FACULDADE IMPACTA DE TECNOLOGIA
Gestão em Tecnologia de Segurança da Informação

CIBERCRIMES: Mecanismos de Combate

FERNANDA APARECIDA DARE
PAULO FERNANDO PORTEZAN MIRANDA
SILVIO DADARIO DIONISIO

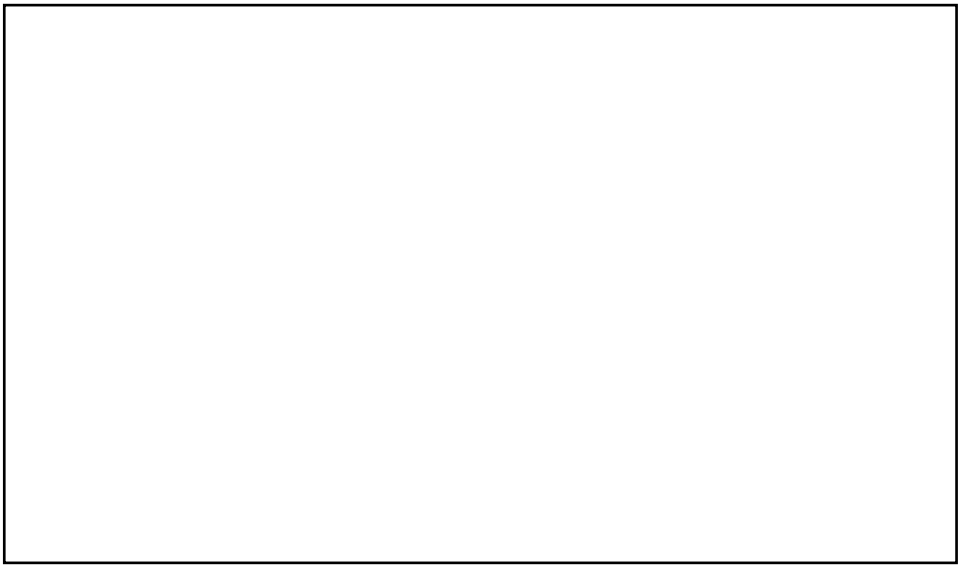
SÃO PAULO
2011

FACULDADE IMPACTA DE TECNOLOGIA
Gestão em Tecnologia de Segurança da Informação

CIBERCRIMES: Mecanismos de Combate

FERNANDA APARECIDA DARE
PAULO FERNANDO PORTEZAN MIRANDA
SILVIO DADARIO DIONISIO

SÃO PAULO
2011



FACULDADE IMPACTA DE TECNOLOGIA
Gestão em Tecnologia de Segurança da Informação

CIBERCRIMES: Mecanismos de combate

Trabalho de Conclusão de Curso apresentado ao Curso de Gestão em Tecnologia em Segurança da Informação da Faculdade Impacta de Tecnologia, orientado quanto a forma pelo Profº. Ms. Renato Mauro Richter e orientado quanto ao conteúdo pelo Profº. Hélio Cordeiro Novais Prates, como requisito para obtenção do grau de Especialista em Segurança da Informação.

Aprovados em _____ de _____

BANCA EXAMINADORA

_____

Prof. (a)

_____

Prof. (a)

_____

Prof. (a)

Dedicamos este trabalho, aos nossos pais, cônjuge e filhos, pelo esforço, dedicação e ajuda dada para a concretização de mais esta etapa da nossa vida.

AGRADECIMENTOS

Ao Profº. Hélio Cordeiro, nosso orientador de conteúdo, pela orientação, pelo cuidado na leitura, pelas recomendações precisas, pelo apoio e dedicação na elaboração e desenvolvimento deste trabalho.

Ao Profº. Renato Richter, orientador quanto a forma, por toda sabedoria transmitida ao longo do curso, pelo esforço concedido, paciência e compreensão.

"A educação faz um povo fácil de ser liderado, mas difícil de ser dirigido; fácil de ser governado, mas impossível de ser escravizado."
Henry Peter Broughman

RESUMO

A internet revolucionou o mundo e os hábitos das pessoas, que cada vez mais se tornam dependentes desta tecnologia, utilizando-a como um dos principais meios de comunicação e de acesso à informação.

Com diversificação de informações disponibilizadas pela internet e o crescente aumento de usuários, surgem também o cibercrime, ou crimes cometidos em meios digitais.

Esta pesquisa relata os principais tipos de crimes realizados pela internet, as ferramentas utilizadas para execução dos crimes e as principais técnicas utilizadas para identificação e prevenção destes crimes.

Descreve as técnicas de análise e obtenção de vestígios para serem utilizados como provas, e os problemas relacionados a ausência de leis especificas para os crimes digitais.

Palavras-chave: internet, cibercrime e ferramentas de combate

ABSTRACT

The Internet has innovated the world and people's habits, which become increasingly dependent on this technology, using it as a major means of communication and information access.

With the wide range of information available on the Internet and the increasing growth of users, there are also cyber crime, or crimes committed in digital media.

This research describes the main types of crimes carried out by the internet, the tools used for execution of the crimes and the main techniques used to identify and prevent these crimes.

Describes the techniques of analysis and retrieval of traces to be used as evidence, and problems related to lack of specific laws for computer crimes.

Keywords: internet, cybercrime and tools to fight.

SUMÁRIO

Lista de Ilustrações

Lista de Abreviaturas, Siglas, Símbolos e Significados

ARPA	*Advanced Research Project Agency*.
CCR	*Command and Control Research*.
CERN	*Centre Eoropéen por la Recherche Nucléaire*.
DEL	*Decode Encode Language*.
DISA	Defense Information Systems Agency.
FTP	*File Transfer Protocol.*
HTML	Hyper Text Markup Language.
IMP	*Interface Message Processor.*
NCP	*Network Control Protocol*.
NIL	*Network Interchange Language*.
NSF	National Science Foundation.
NWG	*Network Working Group*.
SRI	Stanford Research Institute.
TCP/IP	Transmission Control Protocol and Internet Protocol.
USA	United States of America (Estados Unidos da América).
WWW	World Wide Web.
MHZ	Frequência de Transição de Ciclos por Segundo
UCLA	University of California, Los Angeles
IBM	International Business Machines
IPTO	Information Processing Techniques Office
Arpanet	Advanced Research Projects Agency Network
CSNET	Computer Science network
NSFNET	National Science Foundation Network
CERN	Conseil Européen pour la Recherche Nucléaire
DEC PDP-10	Mainframe produzido pela Digital Equipment Corporation em 1960.
.INF	Information File
SOA	Statement of Applicability
IETF	Internet Engineering Task Force
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
SMTP	Simple Mail Transfer Protocol
HTTP	HyperText Transfer Protocol
DNS	Domain Name Server
VOIP	Voz Sob IP
IP	Internet Protocol
NAT	Network Address Translation

DHCPv6	Dynamic Host Configuration Protocol
IPSEC	Secure Internet Protocol
6to4	Internet Transition Mechanism that allows IPv6 packets to be transmitted over IPv4 network.
RFC 3056	Connection of IPv6 domains over IPv4 Clouds
ISP	*Internet Services Provider*
US-CERT	United States Computer Emergency Readiness Team
CPU	Central process Unit
TCP/SYN	Deny of Services attack
TCP/SYN-ACK	Deny of Services attack
ACK	Acknowledgement of data transfer
PPI	Pay-per-install
DDoS	Negação de Serviços distribuidos
DC++	Redes ponto a ponto
P2P	Rede ponto a ponto
ICMP	Internet Control Message Protocol
Timeout	Esgotamento de tempo de espera
Host	Dispositivo de rede
Routing	Roteamento de pacotes entre redes+B48
Telnet	Emulação de Terminal sob redes TCP IP
Hardware	Toda parte física da informática
on-line	Esta com conectado a internet
Ethernet	Rede Local de Computadores
Fuzzy Logic	Forma de lógica booleana
Handshakingsinal	Enviado entre dois hosts para indicar que a conexão esta estabelecida
Checksum	Verificar a integridade de dados transmitidos ou armazenados
Bits	É a menor unidade de informação que pode ser armazenada ou transmitida
Multicast	Envio de mensagens a grupo de hosts
Coaxiais	Conductor utilizado para transmitir sinais
Softwares	Toda parte não física da informática
Firmware	Conjunto de instruções operacionais programada diretamente no
Trojans	É um malware
Worms	É um malware
Malwares	Softwares maliciosos que danificam o computador
keyloggers	Gravadores de digitação do teclado

Defense	Defesa
Browsers	Navegadores de Internet
LYNX	Browsers
Mosaic	Browsers
Router	Equipamento utilizado para interligar redes
web sites	Páginas da internet
hacker	Especialista em informática
fóruns	Local onde pessoas discutem e trocam informações
blogs	Local onde pessoas trocam informações
chat´s	Local onde pessoas trocam informações
VeriSign	Emissora de certificado digital
BIOS	Basic Imput / Output System
Login	Acesso
ICMP Flood	Inundação do link por requisições smtp
Ping flood	O mesmo que ICMP Flood
smurf attack	Ataque de negação de serviços
Peer-to-Peer	Rede ponto a ponto
Botnetagentes	De software autonomos
Trojans	Tipos de malware
Flood	Inundação
fraggle attack	Ataque de negação de serviços
smurf attack	Ataque de negação de serviços
Sywares	São tipos de malwares
Websites	Páginas da web
print screen	Captura tela
cracks	Ferramentas para piratear softwares
serials	Ferramentas para piratear softwares
keygens	Ferramentas para piratear softwares
virus	São tipos de malwres
worms	São tipos de malwres
trojan	São tipos de malwres
horses	São tipos de malwres
spywares	São tipos de malwres

adwares	São tipos de malwres
rootkits	São tipos de malwres
spams	São tipos de malwres
Conectado	Quando alguém se conecta, está presente naquele exato momento em algum lugar.
Roteamento	Ato de interligar duas ou mais redes
Encapsulamento	IP - Inserir um trafego de TCP IP dentro de outro (IPSEC)
Infracional	Cometer infração
Reconfigurado	Alterar configuração
Escaneadores	Buscadores de arquivo
LOG	Informação de execução de sistemas
Código Malicioso	Programa cuja intenção é danificar o computador
Forense	Aplicação de técnicas cientificas dentro de um processo legal.

1. INTRODUÇÃO

Com o aumento do uso da internet e a facilidade com que cada vez mais pessoas conseguem acesso à rede, surgiram novas ferramentas de interação como as lojas virtuais, comunicadores, dentre outros. Com este crescente número de usuários na internet, um novo tipo de crime surge, onde a vítima é lesada no ambiente virtual, através de roubo de informações ou manipulação indevida de dados pessoais. O criminoso pode estar distante de suas vítimas, podendo até estar em outro país.

Com o intuito de minimizar os cibercrimes, atualmente a forense computacional tem sido a melhor ciência que se volta para a coleta de informações capazes de comprovar e esclarecer um crime real em ambiente virtual ou misto. A forense computacional surgiu em virtude deste novo tipo de crime que não pode ser controlado e identificado através de meios convencionais, pois as evidências destes crimes podem não estar disponíveis no ambiente físico.

As ferramentas de prevenção são utilizadas para monitorar o ambiente e evitar que o crime aconteça, as ferramentas de identificação são utilizadas para identificar os cibercrimes após sua ocorrência.

Para cada nova tecnologia desenvolvida novas ferramentas de prevenção e análise são necessárias, devido ao crescente número de ataques e suas diversificações.

Nos cibercrimes, como também acontece com os crimes em ambientes físicos, as provas devem ser isoladas a fim de proteger a integridade das informações a serem periciadas.

Para proteger a integridade destas provas que não são físicas é necessária a aplicação das ferramentas de identificação, para que seja possível extrair o máximo de informações dos equipamentos e sistemas para serem analisados de forma a torná-las provas concretas.

Em diversos países, como o Brasil, ainda não há legislação específica para tratar o assunto, portanto todas as evidências obtidas devem ser apoiadas em leis já existentes para que possam ser utilizadas no andamento do processo de investigação.

O trabalho descreve as modalidades de cibercrimes relacionados ao aumento da utilização da internet e as técnicas para equiparar provas de cibercrimes a provas de crimes comuns para que sejam utilizadas as legislações vigentes no tratamento de tal crime.

2. OBJETIVOS

2.1 Objetivo Geral

Investigar as formas de cibercrimes e os mecanismos de combate.

2.2 Objetivos Específicos

Pesquisar e descrever:

– A evolução da internet

– Tipos de Cibercrimes;

– Técnicas e ferramentas de ciberataques

– Técnicas de combate à cibercrimes e ferramentas disponíveis;

– Legislações e meios de equiparação às leis gerais;

3. JUSTIFICATIVA

Com o expressivo progresso do uso da internet pela sociedade e com o número cada vez mais significativo de cibercrimes e suas modalidades, como fraudes e golpes de falsidade ideológica, este estudo pretende oferecer um conhecimento mais específico sobre os problemas causados pelos cibercrimes à sociedade, os principais mecanismos de controle e suas deficiências.

A pesquisa aborda as principais deficiências relacionadas a padrões de pericia atualmente e a ausência de leis específicas para criminalizar os autores. Estas deficiências resultam no atraso da elucidação destes crimes, impunidade e criminalizações inadequadas dos atos.

Este trabalho descreve as diversas ferramentas e técnicas disponíveis para evidenciar os fatos e os problemas relacionados à ausência de padronização das ferramentas, que podem resultar em perda de evidências por utilização inadequada.

As dificuldades no processo de obtenção de evidências são descritas, e os cuidados necessários para que as evidências não sejam adulteradas e possam ser utilizadas como prova.

4. INTERNET

A criação e evolução da internet propiciam à sociedade diversos benefícios, dentre eles: a facilidade e agilidade de acesso a um número diversificado de informações disponibilizadas mundialmente e utilizadas para inúmeros fins; os serviços descentralizados disponibilizados na grande rede de computadores, tais como: comércio eletrônico e banco eletrônico; o desenvolvimento e acompanhamento de projetos; possibilidade de compartilhamento de informações de forma fácil e ágil através dos sites de relacionamento, *blogs*, *fóruns* de discussão e *chats*; geração de emprego e novas profissões, tais como: *web designer* e programador. (ROSA, 2007)

Apesar de existirem benefícios com a criação e evolução da internet, existem também diversos problemas, tais como: a segurança, que implica na violação, falsificação e manipulação indevida da informação; acesso indevido a informações confidenciais; vulnerabilidades, que resultam na inovação de crimes já tipificados ou na pratica de novos crimes. (ROSA, 2007)

4.1 Evolução

4.1.1 Web 1.0

Em 1990, com o fim da Arpanet foi criada NSFNET que foi responsável por popularizar o nome internet no mundo todo. A expansão da internet foi possibilitada pela *World Wide Web* (www) criada por dois engenheiros do *Centre Eoropéen por la Recherche Nucléaire* (CERN) Robert Caillaiu e Tim Berners-Lee, do *HyperText Markup Language* (HTML) e dos *browsers*. O primeiro *browser* utilizado foi o LYNX que apenas permitia a transferência de textos (BRASIL, 2001).

