, os crimes de informática estão sendo praticados por pessoas jovens e, que com certa habilidade e conhecimento, acham que nunca serão descobertas na grande rede por causa de sua magnitude e complexidade.

Palavras Chave: Crimes de Informática, Crimes Cibernéticos, Hackers, Segurança Digital, Computação Forense.

AGUIAR, Daniel Pedrosa. **Research about cyber crimes**. 2009. 68f. Monography (Graduation in Computing Technology: Business Management Concentration) – Faculdade de Tecnologia da Zona Leste.

ABSTRACT

The use of computers for cyber crimes are becoming an usual practice. The news industry is giving a lot of importance to this fact, and it´s continnuos growth with the development of the society and the digital inclusion. Authought this isn´t a new type of crime, ultimately it´s has been practiced by teens, with high knowledge and the certainty of never been caught, covered by the anonymity and complexity provided by the internet.

Key words: Computer crimes, Cyber crimes, Hackers, Digital Security, Forensic Computing

LISTA DE FIGURAS

Figura 1 - Posicionamento e operação de uma caixa NAT..... 28

Figura 2 - Serviço Proxy..... 29

Figura 3 - Tela do Programa Proxy Ultrasurf 8.8..... 30

Figura 4 - Conceito de Firewall..... 31

Figura 5 - Cartão de Segurança do Bradesco..... 37

Figura 6 - Itoken do Banco Bradesco..... 38

Figura 7 - Itoken do Banco Itaú..... 38

Figura 8 - Situação de Spoofing..... 45

Figura 9 - Modelo de ataque DDos..... 46

Figura 10 - Administrador de Roteador D-Link..... 52

LISTA DE GRÁFICOS

Grafico 1 - Domicílios com Acesso a Internet em %..... 47

Grafico 2 - Incidentes de Segurança Reportados ao CERT.BR de 1999 a 2009 48

Grafico 3 - Incidentes Reportados ao CERT.br -- Julho a Setembro de 2009..... 49

Grafico 4 - Incidentes Reportados ao CERT.br – Por dias da Semana..... 49

Grafico 5 - Origem dos Incidentes Reportados ao CERT.BR..... 50

Grafico 6 - Países que mais usam o Orkut..... 56

Grafico 7 - Ranking de Usuários por Países..... 57

SUMÁRIO

1. INTRODUÇÃO.....14

2. CRIMES PRATICADOS COM O USO DO COMPUTADOR.....16

2.1 Conceito de Crime. 16

2.1.1 Crime Comum.....16

2.1.2 Crimes de Informática.....17

2.2 Legislações pertinentes sobre o assunto.....18

2.2.1 Constituição Brasileira 20

2.2.2 Código Penal 21

2.2.3 Código de Processo Penal 21

2.2.4 Lei das Telecomunicações 22

2.3 Conceito de Redes e Telecomunicações.....23

2.3.1 Local Área Network - LAN 23

2.3.2 Intranet, Internet e Extranet 24

2.3.3 Protocolo TCP IP 26

2.3.4 Serviços de NAT 27

2.3.5 Conexões com Proxy.....28

2.3.6 Firewall 30

3. ANÁLISE CRIMINAL.....32

3.1 Tipos mais comuns de crimes cometidos pela Internet 33

3.1.1 Pornografia Infantil.....34

3.1.2 Calúnia e Difamação.....34

3.1.3 Ameaça.....35

3.1.4 Discriminação 35

3.1.5 Espionagem Industrial 35

3.1.6 Furto de valores através de transações bancárias 36
3.1.7 Invasões a Servidores 39
3.2 Ferramentas e meios utilizados pelos criminosos 40
3.2.1 Phishing Scan 41
3.2.2 Cavalo de Tróia (Trojans Horse) 41
3.2.3 Mail Bomb 42
3.2.4 Sniffers 42
3.2.5 Scanner Ports 43
3.2.6 Ping of Death 43
3.2.7 Quebra de Senha 44
3.2.8 Spoofing de Servidor DNS 44
3.2.9 Denial of Service (Dos) e Distributed Denial of Service (DDos) 45
3.3 Migração dos Delitos nos Meios Convencionais para o Meio Virtual 47
3.4 Apuração dos crimes cometidos através do uso do computador 51
3.4.1 Análise de Roteadores 52
3.4.2 Análise de Logs 53
3.4.3 Rastreabilidade das Conexões 53
3.4.4 Perícia Forense e Provas Técnicas 55
4. ESTUDO DE CASOS: ORKUT, AMEAÇAS E FRAUDES BANCÁRIAS 56
4.1 Caso 1 – Uso do Orkut no Brasil 56
4.1.1 A Situação 57
4.1.2 Solução 58
4.2 Caso 2 – Ameaça via e-mail 59
4.2.1 A Situação 59
4.2.2 Solução 59

4.3 Caso 3 – Quadrilha de Fraudes Bancárias 61
4.3.1 A Situação 61
4.3.2 Solução 61
5. MÉTODOS DE PREVENÇÃO 63
6. CONSIDERAÇÕES FINAIS 65
REFERÊNCIAS 67
ANEXO A – PROJETO DE LEI 94/99 70
ANEXO B – MANUAL DO MINISTÉRIO PÚBLICO FEDERAL 79

1. INTRODUÇÃO

Toda sociedade carece de regras. As regras são de extrema importância para o convívio harmonioso entre seus integrantes e é a partir do exemplo delas que os demais indivíduos se guiam para o seu cumprimento temendo suas punições.

Quando algumas regras são quebradas, ignoradas ou esquecidas é sinal que alguma coisa não está de acordo; alguma condição não foi bem especificada ou definida perante um conjunto total de pessoas.

Isto é visto exatamente quando se refere aos crimes cometidos pela Internet. Estes crimes, normalmente oriundos dos demais crimes anteriormente praticados na vida comum, estão sendo paulatinamente praticados com o auxílio de uma nova ferramenta, o computador.

Quem o pratica tem a falsa sensação de que nada irá lhe ocorrer, pelo fato da Internet ser uma rede pública e com milhões de adeptos pelo mundo. Tal sensação se sublima ainda com a falta de controle sobre o que é certo ou errado na rede e termina com a morosidade do poder público em combater ou conseguir resultados breves no andamento dos casos deste tipo de delito.

O objetivo deste trabalho é demonstrar a crescente utilização da pratica delituosa através da Rede Mundial de Computadores (Internet) e a forma pela qual o Estado se utiliza para combater tais delitos e suas conseqüências na vida das pessoas.

A metodologia utilizada para este trabalho conta com revisão de referências bibliográficas e apresentação de alguns estudos de casos, os quais ilustram de forma prática a aplicação desta nova modalidade delituosa.

A tendência que move a migração dos crimes convencionais para os meios virtuais são muito fortes, pois se observa que em pouco tempo, no Brasil, o uso do computador será tão comum como o de qualquer outro eletrodoméstico.

Em contra partida fala-se pouco das ferramentas usadas no combate aos crimes cometidos pela internet, que precisam ser adequadamente aprimoradas para dinamizar os processos de investigações nesta área, o que significará em desencorajar quem está disposto a entrar nesta nova modalidade de crime.

A motivação para o desenvolvimento desta Monografia está no fato do trabalho realizado pela Polícia Judiciária, que é a responsável por esclarecer os crimes, e o envolvimento deste processo com a Tecnologia da Informação ser fator de poder aglutinar ambos os segmentos criando base sólida para desenvolvimentos futuros em nível de mestrado na área de Segurança Digital e Cyber Crimes.

2. CRIMES PRATICADOS COM O USO DO COMPUTADOR

Para definir os crimes praticados através do uso da informática, devem-se analisar os mesmos crimes cometidos pelos meios convencionais, suas definições e tipificações de acordo com as Leis vigentes.

Há também a necessidade de se abordar a carência de uma legislação específica, que tipifique diretamente a conduta utilizada pelo infrator, pois nem sempre há como se enquadrar um determinado delito na legislação atual, a qual será exposta ao final deste capítulo.

2.1 Conceito de Crime.

Para caracterizar as ocorrências de crimes envolvendo o uso do computador torna-se necessário a definição do conceito de crime.

2.1.1 Crime Comum.

Crime é uma palavra derivada do latim *"crimen"*, que significa acusação.

Para a existência do crime é necessária uma conduta humana positiva (ação) ou negativa (omissão), que seja típica e descrita na lei como infração penal e somente haverá crime se o fato for antijurídico, contrário ao direito por não estar protegido por causa que exclua sua antijuridicidade.

A Lei de Introdução ao Código Penal, Decreto-Lei Nº 3.914, de 09 de dezembro de 1941, em seu artigo 1º esclarece:

> Art. 1º - Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.

De acordo com Jesus (2000, p.125), o crime tem como requisitos:

- Fato típico, ou seja, aquele que está contido em uma norma penal incriminadora;
- Antijurídico (Antijuricidade), é a ação contrária a todo o anseio da sociedade, aquele que foge as regras impostas por um determinado grupo de pessoas;
- Culpável (Culpabilidade), é a ação praticada pelo agente, seja ela com dolo (vontade) ou não em querer o resultado obtido.

2.1.2 Crimes de Informática

Podemos definir o crime de informática como qualquer ato ilegal onde o conhecimento especial de tecnologia de informática faz com que o sujeito da ação infratora tenha êxito na sua conduta.

Segundo Paiva (2006, p.5):

> Apesar da discrepância doutrinária, são denominadas de "crimes de informática" as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenamento ou processamento).

Em determinadas vezes o crime de informática se assemelha muito ao crime comum, tendo somente a diferença que o objeto utilizado para o êxito foi um computador ou sistema informatizado.

Tendo exatamente estas características é que alguns autores classificam os crimes de informática em três subgrupos:

- Crimes de Informática Puros: É o crime de informática que se utilizando de um computador, visa pura e somente o ataque a qualquer outro computador ou sistema de Informática.

Costa (1997, p.29) define Crimes de Informática Puros:

> São aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Tal conduta, infelizmente, é a mais impune, pois não permite sua tipificação, na maioria das vezes, em nenhuma Lei específica que puna tais delitos.

- Crimes de Informática Mistos: os crimes de informática mistos não visam o sistema de informática em si, mas se utilizam dos mesmos como ferramenta ou modo para tal delito.

  Neste aspecto Costa (1997, p.29) afirma: “São todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação.”

- Crimes de Informática Comum: São atos em que o agente utiliza o sistema de informática como mera ferramenta para a prática do crime comum; porém o mesmo poderia ser praticado por qualquer outro meio. Costa (1997, p.30) termina sua explicação resumindo:

  > São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta. Um exemplo que ilustra perfeitamente este tipo de crime é o Estelionato. (Artigo 171 do Código Penal)

2.2 Legislações pertinentes sobre o assunto

Como a idéia de crimes na internet é nova, não existem leis específicas para esse ato. O que se tem hoje, que pode condenar, são alguns artigos do código civil, como os Art. 927, 186, 187. Esses códigos falam em possíveis atos criminosos, ou àquele que viola por omissão voluntária cometer um ato ilícito.

Afirma BACELAR (apud CARVALHO, 2001, p. 59) "internet não cria um espaço livre, alheio ao direito. A legislação vigente se aplica, aonde e quando for cabível as relações jurídicas decorrentes de fatos jurídicos ocorridos na internet e pela internet".

Hoje não existem leis específicas para os crimes na internet, o que existe são leis que punem em relação da conseqüência. Por isso, já estão em fase de elaboração e votação, projetos de lei que buscam punir casos de crimes na internet, com objetivos de diminuir o número desses crimes.

As legislações atuais sobre crimes cometidos pelo computador não contemplam nenhuma tipificação própria, ou seja, os mesmos crimes atualmente são tipificados em outros crimes a qual apenas o resultado alcançado possa ser caracterizado, fazendo com que o meio pelo qual o agente se utilizou seja praticamente ignorado.

Em alguns casos, tais utilizações acabam gerando falhas nas tipificações de alguns crimes cometidos através do computador.

Segundo Pinheiro (2008), “ao usarmos a tipificação de crime de furto no ambiente digital, estamos invalidando o crime, pois no caso em que o agente criminoso apenas invade um servidor e copia determinados dados, não poderá ser classificado como furto, pois a tipificação do mesmo significa subtrair coisa alheia”. Note que neste caso o fato de copiar o dado não o subtraiu, o que faz com que este tipo de delito passe a ser desqualificado.

Paulo José Tupinambá apresentou um projeto de lei no senado e afirma:

> Acredito que a partir da aprovação da lei, a tendência é de que o número de crimes de informática diminua, já que a punição aos crimes será muito mais contundente que a atual. A lei deverá prever situações como a reincidência no crime eletrônico, que atualmente não existe. (Apresentação de Projetos de Lei no Senado, 2004).

O Projeto de Lei n.º 84/99 na câmara dos Deputados ou o PL 89/03 do Senado e o Projeto de Lei n.º 1713/96 são os dois projetos mais importantes que estão em tramite no Congresso Nacional e tem como objetivo a regulamentação dos crimes digitais.

O Projeto de Lei n.º 84/99, vide anexo a este trabalho na íntegra, dispõe sobre crimes cometidos na área da informática e suas penalidades. Esse projeto prevê sete modalidades de delitos com relação à informática, que são chamados de crimes digitais, podendo chegar até 6 anos de reclusão e multa. O principal objetivo do projeto é o preenchimento das lacunas na legislação brasileira, isto é, retratar atos que não existem na legislação penal em vigor.

O capítulo I do Projeto de Lei nº 84/99 preceitua os princípios que

regulam a prestação de serviço por redes de computadores. Os serviços de rede devem fornecer segurança, garantia de acesso as informações e devem respeitar os direitos individuais e coletivos.

O capítulo II regulamenta o uso de informações disponíveis em computadores ou redes de computadores. A informática é alvo de muitas atividades, desde sociais até criminais.

De acordo com Paiva (2008, p. 7):

> O Projeto citado não apenas cria tipos penais novos, mas estende o campo de incidência de algumas figuras já previstas no CP para novos fenômenos ocorrentes nos meios desmaterializados, impossíveis de terem sido previstos pelo legislador de 1940, ano de edição do atual Código Penal, como pretende inserir ainda a Seção V no Capítulo VI do Título I do Código Penal, onde seriam definidos os crimes contra a inviolabilidade dos sistemas informatizados.

É muito importante que se realize um trabalho de base nas faculdades de direito, para que se amplie gradativamente a capacidade técnica sobre este assunto no poder judiciário, assunto este que cedo ou tarde estará nos tribunais. Por isso é importante que haja um destaque na realização de eventos que proporcionam debates sobre o Direito e a Internet.

Para que não haja crimes é preciso investir na prevenção. Deve haver discussões tanto no âmbito estatal quanto no privado, para encontrar maneiras de aumentar a confiança nas novas tecnologias. Como é algo recente, a Grande Rede se torna um desafio, para o Direito, que visa pacificar e acabar com conflitos sociais.

2.2.1 Constituição Brasileira

A Constituição Brasileira por ser muito recente (foi promulgada em 1988) acaba por ser bem focada nos fatos atuais e é a Lei maior que garante todas as garantias individuais dos cidadãos brasileiros. Nela em seu artigo 5.º estão contidas todas as garantias de individualidade, direitos e proteções que todos nós temos amparado:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Há de se destacar no inciso XII da Constituição, que as comunicações telegráficas e de dados são protegidas, exceto quando houver investigação criminal ou instrução processual. Para tal fato ocorrer, haverá sempre e sem nenhuma exceção, a necessidade de uma ordem judicial para a quebra do referido sigilo telefônico ou de dados.

2.2.2 Código Penal

Como no momento não há uma Legislação específica que puna os delitos praticados através do uso do computador, mas apenas os resultados causados por eles, o uso do código penal tem sido o mais comum para o enquadramento destas ações delituosas.

Apesar de muitos acharem este tipo de ação muito genérica, pois por muitas vezes o enquadramento de determinada conduta num artigo (Art. 155 - Furto, por exemplo) fará com que o criminoso se compare a um furtador de rua comum; ignora-se o conhecimento e potencial valor de perigo do criminoso, que poderá nem permanecer preso ou o ficará por breve tempo e voltará cometer tais delitos, de uma forma mais grave e causando maiores danos a sociedade.

2.2.3 Código de Processo Penal

Para tratar e investigar qualquer tipo de crime é necessário o conhecimento prévio sobre a Lei de Código de Processo Penal. Nela estão contidas todas as normas necessárias para que o Estado possa buscar os autores de delitos e regras para que o mesmo não haja com arbitrariedade, garantindo assim, os

direitos previstos na Constituição. Um dos pontos mais importante contidos no Código de Processo Penal e que envolverá diretamente o processo de apuração dos crimes de informática é a Busca e Apreensão:

> Art. 240. A busca será domiciliar ou pessoal.
> § 1.º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para:
> a) prender criminosos;
> b) apreender coisas achadas ou obtidas por meios criminosos;
> c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos;
> d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso;
> e) descobrir objetos necessários à prova de infração ou à defesa do réu;
> f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;
> g) apreender pessoas vítimas de crimes;
> h) colher qualquer elemento de convicção

2.2.4 Lei das Telecomunicações

A Lei das Telecomunicações, criada em Julho de 2007, tem como objetivo regulamentar os órgãos prestadores de serviços nas diversas área e modalidade que envolva as Telecomunicações.

Em seu Capítulo I artigo 60, definições, a Lei deixa bem claro o que são os serviços de Comunicações:

> Art. 60. Serviço de telecomunicações é o conjunto de atividades que possibilita a oferta de telecomunicação.
> § 1° Telecomunicação é a transmissão, emissão ou re cepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza.
> § 2° Estação de telecomunicações é o conjunto de eq uipamentos ou aparelhos, dispositivos e demais meios necessários à realização de telecomunicação, seus acessórios e periféricos, e, quando for o caso, as instalações que os abrigam e complementam, inclusive terminais portáteis.
> Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações.
> § 1º Serviço de valor adicionado não constitui serviço de telecomunicações, classificando-se seu provedor como usuário do serviço de telecomunicações que lhe dá suporte, com os direitos e deveres inerentes a essa condição.

> § 2° É assegurado aos interessados o uso das redes de serviços de telecomunicações para prestação de serviços de valor adicionado, cabendo à Agência, para assegurar esse direito, regular os condicionamentos, assim como o relacionamento entre aqueles e as prestadoras de serviço de telecomunicações.

Portanto, os serviços oferecidos pelos provedores de acesso a Internet se enquadram no artigo 61 do dispositivo desta Lei.

2.3 Conceito de Redes e Telecomunicações

As redes de computadores estão se tornando muito comuns. Qualquer instalação comercial com mais de um computador geralmente os têm em rede; transportar discos ou pen-drives de uma estação à outra é bem pouco produtivo. Sendo assim, não basta possuir uma sala cheia de computadores.

É necessário interligá-los de modo a permitir a troca de dados. Se tivesse de dividir uma rede em seus componentes mais simples, se teria duas partes. Uma seria a rede física - os fios, as placas de rede, os computadores, e outros equipamentos utilizados pela rede para fazer a transmissão dos dados. A outra seria a organização lógica dessas partes físicas - as regras que permitem que as partes físicas trabalhem em conjunto.

2.3.1 Local Área Network - LAN

As redes locais ou Local Área Network (LAN) como são conhecidas são redes criadas entre computadores para facilitar e automatizar as tarefas atinentes entre eles. Sua utilização é bastante ampla, pois onde há mais de um computador surge a necessidade de se compartilhar recursos (arquivos, impressoras, internet e etc.) entre eles.

As LAN´s, dependendo de seu tamanho, podem ser de dois tipos: ponto a ponto para redes pequenas ou cliente/servidor para redes de maiores dimensões.

Tanenmbaum (2002 p.29) define Redes Locais:

> As redes locais, muitas vezes chamadas LANs, são redes privadas contidas em um único edifício ou campus universitário com até alguns quilômetros de extensão. Elas são amplamente usadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais de empresas, permitindo o compartilhamento de recursos (por exemplo, impressoras) e a troca de informações.

2.3.2 Intranet, Internet e Extranet

INTRANET: Ao se usar uma LAN, ou seja, uma rede privada empregando os padrões da internet pode-se criar uma Internet interna. A esta Internet interna dá-se o nome de Intranet.

As Intranets, muito usadas em ambientes corporativos, têm como finalidade padronizar os processos nas organizações e torná-las mais competitivas e abertas às novas tecnologias.

Sawaya (1999, p. 245) define Intranet como:

> Uma rede local projetada para atender às necessidades internas de uma única organização que pode ou não estar conectada à Internet, mas que não é acessível a partir do ambiente externo. Utiliza o mesmo protocolo e os mesmos sistemas e programas usados na Internet para acesso remoto, cópia de arquivos, correio eletrônico e acesso a hipertexto e multimídia. Algumas organizações instalam servidores da WWW dentro de suas próprias redes internas, de modo que seus empregados tenham acesso aos documentos da Web. É como se fosse uma Internet privada.

