Crimes cibernéticos : abordagem, práticas e considerações

Luana Natielle Costa Leal de Jesus [1], Arley Oliveira da Mota[2], Áquilla Odlanier Faria Nascimento[3], Soraia Ataide Linhares Frota[4]

[123]Instituto Federal do Norte de Minas Gerais – (IFNMG)

Minas Gerais – MG – Brazil

luananatielle15@hotmail.com, arley.msn@hotmail.com, aofnas@hotmail.com,soraialf@oi.com.br

Abstract. *Internet crimes in Brazil is becoming one of the greatest current security problems. However, there are laws and regulations that regulate their practices with their appropriate penalties. This article aims to present a brief relationship between Internet use and crime in cyberspace. Used publications in the area for analysis of the main criminal practices. As a result, there is an outline of the main criminal practices and the laws that support, protect and punish the criminals.*

Resumo. *Crimes de internet no Brasil vem se tornando um dos grandes problemas de seguranças atual. Entretanto existem leis e normas que normatizam as suas práticas com suas devidas penalidades. O objetivo deste artigo é apresentar uma relação sucinta entre o uso da internet e os crimes no ciberespaço. Utilizou-se de publicações na área para análise das principais práticas criminosas. Como resultado, tem-se um esboço das principais práticas criminosas e as leis que amparam e protegem as vítimas e punem os criminosos.*

1. Introdução

Com a evolução dos meios de comunicação, novas tecnologias surgiram com a evolução da internet, proporcionou às pessoas, um novo modo de vida. Possibilitando comprar, vender, relacionar-se com o mundo, conhecer pessoas e estudar, com apenas um *click*. Entretanto, com inúmeras variedades de serviços, muitas vezes, a segurança fica comprometida.

Os cibercrimes são crimes que acontecem via internet, que hoje, popularizou-se pelo mundo e faz muitas vítimas. Vítimas que, muitas vezes, não sabem como se proteger desses crimes, nem mesmo, como agir depois que eles ocorrem.

1 Cursando 2º período do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas– Câmpus Januária

2 Cursando 6º período do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas– Câmpus Januária

3 Cursando 6º período do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas– Câmpus Januária

4 Advogada, Professor do IFNMG – Câmpus Januária

De acordo com Locca (2012) apesar de a internet ser uma ferramenta de comunicação, existem consequências, uma vez que pessoas passaram a usá-la com outras finalidades, como a prática e organização de crimes. Dessa forma, surgiram os cibercrimes: crimes realizados através da internet.

Dados da pesquisa de crimes eletrônicos (2014), realizado pela FecomércioSP, apontam que em mil entrevistados, 18% já foram vítimas de crimes virtuais. A pesquisa aponta que 80,8% das pessoas sentem medo de serem vítimas, e 65,6% fazem uso de programas que impedem a invasão e evitam a captura de senhas (Crimes Pela Internet 2015.)

Percebe-se o uso de tecnologias como programas e aplicativos, para tentar burlar a ação dos criminosos, ato que nem sempre é bem sucedido, pois a maioria dos softwares de segurança não conseguem "proteger" de todos os crimes, dando ao usuário uma ilusão de segurança, e tornando-se, assim, vulnerável a ataques.

O presente artigo tem como objetivo identificar os principais crimes cibernéticos, avaliar os principais alvos e o amparo da lei. Mostrar aos usuários o seu "inimigo", para que esses possam traçar métodos para se defender.

2.Metodologia

O método adotado, neste artigo, foi a revisão de literatura que subsidiou a construção do texto e o estudo sobre os crimes cibernéticos (Gil 2002).

O quadro apresentado neste trabalho, junto com as pesquisas e demais informações, demonstram dados reais, obtidos em ambientes do cotidiano e situações verídicas de como esses ataques cibernéticos se desenvolvem.

3. Principais Tipos de Cibercrimes e Seu Público Alvo

O Departamento de Justiça dos EUA define os crimes cibernéticos, amplamente, como "quaisquer violações de leis criminais que envolvam, para sua perpetração, investigação ou persecução, o conhecimento de tecnologia de computador" [Herman 2011].