O Mosaic foi o primeiro browser criado capaz de visualizar figuras e textos de forma mais amigável e a partir dele basearam se os o Netscape e Internet Explorer que foram responsáveis por popularizar o uso da internet.
(SOBRAL, 2001).

4.1.2 Web 2.0

O termo foi criado por Tim O´Reilly em 2002, um especialista em arquitetura de informações eletrônicas ao citar os novos *web sites* que se utilizam de conteúdo dinâmico para entreter os usuários em vista dos sites convencionais da época que somente forneciam ao usuário a experiência de leitura.

A Web 2.0 é um novo paradigma que surgiu para criação e utilização de web sites, que foi possibilitado pela evolução dos computadores e o incremento da largura de banda da internet. Os Web sites criados com essa concepção podem prover aos usuários uma *interface web* mais agradável, aplicativos web, compartilhamento de informações e armazenamento remoto através do *browser* de *internet*. Este conceito é chamado “Internet como uma plataforma”.

A Web 2.0 pode ser vista como uma internet participativa, pois fornece aos usuários liberdade para interagir com o conteúdo dos sites como atributo essencial.

As principais tecnologias utilizadas nos *web browsers* para permitir a utilização com sites web 2.0 são JavaScript, XML(Ajax), Adobe Flash, Adobe Flex framework, Microsoft SilverLight.

A Web 2.0 pode ser descrita em três partes, sendo elas:

- *Rich Internet Application* (RIA), define a experiência gráfica agregada ao browser através de tecnologias como Ajax e Flash.
- *Service-oriented archtecture* (SOA), é o principal componente da Web 2.0, que define o nível de integração com outros aplicativos.
- Social *Web* define o grau de interação entre o web site e os usuários. (TIM O’REILLY, 2005)

4.1.3 Web 3.0

Web 3.0 é um conceito que ainda esta em construção, a web semântica, nesta estrutura as informações da web seriam classificadas de maneira lógica, conforme entendimento humano, e seria inserido em cada página um código metadata de máquina capaz informar os softwares de navegação o quão relacionado este site esta com todos os outros da web, com isto os softwares conseguiriam realizar consultas de forma muito mais inteligentes entendendo o que o usuário esta buscando.

A proposta da web semântica é permitir que *softwares* entendam e respondam a requisições complexas humanas levando em consideração o seu significado e as preferências do usuário em questão, permitindo que os usuários pesquisem, compartilhem ou busquem informações de maneira mais simples e eficiente.

Os desafios da Web 3 são:

- Os *softwares* e equipamentos com acesso a *web* que precisariam estar interligados possibilitando ao usuário estar sempre conectado a um sistema que tenha conhecimento de suas preferências e gostos, realizando sugestões na hora das buscas, ao usuário, de forma inteligente.
- A vastidão de *sites*, aproximadamente 26 bilhões de páginas, que precisariam ser catalogadas de forma a eliminar as duplicidades de semântica existentes entre elas para que as buscas retornem resultados corretos.
- Conceitos vagos buscados pelos usuários, como por exemplo, a palavra “bonito”, precisam ser tratados de forma a exibir realmente o que usuário esta buscando e não todos os significados. Através de tecnologias como *Fuzzy Logic* os sistemas devem ser capaz de localizar qual o contexto do que o usuário esta buscando analisar a probabilidade em relação a todos os termos que estão contidos na busca e pesquisando também nas bases de dados que armazena o comportamento do usuário. Assim o sistema deve realizar a entrega dos resultados de maneira mais correta possível.
- Incertezas e inconsistências, os sistemas precisaram ser capazes de lidar com contradições e resultados incertos de consultas através de técnicas de contramedida.

- Criptografia e Segurança deve ser o padrão garantindo a segurança do usuário. (JEFFREY T. POLLOCK, 2009)

4.1.4 Protocolo IPv4

O TCP/IP V4 é a quarta versão do protocolo IP que surgiu dos estudos que originaram a DARPANET e esta publicado na sessão 791 IETF), este é o protocolo mais utilizado na atualidade para redes de computadores. O protocolo é dividido em 4 camadas:

- Camada de Rede é a camada um 1, sendo a camada mais baixa do protocolo TCP/IP, que é responsável pela movimentação dos pacotes de dados através da interface de rede, entre outros dispositivos. (Smith, Lucie; Lipner, Ian, 2011)
- Camada de Internet é a camada 2, que é r(Smith, Lucie; Lipner, Ian, 2011) esponsável pelo roteamento dos pacotes a serem enviados pela camada de rede.
- Camada de Transporte é a camada 3, prove os serviços e as portas de conexão para aplicativos utilizarem os serviços de rede, ambos protocolos de transporte TCP e UDP possuem 65535 portas para encaminhar pacotes para as camadas inferiores, o protocolo TCP é orientado a conexão portanto tudo que for enviado através de suas portas será garantida (Handshaking) a integridade e o recebimento do arquivo através de confirmações do envio dos pacotes e checagens (checksum) da integridade dos pacotes, já o protocolo UDP não é orientado a conexão, portanto não há garantia da correta transmissão de dados mas há uma velocidade de transmissão muito maior devido a não necessidade de confirmações de recebimento. (Smith, Lucie; Lipner, Ian, 2011)
- Camada de Aplicativo é a camada 4, que é a última camada (mais alto nível) do protocolo IPv4 onde estão disponíveis os protocolos (serviço de rede) como por exemplo, FTP (porta 21 TCP), SMTP (porta 25 TCP), HTTP (porta 80 TCP), TELNET (porta 23 TCP), DNS (porta 53 UDP) e VOIP (porta 5100 UPD).

O endereçamento utilizado pelo IPv4 possui 32 bits, o que limita a utilização de apenas 4 294 967 296 endereços, contudo alguns blocos são reservados para serviços de rede como, por exemplo, o multicast que consome aproximadamente 270 milhões de endereços dentre outros serviços especiais fazendo com que o

número real de endereços disponíveis para internet seja reduzido consideravelmente. (Smith, Lucie; Lipner, Ian, 2011)

Os endereços deste protocolo podem ser escritos em qualquer formato que expresse valores de 32 bits, como por exemplo, decimal, hexadecimal, octal e o padrão decimal separado por pontos. (Smith, Lucie; Lipner, Ian, 2011)

O endereço IP é divido em duas partes, sendo que a primeira é o identificador da classe da rede e a segunda o número IP do dispositivo. Existem 5 classes de redes no protocolo IPv4 chamadas A, B, C, D e E, as classes A, B e C têm diferentes tamanhos de endereçamentos para dispositivos de rede, a classe D é destinada a multicast e a classe E é reservada para aplicações futuras. A classe A, é utilizada normalmente quando necessitamos criar grandes redes, possui blocos de 24 bits com endereços que variam de 10.0.0.0 a 10.255.255.255, o que dá um total de 16.777.216 endereços. A classe B, utilizada em redes de médio porte possui blocos de 20 bits e possui endereços entre 172.16.0.0 e 172.31.255.255 com 65.536 endereços disponíveis para uso em dispositivos de rede. A Classe C, utilizada por pequenas redes, possui blocos de 16 bits e endereços que variam de 192.168.0.0 a 192.168.255.255 com 256 endereços liberados para dispositivos. As classes D e E são de uso restrito sendo que a primeira é reservada para *multicast* e a segunda para aplicações futuras. (Smith, Lucie; Lipner, Ian, 2011)

4.1.5 Protocolo IPv6

Durante os primeiros anos de funcionamento da internet, apesar de todos os métodos desenvolvidos para conservar endereços IPv4, ficou claro que 4,3 bilhões de endereços não seriam suficientes e mudanças profundas na infrasestrura da internet seriam necessárias para que a rede continuasse crescendo.

No inicio de 1993 a IETF criou uma área de pesquisas para a nova geração do protocolo IP e através destas pesquisas surgiu em 1996 o protocolo IPv6.

Este novo protocolo trabalha da mesma forma que o IPv4, com divisão dos dados em pacotes e transmissão através de varias redes de IP, mas a principal diferença entre eles é que o IPv4 possui barramento de endereços de 32bits provendo aproximadamente 4,3 bilhões de endereços e o IPv6 trabalha com barramento de 128bits provendo cerca de 340 decilhões de endereços, esta grande

quantidade de endereços eliminaria a necessidade de se utilizar equipamentos NAT como *gatways* de rede.

Exemplo de endereço IPv6 2011:0fb8:73b3:0341:08e2b:0ff44:7443.

Os primeiros 64bits representam o prefixo da rede (subrede) e os últimos 64bits representam o dispositivo ou *interface* de rede.

Além de mais endereços o IPv6 contém novas funcionalidades que não estão presentes na versão IPv4, como, configuração automática de endereço através do protocolo ICMPv6, onde o *host* IPv6 envia uma solicitação de configuração da rede via *multicast* para o roteador IPv6, este, estando habilitado para isto, responderá com a configuração da rede para o *host*, um outro meio de se obter as configurações da rede é através do protocolo DHCPv6, que também possui versão similar no protocolo IPv4.Outra característica nova do IPv6 é a existência de segurança integrada em sua arquitetura, concebida através do protocolo IPSEC que realiza criptografia de todo envio e recebimento de pacote realizado em redes IPv6. Neste protocolo o endereço reservado para subredes é de 64Btis e o prefixo para roteamento da rede é também de 64 bits portando alterações em provedores de serviços causam pouco impacto no IPv6 devido ao host conhecer apenas os 64bits de subrede, diferente do que acontece com o IPv4. Os cabeçalhos dos pacotes IPv6, apesar de serem maiores que os cabeçalhos IPv4 são mais simples, portanto processados mais rapidamente pelos roteadores IPv6 o que incrementa a velocidade da troca de pacotes em redes IPv6.

Todas estas melhorias colocam o protocolo IPv6 muito a frente do atual IPv4, porém os altos custos de melhoria em alguns sistemas e troca de roteadores para suportar o IPv6 esta atrasando muito a sua migração, e durante o período de existência dos dois, existirão técnicas que permitam a troca de informações entre redes IPv6 e IPv4, visto que nativamente elas são incompatíveis. A principal técnica de comunicação é 6to4, que é a técnica recomendada pela RFC 3056, é uma técnica automática de tunelamento entre as duas redes, esta técnica realiza o encapsulamento do trafego IPv6 através de uma rede IPv4 de forma a unir duas redes IPv6, ou computadores IPv6 através de uma rede IPv4 possibilitando as duas redes coexistirem.(S. Deering, R. Hinden RFC 2460,1998)

5 CIBERCRIME

5.1 Definição

Cibercrime e crime informático são sinônimos. Muitos autores procuram esclarecer a melhor definição para o conceito de "crime informático", temos inúmeras definições sobre o assunto, vistos de forma diferente. Todos os crimes relacionados às informações guardadas ou transitando por redes e computadores, sendo essas informações, acessadas de forma ilícita, para serem usadas para ameaçar ou fraudar. Percebe-se que há uma preocupação sobre os crimes contra as pessoas, computadores e sistemas com informações gravadas ou interceptação indevida nessas informações ou dados. (CORRÊA, 2000)

É importante relevar que o meio informático abre possibilidade para a prática de novos crimes ou cria novas maneiras para praticar crimes existentes como a falsa identidade e o furto. Portanto existem crimes ocorridos pelo computador onde o computador seria a ferramenta para o crime, e os ocorridos contra o computador, isto é, contra seu *hardware* (parte física) e *software* (parte lógica), pois seria o objeto do crime. (GOMES, 2000)

5.1.1 Classificação dos crimes informáticos

Os crimes informáticos estão classificados em:

- Crime virtual puro: é a prática criminosa que ataca apenas o computador em si, o ataque pode ser físico ou tecnicamente o equipamento (*hardware*) e logicamente (informações e *softwares*), exemplo de vírus que ataque o *hardware* ou *software* do computador.

- Crime virtual misto: é a utilização da internet para a prática do crime, exemplo de um vírus para armazenar senhas digitadas em páginas de bancos na internet (keyloggers) para desvio de valores financeiros posteriormente.

- Crime virtual comum: é utilizar a informática somente como ferramenta para a inovação de um crime já tipificado pela lei penal, por exemplo, a pornografia

de menores divulgada pela internet e não mais de outros meios antigos como jornais, revistas ou periódicos. (PINHEIRO, 2010)

5.1.2 Categorização dos crimes informáticos

- Crimes informáticos impróprios: Quando o computador é o instrumento para a execução do crime, porém não há alteração ou furto da informação, por exemplo, usar o computador enviando um email para fazer calúnias, difamação ou injúria.
- Crimes informáticos próprios: Quando o computador é o instrumento para a execução do crime e a informação é violada, por exemplo, a interceptação telemática ilegal.
- Crimes informáticos mistos: São crimes complexos, além da informação violada, na lei à proteção sobre o equipamento (bem jurídico) de qualquer natureza diversa.
- Crimes informáticos indiretos: É o crime que se concretizou na vida real, que se originou pelo meio informático. (VIANNA, 2003)

5.2 Tipos de Cibercrimes

5.2.1 Ameaça

Esse crime consiste em ameaçar alguém de forma escrita, verbal, por gestos ou por qualquer meio, a fim de querer restringir a liberdade de outra pessoa. Qualquer pessoa pode praticar esse crime. E a vítima pode ser qualquer pessoa que goze de liberdade plena.

O crime de ameaça está tipificado no artigo 147 no Decreto-Lei 2848 de 07 de dezembro de 1940. A pena cominada é: detenção de um a seis meses, ou multa.

Prática equiparada no meio cibernético: uso de mensagens eletrônicas, *chats*, páginas eletrônicas, *webcam*, redes sociais, *blogs* etc (BRASIL, Decreto-Lei 2.848 de 07 de dezembro de 1940).

