Faculdade de Tecnologia de Americana

Vulnerabilidades invisíveis

Mayara Tatiellen Silva Viana

Wendel Mécca Pétta

Americana, SP.
2018

Faculdade de Tecnologia de Americana

Vulnerabilidades invisíveis

Mayara Tatiellen Silva Viana

Wendel Mécca Pétta

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Tecnólogo em Segurança da Informação, sob a orientação do Prof.º Me. Benedito Luciano Antunes de França.

Área de concentração: Segurança da Informação

Americana, SP.
2018

Faculdade de Tecnologia de Americana

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

V668v VIANA, Mayara Tatiellen Silva

Vulnerabilidades invisíveis. / Mayara Tatiellen Silva Vianna, Wendel Mécca Pétta. – Americana, 2018.

45f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Benedito Luciano Antunes de França

1 Segurança em sistemas de informação I. PÉTTA, Wendel Mécca II. FRANÇA, Benedito Luciano Antunes de III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Faculdade de Tecnologia de Americana

Vulnerabilidades invisíveis

Mayara Tatiellen Silva Viana

Wendel Mécca Pétta

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Tecnólogo em Segurança da Informação, sob a orientação do Prof.º Me. Benedito Luciano Antunes de França.

Área de concentração: Segurança da Informação

Americana, 13 de dezembro de 2018.

Banca Examinadora:

Benedito Luciano Antunes de França
Mestre
Pontifícia Universidade Católica de Campinas – PUC

Wladimir da Costa
Mestre
Universidade Metodista de Piracicaba - Unimep

Clerivaldo Jose Roccia
Mestre
Universidade Estadual de Campinas - Unicamp

AGRADECIMENTOS

Nós agradecemos a todos os professores da Fatec Americana por todo o ensinamento e dedicação, em especial ao professor Marcus Lahr pelo apoio em materiais e auxílio nos testes realizados, ao professor Benedito França, por nos orientar, dar todo o suporte para que a realização desse trabalho fosse possível e não perder a esperança em nós, agradecemos também ao William Toshio Nakagawa por ajudar na realização dos testes agilizando a utilização dos laboratórios da Fatec, agradecemos também ao coordenador do curso, Wladimir da Costa por coordenar o curso de forma com que tenhamos aprendido toda a matéria de forma coerente no decorrer do curso, o que nos possibilitou a apresentação deste.

Agradecemos também a nossas famílias por nos apoiar e incentivar nos momentos mais difíceis.

Obrigado a todos que fizeram parte de nossa vida acadêmica.

DEDICATÓRIA

Dedicamos esse trabalho a todos os amantes de tecnologia, aos nossos familiares e a todos aqueles que nos ajudaram na jornada da graduação.

RESUMO

O objetivo desde trabalho é apresentar as vulnerabilidades existentes em servidores e serviços atuais que podem levar a consequências financeiras ou morais, as quais podem atrapalhar a imagem de uma pessoa ou empresa. Neste trabalho é apresentado formas de como pessoas mal-intencionadas fazem uso da tecnologia para enganar pessoas e conseguir o que querem, e uma vez conseguido, utilizam desta brecha para usar pessoas ou computadores para sua finalidade, sendo ela boa ou ruim como uma correção de vulnerabilidade ou um ataque em massa.

Palavras-Chave: DDoS; Vulnerabilidades; Segurança; Ataque, Flood.

ABSTRACT

This document objective is to presente the existente vulnerabilities inside servers and services running on them that may take to financial or moral consequences that can interfere in the company or person image. In this work, is presented ways of how bad intentioned people use technology to misguide people and get what they want, and once they get it, they explore this breach to use people or computers to your benefit, this one that could be an evil or a good thing, like correcting a vulnerability or doing one mass attack.

Keywords: DDoS; Vulnerability; Security; Attack, Flood.

SUMÁRIO

LISTA DE IMAGENS

LISTA DE TABELAS

LISTA DE GRÁFICOS

INTRODUÇÃO

Para os negócios “tempo é dinheiro” e mais do que nunca essa frase faz todo o sentido, pois se um determinado *site* de vendas ficar indisponível por um certo período, a perda de dinheiro será iminente.

Esse trabalho irá apresentar as várias vulnerabilidades de sistemas e redes que podem facilitar um ataque de negação de serviço (*DDoS*), deixando uma rede, um servidor, ou até mesmo um computador “travado” sem que responda mais nenhuma requisição. Abordaremos de forma prática como são esquematizados e/ou feitos os ataques de negação de serviço em servidores mal configurados, com vulnerabilidades de protocolos ou serviços que estão em execução.

Ataques de negação de serviço são ataques por meio dos quais um *hacker* explora uma vulnerabilidade, falha de serviço ou de configuração, e através desta, força um computador de uma *botnet* a realizar várias requisições de dados ou de informações de um outro computador, fazendo com que a taxa de transferência deste se eleve, deixando-o inoperante ou indisponível até ter a falha ou o ataque corrigido ou percebido, e o servidor for recuperado, voltando a oferecer o serviço a seus clientes com o tráfego regularizado.

No Capítulo 1 nós iremos abordar a importância e o valor da informação tanto no ambiente corporativo como no ambiente familiar, como também trataremos sobre as questões morais, as quais os usuários de internet estão expostos, além de ofertar a conceituação e composição técnica de *DoS* ou *DDoS*. No Capítulo 2 discorreremos sobre as políticas de segurança para mitigar ataques, além de conceituar a engenharia social relacionando-a aos ataques de negação de serviço, às vulnerabilidades técnicas que podem levar a ataques *DDoS* e acerca dos crimes relacionados a tais ataques.

Para finalizar, no Capítulo 3 será exposto um teste que irá revelar que um computador invadido pode se tornar parte de uma *botnet* vindo a atacar um servidor vítima sem nem estar sabendo que participa de tal *botnet*.

E, por último, apresentaremos as considerações finais visando motivar os incautos a não deixarem vulnerabilidades ou serviços abertos para possíveis atacantes, haja vista que, no futuro próximo, na era da internet das coisas, vários dispositivos terão acesso à internet, incrementando as potencialidades de riscos e de ataques.

CAPÍTULO 1 - DATA COMO INFORMAÇÃO DE VALOR

É possível afirmar que no mundo tecnológico tudo gira em torno de dados e de informações, e, por conseguinte, eles possuem um valor, o qual pode ser absurdamente importante e crucial, por exemplo, para o funcionamento de uma empresa e até mesmo de um órgão público. Isso também pode afetar o ambiente familiar, uma vez que, se algum dado pessoal, como, por exemplo, uma foto das férias familiares, for parar em mãos de algum atacante, pode significar um risco para o relacionamento afetivo, profissional ou vida particular. Por esse motivo a proteção preventiva desses elementos é indispensável e de extrema importância, haja vista que qualquer dado vasado pode trazer riscos.

Para Cezar Taurion (2014, p. 2) os dados possuem valores significativos e isso têm real importância para o cenário global:

> Um recente estudo do Federal Reserve, nos EUA, estima que o total de dados e outros ativos intangíveis das empresas, como patentes, marcas registradas e direitos autorais podem valer mais de oito trilhões de dólares, que é um valor quase igual ao PIB somado da Alemanha, França e Itália. Estes ativos intangíveis estão se tornando parte cada vez mais importante da economia global (TAURION, 2014, p. 2).

Os valores *dos* dados empresariais mesmo que intangíveis são significativamente caros e podem representar valores financeiros exorbitantes.

1.1 - O VALOR DA INFORMAÇÃO PARA O AMBIENTE CORPORATIVO

O ambiente corporativo está constantemente à mercê de ataques, invasões, e/ou de fenômenos da natureza que possam ameaçar a segurança de dados e informações, não obstante, quais seriam os prejuízos que a perda de tais dados poderia causar para a empresa? Por que informações informáticas e computacionais podem provocar tais efeitos?

As informações e dados de uma empresa são aquilo que irá moldá-la, são de lá que todas as estratégias e decisões são tomadas, se tais itens de tão grande importância forem subtraídos da corporação, além de prejuízos financeiros enormes, podem

causar até mesmo a dissolução da organização, por outro lado, quanto mais dados e informações uma empresas conseguir adquirir mais bem sucedida ela se tornará no mercado de trabalho.

A informação no ambiente empresarial tem como finalidade o conhecimento dos ambientes externo e interno da organização para a atuação nesses meios (CHAUMIER, 1986), dentre os estragos que uma empresa pode enfrentar com a perda dos dados podemos citar os custos para a recuperação dos dados, eventuais multas e penalidades quando terceiros estiverem envolvidos e, com efeito, forem prejudicados; ademais, a perda de componentes físicos e *softwares* de informática ocorrida por danos causados por *malwares*, perda no controle dos processos, prejuízos financeiros e perda de clientes são outros ônus derivados destas invasões.

1.1.1 - DIMENSÃO COMPUTACIONAL

Os dados computacionais de uma empresa trazem muitas vantagens para o meio corporativo, além de maximizarem os processos, economizarem tempo e eliminarem as enormes pilhas de papel, também possibilitam um crescimento significativo de dados a serem processados, armazenados e protegidos. Bancos de dados são usados para o armazenamento de diversos tipos de informações, desde a ficha de todos os funcionários da empresa até informações sobre fornecedores e clientes.

Feitosa (2013, p. 14) define banco de dados como “bancos de dados interrelacionados, organizados de forma a permitir que sistemas de aplicação armazenem novo dados, encontrem dados armazenados, alterem seu conteúdo e excluam dados indesejáveis por meio de métodos precisos de manipulação e localização”.

Contudo, essas facilidades têm um preço, com as facilidades, existem também vulnerabilidades que podem ser exploradas, causando possíveis perdas desses dados armazenados. Em caso de perda de algum banco de dado ou arquivo, pode estar ferindo diretamente qualquer uma das principais bases da segurança da informação. Em caso de um arquivo ser modificado indevidamente, a pessoa não poderá mais confiar no mesmo, já que o criador do arquivo não saberá exatamente o que foi modificado por um atacante, o que prejudica a integridade do arquivo. Em caso

de um ataque em que a intenção seja de prejudicar financeiramente alguma empresa, deixa seus serviços indisponíveis, além da disponibilidade que seria afetada, juntamente com a integridade de um arquivo, que, por não ser o mesmo que o autor criou, pode conter algum código malicioso. Essas brechas criadas podem comprometer a empresa e pode, eventualmente, acarretar prejuízo no tocante à confidencialidade, terceiro pilar da segurança, pois um atacante, após deixar os serviços da empresa inoperantes e alterar arquivos furtados, pode tomar o controle de algum computador da empresa e acabar tendo acesso a arquivos confidenciais, como o financeiro da empresa ou a lista de funcionários e seus respectivos e-mails e telefones particulares, o que causaria danos ao grupo de colaboradores desta empresa.

Os pilares da Segurança da Informação são definidos como:

> **Princípio da Disponibilidade:** (...) os dados e sistemas devem estar disponíveis para visualização e modificação, a qualquer momento, para as pessoas certas. (Algumas) medidas podem ser adotadas, como o uso de criptografia e a implementação de métodos de exclusão segura de arquivos;
> **Princípio da Confidencialidade**: o acesso a todos os registros e sistemas digitais deve ser restrito apenas às pessoas certas. (...);
> **Princípio da Integridade:** nenhum dado deve ser modificado indevidamente. Em outras palavras, a infraestrutura de TI deve estar protegida contra qualquer brecha (...). Esse conceito também é aplicado à integridade de sistemas (...) (MOREIRA, 2017, p. 2).

