MARINHA DO BRASIL

DIRETORIA DE ENSINO DA MARINHA

CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

INTERNET OF THINGS (IoT):
Estudo de vulnerabilidades e boas práticas para segurança da informação

PRIMEIRO-TENENTE WILLIAN ALVARES DOS SANTOS

Rio de Janeiro
2020

PRIMEIRO-TENENTE WILLIAN ALVARES DOS SANTOS

INTERNET OF THINGS (IoT):
Estudo de vulnerabilidades e boas práticas para segurança da informação

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Orientadores:
Capitão de Corveta (T) Dulcineia Santos Sennejunker
Professor PhD. Anderson Oliveira da Silva

CIAW
Rio de Janeiro
2020

Santos, Willian Alvares dos

Internet of Things (IoT): estudo de vulnerabilidades e boas práticas para a segurança da informação / Willian Alvares dos Santos. -- Rio de Janeiro, 2020.

54 f.

Orientador técnico: CC(T) Dulcineia Santos Sennejunker e orientador acadêmico: Prof. PhD. Anderson Oliveira da Silva.

Trabalho de Conclusão de Curso (Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações). -- Centro de Instrução Almirante Wandenkolk, Centro de Coordenação de Pós-Graduação, 2020.

1. Internet of Things. 2. Segurança da informação. 3. Mirai. 4. Botnet. 5. Negação de Serviço. I. Sennejunker, Dulcineia Santos; e Silva, Anderson Oliveira da. II. Título.

PRIMEIRO-TENENTE WILLIAN ALVARES DOS SANTOS

INTERNET OF THINGS (IoT):

Estudo de vulnerabilidades e boas práticas para segurança da informação

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da informação e comunicações.

Aprovada em de de 2020.

Banca Examinadora:

Capitão de Mar e Guerra (RM1-EN) Gian Karlo Huback Macedo de Almeida, CIAW

Capitão de Corveta (T) Dulcineia Santos Sennejunker, CTIM

Professor PhD. Anderson Oliveira da Silva, PUC-RIO

CIAW

Rio de Janeiro

2020

Dedico esse trabalho à minha querida avó Ione (*in memorian)* que sempre foi uma grande incentivadora na minha vida.
Agora, dada por finda sua derrota e ao soar do toque do silêncio, em companhia dos anjos, a senhora pode finalmente descansar. E estará sempre comigo.

AGRADECIMENTOS

Agradeço primeiramente à minha família, meus pais Wilson e Claudia e minha irmã Jaqueline, pois sem o seu suporte, certamente eu não seria a pessoa que sou hoje. À minha querida noiva, Renata, agradeço pelo companheirismo, amizade e amor por, mesmo longe, me ajudar a ter forças para caminhar nessa longa e difícil singradura. Vocês são a base da minha vida.

Ao CMG (RM1-EN) Gian Karlo Huback Macedo de Almeida, coordenador do CApA-SIC, agradeço pelo trabalho diuturno em prol da busca pela excelência do curso e pela constante preocupação com o bem-estar dos alunos.

Ao CF (RM1-T) Wagner Santans de Freitas, do Centro de Eletrônica, instrutor de diversas disciplinas na área de TI, agradeço por me apresentar ao vasto universo de uma área tão importante e despertar em mim o desejo de me aperfeiçoar nela.

Aos meus orientadores: CC (T) Dulcineia Santos Sennejunker (orientadora técnica), agradeço a constante disponibilidade e vontade de ajudar, mesmo frente a sua grande demanda e responsabilidade como encarregada do Centro Local de Tecnologia da Informação do Edifício Barão de Ladário (CLTI-EdBL); Professor Dr. Anderson Oliveira da Silva (orientador acadêmico), agradeço pelos ensinamentos, não apenas na elaboração deste trabalho, mas também pelos valiosos conselhos sobre a área de Segurança da Informação.

Ao Professor Dr. Sérgio Colcher, agradeço pelo seu amor à profissão e pela maneira como transmitiu os conhecimentos durante as aulas, sendo de fundamental importância para aumentar meu interesse pela área de TI.

Por fim, mas não menos importante, agradeço aos meus amigos de turma: Cristo, Gouvêa, Walmor e Ramalho. Muito obrigado por estarem sempre ao meu lado nos momentos mais difíceis desse curso, fosse academicamente ou na vida pessoal. Contem sempre comigo. *O Mar nos une!*

"A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original."

(Albert Einstein)

INTERNET OF THINGS (IoT):
Estudo de vulnerabilidades e boas práticas para segurança da informação

RESUMO

O ser humano, atualmente, vive em uma sociedade extremamente dependente da tecnologia. Esta evolui cada vez mais rápido, exemplo disso está na crescente quantidade de dispositivos conectados à internet. Porém, a popularização da Internet das Coisas (IoT) fez que a demanda por endereçamento de IP crescesse e surgisse a necessidade da evolução do IPv4 para o IPv6, a fim de que o problema de endereçamentos fosse resolvido. No entanto, o crescimento acelerado e sem controle da IoT, que foi projetada para melhorar a qualidade de vida das pessoas, vem acompanhado de problemas sérios tais como: baixa segurança da informação processada, falta de uma padronização que garanta interoperabilidade entre os equipamentos e um fator mínimo de qualidade e segurança a ser oferecido. A partir destes problemas, surgem *malwares*, como o Mirai, que exploram as vulnerabilidades destes equipamentos, utilizando-os como parte de uma armada de zumbis (*bots*) para amplificar Ataques Cibernéticos. Neste trabalho, através de um estudo de caso do Mirai, é feito um levantamento de boas práticas para a estruturação de uma rede de IoT com um mínimo de segurança aceitável. Além disso, através do plano de ação para IoT elaborado pelo BNDES, faz-se um paralelo com sua aplicabilidade dentro da Marinha do Brasil.

Palavras-chave: Internet das Coisas. Negação de Serviço. Mirai. Botnet. Segurança da Informação.

SUMÁRIO

1 INTRODUÇÃO

A sociedade é como um organismo vivo, está sempre em evolução e, por natureza, o ser humano é comunicativo, buscando cada vez mais formas de diminuir as distâncias para comunicação. Da mesma maneira, a tecnologia evolui ferozmente para atender à uma sociedade sedenta por evoluções tecnológicas que facilitem, não apenas, as comunicações, mas também as atividades cotidianas.

Nesse universo de evolução, a tecnologia deu um grande salto em poucas décadas, do ENIAC ao smartphone, da ARPANET à Internet. Agora chegamos a um novo universo: a Internet das Coisas (IoT).

Segundo Santos (2018), a internet nos deu a oportunidade de nos conectar de maneiras que jamais poderíamos imaginar que fossem possíveis. A IoT nos levará além da conexão para nos tornarmos parte de um sistema nervoso global vivo e em movimento, que abre uma infinidade de novas oportunidades (otimizar operações, aumentar a produtividade e economizar recursos e custos).

No entanto, segundo Migrani (2018), essa interconectividade pode acarretar uma vasta gama de problemas e questões discutíveis, entre as quais as fragilidades em relação à privacidade e segurança dos usuários. No tocante à segurança, ainda não há um consenso e muito menos uma noção completa do que realmente é necessário por parte dos fabricantes e desenvolvedores dos produtos de IoT.

1.1. O Problema

O grande crescimento da internet proporcionou uma maior integração dos sistemas em todo o mundo. É uma nova era da tecnologia. Porém, com essa integração surge uma nova questão, o limite entre conectividade e segurança da informação. É a Era Digital.

O avanço nas tecnologias gerado pela quarta revolução industrial proporcionou um novo tipo de ambiente, o ciberespaço.