5.2.2 Discriminação ou preconceito

Esse crime consiste em praticar, induzir, incitar discriminação ou agir de forma preconceituosa em relação à cor, etnia, religião, raça e/ou procedência nacional. Também é enquadrado às pessoas que comercializam, divulgam, distribuem ou veiculam símbolos que incitem discriminação ou preconceito.

Qualquer pessoa pode cometer o crime, como qualquer pessoa pode ser vítima de discriminação ou preconceito.

O crime de discriminação ou preconceito está tipificado no artigo 20 da Lei 7716 de 05 de janeiro de 1989.

Prática equiparada no meio cibernético: comentar em chats, mensagens eletrônicas e outros de forma negativa sobre raças, religiões e etnias.(BRASIL, Lei 7716 de 05 de janeiro de 1989)

5.2.3 Violação de imagem

Esse crime consiste em violar a imagem das pessoas, ou seja, usar a imagem das pessoas sem o prévio consentimento ou mesmo com o consentimento divulgar a imagem de forma depreciativa ou de forma vulgar.

Qualquer pessoa pode cometer o crime, como qualquer pessoa pode ser vítima de violação de imagem.

É assegurado o direito a indenização pelo dano moral ou mesmo material decorrente de sua violação.

O crime de violação de imagem está tipificado no título 2 no capítulo 1 pelo artigo 5º da Constituição Federal de 1988

Prática equiparada no meio cibernético: expor fotos de pessoas sem a autorização de forma desonrosa ou expondo vídeos não autorizados em rede sociais ou canais de vídeo.(BRASIL, Constituição Federal de 1988)

5.2.4 Falsa identidade

Esse crime consiste em passar por alguém ou atribuir a terceira pessoa falsa identidade para obter vantagem para proveito próprio ou de terceiros e/ou só para causar danos a outras pessoas.

Qualquer pessoa pode cometer o crime, como qualquer pessoa pode ser vítima de danos causados por falsa identidade.

O crime de falsa identidade está tipificado no artigo 307 e 308 no Decreto-Lei 2848 de 07 de dezembro de 1940. A pena cominada é: detenção de três meses a um ano ou multa, se o fato não constituir elemento de crime mais grave.

Prática equiparada no meio cibernético: emprestar o *login* e/ou senha de email ou de sistemas de empresas.(BRASIL, Decreto-Lei 2.848 de 07 de dezembro de 1940)

5.2.5 Dano

Esse crime consiste destruir, inutilizar ou deteriorar bens de terceiros. Esse crime se estende com o uso de violência ou grave ameaça a terceiros.

Qualquer pessoa pode causar dano a terceiro, ou seja, também qualquer pessoa pode sofre dano como vítima.

O crime de dano está tipificado no artigo 163 no Decreto-Lei 2848 de 07 de dezembro de 1940. A pena cominada é: detenção de um a seis meses ou multa. Caso o crime possuir agravantes como o uso de substâncias inflamáveis, por exemplo, pode haver agravante de pena.

Prática equiparada no meio cibernético: enviar ou espalhar vírus, worms, ou qualquer código malicioso que pode causar dano a terceiros.

5.2.6 Ato infracional contra o menor

Esse crime consiste em divulgar, sem autorização devida, total ou parcial, por qualquer meio de comunicação, nome, ato ou documento de ato infracional relativo a criança ou adolescente.

Qualquer pessoa pode ser o infrator, a vítima necessariamente será uma criança ou adolescente menor.

O crime de dano está tipificado no artigo 247 na Lei 8069 de 13 de julho de 1990. A pena cominada é: multa de três a vinte salários de referência aplica-se o dobro pela reincidência.

Prática equiparada no meio cibernético: Envio de fotos de crianças e/ou adolescentes nus ou vídeos expondo menor de forma vexatória.(BRASIL, Lei 8.069 de 13 de julho de 1990)

5.2.7 Difamação

Esse crime consiste em difamar ou maldizer alguém, imputando-lhe fato depreciativo à sua reputação.

Qualquer pessoa pode ser o infrator, a vítima é pessoa difamada.

O crime de difamação está tipificado no artigo 139 no Decreto-Lei 2848 de 07 de dezembro de 1940. A pena cominada é: detenção de três meses a um ano e multa.

Prática equiparada no meio cibernético: Espalhar boatos eletrônicos sobre pessoas.(BRASIL, Decreto-Lei 2.848 de 07 de dezembro de 1940)

5.2.8 Calúnia

Esse crime consiste em caluniar alguém, atribuindo-lhe um fato criminoso que não ocorreu (falso).

Qualquer pessoa pode ser o infrator, a vítima é pessoa caluniada.

O crime de calúnia está tipificado no artigo 138 no Decreto-Lei 2848 de 07 de dezembro de 1940. A pena cominada é: detenção de seis meses a dois anos e multa.

Prática equiparada no meio cibernético: Insultar a honra de alguém a respeito de fatos tipificados como crime ou contra os valores morais que não são verdadeiros em relação ao destinatário de tais ofensas. Os meios mais comuns utilizados para praticar esse crime são: mensagens eletrônicas, *blog*, redes sociais e *chats*. (BRASIL, Decreto-Lei 2.848 de 07 de dezembro de 1940)

5.2.9 Injúria

Esse crime consiste em injuriar terceiro, ofendendo-lhe a dignidade e/ou decoro.

Qualquer pessoa pode ser o infrator, a vítima é pessoa injuriada.

O crime de injúria está tipificado no artigo 140 no Decreto-Lei 2848 de 07 de dezembro de 1940. A pena cominada é: detenção de um a seis meses ou multa. Pode-se agravar a pena quando o insulto refere-se a: raça, cor, etnia, religião,

origem ou a condição de pessoa idosa ou portadora de deficiência, a pena cominada é: reclusão de um a três anos e multa.

Prática equiparada no meio cibernético: Insultar pessoas considerando suas características ou utilizar apelidos grosseiros. Os meios mais comuns utilizados para praticar esse crime são: mensagens eletrônicas, *blog*, redes sociais e *chats*.(BRASIL, Decreto-Lei 2.848 de 07 de dezembro de 1940)

5.2.10 Interceptações em sistemas de telefonia, informática e telemática

Esse crime consiste em gravações clandestinas ou reter documentos sem autorização ou alterar documentos sem permissão ou divulgar arquivos não autorizados ao meio público ou particular, no meio informático.

Segundo a lei nº 9.296 de 24 de julho de 1996 são definidos crime tipificado “a conduta de realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei”.

Qualquer pessoa pode ser o infrator, a vítima é pessoa ou sistema interceptado de dados.

A prática desse crime tem a cominação de reclusão de dois (2) a quatro (4) anos e multa.

Prática equiparada no meio cibernético: invasões em servidores com roubo de informações ou alterações ou inclusões de informações não autorizadas; intercepções de informações e arquivos confidenciais por meio de mensagens eletrônicas ou outros diretórios na rede mundial de computadores.(BRASIL, Lei 9.296 de 24 de julho de 1996)

5.2.11 Violação da propriedade intelectual de programas de computador

Esse crime consiste em violar o direito exclusivo de autorizar ou proibir o aluguel comercial de *softwares* e/ou programas registrados ou não. Consiste em efetuar, reproduções e guardas de cópias não autorizados de *softwares* e/ou programas.

Segundo a Lei nº 9.609 de 19 de fevereiro de 1998 é definido crime tipificado “violar direitos de autor de programa de computador de reprodução ou guarda de cópias não autorizada ou copiar o código fonte sem autorização para fins comerciais”.

Qualquer pessoa pode ser o infrator, a vítima é o software e/ou programa informático.

A prática do crime de violar direitos de autor de programa de computador tem a cominação de detenção de seis meses a dois anos ou multa, com agravante se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente com reclusão de um a quatro anos e multa.

Prática equiparada no meio cibernético: guardar softwares e/ou programas comercializados sem a devida licença do uso ou aquisição e distribuí-la sem o consentimento do proprietário. Também podemos definir que o uso de técnicas para tirar o bloqueio do uso do software sem a aquisição devida, conhecido com a técnica de *cracks*, serials e *keygens* etc.(BRASIL, Lei 9.609 de 19 de fevereiro de 1998)

5.2.12 Monitoramento não avisado previamente

Esse crime consiste em gravações ou escutas clandestinas com retenções de informações sem autorização da justiça.

Segundo a lei nº 9.296 de 24 de julho de 1996 é definido crime tipificado no artigo 10 e na Constituição Federal, no artigo 5º em seu inciso XII parte final “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”.

Qualquer pessoa pode ser o infrator, a vítima é pessoa ou sistema monitorada sem a devida autorização ou comunicação das partes.

A prática desse crime tem a cominação de reclusão de dois (2) a quatro (4) anos e multa.

Prática equiparada no meio cibernético: monitoramento de mensagens eletrônicas, de visita de sítios, com *print screen*, de mensagens instantâneas, de uso de sistemas e programas e de arquivos.(BRASIL, Lei 9.296 de 24 de julho de 1996)

5.2.13 Usar logomarca/sinal de empresa sem autorização

Esse crime consiste em usar sinal, marca, produto de alheio sem consentimento ou imitá-lo, quebrar patente ou segredo industrial, colocar o nome empresarial próprio em produto de outros fabricantes, vender ou comercializar produto adulterado ou falsificado de outros estabelecimentos.

Segundo a Lei nº 9.279 de 14 de maio de 1996 em seu artigo 195, é definido crime tipificado nos incisos:

> *"IV - usa expressão ou sinal de propaganda alheios, ou os imita, de modo a criar confusão entre os produtos ou estabelecimentos;*
>
> *VI - substitui, pelo seu próprio nome ou razão social, em produto de outrem, o nome ou razão social deste, sem o seu consentimento;*
>
> *VIII - vende ou expõe ou oferece à venda, em recipiente ou invólucro de outrem, produto adulterado ou falsificado, ou dele se utiliza para negociar com produto da mesma espécie, embora não adulterado ou falsificado, se o fato não constitui crime mais grave;*
>
> *XIII - vende, expõe ou oferece à venda produto, declarando ser objeto de patente depositada, ou concedida, ou de desenho industrial registrado, que não o seja, ou menciona-o, em anúncio ou papel comercial, como depositado ou patenteado, ou registrado, sem o ser;"*

Qualquer pessoa pode ser o infrator, a vítima é pessoa ou empresa estabelecida.

A prática desse crime tem a cominação de detenção de 3 (três) meses a 1 (um) ano ou multa.

Prática equiparada no meio cibernético: criar logomarcas ou sinais que lembre o estabelecimento concorrente, criar *sites* muito parecido (clonar *sites*) e as mesmas maneiras de entendimento do mesmo negócio e os mesmo tipos de anúncios de produtos, serviços e promoções e maneiras de como adquirí-lo. Colocar o seu nome da rede mundial de computadores como fornecedor oficial de determinado produto, como fosse fabricado ou dono da patente. Usar o meio virtual para venda de produtos falsificados, clonados ou adulterados de marcas de outros

fabricantes e divulgar a idéia ou produto de autoria ou fabricação própria.(BRASIL, Lei 9.279 de 14 de maio de 1996).

5.2.14 Apologia e incitação ao crime

Esse crime consiste em incitar, elogiar ou discursar publicamente a favor da prática criminosa ou de criminoso.

O crime de apologia e incitação ao crime está tipificado nos artigos 286 e 287 no Decreto-Lei 2848 de 07 de dezembro de 1940. A pena cominada é: detenção de três a seis meses ou multa.

Prática equiparada no meio cibernético: Em *fóruns* é muito comum a indução ou persuasão, através de um conselho ou argumentação bem elaborada, pressupondo-se que a prática criminosa seria uma forma da resolução adequada do problema sem o uso dos mecanismos legais. Incitar é instigar, excitar ou provocar a prática do crime, por qualquer meio ou de qualquer forma, podendo se iniciar na internet e concluir na vida real, ou independe se ocorreu o crime, apenas pelo fato de provocar ou incitar já constitui o crime.(BRASIL, Decreto-Lei 2.848 de 07 de dezembro de 1940)

5.2.15 Apologia e incitação a práticas cruéis contra animais

Esse crime consiste em abusar, mal-tratar, ferir ou mutilar animais.

O crime de apologia e incitação a práticas cruéis contra animais está tipificado no artigo 32 da Lei 9.605 de 12 de fevereiro de 1998. A pena cominada é: detenção de três meses a um ano e multa. Aumenta-se a penalidade de um sexto a um terço caso haja experiência sobre animal vivo de forma dolorosa que tenha outra forma de ser realizado, resultando a morte do animal.

Esse crime pode ser realizado por qualquer meio ou de qualquer forma, podendo se iniciar na internet e concluir na vida real, ou independe se ocorreu o crime, apenas pelo fato de provocar ou incitar já constitui o crime.

Prática equiparada no meio cibernético: Em *fóruns,* mensagens eletrônicas*, blogs e chat´s* é muito comum a divulgação de relatos, fotos e práticas ou a instigação de maneiras ou técnicas de provocar tortura ou maldades com gatos,

cãos, tartarugas, aves ou outro tipo de animal.(BRASIL, Lei 9.605 de 12 de fevereiro de 1998)

5.3 Impactos na Sociedade

O cibercrime é uma realidade atual, seu combate só será possível caso haja denúncia às autoridades competentes pelas vítimas, no entanto alertam que "caberá a cada internauta buscar sistemas que proteja de forma adequada.

Os impactos econômicos dos ilícitos associados ao cibercrime ainda não conseguiram ser medidos de forma exata.

O principal motivo da dificuldade está na falta das vítimas, na maioria dos casos, não denunciarem o ocorrido, por isso se torna dificilmente identificar e responsabilizar o(s) autor(es) do(s) ilícito(s).

Outro fato identificado é a omissão de denúncia em casos de cibercrime, pois a propagação da publicidade negativa poderá resultar em prejuízos para a imagem de da empresa lesada, caso seja de conhecimento público que foi vítima de um cibercrime, uma vez que os clientes dessa empresa podem imaginar que a empresa está vulnerável em relação à segurança da informação.

Existe dificuldade de investigar e punir os ilícitos provocados pelo cibercrime Nos dias de hoje, estima-se que existam mais de um bilhão de internautas de internet em todo o mundo. No entanto, não é possível identificar a percentagem de pessoas que usam a internet para praticar cibercrimes.

Outra questão relevante é que as polícias especializadas que investigam estes ilícitos virtuais está no fato que as pessoas que praticam esses crimes, usam terminais ou pontos de acesso a rede mundial de computadores públicos, dificultando a identificação dos agentes.