Outro ponto de suma importância são os meios que a empresa utiliza para armazenar seus dados e informações e a forma como estes são protegidos, visto que as informações cruciais de uma organização devem ser protegidas não apenas de ataques cibernéticos como também de desastres naturais, como, por exemplo, tempestades, terremotos e deslizamentos; também é importante lembrar que eventuais acidentes podem vir a acontecer a qualquer momento e sem aviso prévio, sendo eles, propositais (terrorismo) ou não. Para isso, algumas políticas de segurança deverão ser implementadas, como planejar o local de instalação de sua sede com antecedência, evitando assim zonas de desabamento, terremotos e coisas do tipo. Com esse planejamento a empresa já pode começar a prevenir alguns desastres naturais, assim como que, por políticas, também pode se estabelecer um outro local longe da empresa matriz, para armazenar um *backup* dos dados da empresa, assim,

em caso de algum ataque terrorista, os dados da empresa estarão salvos em outro prédio ou instalação.

> As cópias de segurança em computadores são instrumentos importantes para compensar – ou sanar – problemas advindos de hardware, como a invasão do sistema por hackers, ataques de vírus, perda acidental de arquivos, conflitos no sistema operacional etc. Por isso a cópia de segurança é a melhor forma de prevenção e recuperação das informações, já que os dados podem voltar fielmente para o disco, quando for necessário. Em várias empresas que dependem de sistemas de computadores, a perda de dados representa a perda de capital. Trazendo esta realidade para a sua vida cotidiana, na qual o computador é usado como ferramenta de trabalho, perder dados significa perder tempo, perdendo tempo, perde-se dinheiro e, por conseguinte, o cliente (FIALHO JÚNIOR, 2007, p. 6).

A maneira como uma empresa guarda suas valiosas informações e dados é o pilar que irá protegê-la de qualquer sinistro no futuro, fazendo com que essas organizações se recuperem o mais rápido possível e sem grandes perdas. Um dos meios de manter toda a informação protegida e segura de qualquer tipo de incidente ou até mesmo de ataques é a realização de *backups* regularmente.

1.1.2 - DIMENSÃO MORAL

Nós abordaremos também as dimensões morais que uma segurança vulnerável pode acarretar para a organização, pois esta carrega um nome e uma reputação, fundamentada em valores, princípios e missão, que, quando sucumbidos, trazem até mais prejuízos e reflexos do que a perda de dados computacionais em si.

1.1.3 - DIMENSÃO ECONÔMICA

Citaremos um exemplo de empresa que foi atacada e teve os seus dados furtados. É o caso publicado pelo documento internacional “Global Internet Report”, de 2016, sobre a empresa americana Target. No caso estudado, a empresa de segurança Target possuía todo o controle de seus computadores e ações, no entanto, ela não tinha políticas de segurança com seus fornecedores, como, por exemplo, prestar apoio aos fornecedores sobre segurança de informação para usuários terem cautela com os equipamentos e se protegerem contra possíveis atacantes, políticas preventivas que poderiam sugerir que os antivírus fossem atualizados regularmente,

que usuários não poderiam, por exemplo, usar aparelhos USB sem serem analisados previamente, evitar ainda *login* de acesso com senhas fracas, entre outras políticas básicas de segurança. Graças a esta falha de gestão de segurança, a Target foi invadida, indiretamente, e teve seus dados furtados, a partir da rede de um fornecedor de refrigeradores. Conforme o documento da "Global Internet Report", a máquina de refrigeração do fornecedor da Target usava um sistema de antimalware gratuito e não fazia, em tempo real, a proteção de suas informações. Após tal acontecimento, a Target e a fornecedora das máquinas internas tiveram a vulnerabilidade explorada por atacantes que, por meio de ação invasiva, atingiram as máquinas de cartão de crédito fabricadas pela Target, as quais foram para as lojas infectadas com o *malware* e, por conseguinte, os atacantes conseguiram desviar milhões de dados de usuários de cartões de crédito, incluindo nome, número de cartão e inclusive senha[1].

Em casos como este, muitas empresas acabam perdendo credibilidade, além de possíveis prejuízos financeiros com auxílios às vítimas, tendo ainda que reparar eventuais danos causados pelos atacantes. Muitas vezes, empresas desprevenidas acabam indo à falência ou tendo sua marca gravemente prejudicada, com danos consideráveis as ações e/ou produtos comercializados.

1.2 - O AMBIENTE FAMILIAR

Outro ambiente distinto que sofre com o crescente uso da Tecnologia da Informação é o ambiente familiar. A evolução da tecnologia foi extremamente célere na escala do domínio privado, por efeito, a capacidade de manipular tais tecnologias pode ocasionar alguns prejuízos para os entes familiares. Um usuário doméstico, por exemplo, está potencialmente sujeito a vários pontos críticos de segurança de informações quando faz uso dessas tecnologias disponíveis, que vão desde passar a

[1] "Attackers entered Target's systems through the computer system of a Target refrigeration contractor. They installed software on Target's point-of-sale terminals, collected customer information on an internal host, and then forwarded it back to themselves (see next figure). The initial attack used known malware that may not have been found because the refrigeration contractor only used free anti-malware software that did not offer real-time protection. It also appears Target itself was vulnerable, in part, because of weak or default passwords.". INTERNET SOCIETY. **Global Internet Report**, p. 73-74. *Tradução nossa!*

senha de acesso de vários sites e serviços da internet para terceiros, fazer *downloads* de *malwares* sem intenção ou consentimento, deixar contas pessoais conectadas em computadores públicos, tomar pouco ou nenhum cuidado no acesso às redes sociais, entre outros. Estes descuidados facilitam, por exemplo, na divulgação de informações que podem ser facilmente acessadas e utilizadas por criminosos, tornando entes familiares em vítimas de *phishing* (*e-mails* e propagandas falsos), fornecedores leigos de informações que um criminoso pode utilizar, para acessar *sites* de compras falsos, tornando-os potenciais vítimas de fraudes de diferentes naturezas e até mesmo participarem de redes de *botnets*.

1.2.1 DIMENSÃO COMPUTACIONAL NO AMBIENTE FAMILIAR

O meio mais eficiente de evitar que coisas desse tipo aconteçam é ensinar todos os usuários domésticos sobre o uso dessas tecnologias, informando e conscientizando sobre os inumeráveis riscos que o uso indevido do meio digital pode causar efeitos catastróficos na vida real.

Existem diversas cartilhas de educação digital na própria internet, como por exemplo as cartilhas disponíveis no Portal do Planalto, como a “Cartilha de Segurança: simples atitudes podem evitar grandes problemas”, entre outros sítios eletrônicos, tais como “mpdft.mp.br”, que disponibiliza a cartilha “Ética e segurança digital: cartilha orientativa”. Esses materiais mostram cenários e situações no qual a família está exposta quando faz uso da internet e orienta no uso correto e seguro das tecnologias atuais, procurando conscientizá-la e protegê-la.

1.2.2 DIMENSÃO MORAL NO AMBIENTE FAMILIAR

Como no presente momento, a internet e tecnologia regem a vida de grande parte da população, tudo o que se faz ou se deixa de fazer na vida digital tem severos reflexos na vida real, qualquer informação mal interpretada, incompleta ou incorreta, pode mudar o rumo de uma vida permanentemente, trazendo, inclusive, prejuízos diretos a

honra dos usuários. Tudo o que é feito na internet é rapidamente propagado, por exemplo, um comentário mal escrito, um vídeo constrangedor postado em redes sociais, uma foto íntima vazada, dentre diversas outras coisas que podem vir a ser motivo de julgamento e zombaria por toda a internet, afetando diretamente a vítima. Não podemos deixar de citar também os crimes de dimensões morais que são cometidos no meio digital e que infelizmente a nossa legislação ainda não é clara em relação a eles, como foi dito por Araújo (2010): “(...) Nossa legislação não tem Lei que especifique os crimes praticados via internet e a responsabilidade civil de autores de matérias ou mensagens que causem danos morais às vítimas”.

Como os meios digitais possibilitam o anonimato, a ocorrência de assédios, *bullying* e depredação moral tem uma dimensão enorme e as autoridades legislativas ainda não possuem o controle desses atos danosos. Outro ponto que também não deve ser esquecido, é o fato de que nossas crianças possuem um amplo acesso a tudo que está exposto na internet, e se a supervisão dos guardiões for falha, as crianças podem ter acesso a conteúdo de caráter adulto, como, por exemplo, pornografia e violência e, no pior dos casos, além de perderem a inocência podem ser vítimas de crimes horríveis como a pedofilia ou até mesmo casos de automutilação, como recentemente vimos, no caso da “Baleia azul” e da escultura japonesa “Momo”, registrados a pouco tempo no mundo.

O caso da “Baleia azul” foi registrado em vários países distintos, tendo como origem, em 2013, a Rússia. O ocorrido era que uma pessoa começava com jogos de automutilação e sofrimento e acabava quando chegavam no último nível, cometendo suicídio. Os criadores usavam de pesquisas para identificar possíveis vítimas para participar do jogo. Como o *link* do jogo não era público, os criadores selecionavam pessoas pelos seus perfis, geralmente pessoas com baixa estima, depressão, e jovens adolescentes que passavam por momentos difíceis da vida, cujos perfis permeavam questões, tais como: “as pessoas gostam de mim”, “sou suficiente para meus amigos” ou “quem sou eu”?

Assim que uma dessas vítimas selecionadas clicava no *link* do jogo, enviado, prévia e especificamente, pelo criador para eles, os dados dos seus *smartphones* eram copiados para os administradores e assim o jogo começava, e o usuário ficava preso, já que uma vez que os administradores obtinham seus dados, eles começavam a

ameaçar os jovens em caso de desistência. Os desafios variavam desde cortar os próprios pulsos, até assistir um filme de terror no meio da noite, no intuito de conduzi-los à prática do suicídio.

O jogo da “Baleia azul” foi responsável por mais de 100 mortes em vários países, isso identifica como o uso doméstico de computadores também precisa ser educado, pois por um simples descuido, tanto dos pais como da própria criança, pode acarretar uma coisa gravíssima, podendo dar fim a uma vida (SHARMA, 2017).

O desafio viral da “Momo do *WhatsApp*” é uma lenda urbana que se espalhou pela internet do mundo todo com o propósito de assustar os usuários do aplicativo de mensagens instantâneas *WhatsApp.* O desavio se trata de um número de celular onde a foto de perfil da conta é uma imagem assustadora de uma escultura japonesa exposta no museu *Vanilla Gallery*, no Japão, em 2016, cuja escultura é nomeada como “mulher-pássaro”.

O desavio consiste em incitar a vítima a ter coragem de entrar em contado com a assustadora Momo. As pessoas que salvaram o número desse perfil e conseguiram entrar em contado dizem que a boneca japonesa adivinha informações pessoais, liga de madrugada, e envia fotos e vídeos de cunho violento e assustador, e que até mesmo fazia ameaças; outras pessoas, no entanto, dizem que ela nem sequer respondia. Com a fama que esse desafio alcançou várias pessoas ao redor do mundo, muitos começaram a criar perfis se passado pela Momo, o que causou muitos problemas para a segurança desses usuários que se submetiam a tal desafio.

Segundo o site BBC, os riscos que essas pessoas podem correr participando desse viral é o furto de informações pessoais, incitação ao suicídio e a violência, além de assédio e extorsão, bem como são ações que podem afetar a saúde mental com transtornos físicos e psicológicos, tais como ansiedade, depressão, insônia, crises de pânico, etc. (BBC, 2018).

