**Crimes cibernéticos na legislação Brasileira**

**Grupo 6**

**Resumo**

A internet dá voz para muitas coisas estúpidas acontecerem. A internet como instrumento de tecnologia acaba potencializando o que o ser humano tem de melhor e o que ele tem de pior. O número de vítimas de Exposição e compartilhamento de fotos íntimas em sites e aplicativos de smartphone tem aumentado ano a ano de acordo com a ONG Safernetbrasil, em 2016 foram atendidas por chat ou email 301 pessoas com essas denúncias.

No Brasil os crimes cibernéticos no ano de 2012 entrou em vigência a Lei N° 12.737 de 30 de novembro, esta lei está apelidada de Carolina Dieckmann e mais tarde no ano de 2014 a Lei N° 12.965 de 23 de abril, mais conhecida como Marco Civil da Internet

O estudo em tese é sobre a má utilização da internet para a pratica de crime virtual, mais conhecidos como crimes cibernéticos, esse tipo de crime é consumado por meio de, roubos de dados, golpes virtuais, roubo de identidade, difamação virtual ,criação de perfis falsos,utilização de software falsos,e outros mais.

Os crimes informáticos podem ser definidos como o lado negativo do desenvolvimento tecnológico da tecnologia da informação.

**INTRODUÇÃO**

O surgimento da rede mundial de computadores, ou internet se deu em plena guerra fria, inventada para objetivos militares.Tudo começou em 1969 onde nasceu o que seria um dos grandes marco descobertos pelo homem no último século, hoje em dia não conseguimos nos imaginar sem os serviços disponíveis pela internet.

“A internet no Brasil iniciou-se em setembro de 1988 quando no Laboratório Nacional de Computação Científica (LNCC), localizado no Rio de Janeiro, conseguiu acesso à Bitnet, através de uma conexão de 9 600 bits por segundo estabelecida com a Universidade de Maryland. Dois meses depois foi a vez da Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) que também ligou-se à Bitnet, por meio de uma conexão com o Fermi National Accelerator Laboratory (Fermilab), em Chicago.”

**(fonte: HTTPS://www.oficinadanet.com.br)**

“Em 1994, quando a Internet ultrapassou as fronteiras acadêmicas e começou a chegar ao ouvido de muitos brasileiros ,em 17 de julho ,o jornal Folha de S.Paulo dedicou a edição dominical do seu caderno Mais! à “super infovia do futuro”. E anunciava: “nasce uma nova forma de comunicação que ligará por computador milhões de pessoas em escala planetária”.

**(fonte: HTTPS://www.oficinadanet.com.br)**

Assim internet começou a ser oferecida no Brasil, para pessoas comuns, a conexão comercial para a rede mundial de computadores. Naquela época, pesquisadores e acadêmicos brasileiros já usufruíam dos benefícios em algumas universidade Sabe-se que aumentou em mais de dez vezes o volume de internautas, de 21 milhões para 250 milhões . Além disso, eles passaram de uma média de 30 minutos conectados para 27 horas mensais.

Como era de esperar, a internet também tornou-se bem mais rápida. Em 1996, um site demorava, e média, 30 segundos para carregar, hoje esse tempo caiu para apenas 6 segundos.

Mas como nem tudo é perfeito, esse meio também possui características negativas, que podem acabar nos prejudicando, sem ao menos percebermos. Com o surgimento da Internet, apareceram várias outras modalidades de crimes.

**VIRUS**

“O nome é o mesmo dos agentes causadores de doenças infecciosas, os vírus. No caso do computador, no entanto, esse organismo não é biológico e sim eletrônico. "Vírus nada mais são do que pequenos programas desenvolvidos com o objetivo de causar algum dano ao usuário do computador", explica João Eduardo Vieira, professor de Análise de Sistemas e Tecnologias da Informação da Faculdade de Tecnologia (Fatec) de Carapicuíba (SP).”