No que tinge ao acesso e distribuição de conteúdos ilegais via internet, as autoridades tem percebido que os conteúdos são protegidos, pois exigem pagamento para o acesso, portanto se torna mais difícil encontrar pistas de crimes virtuais.

No caso das violações dos direitos de propriedade intelectual, a maior dificuldade enfrentada pelas autoridades policiais é o fato do compartilhamento dos *softwares* na rede mundial de computadores, estarem espalhado em diversos *sites* e

dificultando a busca desse programas que são pagos, mas distribuídos a muitos internautas com fossem *freewares*.

No que cabe aos Provedores - *ISP* (Internet Service Providers), a legislação exige que os fornecedores de serviços de internet preservem os dados informáticos referentes a um sistema informático, ou dados relativos a um cliente por determinado tempo. É um mecanismo que as autoridades possam analisar e mapear rastros para encontrar os culpados.

O combate apenas será possível se cada internauta procurar ferramentas, softwares e sistemas de proteção adequada nas tecnologias por si utilizadas, de modo a evitar invasões que cuminem punições civis e/ou criminais.

6 FORENSE COMPUTACIONAL

Este capítulo abordará a importância da analise forense computacional para identificação dos cibercrimes e os métodos utilizados nas análises.

6.1 Definição

A palavra forense é derivada do latim forensus, que significa "do fórum". E entende-se como a aplicação de técnicas científicas, realizando analise para reconstituição de eventos criminais e obtenção de vestígios, para transformá-los em evidencias. Esta prática envolve pesquisadores, criminalistas e outros profissionais especializados na localização de vestígios. (HISTÓRIA DA INFORMÁTICA FORENSE, 2011) e (CRIME & FORENSICS, 2011).

Os primeiros procedimentos de analise forense foram realizados por médicos, com o intuito de desvendar o motivo das mortes.

Foram criados procedimentos específicos para realizar exames médicos, entrevista com os entes mais próximos, marcas na vítima, ingestão de venenos e temperatura do corpo.

O primeiro laboratório forense foi construído em 1910, Lyon na França pelo cientista forense Edmond Locard, que estabeleceu o principio que por menor que seja a prova do crime, sempre é possível identificá-la e encontrar seu autor, a partir de um simples contato com a cena do crime que pode produzir uma enorme quantidade de rastros. (FONSECA,2011) e (CRIME & FORENSICS, 2011)

Na forense contemporânea tem inicio em 1932, com as técnicas de analise de evidência das cenas do crime. Em 1970 foi utilizado pela primeira vez o laser para identificar as impressões digitais e em 1985, foi realizado o primeiro teste de DNA, que causou uma revolução na medicina forense. (FONSECA,2011)

6.2 Análise Forense Computacional

Diariamente há diversos casos de crimes eletrônicos e a análise forense computacional é o ramo da criminalística, que analisa estes casos

Assim como nas demais classes da análise forense, a computacional utiliza técnicas dentro de um processo legal que envolvem diversos profissionais especializados que são responsáveis pela coleta de dados seguindo uma metodologia de obtenção de provas para que sejam utilizadas judicialmente.

Atualmente já existe um padrão para realização da análise, seguindo as etapas abaixo:

- Obtenção e Coleta de Dados:

A obtenção de dados deve ser formal, seguindo uma metodologia de como obter provas para apresentação judicial.

- Identificação:

Os fatos devem ser separados dos fatores.

- Preservação:

As evidencias extraída deve ser adequadamente manuseada e protegida, para que não sejam danificadas, destruídas ou adulteradas.

- Análise:

Trata-se da analise de todos os vestígios coletados

- Apresentação:

  As evidencias precisam ser enquadradas nos formatos exigidos judicialmente.

Os profissionais precisam estar muito bem preparados para que a análise seja minuciosa e possa ser utilizada judicialmente, pois a coleta errônea de uma prova pode torná-la ilícita ou inválida. (PINHEIRO, 2007).

Além da necessidade de obter as provas seguindo uma metodologia que garantam que todos os dados foram analisados adequadamente, que as provas não foram alteradas e que o possível autor do crime não tenha seus direitos violados.

Abaixo constam, as 5 regras para a evidências eletrônicas, citados (PINHEIRO, 2007)

- Admissibilidade
- Deve ter condições de ser usadas no processo.
- Autenticidade
- Deve ser certa e de relevância para o caso
- Completa (no túnel vision)
- Não pode causar ou levar a suspeitas alternativas
- Confiável
- Sem duvidas sobre a sua veracidade e autenticidade
- Possuir crédito (fazer acreditar)
- Clareza fácil entendimento e interpretação.

7 ATAQUE E FERRAMENTAS DE PREVENÇÃO E ANÁLISE

Este capítulo abordará as principais técnicas existentes para realização de ciberataque, as principais ferramentas utilizadas para prevenção destes ataques e as principais ferramentas e técnicas disponíveis para identificação de cibercrimes.

7.1 Ameaças

Neste tópico será descrito as principais técnicas utilizadas em ciberataques que constituem cibercrimes.

7.1.1 Negação de Serviços (DDOS)

Ataques de negação de serviços são ataques realizados contra um *website* ou serviço via *web*, explorando falhas do protocolo TCP/IP ou outros protocolos de mais alto nível a fim de sobrecarregar o link de dados ou os recursos computacionais da empresa vitima fazendo com que a mesma fique indisponível temporariamente ou permanentemente. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

Empresas que dependem de serviços que devem estar sempre *on-line* são os principais alvos deste tipo de ataque como, por exemplo, bancos, empresas de cartão de credito e comercio eletrônico. O objetivo deste tipo de ataque pode ser o ciber terrorismo, extorsão ou até mesmo espionagem industrial. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

Conforme estatísticas levantadas por uma pesquisa financiada pela *VeriSign* em setembro de 2008 com grandes empresas onde os serviços online são uma parte fundamental do processo de negócios é possível verificar abaixo na FIGURA1 a estatística de ataques de DDoS e na FIGURA2 o impacto financeiro a empresas do segmento financeiro, provedores de internet e comercio eletrônico. (VERISIGN, 2008).

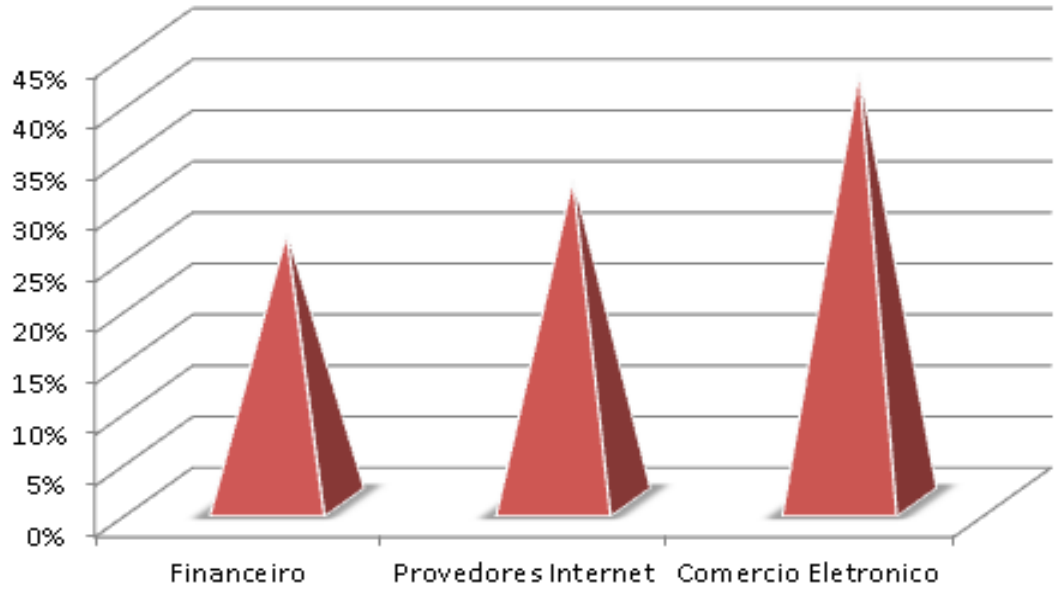


FIGURA1: Percentual de ocorrências de DDoS (VERISIGN, setembro de 2008).

SETOR	RTO	Receita Perdida por cada 1H parada Valores em Mil
FINACEIRO	5Min	240 a 20000
PROVEDORES INTERNET	60Min	5 a 100
COMERCIO ELETRONICO	30Min	190 a 700

FIGURA2: Receita perdida por cada 1 hora com os serviços interrompidos (VERISIGN, 2008).

Conforme definição do US-CERT, (time de resposta a emergências computacionais dos estados unidos), foi definido em 2 de outubro de 1997 três principais formas de ataque de DDoS:

- Esgotamento de recursos computacionais e link de dados;
- Destruição de componentes computacionais e de rede; e
- Alteração de configuração ou informações de componentes de rede.

7.1.1.1 Alteração de configuração ou informações de componentes de rede

Existe uma grande variedade de formas de se realizar este tipo de ataque, e os princípios básicos abaixo podem ser destacados:

- Esgotamento de recursos computacionais e link de dados:

Este ataque explora os recursos básicos para a operação de um computador ou rede de computadores como link de dados, rede local, sistema operacional, espaço em disco do servidor, memória física, utilização de CPU, fornecimento de energia ou refrigeração dos componentes de hardware. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

- Conectividade congestionada:

Nesta categoria de ataque o atacante utiliza-se de um processo para estabelecer conexão ao servidor da vítima, mas interrompe o processo de conexão antes de sua conclusão e em seguida realiza o processo novamente, o resultado é indisponibilidade a conexões legitimas. O atacante não precisa estar em máquina com poder de processamento e link de dados superior ao da vítima, pois o processo consome recursos computacionais envolvidos com o processo de conexão apenas.

- Congestionamento de link de internet:

Este ataque precisa ter origem de vários computadores para ser eficaz e visa consumir todo o link de internet da vítima com o envio de solicitações as quais são respondidas pelo computador vítima intermitentemente.

- Utilização de seus próprios recursos contra você:

Neste caso o atacante faz com que uma máquina realize o envio de uma requisição a outra dentro da mesma rede, que responde e o ciclo reinicia com a máquina que respondeu enviando uma requisição a outra. Isto pode afetar toda a rede conectada a estas duas maquinas. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

- Esgotamento de recursos computacionais:

Atacantes podem implantar softwares maliciosos capazes de atacar processos responsáveis por manter serviços ativos, consumir toda a capacidade da CPU, esgotar o espaço em disco do servidor causando a paralisação do serviço web ou web site hospedado neste servidor. O atacante também pode explorar a trava de contas de usuário por tentativas invalidadas de *login*, digitando senhas incorretas até que todas as contas da rede sejam travadas automaticamente pelo sistema, inclusive a do administrador da rede. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

- Destruição de componentes computacionais e de rede:

O atacante pode se utilizar de falhas ou ausência de controle de acesso a ambientes onde estão os componentes físicos de informática e ter acesso direto aos dispositivos. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

- Alteração de configuração ou informações de componentes de rede:

A falta de segurança em acesso a dispositivos de uma rede, pode proporcionar ao atacante uma grande facilidade de ganhar acesso a rede e realizar modificações em componentes para paralisar a rede, como por exemplo, o acesso a

um gateway de rede para modificar os parâmetros do link de internet. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

7.1.1.2 ICMP Flood

Este tipo de ataque, também conhecido como *Ping flood*, configura-se através de um grande numero de pacotes ICMP enviados a uma maquina que ao tentar responder a todos eles trava ou consome toda a largura de banda do link de internet fazendo com que solicitações verdadeiras enviadas a esta maquina não sejam processadas, este tipo de ataque é mais bem sucedido se o atacante se utiliza de diversos links (hosts) para realizar o envio simultâneo de pacotes ICMP Existe também uma variante deste tipo de ataque, chamada *smurf attack* que explora uma vulnerabilidade na conexão de rede de determinado dispositivo, utilizando-o para replicar envio de pacotes ICMP para dentro da rede via broadcast, os outros pcs da rede interna enxergam os pacotes como provenientes do dispositivo vitima e os respondem fazendo com que a rede interna fique congestionada ou praticamente travada. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

7.1.1.3 Ataques à rede Peer-to-Peer

Este tipo de ataque explora vulnerabilidades de redes DC++ de redes P2P, onde o atacante consegue redirecionar clientes P2P, que não possuem correção para esta vulnerabilidade para o servidor P2P que ele desejar, fazendo com que o site seja sobrecarregado com um número de conexões acima do que foi projetado. Existe maneiras de bloquear ativamente os Ips não autorizados porem o número de IPs a serem bloqueados é muito grande e muitos deles são clientes que rodam em IP dinâmico o que dificulta muito a contenção deste tipo de ataque. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

7.1.1.4 SYN Flood

Este tipo de ataque ocorre quando o atacante envia uma solicitação de conexão incompleta ao servidor vítima, pois o pacote de sincronização de conexão do protocolo TCP/IP, TCP/SYN é enviado com um endereço de remetente inválido e

quando o servidor tenta responder (TCP/SYN-ACK) o mesmo não consegue chegar ao destino, portanto aguarda o *timeout* padrão da resposta da instrução ACK para liberar a conexão. Quando vários pacotes deste tipo são enviados a um dispositivo, ele pode ficar indisponível para conexões legitimas enquanto responde a todos os pacotes. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

7.1.1.5 Botnet e DDoS Distribuído

Um ataque de negação de serviços distribuído pode ser causado de várias maneiras, mas em todas elas um grande número de computadores é utilizado para derrubar um ou mais *web sites* ou serviços de rede.