INTERNET: A internet é uma rede de redes. Embora ninguém saiba realmente quem foi o primeiro a dizer isso, provavelmente é o termo mais genérico para explicá-la.

Segundo Tanenmbaum (2002 p.54):

> A Internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns. É um sistema pouco usual no sentido de não ter sido planejado nem ser controlado por ninguém.

A internet é uma série de redes privadas de computadores (LANS, MANS e WANS) interligadas umas as outras. Cada rede privada é formada por uma série de computadores interligados dentro de uma Organização.

Seguindo a mesma linha de raciocínio, Inellas (2009, p.6) esclarece:

> Portanto, resta evidente que a Internet não é uma entidade autônoma; é simplesmente uma Rede de computadores, integrada por diversas outras Redes menores, unidas pela capacidade de comunicação, uma com as outras.

Cada Organização tem responsabilidade apenas pelos computadores que se encontram dentro de sua esfera de influência. Normalmente as redes individuais são interligadas através de dispositivos especiais, chamados roteadores, que são responsáveis pela definição de quais dados devem permanecer dentro da rede local e quais dados devem ser passados para as outras redes.

EXTRANET: Ocorre quando é usada a Intranet na empresa, porém de forma externa, ou seja, utilizando a Internet como acesso a mesma. Ao se conectar a Intranet à Internet e oferecer recursos para que clientes e parceiros comerciais usem parte de sua intranet para fazerem negócios.

As extranets são basicamente intranets que usam a internet como veículo para interagirem com seus clientes, fornecedores e parceiros comerciais.

Com as devidas precauções de segurança, as extranets têm enorme valor; elas reduzem os custos de conexão do seu sistema de computadores aos sistemas dos diversos parceiros comerciais e, possivelmente, expõe seus produtos a um público enorme.

Sawaya (1999, p.172) define extranet como:

> Uma extensão da Intranet, baseia-se na cessão de uma parte da Intranet corporativa para a conexão de clientes, representantes e/ou parceiros externos, que podem ter acesso externo à sua informação por meio de senha. É, na verdade, uma conexão da Intranet com a Internet.

2.3.3 Protocolo TCP IP

Ao utilizar o computador em qualquer uma das redes citadas anteriormente, é preciso uma linguagem para que eles conversem entre si.

A esta linguagem dá-se o nome de Protocolo; sem eles os computadores seriam praticamente zumbis num emaranhado de fios e redes ligados, porém não se comunicando.

O protocolo mais comum, tanto nas redes Intranets quanto na Internet é o TCP/IP. Segundo Torres (2001): “Por ser um protocolo de arquitetura aberta, onde qualquer fabricante pode adotar a sua própria versão não precisando repassar direitos autorais a ninguém”, o protocolo TCP/IP é hoje o mais popular e conhecido em todos os Sistemas Operacionais.

O protocolo TCP/IP se assemelha ao endereço de um logradouro, onde se conhece exatamente o que irá mandar (pacote de dados) e para onde se quer direcionar tais pacotes (endereçamento).

O mesmo pode ser definido também como um conjunto de protocolos de comunicação entre computadores em rede (também chamado de pilha de protocolos TCP/IP). Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Interconexão)

De acordo com Tanenbaum (2003 p. 48):

> Diante da preocupação do Departamento de Defesa dos EUA de que seus preciosos hosts, roteadores e gateways de interconexão de redes fossem destruídos de uma hora para outra, definiu-se também que a rede deveria ser capaz de sobreviver à perda do hardware de sub-redes, com as conversações existentes sendo mantidas em atividade. Em outras palavras, o Departamento de Defesa dos EUA queria que as conexões permanecessem intactas enquanto as máquinas de origem e de destino estivessem funcionando, mesmo que algumas máquinas ou linhas de transmissão intermediárias deixassem de operar repentinamente. Além disso, era necessária uma arquitetura flexível, capaz de se adaptar a aplicações com requisitos divergentes como, por exemplo, a transferência de arquivos e a transmissão de dados de voz em tempo real.

Portanto, a estrutura da rede TCP/IP é feita justamente para suportar diversas conexões, mas uma não dependerá exclusivamente da outra, ou seja, ela não é ligada em cascata ou série, mas sim com conexões independentes.

O Protocolo TCP/IP, ou mais expressivamente o Endereço IP é o que guiará boa parte deste trabalho, pois é através dele que a máquina delituosa será descoberta.

2.3.4 Serviços de NAT

Um ponto importante a ser levantado é se o endereçamento IP de determinada máquina é ou não um IP válido na Internet. Tal afirmação se dá pelo fato de alguns computadores, principalmente os de empresas, funcionarem em rede, e esta rede está operando somente com uma única conexão para a Internet, ou seja, somente com um único IP reconhecido na rede mundial de computadores.

Para os endereços IP´s definidos dentro de uma rede ou seja, válidos somente na mesma LAN, dá-se o nome de **NAT (Network Address Translation).**

O serviço de NAT é feito justamente para reduzir o número de IP´s válidos em uma única rede, pois a quantidade de IP´s disponíveis neste molde (IP Versão 4) na Internet é limitada. Acredita-se que com a implantação do novo sistema de IP (IP Versão 6) acabe este problema.

Para Sawaya (1999, p. 311) o conceito de NAT pode ser definido como: “Sistema incluído em vários roteadores e alguns sistemas operacionais. Vários hospedeiros “atrás” do roteador, ou hospedeiro firewall são traduzidos para um único endereço IP (Internet Protocol) real.”

Tanenbaum (2003. p. 343) ainda conclui:

> A idéia básica por trás da NAT é atribuir a cada empresa um único endereço IP (ou no máximo, um número pequeno deles) para tráfego da Internet. Dentro da empresa, todo computador obtém um endereço IP exclusivo, usado para roteamento do tráfego interno. Porém, quando um pacote sai da empresa e vai para o ISP, ocorre uma conversão de endereço. Para tornar esse esquema possível, três intervalos de endereços IP foram declarados como privativos. As empresas podem utilizá-los internamente como desejarem. A única regra é que nenhum pacote contendo esses endereços pode aparecer na própria Internet. Os três intervalos reservados são:
> 10.0.0.0 — 10.255.255.255/8 (16.777.216 hosts)
> 172.16.0.0 — 172.31.255.255/12 (1.048.576 hosts)

> 192.168.0.0 — 192.168.255.255/16 (65.536 hosts)
>
> O primeiro intervalo permite a utilização de 16.777.216 endereços (com exceção de 0 e -1, como sempre) e é a escolha habitual da maioria das empresas, mesmo que elas não necessitem de tantos endereços.

A figura abaixo mostra de forma mais detalhada a estrutura de um serviço NAT:

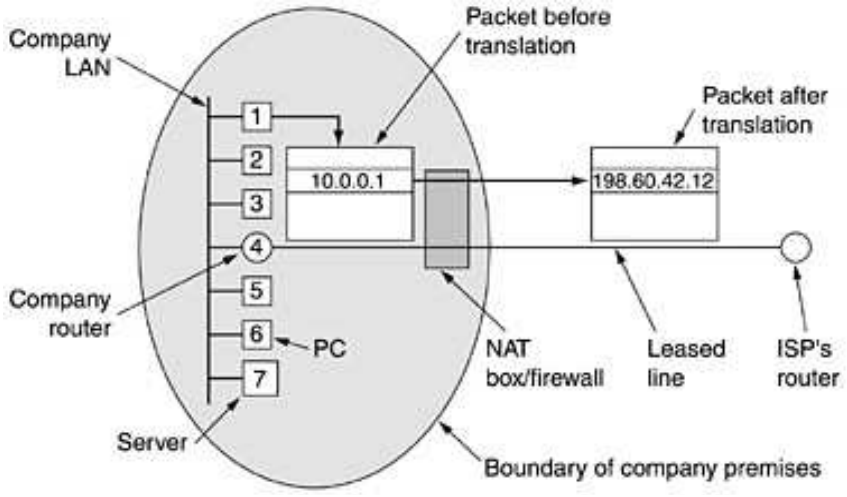


Figura 1: Posicionamento e operação de uma caixa NAT
Fonte: Adaptação de Tanenbaum (2003, p.344)

Haverá alguns casos em que o endereçamento IP colhido nas provas eletrônicas foi “NATeado”, portanto, terá que ser obter uma análise dos roteadores internos do local, para se chegar realmente a estação que partiu a ação.

2.3.5 Conexões com Proxy

Sawaya (1999, p.172) define Proxy como:

> Um programa de segurança utilizado para acessar a Internet que tem a função intermediária entre uma rede interna e a Internet, interceptando solicitações externas. Impede que usuários externos acessem diretamente recursos existentes na rede interna ou saibam onde estão localizados. Em geral, o Proxy integra um firewall (parede corta-fogo), colocado para garantir maior segurança de um sistema de uma rede interna.

Normalmente o uso de Servidores Proxy é feito objetivando um maior controle do que está sendo acessado pelos seus usuários, pois o mesmo tem entre diversas outras funções, a de controlar o acesso com log´s e sistema de login

nos próprios navegadores de internet.

Figuira 2: Serviço Proxy
Fonte: Site http://pplware.sapo.pt/

Ao se usar um Proxy localizado em outro país e que o endereçamento IP deste esteja visível na Internet e não em uma rede Interna, ou seja, aberto na grande rede, adota-se a estratégia de “Proxy de Túnel”, que acaba fazendo a função totalmente inversa dos servidores proxy´s usados nas empresas; ao invés de controlar o acesso, escondem o real endereço IP do computador que está efetuando o acesso.

Aragão (2009) em seu artigo detalha Proxy de Túnel como:

> Este tipo de proxy é usado para escapar ás políticas de controle de acesso feitas pelas empresas desbloqueando as páginas Web bloqueadas.
> Este proxy recebe os pedidos dos clientes, efectua-os e no fim transmite o resultado ao utilizador, fazendo que este esteja a navegar na internet apenas por uma página.
> Mas é necessário ter cuidado, pois podem haver proxies destas que escondem servidores com intenções ocultas, como recolher informações pessoais dos computadores. Por isso é desaconselhado fazer compras online por servidores proxies de túneis.

Há na Internet disponível para quem quiser ter acesso, algumas centenas de proxys e aplicativos para proxys de túneis internacionais. Um dos mais comuns e com bastante utilização é o UltraSurf, conforme mostra a figura abaixo:

Figura 3: Tela do Programa Proxy Ultrasurf 8.8
Fonte: Site baixaki.com.br

O uso destes aplicativos ou endereços proxys para o acesso a internet têm se tornado uma constante para as pessoas que não querem que seu endereço IP seja divulgado para o destinatário da comunicação ou em redes protegidas com limitações de acesso alguns sites.

Tal utilização revela no decorrer das investigações, um número IP incorreto ao que está sendo realmente utilizado pelo infrator, o que poderá causar grandes dificuldades a quem investiga tais delitos, ou até mesmo, ser arquivado por falta de provas.

2.3.6 Firewall

Para se entender o conceito de Firewall, primeiro é preciso definir o que é porta e qual sua finalidade.

Sawaya (1999, p.172) define Porta como:

> Canal lógico por onde a informação entra e sai de um computador conectado à Internet, ou hospedeiro (host). Normalmente, cada serviço ou protocolo da Internet funciona com uma determinada porta, que recebe um número; esse número, às vezes, consta de um endereço do tipo URL da WWW (World Wide Web), depois do sinal de dois pontos (:).

Seguindo este conceito de canais lógicos, é possível definir Porta como sendo o meio lógico de comunicação entre o computador a uma ou mais redes. Todos os computadores e sistemas operacionais possuem portas; elas nada mais são do que meios de entrada e saída de dados; dependendo de quem as acessam podem causar danos irreversíveis ou apenas receber o conteúdo de uma página da internet (por padrão sendo porta 80) ou enviar ou receber e-mails via servidores pop3 e smtp (portas 25 e 110).

A função do Firewall é justamente vigiar o conteúdo destas portas, fazendo com que apenas trafeguem nelas dados autorizados por ele. Seguindo esta linha de raciocínio, Torres (2001, p.415) conclui: “Como regra geral, praticamente tudo era proibido e, aos poucos, eram criadas regras permitindo a passagem do tráfego especial. “

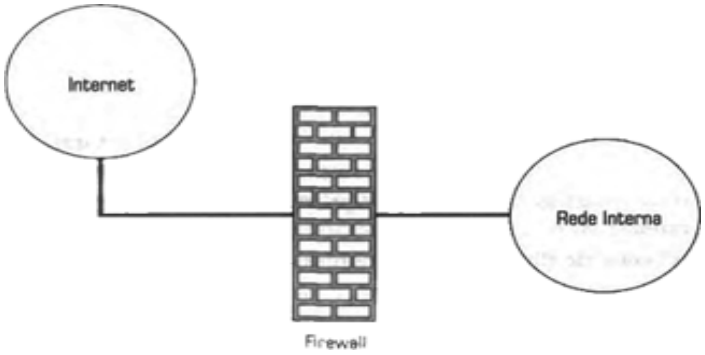


Figura 4: Conceito de Firewall
Fonte: Adaptação de Torres (2001, p.416)

3. ANÁLISE CRIMINAL

Este capítulo contempla as formas como os crimes de informática são praticados, investigados e analisados. As regras usadas para se investigar os crimes de informática são completamente diferentes das usadas para se combater um crime comum. Na prática delituosa comum, tem-se como materialidade o objeto ou prova do crime um instrumento concreto, sendo este submetido ao crivo pericial, conforme regula o Código de Processo Penal Brasileiro:

> Art. 158. Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.
> Art. 159. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.

Nos crimes de informática apesar de sempre haver o objeto do crime, o mesmo por padrão torna-se sempre abstrato, ou seja, a materialidade do ato criminoso estará sempre no meio eletrônico e seu trato deverá seguir regras específicas de manuseios, para se evitar perdas de provas preciosas.

O Delegado de Polícia em São Paulo, Mauro Marcelo de Lima e Silva, titular á época da entrevista na Delegacia de Crimes Eletrônicos do DEIC, na obra de Inellas (2009, p.14), esclarece que:

> A sociedade tem que ter em mente que o crime sempre, sempre está um passo a frente da polícia e o que define se essa polícia é eficiente, ou não, é à distância desse passo, o chama gap entre o crime e a polícia. Para diminuir este gap, a palavra de ordem é se preparar e antecipar, e no caso da investigação de crimes digitais, devemos maximizar a cooperação entre as polícias nacionais e internacionais, preparando e treinando policiais com novas técnicas de investigação, que devem agir rápido como a era digital exige.

Observa-se ainda que nas Academias de Polícia, tanto Civis, como a Federal em todo território Brasileiro, em seus cursos de formação para policiais, já é focado este tema em uma matéria própria na grade disciplinar para a formação de seus agentes.

3.1 Tipos mais comuns de crimes cometidos pela Internet

Existe sem dúvida, certa facilidade para a atuação de pessoas mal intencionadas na internet.

Como afirma Guimarães (2000, p.120):

> Em vez de pistolas automáticas e metralhadoras, os ladrões de banco podem agora usar uma rede de computadores e sofisticados programas para cometer crimes. E o pior, fazem isso impessoalmente, de qualquer continente, sem a necessidade de presença física, pois atuam num "território" sem fronteiras, sem leis, acreditando que , por isso, estão imunes ao poder de policia.

Ao analisar os crimes que são cometidos com maiores freqüências na Internet, é constatado que o principal é o Roubo de Identidade, ou Falsa Identidade segundo descreve o Código Penal Brasileiro em seu Artigo 307:

> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
> Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

O atual delegado da Delegacia de Crimes Eletrônicos do DEIC José Mariano Araújo, em artigo publicado por Demetrio (2009) esclarece:

> Atualmente, o que mais chega à delegacia são as denúncias enquadradas como “crime de honra e ameaça”. É o famoso “criaram um Orkut para mim” ou “divulgaram fotos em certas condições”, diz. Para as fraudes no sistema de Internet Banking e comércio eletrônico fica o segundo lugar das denúncias.
> A porcentagem de casos solucionados ainda não é um dado oficial, mas o delegado acredita que entre 70% e 75% dos casos tenham tido um resultado positivo.

Carpanez (2006) em seu artigo no jornal Folha de São Paulo ainda complementa:

> Apesar de o pódio estar muito bem definido, não há um consenso sobre a posição que outras transgressões ocupam no ranking da criminalidade virtual. Em uma proporção menor que o roubo de identidade, crimes como pedofilia e difamação cumprem bem seu papel na hora de incomodar internautas, empresas, governos e autoridades de todo o mundo.

Outros crimes praticados na grande rede também são bastante comuns e serão vistos a seguir.

3.1.1 Pornografia Infantil

A pornografia infantil se caracteriza quando internautas criam sites ou fornecem conteúdo (imagens e vídeos) relacionado ao abuso sexual infantil. Tais atitudes vêm sendo veementemente condenadas pela mídia e pela sociedade em geral, e erroneamente recebem a denominação de “pedofilia”.

Como explica Nogueira (2009, p.129):

> A palavra pedofilia vem do grego παιδοφιλια onde παις (significa "criança") e φιλια (“amizade”; “afinidade”; “amor”, “afeição”, “atração”; '"atração ou afinidade patológica por”). A pedofilia, por si só, não é um crime, mas sim, um estado psicológico, e um desvio sexual. A pessoa pedófila passa a cometer um crime quando, baseado em seus desejos sexuais, comete atos criminosos como abusar sexualmente de crianças ou divulgar ou produzir pornografia infantil.

Seguindo esta linha de raciocínio, pode-se definir que um pedófilo nem sempre pode ser considerado um criminoso, mas sim um ser que necessita de tratamento psiquiátrico, porém quem comete pornografia infantil provavelmente terá como causa esta patologia. Tal conduta criminosa, porém, não isenta o autor das conseqüências penais existentes em nossas legislações.

Inellas (2009, p. 69) conclui que:

> A pedofilia pode ser definida como perversão sexual, onde a pessoa adulta experimenta sentimentos eróticos, em relação a crianças ou adolescentes. A veiculação de imagens ou ilustrações com cenas de pedofilia caracteriza o crime capitulado no art. 241, do Estatuto da Criança e do Adolescente.

3.1.2 Calúnia e Difamação

Divulgação de informações, muitas vezes mentirosas, que podem prejudicar a reputação da vítima. Estes crimes tornaram-se mais comuns com a popularização do site de relacionamentos.

Neste tipo de crime, a pessoa veicula informações contra a vítima, visando atacar principalmente a sua reputação ou a de familiares.

3.1.3 Ameaça

Ameaçar uma pessoa via e-mail ou postagens em sites, por exemplo, afirmando que ela será vítima de algum mal.

Inellas (2009, p.77) afirma:

> Sua conduta é a de ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave. A pena é de Detenção, de um a seis meses ou multa. Portanto, a finalidade do delito ou ameaça é atemorizar a vítima.

3.1.4 Discriminação

Divulgação de informações relacionadas ao preconceito de raça, cor, etnia, religião ou procedência nacional. Tornou-se mais comum com a popularização do Orkut e outros sites de relacionamento.

Muito comum neste tipo de delito estão também os relacionados a homofobia, descriminação de outras nacionalidades, religião e afins. Ocorre em alguns casos também nestes sites a marcação de encontro destes grupos com o objetivo de causar algum mal a pessoas discriminadas por eles.

3.1.5 Espionagem Industrial

Transferência de informações sigilosas de uma empresa para outra concorrente. A tecnologia facilita este tipo de ação, já que um funcionário pode copiar em um palmtop, ou memory stick ou no próprio celular, por exemplo, o equivalente a milhares de documentos.

A espionagem industrial na maioria das vezes envolve pessoas que já trabalharam na empresa e com algum conhecimento técnico, dispõe de métodos para a cópia das informações da mesma. Esta cópia costuma ser feito quando o criminoso ainda é funcionário, e somente após o seu desligamento da organização é

que ele usará estes dados contra a empresa, repassando-as aos concorrentes e causando assim grandes prejuízos.

Para se prever deste tipo de ação, Pinheiro (2009) destaca:

> Para se proteger é essência alinhar uma estratégia que amarra aspectos técnicos e jurídicos, com uso de alguns softwares de monitoramento, adequação legal para que o mesmo possa ser feito sem riscos para a empresa, definição de alguns processos e sua documentação em norma própria e, acima de tudo, conscientização dos usuários de maior acesso a informações privilegiadas, dos gestores ao conselho.

A mesma autora deste artigo termina concluindo:

> Com a baixa cultura de segurança da informação nas empresas, associada a característica solícita do brasileiro, o espião não precisa mais invadir ou interceptar, ele entra pela porta da frente. Precisamos estar mais atentos, sob pena de responsabilidade por negligência e omissão, conforme reza o artigo 1016 do Novo Código Civil Brasileiro.

Muitas empresas estão revisando suas políticas de acesso a informação para que este tipo de delito não comprometa suas atividades. Não é raro um produto que foi lançado por uma empresa ter sido projeto em outra; com o desligamento de algum funcionário a informação acabou indo parar nesta outra, que se apressou para lançá-lo e patenteá-lo em seu nome.