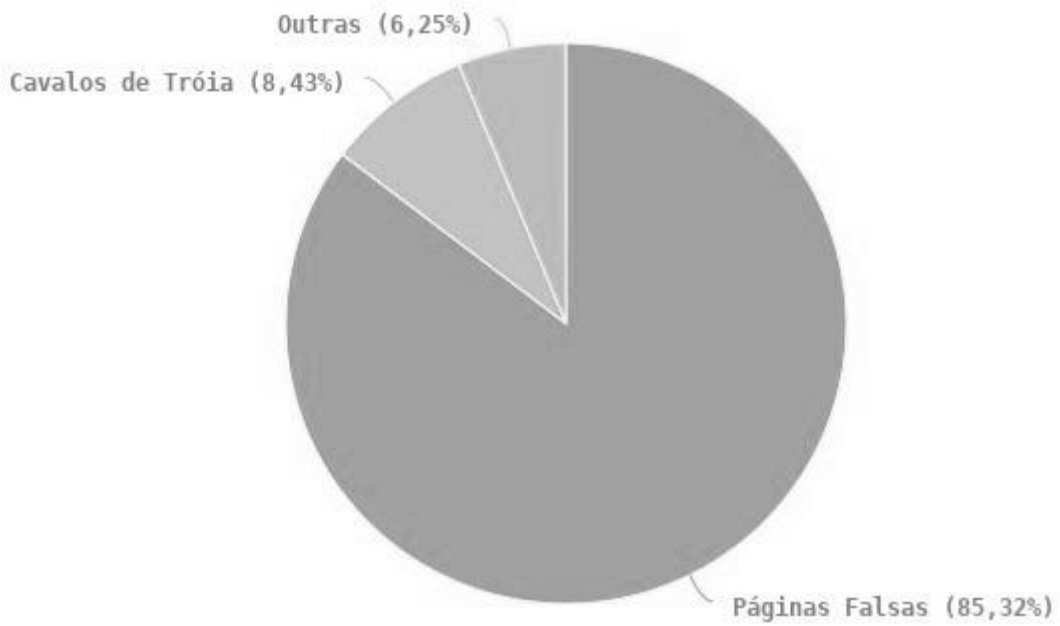
1.2.3 DIMENSÃO ECONÔMICA NO AMBIENTE FAMILIAR

Como se não bastassem todos os perigos já citados, a família também deve ser cautelosa e preparada para não sofrer prejuízos financeiros com o uso incorreto da internet.

As fraudes digitais de cunho financeiro são um pouco mais difíceis de serem aplicadas ou planejadas do que os furtos e roubos convencionais, pois o criminoso precisa ter conhecimentos específicos para a concretização dos delitos digitais, assim como utilizarem de técnicas específicas da Engenharia Social para ludibriar os usuários de internet, como, por exemplo, na criação de *sites* falsos, e na elaboração de *phishing.*

No gráfico apresentado abaixo mostraremos dados recolhidos pelo Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil (CERT.br) em relação as tentativas de fraudes em 2017.

Gráfico 1 - Incidentes Reportados ao CERT.br (janeiro a dezembro de 2017): tentativas de fraudes



Fonte: Cert.br, 2017

O gráfico 1 apresenta informações sobre os incidentes, e podemos observar números realmente preocupantes em relação a páginas falsas, seguido por cavalos de tróia e outras tentativas de fraude.

Podemos observar ainda a Tabela 1 com os principais temas usados por criminosos para a propagação dos *e-mails* falsos.

Tabela 1: Exemplos de temas de mensagens de *phishing*

Tema	**Texto da mensagem**
Cartões virtuais	UOL, *Voxcards*, Humor Tadela, O Carteiro, *Emotioncard*, Criança Esperança, AACD/Teleton.
SERASA e SPC	Débitos, restrições ou pendências financeiras.
Serviços de governo eletrônico	CPF/CNPJ pendente ou cancelado, Impostos de Renda (nova versão ou correção para o programa de declaração, consulta de restituição, dados incorretos ou incompletos na declaração), eleições (título eleitoral cancelado, simulação de urna eletrônica).
Álbuns de fotos	pessoa supostamente conhecida, celebridade, relacionado a algum fato noticiado (em jornais, revistas, televisão), traição, nudez ou pornografia, serviço de acompanhantes.
Serviço de telefonia	pendência de débito, aviso de bloqueio de serviços, detalhamento de fatura, crédito gratuitos para celular.
Antivírus	a melhor opção do mercado, nova versão, atualização de vacinas, novas funcionalidades, eliminação de vírus do seu computador.
Notícias/boatos	fatos amplamente noticiados (ataques terroristas, tsunami, terremotos, etc), boatos envolvendo pessoas conhecidas (morte, acidentes ou outras situações chocantes)
Reality shows	BigBrother, Casa dos Artistas, etc -- fotos ou vídeos envolvendo cenas de nudez ou eróticas, discadores.
Programas ou arquivos diversos	novas versões de *softwares,* correções para o sistema operacional Windows, músicas, vídeos, jogos, acesso gratuito a canais de TV a cabo no computador, cadastro ou atualização de currículos, recorra das multas de trânsito.
Pedidos	Orçamento, cotação de preços, lista de produtos
Discadores	para conexão Internet gratuita, para acessar imagens ou vídeos restritos.
Sites de comércio eletrônico	atualização de cadastro, devolução de produtos, cobrança de débitos, confirmação de compra.
Convites	convites para participação em sites de relacionamento (Como Orkut) e outros serviços gratuitos
Dinheiro Fácil	descubra como ganhar dinheiro na Internet.
Promoções	diversos.
Prêmios	loterias, instituições financeiras.
Propaganda	produtos, cursos, treinamentos, concursos.
FEBRABAN	cartilha de segurança, avisos de fraude.
IBGE	censo.

Fonte: Informação adaptada de Comitê Gestor da Internet (2018, p. 2)

Todos os temas apresentados nessa tabela são muito comuns, o que indica que qualquer pessoa é vulnerável a sofrer com *phishing.*

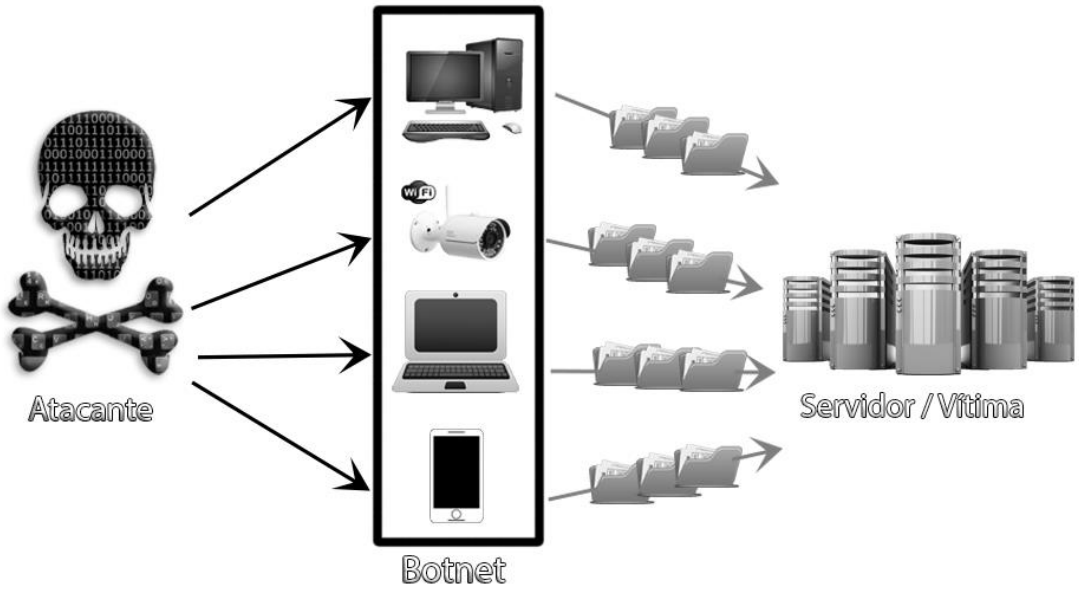
1.3 - CONCEITUAÇÃO DE *DOS* OU *DDOS* E A COMPOSIÇÃO TÉCNICA

Um ataque silencioso, muito vezes imperceptível, e que não tem intenção no primeiro momento de submergir e conseguir informações, mas de destruir um dos pilares da segurança, a disponibilidade, nós chamamos tal ato como ataque de negação de serviço, *Denial of Service* (*DoS*).

Segundo o *site* Cert.br (2016) *DoS* é uma técnica pela qual um atacante utiliza um equipamento conectado à rede para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de ataque Distribuído de Negação de Serviço (*DDoS* - *Distributed Denial of Service*).

Na imagem 1, será ilustrada um ataque distribuído de negação de serviço, em que um atacante, por meio de pacotes enviados para dispositivos com possíveis falhas de segurança, transforma esses dispositivos em “zumbis”, no intuito de enviar pacotes multiplicados para um servidor. Este dispositivo será vítima de um ataque de negação de serviço, pois terá um serviço, ou mesmo o servidor inteiro, retirado de operação por uma vulnerabilidade explorada.

Imagem 1- Ilustração de ataque



Fonte: Imagem adaptada de Rossow (2014, p. 2)

Como visto, o atacante faz o uso de uma *botnet* para realizar o ataque. O atacante envia um único pacote pequeno de dados que, uma vez interpretados pelos dispositivos componentes da *botnet,* começam a enviar dados para os servidores. Esses dados são variados, vão de requisições de nomes, requisição de definição da hora do sistema, requisição de *login* em servidores de jogos, requisições de *logs* de servidores, entre muitas outras requisições, que aparentemente são tráfego legitimo de informações, porém, um atacante pode utilizar-se disso para realizar como se fosse uma requisição múltipla e repetitiva desses dados, causando assim, a indisponibilidade do sistema atacado.

Segundo o artigo “Amplification hell”, de Christian Rossow, um atacante manda requisições para os amplificadores com o IP da vítima como pacotes para os amplificadores. Em retorno, os amplificadores enviam (multiplamente) várias respostas para o destinatário (no caso, a vítima).[2]

[2] “An attacker sends requests to amplifiers with the victim’s IP address as IP packet source. In turn, the amplifiers send (potentially multiple) large responses to the victim”. Christian ROSSOW. **Amplification hell,** *p. 2. Tradução própria!*

CAPÍTULO 2 - ENGENHARIA SOCIAL E POLÍTICA DE SEGURANÇA

O elo mais fraco e imprevisível em relação a segurança de uma empresa é o ser humano, ou seja, o fator humano, a organização pode tentar blindar todo o seu sistema de informações de todas as maneiras possíveis, mas se seus funcionários não forem conhecedores e muito bem conscientizados sobre as políticas de segurança da empresa, nenhum sistema de segurança será capaz de proteger os dados dessa companhia. É muito importante abordar o tema Engenharia social, e treiná-los para que evitem ao máximo esse tipo de ataque.

Engenharia social é quando uma pessoa, por meio de conversa, documentos falsos, itens deixados para trás propositalmente, etc., tenta entrar em uma empresa para furtar dados ou instalar *softwares* maliciosos nos computadores das empresas, a fim de poder tomar o controle de suas máquinas em caso de ataques *DDoS*, furtar dados para vendê-los para empresas adversárias do mesmo ramo ou simplesmente para sequestrar os arquivos de uma empresa para pedir resgate posteriormente.

> Engenharia social, dentro da área de segurança de sistemas computacionais, é um termo utilizado para qualificar os tipos de intrusão não técnica, que coloca ênfase na interação humana e, frequentemente, envolve a habilidade de enganar pessoas objetivando violar procedimentos de segurança. Um aspecto relevante da engenharia social compreende a inaptidão dis indivíduos manterem-se atualizados com diversas questões pertinentes à tecnologia da informação, além de não estarem conscientes do valor da informação que eles possuem e, portanto, não terem preocupação em protegê-la (PORTAL EDUCAÇÃO, 2013).

Essas características, por mais que não parecem, são muito comuns, um ótimo exemplo é quando um funcionário encontra um *pendrive* no chão, a primeira coisa que ele faz é levar o *pendrive* para a empresa ou sua casa e ir direto espetando em um computador. Isso não está correto, pois este dispositivo pode ter sido deixado lá por uma pessoa mal-intencionada, e conter um vírus que vai prejudicar sua empresa ou computador pessoal, para isso, as pessoas deveriam pedir a algum administrador de rede para que o analisassem ou o objeto deixado em questão a fim de verificar possíveis arquivos falsos ou danosos. Por esses motivos de descuidos de usuários

ou até mesmo um possível descuido de um administrador de rede de fazer o mesmo, existem as políticas de segurança.

Segundo o Portal “Alerta Security” (2017):

“Uma Política de Segurança da Informação (PSI) funciona como um planejamento da forma como a empresa lida com seus ativos de informação, ou seja, aquilo que produz ou contém informações de valor" (ALERTA SECURITY, 2017).