Assim como os ambientes terrestre, aeronáutico e marítimo são importantes para a defesa da soberania nacional, o ciberespaço também merece atenção, principalmente pelo fato de hoje todos nós vivermos em um mundo extremamente conectado e dependente da

internet, o ciberespaço é um ambiente que permeia os ambientes mais tradicionais no mundo militar.

"A SIC (Segurança da Informação e Comunicações) e a SegCiber (Segurança Cibernética) têm, portanto, impactos amplos na soberania nacional, na construção da cidadania e no desenvolvimento econômico" (BRASIL, 2015).

E devido a essas peculiaridades, segundo Clarke e Knake (2015) foi criado em 1º de outubro de 2009 o Comando Cibernético dos Estados Unidos, uma organização militar com a missão de utilizar a Tecnologia da Informação (TI) como arma.

A Guerra Cibernética não é um novo tipo de guerra, limpa e sem vítimas, que devemos adotar. Nem mesmo um tipo de arma secreta que deva ser mantida escondida da luz do dia e do público em geral. Pois é o público, a população civil e as organizações do público em geral que operam sistemas nacionais críticos que provavelmente sofrerão em uma guerra cibernética (CLARKE; KNAKE, 2015).

Segundo Clarke e Knake (2015), podemos citar como exemplo do uso deste tipo de arma (anexo I):

- O bombardeio da Força Aérea Israelense à Síria (2007);
- A campanha americana na segunda invasão ao Iraque (2003); e
- O conflito envolvendo a Rússia e a Geórgia (2008)

Com esses exemplos, fica bem claro que os maiores afetados com os ataques cibernéticos são a população civil e as organizações públicas.

O cenário de uso da Internet e, consequentemente, de uso das Tecnologias de Informação e Comunicação (TIC) permanece crescente e sem dúvida além de qualquer expectativa e prospecção, operando-se em cifras bastante expressivas no mundo e no País, especialmente frente aos avanços do uso de dispositivos móveis, da computação em nuvem e da evolução da chamada *internet das coisas* (BRASIL, 2015)

> A Internet das Coisas traz o conceito de interligar dispositivos computacionais utilizados no dia a dia a internet, aproximando cada vez mais o mundo físico com o digital. E por 'coisas', entende-se como objetos comuns presentes no cotidiano, tais como cafeteiras, relógios, câmeras de vigilância, despertadores, entre outros, que são conectados à rede possibilitando a troca de informações de um lugar para outro a qualquer momento (PRADO, 2018).

Essa nova realidade da internet conduzida pela IoT, diminuirá a segurança da internet como um todo. Cada um dos dispositivos IoT pode ser, potencialmente, um ponto

de vulnerabilidade onde um código mal-intencionado pode ser inserido, afetando a segurança dos sistemas (FIGUEIRA, 2016).

A rápida adoção da IoT veio, infelizmente, à custa dos padrões de segurança. No primeiro semestre de 2017, o número de ataques de IoT aumentou em impressionantes 280%. É claro que é necessária uma ação rápida para abordar os buracos na segurança IoT que podem devastar organizações e consumidores (SANTOS, 2018)

Nesse contexto, destacam-se os Ataques Distribuídos de Negação de Serviço (DDoS) que exploram as vulnerabilidades dos dispositivos IoT. A ideia de um ataque DDoS é reunir um conjunto de máquinas infectadas e utilizá-las para enviar requisições simultâneas ao mesmo alvo, sobrecarregando assim seu sistema e impedindo que usuários legítimos de um serviço usem os recursos desejados (LAU *Et al.*, 2000, *apud* PRADO, 2018).

Assim, o objetivo deste trabalho é analisar as vulnerabilidades destes dispositivos através do estudo de caso da Botnet Mirai e apresentar boas práticas para segurança de redes IoT, contribuindo para a disseminação da mentalidade de segurança da informação, porém, sem desenvolver métodos de combate ao malware citado.

1.2. Motivação

O universo de aplicabilidade para IoT é gigantesco e abrange *smart city*, saúde, *smart home*, indústria, agronomia. Com isso, a motivação para esse trabalho é trazer conhecimentos de uma tecnologia que pode vir a se tornar uma importante ferramenta para melhorar o gerenciamento de recursos e segurança orgânica das organizações militares na Marinha do Brasil.

Segundo Migrani (2018), já existem governos estaduais implementando iniciativas para o uso de IoT, ressaltando:

- São Bernardo do Campo (SP), que inaugurou o Centro Integrado de Monitoramento (CIM), um sistema com 400 câmeras instaladas em áreas estratégicas, que transmitem imagens em tempo real durante 24 horas por dia;
- Recife (PE), está desenvolvendo um dispositivo que tem capacidade de captar sons, ajudando na comunicação de arrombamentos, disparos de armas e até quedas de pacientes em hospitais;

- Vitória (ES), o *botão do pânico* foi desenvolvido como forma de proteger vítimas de violência doméstica; e
- O governo do Paraná decidiu investir em três áreas (água, luz e gás), criando redes inteligentes de energia elétrica, que vão reduzir o número e o tempo de desligamentos na rede elétrica, medir consumo de energia, água e gás a distância e descentralizar a geração de energia.

Para os militares, como em qualquer área, setor ou indústria, não existe uma solução única para a IoT. Podendo ser empregada com diversos propósitos, seja na redução de custos e melhor gerência de recursos ou para um melhor sistema de vigilância.

1.3. Metodologia

A elaboração deste trabalho pode ser dividida em duas fases: na primeira empregou-se a pesquisa bibliográfica do material necessário; e na segunda, realizou-se estudo de caso da *Botnet* Mirai que ganhou grande atenção dos profissionais da área de segurança da informação a partir do segundo semestre de 2016 ao ser empregada para ataques de negação de serviço a servidores.

Segundo Lakatos e Marconi (2009), a pesquisa bibliográfica tem como finalidade colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto.

Já o uso do estudo de caso, segundo Gil (2002), consiste no estudo profundo e exaustivo de um ou poucos objetos, de maneira que permita seu amplo e detalhado conhecimento.

2 REFERENCIAL TEÓRICO

2.1. Segurança da Informação e Comunicações

Segurança da Informação e Comunicações (SIC) é definida como conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, integridade e confidencialidade de dados e informações de forma a minimizar os incidentes de segurança da informação. Dessa forma, podemos elencar como pilares da SIC: disponibilidade, integridade, confidencialidade e autenticidade, definidos a seguir, (BRASIL, 2019; BRASIL, 2015; BRASIL, 2007):

a) Disponibilidade - capacidade da informação digital estar disponível para alguém autorizado a acessá-la no momento próprio.
b) Integridade - capacidade da informação digital somente ser modificada por alguém autorizado;
c) Confidencialidade - capacidade da informação digital somente ser acessada por alguém autorizado; e
d) Autenticidade - capacidade da origem da informação digital ser aquela identificada.

"Uma política de segurança estabelece o que precisa ser feito para a proteção das informações armazenadas nos computadores. Uma política bem escrita contém a definição suficiente do 'que' fazer de modo que o 'como' possa ser identificado e medido ou avaliado." (NORTHCUTT, 2002).