3.1.6 Furto de valores através de transações bancárias

Este tipo de delito sempre foi bastante comum entre os usuários de Internet Banking. Nele o criminoso tenta atrair a atenção da vítima com algum e-mail malicioso (phishing scan), que após aberto, instala no computador da vítima um programa capaz de capturar as senhas destas vítimas.

Há também autores renomados que caracterizam a invasão de servidores do banco para a transferência de fundos direto destes para contas de terceiros, porém, como as instituições bancárias detêm alta tecnologia em seus serviços e os monitoram 24 horas por dia, 7 dias por semana, fica evidente que a configuração deste delito se faz sempre pelo lado do cliente, principalmente utilizando fatores apelativos, também denominada de engenharia social.

Faustino da FEBRABAN, em artigo publicado por Fukushiro (2009) ainda completa e aconselha:

> "Os bancos estão fazendo sua parte, investindo em segurança, por isso os golpistas não invadem os sites de bancos, porque a segurança é muito grande. Eles vão tentar pelo lado mais fraco, que é o usuário. Por isso todos devem tomar atitudes mais seguras na Internet".

Inellas (2009, p.57) relata em seu livro o seguinte caso:

> No dia 5 de janeiro de 2004, vários clientes de um renomado Banco, receberam mensagens, através da Internet, supostamente enviadas pelo estabelecimento bancário, mas, falsas, solicitando-lhes que conferissem se havia registro de transações desconhecidas em suas contas. A mensagem fornecia um Link para uma página falsa, para que os criminosos tivessem acesso aos dados bancários dos correntistas.

É evidente que o fator apelativo neste caso foi a engenharia social, que induz o cliente a clicar no link pelo interesse no assunto da mensagem.

Para evitar a continuidade deste tipo de ocorrência, os bancos implantaram ferramentas de segurança, o que fez com que a incidência deste tipo de delito caísse drasticamente, principalmente com a ferramenta Itoken (Figuras 6 e 7) que nada mais é do que uma seqüência de algoritmos que nunca se repetirão e sua interceptação se torna praticamente impossível, sem que haja o vazamento deste algoritmo.

Além destas ferramentas, algumas instituições bancárias ainda utilizam certificação digital, através de componentes instalados nos computadores de seus clientes.

Figura 5 – Cartão de Segurança do Bradesco
Fonte: site Bradesco

Esta primeira ferramenta (Figura 5 - Cartão de Segurança do Bradesco) diminuiu bastante a ocorrência de fraudes bancárias, porém os criminosos se adaptando a esta ferramenta, passara a utilizar sites falsos pedindo aos clientes que digitassem todas as posições (01 a 70) da mesma.

Figura 6 – Itoken do Banco Bradesco
Fonte: site Bradesco

Figura 7 – Itoken do Banco Itaú
Fonte: site Itaú

Com esta nova ferramenta (Figuras 6 e 7 – Itoken Bradesco e Itaú respectivamente) as interceptações dos códigos gerados por esta se tornaram praticamente impossíveis, pois os sites bancários, somente em operações que envolvam valores, sempre solicitam o código contido nestes aparelhos. Como o algoritmo contido nos mesmos faz com que a numeração mude em um curto intervalo de tempo, o mesmo número não se repetirá e mesmo o cliente tendo o seu computador infectado por alguma ferramenta de interceptação de dados, ela nunca terá acesso aos dados destes pequenos, porém bem funcionais equipamentos.

3.1.7 Invasões a Servidores

Esta modalidade criminosa requer do agente causador alto nível de instrução em informática e tecnologias digitais, e por conseqüência é a de menor ocorrência na Internet. Porém o seu poder de prejuízo se torna bem maior do que qualquer outra forma de ataque em crimes cometidos pelo computador.

Rodrigues (2009) em seu artigo divulgado na Folha de São Paulo relata o seguinte acontecimento:

> **Hackers invadem site do governo, praticam extorsão e podem até apagar luzes de várias cidades no Brasil.**
> Um hacker baseado num país do Leste Europeu invadiu o servidor de computadores de um órgão ligado a um ministério no ano passado. O criminoso trocou a senha do sistema. Paralisou a operação de acesso aos dados. Deixou apenas um recado: só recolocaria a rede novamente em operação após receber US$ 350 mil.

O autor do artigo informa quais atitudes que foram tomadas pelo Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República, através de seu diretor, o matemático Raphael Mandarino Junior:

> Foram momentos tensos. Acionamos a Polícia Federal. Havia um backup [cópia] de todos os arquivos em outro lugar. Uma equipe reconstruiu o servidor com as mesmas informações que o hacker havia tentado destruir. Mas ainda demorou uma semana para quebrar os códigos deixados pelo criminoso no servidor original.
> Uma vez decodificada a senha deixada pelo hacker, notou-se que a máquina da qual partira o ataque estaria localizada no Leste Europeu. “Foi possível descobrir isso pela natureza do IP registrado no servidor atacado", diz Mandarino. "IP" é a sigla para "internet protocol", o número individual de cada máquina e que serve para indicar a localização possível do equipamento.

O desfecho deste caso, também publicado no jornal Folha de São Paulo, se deu da seguinte forma:

> A PF repassou os dados do episódio à Interpol, a força policial internacional. Não houve progresso nas buscas ao hacker, que até hoje não foi capturado. Esse tipo de invasão sai **dos chamados computadores zumbis** (máquinas que servem de ponto de passagem para um ataque, por meio de conexões de internet, que nunca são de propriedade do criminoso).
>
> Essa invasão a um órgão de um ministério brasileiro com tentativa de extorsão é um exemplo da extrema vulnerabilidade dos computadores usados na administração pública no país. Em palestra recente, Mandarino afirmou que "faltam ao país elementos que garantam a segurança e a

> defesa do seu espaço cibernético para proteger a sociedade e nortear a ação dos diversos atores que interagem na grande rede".
> Para comprovar esse diagnóstico basta verificar a maneira banal usada pelo hacker responsável pelo ataque em 2008.
>
> "Essa invasão se deu por uma razão simples: o sistema do servidor desse órgão atacado estava com a senha original que veio no software. Os hackers ficam fazendo varredura e tentando penetrar com as senhas básicas de sistemas originais. Foi o que ocorreu nesse caso."
> Ou seja, o funcionário encarregado de manter em operação um importante órgão público não havia se dado ao trabalho de trocar a senha de fábrica do sistema. Essas senhas são números sequenciais, como "123456", ou palavras como "admin" (abreviação de "administrador"). O hacker precisou apenas fazer varreduras pela internet até achar essa porta praticamente aberta num sistema do governo brasileiro.
> O ataque ocorreu de madrugada. De manhã, o funcionário responsável pelo servidor atingido leu a mensagem que pedia US$ 350 mil. Desconsiderou-a, pois entendeu ser uma piada. Pouco antes do meio-dia, notou que tudo estava indisponível. Só então as primeiras providências foram tomadas.

3.2 Ferramentas e meios utilizados pelos criminosos

Desde o início do uso da Internet, diversas formas de praticar crimes com o uso do computador foram inventadas, renovadas, e ainda continuam sendo.

As formas usadas pelos cybers criminosos vêm se modificando cada vez que as políticas de segurança se moldam para combater este tipo de delito. O crime virtual, assim como o real, nunca irá acabar apenas terá sua forma de agir controlada e sempre modificada.

A internet é um ambiente em extrema mutação. O que é comum hoje daqui a um ano poderá ser totalmente obsoleto e a mesma linha de raciocínio deve ser adotado.

Com os crimes de informática aplica-se a mesma regra, ou seja, sempre estão ocorrendo evoluções na forma e nos tipos de ataques maliciosos, seja eles por hacker, por vírus, ou até mesmo via dispositivos móveis (pen-drives).

3.2.1 Phishing Scan

O Phishing Scan é uma das formas mais comuns de crimes cometidos pela Internet. Ele consiste em o indivíduo enviar milhares de e-mails para as pessoas, normalmente utiliza-se de fator apelativo ou fato que chame a atenção.

A vítima, ao abrir o e-mail visualiza uma mensagem em que é incitada a clicar num determinado campo ou link. O apontador para este link é na verdade um vírus, que se instala automaticamente no computador da vítima e fica monitorando sua navegação. Ao entrar em sites de bancos, este vírus captura os dados digitados pela vítima e os envia, normalmente via comando FTP (File Transfer Protocolo) ou similar, o conteúdo de todas as informações obtidas.

Segundo Nogueira (2009, p.45):

> O termo phishing, pode ser considerado como o envio de e-mails enganosos (com iscas), com a finalidade de disseminação de vírus, furto de dados pessoais e senhas, entre outros. Este tipo de crime acontece muito, normalmente o autor manda um e-mail e quem o recebe ao abri-lo instala uma espécie de programa espião que furta suas senhas e seus dados guardados no seu computador.

3.2.2 Cavalo de Tróia (Trojans Horse)

O Cavalo de Tróia é um programa que se aloca como um arquivo no computador da vítima. Normalmente ele é instalado em decorrência de um phishing scan.

Ele tem o intuito de roubar informações como passwords, logins e quaisquer dados, sigilosos ou não, mantidos no micro da vítima. Quando a máquina contaminada por um Trojan conecta na Internet, poderá ter todas as informações contidas no HD visualizadas e capturadas por um intruso qualquer. Estas visitas são feitas imperceptivelmente.

Ao contrário dos vírus, que tem o pode de se replicar, os cavalos de tróia são programados para agir em determinados espaços de tempo e com a finalidade de apenas capturar dados numa única máquina.

3.2.3 Mail Bomb

O Mail Bomb é caracterizado pelo envio ao mesmo tempo de muitas mensagens por e-mail, superlotando a conta do usuário e fazendo com que a mesma fique indisponível.

Estevão (2009) em artigo publicado no seu site explica:

> É a técnica de inundar um computador com mensagens eletrônicas. Em geral, o agressor usa um script para gerar um fluxo contínuo de mensagens e abarrotar a caixa postal de alguém. A sobrecarga tende a provocar negação de serviço no servidor de e-mail.

3.2.4 Sniffers

É um programa de computador que monitora passivamente o tráfego de rede, ele pode ser utilizado legitimamente pelo administrador do sistema para verificar problemas de rede ou pode ser usado ilegitimamente por um intruso para roubar nomes de usuários e senhas. Este tipo de programa explora o fato dos pacotes das aplicações TCP/IP não serem criptografados.

Estevão (2009) ainda complementa: “O sniffer é um programa ou dispositivo que analisa o tráfego da rede. Sniffers são úteis para gerenciamento de redes. Mas nas mãos de hackers, permitem roubar senhas e outras informações sigilosas.”

Entretanto, para utilizar o sniffer é necessário que ele esteja instalado em um ponto da rede onde passe tráfego de pacotes de interesse para o invasor ou administrador.

3.2.5 Scanner Ports

O objetivo da utilização de scanner ports é a verificação, principalmente na internet, de porta abertas que possam originar uma futura invasão a um computador ou servidor.

Estevão (2009) contempla:

> Os scanners de portas são programas que buscam portas TCP abertas por onde pode ser feita uma invasão. Para que a varredura não seja percebida pela vítima, alguns scanners testam as portas de um computador durante muitos dias, em horários aleatórios.

Existe na Internet uma gama de aplicativo que vasculham a rede a procura de portas abertas ou de falhas nos sistema operacionais dos servidores.

3.2.6 Ping of Death

É uma técnica consiste em se enviar um pacote IP com tamanho maior que o máximo permitido (65535 bytes), para a máquina que se deseja atacar. O pacote é enviado na forma de fragmentos e quando a máquina destino tenta montar estes fragmentos, inúmeras situações podem ocorrer: a maioria da máquinas trava, algumas reinicializam, outras abortam e mostram mensagens no console, etc.

Praticamente todas as plataformas eram afetadas por este ataque, e todas as que não tiveram correções de segurança instaladas, ainda o são. Este ataque recebeu o nome de Ping Of Death porque as primeiras ocorrências deste ataque foram a partir do programa ping, entretanto, qualquer pacote IP com mais de 65535 (pacote inválido) provoca o mesmo efeito.

3.2.7 Quebra de Senha

A quebra de senha é muito utilizada por crackers (termo usado para quebradores de bloqueios e restrições e programadores mal intencionados) na Internet, principalmente com o objetivo de piratear softwares e disponibilizar os mesmos para uso geral.

A quebra de senha é muito comum também em invasões a servidores onde normalmente o criminoso utiliza um aplicativo para efetuar tentativas automáticas, baseado em dicionários e combinações numéricas. Muito comum na quebra de senhas para acesso a serviços diversos é a engenharia social, onde o invasor analisa dados das vítimas (data de nascimento, casamento, endereço e números diversos) a através destes dados tentam invadir tais serviços.

3.2.8 Spoofing de Servidor DNS

Nesta técnica o invasor convence alguém de que ele é algo ou alguém que não é, conseguindo assim autenticação para acessar o que não deveria ter acesso, falsificando seu endereço de origem. É uma técnica de ataque contra a autenticidade onde um usuário externo se faz passar por um usuário ou computador interno.

Spoofing é o ato de usar uma máquina para personificar outra. Isso é feito forjando o servidor Dinâmico de Serviços de Nomes (DNS) de origem de um ou mais hosts empenhados na autenticação das máquinas individualmente. Para realizar uma sessão bem sucedida de spoofing, alguns criminosos temporariamente isolam os servidores que foram clonados.

Na figura abaixo é mostrado um bom exemplo de spoofing, que ilustra claramente esta situação: (a) Situação normal. (b) Um ataque baseado na invasão do DNS e na modificação do registro de Bob que passa a ser visto pelo infrator Trudy´s.

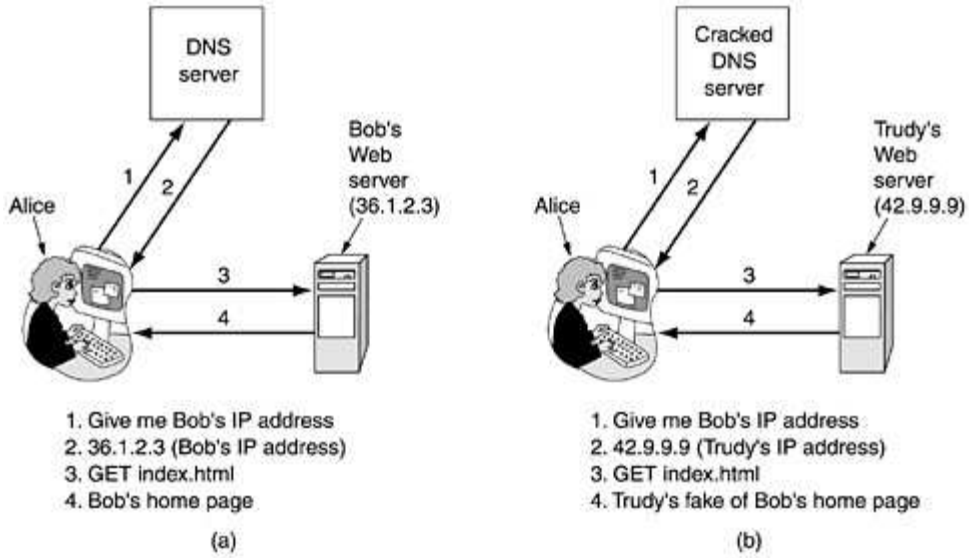


Figura 8: Situação de Spoofing
Fonte: Adaptação de Tanenbaum (2003, p.604)

3.2.9 Denial of Service (Dos) e Distributed Denial of Service (DDos)

Nesta modalidade de crime na Internet, o criminoso efetua automaticamente uma grande quantidade de solicitações a servidores web, utilizando toda a sua banda de tráfego limite com a finalidade de torná-lo indisponível.

O objetivo do autor deste ataque é o dano ao sistema atacado, normalmente os alvos são empresas de grande porte e que utilizam a internet como uma das formas vitais para estrutura do seu negócio. É comum também os criminosos atacarem os servidores governamentais.

A diferença entre o Dos e o DDos é que na primeira apenas uma máquina efetua o disparo de várias solicitações de serviços ao mesmo tempo, enquanto na segunda o criminoso se utiliza de várias estações, normalmente máquinas infectadas para a realização dos ataques simultâneos.

Tanenbaum (2003, p.584) conceitua Dos pelo exemplo:

> Por exemplo, para incapacitar um Web site, um intruso pode enviar um pacote SYN do TCP para estabelecer uma conexão. Então, o site alocará um slot de tabela para a conexão e enviará um pacote SYN + ACK em resposta. Se o intruso não responder, o slot de tabela ficará retido por alguns segundos até o timeout. Se o intruso enviar milhares de solicitações de conexão, todas os slots de tabela serão preenchidos e nenhuma conexão legítima poderá passar.
> Os ataques em que o objetivo do intruso é desativar o destino em vez de roubar dados são chamados ataques DoS (Denial of Service — negação de serviço). Em geral, os pacotes solicitados têm endereços de origem falsos, para que o intruso não possa ser rastreado com facilidade.

Tanenbaum (2003, p.584) ainda diferencia DDos da seguinte forma:

> Uma variante ainda pior é aquela em que o intruso já entrou em centenas de computadores em outros lugares do mundo, e depois comanda todos esses computadores em um ataque ao mesmo alvo ao mesmo tempo. Essa estratégia não apenas aumenta o poder de fogo do intruso, mas também reduz a chance de detecção, pois os pacotes estão vindo de um grande número de máquinas pertencentes a usuários insuspeitos. Um ataque desse tipo é chamado DDoS (Distributed Denial of Service), e é muito difícil proteger-se contra ele. Ainda que a máquina atacada pode reconhecer rapidamente uma solicitação falsa, processar e descartar a solicitação é um processo que leva algum tempo e, se chegarem solicitações em número suficiente por segundo, a CPU passará todo seu tempo lidando com elas.

A figura abaixo, mostra de forma clara como é efetuado os ataques aos servidores:

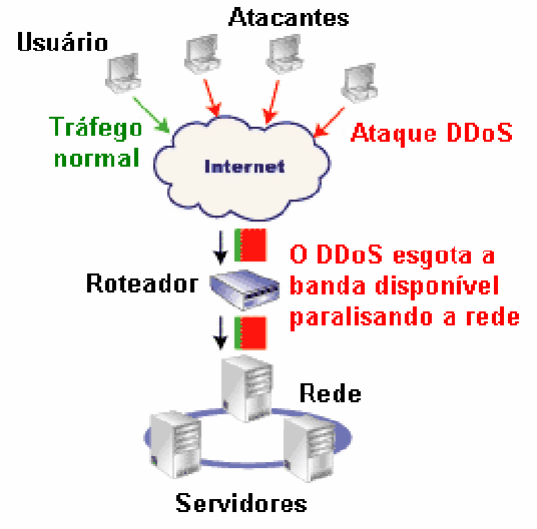


Figura 9: Modelo de ataque DDos

Fonte: Adaptação do Site Aula de Redes

3.3 Migração dos Delitos nos Meios Convencionais para o Meio Virtual

A teoria utilizada para se analisar os aumentos da incidência de crimes virtuais é bem parecida com a do crescimento populacional de uma determinada cidade ou região.

Em uma cidade com poucos habitantes, por exemplo, a incidência de crimes é bem pequena, principalmente devido ao fato de todos se conhecerem e saberem quem são. Nas cidades maiores, acontece o inverso. O número de habitantes é exponencialmente maior, as pessoas pouco se conhecem, e a sensação de anonimato estimula o infrator a cometer seus delitos.

Na Internet ocorre fenômeno parecido. Os crimes cometidos na grande rede vêm crescendo proporcionalmente com o aumento do uso da mesma e a tendência com este crescimento é que aumente proporcionalmente ao seu uso. Aliado a este fator, estão os rootkits (kits de invasão), a qual programadores experientes disponibilizam para usuários leigos (conhecidos como lammers) ferramentas automatizadas para a execução de tais crimes.