As políticas de segurança da informação servem para colocar margens a possíveis erros causados por usuários como seres humanos. Elas são elaboradas pela equipe técnica em parceria com as gerências de setores para definir quais são as melhores práticas para se adotar em determinadas situações, como, o usuário não poder espetar um USB sem antes passar por análise, o financeiro não aprovar um pedido sem antes passar pelo gerente, usuários com baixo acesso não poderem instalar programas sem o auxílio de um administrador, entre outros exemplos.

Uma política de segurança pode ajudar o administrador de rede a não cometer erros, como conter algum procedimento que exija que o administrador faça testes ou mesmo preveni-lo de realizar alguma ação já discutida previamente pela equipe responsável pelas políticas de segurança e que, eventualmente, acarrete algum dano à empresa, ou, pelo menos, ao autor da infração à política de segurança, que deve necessariamente se responsabilizar pelos seus atos. Enfim, uma boa política de segurança sozinha, bem aplicada e com usuários conhecedores dela, pode evitar muitos problemas, entre eles, o do ataque de *DDoS*.

2.1 – ENGENHARIA SOCIAL E VULNERABILIDADES

Como em todo ataque cibernético, os humanos possuem um grande papel no sucesso ou fracasso. A capacidade de manipulação dos criminosos é muito preocupante e deve receber a devida atenção de todos os funcionários. Em um primeiro momento é muito difícil relacionar ataques de negação de serviço com a tão temida Engenharia social, pois o atacante não precisa estabelecer um contado direto com a vítima, mas se esse contado for estabelecido ele pode desfrutar de todo o seu poder de manipulação em benefício próprio.

A Engenharia social usada em conjunto com qualquer ataque ou exploração de vulnerabilidades, pode potencializá-los radicalmente. Uma vez que um atacante ganhar acesso a uma máquina, ele terá várias formas de utilizá-la; imagine, portanto, se este atacante, ainda contar com a ajuda de um usuário desavisado? Um ótimo exemplo disso é que, muita gente, sem ter conhecimento dos perigos de segurança, acabam comprando *pendrives* baratos e levando-os diretamente ao seu trabalho ou residência sem ter consciência dos riscos que possa estar sofrendo.

Uma empresa com uma boa política de segurança alertaria esse usuário de que antes de plugar um *pendrive* em qualquer máquina, o dispositivo móvel deveria ser analisado para verificar a possibilidade de causar danos a empresa ou máquinas da empresa, visto que esse dispositivo pode estar infectado com algum código malicioso. Esse artefato, por sua vez, pode ser deixado propositadamente pelo atacante em frente a uma empresa qualquer, visando justamente furtar informações com a ajuda de um funcionário desavisado que poderia inserir o dispositivo em um computador.

A prática citada é considerada Engenharia social, pois conta com a ajuda de um intermediário humano para levar o *pendrive* corrompido para a empresa, para então, liberar as portas para um atacante. Fora isso, muitas pessoas podem se passar por chefes e/ou supervisores, para conseguir senhas de acesso interno à empresa, facilitando também o uso não autorizado por atacantes que podem usar um único computador dentro de uma empresa para fazerem todos os computadores virarem zumbis para auxiliarem em um ataque em larga escala.

2.2 – POLÍTICA DE SEGURANÇA E *DDOS*

As políticas de segurança são extremamente eficientes para a prevenção das ações de engenharia social e para uma conscientização global das normas de segurança de uma empresa. As políticas de segurança funcionam como uma parede entre os funcionários e os atacantes. Com uma boa e complexa elaboração e com ampla divulgação, as chances de que os funcionários causem danos por engano à corporação diminui muito. Investir em uma boa política de segurança pode evitar que ataques possam partir da própria rede ou gerados pelos dispositivos dos usuários. Muitas vezes, investir em uma boa política de segurança é mais seguro que gastar

com uma infraestrutura de custos altos. Uma vez que o usuário for conscientizado, ele irá se policiar antes de expor a empresa às vulnerabilidades; um usuário que foi treinado e adaptado a ler seus *e-mails* sem sair clicando em qualquer *link* que aparece dentro, ajudará muito no tocante à questão de segurança. Um usuário não vai aprender da noite para o dia as políticas de segurança ou até mesmo como se defender de arquivos maliciosos e seus atacantes, mas uma boa política de segurança implica que o recrutador do trabalhador deve repassar toda a informação da política para o funcionário. E não basta apenas isso, o acompanhamento no dia a dia é extremamente necessário para que o usuário não cometa um deslize e caia em um *e-mail* de *phishing,* por exemplo. Para isso, muitos administradores de rede recorrem ao uso de ferramentas de manipulação de eventos e situações para acostumar o usuário a seguir e se atentar às normas e regras estabelecidas nestas políticas de segurança de uma empresa.

Um exemplo que podemos citar sobre danos que podem ser causados à empresa que não possui política de segurança é o caso da empresa norte americana Federal *Deposit Insurance Corp* em que “um ex-funcionário baixou informação sensível para um dispositivo de armazenamento pessoal inadvertidamente e sem uma má intenção” (ESET, 2017, p. 2).

2.3 – EXEMPLOS DE VULNERABILIDADES TÉCNICAS CAUSADORAS DE “ATAQUES” *DDOS*

Como os ataques de negação de serviço nem sempre são facilmente detectados, as formas de prevenir tais ataque acabam por ficar mais difíceis e menos intuitivas. Nesta seção iremos abordar várias vulnerabilidades que podem se tornar a porta de entrada para ataques *DDoS*. Grandes meios de acesso por atacantes para realizar um ataque de negação de serviço são os protocolos, com falhas ou mal configurados, que podem apresentar riscos para qualquer usuário.

Alguns protocolos de uso legítimo como o *snmp*, são usados, por exemplo, por atacantes controlando uma *botnet* para poder derrubar uma vítima. O protocolo *snmp* é usado para requisitar informações de um computador para verificação de hardware, *software* e processos rodando em uma máquina; esse relatório gerado pelo *snmp*

pode ajudar um administrador de rede a coletar informações de máquinas em sua rede sem precisar sair de sua sala. No entanto, se este protocolo estiver aberto a qualquer pessoa ou acessível por qualquer lugar em uma rede aberta, por exemplo, poderá ser usado para enviar as informações de um computador para a vítima ao invés de enviar para o seu administrador de rede, encaminhando dados massivos da máquina, como o conteúdo do protocolo *snmp*, para uma vítima, que pode derrubar a rede por receber um tráfego muito grande de informações em um curto período de tempo. A princípio, o protocolo e seus dados são legítimos, mas em grande quantidade um servidor pode não ter tempo de processar o que é informação utilizável e o que é lixo de rede, assim não consegue descartar os pacotes a tempo, fazendo com que sua rede caia, derrubando o servidor e os serviços contidos nele[3].

Outro protocolo muito utilizado é o NTP. No artigo de Christian Rossow sobre ataques *DDoS*, é citado que dentro dos servidores contendo configurações para acerto de hora e data são encontrados requerimentos chamados de *monlist*, os quais podem ser usados como amplificadores, pois quando um servidor de tempo requisita a *monlist* armazenada, o servidor envia a lista de clientes recentes que fizeram esta requisição. Esta lista, por sua vez, pode conter vários clientes, o que acaba por aumentar amplamente o número de pacotes enviados à vítima. Este é o protocolo com maior amplificação de banda dos protocolos estudados. Na lista abaixo, retirada do documento de Rossow, podemos ver os protocolos utilizados para a exploração de negação de serviço, a banda multiplicada consumida por protocolo (BAF) e o amplificador de pacotes do protocolo (PAF).[4]

---

[3] "We found that SNMP v2 supports the GetBulk operation, in which a device returns a list of SNMP identifiers that can be monitored. In the legitimate use case, this request can be used to iterate all monitoring values. An attacker can abuse this feature to amplify traffic by factor 6.3. The exact response size is determined by the number and length of identifiers in the returned item list. If an attacker abuses only the 10% subset of the amplifiers that reply with the largest payload, the BAF increases to 11.3.". Christian ROSSOW. **Amplification Hell:** Revisiting Network Protocols for *DDoS* Abuse, p. 5. - *Tradução nossa!*

[4] "We found that NTP servers support the monlist request, (…). One response datagram specifies statistics for NTP clients (such as the client's IP address, its NTP version and the number of requests) who contacted this NTP server – a useful debugging feature in the legitimate use case. The total response length depends on the number client statistics a server shares upon request. On average, monlist requests amplify the request traffic by factor 556.9–4670.0, the highest BAF in our measurements.". Christian ROSSOW. **Amplification Hell:** Revisiting Network Protocols for *DDoS* Abuse, p. 5. - *Tradução nossa!*

Tabela 2 – Protocolos *DDoS* e seus amplificadores

Protocol	BAF *all*	BAF 50%	BAF 10%	PAF *all*	Scenario
SNMP v2	6.3	8.6	11.3	1.00	*GetBulk* request
NTP	556.9	1083.2	4670.0	10.61	Request "monlist" statistics
DNS_{NS}	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS_{OR}	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	*SEARCH* request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Sality	37.3	37.9	38.4	1.00	URL list exchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

Fonte: Rossow, 2014, p. 5.

Na Tabela 2 é demonstrado os protocolos citados e seus fatores de amplificação.

2.4 – CRIMES CIBERNÉTICOS VIA "ATAQUES" *DDOS*: MUNDO CRACKER

Para começarmos a discorrer sobre crimes cibernéticos é importante que saibamos o que é, e de onde surgiu tal termo. Segundo o Blog Cibercrimes (2018), vinculado à disciplina de "Comunicação e Tecnologia", sob a orientação do prof. André Lemos, da Faculdade de Comunicação, na Universidade Federal da Bahia, o termo teve sua origem em uma reunião de sete grupos compostos pelas maiores potencias econômicas e a Rússia, denominados de Brics, que, por volta dos anos 90, discutiam o combate a tais práticas, e foi daí que o termo "cybercrime" em inglês surgiu, que traduzido para o português se torna "ciber crime" ou "crimes cibernéticos" (CIBERCIMES, 2018).

Os crimes cibernéticos são definidos de vários pontos de vista por diversos autores diferentes, para o autor Sérgio Marcos Roque, por exemplo, citado por Rossini, “crime informático é conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material” (ROQUE *apud* ROSSINI, 2004, p. 109).

Já para André Queiroz, crime cibernético é:

> […] Um delito típico de *internet* seria quando uma pessoa se utiliza de um computador acessando a rede, invade outro computador e obtém, destrói, ou altera um arquivo pertencente ao sistema, ainda que não havendo qualquer obtenção de vantagem patrimonial, mas tão somente a obtenção, destruição ou alteração de dados daquele sistema restrito – circunstância esta que já caracterizaria o tipo penal específico (QUEIROZ, 2008, p. 174).

Aqui no Brasil o assunto crime cibernético para as legislações é bastante novo, e por esse motivo as definições de crimes cibernéticos envolvendo *DDoS* é muito vaga, mas muitos atos no qual esse tipo de ataque está envolvido podem sim ser considerados crime.

Em 2012 a Lei 12.737, mais conhecida como "Lei Carolina Dieckmann", alterou o Código Penal para incluir como crime a ação que "interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento" (BRASIL, 2012). Como podemos notar a lei é muito vaga, devemos nos lembrar que tudo isso é muito novo no Brasil e os juízes podem ter diferentes interpretações da lei, mas o que chama muito a atenção é que mesmo que os ataques *DDoS* não tenham tido nenhum caso de condenação e repercussão, estes podem causar muitos danos e podem estar previstos e protegidos pela lei, como, por exemplo, no Brasil, a invasão de computadores de terceiros é considerado crime, e esse computadores que estão sendo invadidos talvez podem estar participando de uma *botnet* que, por consequência, leva a participação desses computadores em ataques *DDoS*.