Segundo Hintzbergen *Et al.* (2015):

> A segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, onde necessário, para assegurar que os objetivos específicos de segurança e do negócio da organização sejam atendidos. Isso deve ser feito em conjunto com outros processos de gerenciamento de negócio. (HINTZBERGEN *Et al.*, 2015)

De acordo com Hintzbergen *Et al.* (2015):

> A abordagem de processo para a gestão da segurança da informação apresentada na ISO 27002:2013, "Código de prática para a segurança da informação" (*Code of practice for Information security*)", inclui a importância de:
>
> A. Compreender os requisitos de segurança da informação da organização e a necessidade de estabelecer políticas e objetivos para a segurança da informação.
>
> B. Implementar e operar controles para gerenciar os riscos de segurança da informação da organização no contexto dos riscos gerais de negócio da organização.
>
> C. Monitorar e revisar o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação (*Information Security Management System* - ISMS).
>
> D. Melhoria contínua baseada em medições objetivas. (HINTZBERGEN *Et al.*, 2015)

2.2. IoT

A grande variedade dos tipos de dispositivos e as diversas formas de comunicação, na qual a escolha vai depender de fatores como o alcance, requisitos de dados, exigências de segurança, potência de vida da bateria (anexo II), associados a um crescimento acelerado e sem a devida padronização, dão à IoT um alto grau de complexidade.

"A padronização é fundamental para a integração de diferentes dispositivos, sendo necessário que todos os dispositivos 'falem uma mesma língua', definida em um protocolo de comunicação da Internet das Coisas." (PÖTTER, 2015).

Ao analisar as definições sobre IoT, é possível verificar que ainda não existe um consenso entre os autores, como pode ser verificado no quadro 2.1 extraída do artigo de Mancini (2018).

Quadro 2.1 - Algumas definições para IoT

AUTOR	DEFINIÇÃO
Atzori *Et al* (2011, p. 2787)	A ideia básica desse conceito é a presença generalizada à nossa volta de uma variedade de coisas ou objetos – como *tags* de identificação por radiofrequência (RFID), sensores, atuadores, telefones celulares, etc. – que, por meio de esquemas de endereçamento exclusivos, são capazes para interagir uns com os outros e cooperar com outros objetos para alcançar objetivos comuns.
CERP IoT (2009)	Uma infraestrutura de rede dinâmica e global com capacidades de autoconfiguração baseadas em protocolos de comunicação padronizados e interoperáveis nos quais as 'coisas' físicas e virtuais têm identidades, atributos físicos, personalidades virtuais, usam interfaces inteligentes e são completamente integradas na rede de informação. Na IoT é esperado que as 'coisas' se tornem participantes ativas dos negócios e dos processos informacionais e sociais nos quais eles são capazes de interagir e comunicar-se entre eles e com o ambiente através da troca de dados e informação percebida sobre o ambiente, enquanto reagem de forma autônoma aos eventos do 'mundo físico/real' e o influenciam ao iniciar processos que engatilham ações e criam serviços com ou sem intervenção humana direta. (CERP IoT, 2009, p. 6, tradução nossa)
ITU-T Study Group 13	Uma infraestrutura global para a sociedade da informação, permitindo serviços avançados por meio da interligação das coisas (físicas e virtuais) baseada na interoperabilidade das tecnologias de informação e comunicação existentes e em evolução. NOTA 1 – Por meio da exploração das capacidades de identificação, captura de dados, processamento e comunicação, a IoT faz pleno uso das coisas para oferecer serviços a todos os tipos de aplicações, garantindo o cumprimento dos requisitos de segurança e privacidade. NOTA 2 – A partir de uma perspectiva mais ampla, a IoT pode ser compreendida como uma visão com implicações tecnológicas e sociais.
IEEE (2014)	Uma rede de itens – cada um incorporado com sensores – que estão conectados à internet.

Fonte: Mancini (2018, adaptado)

"A Internet das Coisas permite que pessoas e coisas estejam conectadas a qualquer hora, em qualquer lugar, com qualquer coisa, com qualquer outra pessoa e idealmente usando qualquer caminho/rede e qualquer serviço." (GUILLEMIN e FRIESS, 2009, *apud* PÖTTER, 2015).

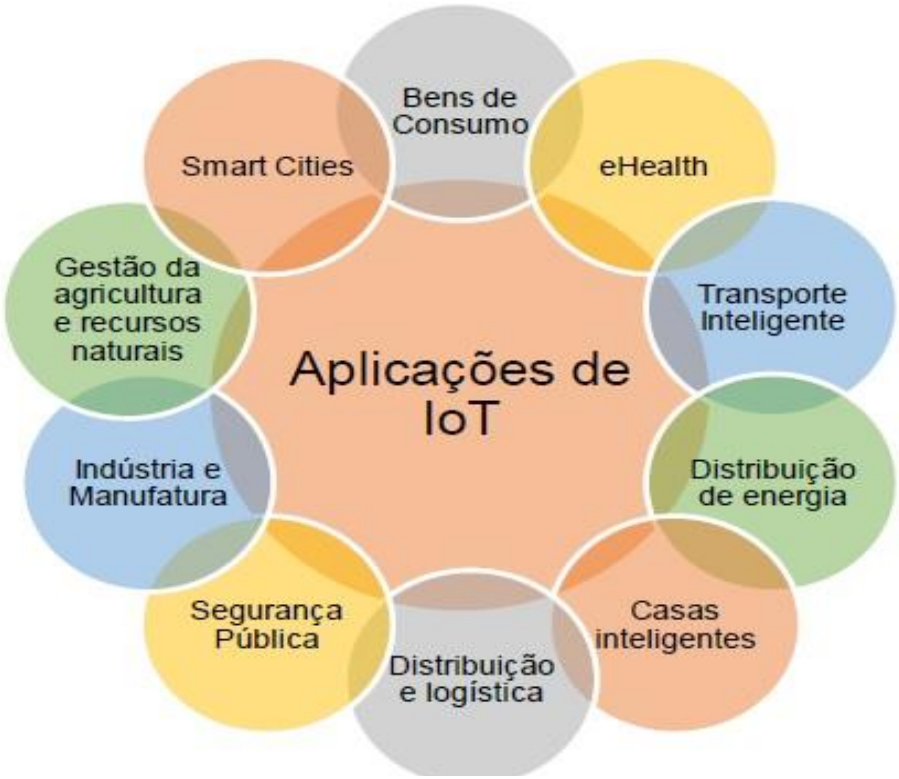
A arquitetura de infraestrutura para Internet das Coisas proposta é basicamente dividida em cinco camadas (TAN e WANG, 2010; WU *Et al.* 2010, *apud* JUNIOR e MORENO, 2015):

a) camada de percepção (device layer): responsável pelo levantamento dos aspectos físicos e interação com o meio, formada de objetos, sensores e atuadores;
b) camada de rede (Transmission layer): camada que transmite, de forma segura, a informação coletada no estrato anterior para os sistemas de processamento apropriados;
c) camada middleware: esta camada visa abstrair a especificidade tecnológica subjacente, provê o gerenciamento dos serviços e a ligação com a estrutura de armazenamento de dados;
d) camada de aplicação: faz o gerenciamento global dos serviços providos pela camada de middleware nas áreas de saúde inteligente (smart health), cidade inteligente (smart city); e
e) camada de negócio: responsável pela gestão de toda a infraestrutura para IoT.

Para efeitos de simplificação deste estudo, consideraremos as camadas da infraestrutura para IoT sob três perspectivas: (i) rede de sensores (camadas de percepção e rede); (ii) middleware; e (iii) computação em nuvem (camadas de aplicação e negócio).

No campo das aplicações, são vastas as possibilidades de emprego da tecnologia IoT, como pode ser observado na figura 2.1.