Softwares maliciosos, como *trojans*, podem infectar maquinas espalhadas pelo mundo todo e utilizá-las em ataques ICMP *Flood* como *fraggle attack*, onde grande quantidade de informação é enviada ao computador destino através do protocolo UPD, todos eles contendo falsa origem e ataques *smurf attack* que são realizados através de envio de pacotes ICMP de conteúdo modificado e falsa origem, para ambos os casos o destinatário consome todo o sua capacidade computacional e link de dados respondendo as falsas comunicações. O intuito deste tipo de ataque é se utilizar do maior número possível de máquinas e links de *internet* para perpetrar um ataque a um ou mais *websites* de uma só vez causando a provável queda do site ou muita lentidão, este tipo de ataque também pode ser chamado de *botnet*. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

7.1.1.6 Ataque de negação de serviços permanente (PDoS)

PDoS é a forma mais destrutiva de ataque de negação de serviços existente, pois é um tipo de ataque que explora vulnerabilidades de dispositivos de rede como por exemplo, um *router*. Através de falhas existentes no *firmware* do dispositivo que permitam o acesso remoto, atacante obtém acesso ao equipamento realiza uma atualização de BIOS ou *Firmaware* inserindo uma versão corrompida no equipamento, que depois de atualizado não mais funcionará e precisará ser substituído ou reconfigurado. Pouco se pode fazer para precaver este tipo de ataque, pois são as vulnerabilidades do equipamento que o permitem acontecer. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

7.1.1.7 Softwares Maliciosos

Softwares maliciosos, como *trojans*, podem atacar um servidor e estações de trabalho consumindo toda capacidade computacional dos equipamentos fazendo com que a rede fique lenta e serviços indisponíveis. Este tipo de ataque não somente é causado por um *hacker* tentando causar danos aos serviços de uma empresa, mas também pode ser causado pelo próprio usuário quando instala programas de origem duvidosos e que pode conter código malicioso. Uma vez infectado o programa age por si só não precisando estar outra pessoa controlando diretamente suas atividades. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

7.1.1.8 Ataque refletido

Este tipo de ataque se baseia no envio de solicitações onde o endereço de origem do atacante é alterado com endereço de origem de um servidor da *web site* ou serviço *web* alvo, ao maior número de computadores possíveis, os computadores que responderem a solicitação enviarão diretamente a vítima escolhida sobrecarregando o sistema e o link de dados do mesmo. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

7.1.1.9 Ataque não intencional

Esta situação ocorre quando várias conexões derrubam ou causam muita lentidão em *web* sites que não estão preparados para grande número de conexões como, por exemplo, um site popular preparado para um grande número de conexões coloca um link para outro site não preparado para isto, caso ocorra acesso em massa dos usuários do site principal ao segundo site não preparado através do link ocorrerá provavelmente à queda deste site secundário. (Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman, 2000)

7.1.2 Malwares

Malwares é o nome dado ao software ou código que causa impactos negativos em sistemas. Eles podem ser utilizados para roubar informação pessoal,

ganhar acesso nao autorizado a um sistema, causar lentidao ou indisponibilidade em sistemas, possibilitar o controle remoto de um computador e outros comportamentos negativos. (Thomas Chen, Jean-Marc Robert, 2004)

Estas ferramentas sempre estão presentes nas ocorrências de crimes da *internet*, pois são atravez delas que os *hackers* conseguem atingir seu objetivo.

Conforme estudo realizado em 2011 pela Universidade da California e o institudo de Estudos Avançados de Madrid, os desenvolvedores de *malwares* agora tem a possibilidade de pagar por serviços PPI (Pay-per-install) para ter seus *malwares* transferidos aos alvos desejados embutidos em programas falsos e *websites* maliciosos, para evitar que os *malwares* sejam capturados durante o seu caminho até as vítmas eles ficam normalmente encapsulados em pacotes que os *antimalwares* nao conseguem detectar. (Thomas Chen, Jean-Marc Robert, 2004)

Podemos dividi-los em categorias como: vírus, worms, trojan horses, spywares, adwares, rootkits e spams e vamos descrever as caracteriscas de cada uma delas. (Thomas Chen, Jean-Marc Robert, 2004)

7.1.2.1 Vírus

Um vírus de computador é basicamente um programa com intensões maliciosas capaz de se replicar dentro de um mesmo computador e espalhar-se por uma ou mais redes de computadores, para disseminar-se o vírus comum tem seu código executavel geralmente mascararado em arquivos de aparencia normal, como por exemplo, um arquivo de imagem JPGE, pode usar diversos meios como, por exemplo, *internet*, rede local e mídias (dvd, disquete ou usb). Portanto para disseminar-se um precisa ser executado pelo usuário e não de forma automatica. (Thomas Chen, Jean-Marc Robert, 2004)

Hoje, na era da informação uma vírus de computador é uma ameça muito grave a empresas e instituições do governo. Um vírus bem projetado pode ser capaz de derrubar os serviços responsaveis por manter a area de negocios de uma empresa e causar milhoes em prejuizo. (Thomas Chen, Jean-Marc Robert, 2004)

A possibilidade da existência de vírus de computadores foi proposta por John Von Neumann através de seu trabalho publicado “Teoria de automatos auto-replicaveis”, onde ele sita como seria possivel criar o um programa de computador que se auto-replique. (Thomas Chen, Jean-Marc Robert, 2004)

O primeiro vírus detectado foi o Creeper vírus, construido por Bob Thomas em 1971 para infectar os computadores DEC PDP-10 executando o sistema operacional TENEX, utilizava a Arpanet como meio de transporte. O único efeito causado por este vírus era a exibição de uma mensagem na tela do computador em períodos pré-agendados. Hoje existem vírus capazes de interromper o funcionamento de toda uma rede. (Thomas Chen, Jean-Marc Robert, 2004)

7.1.2.2 Vírus não residentes

Vírus não residentes são aqueles que não ficam armazenados diretamente como arquivo dentro de um computador, mas dentro de outros programas legítimos ou documentos, para conseguir isto o vírus consegue inserir seu código fonte dentro de programas legítmos fazendo com que a primeira parte carregada, quando o usuários abre o programa, seja o vírus. (Thomas Chen, Jean-Marc Robert, 2004)

Este tipo de vírus é composto basicamente por dois módulos, o primeiro chamado módulo de busca é responsável por encontrar programas ou documentos capazes de se tornar hospedeiros e o segundo chamado módulo de replicação é responsável adicionar o código do vírus ao hospedeiro selecionado. (Thomas Chen, Jean-Marc Robert, 2004)

O ciclo de infecção por vírus não residentes funciona destar forma

- O módulo de busca localiza um programa ou documento alvo;
- O módulo de replicação é ativado;
- O código fonte do vírus é incluído no arquivo alvo;
- Altera o ponto de inicio do código do arquivo para iniciar pelo código malicioso;
- Salva o arquivo.

O resultado desta modificação acima é um arquivo com aparência legítima, mas que contém o código malicioso do vírus embutido, que vai ser executado imediatamente após a execução do arquivo. (Thomas Chen, Jean-Marc Robert, 2004)

7.1.2.3 Vírus residentes

Vírus residentes são aqueles que se instalam no disco rígido do computador ou dispositivo móvel modificam os registros de inicialização dos sistemas operacionais incluindo uma entrada para que sejam inicializados automaticamente a cada reinicio do equipamento. Diferentemente dos vírus não residentes não há módulo de busca para acionar o módulo de replicação, pois o mesmo ja vai subir executando na memória do computador a cada reinicio do mesmo. Uma vez carregado na memoria o módulo de replicação passa a analisar todos os programas em execução em busca de hospedeiros compativeis para infectar. Estes vírus podem ser divididos em duas categorias, vírus de infecção rápida e vírus de infecção lenta. (Thomas Chen, Jean-Marc Robert, 2004)

7.1.2.3.1 Vírus de infecção rápida

Este vírus é destinado a infectar o maior número de arquivos possíveis e devido a este comportamento agressivo é detectado mais cedo pelos anti-vírus, devido ao rápido aparecimento dos danos causados no computador. Além disto pode se utilizar de verficadores de vírus, que nao conseguem eliminá-los, para infectar toda a lista de programas escaneados pela ferramenta anti-vírus. Este tipo de vírus é utilizando quando a intenção é causar muito dano em pouco tempo. (Thomas Chen, Jean-Marc Robert, 2004)

7.1.2.3.2 Vírus de infecção lenta

Este tipo de vírus residente é projetado para manter-se invisivel pelo maior tempo possivel, infectando poucos arquivos e causando dano perceptivel somente com o passar do tempo. Com esta habilidade, este tipo de vírus pode permancer por um longo período de tempo se disseminando para vários computadores entre várias redes sem causar muito dano imediato, mas sim com o passar do tempo. (Thomas Chen, Jean-Marc Robert, 2004)

7.1.2.4 Tipos de infecção

Abaixo seguem os tipos de arquivo e vulnerabilidades exploradas por vírus para infecção de computadores:

- *Scripts* de auto execução com extensão .INF utilizados pelos sistemas operacionais Windows para auto execução de *softwares* e mídias removíveis são substituídos por versões capazes de auto instalar o vírus assim que o dispositivo móvel for conectado ou o programa for executado em computadores com a auto execução ativada. (Thomas Chen, Jean-Marc Robert, 2004)

- Arquivos executáveis, como por exemplo as extensões de Windows COM, CPL e EXE, a extensão Mach-O em MAC OSX e a extensão ELF em Linux podem ter seu contudo modificado por códigos maliciosos. (Thomas Chen, Jean-Marc Robert, 2004)

- Scripts de execução de tarefas como arquivo de lote e scripts de Visual Basic, ambos para Windows e Shell Script para Unix/Linux. (Thomas Chen, Jean-Marc Robert, 2004)

7.1.2.5 Tecnicas para evitar a detecção

Para evitar a sua detecção um vírus pode se utilizar de diversos recursos confome mostramos abaixo:

- Invisibilidade:

Para enganar os *softwares* anti-vírus alguns vírus são capazes assumir o controle de solicitações enviadas ao sistema operacional do computador, portanto quando o antivírus solicitar ao sistema operacional um arquivo para verificar quem vai responder é o vírus com uma versão “saudável” do arquivo. Após a verificação o anti-vírus informa que não há vírus no computador. (Thomas Chen, Jean-Marc Robert, 2004)

- Evitar armadinhas armadas por softwares anti-vírus:

Os softwares anti-vírus costumam criar armadinhas, arquivos executaveis pequenos, em locais estratégicos do sistema operacional, o intuito destes arquivos é servirem de hospedeiro para o vírus, que após infectar o arquivo é automaticamente descoberto e tratado pelo anti-vírus. Alguns vírus por si são capazes de reconhecer estes tipos de arquivo e não infectá-los para continuarem na obscuridade. (Thomas Chen, Jean-Marc Robert, 2004)

- Código fonte dinamico, criptografia e polimorfismo:

Esta técnica consiste no vírus alterar parte de seu código fonte a cada infecção fazendo com que verificações de anti-vírus por assinaturas de vírus não consigam identificar o vírus por completo. Verificações por assinatura de vírus são aquelas onde o fabricante do anti-vírus conhece o vírus, portanto torna o anti-vírus capaz de reconhecer certas partes de seu código fonte em arquivos no computador. Com esta capacidade o vírus pode até ser detectado por um bom anti-vírus porem copias dele podem escapar ilesas da verificação devido à alteração do código fonte. Alguns tipos de vírus conseguem inclusive programar criptografia em seu código fonte polimorfico de forma a dificultar a detecção, neste caso temos dois módulos sendo o primeiro o proprio vírus criptografado e o segundo o módulo de descriptografia utilizado para descriptografar o vírus e criar novas chaves de criptografia. Neste caso o anti-vírus pode detectar o vírus através do módulo de descriptografia, que não é criptografado, mas para dificultar ainda mais as coisas existem vírus que possuem a capacidade aplicar polimorfismo de código no módulo de descriptografia também, o metodo utilizado pelos anti-vírus para detecção destes casos é emulação de ambiente, onde o software anti-vírus emula um ambiente do computador para que o vírus o infecte, cause danos e se mostre. Concluimos então que o vírus poliformico tem a capacidade de alterar parte de seu código fonte mas não o todo. (Thomas Chen, Jean-Marc Robert, 2004)

- Vírus Metamorficos:

Vírus que se utilizam de código metamorfico são capazes de alterar todo o seu código fonte automaticamente a cada infecção tornando-se para o antivírus um vírus completamente diferente, vírus com estas caracteristiscas são muito mais dificeis de serem identificados, pois exigem que o antivírus possua complexos algoritmos que sejam capazes encontrar algum vestigio de variantes conhecidas destes vírus para identificar as novas ameaças. (Thomas Chen, Jean-Marc Robert, 2004).

7.1.2.6 Worms

Um verme (computer worm) de computador é um software que diferentemente do vírus não necessita infectar um arquivo para agir, pois é um programa autonomo capaz de se reproduzir automaticamente, ou seja, sem que o

usuário dispare um comando. Para se disseminar um verme pode utilizar diversos meios. Este tipo de Malware explora vulnerabilidades no sistema operacional para agir. Os sintomas causados por estes malwares são geralmente similares aos causados por vírus porem a grande maioria deles causam problemas que levam a lentidão das conexões de rede.(IEEE Computer Society, 2008).

7.1.2.6.1 Vermes de email

Este tipo de verme chega ao computador da vitma através de emails falsos, as vezes provenientes de contatos conhecidos ja infectados, na forma de anexos ou links para *websites* que disparam a instalação do verme. Uma vez instalado no computador este verme pode acessar a lista de contatos do cliente de email instalado e enviar copias de si mesmo para estes contatos através do próprio cliente de email ou através de cliente SMTP embutido no código fonte do verme.(IEEE Computer Society, 2008)

7.1.2.6.2 Vermes de comunicadores instantaneos

Este verme dissemina-se através de comunicadores instantaneos, chegando ao destino através de uma mensagem com um link, que quanto acessado transfere o verme ao computador. Assim que devidamente instalado este verme ganha acesso a lista de contados do comunicador instantaneo e envia copias para todos os contatos varias vezes, sem o usuário do computador infectado perceba.(IEEE Computer Society, 2008)

7.1.2.6.3 Vermes de internet

Esta categoria de vermes explora vulnerabilidades dos sistemas operacionais e softwares que estão em contato com a internet para ganha acesso ao computador. Ele pode agir em uma rede local ou diretamente pela internet buscando por computadores que possuem as vulnerabilidades que lhes permitem ganhar o controle total do computador, quando conseguir achar uma brecha e infectar o computador ele inicia nova busca.(IEEE Computer Society, 2008)

7.1.2.6.4 Vermes de redes p2p

Este verme infecta computador via redes p2p e coloca uma copia de si mesmo nas pastas que estão compartilhadas para rede p2p, do computador infectado, e utiliza um Trojan Horse, como se fosse um arquivo inocente, como, por exemplo, uma musica muito buscada na rede. Para criar o acesso que o possibilita chegar a outro computador.(IEEE Computer Society, 2008)

7.1.2.6.5 Vermes que trazem beneficios

Existem alguns tipos de vermes que foram criados com boas intensões, como para monitorar diversos tipos de rede em busca de vermes maléficos buscando registrar o seu funcionamento e ajudar na criação ferramentas de detecção e remoção dos mesmos, existem também vermes como a familia de vermes Nachi criados pela Xerox cuja intensão era explorar as vulnerabilidades dos sistemas operacionais Windows e ao encontra-las baixar a correção para as mesmas no site da Microsoft fechando a porta que estava aberta, porem este verme causa grande utilização do link da internet quando liberado em uma grande rede, pois precisa realizar repetidas vezes downloads do mesmo pacote de correção em todas as maquinas com o problema alem de reiniciar a maquina automaticamente, sem o consentimento do usuário ao termino da implantação do pacote. Estes tipos de verme são geralmente raros e por enquanto somente utilizados em ambientes restritos.(IEEE Computer Society, 2008)

7.1.2.7 Outros Malwares de alto risco

7.1.2.7.1 Trojan Horses

O Malware conhecido como trojan é um *software* diferente do vírus e vermes principalmente por ele nao ter a habilidade de criar copias de si mesmo. Sua ação pode trazer alguns danos para o computador, mas seu principal objetivo é agir como um meio de transporte para outras ameaças como vermes e *sywares*, pois ele abre o caminho, no computador, para a entrada destes outros *malwares*. O *Trojan*

também pode abrir caminho para um *hacker* tomar o controle do computador e roubar informações. (Michael Sikorski, Andrew Honig, 2011)

7.1.2.8 Spywares

Spywares são *softwares* desenvolvidos com o intiuito de espionar computadores. Eles são programas minúsculos, que nao causam dano algum ao computador, salvo em casos de lentidão no link de *internet* provocada pelo envio de informações. Estes programas, ao serem instalados ficam escondidos coletando dados dos usuários sem o consentimento dos mesmos como, páginas visitadas, teclas pressionadas do teclado e cliques de mouse em links. Esse pacote de informações é enviado periodicamente para o criador do *Malware*. Para garantir a sua permanência e execução no computador o *malware* insere no registro do sistema operacional vários atalhos, que são acionados no boot da maquina. (Michael Sikorski, Andrew Honig, 2011).