Os H*ackers* são pessoas que possuem conhecimento em TI (tecnologia da informação) e TC (tecnologia da comunicação), e que utilizam a sua capacidade para explorar a vulnerabilidades e aperfeiçoar sistemas (Souza 2015).

No entanto, os *Hackers* buscam melhoria de *software*, de sistemas e de redes de uma forma legalizada. Já os *Crackers* são como os *Hackers*, entretanto, utilizam sua capacidade para fins ilícitos visando a obtenção de proveito pessoal. Segundo Vilela (2006), *Hackers* são contratados por empresas para proteger seus sistemas contra o ataque de *crackers*. Entende-se que há diversos tipos de crimes cibernéticos, alguns deles são:

- *Mobile malware*: Vírus desenvolvidos para roubar informações e causar danos.

Espionagem industrial: Roubar informações sigilosas de empresas, e fornecê-las a seus concorrentes.

Worm: Atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

Dos: Ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

Scan: Varreduras em redes de computadores, com o intuito de identificar quais estão ativos e quais serviços estão sendo disponibilizados por eles.

As Figuras 1 e 2 demonstram graficamente os incidentes reportados, no Brasil, no período de janeiro a dezembro de 2015.

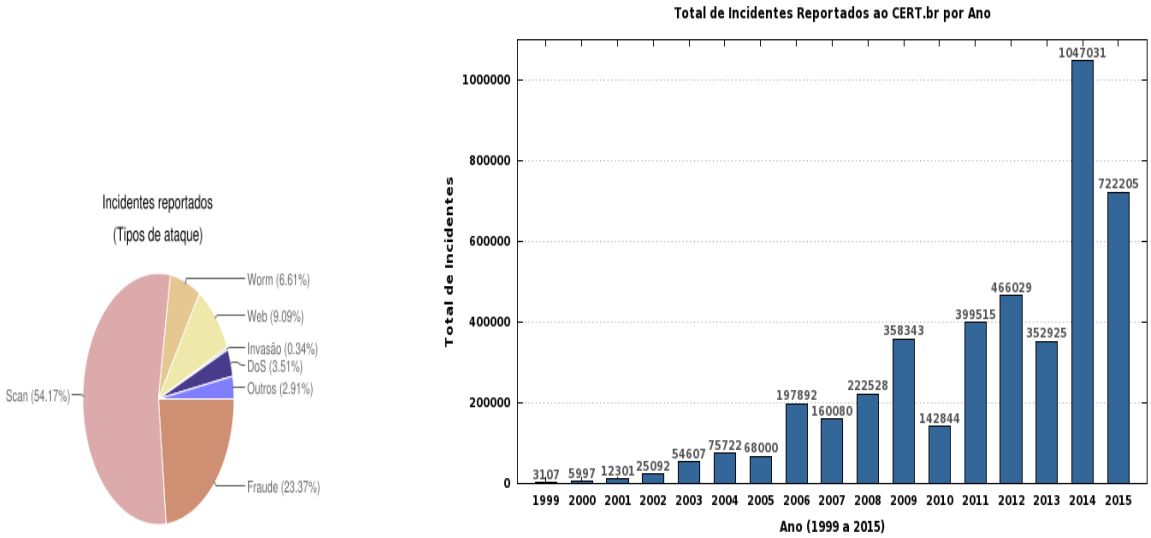

Figura 1 e 2 - Incidentes Reportados ao CERT.br - Janeiro a Dezembro de 2015

Observa-se, a partir da Figura 1, que 54,17% dos ataques são *Scan*, sendo o maior dos tipos de ataque praticados no Brasil. A fraude engloba 23,37% desses ataques e os demais como *worm, web*, invasão, DoS e outros possuem menos de 10% cada. Já a Figura 2 demonstra o crescimento desses incidentes com o passar dos anos.

Mais da metade dos 67 milhões de domicílios brasileiros passaram a ter acesso à internet em 2014 (54,9%). Em 2013, esse percentual era 48% (IBGE, 2016). A figura 2 mostra a evolução dos casos de ataques cibernéticos com o passar dos anos. Fazendo, assim, uma relação clara, que com o aumento da utilização da internet houve também um aumento nos casos de crimes virtuais.