Figura 2.1: Aplicações de IoT



Fonte: Mancini (2018)

2.3. Botnet

Segundo Hintzbergen *Et al.* (2015), podemos definir uma botnet como:

> *Botnet* é uma combinação das palavras *robot* e *network*. O termo é normalmente utilizado com uma conotação negativa ou maliciosa. Um *botnet* é uma coleção de programas conectados a outros programas similares, via internet, a fim de realizar tarefas no computador de alguma pessoa. Esses programas podem se comunicar por meio de vários canais para realizar diferentes tarefas, tais como enviar e-mails de spam ou participar de um ataque distribuído de negação de serviço. É possível se tornar parte de um *botnet* clicando em um link em um e-mail ou em uma página *web*, ou abrindo um anexo inseguro de e-mail onde um *malware* está escondido. Muitas vezes, *malwares* podem ser baixados sem qualquer noção do usuário. Quando um computador se torna um *bot*, é mantida uma conexão com um servidor de comando e controle, de onde o operador do *botnet* pode instruir

> todos os computadores comprometidos a realizar tarefas. (HINTZBERGEN *Et al.*, 2015, p.264).

Bot é um termo genérico usado para descrever qualquer dispositivo que executa um *script* ou um conjunto de *scripts* criados para desempenhar funções pré-estabelecidas de forma automatizada. Alguns exemplos de uso dos *bots* são na utilização por máquinas de buscas para caminhar pela *web* tomando conhecimento dos conteúdos de *websites*, em jogos *online* para prover oponentes virtuais, e em Ataques de Negação de Serviço (GOMES; ARAUJO; CAMPOS, 2018, *apud* PRADO, 2018).

Segundo Prado (2018), uma botnet é composta pelos seguintes elementos:

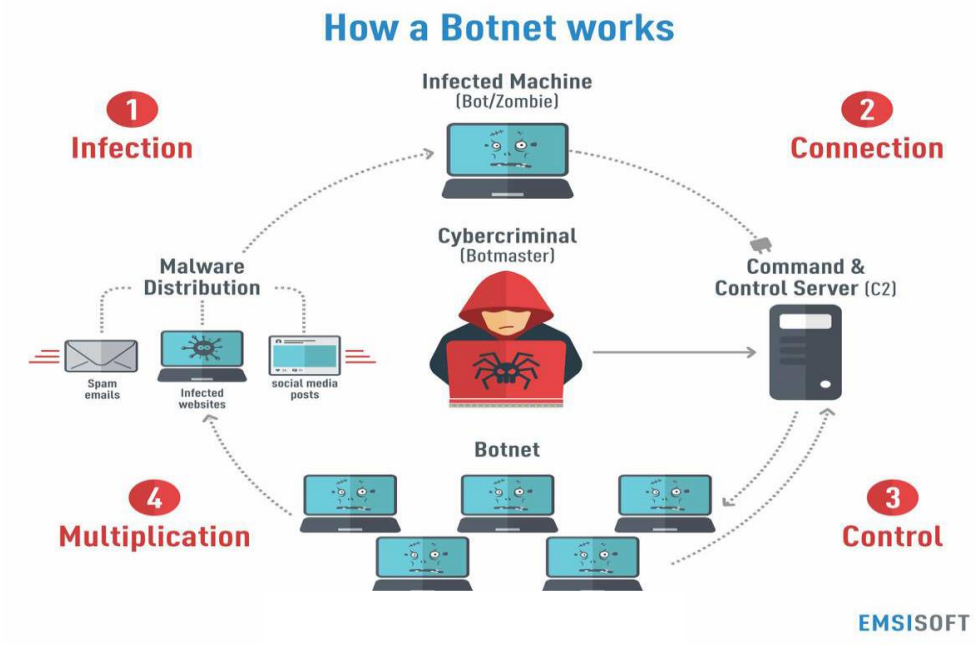
a) Bot: Dispositivo alvo que foi infectado pelo malware.
b) Botmaster: Usuário que detem o controle da rede de bots.
c) Servidor de Comando e Controle (C&C): meio pelo qual o botmaster envia os comandos para os bots.

Assim, botnet é uma rede de bots gerenciada pelo botmaster através do servidor de comando e controle (C&C), que coordena todos os dispositivos, como se verifica na figura 2.2. Essa rede pode ser de dois tipos: centralizada ou descentralizada.

A botnet centralizada segue o modelo cliente-servidor e é o mais utilizado, de forma que os bots estabelecem comunição com o servidor C&C, sob o controle do botmaster.

Já a descentralizada segue o modelo de rede peer-to-peer (P2P), que não possui um servidor central para controlar a botnet (GONÇALVES, 2012, *apud* PRADO, 2018).

Figura 2.2 – Funcionamento de uma botnet



Fonte: Prado (2018)

2.4. Negação de serviço

A arquitetura da Internet expõe os usuários a diversos tipos de ataques e pragas digitais. Ataques comuns que causam enormes prejuízos à vítima são os ataques de negação de serviço. Prevenir-se contra tais ataques é um desafio, mesmo para computadores regularmente atualizados e superdimensionados (LAUFER *Et al*, 2005).

Segundo Laufer *Et al.*(2005), diferentemente da maioria dos ataques da Internet, um ataque de negação de serviço (*Denial of Service*–DoS) não visa invadir um computador para extrair informações confidenciais, como números de cartões de crédito e senhas bancárias, e nem para modificar o conteúdo armazenado neste computador, como sítios da Internet. Tais ataques têm como objetivo tornar inacessíveis os serviços providos pela vítima a usuários legítimos.

De acordo com o mesmo autor:

> No que se refere a negação de serviço na Internet, um estudo recente estima em mais de 4000 o número de ataques em um período de uma semana [Moore et al., 2001]. Um resultado importante mostra ainda que grande parte dos ataques são concentrados em vítimas brasileiras. De acordo com as informações analisadas, o domínio .br é o quarto domínio mais atacado por inundações visando a negação de serviço, concentrando cerca de 5 a 7% dos ataques. Em toda a Internet, somente os domínios .net, .com e .ro foram mais atacados que o domínio brasileiro. Uma informação do relatório anual do CSI/FBI (*Computer Security Institute/Federal Bureau of Investigation*) [Gordon et al., 2005] sobre crimes na área de computação afirma ainda que os ataques de negação de serviço estão entre os incidentes de segurança que mais causam prejuízo às instituições americanas. (LAUFER *Et al.*, 2005)

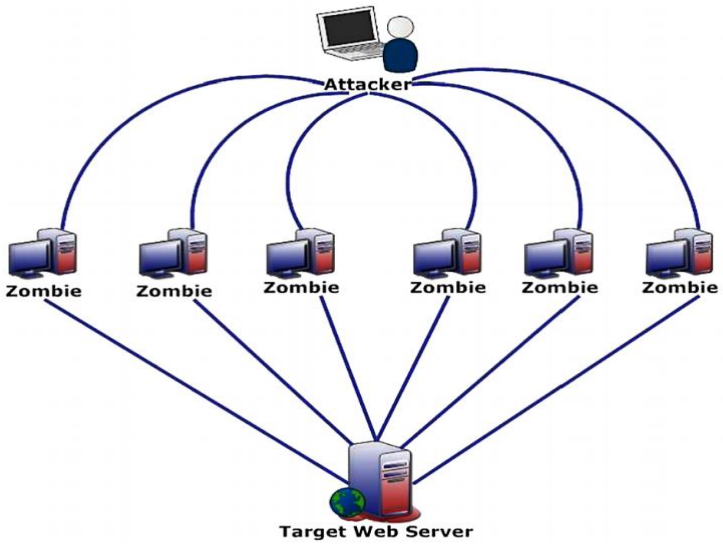
Hoje, os ataques de negação de serviço são comuns e os prejuízos financeiros e de imagem que eles causam atingem cifras enormes. Sem sombra de dúvida, o estudo e o desenvolvimento de técnicas contra-ataques de negação de serviço tornaram-se importantes temas na área de segurança. (LAUFER Et al, 2005).