No gráfico abaixo é possível analisar que a quantidade de usuários na Internet vem aumentando gradativamente a cada ano:

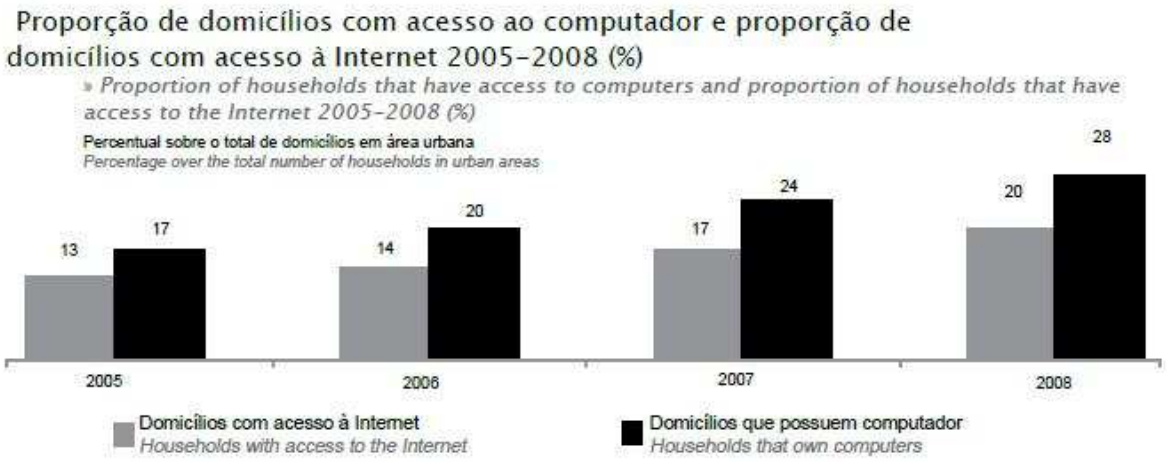


Gráfico 1 – Domicílios com Acesso a Internet em %
Fonte: Adaptação de Cetic.br - 2008

Concomitantemente com o aumento de seus usuários a internet vem sendo, de maneira crescente, alvo de incidentes de segurança podendo ser comprovado pelo gráfico abaixo retirado do site da CERT.BR, que demonstra a enorme evolução deste incidentes de 2006 e 2009, principalmente em comparação aos outros anos:

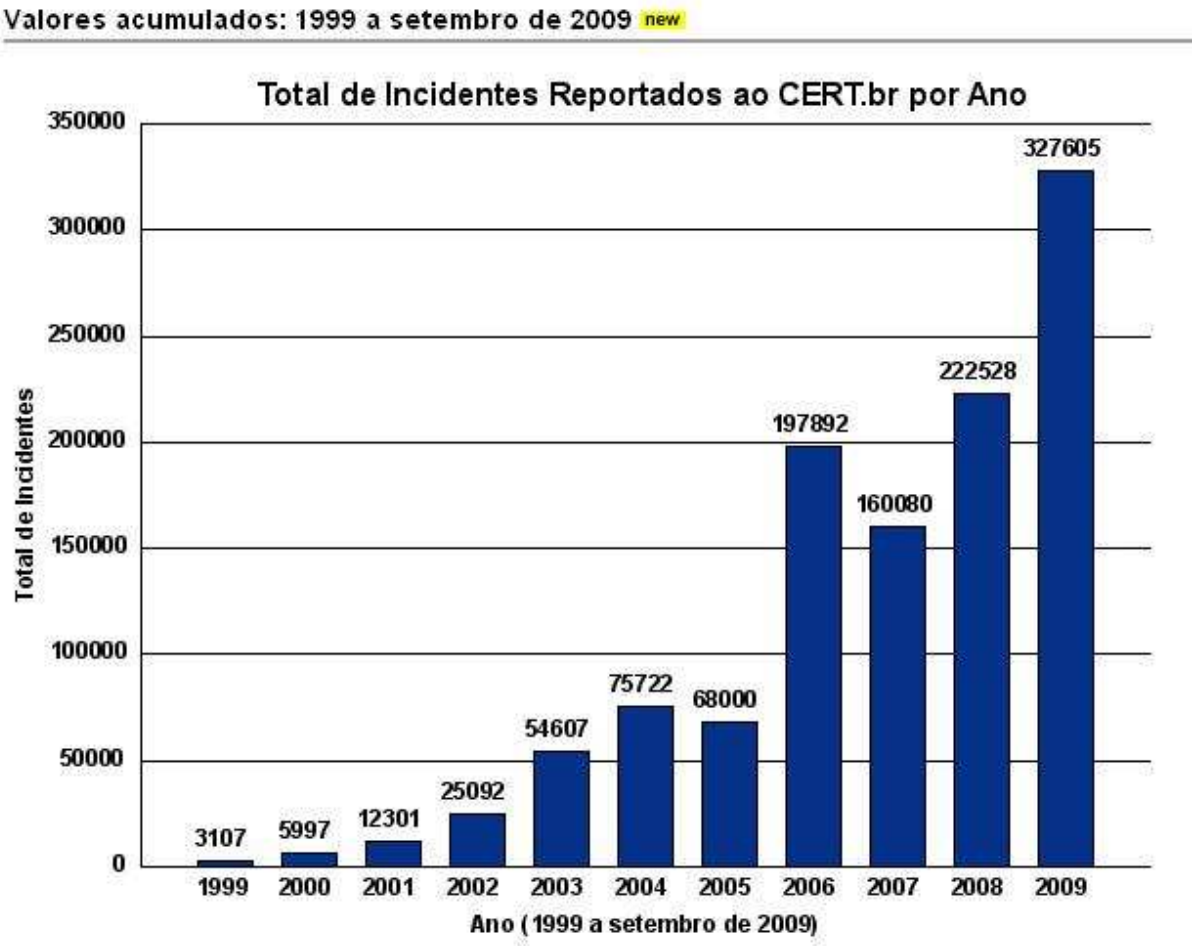


Gráfico 2: Incidentes de Segurança Reportados ao CERT.BR de 1999 a 2009

Fonte: Adaptação de CERT.BR

Ainda de acordo com o site CERT.BR, a maioria da fraudes reportadas ao mesmo foi o de Cavalos de Tróia (72,61%) e as tentativas ocorrem na maioria das vezes na segunda-feira, o que indica uma forte tendência dos criminosos na busca por dados de usuários, principalmente os de Internet Banking, conforme demonstram os gráficos abaixo:

Gráfico 3: Incidentes Reportados ao CERT.br -- Julho a Setembro de 2009
Fonte: Adaptação de CERT.BR

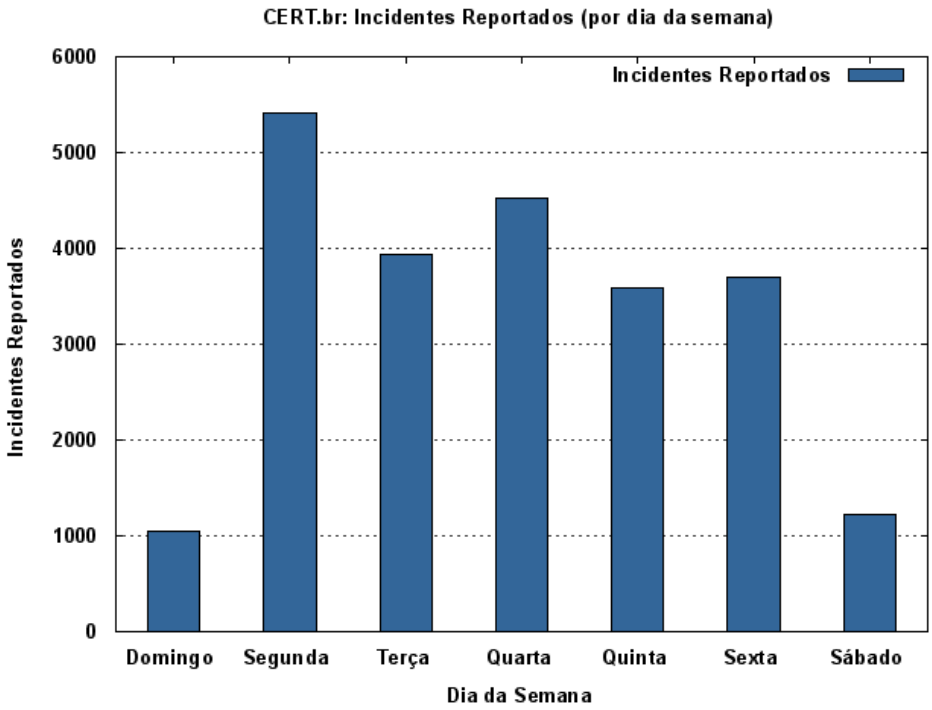


Gráfico 4: Incidentes Reportados ao CERT.br – Por dias da Semana
Fonte: Adaptação de CERT.BR

Um dado relevante mostrado pela CERT.BR é que a maioria dos incidentes reportados têm como origem o Brasil, seguido pelos Estados Unidos. Estes dados revelam ainda que a maioria dos criminosos digitais parte e originam as condutas criminosas em território brasileiro.

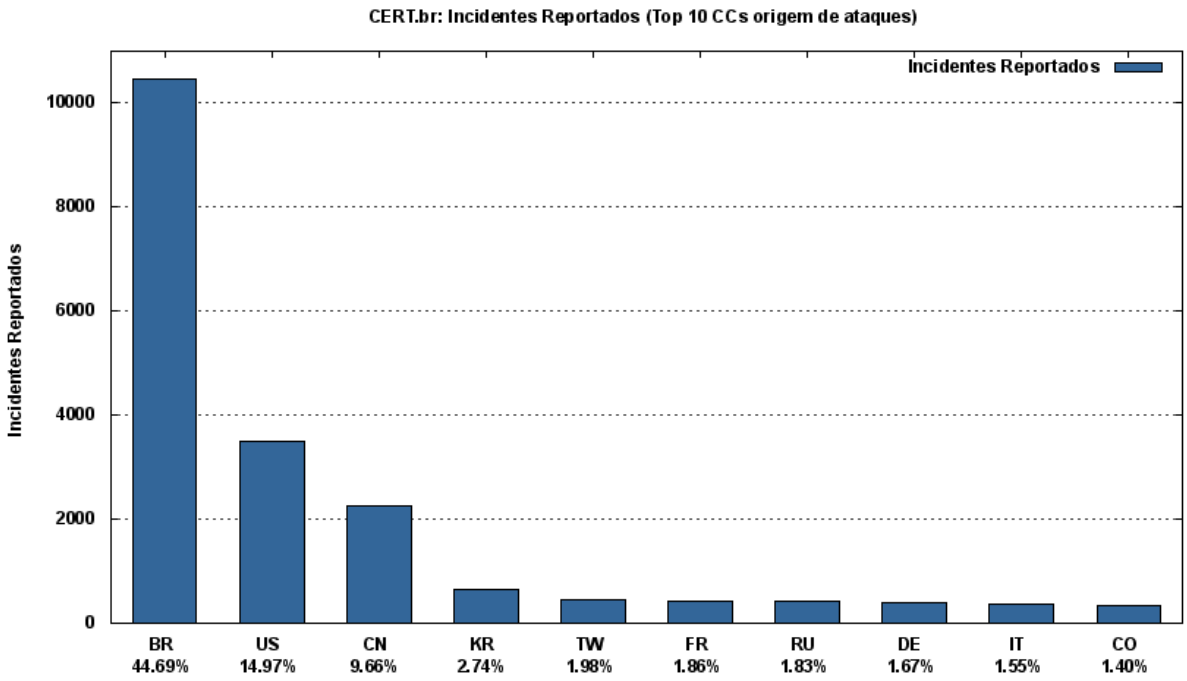


Gráfico 5: Origem dos Incidentes Reportados ao CERT.BR -- Julho a Setembro de 2009
Fonte: CERT.BR

3.4 Apuração dos crimes cometidos através do uso do computador

A apuração de um crime praticado através do uso do computador não é uma tarefa simples. Por envolver o uso de tecnologias muitas vezes pouco aplicadas a pessoas fora da área de informática, torna-se necessária a condição de que o agente responsável por tais investigações tenha uma base sólida nesta área e consiga embasar suas provas de forma clara, e principalmente, tecnicamente sólida.

O início de uma investigação sobre um crime digital quase sempre se dá pela denúncia ou queixa da vítima, é raro o caso em que o crime é descoberto sem o auxílio de pessoas diretamente envolvidas na ocorrência.

Após a vítima ter lavrado o Boletim de Ocorrência em uma delegacia mais próxima, o mesmo, se não houver indicação de autoria é enviado ao Departamento de Investigações sobre o Crime Organizado – DEIC, ou investigado na própria delegacia quando há a autoria constatada do fato.

Umas das primeiras providências tomadas pela autoridade policial é o pedido de perícia na máquina da vítima. Nela estarão todas as evidências necessárias para que se descubra como foi cometido o crime, quando e por quem. É importante destacar neste aspecto, que na própria solicitação de perícia o delegado deverá, sempre que possível, informar o motivo da mesma e quais áreas do computador precisam ser periciadas, evitando assim que laudos ou análises inoportunas sejam anexados aos autos.

Outro ponto importante é o tipo de delito a ser apurado. Dependendo do crime, a apuração se faz de uma maneira e nem sempre a mesma técnica é utilizada para outros delitos. **O Manual do Ministério Público Federal – Crimes de Informática – Coletando e Analisando Evidências, vide Anexo B deste trabalho, contempla algumas das diversas formas de delitos e suas respectivas medidas a serem adotadas.**

3.4.1 Análise de Roteadores

A análise de roteadores consiste em verificar nos dispositivos a qual uma ou mais conexões foram feitas com o objetivo de aplicação do crime virtual. Normalmente nestes equipamentos, são guardados registros recentes de conexões efetuadas (logs), assim como a descrição dos computadores conectados e por quanto tempo permaneceram em uso. Sua análise como objeto de prova é fundamental para o desfecho de casos.

É possível comparar a análise do roteador na área de informática, como sendo os últimos passos dados pelo criminoso na vida real. Ele indicará, a menos que o criminoso ou alguém tenha apagado seus registros, toda a movimentação e a quantidade de dados trafegados pela rede através de seus logs.

A figura abaixo mostra a tela de configuração de um roteador e seus respectivos registros de conexão, inclusive com o Mac Adress da placa que se conectou:

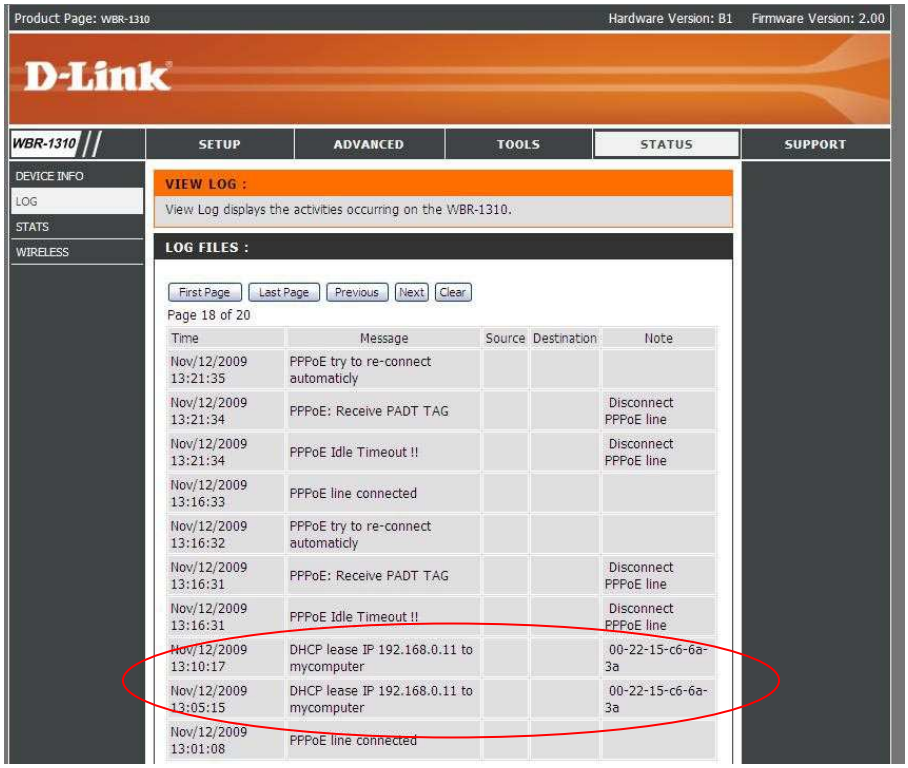


Figura 10: Administrador de Roteador D-Link

Fonte: Roteador D-Link

3.4.2 Análise de Logs

O conceito de Log pode ser bem definido pela Cartilha de Segurança para Internet Parte VII: Incidentes de Segurança e Uso Abusivo da Rede, (2003 p.4):

> Os logs são registros de atividades gerados por programas de computador. No caso de logs relativos a incidentes de segurança, eles normalmente são gerados por firewalls ou por sistemas de detecção de intrusão.
> Os logs relativos a ataques recebidos pela rede, em geral, possuem as seguintes informações:
> - Data e horário em que ocorreu uma determinada atividade;
> - Endereço IP de origem da atividade;
> - Portas envolvidas;
>
> Dependendo do grau de refinamento da ferramenta que gerou o log ele também pode conter informações como:
> - O timezone do horário do log.;
> - Protocolo utilizado (TCP, UDP, ICMP, etc).
> - Os dados completos que foram enviados para o computador ou rede.

O log é uma ferramenta importantíssima para a constatação de autoria de qualquer atividade eletrônica. Nele é possível encontrar padrões e hábitos de usuários, ver qual a demanda maior de acesso e em quais horários além também de ser uma ferramenta coercitiva para o uso adequado das conexões de internet, principalmente em ambientes corporativos.

Em se tratando de crimes cometidos pelo computador, os logs devem ser preservados e enviados para a perícia, para que a mesma comprove através de laudos a autoria do delito em questão e qual endereço IP praticou tal ato.

3.4.3 Rastreabilidade das Conexões

A rastreabilidade das conexões de internet é feita usando os dados adquiridos nos respectivos logs (em caso de logs gerados por roteadores e firewalls), nos corpos das mensagens de e-mail (mensagens de e-mail) ou em qualquer outra mídia que possibilite a identificação do endereço IP do autor.

De posse destes dados, o delegado responsável pelo caso, deverá requerer via ofício a provedora, os dados do usuário relacionados com aquele

endereçamento IP.

De acordo com Paiva (2006, p.9):

> A primeira preocupação do investigador ao se deparar com um delito cometido por meios eletrônicos é a autoria, isto é, a identificação do autor da infração penal. Na maioria das vezes, a pessoa que pretende cometer uma infração penal utiliza-se de identidade falsa, daí a importância da cooperação das Provedoras de Acesso nesse tipo de investigação.

Alguns autores discorrem ainda, que pelo fato de os provedores não gerenciarem o tráfego das informações que são transmitidas pela internet, os mesmos não se enquadram diretamente na Lei das Telecomunicações, e sendo assim passam a vigorar como serviços adicionais, como cita o artigo 61 da Lei das Telecomunicações:

> Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações.
> § 1º Serviço de valor adicionado não constitui serviço de telecomunicações, classificando-se seu provedor como usuário do serviço de telecomunicações que lhe dá suporte, com os direitos e deveres inerentes a essa condição.

Ainda neste ponto, Inellas (2009 p.25) ainda complementa:

> E mais, a análise dos dados constantes dos Cadastros dos Clientes das Provedoras de Acesso, não caracteriza interceptação do fluxo de comunicações em sistemas de informática (Lei n.9.296/1996), sendo certo, portanto, que a Requisição Judicial (Lei n.9.296/1996 art. 10), a elas não se aplica.

Seguindo esta linha de trabalho, ao obter o endereço IP do autor do delito, a autoridade policial deverá efetuar a pesquisa nos diversos sites para localização de IP (“registro.br” no Brasil e “Whois” em outros países) para descobrir qual operadora de Telecomunicação atribuiu o endereço IP para o suposto usuário criminoso.

De posse destes dados, basta notificarem a operadora e obter o provedor a qual o mesmo usuário foi autenticado; esta ação não caracteriza quebra de sigilo e através da cooperação destes órgãos tentar obter os dados da conexão inicial do delito, o que por muitas vezes, não significa chegar de fato ao autor do crime.

3.4.4 Perícia Forense e Provas Técnicas

Tão importante quanto o processo investigatório para a descoberta do autor nos crimes cometidos pelo computador é a sua correta coleção e guarda de provas, que no decorrer do processo irão dar aos aplicadores da persecução penal (Ministério Público e Judiciário) fatores concretos e contundentes da autoria do delito em questão.

O Código de Processo Penal em seu artigo 157 expõe: “São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.“ Esta afirmação indica que provas com sua legitimidade contestada serão ignoradas no decorrer do processo e, portanto terão validade nula.

É por estes motivos que os agentes, ao se depararem com determinados tipos de provas digitais, precisam estar preparados para lidar com elas. Em determinadas situações a prova colhida num computador só poderá ser analisada se o mesmo permanecer ligado, pois os dados poderão estar em sua memória volátil (RAM – Random Acess Memory). Valerá mais a pena esperar a chegada de um Perito especialista ao local do fato, do que simplesmente desligar a máquina e enviá-la para a perícia.

Outro fator importante é tentar ao máximo fazer com que todas as provas colhidas na cena do crime ou até mesmo em investigações obtidas pela internet ou quaisquer outros meios sejam enviadas também para a análise pericial. Os laudos obtidos através destas análises são indispensáveis para a apreciação do judiciário e obrigatório conforme os artigos 158 e 159 do Código de Processo Penal:

> Art. 158. Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.
> Art. 159. O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior.

4. ESTUDO DE CASOS: ORKUT, AMEAÇAS E FRAUDES BANCÁRIAS

Os estudos de caso mostrados neste trabalho tomam como fonte os principais fatos que envolvem os crimes na Internet no Brasil.