Segundo o *site* Olhar Digital (2005-2018), um dos maiores ataques de negação de serviço já registrado foi ao site GitHub, destinado a programadores e tem como objetivo compartilhar códigos de *softwares*, livres ou fechados. O ataque aconteceu no dia 28 de fevereiro deste ano, teve duração de 10 minutos e, no seu pico, foi

registrado um tráfego de 135 *Terabits* por segundo. A organização afirma que foram usados "mais de mil sistemas autônomos diferentes em dezenas de milhares de terminais únicos" (OLHAR DIGITAL, 2005-2018) para a efetivação do ataque. Os hackers tiraram proveito de uma vulnerabilidade do protocolo de distribuição que colocava dados de cache na memória RAM do servidor, assim, acelerando muito a navegação de sites que dependem de bancos de dados, como resultado, o site ficou fora do ar durante o ataque. No entanto, o GitHub afirma que os dados não foram comprometidos; dizem, ainda, que outros ataques já estão sendo previstos e que estão tomando todas as providencias necessárias para mitigá-los (CARVALHO, 2018 *IN.:* OLHAR DIGITAL, 2005-2018).

CAPÍTULO 3 - TESTES EXPLORATÓRIOS DE VULNERABILIDADES EM FACE DOS “ATAQUES” *DDOS*

3.1 – DESCRITIVO DO PROCESSO TÉCNICO

Para a realização dos testes nós iremos montar um ambiente controlado para que possamos identificar e mostrar as vulnerabilidades em que os ataques de negação de serviço se beneficiam.

Para a realização destes testes iremos utilizar dez computadores físicos *desktop* com as seguintes configurações: Sistema operacional Windows 10 Enterprise x64 bits, com um processador i5-7500 de 3.4GHz e 8GB de memória RAM. Estas configurações são das máquinas *hosts*, as máquinas virtuais (VM’s) foram utilizadas em todos os dez computadores com as seguintes configurações: Windows 7 Professional x64 bits, com um i5-7500 de 3.4GHz, igual ao da máquina *host*, pois o processador é herdado, e memória de 2GB. O *software* para emular as máquinas virtuais foi o VirtualBox em sua versão 5.2.20 r125813. Como servidor para ser atacado, utilizamos o FreeBSD na versão 11.2-RELEASE com o auxílio de pacotes para simular um servidor web, que seria derrubado pelo ataque; para isso, utilizamos os pacotes do Apache 2.4.37 em união com o PHP 5.6.38, a fim de poder exibir uma página de informações em que pudéssemos ver quando ela pararia de ser acessada.

Para visualizar o tráfego da rede no servidor FreeBSD, utilizamos o pacote *IPAudit* que nos mostra a quantidade de pacotes entrando no servidor. Do outro lado, no Windows 7, utilizamos o *software* HOIC (High Orbit Ion Cannon) que foi projetado para fazer testes de stress em servidores web.

Salientamos, ainda, que *softwares* como este servem para uso legítimo de teste de performance de servidores, porém, usados ilegalmente, podem causar danos profundos.

Neste teste, nós colocamos a página web de teste no programa atacante e definimos cinco *threads* para o programa realizar acesso ao servidor, isso se fez necessário, pois torna-se possível enviar várias vezes requisições de acesso a página, mas com um *delay* para retornar a página, fazendo com que o servidor fique aguardando o “resto” do acesso, sem enviar a página completa de volta para o requisitante. Fazendo isso, o servidor fica com muitos requerimentos de acesso a página e não retorna todos

no momento exato, fazendo com que ele inunde de requisições sem devolver a resposta a ninguém.

Todos os dez computadores utilizados para os testes tiveram a mesma configuração no *software* HOIC, isso exemplificou uma *botnet* de apenas dez máquinas atacando um servidor web, cada um contou com os cinco threads como citado, sendo que o programa permite, dependendo dá potência da máquina utilizada, rodar até 100 *threads* ao mesmo tempo.

Este teste de ataque é considerado como ataque moderado, sendo que não envia muito tráfego de rede para o servidor atacado, mas sim várias requisições de acesso à página. Existem outros testes e ataques reais, como o ocorrido no caso já citado do GitHub, em que mais de mil máquinas são utilizadas para enviar dados de rede para o servidor atacado, testes em grande escala ou com grandes *botnets* podem derrubar sites de grande porte.

3.2 – *PRINTS*, TABELAS COMPARATIVAS, IMAGENS, ETC., NO INTUITO DE VALIDAR AS FALHAS DE ENTREGAS DE SERVIÇOS (*DDOS*)

Nas *prints* abaixo, podemos observar a configuração das máquinas tanto físicas quanto virtuais:

Imagem 2- Configuração máquinas *host*

Fonte: Autoria própria (2018) com base no Sistema operacional Windows 10

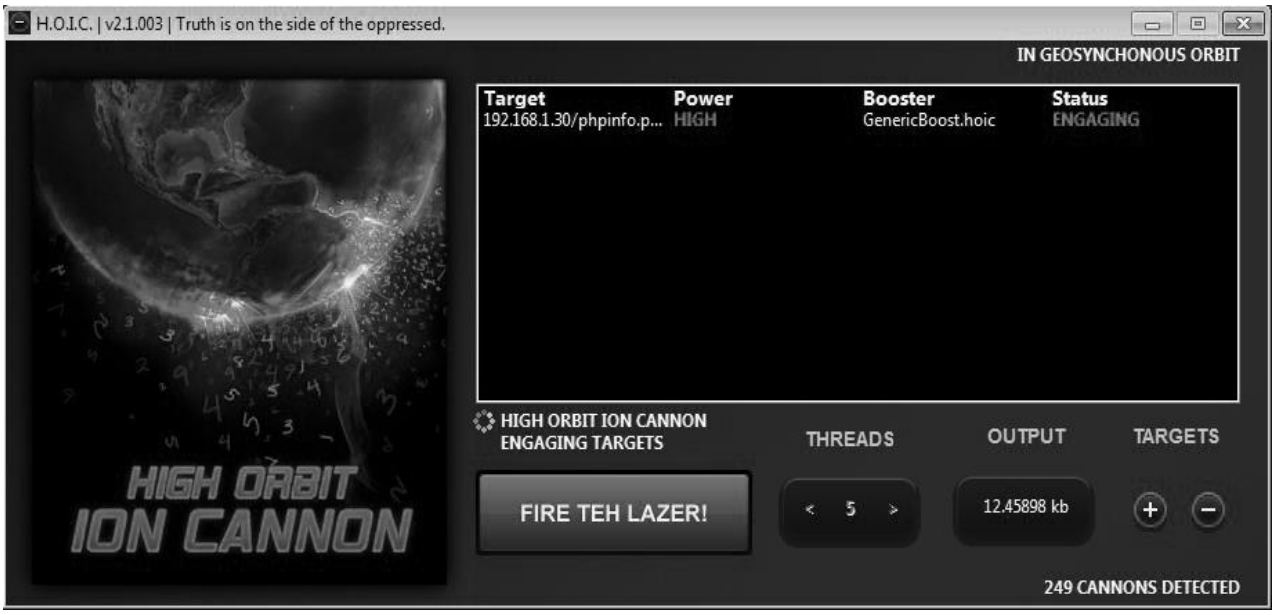
Na Imagem 2, observamos as configurações do computador hospedeiro como citado, Windows 10 Enterprise, com i5-7500 3.4GHz e 8GB de memória.

Imagem 3- Configuração das máquinas virtuais

Fonte: Autoria própria (2018) com base no Sistema operacional Windows 7

Na Imagem 3, observamos a descrição da máquina virtual como citado, Windows 7 Professional com i5-7500 3.4GHz e 2GB de memória.

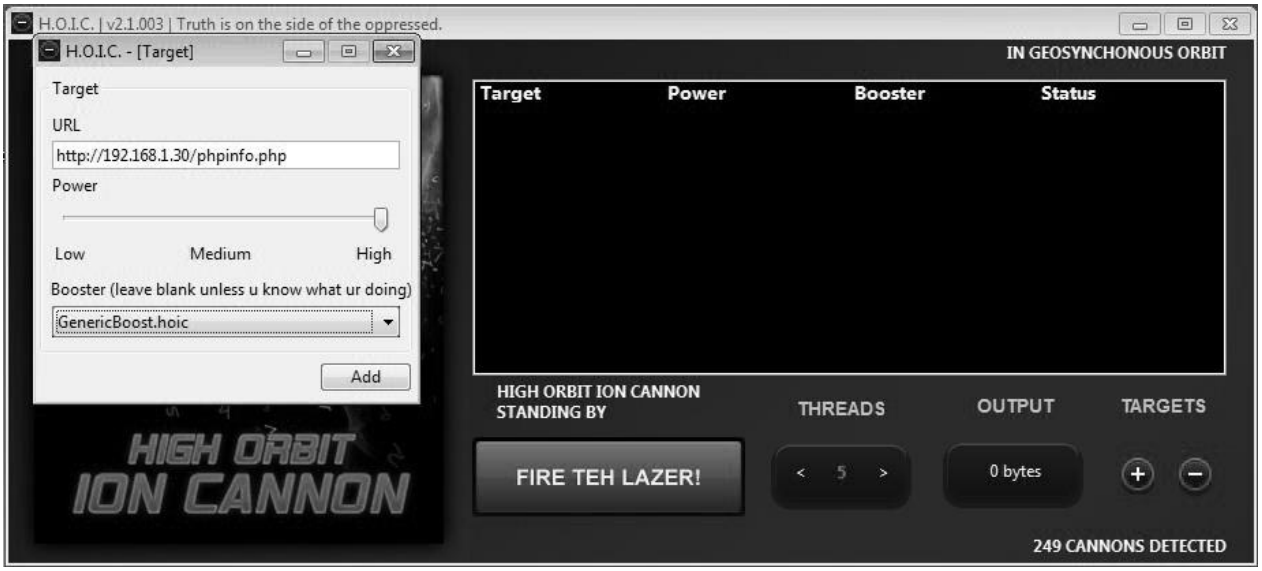
Imagem 4 – Configuração do programa HOIC



Fonte: Autoria própria (2018) com base no HOIC

Na Imagem 4, podemos observar a configuração do programa HOIC para realizar o *stress* do servidor web. Essa configuração foi feita com base em tutoriais retirados de vídeos do *Youtube,* entre eles o vídeo “Como baixar instalar e usar o (HOIC)”, disponibilizado pelo canal “Estilizando”.