**(FONTE: https://novaescola.org.br)**

O primeiro grande passo de vírus baseado na internet foram os que se propagam por e-mails. O modo mais presente de infecção não mudou quase nada ao que é utilizado hoje, onde um documento infectado, por exemplo, é anexado a uma mensagem que tem forte apelo para que seja baixado. Uma vez que o usuário faz o download, o vírus usa o computador infectado para replicar e estender-se o máximo possível. Em 2000, vírus como Melissa e ILOVEYOU causaram estragos usando esse método.

O surgimento de worms, forma de malware ou software infectado que é propagado por redes da internet, foi o passo seguinte no desenvolvimento de vírus, conta Ana Clara. Usando os buracos em sistemas operacionais ou softwares, os worms exploram as vulnerabilidades e se replicam movimentando-se de máquina para máquina a partir da rede. Criam uma porta em qualquer computador que encontram no seu caminho, permitindo que mais softwares prejudiciais entrem no computador depois.

Veja abaixo os vírus mais conhecidos para PCs.

**Adware** É qualquer programa que executa automaticamente e exibe uma grande quantidade de anúncios (ad = anúncio, software = programa) sem a permissão do usuário.

**Backdoor (Porta dos Fundos)** É um recurso utilizado por diversos malwares para garantir acesso remoto ao sistema ou à rede infectada, explorando falhas críticas não documentadas existentes em programas instalados, softwares desatualizados e do firewall para abrir portas do roteador.

**Browser Hijacker (sequestro do navegador**) É um tipo de vírus que tem por objetivo a alteração das principais configurações do navegador. Quando instalado, altera a homepage e os mecanismos de busca. Exibem anúncios em sites legítimos e redirecionam a vítima para sites maliciosos que podem conter exploits ou outras pragas digitais.

**Cavalo de Troia (Trojan Horse**) Conhecidos por normalmente responder pelo primeiro estágio de infecção de dispositivos digitais, os Cavalos de Troia têm como objetivo manter-se ocultos enquanto baixam e instalam ameaças mais robustas em computadores e laptops. Podendo vir em arquivos de música, mensagens de e-mail, escondidos em downloads e sites maliciosos, se aproveitam de vulnerabilidades do navegador utilizado para instalar a praga no computador.

**Rogue Security Software** Rogueware é um vampiro que busca sugar suas informações confidenciais para roubar dinheiro. Esses softwares maliciosos se passam por programas de segurança (como antivírus ou antispywares) e de otimização, e são abertos sem a interferência do usuário, exibindo resultados de uma varredura por vírus, que mostram a detecção de diversas infecções – que na verdade não existem, ou de diversas otimizações disponíveis para “turbinar” o computador.

**Rootkit** Rootkit são trojans que utilizam métodos avançados de programação para serem instalados em camadas profundas ou não documentadas do sistema operacional. Seus aspectos mais devastadores são sua capacidade de se autorrecuperar, reinstalando-se mesmo após limpeza do computador e sua rápida disseminação.

**Spyware** Os spywares são programas espiões utilizados para captar informações sobre os costumes dos usuários na internet, com o propósito de distribuir propaganda “customizada”.

**Time Bomb** É um malware de contagem regressiva. Uma ameaça programada para ser executada em um determinado momento no sistema operacional, causando danos.

**Worm (verme)** Podem se autorreplicar sem a necessidade de infectar arquivos legítimos, criando cópias funcionais de si mesmos. Essas características permitem que os worms se espalhem por redes de computadores e drives USB. Também podem ser distribuídos por mensagens de e-mail, criando anexos maliciosos e os enviando para as listas de contato da conta invadida

**Greyware** Situa-se na chamada zona cinzenta, entre o software normal e um vírus, causando mais irritação que problemas, como programas de piada e adware. Greyware refere-se a uma ampla gama de programas que são instalados sem o consentimento do usuário e rodam em seus computadores.

**Joke Program** Tratam-se de programas ou códigos criados para causar danos temporários ao sistema operacional, como travamentos e mudanças inesperadas de comportamento. Os códigos dessa categoria não causam nenhum dano real ao computador.