Alguns casos servem como alerta sobre a falta de punibilidade aos autores; o caso do Orkut acaba sendo um marco e será abordado de forma mais ampla neste capítulo.

4.1 Caso 1 – Uso do Orkut no Brasil

Este estudo de caso abordará o uso do Orkut, um fenômeno em sites de relacionamentos aqui no Brasil, pela grande quantidade de usuários que o mesmo abrange.

O Orkut acabou virando uma mania, principalmente entre os jovens, e que este serviço prestado pela Google, tem a sua maioria de usuários aqui no Brasil, conforme mostram os gráficos abaixo:

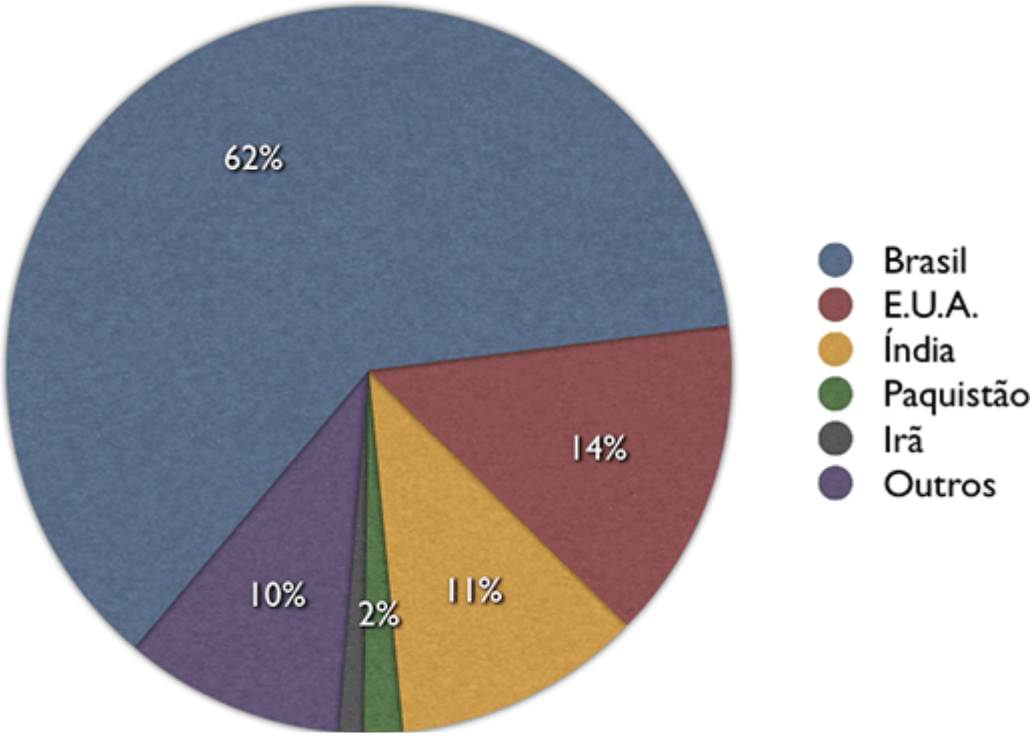


Gráfico 6 – Países que mais usam o Orkut
Fonte: Google

Ranking de usuários por países			
Demografia do Orkut em 31 de Março de 2004[24]			
	Estados Unidos		51,36%
	Japão		7,74%
	Brasil		5,16%
	Países Baixos		4,10%
	Reino Unido		3,72%
Demografia do Orkut em 6 de Novembro de 2008			
	Brasil		51,18%
	Estados Unidos		17,46%
	Índia		17,40%
	Paquistão		1,01%
	Reino Unido		0,49%
	Afeganistão		0,48%
	Japão		0,43%
	Portugal		0,39%
	Alemanha		0,39%
	Austrália		0,39%

Gráfico 7 – Ranking de Usuários por Países
Fonte: Google

4.1.1 A Situação

Por se tornar o maior site de relacionamentos em uso no Brasil, e por ter seus servidores hospedados em áreas internacionais, o Orkut passou a ser uma incubadora de crimes.

A sensação de impunidade movia os seus integrantes a realizar diversos crimes, entre eles racismo, ameaças, apologias diversas, homofobia entre tantos.

Tal situação deixava as autoridades sem poder de ação, já que como os servidores estão em territórios estrangeiros, nada podia ser feito contra os autores de tais delitos; inclusive a quebra de sigilo nas operações criminosas era impedida por tal situação.

4.1.2 Solução

Depois de uma grande repercussão nas mídias Brasileiras e temendo uma ação de maior rigor aqui no Brasil, a Google, que é detentora do serviço Orkut, resolveu firmar um acordo com o Ministério Público Federal, criando ferramentas que bloqueiem alguns conteúdos impróprios e criando uma equipe para avaliar os incidentes ocorridos no site e notificar o Ministério Público Federal em casos de ocorrência de crimes.

Tal situação só foi possível após um pedido formal de uma CPI – (Comissão Parlamentar de Inquérito) instaurada sobre os crimes de pedofilia. A mesma CPI chegou à conclusão de que era necessário o fechamento das atividades da google.com em território Brasileiro se nenhuma atitude fosse providenciada contra tais práticas criminosas.

Temendo pela perda de seus serviços em território brasileiro e pelo fechamento do site de relacionamentos, a Google resolveu fechar um acordo com as autoridades brasileiras, se disponibilizando a colaborar com os órgãos responsáveis pelas apurações de delitos na internet, além de criar uma equipe que receba denúncias e exclua o usuário do site.

Entretanto, segundo Braun (2009), em seu artigo publicado no site IdgNow: “Denúncias de crimes no Orkut crescem mais de 10 vezes, diz relatório”, não houve redução, mas sim o aumento das denúncias:

> Embora o Google tenha ampliado a equipe de monitoramento de comunidades e usuários ilegais no Orkut, aumentado a velocidade na retirada de comunidades criminosas do ar e tenha aberto canais diretos para envio de dados de criminosos à Justiça brasileira, aos olhos do Ministério Público Federal em São Paulo (MPF-SP) e da ONG Safernet, retirar as comunidades do ar não é suficiente.

Ainda no próprio artigo, a autora entrevistou Thiago Tavares, presidente da ONG Safernet que concluí:

> A página pode sair do ar, mas o criminoso não, alerta Tavares. As comunidades de pedofilia são retiradas do ar em até dois dias. O processo é mais demorado quanto a crimes de racismo, por exemplo (...). Sem dúvida é uma ação importante, mas não suficiente, alerta.

4.2 Caso 2 – Ameaça via e-mail

Este estudo de caso mostra a forma como uma pessoa recebe em sua caixa postal diversas mensagens ameaçadoras, e quais as conseqüências ocorridas neste caso. O mesmo foi Retirado do Livro Crimes de Informática, (Nogueira, p. 31) e segundo o autor, foi “O Primeiro caso de crime pela internet esclarecido no país.”

4.2.1 A Situação

Em 28/08/1997 famosa jornalista da TV Cultura recebeu 105 mensagens (e-mails) de cunho erótico-sexual além de ameaçador a sua integridade física. As mensagens foram recebidas a partir das 00h31min24seg do dia 21 de agosto de 1997, quinta-feira, encerrando as 00h52min22seg do mesmo dia, numa média de uma mensagem a cada 11,9 segundos, o que, em princípio, indicava ter o ameaçador utilizado de programa específico de envio de mensagens simultâneas (MAIL BOMB).

4.2.2 Solução

O nome utilizado (username) “estrupador@macho.com.br” (sic), nome inexistente, indicava ser nome fictício. A identificação começou pela análise feita pelo caminho inverso da mensagem: a identificação do cabeçalho da mensagem (header) apontava que, antes de chegar na TV Cultura, as mensagens passaram pelo provedor galileo.base.com.br (IP-200.240.10.101), que foi recebido como macho.com.br (IP-200.224.16.120). Com essas informações e através de computadores da delegacia de polícia, utilizamos comandos de busca (ferramentas de software) chamada traceroute e descobrimos que o provedor que possui números IP 200.224.16.x, e seguintes, está ligado a GlobalOne. A GlobalOne recusou-se a

colaborar com a polícia, entretanto foi possível descobrir utilizando ferramentas de localização (software whois), concluindo-se que a mensagem foi encaminhada através de outro provedor, o STI-NET São PauloOn Line S/C Ltda. (Classe IP netnumber 200.224.16.0., Classe IP Netblock 200.224.16.0 – 200.224.16.255, IP Netnumber 200.224.16.0/24). De posse desses dados, nos dirigimos até o STI que colaborou plenamente com a polícia sendo possível analisar os arquivos de registros de eventos (logs). Ao analisarmos esses registros, iniciamos a busca pelo horário exato do envio da mensagem, e quem teria sido o autor.

A dificuldade desse rastreamento deveu-se ao fato de que o nome de usuário “username” havia sido deliberadamente falsificado para “estrupador@macho.com.br”. Mas, como a mensagem havia sido direcionada através do provedor base.com.br, analisamos os usuários do provedor STI que teriam utilizado, nas últimas semanas, qualquer envio de mensagem através da base.com.br, utilizamos para isso a ferramenta de software (finger), ocasião em que localizamos o usuário, (username) “jasoft”, pertencente a Fulano de Tal, Analista de Sistemas, residente a Rua ..., n.º 111 – Socorro. Com essas informações, solicitamos autorização judicial para efetuar busca e apreensão do computador de tal usuário.

O mandado foi cumprido, sendo o acusado surpreendido, na manhã do dia 28 de agosto, em sua residência, quando se preparava para ir trabalhar. Não houve qualquer reação, entramos na residência e vistoriamos o seu computador, sendo possível localizar um programa de computador fantasma, chamado Unabomber, e especialmente criado para envio de milhares de mensagens simultâneas, além de mudar o nome do usuário dando, assim, uma aparência apócrifa ao criminoso virtual.

Numa análise mais apurada do computador, foi possível encontrar o arquivo “texto.txt”, onde estava a cópia da mensagem que foi enviada a vítima. Descobrimos também outra mensagem, com o mesmo conteúdo, mas endereçada a uma pessoa de prenome (...), sendo que, diante das evidências, não restou ao acusado outra opção senão confessar a autoria do delito, dizendo, ainda, que além das ameaças encaminhadas aquela jornalista, enviou outras para uma famosa Jornalista da Folha de São Paulo. Meses depois o acusado, um excelente analista de sistemas, foi condenado pelo Juiz do Fórum da Lapa a prestar serviços junto a Academia de Polícia Civil, dando aulas de informática para novos policiais.

4.3 Caso 3 – Quadrilha de Fraudes Bancárias

O caso a seguir mostrará o processo investigatório que culminou na prisão de uma quadrilha de piratas virtuais, que enviavam mensagens as pessoas por e-mail e através da ingenuidade de alguma delas, conseguiam obter os dados bancários e efetuar transferências e saques de quantias diversas.

Segundo divulgado pela própria equipe de investigação, o grupo foi responsável por capturar dados de pelo menos 3.000 usuários por meio de e-mails falsos de instituições financeiras e órgãos públicos. Os dados obtidos nos computadores das vítimas permitiam que os piratas virtuais acessassem as contas bancárias das vítimas.

4.3.1 A Situação

O usuário do computador, neste caso, recebe em seu e-mail uma mensagem de conteúdo apelativo, quase sempre ligado a fatos dos momentos ou assuntos instigantes.

Ao abrir a mensagem, a mesma instala automaticamente no computador da vítima um programa espião (Phishing Scan), que fica monitorando o uso do mesmo, e ao adentrar num site bancário e digitar suas informações bancárias, o mesmo envia automaticamente estas informações para um servidor hospedado fora do país, dificultando o rastreamento destas práticas delituosas.

4.3.2 Solução

Ao se deparar com o caso, os policiais responsáveis pelo mesmo primeiramente procuraram a vítima que relatou o caso através do Boletim de Ocorrência. Fizeram diversas perguntas a vítima, entre elas a onde costuma acessar o sistema bancário e qual a freqüência que o fazia.

O banco, por dispor de seguro, ressarciu o seu cliente imediatamente, mas se colocou a disposição para colaborar com as investigações no que fosse necessário.

O primeiro passo para o levantamento dos dados deste caso é fazer o caminho reverso, ou seja, fazer o levantamento dos dados através das operações efetuadas pelos criminosos, pois o rastreamento de sites internacionais usados para a coleta dos dados das vítimas é bem mais complexo e demorado.

Levantou-se que foram feitas cinco recargas de celulares pré-pagos e o pagamento de aproximadamente quatro contas de consumo. O passo seguinte para o andamento das investigações foi o pedido de quebra de sigilo telefônico dos telefones celulares ao juiz através de ofício e o detalhamento das contas através do sistema do Banco.

Em levantamento das interceptações telefônicas autorizadas pela justiça, descobriu-se que os criminosos iriam se reunir em uma determinada data. As contas de consumo levantadas mostraram também que os titulares das mesmas eram parentes dos levantados pela interceptação.

Um novo pedido ao Judiciário foi realizado, solicitando o mandado de Busca e Operação para o logradouro descoberto na escuta, além do mandado simultâneo nos endereços envolvidos, que constavam nas contas pagas.

Após dois dias de monitoramento, averiguo-se que havia muita movimentação no local do encontro, e que muitas pessoas adentravam o mesmo e após alguns minutos, iam embora. Foi decidido que a Busca se daria no dia e hora marcado para a reunião do grupo, onde seria mais fácil efetuar a prisão de todo o bando.

No dia e hora marcados foram executados quatro mandados de busca, onde após intensa averiguação constatou-se formar uma quadrilha composta por ex-assaltantes de bancos que decidiram migrar para esta nova prática delituosa.

Após o fim das investigações e conclusão do Inquérito Policial, descobriu-se também que o grupo comprava os Kits de invasão de um hacker, e os enviava para as vítimas de computadores diversos, para não chamar a atenção. Foram presos e indiciados, no total 15 pessoas, além da apreensão de um menor de 16 anos, indicado como o hacker responsável pela criação dos Kits.

5. MÉTODOS DE PREVENÇÃO

Grande parte das pessoas que são vítimas de crimes eletrônicos acaba revelando que desconhecia formas de proteção ou os perigos causados por um uso não adequado de seu equipamento.

Por este tipo de perfil ser o mais comum nos registros das vítimas, torna-se necessário um projeto para a conscientização digital para quem usa e depende de computador no seu dia-a-dia.

Nota-se, porém, que grandes empresas como a Microsoft e outras, apostam mais em sistemas blindados contra uso irregulares do que tentar informar o usuário que algumas utilizações poderão ser prejudiciais.

É recomendado aos usuários de computadores em geral que adotem as seguintes medidas:

- **Utilização de Antivírus**: a utilização de sistemas antivírus, principalmente com os mesmos atualizados reduz drasticamente o risco de se contrair um vírus ou demais pragas em seu computador. É recomendado que, se o usuário utilizar o computador para processos críticos e que envolvam valores, que se utilize uma ferramenta de antivírus paga, pois estas possuem atualização mais freqüente e proteção mais eficiente.

- **Utilização de Firewalls**: Programas ou Equipamentos Profissionais de Firewall ajudam a proteger os computadores contra invasões externas, principalmente os servidores que ficam ligados permanentemente e têm sempre o mesmo endereço de IP. Usuários domésticos, por usar conexões de banda larga com IP´s dinâmicos, que mudam seu endereço toda vez que se realiza uma conexão, podem usar o próprio Firewall do sistema operacional ou um gratuito disponível na Internet.

- **Uso de Sistemas Operacionais Alternativos**: o sistema operacional Windows da Microsoft por ser o mais popular e conhecido mundialmente tem sido o preferido para o desenvolvimento de vírus e pragas. Este fato ocorre porque o mesmo sistema operacional além de ser de longe o mais conhecido e disseminado, é o mais afetado quando o assunto são ataques e invasões. Para quem busca uma navegação segura e com pouca probabilidade de ocorrência em crimes eletrônicos, recomenda-se que utilize um sistema operacional de código aberto, como o Linux, por exemplo.

- **Navegação Segura**: a navegação segura é uma das formas mais eficientes de não ser vítima na internet. De nada adianta ter antivírus poderosos, programas de proteção personalizados no computador se os sites acessados pelo usuário são de conteúdo duvidoso ou maléfico. A adoção de navegação somente em sites conhecidos é certamente uma forma bem abrangível de se evitar danos ao computador. Além disso, existe o fator de que muitos computadores são compartilhados entre membros da família, o que torna a máquina mais suscetível a contaminação. Neste caso, o melhor a ser feito é criar contas de usuários diferentes para cada pessoa e sempre mantendo-as com limitações.

- **Prevenção ao abrir e-mails**: devido aos Phishing Scan constantes na internet, recomendam-se a quem lê os e-mails que somente proceda à abertura de quem lhe são confiáveis. Desconfie de ofertas milagrosas ou notícias bombásticas; certamente será uma armadilha para a instalação de uma praga. Quanto aos anexos, nunca abra sem examinar antes pelo programa antivírus ou arquivos com as extensões .scr, .exe, .bat e etc.

6. CONSIDERAÇÕES FINAIS

Os crimes cometidos através do uso de computadores deixaram de ser apenas um sinal de ameaça para se tornarem bastantes comuns, reais e cotidianos na vida das pessoas.

A atual tendência de que todos os serviços prestados, tantos pelas empresas privadas como órgãos públicos sejam migrados para a Internet é sem sombra de dúvida uma evolução e democratização para todos, mas requer uma contra medida para que estes mesmos serviços não sejam alvos de criminosos e se forem, sejam rapidamente identificados e punidos.

A mensuração das perdas provocadas por este tipo de crime ainda não são calculadas com exatidão, porém, pode-se prever que os mesmos possam provocar desfalques enormes e imensuráveis em todos os ramos da sociedade se nada for feito ou regulamentado.

É preciso, portanto, que os projetos de lei que abordam os crimes digitais e suas condutas passem em todas as suas esferas de tramitação, e comecem a vigorar como lei o quanto antes, pois no momento não há nenhuma ferramenta que consiga penalizar tais atitudes, apenas os resultados causados por elas, o que nem sempre acaba sendo eficaz.

Paralelamente é preciso treinar os agentes públicos para que de maneira adequada consigam detectar e rastrear rapidamente os incidentes ocorridos e possam dar a sociedade uma resposta rápida e ágil no combate a este tipo de delito. As academias de polícia, em seus processos de seleção, já estão dando maior enfoque aos candidatos que tenham maiores conhecimentos em informática, principalmente em nível técnico, pois a carência de profissionais com estas características é muito grande.

No âmbito da sociedade em geral também é necessária que se faça uma campanha de conscientização e mobilização para o uso consciente e seguro da internet e de suas ferramentas disponíveis para todos. O computador, há tempos, deixou de ser um instrumento de apenas diversão para se tornar o meio que mais controla as coisas e principalmente, a vida das pessoas.

Por outro lado, não se pode tornar a internet um local totalmente censurável e controlado, pois o intuito deste meio de comunicação é a democratização da informação, da cultura e do conhecimento em geral. Controlar e censurar este tipo de informação vai contra tudo o que os idealizadores desta grande rede e a sociedade como um todo anseiam.

Portanto é preciso que diante desta vasta rede e com milhões de usuários, se acabe com a sensação de que a impunidade e a desordem façam parte deste cenário e, com isto, a transformem num local seguro, agradável e principalmente confiável para que todos possam aproveitá-la. A substituição do termo censura por monitoramento seria a solução mais simples e eficiente.

REFERÊNCIAS

ARAGÃO, Francisco. **Proxies o que são?**. 12 de outubro de 2009.
Disponível em <http://pplware.sapo.pt/2009/10/12/proxies-o-que-sao/>
Acessado em 04 de nov. de 2009.

BRASIL, **Constituição da República Federativa do**.
Disponível em <www.planalto.gov.br/ccivil_03/Constituicao/Constitui%E7ao.htm>.
Acessado em 10 de set. de 2009.

BRAUN, Daniela. **Denúncias de crimes no Orkut crescem mais de 10 vezes, diz relatório**. 23 de abr. de 2007.
Disponível em: <http://idgnow.uol.com.br/internet/2007/04/23/idgnoticia.2007-04-23.6011316931/>
Acessado em 10 de out. de 2009.

CARPANEZ, Juliana. **Conheça os Crimes mais comuns**. 07 de jan. de 2006.
Disponível em <http://www1.folha.uol.com.br/folha/informatica/ult124u19455.shtml>
Acessado em 20 de set. de 2009.

CERT.BR. **Cartilha de Segurança para Internet**. Versão 3.1 - ©2006 CERT.br
Disponível em <http://cartilha.cert.br/>
Acessado em 05 de nov. de 2009.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Jus Navigandi, Teresina, ano 1, n.º 12, mai de 1997.
Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1826>
Acessado em 27 de set de 2009.

DEMETRIO, Amanda. **Entenda como funciona uma delegacia que investiga crimes eletrônicos**. W News – UOL. 24 de jun de 2009.
Disponível em
<http://wnews.uol.com.br/site/noticias/materia.php?id_secao=4&id_conteudo=13706>
Acessado em 05 de nov. de 2009.