Os ataques de negação de serviço podem ocorrer de forma direta ou indireta.

a) Direta: o atacante deve impor um volume de requisições maior que a capacidade computacional da vítima para que haja interrupção ou congelamento no fornecimento de determinado serviço; e
b) Indireta: para amplificar o poder de seu ataque, o atacante recorre à ataques distribuídos (DDoS) ou refletidos (DRDoS).

I. Ataques Distribuídos (DDoS):
Os ataques de negação de serviço distribuídos são geralmente usados em ataques por inundação, quando uma estação sozinha não é capaz de consumir algum recurso da vítima. Portanto, diversas estações precisam ser usadas para gerar o tráfego de ataques em direção à vítima e negar o seu serviço. Estas estações geralmente não pertencem ao atacante e são simplesmente computadores comprometidos por alguma falha de segurança. (LAUFER *Et al.,* 2005*)* (Figura 2.4)

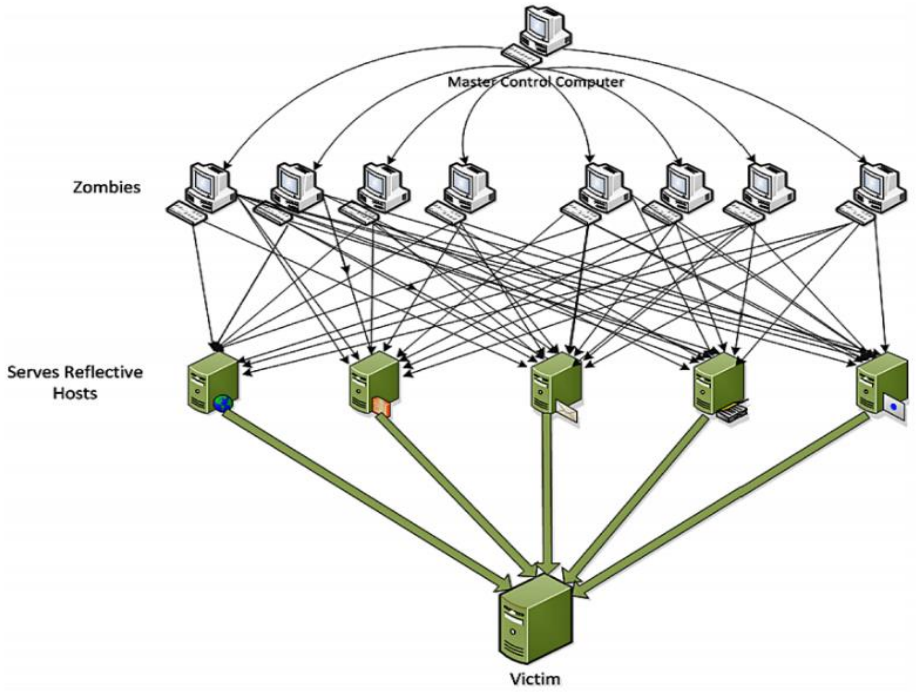
Figura 2.4 – DDoS – Ataque Indireto



Fonte: Alomari *Et al* (2016)

II. Ataques Refletidos (DRDoS):
Um outro tipo de ataque de negação de serviço conhecido é o ataque por refletor. Este ataque também é um ataque por inundação que visa consumir recursos da vítima. Porém, devido a presença de uma estação intermediária entre o atacante e a vítima, ele é aqui tratado como um ataque diferenciado. A ideia é usar a estação intermediária para refletir o tráfego de ataques em direção à vítima. Tal manobra dificulta ainda mais a descoberta da identidade dos atacantes, uma vez que o tráfego que chega à vítima é originado no refletor, e não no próprio atacante. Para a reflexão do tráfego de ataque, é necessário que o atacante envie algum tipo de requisição para o refletor, usando como endereço de origem o endereço da vítima ao invés do seu próprio endereço. Ao receber uma requisição, o refletor não consegue verificar a autenticidade da origem dessa requisição e, consequentemente, envia uma resposta diretamente para a vítima.
Uma das vantagens deste tipo de ataque é que o próprio refletor pode contribuir para o consumo de recursos da vítima. Isso ocorre quando uma mensagem de requisição enviada pelo atacante é menor que a mensagem de resposta enviada pelo refletor. Neste caso, é dito que o refletor também atua como amplificador do tráfego de ataque. (LAUFER *Et al.,* 2005*)* (Figura 2.5)

Figura 2.5 – DRDoS – Ataque Indireto



Fonte: Alomari *Et al*., 2016

Segundo Laufer *et al.* (2005) podemos separar as técnicas de negação de serviço da seguinte maneira:

1) **Inundação**:

Neste caso, a vítima não consegue processar os pedidos de conexão em tempo hábil, o que faz com que a fila de pedidos encha e que muitos deles sejam descartados. Isso ocorre porque o tráfego do usuário legítimo precisa disputar o mesmo recurso com os inúmeros segmentos enviados pelo atacante.

É importante ressaltar que o consumo de processamento neste tipo de ataque pode ser realizado por diversos protocolos, uma vez que todas as mensagens recebidas precisam ser processadas. O ataque à memória por outro lado, depende da alocação de recursos de memória da vítima para ter sucesso;

2) **Ataque à Infraestrutura de Rede**:

Neste caso, o atacante concentra seus esforços em algum ponto crucial para o funcionamento do serviço que não dependa da vítima, como por exemplo:

a. Consumir toda a banda passante da vítima;
b. Atacar onde o tráfego direcionado à vítima é maior do que o enlace de saída pode suportar, como por exemplo um roteador que represente um *gargalo* no tráfego;
c. Ataque aos seus servidores DNS. Como geralmente as pessoas utilizam nomes para acessar um determinado servidor, um ataque ao serviço de resolução de nomes acaba por negar serviços de outros servidores; e
d. Atacar os roteadores responsáveis por encaminhar os pacotes até a vítima e, dessa forma, fazer com que o roteador atacado encaminhe o tráfego legítimo para um local errado ao invés de entregá-lo à vítima.

3) Ataques por Vulnerabilidade:

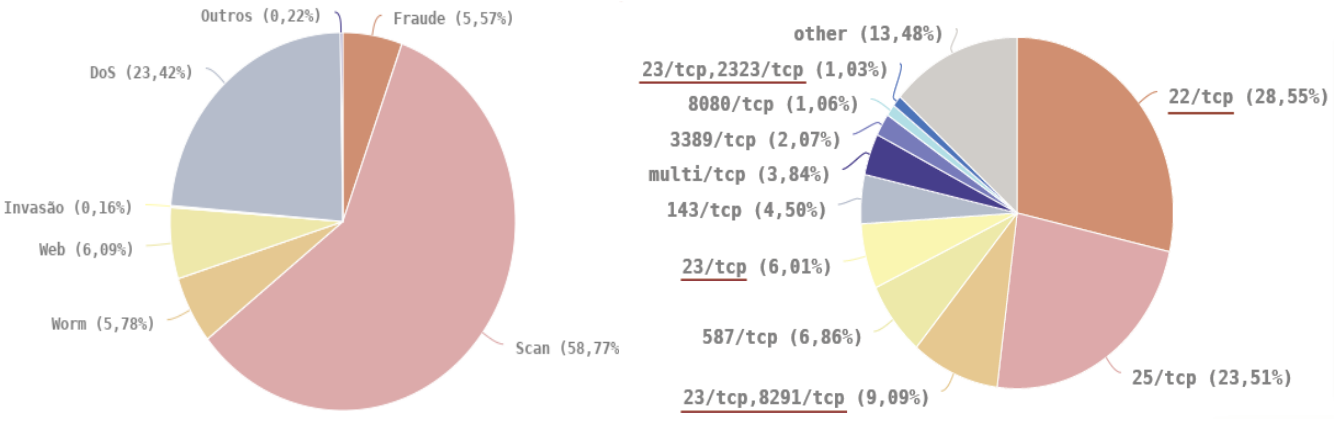
Uma outra forma de negar os serviços providos pela vítima é deixá-la inoperante de alguma forma. Uma das maneiras de atingir este objetivo é explorar alguma vulnerabilidade na implementação da pilha de protocolos ou da própria aplicação da vítima.