**Keylogger** Os keyloggers são programas de computador capazes de monitorar, armazenar e enviar todas as teclas digitadas pela vítima para um cracker. Atualmente, os keyloggers são incorporados em outros códigos maliciosos como trojans, para o roubo de logins ou dados bancários.

**Macros** Os Macros são uma série de comandos automatizados que podem ser configurados em softwares como Word e Excel. Dessa forma, muitos documentos com instruções maliciosas podem ser criados, infectando outros arquivos ou executando ações prejudiciais toda vez que eles forem executados. Em sua grande maioria, a ação é realizada ao abrir ou fechar um documento dessa extensão.

**Ransonware** São códigos maliciosos que sequestram arquivos ou todo o sistema da vítima por meio de técnicas de criptografia. Após o “sequestro”, o malware exibe mensagens exigindo o depósito de uma quantia em dinheiro, ou a compra de um determinado produto, prometendo o envio de senha que irá liberar os arquivos. Porém, mesmo após o pagamento, a vítima não recebe senha alguma.

**Trojan Banking** É o trojan caracterizado pelo roubo de dados bancários, de sites de compras, redes sociais e servidores de e-mail. As técnicas são as mesmas de um trojan comum, sendo distribuído como um programa ou arquivo legítimo, em sites infectados ou mensagens de e-mail.

**Vírus Stealth** São malwares que utilizam técnicas de programação para evitar a detecção por ferramentas de segurança. A maioria utiliza métodos de criptografia, embaralhando o código para que o antivírus não o reconheça como malicioso.

(**FONTE: https://www.itforum365.com.br)**

**ATAQUES VIRTUAIS:**

Nos últimos anos, esse tipo de crime evoluiu para se tornar uma atividade muito lucrativa e muitas vezes com muito baixo risco para organizações criminosas. A sociedade atual mais e mais conectada tornou-se um campo de atividade ilimitada para os criminosos que têm como alvo especialmente nos setores financeiro e empresarial.

Ataques de computador implicam perdas econômicas e de produtividade imprevisíveis, mas eles não estão limitados a esse tipo de perda. As empresas afetadas devem arcar com os custos da limpeza de malware, investigação e gerenciamento pós-ataque. Às vezes, as empresas também correm o risco de não se recuperarem após ataques cibernéticos: perda de dados e roubo de segredos industriais podem ser fatais para empresas que dependem muito do sigilo de sua produção. Muitas empresas também enfrentam a perda de credibilidade exposição no mercado.

A concentração do cibercrime no setor financeiro de pequeno e médio porte de empresas chegam em um momento delicado, especialmente no Brasil, onde as empresas afetadas pela recessão tenta lidar com medidas duras e lucros baixos.

Cibercrime é um fenômeno criminoso que é caracterizado pelo abuso de tecnologia de

informática tanto de hardware como de software.

Alguns crimes, em particular, visam a exploração comercial da Internet, que colocam em risco os sistemas de informação da segurança nacional.

O crimes virtuais pode geralmente ser definido como uma atividade criminosa envolvendo

estrutura de tecnologia da informação, incluindo acesso ilegal (acesso não autorizado),

intercepção (por meios técnicos de transmissão não pública de dados informáticos para, de ou

dentro de um sistema de informação), a interferência de dados (dano, supressão,deterioração, alteração ou supressão de dados informáticos), sistemas de interferência (interferência

com a operação de um sistema de informação pela entrada, transmissão,dano, cancelamento, deterioração, alteração ou exclusão de dados de computador), uso de dispositivos impróprios, roubo de identidade e fraude eletrônica.

No início da subcultura hacker, as condenações criminais eram raras, já que a abordagem era de conhecimento dos sistemas de informação e sua segurança, violando sistemas com ações não prejudiciais. Com o crescimento da indústria de tecnologia da informação, os

casos de violação de sistemas de computador para lucro pessoal exclusivo aumentaram consideravelmente.

**INVASAO**