7.1.2.9 Rootkits

Rootkits são tecnologias aplicadas em códigos maliciosos a fim de torná-los invisíveis para os programas anti-malware e para o sistema operacional. Para fazer isto o *malware* que se utiliza desta tecnologia consegue ocultar seus processos do gerenciador de processos do sistema operacional e tomar controle de certas APIs do sistema que podem ser utilizadas por um *software anti-malware* para chegar até o *malware*, tomando o controle destas APIs o anti-malware receberá uma resposta negativa se buscar pelo *malware* no computador. Outra técnica que utilizam é manter sempre uma cópia do processo, com outro nome, rodando junto com o processo principal, ambos mascarados com nomes de processos nativos do sistema operacional, assim caso o processo principal for detectado e derrubado o processo reserva o recupera em uma fração de segundos e vice versa, assim fica muito difícil de interromper as atividades do *malware* . (Michael Sikorski, Andrew Honig, 2011)

7.1.2.10 Blended Threats

Este *malware* envolve uma combinação de diversos tipos de ameaças e diversos tipos de ataque, como vírus, vermes, trojans, adwares, rootkits, todos presentes em um único malware que possui a grande velocidade de replicação de um verme, abre portas e faz *downloads* de novos *malwares* como os *trojans*, infecta arquivos como os vírus, coleta informações do computador como os *adwares* e utiliza-se de tecnicas para ficar invisível e manter-se sempre no computador. Para se disseminar este *malware* pode utilizar-se de todos os meios disponíveis como *email*, comunicador instantaneo, rede local, conexões como VPN e dispositivos removiveis. Uma vez dentro do computador o *malware* toma o controle das APIs necessarias a se manter oculto, desabilita os *softwares anti-malware*, baixa outros *malwares* específicos para causar algum dano em especial ao sistema operacional em execução, coleta informações que envia para o atacante, tudo isso ao mesmo tempo e no menor tempo possivel.(Stuart McClure, Joel Sambray, George Kurtz, 2009)

7.1.3 Web Sites Maliciosos

São geralmente web sites com conteúdo atrativo, utilizados para disseminar *malwares*. Estes *malwares* são transferidos para o computador da vítima assim que a mesma executa conteúdos ativos destes *web sites*. Muitos dos mais poderosos *malwares* utilizam deste meio para ampliar sua disseminação.

Conforme estatísticas da Symantec, segue abaixo o percentual de web sites maliciosos por gênero. (Autor anônimo, 1998)

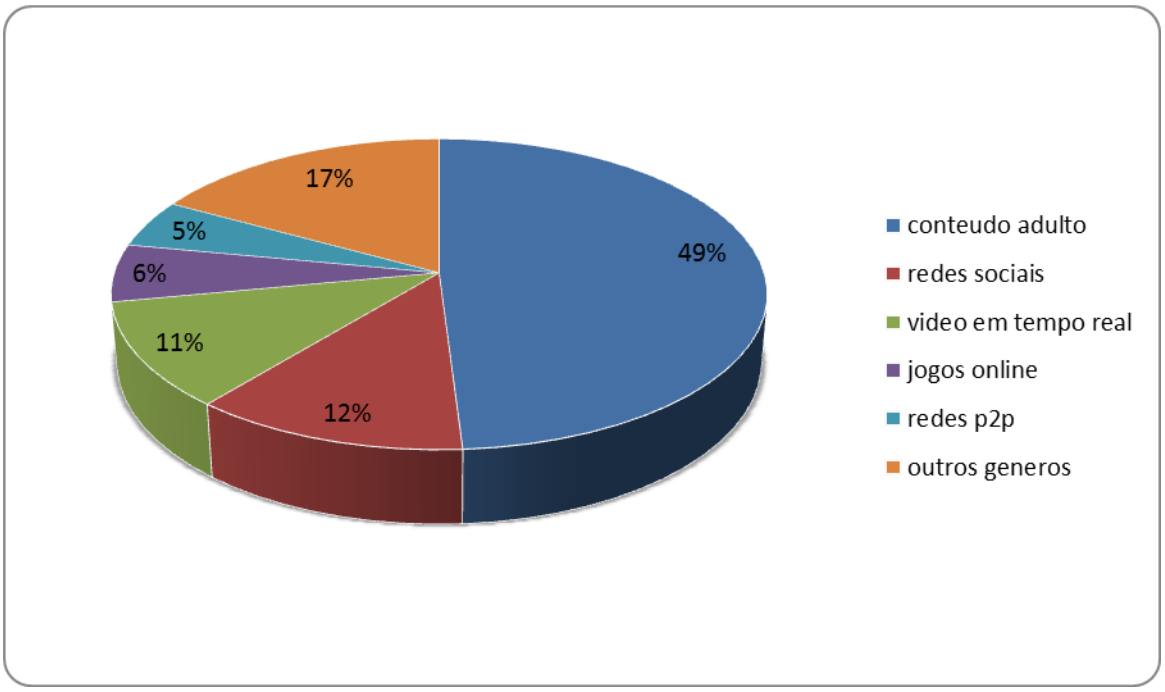


FIGURA 3: Percentual de ocorrências de web sites maliciosos (Symantec Corporation, 2011)

7.1.4 Engenharia Social

Engenharia social é a técnica utilizada por atacantes para manipular pessoas para que as mesmas forneçam inconscientemente informações confidenciais ou realizem tarefas que permitam o atacante a ganhar acesso a uma rede privativa. (Kevin Mitnick, Willian Simon, Steve Wozniak, 2002)

Varias técnicas são utilizadas para este fim e dentre elas podemos destacar:

- Falso suporte tecnico: onde o atacante liga para diversos números de telefone aleatórios informando estar retornando um chamado de suporte técnico, eventualmente ele encontrará uma pessoa que realmente estava esperando o suporte, durante a resolução do problema ele pede a pessoa que faça um *download* ou receba um email que instalará um *malware* que permitirá que o atacante tenha acesso a rede. (Kevin Mitnick, Willian Simon, Steve Wozniak, 2002)
- Familiarização: este caso o atacante vai frequentar o ambiente até que se torne uma pessoa familiar aos outros, assim fica mais fácil de obter informações

sigilosas dos outros, pois as pessoas tendem a ser mais abertas a quem lhes é familiar. (Kevin Mitnick, Willian Simon, Steve Wozniak, 2002)

- Phishing: esta técnica consiste em enviar emails falsos, que no lugar do remetente original estão emails de instituições confiaveis a empresas. O conteudo do email instrui a vítima a responder com informações sigilosas ou acessar um anexo que na verdade é um malware. (Kevin Mitnick, Willian Simon, Steve Wozniak, 2002)
- Deixar uma isca: Esta tecnica consiste em deixar em lugares públicos de uma empresa e que atraiam atenção, mídias removiveis como pen drives ou DVDs, com malwares. Caso estas mídias forem inseridas em um micro da empresa podem iniciar uma infecção em toda a rede (Kevin Mitnick, Willian Simon, Steve Wozniak, 2002).

7.1.5 Penetração de Redes

- Escaneadores de portas: *softwares* com esta característica são capazes de identificar as portas abertas de um host, com este conhecimento o atacante pode projetar melhor o seu ataque. (Autor anônimo, 1998)
- *Sniffers*: estes *softwares*, quando instalados em uma maquina que participa de uma rede consegue monitorar todo o trafego de informações que ocorre na mesma rede, mesmo que este trafego não seja de origem e destino na própria maquina. Isto torna possível para o atacante que consegue implantar a ferramenta dentro da empresa, monitorar informações como senhas digitadas para acesso a sistemas em rede. (Autor anônimo, 1998)
- Quebrar de senhas: esta técnica consiste em se utilizar de métodos para descobrir a senha de acesso a uma rede e é utilizada geralmente em redes sem fio. Existem duas formas de se realizar este tipo de ataque a primeira delas é o chamado ataque de força bruta, que testa todas as possibilidades de senha até localizar a correta, a segunda forma é o ataque por dicionário, onde o atacante utiliza um software que combina palavras do dicionário da língua escolhida fazendo pequenas variações para tentar localizar a senha. A segunda forma consegue localizar a senha mais rapidamente quando a vitima utiliza palavras para compor suas senhas. (Autor anônimo, 1998)

7.1.6 Uso de software pirata

Empresas que se utilizam de softwares piratas, alem de estarem sucetiveis a multas estão colocando sua rede em risco. O risco em si não esta no software mas sim na ferramenta hacker utilizada para remover a ativação que ocorrem quando se compra o software, pois estas ferramentas contem malwares embutidos. Para piratear um software através destas ferramentas o usuário é obrigado a desativar seu anti-malware temporariamente, o que abre caminho para o malware provocar a infecção do computador. (Paul Craig, Mark Burnett, 2005).

7.2 Ferramentas de Prevenção

7.2.1 Anti-Malware

Esta categoria de software evoluiu do simples anti-vírus e é utilizado para realizar a proteção em tempo real e busca por ameaças que podem ser vírus, vermes, spywares, trojans e outros malwares. (Autor anônimo, 1998)

Existem quatro métodos utilizados por estes softwares para identificar malwares, que podem eventualmente ser combinados. (Autor anônimo, 1998)

- Busca por malwares a partir de definições já conhecidas

Este tipo de detecção se utiliza de uma lista de malwares já identificados pelo desenvolvedor do software, portanto o software possui uma instrução especifica de como remove-lo. Este método protege apenas contra malwares já conhecidos pela ferramenta e não é eficaz contra códigos polimórficos e metamórficos devido a capacidade de mutação dos mesmos. (Autor anônimo, 1998)

- Busca com definições genéricas

Neste caso o software é capaz de detectar variantes de malwares polimórfico e metamórfico a partir de definições genéricas, ou seja, caso exista em sua lista de malwares um exemplar que seja semelhante. Para realizar esta tarefa o software anti-malware busca padrões de comportamento de ameaças que ele já conhece. (Autor anônimo, 1998)

- Busca com Heuristicas

Esta tecnologia busca por padrões de funcionalidade que não estão presentes em programas legítimos como por exemplo a capacidade de se replicar.

Com isto, o anti-malware é capaz de observar um processo em execução e comparar as atividades que este realiza perante uma lista de regras que os códigos maliciosos seguem, caso localize o comportamento improprio o processo será notificado como malware. (Autor anônimo, 1998)

- Emulação de ambiente real

Esta técnica utilizada em conjunto com a busca por heurísticas proporciona que o software mova o possível malware para um ambiente virtual e o deixe agir, para tentar localizar algum comportamento que possa classifica-lo como ameaça, fazendo isto, o possível malware não afeta os arquivos verdadeiros durante o processo. (Autor anônimo, 1998)

7.2.1.1 Funcionalidades disponíveis nos anti-malwares.

- Proteção em tempo real

Este módulo do software anti-malware é responsável por analisar o trafego de informações no computador como, processos carregados na memoria, informações que trafegam pela interface de rede e dados armazenados em dispositivos removíveis localizando e bloqueando os processos maliciosos antes que alcancem seus objetivos. (Autor anônimo, 1998)

- Busca por malwares

Responsável por realizar as buscas por processos, registros e arquivos que possam conter código malicioso ou ferramentas maliciosas. Ao localizar ameaças, dependendo do tipo, este módulo pode ser capaz de reparar arquivos para seu estado original ou apenas excluir toda ameaça que encontrar. (Autor anônimo, 1998)

- Alertas

Este módulo é responsável por notificar o usuário quando algo errado é localizado pelos módulos de proteção em tempo real e buscas por malware. (Autor anônimo, 1998)

- Atualização de definições

Como a cada dia surgem novas ameaças o software precisar receber definições de malwares da fabricante para que possa ser eficaz contra novos tipos de malwares. (Autor anônimo, 1998)

- Quarentena

Este sistema cria um ambiente virtual dentro do computador, onde arquivos suspeitos de serem malwares são colocados para que possam agir sob monitoramento do anti-malware, revelando assim para o mesmo a sua verdadeira intenção sem causar danos ao computador. Caso o arquivo em quarentena seja considerado malicioso o mesmo será removido caso contrario será restaurado ao seu local original. (Autor anônimo, 1998)

7.2.2 Firewall

Podemos classificar os firewalls conforme os tipos a seguir:

- Firewall de primeira geração: Filtro de pacotes

Este firewall possui um filtro que permite o bloqueio e liberação de pacotes, onde podemos especificar qual o protocolo utilizado, TCP, UDP ou ambos e destes protocolos especificamos quais portas das 65535 de cada protocolo devem estar abertas para acesso externo para rede interna ou acesso interno para rede externa. Podemos também estabelecer que determinadas portas estejam abertas apenas para determinados hosts para acesso externo e vice versa.