Apesar do empenho das áreas acadêmica e industrial na busca de soluções para evitar e remediar tais ataques, as ferramentas existentes são capazes de lidar apenas com ataques pouco refinados. Por isso, os ataques de negação de serviço são, em sua maioria, bem-sucedidos. É fácil burlar as ferramentas de defesa e negar o serviço da vítima durante o tempo desejado pelo atacante, sem que nenhuma medida efetiva possa ser tomada. (LAUFER *Et al.*, 2005*).*

As figuras 2.6 e 2.7 apresentam gráficos sobre atividades de ataques. Na figura 2.6, no gráfico da esquerda, obtido através dos incidentes reportados, apresenta-se uma boa medida sobre a grande porção que os ataques de negação representam, apesar de os dados não representarem a total realidade por apenas utilizar eventos reportados. Já no

gráfico da direita pode-se notar a grande atividade nas portas 22, 23 e 2323, tipicamente usadas em dispositivos IoT.

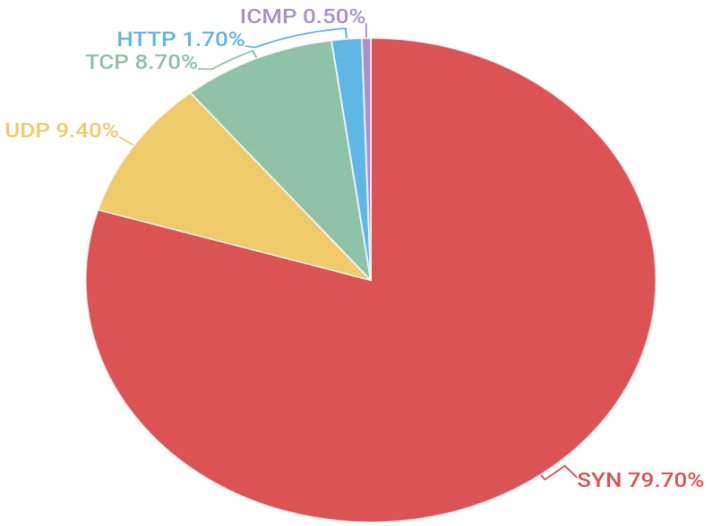
Figura 2.6: Incidentes reportados ao CERT.br em 2018



Fonte:CERT.br (2018)

Já na figura 2.7, formada por dados colhidos dos servidores da Kaspersky (2019), pode-se observar como estão distribuídos os métodos utilizados para ataques de negação, observando que o SYN-FLOOD, umas das técnicas de ataque adotadas pelas ferramentas presentes no arsenal do Mirai, é a mais utilizada.

Figura 2.7: Principais ataques detectados no 3º trimestre de 2019



Fonte: Kaspersky (2019)

2.5. Trabalhos Relacionados

Junior, Silva e Xavier (2017), apresentam como de extrema importância a discussão de propostas de segurança específicas para as necessidades da IoT.

Os autores apontam soluções de segurança *lightweight* (peso leve) como indicadas para IoT, por serem técnicas, arquiteturas, esquemas, e tecnologias de segurança que são leves em termos de processamento e consumo de recursos e têm capacidade de funcionamento em dispositivos heterogêneos. Do trabalho destes autores, podemos ressaltar os seguintes trabalhos relacionados no quadro 2.2.

Quadro 2.2- Algumas soluções para IoT

AUTOR	TRABALHO
Kong et al. (2015)	Criptografia simétrica para dispositivos com recursos limitados.
Borgohain et al. (2015)	Apresentar problemas de segurança e privacidade para usuário final da *IoT*.
Alaba et al. (2017)	Estado-da-arte das ameaças de segurança no contexto de aplicação, arquitetura e comunicação.
Mendez et al. (2017)	Desafios de segurança e privacidade em *IoT*, com vistas a tecnologias e arquiteturas.
Tiburski et al. (2016)	Abordagens lighweight para a padronização de uma arquitetura segura para sistemas de middleware para *IoT*.
Granjal et al. (2015)	Problemas concernentes a protocolos e pontos de pesquisa em aberto na *IoT*.

Fonte: Junior, Silva e Xavier (2017, adaptado),

Também levantam como desafios para segurança em IoT a enorme oferta de dispositivos já disponíveis e, principalmente, a heterogeneidade e escalabilidade que, somados às muitas tecnologias de comunicação, tornam o assunto extremamente complexo.

Os trabalhos de Prado (2018) e Camargo (2018) realizam uma análise estática do código e dinâmica em ambiente virtual do modo de operação do malware Mirai, botnet que ganhou grande atenção após efetuar ataques de negação de serviço em uma escala não vista até o momento de seu aparecimento, e como esse malware explora as vulnerabilidades de dispositivos IoT.

Camargo (2018) ainda apresenta um estudo sobre as variantes do Mirai surgidas após seu código fonte tornar-se público.

Oliveira (2018) estuda em seu trabalho como os dispositivos IoT se apresentam como potencial instrumento de uso em ataques de DDoS.

Alharbi e Aspinall (2018) apresentam em seu trabalho, um estudo detalhado sobre vulnerabilidades encontradas em smart câmeras. Utilizando diversos tipos de equipamentos, os autores forneceram informações de maneira genérica, diferente de trabalhos anteriores onde os elementos estudados se restringiam a tipo ou marca de equipamento. Assim, os autores apresentaram um trabalho que futuramente pode ser usado por especialistas de segurança, para que se obtenha uma melhoria na segurança dos dispositivos IoT.

3 MIRAI

Este capítulo tem como objetivo apresentar com maior detalhes a *Botnet* Mirai, que atraiu as atenções dos especialistas em segurança por explorar vulnerabilidades de equipamentos, como câmeras IP, para produzir um ataque devastador de negação de serviço.