Imagem 5 – HOIC em execução



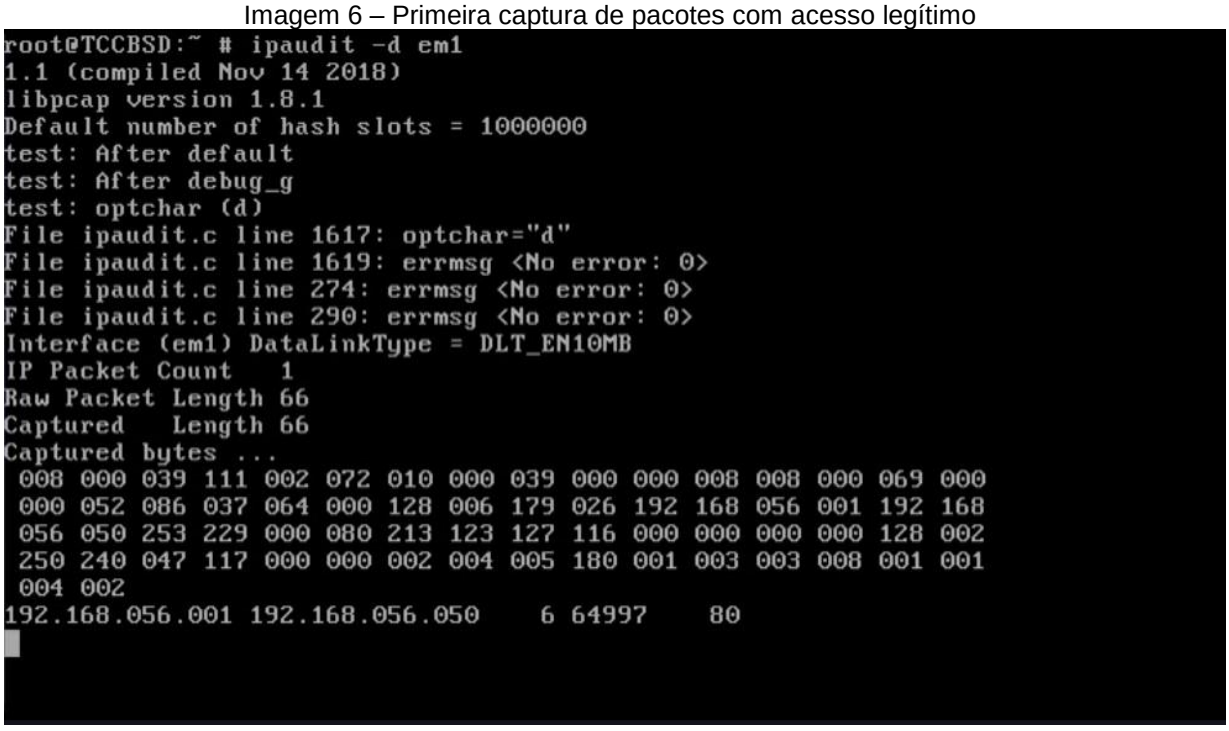
Fonte: Autoria própria (2018) com base no HOIC

Na Imagem 5, podemos observar o HOIC em execução; ele está enviando pacotes para o servidor web. Podemos verificar os pacotes enviados no campo *output* do

programa. Como observado, na *interface* do programa fica o *Targert,* que é o servidor/página que nós estamos atacando, logo à frente fica o *Booster,* que é o amplificador utilizado; nesse caso, é um genérico disponibilizado pelo próprio programa em seu código, e mais a frente podemos ver o *Engaging,* que significa que o programa está executando.

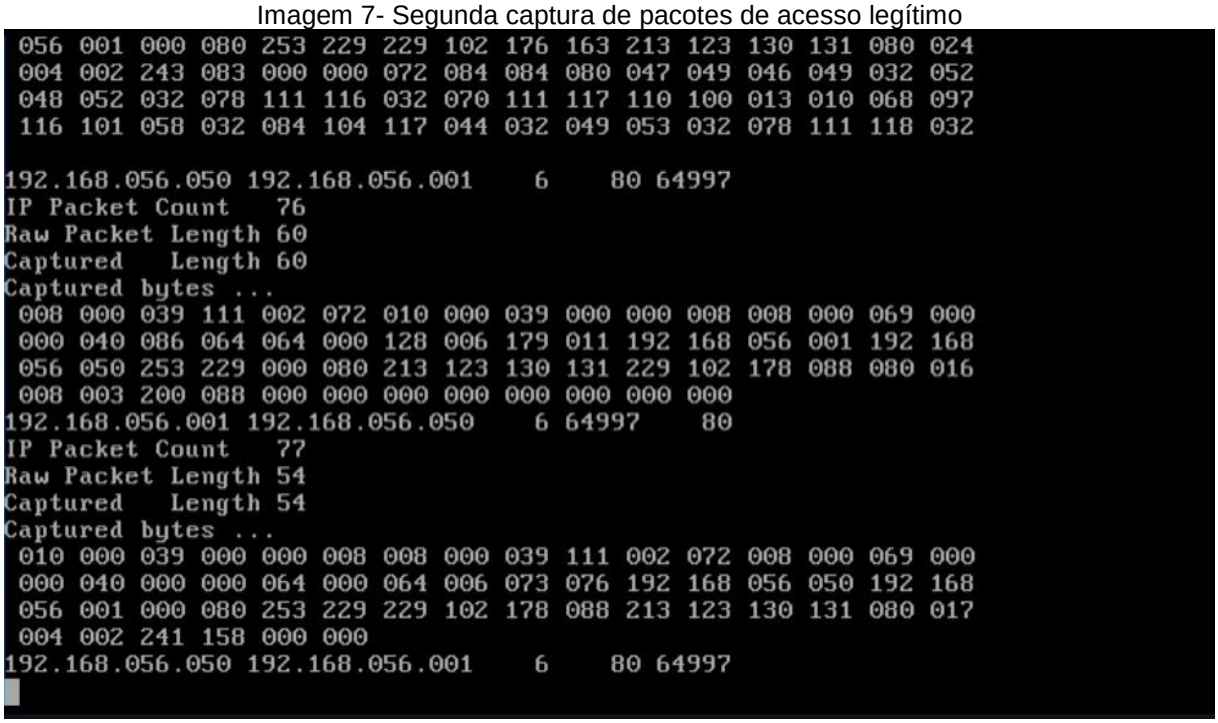
Nas páginas seguintes, exporemos as Imagens 6 e 7, nas quais verificaremos a captura de pacotes com acesso legítimo, em duas etapas: primeira e segunda capturas.

Imagem 6 – Primeira captura de pacotes com acesso legítimo



Fonte: Autoria própria (2018) com base no Sistema operacional FreeBSD

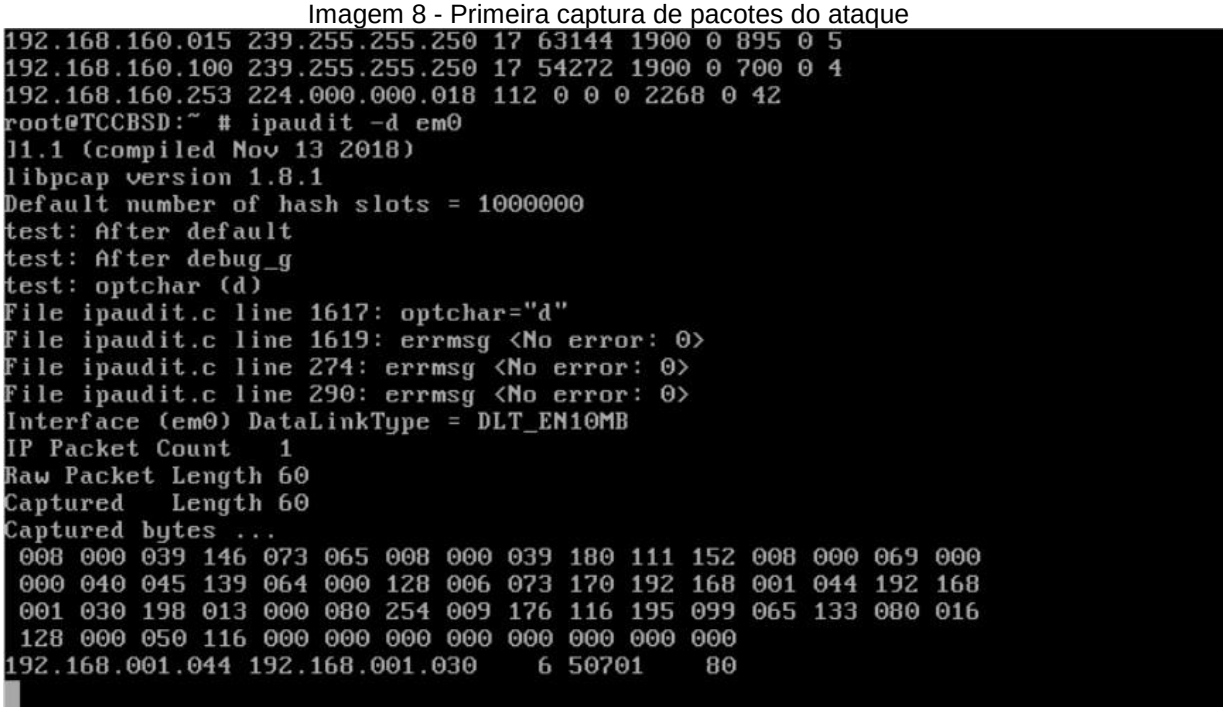
Imagem 7- Segunda captura de pacotes de acesso legítimo



Fonte: Autoria própria (2018) com base no Sistema operacional FreeBSD

Na Imagem 6, podemos observar o começo da captura dos pacotes pelo *software IPAudit*. Nesta, na décima segunda linha, podemos verificar a saída de comando *IP Packet Count,* com isto, verificamos que começa a contagem de pacotes recebidos em 1, que é como deve começar em um acesso legítimo, após a requisição de um computador para exibir a página de informações do servidor. Na Imagem 7, por exemplo, explicita o carregamento concluído da página web, ainda com uma contagem pequena e legítima de pacotes, ou seja, com 77 pacotes, conforme indicado na décima quinta linha da Imagem correspondente.

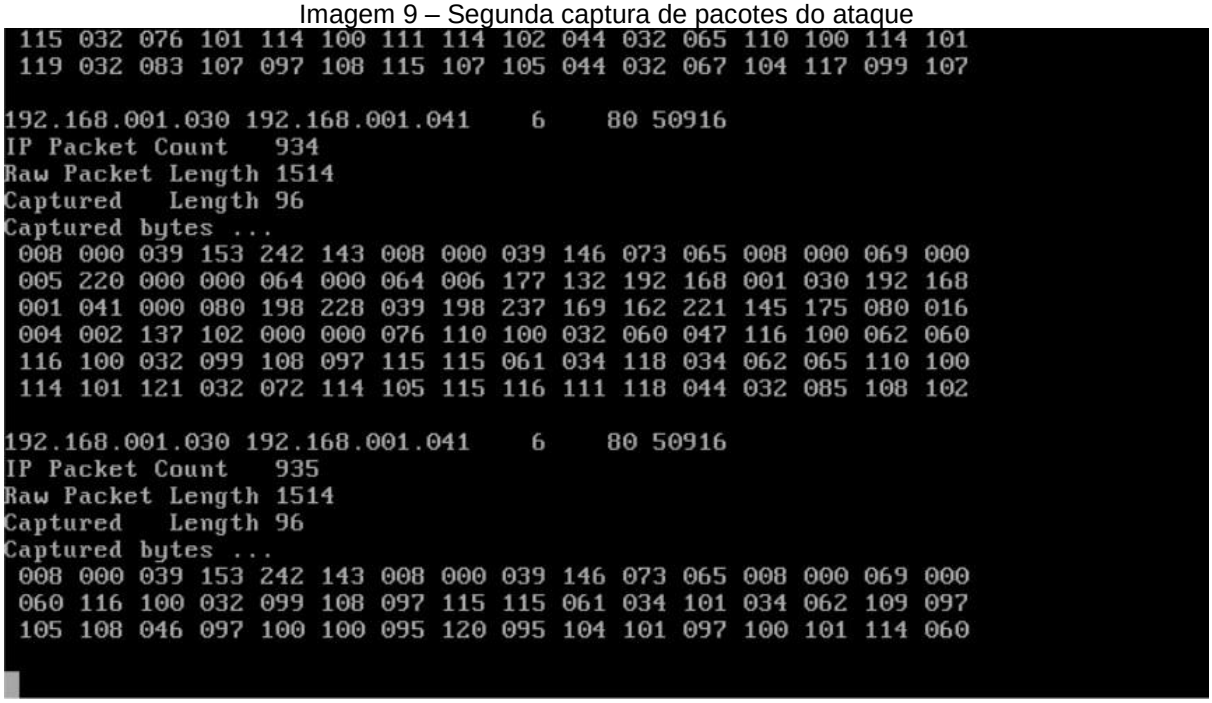
Imagem 8 - Primeira captura de pacotes do ataque



Fonte: Autoria própria (2018) com base no Sistema operacional FreeBSD

Como podemos analisar na Imagem 8, o início de qualquer ataque é parecido com um acesso legítimo; ele começa com a contagem de pacotes em 1 e o tamanho do pacote é semelhante ao acesso normal. Porém, nas próximas imagens, verificaremos como se revela o comportamento de um ataque.