O firewall de primeira geração trabalha entre a camada de rede e camada de conexão física do modelo OSI. (Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2000)

- Firewall de segunda geração: Filtro de estado

Este tipo de firewall geralmente é utilizado em conjunto com o filtro de pacotes para adicionar funcionalidades no mesmo, como a capacidade de identificar se um pacote esta iniciando uma nova conexão, se faz parte da conexão existente e se é um pacote invalido para a conexão existente. Com isso o firewall consegue interceptar trafego malicioso durante a transferência de vários pacotes de uma conexão.

Outra capacidade deste firewall é que ele realiza o armazenamento em memoria de todos os pacotes transferidos durante uma conexão para que sejam combinados e analisados em busca de códigos maliciosos antes que cheguem ao destino final dentro da rede. (Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2000)

- Firewall de terceira geração: Gateway de aplicações

Este é o firewall mais inteligente, pois consegue entender e monitorar o trafego de aplicativos em suas determinadas portas garantindo que o trafego gerado por estes aplicativos sejam legítimos e consegue também analisar se os protocolos não estão utilizando portas fora dos padrões destes e realizar bloqueios nestes casos.

Algumas ferramentas desta geração ainda são capazes de trabalhar com definições intrusões que funcionam conforme as definições de malware de um anti-malware, que são baixadas da fabricante da ferramenta para instruir o firewall sobre como identificar e bloquear novos comportamentos suspeitos e novos métodos de negação de serviço.

Outra grande vantagem deste firewall para redes empresariais é que ele permite que criemos perfis de usuários com determinados níveis de acesso a portas e conexões enquanto os outros anteriores eram aplicados em toda rede. (Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2000)

Os firewall gateway de aplicações ainda possuem variações conforme a seguir:

- Proxies

Este firewall age conforme o anterior porem com funcionalidades extras fazendo também, o armazenamento do conteúdo acessado externamente pelos usuários a fim de acelerar os próximos acessos, pois o mesmo consegue verificar se determinado conteúdo não sofreu alteração e oferecer ao usuário, quando houver necessidade, o conteúdo armazenado na memoria sem que haja necessidade de baixa-lo novamente. Outra funcionalidade é que este firewall é capaz de criar um histórico de conteúdos acessados pelos usuários com informações detalhadas como tempo gasto por conteúdo acessado. Alguns proxies mais avançados também adicionam a lista de funcionalidades um filtro de conteúdo que permite restringir determinado usuário de acessar determinados tipos de conteúdo na web. (Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2000)

- NAT

Este firewall além das funcionalidades da terceira geração realiza a ocultação dos endereços IP da rede local pois externamente será visto apenas como

um IP, o IP publico. Outra grande utilidade deste firewall é reduzir a necessidade de uma grande empresa de ter vários IPs públicos. (Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2000)

7.2.3 Tecnologias de firewall.

- DMZ – zona desmilitarizada

Esta tecnologia foi criada para permitir que seja possível colocar um ou mais hosts internos em uma área onde o firewall não esta atuando com a máxima proteção, esta técnica é útil quando precisamos prover serviços tanto para rede externa quanto para rede interna e o firewall normalmente bloquearia este tipo de trafego, para garantir a segurança o firewall realiza a analise do trafego entre as maquinas na DMZ e a rede protegida. (Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2000)

Os serviços de VOIP são um exemplo que se utilizam da DMZ, pois um router normalmente interpreta pacotes VOIP como negação de serviços devido a grande quantidade e pouco intervalo, realizando o bloqueio do mesmo. Com o equipamento que prove o VOIP inserido na DMZ o firewall passa a ignorar certas regras entre o trafego externo para este equipamento, não mais bloqueando os serviços. (Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2000)

- Back to Back Firewall

Este modelo de firewall implementa muito mais segurança para a DMZ pois utilizamos dois firewalls de gateway de aplicativo para proteção da rede, sendo o primeiro deles esta ligado a DMZ e ao segundo firewall e possui regras que permitem certo trafego de informações entre rede externa e maquinas da DMZ. O Segundo firewall vai possuir regras diferentes e mais rígidas impedindo que o atacante, caso consiga passar pelo primeiro firewall, de chegar a rede interna. (Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2000).

7.3 Ferramentas de Analise e Identificação

Estas ferramentas são aplicadas para identificar um fato que ja ocorreu e nao para prevenir crimes virtuais.

O profissional que vai se utilizar destas ferramentas deve possuir conhecimento em sistemas operacionais e tecnologias de rede e arquivos para corretamente manusear as ferramentas. (FREITAS, 2006),

7.3.1 Manutenção da integridade de arquivos

Para que uma investigação possa ser realizada em arquivos armazenados em um computador é necessário que as informações sejam preservadas, para garantir isto técnicas podem ser aplicadas aos arquivos como a técnica de Hash, que se utiliza de formulas complexas para criar combinações de letras e números que referenciam o arquivo analisado no momento em que foi analisado. Caso haja adulteração no arquivo será possível, ao gerar nova analise com a ferramenta de HASH, identificar que a combinação mudou. (FREITAS, 2006)

Adotando este procedimento com a realização de uma copia das informações analisadas em local seguro, é possível conduzir uma investigação sem que haja duvidas da veracidade dos dados utilizados. (FREITAS, 2006)

7.3.2 Recuperação de arquivos

Para que seja possível recuperar dados deletados de forma proposital do computador periciado existe uma serie de ferramentas capazes de analisar o disco rígido em busca de arquivos ainda não sobrescritos, pois quando são deletados, os arquivos ainda permanecem no disco, o que acontece é que o sistema operacional intende que pode gravar por cima dos dados que estão naquele setor. Caso estes dados tenham sido sobrescritos a informação não pode mais ser recuperada, portanto é de extrema importância que esta ferramenta seja executada para periciar arquivos deletados antes de rodar qualquer outro tipo de teste no equipamento apreendido.

7.3.3 Ferramentas de forense computacional

Estas ferramentas são aplicativos profissionais para se realizar perícias em computadores como a ferramenta EnCase® Forensic que consegue realizar todas

as funções necessárias para se extrair arquivo de forma ou recuperar informações apagadas de segura e legal. Por serem ferramentas oficiais já utilizadas por forças policiais, informações e evidências coletadas com elas tem um valor judicial e podem ser utilizadas como prova de crimes. (FREITAS, 2006)

8 DIREITO DIGITAL

O Direito Digital é o conjunto de regras, legislações, jurisprudências e códigos que regem a conduta e a maneira de agir e a relação entre as pessoas e a sociedade, cujo meio de ocorrência ou a prova da manifestação de vontade seja o digital, ou digital até o presencial, ou do presencial para o digital, criando provas ou rastros eletrônicos que representam os fatos ocorridos e sua possível autoria. Portanto, reune princípios que vão ao encontro da realidade social não presencial, interativo e em tempo real. O Direito Digital é a evolução do próprio direito, porém que assiste as relações e os fatos eletrônicos sob o aspecto da legalidade, moralidade e impessoalidade e que atenda as necessidades a nova sociedade da informação (PINHEIRO, 2010).

Direito Digital é uma ramificação do Direito que estuda as relações do homem com o computador e o meio eletrônico (ciberespaço), e o uso da Internet como tecnologia da informação com os aspectos jurídicos, por isso, é um ramo do Direito em constante mudança e sempre se inovando.

O Direto Digital também chamado como Direito da Sociedade da Informação, Direito Eletrônico, Direito da Informática, Direito Informático, Direito Cibernético, Direito da Internet ou Direito da Tecnologia da Informação (ALMEIDA FILHO, 2005).

8.1 Ausência de legislações para infrações digitais.

As infrações digitais são alvo de muitas discussões e projetos de leis que tramitam no congresso nacional. Porém, não existe ainda o código do direito digital.

Estudiosos comentam que há necessidade de um código para o direito da informática, outros apontam que a informática seria mais um ramo do direito penal e processual penal a ser agregado a legislação brasileira.

Adiante, será abordados a coleção de leis, artigos, normas, jurisprudências e entendimentos sobre o direito e o meio digital que servem nos dias de hoje para os julgamentos e embasamentos legais defendidos nos tribunais no mundo e no Brasil.

O projeto de Lei 84/89, do deputado Eduardo Azeredo (PSDB/MG), é um projeto de lei tramitando na Câmara dos Deputados e Senadores, trata-se de um texto legislativo sobre *cybercrime* no país, o substitutivo apresentado pelo Senador Eduardo Azeredo, com a assessoria do Doutor José Henrique Santos Portugal, obteve três projetos de lei que já tramitavam nas casas dos Deputados Federais e Senadores, para tipificar condutas realizadas mediante mal uso de sistema eletrônico, digital ou similares, de rede de computadores, dispositivos de comunicação, telecomunicação ou sistemas informatizados e similares, e dá outras providências. São eles:

- PLC 89, de 2003, do Deputado Luiz Piauhylino, que altera o Código Penal (CP), Decreto-Lei nº. 2.848, de 7 de dezembro de 1940 e a Lei de Interceptações Telefônicas, Lei nº. 9.296, de 24 de julho de 1996.
- PLS 76, de 2000, do Senador Renan Calheiros, nos termos do Substitutivo, altera as duas leis acima e mais o Código Penal Militar (CPM), o Decreto-Lei nº. 1.001, de 21 de outubro de 1969, o Código do Processo Penal (CPP), Decreto-Lei nº. 3.689, de 3 de outubro de 1941, a Lei da Repressão Uniforme, a Lei nº. 10.446, de 8 de maio de 2002 e o Código do Consumidor, Lei nº. 8.078, de 11 de setembro de 1990.
- PLS 137, de 2000, de autoria do Senador Leomar Quintanilha, que determina o aumento das penas ao triplo para delitos cometidos com o uso de informática.

Neste projeto do deputado Eduardo, iniciante no assunto, a pauta das condutas que passam a ser consideradas como crime conta com 11 tipificações:

1. Roubo de senha;
2. Falsificação de cartão de crédito;
3. Falsificação de de número de celular ou meio de acesso;
4. Calúnia, difamação e injúria;
5. Difusão de código malicioso para causar dano;
6. Acesso não autorizado;

7. Obtenção não autorizada de informação e manutenção, transporte ou fornecimento não autorizado de informação;

8. Publicação não autorizada de informações obtidas em banco de dados;

9. Furto qualificado;

10. Atentado contra a segurança de serviço de utilidades públicas; e

11. Ataques a redes de computadores.

O substitutivo inclui também sugestões apresentadas por especialistas em audiências públicas realizadas no Congresso Nacional (CN) para o debate do assunto e outras emendas apresentadas durante em sessões no Senado Federal. Entre elas a emenda número 3 da (Conselho de Justiça) CCJ, do senador Valter Pereira (PMDB-MS), que versa sobre a Lei Afonso Arinos (que proíbe a discriminação no Brasil), passa a abranger os crimes de discriminação de raça e de cor cometidos na rede internet.

No total, o projeto recebeu vinte e quatro (24) emendas. Segundo o deputado, a aprovação da proposta de lei é o objetivo dos palarmentares entendidos sobre o assuntos, que vê essa PLC como uma maneira de aumentar a segurança no de novas tecnologias no Brasil.

O projeto de lei se aprovado, não mais persistirá a ausência de formas de crimes penais específicos para as condutas delituosas, não deixará a possibilidade para dúvidas sobre o enquadramento de tipos de crimes como o furto e o estelionato.Ou seja, as delegacias, e os tribunais, terão o normativo para ser utilizado para os casos apresentados no dia-a-dia.

A criminalização desses atos em harwares e redes deverá ter como contrapartida os ajustes no direito civil, que crie penalidades de ordem financeiras e outras, e que defina a materialidade dos direitos e obrigações na esfera virtual. O grupo que contribuiu para os ajustes da PLS 76/2000 já estão observando as novidades e atualidade, de modo entre a responsabilidade civil e a penal. Somando a isto o quadro regulatório, em que já proliferam as exigências de segurança e as penalidades (LUCA, 2011).

8.2 Analogia de leis vigentes para infrações digitais

A Convenção sobre o Cibercrime, celebrada em Budapeste, Hungria, a 23 de novembro de 2001, pelo Conselho da Europa, teve como signatários 43 países

europeus e ainda Estados Unidos, Canadá e Japão. Cada Estado que assinou ratificaram as disposições constantes da Convenção em suas constituições internas.

A Convenção recomenda processuais penais, a guarda cuidadosa das informações trafegadas na rede mundial de computadores e sua liberação para cumprir os objetivos da Convenção. Além disso, trata da necessária cooperação internacional, das questões de extradição, da assistência mútua entre os Estados, da denúncia espontânea e sugere procedimentos de acordos internacionais específicos, além da da confidencialidade e limitações de uso. Define também a admissão à Convenção de novos Estados por convite e a aprovação por maioria do Conselho.

A legislação brasileira em vigor tipifica os crimes identificados pela Convenção, como os crimes contra os direitos do autor e crimes de pedofilia, e, caso a caso, cuida de alguns outros tipificados no Código Penal. Abaixo, está a relação dos tópicos da Convenção de Budapeste comparada com a legislação brasileira adequada, e legislação penal estadual deve ter o seu relacionamento na legislação do Brasil:

Segue a Convenção de Budapeste relacionado com os artigos das leis ou códigos brasileiros:

- Acesso ilegal ou não autorizado a sistemas informatizados:

154-A e 155 4º,V do CP339-A e 240 6º,V do CPM

- Interceptação ou interrupção de comunicações:

Art. 16 do Substitutivo

- Interferência não autorizada sobre os dados armazenados:

154-D, 163-A e 171-A do CP339-D, 262-A e 281-A do CPM

- Falsificação em sistemas informatizados:

163-A, 171-A, 298 e 298-A do CP262-A e 281-A do CPM

- Quebra da integridade das informações :

154-B do CP339-B do CPM

- Fraudes em sistemas informatizados com ou sem ganho econômico:

163-A e 171-A do CP262-A e 281-A do CPM

- Pornografia infantil ou pedofilia:

241 da Lei 8.069, de 1990, Estatuto da Criança e do Adolescente (ECA), alterado pela Lei 10.764, de 2003;

- Quebra dos direitos de autor:

Lei 9.609, de 1998, (a Lei do Software), da Lei 9.610 de 1998, (a Lei do Direito Autoral) e da Lei 10.695 de 2003, (a Lei Contra a Pirataria);

- Tentativas ou ajudas a condutas criminosas; e

154-A 1º do CP339-A do CPM

- Responsabilidade de uma pessoa natural ou de uma organização

Art. 21 do Substitutivo

Penas de privação de liberdade do indivíduo e de penalidades de ordem econômica, penas com detenção ou com reclusão, maior gravidade, e/ou multa conforme o caso, com agravantes e outras equiparações e em leis citadas.