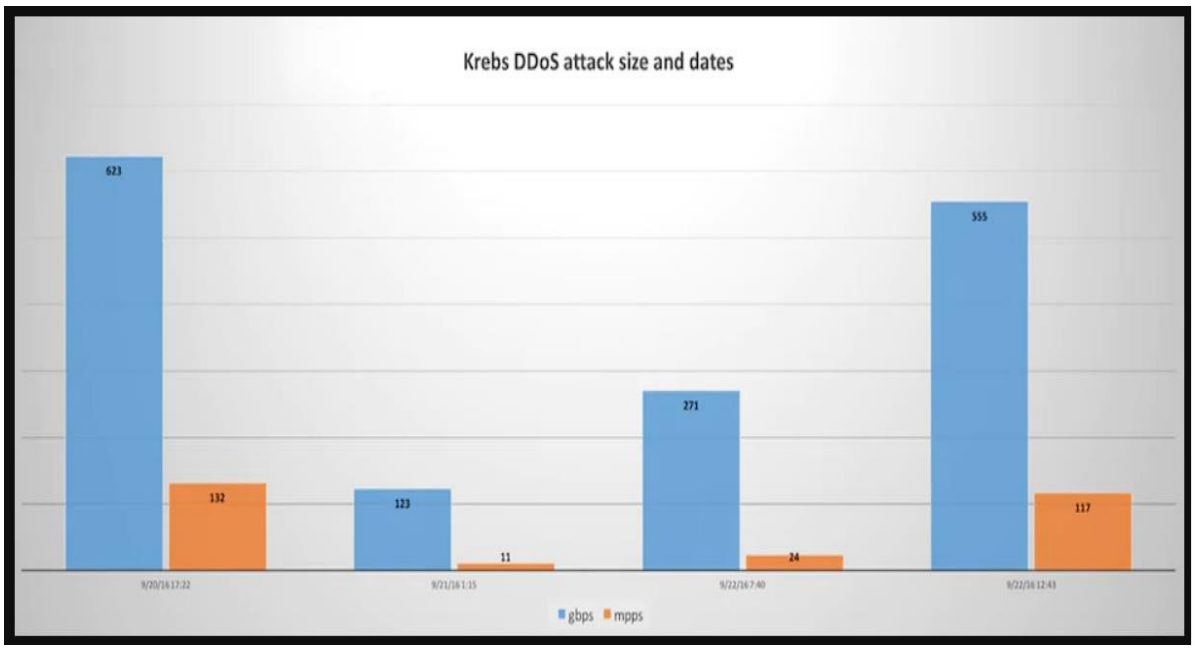
De forma resumida, o Mirai é um malware que explora vulnerabilidade dos dispositivos que possuam a porta 23/TCP liberada, dando acesso remoto ao dispositivo e assim, através de uma biblioteca de credenciais padrão, possa invadir o dispositivo por força bruta e consequentemente infectá-lo e torná-lo membro de sua armada de *bots.*

Esse malware serviu para chamar a atenção à questão da segurança dos dispositivos IoT, expondo vulnerabilidades e apresentando seu potencial para ser usado em ataques de negação. Contudo, se por um lado ressalta-se o uso do código fonte do Mirai para estudo e desenvolvimento de novas soluções para segurança, por outro, surge uma nova preocupação, o surgimento de variantes desse malware mais agressivas e com novas ferramentas de ataques.

3.1.Breve Histórico

O Mirai é uma botnet que ganhou bastante atenção dos pesquisadores da área de segurança após efetuar poderosos ataques de negação de serviço contra o *blog* do pesquisador de segurança Brian Krebs, alcançando 623Gbps no primeiro ataque, segundo o relatório da Akamai (2016). As intensidades dos ataques contra o *blog* de Krebs podem ser observadas na figura 3.1.

Figura 3.1: Ataques de DDoS ao *blog* de Krebs



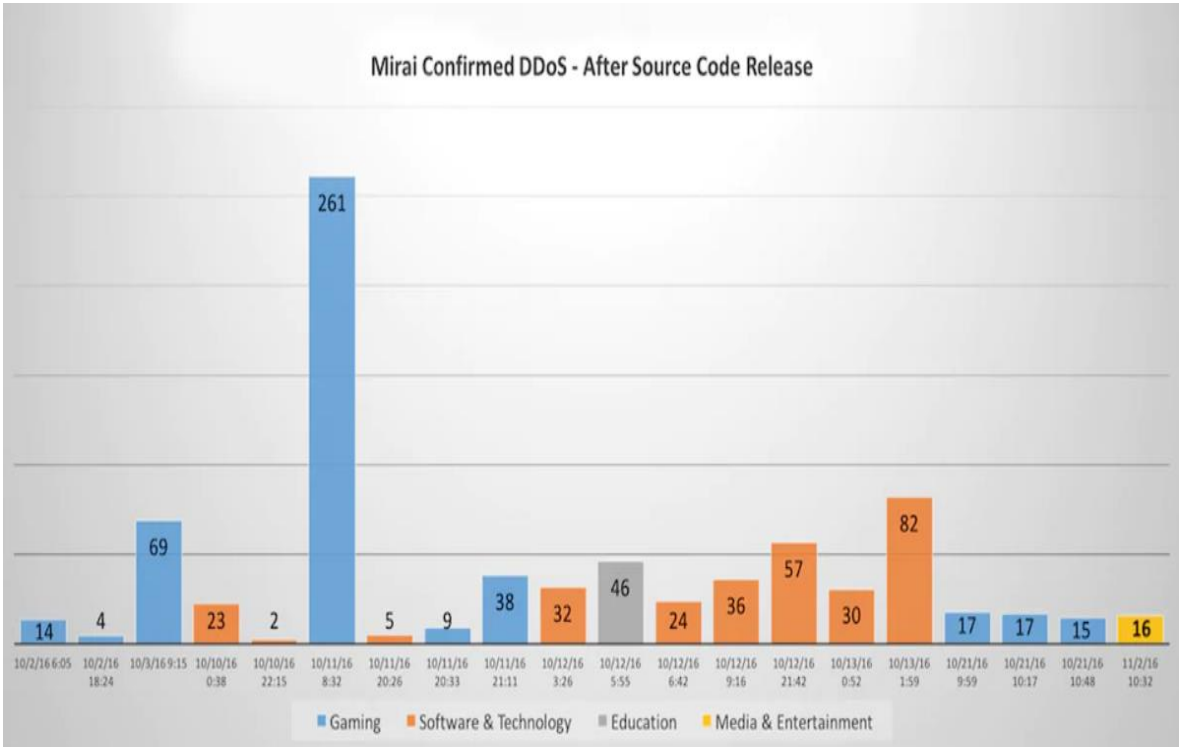
Fonte: Akamai (2016)

Como pode ser observado na figura 3.1, foram feitos três ataques em escalas de Gb (gigabit) e Mb (megabit), sendo o primeiro, no dia 20/09/2016 às 17h22min, com 623Gbps e 132Mbps; no segundo ataque, no dia 21/09/2016 às 01h15min, com 123Gbps e 11Mbps; no terceiro ataque, 22/09/2016 às 07h40min, com 271Gbps e 24Mbps; e o quarto ataque, também dia 22/06/2016 às 12h43min, com 555Gbps e 117Mbps.

Este mesmo relatório da Akamai, destaca que este havia sido o maior ataque mitigado pela empresa até aquele momento.

Apenas alguns dias após essa série de ataques DDoS, o código-fonte do Mirai tornou-se público. O próximo cronograma representa a largura de banda em gigabits por segundo para ataques confirmados do Mirai que ocorrem após o lançamento desse código. O pico de largura de banda, embora ainda substancial, foi observado principalmente abaixo de 100 Gbps em ataques posteriores. Além disso, a maioria dos ataques foi de 30 milhões de pacotes por segundo. (AKAMAI, 2016).

Figura 3.2: Cronograma de ataques que a Akamai atenuou após o lançamento do código do Mirai



Fonte: Akamai (2016)

Um único ataque que atingiu picos com um pouco mais de 30 milhões de pacotes por segundo foi o ataque de 261 Gbps em 11 de outubro, os demais foram todos abaixo dos 82Gbps. Pode-se perceber pela figura 3.2 que após o código do Mirai tornar-se público, a frequência de ataques associados a ele aumentou consideravelmente.