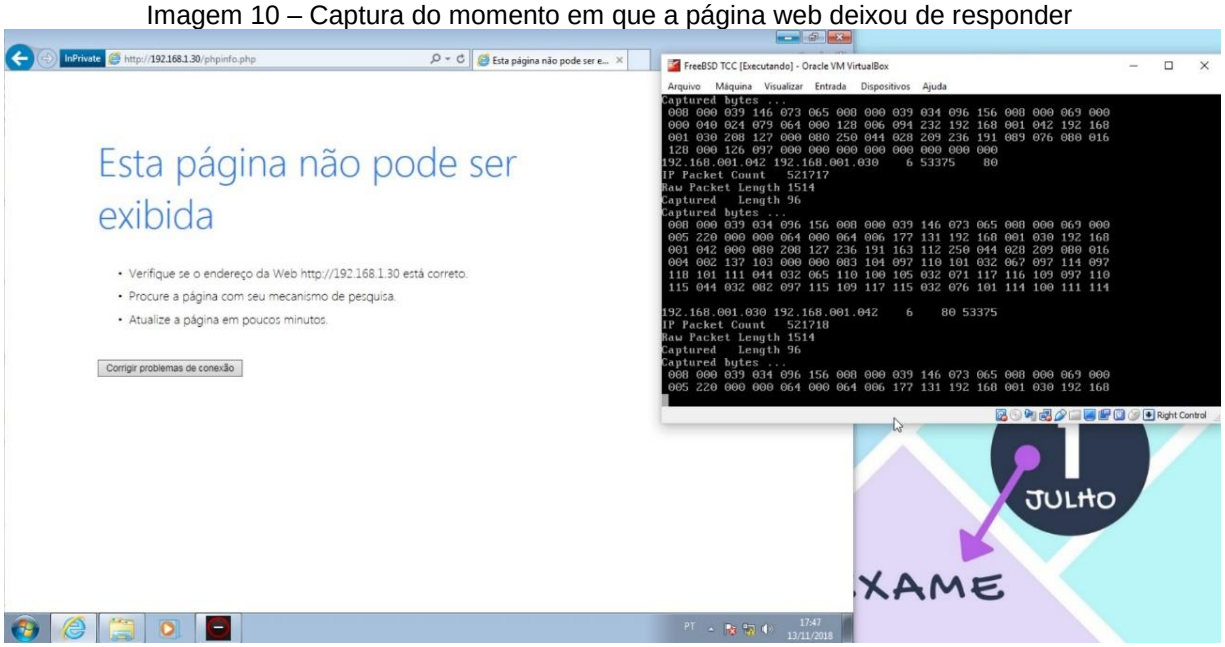
Imagem 9 – Segunda captura de pacotes do ataque



Fonte: Autoria própria (2018) com base no Sistema operacional FreeBSD

Na Imagem 9, notamos que após 1s (um segundo) de captura, o contador de pacotes (IP Packet Count) disparou e está indicando 935 pacotes; isso quer dizer que, no mínimo, vários usuários estão acessando a página ao mesmo tempo.

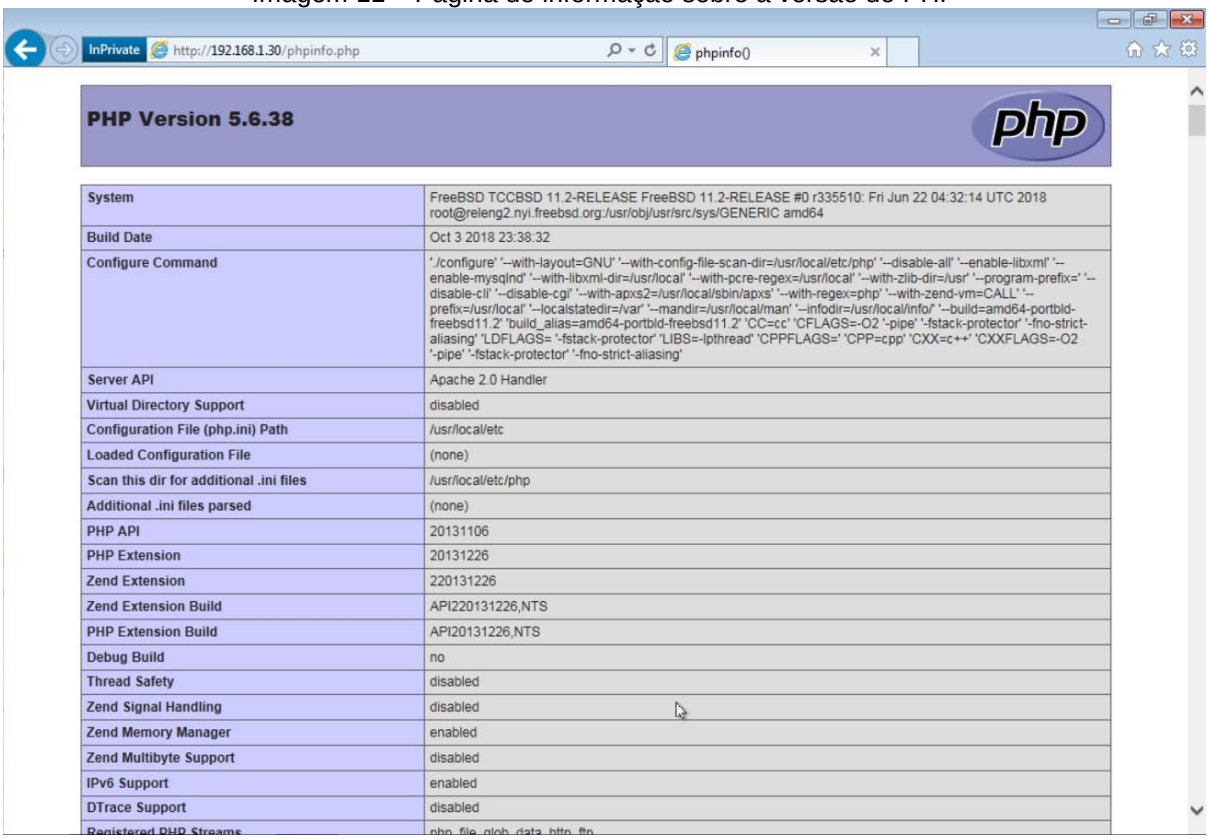
Imagem 10 – Captura do momento em que a página web deixou de responder



Fonte: Autoria própria (2018) com base no Sistema operacional FreeBSD recebendo o ataque do HOIC

Na Imagem 10, podemos avaliar o momento em que o servidor cedeu, ou seja, deixou de responder às solicitações dos clientes. O servidor deixou de responder com menos de dois minutos, ao passo que a contagem de pacotes estava na casa de 521.718 pacotes. Antes desse registro, as máquinas estavam revezando; das dez máquinas usadas no teste, apenas duas acessavam a página web, enquanto as demais não conseguiam realizar o acesso. Após os pacotes chegarem ao patamar de 521.718 pacotes, nenhuma máquina acessou mais a aplicação.

Imagem 11 – Página de informação sobre a versão do PHP



System	FreeBSD TCCBSD 11.2-RELEASE FreeBSD 11.2-RELEASE #0 r335510: Fri Jun 22 04:32:14 UTC 2018 root@releng2.nyi.freebsd.org:/usr/obj/usr/src/sys/GENERIC amd64
Build Date	Oct 3 2018 23:38:32
Configure Command	'./configure' '--with-layout=GNU' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--enable-mysqlnd' '--with-libxml-dir=/usr/local' '--with-pcre-regex=/usr/local' '--with-zlib-dir=/usr' '--program-prefix=' '--disable-cli' '--disable-cgi' '--with-apxs2=/usr/local/sbin/apxs' '--with-regex=php' '--with-zend-vm=CALL' '--prefix=/usr/local' '--localstatedir=/var' '--mandir=/usr/local/man' '--infodir=/usr/local/info/' '--build=amd64-portbld-freebsd11.2' 'build_alias=amd64-portbld-freebsd11.2' 'CC=cc' 'CFLAGS=-O2 -pipe' '-fstack-protector' '-fno-strict-aliasing' 'LDFLAGS= '-fstack-protector' 'LIBS=-lpthread' 'CPPFLAGS=' 'CPP=cpp' 'CXX=c++' 'CXXFLAGS=-O2 -pipe' '-fstack-protector' '-fno-strict-aliasing'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp

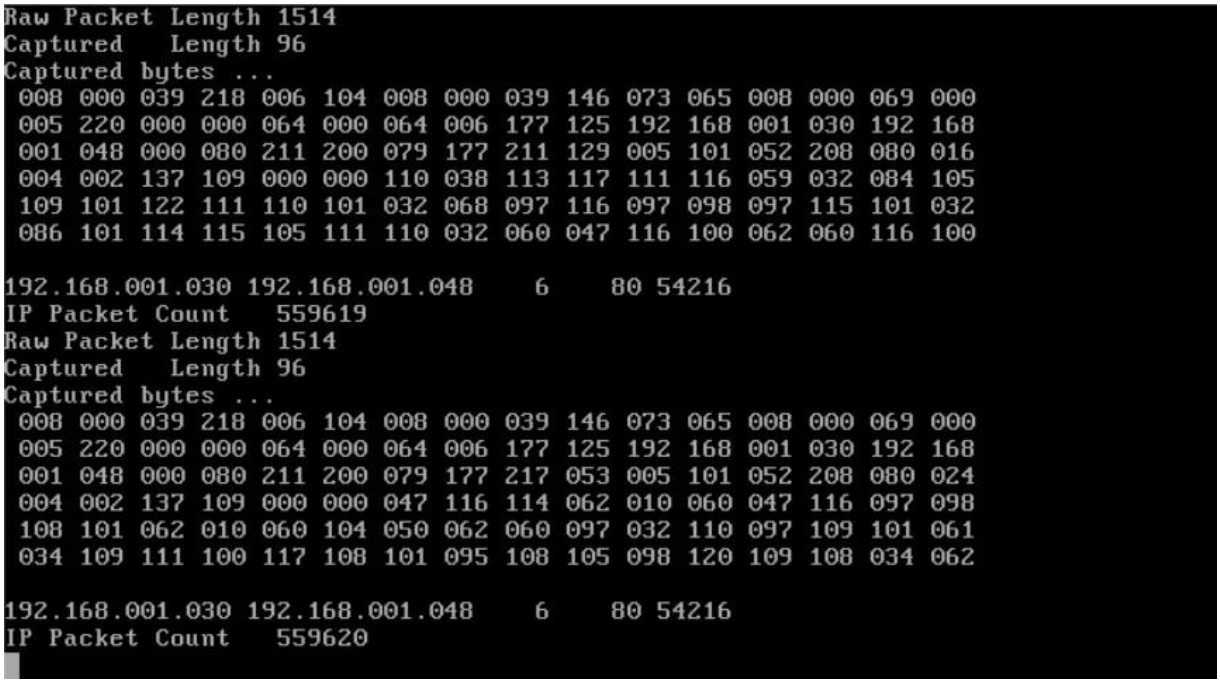
Fonte: Autoria própria (2018) com base no Microsoft Internet Explorer

Na Imagem 11 é revelada a página que utilizamos para realizar os testes, a qual contém informações sobre a versão do sistema operacional do servidor web, a versão do Apache e a versão do PHP utilizados no trabalho.

É uma página relativamente pequena, pois o código utilizado para exibi-la contém apenas 4 linhas de código. Assim, por ser pequena, e, ao mesmo tempo, tão rápida para ser carregada, precisaria de um grande ataque para tirá-la do ar. Em um

ambiente real, por exemplo, seria necessário menos máquinas para derrubar um *website.*

Imagem 12 – Terceira captura de pacotes do ataque



Fonte: Autoria própria (2018) com base no Sistema operacional FreeBSD

Após os testes realizados, interrompemos a captura de pacotes no servidor. Ele explicitou que, conforme a Imagem 12, em uma das máquinas, a captura parou em 559.620 pacotes, ou seja, foram quase seiscentos mil pacotes capturados em pouco mais de três minutos de teste. Considerando-se que isto foi possível diagnosticar em uma única máquina, imaginemos, então, se esse valor de pacotes enviados pudesse ser facilmente multiplicado por dez, visto que são 10 máquinas objeto destes testes?