FUKUSHIRO, Luiz. **Utilize o Internet banking sem medo**. Site UOL. 09 de fev de 2009.
Disponível em
<http://tecnologia.uol.com.br/seguranca/ultnot/2009/02/09/ult6065u26.jhtm>
Acessado em 10 de nov. de 2009.

ESTEVÃO, Ronaldo Bezerra. **Tipos de Ataques**. Site Aulas de Redes. 10 de nov de 2009.
Disponível em
<http://www.auladeredes.com.br/capa/artigos-mainmenu-53/35-seguran/31-tipos-de-ataques.html>
Acessado em 10 de nov. de 2009.

GUIMARÃES, A. **Segurança em redes privadas virtuais** – VPNS. São Paulo: Editora Brasport, 2000.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet** – 2.ª Edição – Edição atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009.

JESUS, Damásio E. de. **Direito Penal**. Parte geral. 26ª ed. São Paulo: Editora Saraiva, 2003.

NOGUEIRA, Sandro D'Amato. **Crimes de Informática** – 2.ª Edição. Leme: BH Editora e Distribuidora, 2009.

PAIVA, Luciano Carneiro de Paiva. **A prova nos crimes de informática**. Aspectos Técnicos e Jurídicos. Dissertação, 2006.

PENAL, **A Lei de Introdução ao Código**, Decreto-Lei Nº 3.914, de 09 de dez de 1941. Disponível em <http://www.planalto.gov.br/ccivil/Decreto-Lei/Del3914.htm>.
Acessado em 12 de set. de 2009.

PENAL, **Código**. Decreto-Lei N.º 2.848, De 7 de dez de 1940.
Disponível em <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>.
Acessado em 18 de set. de 2009.

PENAL, **Código de Processo**. Decreto-Lei N.º 3.689, de 3 de Out de 1941. Disponível em <http:// www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm>.
Acessado em 22 de set. de 2009.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva. 2008.

PINHEIRO, Patrícia Peck. **Espionagem Eletrônica**. São Paulo: 09 de set de 2008.
Disponível em < http://www.pppadvogados.com.br>
Acessado em 07 de nov. de 2009.

RODRIGUES, Fernando. **Hackers invadem site do governo, praticam extorsão e podem até apagar luzes de várias cidades no Brasil**. São Paulo: 08 de Nov de 2009.
Disponível em < http://www1.folha.uol.com.br/fsp/dinheiro/fi0811200903.htm >
Acessado em 08 de Nov. de 2009

SAWAYA, Márcia Regina. **Dicionário de Informática e Internet**. São Paulo: Editora Nobel, 1999.

TANENBAUM, Andrew S. **Redes de Computadores**, São Paulo: Editora Campus, 2003.

TORRES, Gabriel. **Redes de Computadores – Curso Completo**, Rio de Janeiro: Editora Axcel Books do Brasil, 2001.

ANEXO A – PROJETO DE LEI 94/99

SUBSTITUTIVO ao PLS 76/2000, PLS 137/2000 e PLC 89/2003

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências."

O CONGRESSO NACIONAL decreta:

Art.1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Título VIII da Parte Especial do Código Penal fica acrescido do Capítulo IV, assim redigido:

Capítulo IV

DOS CRIMES CONTRA A SEGURANÇA

DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado:

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Ação Penal

Art. 285-C. Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias."

Art. 3º O Título I da Parte Especial do Código Penal fica acrescido do seguinte artigo, assim redigido:

Divulgação ou utilização indevida de informações e dados pessoais:

154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena - detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte."

Art. 4º O caput do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

Dano

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:

Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

"Inserção ou difusão de código malicioso

Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena - reclusão, de 2(dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."

Art. 6º O art. 171 do Código Penal passa a vigorar acrescido dos seguintes dispositivos:

"Art. 171.....

§ 2º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VII - difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado:

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do § 2º deste artigo, a pena é aumentada de sexta parte."

Art. 7º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

"Atentado contra a segurança de serviço de utilidade pública

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:

..... "(NR)

Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores,

de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:

..... "(NR)

Art. 8º O caput do art. 297 do Código Penal passa a vigorar com a seguinte redação:

Falsificação de dado eletrônico oudocumento público

Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento publico verdadeiro:

....."(NR)

Art. 9º O caput do art. 298 do Código Penal passa a vigorar com a seguinte redação:

"Falsificação de dado eletrônico ou documento particular

Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro:

....."(NR)

Art. 10. O art. 251do Capítulo IV do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar),passa a vigorar acrescido do inciso VIao seu § 1º, e do § 4º, com a seguinte redação:

"Art. 251. .....

§ 1º - Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VI - Difunde, por qualquer meio, código malicioso com o intuito de facilitar ou permitir o acesso indevido a rede de computadores, dispositivo de comunicação ou a sistema informatizado, em prejuízo da administração militar

.....

§ 4º - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte."

Art. 11. O caput do art. 259 e o caput do art. 262 do Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

Dano Simples

Art. 259. Destruir, inutilizar, deteriorar ou faze desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar:"(NR)

.....

.....

Dano em material ou aparelhamento de guerra ou dado eletrônico

Art. 262. Praticar dano em material ou aparelhamento de guerra ou dado eletrônico de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas:(NR)

Art. 12. O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 262-A, assim redigido:

Inserção ou difusão de código malicioso

Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte."

Art. 13. O Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VII-A, assim redigido:

"Capítulo VII-A

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 339-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 339-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível, desde que o fato atente contra a administração militar:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

"Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena - detenção, de um a dois anos, e multa.

Parágrafo único - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de crime, a pena é aumentada da sexta parte."

Art. 14. O caput do art. 311 do Capítulo V do Título VII do Livro I da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

Falsificação de documento

Art. 311. Falsificar, no todo ou em parte, documento público ou particular, ou dado eletrônico ou alterar documento verdadeiro, desde que o fato atente contra a administração ou o serviço militar:"(NR)

Art. 15. Os incisos II e III do art. 356 do Capítulo I do Título I do Livro II da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

"CAPÍTULO I

DA TRAIÇÃO

Favor ao inimigo

Art. 356. .....:

.....

II - entregando ao inimigo ou expondo a perigo dessa conseqüência navio, aeronave, fôrça ou posição, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar."(NR)

Art. 16. Para os efeitos penais considera-se, dentre outros:

I - dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

II - sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III - rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

IV - código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;

V - dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

VI - dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de

uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Art. 17. Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado.

Art. 18. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 19. O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20 .....

.....

§ 3º.....

II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.

..... "(NR)

Art. 20. O caput do art. 241 da Lei nº 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:

"Art. 241. Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:

..... "(NR)

Art. 21. O art. 1º da Lei nº 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

"Art. 1º .....

.....

V - os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado.

....."(NR)

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

I - manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

II - preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III - informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.

§ 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.

§ 2º O responsável citado no caput deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Art. 23. Esta Lei entrará em vigor cento e vinte dias após a data de sua publicação."

ANEXO B – MANUAL DO MINISTÉRIO PÚBLICO FEDERAL

MINISTÉRIO PÚBLICO FEDERAL

Crimes de Informática

coletando e analisando evidências

Índice

1 Objetivo do manual
2 A importância e as dificuldades de se obter evidências em crimes de informática
3 Como fazer uma denúncia?
4 Sites na Internet
4.1 Evidências necessárias
4.1.1 Impressão do site (mínimo desejável)
4.1.2 Salvando o conteúdo inteiro do site (recomendável)
4.1.3 Salvando e garantindo a integridade dos dados (procedimento ideal)
4.2 Pesquisa de domínios, localizando o responsável por um site
4.2.1 Domínios nacionais (.br)
4.2.2 Domínios estrangeiros
5 E-mails
5.1 Evidências necessárias
5.2 Localizando o cabeçalho do e-mail
5.3 Analisando o cabeçalho de e-mail
5.4 Localizando o "dono" de um IP
5.5 Localizando o dono de um e-mail
6 Softwares P2P – ponto a ponto (Kazaa, E-Mule, E-Donkey, etc)
6.1 Anonimidade dos softwares "ponto a ponto"
7 Mensagens Instantâneas (ICQ, MSN Messenger, Yahoo, etc)
7.1 Evidências necessárias
7.2 Identificações de alguns "Instant Messengers"
7.3 Localizando o "dono" de um instant messenger
8 Chats (reuniões virtuais)
8.1 Evidências necessárias
8.2 Chats que permitem troca de imagens
8.3 Localizando o responsável por uma mensagem num chat
9 Listas de discussões
10 Colaboradores
11 Bibliografia e links

Apêndice A – Censura na Internet – como e onde é feita
Apêndice B – Censura na Internet – porque ela não é efetiva
Apêndice C – Crimes de computador – panorama no Brasil

1 Objetivo do manual

Todos os dias somos testemunhas do alcance da Internet.
Cyber-Cafes, LanHouses, telecentros, escolas informatizados, acessos gratuitos, conexões rápidas domiciliares exemplificam algumas formas que um indivíduo pode se conectar ao mundo digital.

Na mesma proporção que a Internet distribui benefícios e facilidades, ela cria um meio quase que anônimo para a prática de novos crimes, que por utilizarem técnicas que envolvem conhecimento no campo de Tecnologia de Informação, acabam confundindo vítimas e responsáveis por punições.

Este manual tem dois objetivos, o primeiro é auxiliar as pessoas que efetuam denúncias de crimes utilizando tecnologias de informática, indicando os procedimentos mínimos para se coletar provas, manter sua integridade e encaminhar para que órgãos competentes possam efetivar e analisar a denúncia.

O segundo objetivo é fornecer informações aos analistas, técnicos, peritos ou responsáveis que recebem estes tipos de denúncias, auxiliando nas primeiras análises que podem ser feitas nestas provas, com o intuito de agilizar o andamento do processo.

O tema "crimes de informática" é extremamente extenso em virtude das novas tecnologias que surgem todos os dias, com isso nos detemos a focar uma pequena parte dos crimes de informática como pedofilia em sites, trocas de arquivos, mensagens em correio eletrônico, listas de discussão, aplicativos P2P, chats e instant messengers que são os casos mais comuns que chegam através de denúncias ao Ministério Público Federal.

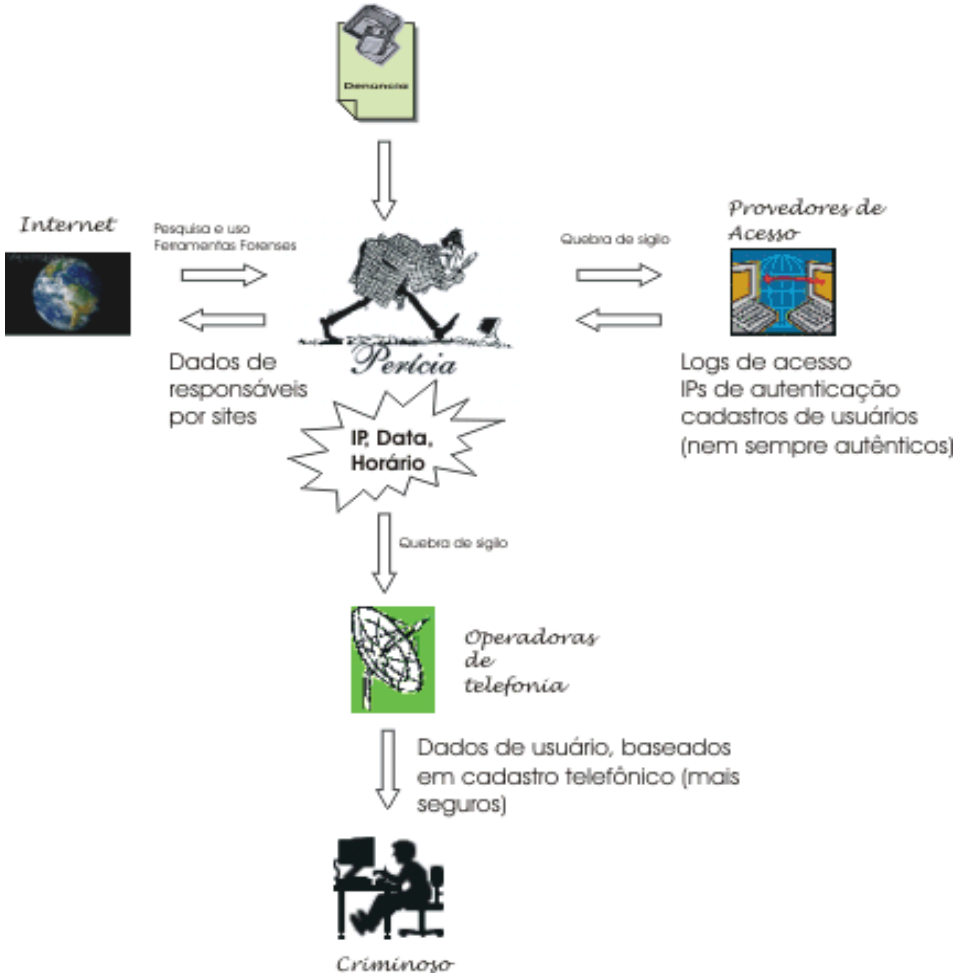
Uma versão atualizada e online deste manual estará disponível em:
http://intranet.prsp.mpf.gov.br
Serviços – Manuais – ítem 17 Crimes de Informática

2 A importância e as dificuldades de se obter evidências em crimes de informática

As evidências ou provas de crimes de informática, caracterizam-se por possuir um formato complexo (arquivos, fotos, computadores, dados digitalizados, etc), serem voláteis (podem ser apagadas, alteradas ou perdidas facilmente) e costumam estar misturadas em meio de uma grande quantidade de dados legítimos, requerendo uma análise mais apurada pelos responsáveis pela denúncia.

Uma das principais evidências que pode ser coletadas, em meio aos dados de uma denúncia é o chamado número IP (Internet Protocol). O número IP é uma identificação que todos os computadores que acessam a Internet possuem e aparece na forma A.B.C.D, onde A, B, C e D são números que variam de 0 a 255 (exemplo 200.158.4.65).

O número IP, acompanhado de data e horário de uma conexão podem levar a identificação de um criminoso.



3 Como fazer uma denúncia?

Via Internet
Ministério Público Federal – PR/SP
http://www.prsp.mpf.gov.br
Digi - Denúncia
A denúncia será considerada ANÔNIMA, caso os dados cadastrais não forem preenchidos.

Via E-mail
denuncia@prsp.mpf.gov.br
O remetente é identificado.

Pessoalmente
Ministério Público Federal
Setor: Coordenadoria Jurídica
R.Peixoto Gomide, 768
Cep: 01409-904 São Paulo
Telefone: 11-3269-5000

Disk-Denúncia
Ministério Público Federal
Telefone: 11-3253-7800

4 Sites na Internet

4.1 Evidências necessárias

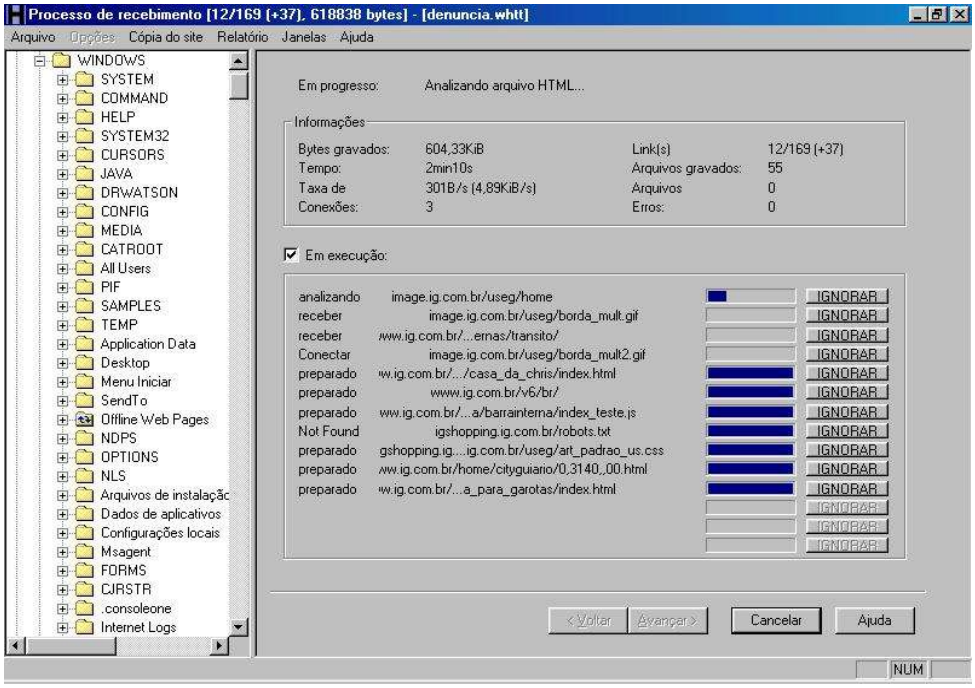
Endereço e impressão do site.

4.1.1 Impressão do site (mínimo desejável)

Infelizmente muitas denúncias chegam ao Ministério Público Federal contendo somente o endereço do site. Com a dinâmica da Internet e as vezes com a própria ação dos provedores que detectam o crime e retiram o site do ar, fica impossível dar andamento a uma denúncia se não for feito no mínimo uma impressão do site, mostrando de maneira clara o objeto da denúncia (foto, texto, diálogo, etc)

4.1.2 Salvando o conteúdo inteiro do site (recomendável)

Existem aplicativos que permitem o download de sites inteiros, incluindo textos e fotos publicadas. Utilizar estes aplicativos é um artifício interessante para casos onde o volume de dados é grande.
Após o download, os arquivos podem ser encaminhados para o órgão competente através de e-mails, disquetes e se possível em mídia não-regravável (CD-R).
Abaixo uma tela do software HTTrack[1] fazendo o download de um site:



O HTTrack, além de permitir o download parcial ou total do site, gera um arquivo de log (hts_log) registrando a data, hora e endereço do site salvo.

[1] ***HTTrack WebSite Copier 3.30 (licença GPL – gratuito) Download: http://www.httrack.com***

4.1.3 Salvando e garantindo a integridade dos dados (procedimento ideal)

Durante o andamento de um processo, a veracidade das evidências podem ser postas a prova diversas vezes. Para evitar este tipo de problema, nos casos onde não é possível gravar os arquivos em mídia não-regravável, é importante a utilização de um aplicativo que garanta a integridade dos dados.

O MD5Sum[2] é um aplicativo de verificação de integridade, na prática ele garante que os dados (provas) que foram gravados no momento da denúncia, não sofreram nenhum tipo de adulteração em todo o trâmite do processo.

Tecnicamente, ao criarmos uma cópia de algum arquivo, criamos também sua assinatura baseada no arquivo original. Esta assinatura, em forma de um arquivo, acompanhará a cópia e permitirá que a qualquer momento o destinatário verifique se o arquivo recebido é idêntico ao original.

Como utilizar o MD5Sum?

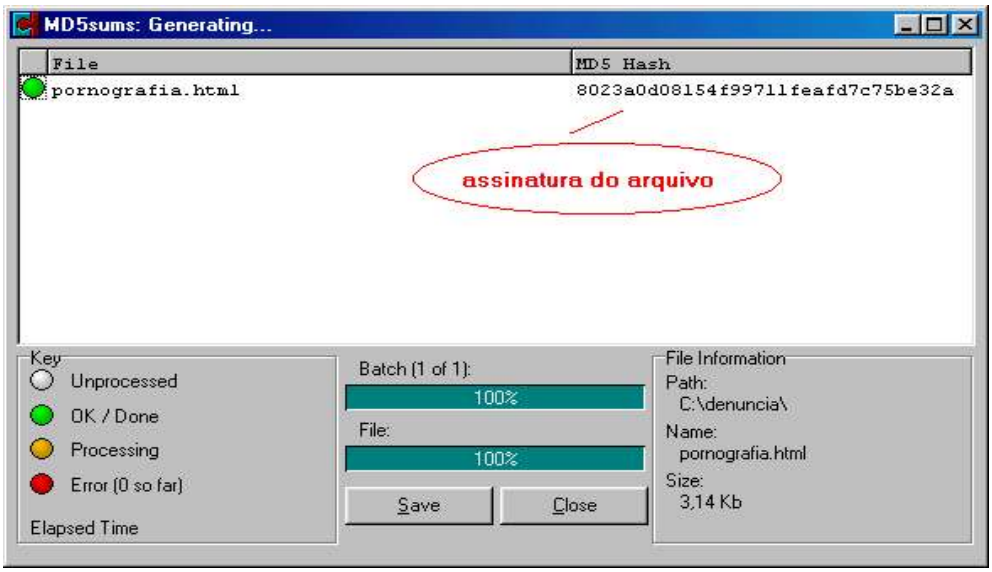
- Compacte seus arquivos para gerar somente um arquivo .ZIP (é mais fácil gerar a assinatura de um só arquivo do que de todos).