O Conselho da Europa consiste em 44 Estados-membros. Instituíndo-se em 1949 como fórum para o fortalecimento dos direitos do indivíduo, e para promover a democracia e o bem estar entre os Estados membros na Europa. Ao decorrer dos tempos, o Conselho da Europa instituído como fórum de negociação para convenções específicas de crimes.

A Convenção contra o crimes eletrônicos, em seu texto, descreve conceito de normas de direito pelos países-membros sobre os direitos e deveres da população emanados pelos países-membros e as suas liberdades, ressalta-se os assuntos de direito de privacidade, intimidade, expressão, acesso a informação e a rede mundial de computadores (FARMER,2007).

8.3 Provas eletrônicas

Deve-se primeiro chegar em um conceito aceitável do que é documento eletrônico, devido a idéia inicial sobre documento está relacionado a materialização em papel.

Segundo o direito civil. *“a) escrito oficial que identifica uma pessoa; b) instrumento escrito que, juridicamente, faz fé daquilo que atesta, tal como contrato, escritura pública, certificado, atestado, recibo, título etc.”; direito processual civil e direito processual penal. “a) Qualquer escrito oferecido em juízo que forneça prova de alegação do litigante; b) qualquer fato que possa comprovar ou testemunhar algo”*.

Os códigos de civil, de processo penal e de processo civil explicam sobre o que é documento com o papel, entretanto, falta melhor definição sobre documento eletrônico, portanto em outra citação explica “qualquer fato que possa comprovar ou testemunhar algo”, concluímos que as provas no direito informático estão nos computadores e máquinas, então o hardware se torna uma testemunha relevante.

Um documento gerado no meio digital é o original, a impressão, portanto é uma é um retrato impresso.

Segundo PL 2644/96 no artigo 1, defini “*documento eletrônico como todo documento, público ou particular, originado por processamento eletrônico de dados e armazenamento em meio magnético, optomagnético, eletrônico ou similar*”.

No PL 4906/01 defini documento eletrônico, como:

“*Art. 2º Para os efeitos desta lei, considera-se:*

I – documento eletrônico: a informação gerada, enviada, recebida, armazenada ou comunicada por meios eletrônicos, ópticos, opto-eletrônicos ou similares;”

Portanto, a fotografia digital também se equipara como documento digital, ou seja, é um documento de cunho eletrônico.

O documento eletrônico possui duas prerrogativas para que tenha força nos processos:

Autenticidade: É um processo que garante através do meio que ateste o real autor do documento eletrônico trafegado em redes ou sistemas eletrônicos. O documento digital que é autêntico é o que não deixa suspeita quanto ao remetente e a sua autoria.

Integridade: Prova que o documento eletrônico após o seu tráfego na rede mundial de computadores ou em sistema eletrônicos que não houve alteração não autorizada de sua integra literal. O documento eletrônico sem alterações é aquele que foi emitido pelo remetente e recebido pelo destinatário sem qualquer alteração.

Os dois conceitos e requisitos acima são usados comumente em países versão sobre o direito digital e sobre o documento eletrônico.

A partir da definição documento eletrônico, os tribunais se preocupam como esse documento digital serviram como prova em processos:

Criptografia é palavra originada da criptologia que é a ciência que reúne e estuda as técnicas matemáticas, computacionais e outras técnicas necessárias à criptoanálise (solução de criptograma) e à criptografia (escrita codificada).

Iniciou-se os estudos no meio militar e para ser utilizada como ferramenta para envio/recebimento de mensagens confidenciais durante a guerra. Democratizou-se nas transações do comércio eletrônico, onde as transações acontecem de maneira segura, as técnicas de criptografia cada vez mais se aprimoram, a criptografia comum atualmente é assimétrica, explicada adiante.

Projeto de Lei 4906/01 define o que é criptografia assimétrica, "*modalidade de criptografia que utiliza um par de chaves distintas e interdependentes, denominadas chaves pública e privada, de modo que a mensagem codificada por uma das chaves só possa ser decodificada com o uso da outra chave do mesmo par*;"

O *Utah Signature Act*, que é a primeira legislação sobre o assunto, defini *digital signature* (assinatura digital) como uma seqüência de bits criada, através de uma função one-way, em relação a uma mensagem claramente delimitada, que encriptará o resultado utilizando-se da criptografia assimétrica e uma chave privada. A de criptografia assimétrica (assinatura digital), cabe ao remetente da informação ou do documento eletrônico, portador de uma chave privada, manter a mesma em segredo, desta forma outras pessoas não poderão ler, alterar ou excluir atos e/ou negócios jurídicos em seu nome.

A criptografia RSA é um algoritmo para codificar, e foi dado com esse nome em homenagem de seus criadores. Os professores da instituição MIT são Ron Rivest, Adi Shamir e Len Adleman. Atualmente a RSA é a melhor criptografia assimétrica, que se baseia na Teoria Clássica dos Números, portanto tornou-se o

mais seguro código de criptografia assimétrica que possibilita a codificação e assinatura digital, comumente usado no Brasil como chave pública.

Certificado Digital tem sempre uma autoridade certificadora e autoridade credenciadora, todos estes conceitos se encontram no Projeto de Lei 4906/01 no artigo 2:

"*IV – autoridade certificadora: pessoa jurídica que esteja apta a expedir certificado digital;*

V – certificado digital: documento eletrônico expedido por autoridade certificadora que atesta a titularidade de uma chave pública;

VI – autoridade credenciadora: órgão responsável pela designação de autoridade certificadora raiz e pelo credenciamento voluntário de autoridades certificadoras."

Na Medida Provisória 2200/02 que instituiu a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), descrita no artigo 1 "*para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras*."

Já no artigo 10, parágrafo 1, consta a presunção de veracidade dos documentos eletrônicos com o uso de processo de certificação disponibilizada pela ICP-Brasil. Os documentos assinados digitalmente tem valor comprobatório definido no Código de Processo Civil no artigo 334:

"*Art. 334.Não dependem de prova os fatos:*

I – notórios;

II – afirmados por uma parte e confessados pela parte contrária;

III – admitidos, no processo, como incontroversos;

IV – em cujo favor milita presunção legal de existência ou de veracidade."

Um dos princípios do contrato eletrônico é o do não repúdio, ou seja, é inválida qualquer alegação no que cinge ao suporte do contrato. Como contrato eletrônico "é um documento eletrônico" seria ilógico não aplicarmos mesmo princípio ao documento eletrônico.

O Código Civil em seu artigo 225:

"*As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, lhes impugnar a exatidão*"

O documento eletrônico, produzido em computadores, pode ser usado como evidência, mesmo não assinado digitalmente, por exemplo, casos de apreensões de hardwares, onde há informações em discos rígidos, mesmo não sendo uma prova , mas serve como elemento nos julgamentos de tribunais de cuidam de cibercrimes atualmente(PINHEIRO, 2010).

9 CONSIDERAÇÕES FINAIS

A internet tornou-se uma ferramenta imprescindível nos dias de hoje, pois é uma ferramenta indispensável para quem deseja continuar no mercado de negócios.

A medida de surgem novas tecnologias, novas ameaças e novos tipos de crimes também surgem apesar desta evolução tecnologia propiciar mais ferramentas para garantir a segurança da informação, este desenvolvimento não é suficiente para conter a criatividade humana.

Por este motivo estaremos sempre a mercê de pessoas mal intencionadas que através da internet podem cometer os mais variados tipos de crime como a negação de serviços, roubo de informações e outros tipos de ataque.

Surge ai a necessidade de se realizar uma pericia após a ocorrência de ataques, pois somente um trabalho bem elaborado de coleta de informações torna possível o entendimento do mecanismo e técnicas empregadas em cada crime.

Este entendimento propicia-nos adotar a correta forma de prevenção ou correção da vulnerabilidade.

A pericia também deve coletar as informações pertinentes ao crime ocorrido visando transformar estas evidências em provas utilizando as ferramentas de análise da forense computacional e equiparar a ocorrência as leis vigentes buscando criminalizar o autor.

A interpretação deste tipo de crime pelo julgador é imprevisível, pois não possuímos leis especificas para o assunto, porém diante dos novos tempos esta interpretação esta mudando.

10 REFERÊNCIAS BIBLIOGRAFICAS

ALMEIDA FILHO, José Carlos de Araújo. **Manual de Informática Jurídica e Direito da Informática**. Rio de Janeiro: Forense, 2005.

AUTOR ANÔNIMO. **Segurança Máxima**. Tradução da 2ª ed. Campus: Rio de Janeiro, 2000.

BRASIL, Cyclades. **Guia Internet de Conectividade**. 7ª ed. São Paulo: Senac, 2001.

BRASIL, **Decreto-Lei 2.848 de 07 de dezembro de 1940**. Dispõe sobre o Código Penal. Diário Oficial [da] República Federativa do Brasil, Brasília, 7 dez. 1940.

BRASIL, **Lei 7716 de 05 de janeiro de 1989**. Dispõe sobre os crimes resultantes de preconceito de raça ou de cor. Diário Oficial [da] República Federativa do Brasil, Brasília, 5 jan. 1989.

BRASIL, **Constituição Federal de 1988 de 05 outubro de 1988**, no artigo 5º. Dispõe sobre a Carta Magna do Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, 5 out. 1988.

BRASIL, **Lei 8.069 de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, 13 jul. 1990.

BRASIL, **Lei 9.296 de 24 de julho de 1996**. Dispõe sobre regulamentação do inciso XII, parte final, do art. 5° da Constituição Federal. Diário Oficial [da] República Federativa do Brasil, Brasília, 24 jul. 1996.

BRASIL, **Lei 9.609 de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, 19 fev. 1998.

BRASIL, **Lei 9.279 de 14 de maio de 1996** . Dispõe sobre direitos e obrigações relativos à propriedade industrial. Diário Oficial [da] República Federativa do Brasil, Brasília, 14 mai. 1996.

BRASIL, **Lei 9.605 de 12 de fevereiro de 1998**. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, 12 fev. 1998.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2000.

CRIME & FORENSICS, Disponível em: <http://www.yourdiscovery.com/crime/_home/index.shtml>. Acesso em: 06 dezembro 2011.

DR SOLOMON´S SOFTWARE, ED 5.1, **Dr. Solomon´s vírus encyclopedia, 1997 IEEE COMPUTER SOCIETY, Dependable and secure computing, IEEE Transaction,** volume 5, Aylesbury : Dr. Solomon's Software, 2008)

ZWICKY, Elizabeth D, COOPER Simon, CHAPMAN, Brent D. **Building Internet Firewalls**. 2 ed. O´Reilly,2000.

FARMER, Dan; VENEMA, Wietse, **Perícia forense computacional:** Teoria e Prática Aplicada. São Paulo: Pearson Prentice Hall, 2007.

FONSECA, Fernando. **Segurança Objetiva**. Disponível em: <http://segurancaobjetiva.wordpress.com/2011/05/09/a-historia-da-forense/>. Acesso em: 04 dezembro 2011.

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada a Informática.** Rio de Janeiro: Brasport, 2006.

GOLDMAN, Alfredo.Disponível em: <http://grenoble.ime.usp.br/~gold/cursos/2008/movel/gradSemCorrecao/FelipeBulleC.pdf.> Acesso 04 dezembro 2011.

GOMES, Flávio Luiz. **IBCCRIM: Instituto Brasileiro de Ciências Criminais**. Disponível em: <www.direitocriminal.com.br>. Acesso em 26 outubro. 2011.

HISTÓRIA DA INFORMÁTICA FORENSE. **DATA RECOVER CENTER.** Disponível em: http://www.datarecovercenter.pt/historia-informatica-forense?_Locale=pt Acesso em: 06 dezembro 2011.

MORVILLE, Peter**. Information Architecture for the World Wide Web**. 3º ed. Louis Rosenfeld, US: O'Reilly Media, 2006

JEFFREY T POLLOCK. **Semantic Web For Dummies**. US: John Wiley & Sons, 2009

KEVIN MITNICK, WILLIAN SIMON, STEVE WOZNIAK, **The art of deception**, US : Wiley, 2002.

LUCA, Cristina de. **Convergência Digital -Circuito**.Disponível em:<http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=21&infoid=11565&sid=54>. Acesso em 30 de outubro de 2011

MICHAEL SIKORSKI, ANDREW HONIQ**, Practical Malware Analysis,The Hands-On Guide to Dissecting Malicious Software**, ed 1, US : No Starch Press,US, 2011).

PAUL CRAIG, MARK BURNETT, **Software Piracy Exposed**, Waltham : syngress,2005

PINHEIRO, Reginaldo César. **Os crimes virtuais na esfera jurídica brasileira**. São Paulo: IBCCrim, 2010.

ROSA, Fabrízio. **Crimes de Informática**. 3ª ed. Campinas: Bookseller, 2007.

S. DEERING, R. Hinden **RFC 2460, Internet Protocol, Version 6 (IPv6) Specification,** 1998. Disponivel em http://www.ietf.org/rfc/rfc2460.txt, acessso em 30 de outubro de 2011.

SMITH, LUCIE; LIPNER, IAN (3 February 2011). **Free Pool of IPv4 Address Space Depleted. Number Resource Organization**. Disponivel em : http://www.nro.net/news/ipv4-free-pool-depleted, acesso em 22 de novembro de 2011.

SOBRAL, Adail. **Internet na Escola**. 2ª ed. São Paulo: Loyola, 2001.

STUART MCCLURE, JOEL SCAMBRAY, GEORGE KURTZ, **Hacking Exposed**, Ed 6 **Blacklick** : McGraw-Hill Osborne Media, 2009

THOMAS CHEN, JEAN-MARC ROBERT**, The evolution of Víruses and Worms.** Disponivel em : http://vxheavens.com/lib/atc01.html, acesso em 28 de novembro de 2011.

TIM O'REILLY, 2005. **What Is Web 2.0 - O´Reilly Media**. Disponível em < http://oreilly.com/web2/archive/what-is-web-20.html> Acesso em 10/10/2011

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003.

WARSCHAUER, Mark. **Tecnologia e inclusão social : a exclusão digital em debate**. São Paulo: Senac, 2006.

VERISIGN, **whitepaper-ddos-threat-forrester.** Disponivel em : http://www.verisigninc.com/assets/whitepaper-ddos-threat-forrester.pdf, Acesso em 30 de outubro de 2011.