No Brasil, o número de ataques é superior ao de muitos outros países, sendo o setor bancário o mais afetado, o cibercrime incide fortemente na vertente financeira [Simas 2014].

3.1 Alvos

Sydow [2013] destaca que "a vítima é um sujeito de foco adequado, um alvo que se mostra preferencial, seja por quem é, por como se porta, por o que possui ou por onde está.". Os principais alvos do cibercrime são as empresas. Com seus grandes servidores, são vítimas mais lucrativas, porém, mais difíceis de atacar. Com isso, faz das pessoas comuns alvos, pois elas não possuem

equipamentos e softwares de segurança potentes para se proteger, e muitas vezes por falta de conhecimento acabam "ajudando" os *crackers*, baixando arquivos sem saber a origem, ou fornecendo seus dados pessoais.

3.2 Ferramentas usadas para cometer e combater crimes

- *Keylogger*: são definidos um tipo de spyware cuja finalidade é capturar tudo o que for digitado em um computador [CERT.br 2007].
- Navegador *Sandcat*: Navegador *web hacker*, baseado no navegador *chrome*; possibilita fazer testes de invasão, com muita rapidez.
- *Hijacker*: sequestra o navegador de internet e a faz navegar por sites diferentes daqueles digitados.

3.3 Descobertas de cibercrimes

Os novos criminosos agem certos da impunidade, porque não estão na presença da vítima. No entanto, há dificuldades técnicas na hora da apreensão do equipamento usado para cometer ato ilícito, necessidade de autorização para quebra de sigilo de suspeitos, falta de tipificação e a questão envolvendo territorialidade, jurisdição e competência nos crimes virtuais (Souza 2015).

Por sua própria natureza, os crimes cibernéticos são difíceis de serem investigados (Herman 2013). Os *Crackers*, muitas vezes, não podem ser rastreados e identificados, pois muitos delitos são cometidos em ambiente da *deep web*, onde permanece o anonimato, é o ambiente que também acomoda os crimes mais 'pesados' como tráfico, contrato de assassinos, venda de corpos, etc.; nos casos que se consegue rastrear o computador de onde surgiu o delito, o proprietário pode alegar que foi outra pessoa que o cometeu. Os dados podem ser criptografados e difíceis de ler Herman (2013) diz que: Muitas vítimas não denunciam crimes cibernéticos, simplesmente, porque elas não sabem que eles ocorreram.

No Brasil, há algumas leis específicas para crimes cibernéticos, nos casos em que a legislação é ausente, aplica-se normas jurídicas já existentes no nosso ordenamento jurídico, como o código penal, por exemplo, para não deixar o infrator cibernético impune.

Há leis que punem os criminosos virtuais, dentre elas, cita-se:

2 **Lei Nº 9.609/98**- Lei de *Software*: Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

3 **Lei 12.737/2012**- Lei Carolina Dieckmann: Tipifica e pune os crimes informáticos de roubo de dados.

4 **Lei Nº12.735/12 –** Altera o código penal para tratar de crimes cibernéticos, tipificando condutas realizadas mediante uso de sistema eletrônico, digitais ou similares.

3.4.1 Como se proteger e como agir ao se tornar uma vítima

Norton (2016) diz que: normalmente, os criminosos tentam obter lucros da forma mais rápida e fácil possível. Quanto mais você dificultar essa tarefa, maior a probabilidade de eles desistirem de você e passarem para um alvo mais fácil.

Quadro 1. As Melhores sugestões de prevenção

Ferramenta / Formas	Função
Antivírus	Programas que protegem o computador de vírus, monitora as atividades on-line, e bloqueiam atividades maliciosas. Devem ser atualizados com frequência.
Ofertas on-line	Software supostamente "gratuito"; concursos que ganhou, sem participar; podem ser softwares mal intencionados, ao clicar, acaba autorizando a entrada e execução deles.
Analisar os extratos bancários	Ao analisar extratos bancários e de cartões de crédito com frequência, têm-se a possibilidade de descobrir que está sendo alvo de roubo de identidade mais rápido, e com menos prejuízos.
S.O e softwares atualizado	Atualizar regularmente o computador, bloqueia a possibilidade de os atacantes tirarem partido de falhas do software. Não protege, mas dificulta o acesso.
Dados Pessoais	Ter cuidado ao partilhar informações pessoais, tanto em sites de compras ou por e-mail; atenção em e-mail falsos; empresas não solicitam informações pessoais por e-mail
Senhas	Escolher palavras que não podem ser facilmente adivinhadas; usar no mínimo 8 caractere, combinando letras, números e símbolos; trocar a senha a cada 90 dias.