- Rode o programa MD5Sum para esta cópia gerada.

- Mande a cópia de seu arquivo zipado, junto com este arquivo adicional criado (assinatura) com extensão .MD5

- Com este arquivo (assinatura) o receptor de seu arquivo poderá a qualquer momento rodar o md5sum no arquivo recebido e comparar as assinaturas, se forem iguais, o arquivo é autêntico.

Abaixo uma tela do MD5Sum criando uma assinatura de um arquivo:

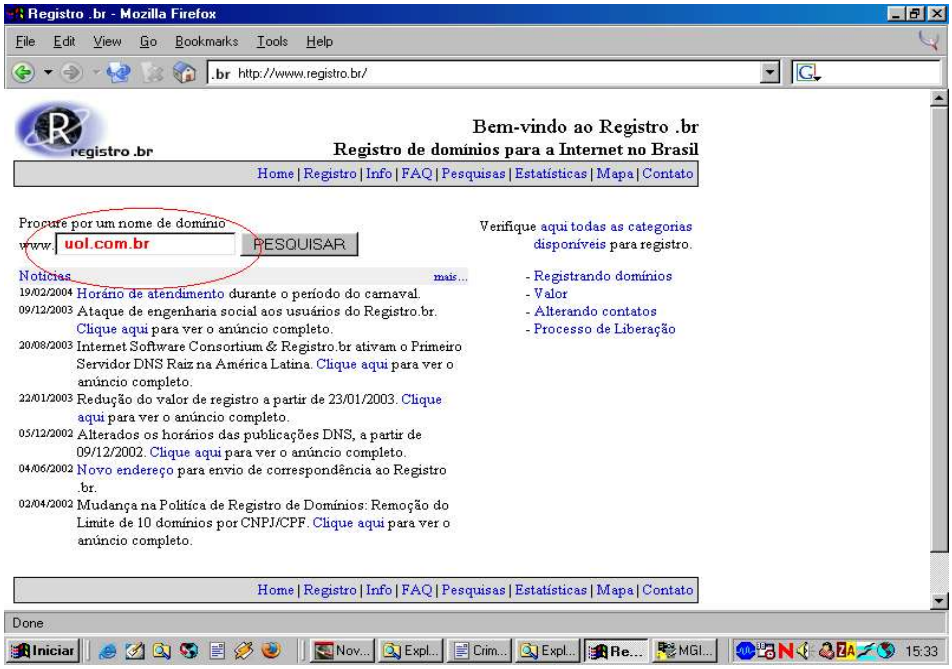


[2] ***MD5Summer 1.2.0.5 (licença GPL - gratuito) download: htpp://www.md5summer.org***

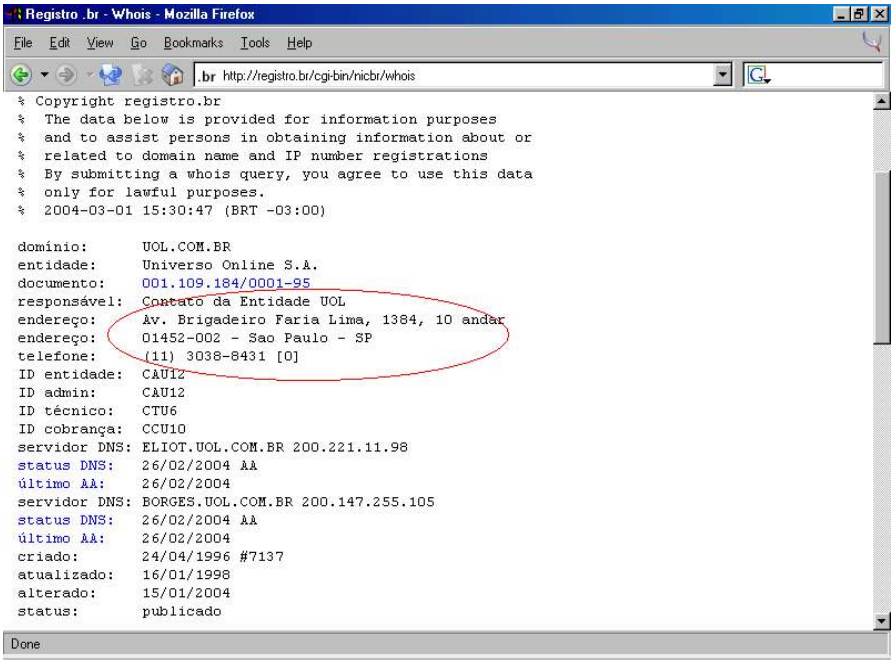
4.2 Pesquisa de domínios, localizando o responsável por um site

4.2.1 Domínios nacionais (.br)

Os sites que ficam sobre a administração da FAPESP são facilmente identificados pela terminação ".br" e podem ser pesquisados pelo site do http://www.registro.br

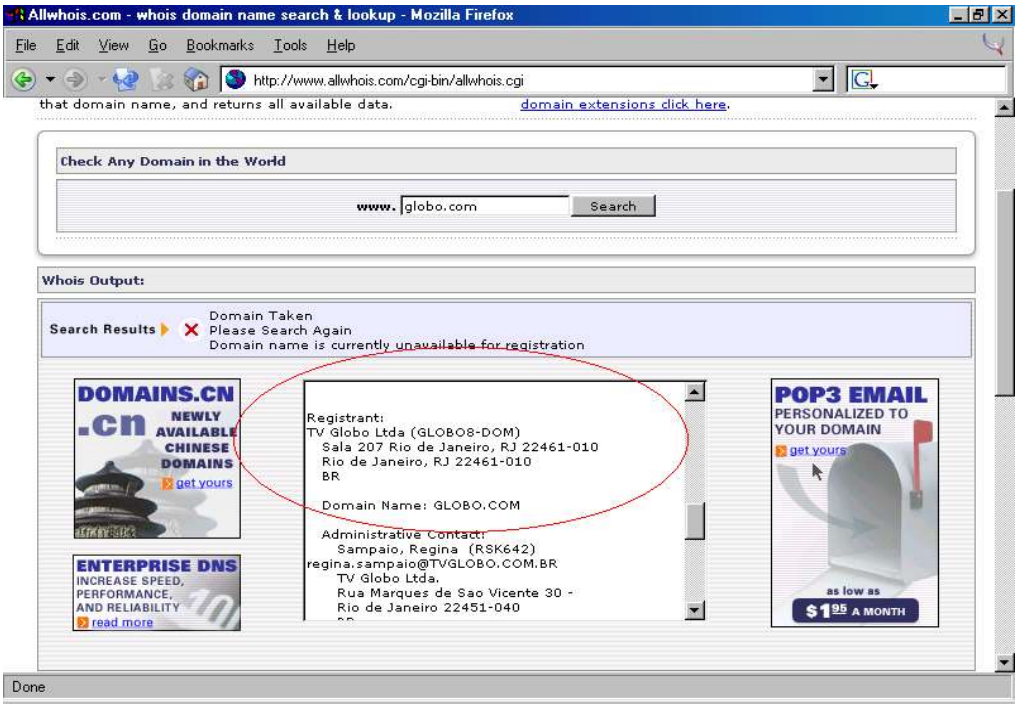


O resultado desta pesquisa pode trazer informações importantes como Responsável Administrativo pelo domínio, Contato de Incidentes de Segurança e o Provedor de Backbone (empresa que detêm blocos de endereços IP´s).
Abaixo uma tela contendo o resultado de pesquisa de um site.


Registro .br - Whois - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
.br http://registro.br/cgi-bin/nicbr/whois
% Copyright registro.br
% The data below is provided for information purposes
% and to assist persons in obtaining information about or
% related to domain name and IP number registrations
% By submitting a whois query, you agree to use this data
% only for lawful purposes.
% 2004-03-01 15:30:47 (BRT -03:00)
domínio: UOL.COM.BR
entidade: Universo Online S.A.
documento: 001.109.184/0001-95
responsável: Contato da Entidade UOL
endereço: Av. Brigadeiro Faria Lima, 1384, 10 andar
endereço: 01452-002 - Sao Paulo - SP
telefone: (11) 3038-8431 [O]
ID entidade: CAU12
ID admin: CAU12
ID técnico: CTU6
ID cobrança: CCU10
servidor DNS: ELIOT.UOL.COM.BR 200.221.11.98
status DNS: 26/02/2004 AA
último AA: 26/02/2004
servidor DNS: BORGES.UOL.COM.BR 200.147.255.105
status DNS: 26/02/2004 AA
último AA: 26/02/2004
criado: 24/04/1996 #7137
atualizado: 16/01/1998
alterado: 15/01/2004
status: publicado
Done

4.2.2 Domínios estrangeiros

A pesquisa de sites estrangeiros pode ser feita por diversos serviços de WHOIS como no endereço http://www.allwhois.com ou http://www.thebigwhois.com
Veja abaixo um resultado de busca neste WHOIS:



Sites que estão sob a responsabilidade de um provedor de outro país, terão a denúncia encaminhada para um órgão que possa intermediar esta pesquisa, através do Ministério Público Federal.

Dica:
Alguns sites, mesmo publicados em provedores externos, trazem links do tipo “contato”, “webmaster” que mostram o endereço de algum e-mail. Vale a pena pesquisar este e-mail, pois as vezes ele pode indicar algum responsável pelo conteúdo do site.

5 E-mails

5.1 Evidências necessárias

Além da mensagem (impressa ou salva), é de extrema importância que seja enviado o cabeçalho do e-mail. Com a disseminação de vírus, que alteram o remente de e-mails, e com a falha de diversos aplicativos de e-mails que permitem o preenchimento do campo "de" (remetente) sem autenticação, nem sempre o endereço que consta no campo remetente, realmente mostra o verdadeiro autor da mensagem.
Com isto, fica caracterizada a importância do cabeçalho de e-mail numa denúncia que envolva algum tipo correio eletrônico.

5.2 Localizando o cabeçalho do e-mail

Em aplicativos como o Outlook ou Outlook Express o cabeçalho de um e-mail pode ser acessado abrindo a mensagem, clicando em Alt+Enter – Detalhes.
No groupwise (aplicativo utilizado no MPF), podemos localizar o cabeçalho de um e-mail abrindo a mensagem e clicando no Menu Arquivo – Anexos – Ver . Selecione o arquivo MIME.822.

5.3 Analisando o cabeçalho de e-mail

A análise do cabeçalho de um e-mail é bastante complexa e é dela que iremos obter pistas de como localizar o remetente de uma mensagem.
Observe que nela podemos (ou não) ter diversas linhas que começam com a palavra "received" que indicam por quantas estações (ou servidores) a mensagem passou. O parágrafo que nos interessa sempre será o **último received**, que mostra a primeira máquina que originou a mensagem ou seja, a máquina do remetente. (os received estão em ordem decrescente, ou seja, o primeiro received mostrará a máquina mais recente que sua mensagem atravessou).

Abaixo um exemplo de cabeçalho de e-mail com endereço falso (típico de estação infectada com vírus), mas contendo o IP verdadeiro do remetente, observe também a data e o horário (incluindo o fuso horário) que o email foi encaminhado:

```
Received: from [pppp.mmm.gov.br
        ([200.158.14.238])
        by pprr.mmm.gov.br; Wed, 03 Mar 2004 07:49:53 -0300
From: pjfkdjkgab@jfpp.gov.br
To: fulano@pppp.mmm.gov.br
Subject: Re: Your archive
Date: Wed, 3 Mar 2004 07:46:27 -0300
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0003_000052ED.00002596"
X-Priority: 3
X-MSMail-Priority: Normal

This is a multi-part message in MIME format.

------=_NextPart_000_0003_000052ED.00002596
Content-Type: text/plain;
        charset="Windows-1252"
Content-Transfer-Encoding: 7bit
```

Abaixo um outro cabeçalho de e-mail que mostra o endereço de e-mail, a data e o horário (incluso o fuso horário):

```
Received: from mpp.gov.br
        (rubi.mpp.gov.br [200.148.51.26])
        by ppppp.pppr.mpp.gov.br; Mon, 08 Mar 2004 21:17:35
-0300
Received: (qmail 3295 invoked by uid 306); 9 Mar 2004
00:15:46 -0000
Received: from direto@mkt.navio.com.br by rubi by uid 303 with
qmail-scanner-1.20
 ( Clear:RC:0(200.184.163.136):.
 Processed in 0.035505 secs); 09 Mar 2004 00:15:46 -0000
Received: from unknown (HELO mkt3.site.br.navio)
(200.184.163.136)
  by rubi.mpp.gov.br with SMTP; 9 Mar 2004 00:15:46 -0000
Received: from mkt3 ([172.26.0.243]) by mkt3.site.br.navio with
Microsoft SMTPSVC(5.0.2195.6713);
         Mon, 8 Mar 2004 21:24:29 -0300
From:    navio Direto <direto@mkt.navio.com.br>
To:      maria <maria@pppr.mpp.gov.br>
Date: Tue, 09 Mar 2004 00:24:28 GMT
Organization: navio
X-MSMail-Priority: Normal
X-mailer: AspMail 4.0 4.03 (SMT4D9FD2F)
```

5.4 Localizando o "dono" de um IP

O IP (Internet Protocol) é uma identificação que todos que acessam a Internet devem possuir. Eles podem ser estáticos (pertencerem a uma mesma pessoa por um período de tempo) ou dinâmicos (mudarem toda vez que o acesso é feito).

IPs dinâmicos são bastante comuns e as únicas entidades que podem informar (seguramente) quem usava um IP, num determinado dia e horário, são as operadoras de telefonia a quem estes IP´s pertencem.

Para localizar o dono de um IP é necessário fazer uma pesquisa nos mesmos sites que pesquisamos os

domínios (ítem 4.2.1 e 4.2.2), mudando somente a entrada do dado, ao invés de ser um domínio, agora será um endereço IP.
Outro site que possui diversas ferramentas para a localização de responsáveis por um IP é o http://www.network-tools.com

Localizado o provedor ou a operadora, o MPF encaminha uma ordem judicial solicitando uma quebra de sigilo aos mesmos, contendo IP, data e hora (com fuso horário), obtidos no cabeçalho de e-mail e solicita dados do usuário ou telefone para se chegar na identificação do remetente da mensagem.
Se for constatado que o provedor não está no Brasil, o MPF encaminha esta solicitação para um órgão intermediador.

Anonimidade dos Cyber-Cafés e LanHouses

(fonte: http://www.infojus.com.br)

A Prefeita Marta Suplicy sancionou a Lei Municipal nº 13.720, de 09-01-2004, que regulamenta as atividades de empresas de locação de máquinas e jogos de computador, também conhecidos como "cyber-cafés" ou "lan houses", na Cidade de São Paulo. Além de exigir que todos os estabelecimentos que explorem esse tipo de atividade sejam registrados como contribuintes do ISS (art. 2o.), a Lei também exige que possuam cadastro dos menores de 18 anos que freqüentam o local, com dados como nome, data de nascimento, filiação, endereço, telefone e documentos.

Parece que nossas autoridades ainda não enxergaram o imenso perigo que constitui o funcionamento de "cyber-cafés" sem qualquer tipo de controle. Utilizando um terminal de acesso público à Internet, uma pessoa pode praticar uma série de crimes, desde um simples *spam* até coisas mais graves como difamação, extorsão, chantagem, ameaça, fraudes de cartões de crédito, acesso não autorizado a sistemas informáticos e disseminação de pornografia infantil(2), só para citar alguns. Se nesses estabelecimentos não se exige identificação dos usuários, as pessoas podem praticar esses crimes sob completo anonimato.

Tem-se dito que a Internet favorece o crime porque facilita o anonimato, mas hoje o anonimato na rede só é conseguido por pessoas que têm sofisticados conhecimentos de comunicações telemáticas (os *hackers*). A navegação das pessoas comuns pode ser facilmente rastreada. A disponibilização de "cyber-cafés" sem qualquer controle inverte essa lógica, possibilitando que qualquer pessoa, mesmo aquela sem conhecimentos técnicos sofisticados, possa praticar crimes sem qualquer receio de ser descoberta. De fato, qualquer um pode ir a um local desses, que hoje são encontrados em todas as grandes cidades do Brasil(3), cometer crimes como difamação e ameaça (por *e-mail*, p. ex.), e sair tranqüilamente da mesma forma que entrou. É preciso, portanto, que as autoridades brasileiras (mesmo a nível federal) desenvolvam algum tipo de política de segurança para esses estabelecimentos.

5.5 Localizando o dono de um e-mail

Se ao analisar o cabeçalho do e-mail, não localizamos o IP que originou a mensagem, mas localizamos o e-mail, o MPF, através de uma ordem judicial, pode solicitar uma quebra de sigilo ao provedor. Nesta pesquisa deve ser solicitado o IP da máquina que autenticou esta conta, na data e horário do e-mail. É importante que nesta solicitação conste o fuso horário que também pode ser obtido no cabeçalho do e-mail.

Lembrando que para localizar o endereço ou o contato de um provedor do e-mail, usa-se o mesmo procedimento de pesquisa dos ítens (4.2.1 e 4.2.2) e se for constatado que o provedor não está no Brasil é necessário encaminhar esta solicitação para um órgão intermediador.

Posteriormente, quando localizados o IP que autenticou o e-mail no provedor, repete-se a pesquisa para localizar o dono do IP (operadora de telefonia) e solicita-se judicialmente, dados do usuário que usava este IP no dia e horário do e-mail, chegando ao remetente.

Logs em provedores de acesso x legislação

Os provedores de acesso mantêm arquivos com o registro (log) de todas as solicitações que recebem. Esse documento permite analisar itens como a procedência do usuário, a frequência com que retornam ao site e seus hábitos de navegação dentro do site.

Na prática observa-se que nem todos os provedores de acesso possuem arquivos de logs (ou os mantém por pouco tempo) que são essenciais para localizar dados de criminosos. Um outro problema observado, é que os provedores nem sempre possuem cadastros de usuários com informações válidas; geralmente contas de e-mails ficam "amarradas" a cadastros com dados falsos ou incompletos.

O Comitê Gestor de Internet no Brasil possui Recomendações que orientam: "fornecedores de meios de acesso (telefonia, cabos e outros), reservem, para o serviço de provimento de acesso, centrais que permitam a identificação inequívoca da origem da chamada, de modo que os provedores de acesso à Internet possam identificar sua origem".

Esta regulamentação está válida e sendo aplicada somente nas Operadoras de Telefonia, inclusive as mesmas mantém logs de acesso por até 5 anos.

É por esta razão que o rastreamento de um usuário quase sempre acaba com a pesquisa nestes logs **de Operadores de Telefonia** que possuem dados mais confiáveis do que os provedores de acesso.

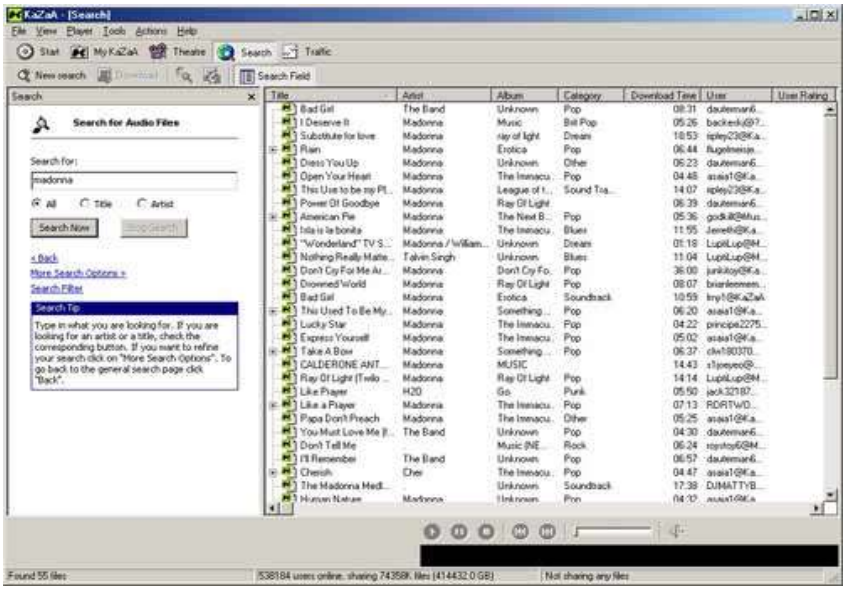
6 Softwares P2P – ponto a ponto (Kazaa, E-Mule, E-Donkey, etc)

6.1 Anonimidade dos softwares "ponto a ponto"

As conexões chamadas "P2P" são caracterizados por não possuir um provedor central da conexão (utilizam diversos servidores independentes e espalhados na Internet). Os arquivos ficam localizados nas estações dos usuários que participam desta "rede" e os servidores independentes somente fornecem uma "ponte" entre a pessoa que disponibiliza o arquivo e quem o quer.
Este estrutura garante a anonimidade e a troca de arquivos é gerada quase sem a criação de logs, nem identificação das estações que efetuam esta troca.
Alguns aplicativos que utilizam esta tecnologia: Kazaa, GnuTella, e-Donkey, AudioGalaxy, Morpheus, BitTorrent e outros

Quando um usuário, de alguns destes softwares, entram neste tipo de "rede", se autenticam num servidor e passam a usufruir dos benefícios deste serviço.
Esta autenticação geralmente é feita em servidores gerenciados por comunidades anônimas, inclusive em países onde não existem legislações rígidas para uso de Internet. Os arquivos de logs gerados, por serem imensos, não são armazenados.
Na prática, se um servidor P2P é fechado, no dia seguinte aparecem outros 2 em qualquer outra parte do mundo.