3.3 – PREVENÇÕES

Uma forma para que possamos prevenir e mitigar ataques de negação de serviço, por exemplo, é com a aquisição de um IPS (Intrusion Prevention System) e/ou um IDS (Intrusion Detection System).

Um IPS é utilizado para prevenir um ataque de intrusão, ou seja, é um equipamento que uma vez na sua rede, vai monitorar o tráfego de rede e derrubar pacotes maliciosos. Uma vez detectados, este dispositivo é muito útil para evitar ataques de

negação de serviço, haja vista que ele detecta uma intrusão. Ele é configurado pelo seu administrador de redes com algumas regras de entrada de pacotes, essas regras, são enxergadas pelo IPS através de m*achine learning,* uma vez detectada a intrusão, através das regras passadas pelo administrador, o IPS toma as suas devidas atitudes. O IDS, por sua vez, detecta uma intrusão, mas não tem a finalidade de derrubar os pacotes considerados perigosos.

Ainda assim, como em um IPS, o administrador de rede realiza a entrada de algumas regras no equipamento, caso ocorra alguma tentativa de invasão ou caso seja detectado um trafego anormal de rede, avisa o seu administrador, porém não toma nenhuma atitude quanto ao tráfego que estaria passando pela rede naquele momento. Dessa forma, por exemplo, é utilizado mais para um administrador de rede que deseja ser notificado de uma possível invasão do sistema, no entanto, apenas este administrador da rede terá que realizar as manutenções necessárias dentro do seu *firewall, proxy* ou ferramenta que utiliza para gerenciar sua rede, para corrigir a falha, visto que o IDS não executa nenhuma ação frente à um ataque de intrusão, apenas notifica.

Temos ainda ferramentas mais recentes como o *Snort – Network Intrusion Detection & Prevention System* que é um sistema completo que já inclui o IDS e o IPS dentro dele. Programas como esse, utilizam da mesma tecnologia que qualquer IPS/IDS, como o *machine learning,* para verificar o tráfego na rede, por ser mais completo, além de notificar o seu administrador para possíveis ajustes extras, ele por si só toma atitudes para cancelar um possível ataque de negação de serviço.

Podemos assegurar, ainda, que um IDS/IPS pode ser colocado em lugares diferentes de uma rede com a finalidade de realizar funções diferentes. Segundo o Blog “Caminhando Livre” (2009), se um IDS/IPS for colocado no meio de uma rede, ele poderá ser utilizado para prevenir ataques a quaisquer servidores. No entanto, se ele for inserido em um servidor, ele poderá monitorar e resolver o tráfego específico daquele servidor, o qual, por exemplo, pode ser um *firewall*. Em outras palavras, o IDS/IPS analisa o tráfego que chega nesse *firewall* que, por sua vez, possui as regras de liberação e bloqueio de acesso à internet. (CAMINHANDO LIVRE, 2009)

CONSIDERAÇÕES FINAIS

Por meio deste trabalho nós tivemos a pretensão de informar o quão perigoso e comum é o ataque de negação de serviço, para isso, apresentamos algumas ferramentas e meios instrumentalizados para a realização deste tipo de ataque. Nós nos preocupamos em demostrar um tráfego normal de pacotes, a fim de revelar e comprovar uma circulação legítima dos dados na rede, e depois explicitamos um tráfego afetado, no intuito de diferenciar um acesso legítimo de um ataque de negação de serviço, a qual pôde ser comprovada com a indicação de uma página que teve falha no carregamento após o ataque sofrido.

Abordamos também as consequências da utilização da internet por empresas e pela família e concluímos que há a necessidade de uma alfabetização relacionada à tecnologia e à internet, tendo em vista os riscos que usuários, físicos e jurídicos, estão suscetíveis.

Esse Trabalho citou o uso da Engenharia Social e como as pessoas podem ser manipuladas e coagidas, tanto nos ambientes corporativos como na vida pessoal. Constatamos ainda que as políticas de segurança bem elaboradas e implantadas são muito eficientes na diminuição das falhas de segurança de uma empresa.

Ademais, vislumbramos que os dispositivos presentes na era da internet das coisas estão conectados à internet, como smart TV's, geladeiras inteligentes, entre outros, consequentemente, enviam pacotes com requisições a servidores, por esse motivo, podem ser utilizados em uma *botnet*, que enviam requisições para atacar um servidor alvo, o que, por conseguinte, podem se tornar propensos alvos de ataques de negação de serviços.

Conforme o *site* "TechRepublic", na Q3, "State of the Internet Security Reports", que são relatórios sobre ataques na internet, afirmam que o uso de ataques de negação de serviço em 2017 aumentou 91% em relação a 2016, graças ao uso desses dispositivos de Internet das Coisas (IoT), que não possuem uma segurança bem configurada. Muitos ataques foram registrados a partir de vulnerabilidades encontradas e exploradas em *webcams*, câmeras de segurança e gravadores de vídeo digitais. Ainda, segundo este *site*, uma vez que um dispositivo é infectado, ele dispara o *malware* entre outros dispositivos com a mesma falha, fazendo com que os

dispositivos infectados e prontos para serem utilizados pelo atacante, aumentem exponencialmente. No entanto, esta não foi a preocupação original deste Trabalho de Graduação, mas pode, certamente, ser explorado em futuras pesquisas monográficas dos estudantes do curso de Segurança da Informação, no intuito de captarem estas vulnerabilidades e oferecerem ferramentas tecnológicas para evitá-las.

Ademais, não podemos deixar de enfatizar a importância da segurança e da atualização de *firmwares* ou *patches* de segurança para que ataques, como este analisado neste Trabalho, não mais ocorram, ou ao menos, diminuam a incidência, preocupações acadêmicas que podem ser percorridas por outros estudantes desta área.

REFERÊNCIAS

AFFILIATES, Cisco And/or Its. **Snort.** 2018. Disponível em: <https://www.snort.org/>. Acesso em: 15 dez. 2018.

ALERTA SECURITY. **Política de segurança da informação:** entenda a sua importância. 2017. Disponível em: <https://alertasecurity.com.br/blog/278-politica-de-seguranca-da-informacao-entenda-a-sua-importancia-2>. Acesso em: 27 set. 2018.

ARAÚJO, Adrecion. **Danos Morais na Internet:** Direito em Geral. 2010. Disponível em: <https://adrecion.wordpress.com/2010/05/08/danos-morais-na-internet/>. Acesso em: 25 set. 2018.

BBC MUNDO. **O que é a 'Momo do WhatsApp' e quais são os riscos que ela representa?** 2018. Disponível em: <https://www.bbc.com/portuguese/salasocial-44961410>. Acesso em: 07 nov. 2018.

BRASIL. Presidência da República. **Lei n.º 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>.Acesso em: 10 nov. 2018, às 15h18min.

BRASIL. Governo Federal. **Cartilha da segurança:** Simples atitudes podem evitar grandes problemas.Simples atitudes podem evitar grandes problemas, 2014. Disponível em: <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/campanha-de-sensibilizacao-em-sic-2014/cartilha-de-seguranca-da-informacao.pdf>. Acesso em: 25 set. 2018.

CARVALHO, Lucas. **Maior ataque *DDoS* da história atinge o site GitHub.** 2018. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/maior-ataque-*DDoS*-da-historia-atinge-o-site-github/74379>. Acesso em: 26 out. 2018.

CEROY, Frederico Meinberg. **Família + segura na Internet:** Ética e Segurança Digital Cartilha Orientativa. Brasília: Comissão do Direito Digital, 2015. 36 p.

CERT.BR (NOME POR EXTENSO). **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (*DDoS*).** 2016. Disponível em: <https://www.cert.br/docs/whitepapers/*DDoS*/>. Acesso em: 26 set. 2018.

_____. **Incidentes Reportados ao CERT.br:** Janeiro a Dezembro de 2017. 2017. Disponível em: <https://www.cert.br/stats/incidentes/2017-jan-dec/fraude.html>. Acesso em: 25 set. 2018.

CHAUMIER, Jacques. **Systèmes d'information:** marchés et technologies. Paris: Entreprise Moderne D'edition, 1986. 117 p.

COMITÊ GESTOR DA INTERNET. **Tipos de Spam.** Disponível em: <http://www.antispam.br/tipos/fraudes/>. Acesso em: 25 set. 2018.

ESET, Comunidade de Segurança da. **3 tipos de funcionários que podem causar uma brecha de segurança.** 2017. Disponível em: <https://www.welivesecurity.com/br/2017/05/29/funcionarios-brecha-seguranca/>. Acesso em: 18 out. 2018.

FEITOSA, Marcio Porto. **Fundamentos de banco de dados:** uma abordagem prático-didática. São Paulo: Edição do Autor, 2013. 314 p.

FIALHO JUNIOR, Mozart. **Guia Essencial do Backup.** São Paulo: Digerati Books, 2007. 127 p.

IT, Equipe Eco et al. **Top 5 problemas da perda de dados nas empresas.** 2018. Disponível em: <https://ecoit.com.br/perda-de-dados-nas-empresas/>. Acesso em: 18 set. 2018.

MOREIRA, Esdras. **Conheça os pilares da Segurança da Informação:** Quais os pilares da segurança da informação. 2017. Disponível em: <http://introduceti.com.br/blog/pilares-da-seguranca-da-informacao/>. Acesso em: 18 set. 2018.

NEVES, Josan. **IDS/IPS, o que é isso afinal?** 2009. Disponível em: <https://caminhandolivre.wordpress.com/2009/01/05/idsips-o-que-e-isso-afinal/>. Acesso em: 20 nov. 2018.

NUNES, Amanda; CARVALHO, Niere; BRANDÃO, Rafael. **Abordagens sobre crimes na Internet:** Mas afinal o que é cibercrime?. 2011. Disponível em: <https://cibercrimes.wordpress.com/2011/03/24/mas-afinal-o-que-e-cibercrime/>. Acesso em: 11 nov. 2018.

PORTAL EDUCAÇÃO. **Engenharia Social.** 2013. Disponível em: <https://www.portaleducacao.com.br/conteudo/artigos/informatica/engenharia-social/28441>. Acesso em: 27 set. 2018.

QUEIROZ, André. **A atual lacuna legislativa frente aos crimes virtuais.** *Revista jurídica Unifox.* Foz do Iguaçu, v.3, n.1, p. 169-178, jul./dez. 2008.

RAYOME, Alison Denisco. **DDoS attacks increased 91% in 2017 thanks to IoT.** 2017. Disponível em: <https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/>. Acesso em: 20 nov. 2018.

ROHR, Altieres. **Crimes em *DDoS* e antivírus para atualizações do Windows:** Pacotão. 2018. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/crimes-em-*DDoS*-e-antivirus-para-atualizacoes-do-windows-pacotao.html>. Acesso em: 26 out. 2018.

ROSSINI, Augusto Eduardo de Souza. ***Informática, telemática e Direito penal.*** São Paulo: Memória Jurídica, 351p, 2004.

ROSSOW, Christian. **Amplification Hell:** Revisiting Network Protocols for *DDoS* Abuse. 2014. Disponível em: <https://christian-rossow.de/publications/amplification-ndss2014.pdf>. Acesso em: 18 out. 2018.set. 2018.

SHARMA, Kalpana. **The reality behind the theory of killer game 'Blue Whale'.** 2017. Disponível em: <https://timesofindia.indiatimes.com/life-style/health-fitness/de-stress/the-reality-behind-the-theory-of-killer-game-blue-whale/articleshow/59881467.cms>. Acesso em: 26 set. 2018.

SOCIETY, Internet. **Global Internet Report.** 2016. Disponível em: <https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf>. Acesso em: 21 set. 2018.

TAURION, Cezar. **Tecnologia:** Você já parou para pensar no valor dos dados?. 2014. Disponível em: <https://imasters.com.br/tecnologia/voce-ja-parou-para-pensar-no-valor-dos-dados>. Acesso em: 18 set. 2018.