Fonte: Adaptado de (Norton 2016)

Denunciar ainda é o modo mais efetivo de combater a criminalidade online [crimes pela internet, 2015]. Há muitas delegacias especializadas em crimes virtuais, porém, qualquer delegacia pode fazer um boletim de ocorrência, e iniciar as investigações.

4. Considerações Finais

Pode-se concluir com o estudo e revisão bibliográfica feito, que os crimes na internet são muito comuns, e que todas as pessoas que utilizam a internet estão sujeitas a serem vítimas de cibercrimes.

Indica-se que os usuários devem tomar algumas precauções quanto ao uso, em especial, dos dados pessoais como identidade, CPF e senhas de contas bancárias e cartões de crédito. É importante verificar se o site tem algum tipo de certificação, bem como utilizar das dicas para se proteger descritas no Quadro 1.

Por outro lado, é importante que as vítimas denunciem, pois há amparo nas leis brasileiras, e delegacias especializadas, para que se combata esse crime, que a cada dia se torna mais comum.

Sendo assim, compreende-se que o objetivo do artigo que é identificar os principais crimes cibernéticos, avaliar os principais alvos e apontar o amparo e as punições constituídas por lei foi realizado de maneira satisfatória, uma vez que os principais crimes, suas punições e as leis que se aplicam foram identificadas.

5. Referências

Cert, Centro de Estudos, Reposta e Tratamento de Incidentes de Segurança no Brasil. (2016a). "Tipos de ataques, Incidentes Reportados ao CERT.br - Janeiro a Dezembro de 2015." http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque.html. Junho de 2016.

Cert, Centro de Estudos, Reposta e Tratamento de Incidentes de Segurança no Brasil, (2016b). Total de incidentes reportados, Incidentes Reportados ao CERT.br - Janeiro a Dezembro de 2015. http://www.cert.br/stats/incidentes. Junho de 2016.

Crimes Pela Internet. (2015a). "Onde denunciar crimes virtuais: lista de delegacias especializadas. Crimes pela internet". http://www.crimespelainternet.com.br/delegacias-de-crimes-digitais/, Junho de 2016.

Crimes Pela Internet. (2015b). Você sabe quais são os crimes virtuais mais comun?. Crimes pela internet. http://www.crimespelainternet.com.br/tipo-mais-comuns-de-crimes-virtuais/, Junho de 2016.

Deepwebbrasil. (2016). "Deep web, Afinal, o que é Deep Web?." http://www.deepwebbrasil.com, Junho de 2016.

Gil, A. C. (2002). "Como elaborar projetos de pesquisa." 4. ed. São Paulo: Atlas.

Herman, S. N. (2011). "Os desafios do crime cibernético." Revista Eletrônica de Direito Penal e Política Criminal, 1(1).

Locca, Erica Cristiane. (2012). "Crimes cibernéticos e a sociedade atual." Revista eletrônica da Faculdade de Direito de Alta Floresta.

Norton. (2016). "As melhores sugestões de prevenção." http://br.norton.com/prevention-tips/article, Junho de 2016.

Simas, Diana V. D. (2014). "O cibercrime." . Universidade Lusófona de Humanidades e Tecnologias.

Souza, Henry Leones. (2015). "Da ausência de legislação específica para os crimes virtuais." Revista eletrônica da Faculdade de Direito de Alta Floresta 8.2.

Vilela, Geraldo Majela. (2006). "O uso do termo hacker nas notícias veiculadas pela internet brasileira." RI UFLA (Universidade Federal de Lavras).