Abaixo uma tela do software KAZAA, disponibilizando e procurando novos arquivos:



Infelizmente o rastreamento de alguma troca de arquivos entre estes sistemas é bastante difícil e estamos estudando uma maneira de normatizar algum procedimento para este tipo de análise.

Novas versões do Kazaa impedem rastreamento

Novas versões independentes do Kazaa, software de compartilhamento de arquivos, impedem o rastreamento de seus downloads.

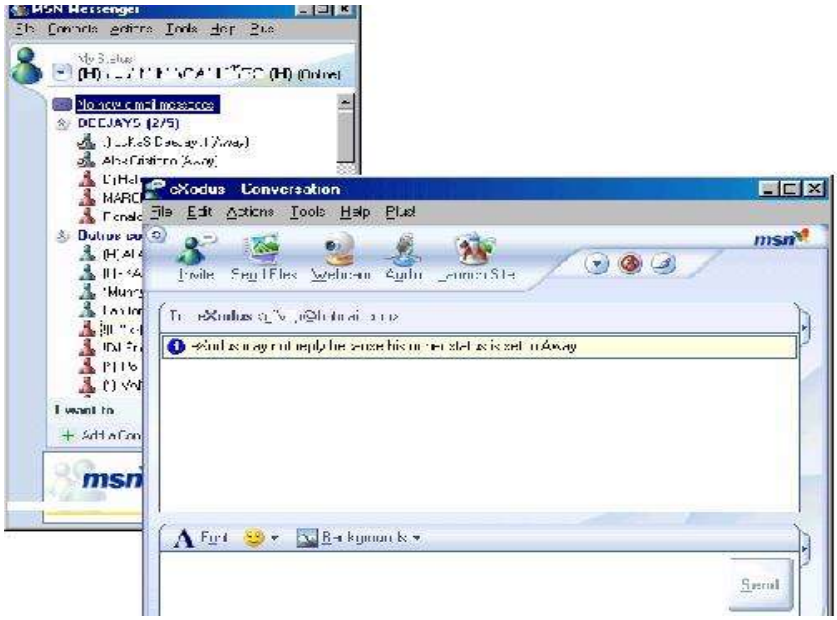
As versões são o Kazaa Lite 2.4.0 e o Kazaa K+++ 2.4.0 e prometem bloquear qualquer tipo de tentativa de rastreamento de seus downloads.

Os autores criaram opções para desabilitar funções que permitem que um usuário veja todos os arquivos pertencentes a outros, sem contar que não salvam o histórico das pesquisas realizadas.

7 Mensagens Instantâneas (ICQ, MSN Messenger, Yahoo, etc)

7.1 Evidências necessárias

Softwares de mensagens instantâneas são bastante populares, e os mais conhecidos são ICQ, MSN Messenger e Yahoo Messenger.
No caso de uma denúncia, é importante imprimir (ou salvar) o conteúdo da mensagem, dados do usuários (números identificadores-UIN, apelidos ou e-mail), data e horário que ocorreu o ato criminoso.
Abaixo uma tela do MSN Messenger com uma tela de chat (conversa) aberta:



7.2 Identificações de alguns "Instant Messengers"

ICQ (AOL – Mirabilis) – utiliza o chamado UIN (Univeral Internet Number) para se autenticar na rede MSN Messenger e Yahoo Messenger – Utiliza um e-mail para fazer a autenticação.

7.3 Localizando o "dono" de um instant messenger

De posse do UIN (ou do e-mail de autenticação) é necessário entrar em contato com o provedor (Mirabilis.com , AOL.com, Msn.com, etc) e solicitar o IP usado na data e horário anotados.

Com o IP em mãos, localiza-se o provedor (ou operadora de telefonia) e solicita-se os dados do usuário.

8 Chats (reuniões virtuais)

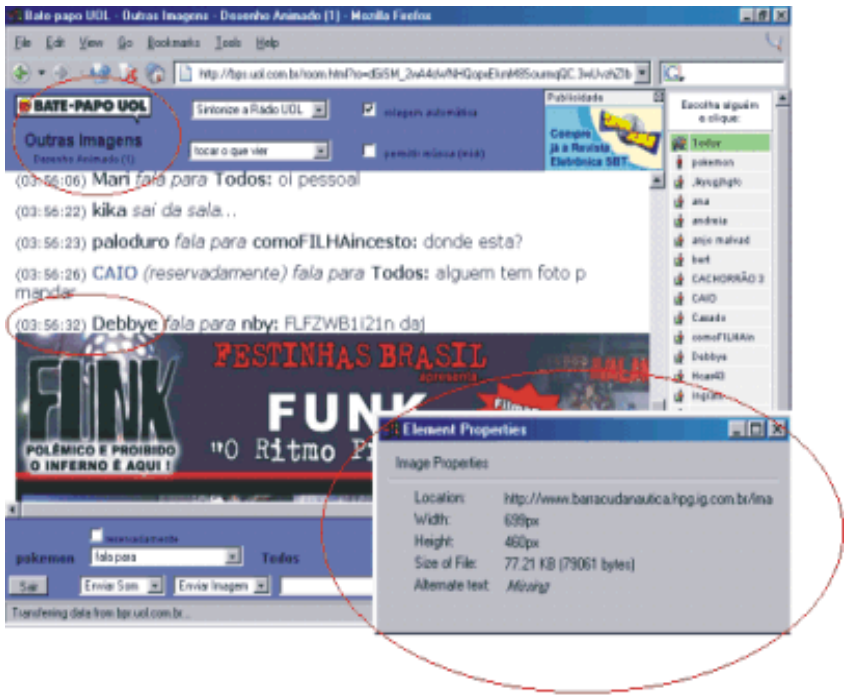
8.1 Evidências necessárias

Além de salvar o conteúdo de uma conversa (ou imprimir) é importante anotar todos os dados possíveis sobre o chat, como site onde o serviço funciona, nome de sala, nicknames usados, data e hora que se realizou a conversa.

8.2 Chats que permitem troca de imagens

Além dos dados relacionados acima, podemos observar que diversos chats permitem a troca de imagens. Um dado adicional que podemos coletar neste tipo de denúncia é capturado simplesmente com o botão invertido do mouse sobre a imagem e escolhendo a opção propriedades.
Imprima (ou salve) esta tela e junte com os outros dados da denúncia.

Veja uma tela que contém os dados de uma imagem trocada num chat:



8.3 Localizando o responsável por uma mensagem num chat

Alguns provedores possuem logs de chats baseados no "nickname" utilizado. De posse do nickname, data e horário que se realizou a conversa virtual, solicitar ao provedor o IP utilizado. Com o IP é necessário localizar a operadora de telefonia e solicitar dados do usuário.

9 Listas de discussões

Basicamente as listas de discussões utilizam o e-mail para troca de mensagens e neste caso podemos utilizar os mesmos procedimentos para rastrear um e-mail, visto no item 5.

NewsGroups – uma lista de discussão diferente

(fonte: http://www.apfn.com.pt/Noticias/Fev2003/pedofilia.htm **)**

Os "newsgroups" - grupos de discussão sobre um determinado tema - são os veículos por excelência da troca de conteúdos de pornografia infantil. Mediante o pagamento de uma mensalidade a partir de 14,95 dólares (13,8 euros), o servidor Usenet, por exemplo, coloca à disposição do usuário cerca de 80 mil grupos de discussão sobre os mais variados temas, onde qualquer pessoa poderá ceder, visualizar, descarregar e trocar conteúdos de pornografia infantil. Mas a troca de arquivos nos "newsgroups" também funciona de forma distinta: os arquivos são apresentados em forma de texto para depois serem decodificados pelos receptores, o que implica uma vontade manifesta para visualizar a imagem.
Como todos os conteúdos da Internet circulam ou gratuitamente ou mediante pagamento, os "newsgroups" também não fogem a esta lógica, mas na grande maioria dos casos é necessário passar por um processo de subscrição e manifestar o desejo de partilhar os seus conteúdos, sejam ilegais ou não

Os *newsgroups* distinguem-se das listas de discussão pelo seu modelo de distribuição. As mensagens das listas são trocadas através de correio eletrônico, enquanto que o *newsgroups* tem um caráter institucional no sentido que é recebido e armazenado em um servidor, ao qual os usuário devem ter acesso. A escolha das categorias de notícias também é de responsabilidade da instituição. Várias listas de discussão reproduzem as mensagens de *newsgroups* correlatos.

Os *newsgroups* são organizados de acordo com suas áreas de concentração específicas. Como os grupos compõem uma estrutura de árvore, as várias áreas são chamadas de "hierarquias". Os nomes dos newsgroups incluem várias partes separadas por pontos. A primeira indica a hierarquia, depois vem o tópico que por sua vez pode ser desmembrado em vários

.

10 Sugestões e críticas:

Ministério Público Federal
??????

Departamento da Polícia Federal
?????

11 Bibliografia e links

-Análise Forense de Instruções em Sistemas Computacionais
Marcelo Abdala dos Reis e Paulo Lício de Geus

-Privacidade na Internet - Uma abordagem integrada da UE no domínio da proteção de dados em linha
Artigo 29 – Grupo de Proteção de Dados Pessoais - Portugal

-Padrão "ACME" para análise forense de instruções em Sistemas Computacionais
Cesar Eduardo Atilio

-Perícia Forense aplicado a Informática
Andrey Rodrigues de Freitas

- Atacantes: suas principais técnicas e ferramentas
Vinicius Serafim

http://www.nbso.nic.br/docs/palestras/

http://www.ibdi.org.br
Instituto Brasileiro de Política e Direito da Informática

Lista de Discussão – Perícia Forense
http://br.groups.yahoo.com/group/PericiaForense/

Fundamentos de Direito Penal Informático: do acesso não autorizado a sistemas computacionais.
Tulio Vianna - Rio de Janeiro: Forense, 2003. 170 p.

Direito & Internet
Newton de Lucca – Adalberto Simão Filho

Dialética do Ciberspaço – Trabalho, Tecnologia e Política no Capitalismo Global (Capítulo 1)
Giovanni Alves – Vinicio Martinez

http://www.google.com

Apêndice A

Censura na Internet – como e onde é feita

Ao contrário das democracias ocidentais, alguns governos possuem controles bastante rígidos sobre o conteúdo de internet que circulam em seus países, ora restringindo o acesso de PC´s da população, ora estatizando e implantando verdadeiros filtros de acessos a conexões para a Internet.
Já existem casos listados de 45 países que fazem este tipo de censura, fomentando a revolta e a liberdade de expressão no chamado Cyberspaço.

CUBA: Possui 4 provedores de acesso que tem como saída um único gateway que é controlado pelo governo. Os filtros são baseados em palavras-chaves, que buscam mensagens anti-governamentais.
CHINA: O governo chinês utiliza um software chamado Internet Police 110 que bloqueia conteúdos que fazem referências a sexo, violência ou religiões não autorizadas. Fechou cerca de 17 mil cyber-cafés e proibiram a abertura de 11 mil novos.
ARÁBIA SAUDITA: O governo faz o controle através de um software chamado Djeddah que possui um gigantesco sistema de lista negra, contendo sites "proibidos" de conteúdo que afrontem a religião do país e a moral islâmica.
BIELO-RÚSSIA: Possui somente um provedor de acesso (estatal) que é controlado pelo governo e possui bloqueados páginas e organizações da oposição.
CÓREIA DO SUL: Governo proibiu o acesso a páginas de conteúdo homossexual desde 2001
EUA: Controle de acesso e censura nos Estados Unidos merecem uma história a parte. Em 1996 e 2000, o congresso americano declarava inconstitucionais as duas tentativas de censura de Internet do Governo Clinton, mas no calor das reações ao atentado de 11 de setembro de 2001, o congresso aprovou o projeto Carnivore. Carnivore é um dispositivo que grava os detalhes de todo o tráfego junto a um provedor de acesso, que na ótica deles, se resume num projeto de segurança nacional, que "justifica" a invasão de privacidade no mundo todo. http://www.fbi.gov/congress/congress00/kerr090600.htm
Pode capturar destinatários e assuntos do email, e mantêm um relatório de páginas visualizadas. Estes dados podem então ser armazenados em disco e serem admitidos como evidência em julgamentos
Adicionado ao projeto Carnivore, surge a ferramenta "magic lantern" que noo melhor estilo dos hackers, permite ao FBI inserir um cavalo de Tróia (espécie de vírus) no computador de suspeitos, segundo informações publicadas pelo serviço online MSNBC. Uma vez no micro, o software, passa a monitorar a digitação do usuário, obtendo senhas (essenciais em muitas investigações), que são enviadas aos agentes.
Para contaminar o alvo, o "vírus espião" é enviado por e-mail para o suspeito. A idéia do FBI é utilizar como remetente algum amigo da pessoa investigada. Além disso, os investigadores também pretendem seguir a estratégia dos hackers explorando vulnerabilidades do computador via Internet para instalar o programa de monitoramento remoto
Existem suspeitas que o FBI utiliza softwares comerciais importantes (como anti-virus) para disseminar este tipo de "cavalo de tróia".
INGLATERRA: Equivalente ao Carnivore americano, existe uma "provável" rede de espionagem chamada ECHELON, que compõem-se de 120 satélites que controlam diariamente cabos de telecomunicações submarinos e correio eletrônicos. É dirigido pela NSA americana e pela agência britânica de comunicações governamentais (GCHQ), mas participam dela também o Canadá, a Austrália e a Nova Zelândia. O Echelon conta com supercomputadores denominados "dicionários", que armazenam um banco de dados com critérios e objetivos específicos (nome, direção, número de telefone, etc). Quando um satélite detecta uma comunicação que possa ser interessante, a mensagem é relacionada e enviada a um determinado centro da NSA e do CGHQ.

A filtragem telefônica é baseado em pré-seleção de números e as vezes através de identidades telefônicas (rastro vocal individual).
Algumas agências acusam o Echelon de espionagem industrial, inclusive no famoso caso Thomson CSF e o Governo Brasileiro em 1994 na negociação do contrato do sistema de supervisão por satélite da selva amazônica. (mais informações no artigo: "Jornalismo científico, lobby e poder" em http://www.mct.gov.br/cee/revista/rev13.htm).
"A prisão, em março de 2003, do líder terrorista Al Qaeda Khalid Sheikh Mohammed foi resultado de meses de rastreamento de 10 telefones celulares, por meio do Echelon, revela a revista US NEWS". (fonte: http://noticias.terra.com.br)

BRASIL: A censura no Brasil é impraticável. Desde meados de 1990, a Embratel, antiga detentora do monopólio de acesso à Internet, começou a abrir o acesso para algumas universidades, culminando na abertura total e comercial em 1995. Hoje existem diversas saídas internacionais para acesso a Internet, como a própria Embratel, a AT&T, Brasil Telecom, Telemar, Impsat e outros. A instalação de filtros ou bloqueadores de sites devem ser feitos em todas as saídas de Internet, o que torna inviável num país onde não existe uma saída centralizada como no Brasil.

Apêndice B

Censura na Internet – porque ela não é efetiva

Uma das formas mais usadas para driblar filtros de acesso à Internet são os chamados "serviços de anonimato".
O mais famoso de todos é o **ANONYMIZER http://www.anonymizer.com**, que após o atentado de 11 de setembro nos Estados Unidos, foi fechado, mas permitiu criar uma geração de softwares de anonimato que trabalham nos mesmos moldes.
O anonymazer foi usado para transmitir informações de Kosovo durante a guerra.
O **SAFEWEB** que constitui-se de uma rede de centenas de servidores proxys (redirecionamento) públicos destinados a tornar anônimo, qualquer usuário que deseja navegar na Internet.
Existe uma outra rede, a **PEEKABOOTY,** que criptografa as conexões de usuários, que a atravessam, "fingindo" ser uma transação financeira.
Técnicas de **ESTEGANOGRAFIA** propõem o uso de métodos de camuflagem de informações sigilosas em mensagens e arquivos aparentemente inofensivos que só poderiam ser extraídas pelo destinatário, que detém o conhecimento do mapa de camuflagem. Esses métodos podem ser aplicados a arquivos binários, voz analógica, imagens eletrônicas e até mesmo a vídeo, em que os gestos aparentemente comuns podem esconder mensagens ocultas.
CAMERA/SHY pemite que usuários escondam mensagens codificadas dentro de imagens, usando um algoritmo chamdo RIJNDAEL que embaralha mensagens até se tornarem inteligíveis para terceiros.
SIX/FOUR PROTOCOL programa P2P (ponto a ponto) que cria uma rede "invisível" que ultrapassa filtros e firewalls.
PRIVATERRA: programa que permite privacidade e sigilo em comunicações.
ZEROKNOWLEDGE SYSTEM http://www.zeroknowledge.com possui um software chamado Freedom que se baseia em 3 retransmissores TCP/IP combinados com uma forte cifragem (mínimo de 128 bits). Cada retransmissor somente conhece sua antecessora e não mantém registros cronológicos, fazendo com que mesmo que identificados 2 retransmissores, não se chegue na informação necessária (rastreamentos).
PRIVADACONTROL: Software que permite utilizar contas digitais totalmente dissociadas de sua identidade real.
IPRIVACY http://www.iprivacy.com permite o comércio eletrônico anônimo, desde a navegação até a expedição, havendo a troca de identidades reais somente entre o consumidor e o utilizador do cartão de crédito.

Apêndice C

Crimes de computador – panorama no Brasil

Uma reportagem de capa da Revista Veja São Paulo (fev/2000), mostra uma nova ação da Polícia Civil de São Paulo, através de Mauro Marcelo de Lima e Silva, delegado da divisão de crimes pela internet.
Considerado "Sherlock da Internet", foi destaque em uma publicação distribuída aos membros da Polícia Federal dos Estados Unidos, o FBI, com comentários sobre ele e seu trabalho pioneiro no Brasil.

Abaixo a relação de alguns de seus casos resolvidos e as técnicas usadas para a solução do crime (nomes verdadeiros retirados para preservar vítimas):

Jornalista da TV Cultura: Recebia e-mails de cunho erótico-sexual, utilizando um software conhecido como MAILBOMB de remetente falso "estrupador@macho.com (sic). Através de análise do cabeçalho de e-mail chegou-se no IP do provedor GlobalOne que se recusou a fornecer informações a Policia Civil. Verificou-se que o criminoso usou o provedor STI-NET para fazer a conexão e este provedor forneceu acesso aos logs. De posse do horário e datas, descobriu-se que o único usuário do STI que se conectou com o provedor usado para enviar os e-mail a jornalista, foi um usuário "jasoft". De posse de um mandado judicial, foi feita uma busca e apreensão do computador do suspeito e encontrou-se o software UNABOMB e cópias dos e-mails enviados a jornalista.
O acusado foi condenado a dar aulas de informática para policiais.

Pedofilia em Pernambuco: Denúncia contra Filipe Vieira acusava-o de distribuição de material pornográfico em uma página de Internet. Através de pesquisas descobriu-se que a página estava em nome de um usuário em SBCampo-SP, mas na realidade pertencia ao Filipe de Pernambuco. O provedor Elogica que postava a página se recusou a fornecer informações do usuário, mas detectou-se que o Filipe é menor de idade e o cso foi remetido ao Juizado de Infância de Pernambuco.

Colégio em SP: Alunos criaram uma página criticando o colégio em um provedor americano. O provedor recusou-se a fornecer dados dos usuários, mas chegou-se ao nome de um aluno que possui cadastro no provedor. Através de mensagens do tipo "isca" chegou-se no acusado que foi expulso do colégio.

Site pornográfico Duda Rafa´s Page: site do provedor xoom.com (americano) que exibia fotos pornográficas de crianças, estava sob registro do menor E.C de 15 anos de Porto Alegre-RS. A polícia utilizou técnicas de "iscas virtuais" e ferramentas de software de rastreamento (mantidas em sigilo pela Policia). Caso encaminhado para o Juiz da Infancia e Juventude de Porto Alegre. A polícia civil também possui técnicas de "grampo de e-mail" que são usadas com ordem judicial em casos de pedofilia.

Denúncia Abranet – João Pessoa-PB: Denúncias de pornografia infantil recebidos pela Abranet que as encaminhou para a Polícia Civil de SP, contra Paulo XXX de e-mail pc@XXX.com.br morador de João Pessoa – Paraíba. Investigadores fazendo-se passar por adolescentes, solicitaram fotos pelo correio, conseguiram gravar conversas do acusado, conseguindo caracterizar a conduta do acusado.