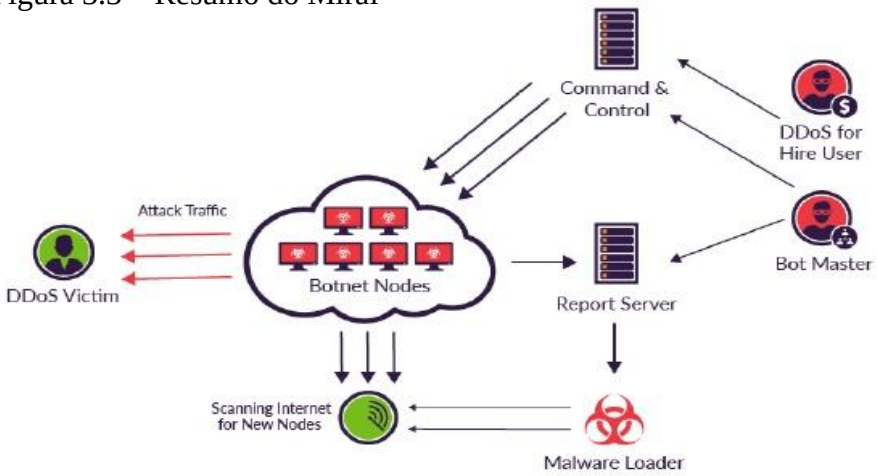
O maior ataque já registrado até hoje atribuído à Mirai foi contra o provedor de DNS da empresa Dyn Inc. que hospeda serviços de sites como Netflix, Airbnb, Twitter, PayPal, Visa, Amazon e The New York Times. O ataque ocorreu em 2016 e atingiu a escala de 1,2Tbps, o que foi mais que suficiente para derrubar os sistemas da provedora na ocasião (EXAME, 2019).

Em se tratando de ataques DDoS, o maior já registrado foi contra a empresa GitHub, que atingiu a escala de 1,35Tbps, porém a autoria do ataque não foi associada ao Mirai (EXAME, 2019).

3.2. Estrutura do Mirai

Segundo Camargo (2018), ao observar a figura 3.3, pode-se dividir a estrutura do Mirai em quatro componentes: (i) *Report Server* (pelas características do código é chamado de *ScanListen*), que é responsável por receber as informações vindas dos *bots*, através da porta 48101, sobre dispositivos vulneráveis, e disponibilizá-las de forma eficiente ao Servidor *Loader*; (ii) o Servidor de Comando e Controle (C&C); (iii) Servidor *Loader*; e (iv) o *Bot*. Os três últimos serão abordados em mais detalhes nas sessões seguintes.

Figura 3.3 – Resumo do Mirai



Fonte: Shoemaker (2017, *apud* CAMARGO, 2018)

3.2.1. *Bot*

Segundo Camargo (2018):

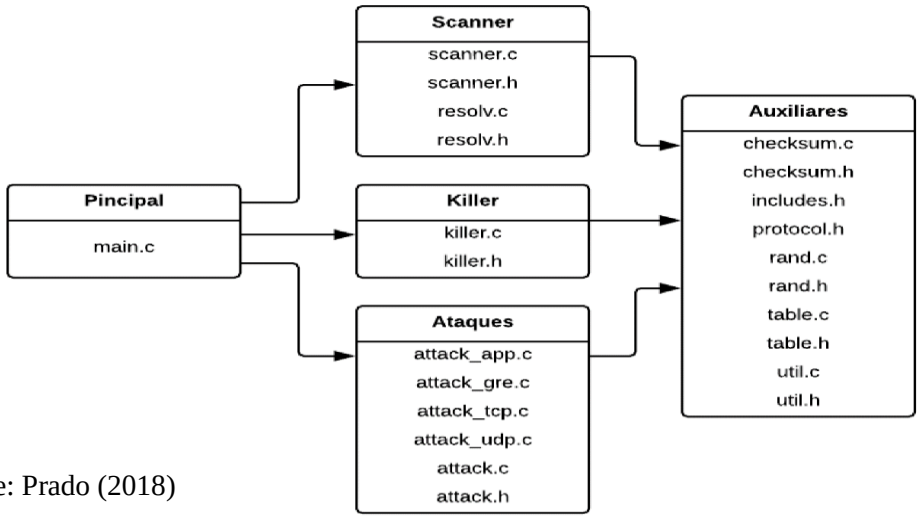
> O código mais longo e mais complexo dentre todos os que compõe o *malware* Mirai é o código do *bot*: os *bots* são a parte mais importante da rede *botnet*, dado que são eles os responsáveis por encontrar outros possíveis *bots* para recrutar para a rede *botnet* Mirai (varrendo a rede a procura de dispositivos vulneráveis) e são eles quem de fato realizam os ataques de negação de serviço requisitados por um cliente do serviço de DDoS *for hire* (CAMARGO, 2018).

A parte do código que representa o *bot* se apresente em três módulos (ataques, *scanner* e *killer*) que serão abordados a seguir.

O ciclo do Mirai inicia no arquivo ‘main.c’, que ao se instalar no dispositivo, deleta seu executável de modo a permanecer apenas na memória RAM do dispositivo e altera o nome dos processos, de modo a dificultar sua detecção. Além disso é responsável por desativar a função *watchdog timer*, responsável por reiniciar o dispositivo em caso de falhas. (PRADO, 2018).

O módulo principal, em seguida, executa a procura por outros programas maliciosos no dispositivo e os elimina, para que o Mirai tenha controle total. Após isso, faz múltiplas chamadas de sistemas para que os módulos ataque, *scanner* e *killer* sejam criados. Após a criação de todos os módulos, é feita uma tentativa de conexão com o servidor de comando e controle (C&C) e, caso bem sucedida, o programa aguarda instruções. (PRADO, 2018). A figura 3.4 apresenta um resumo do módulo *Bot.*

Figura 3.4 – Relação dos arquivos por módulo do código do *bot.*



Fonte: Prado (2018)

3.2.1.1. Módulo *Scanner*

O modulo *Scanner* é responsável por encontrar potenciais novos dispositivos a serem infectados. Ele usa *telnet* e endereços IP públicos gerados aleatoriamente para procurar e checar novos dispositivos IoT vulneráveis (SINANOVIC; MRDOVIC, 2017, *apud* PRADO, 2018). É realizado um *ping* na porta 23 (Telnet) e, a cada decima tentativa de conexão, é utilizada a porta 2323, comumente escolhida por equipamentos IoT como alternativa a porta padrão 23.

Com a lista de endereços IP e credenciais encontradas, esses resultados brutos são enviados a ferramenta *ScanListen*, encontrada na pasta *tools* do Mirai. Essa ferramenta aguarda por conexões TCP na porta 48101, utilizada pelos *bots* para reportar as informações encontradas sobre novos dispositivos no formato **aa.bb.cc.dd:PORTA USUARIO:SENHA** (grifo do autor), ou seja, endereço IP e porta, seguidos do nome de usuário e senha de acesso ao *Telnet* do dispositivo infectado. (PRADO,2018).

3.2.1.2. Módulo *Killer*

Uma vez que o Mirai infecta os dispositivos, ele inicia o modulo *killer*, responsável por verificar e procurar pela existência de processos de malwares rivais tentando executar no dispositivo e eliminá-los caso encontrar. Ele também analisa os serviços rodando nas portas 22 (SSH), 23 (Telnet) e 80 (HTTP), além de reservá-las prevenindo que as aplicações reiniciem (RIEGEL, 2017, *apud* PRADO, 2018).

3.2.1.3. Módulo Ataques

Este módulo implementa funções que são responsáveis por realizar a análise das mensagens de declaração de ataque recebidas do servidos C&C, interpretá-las e fazer com que o *bot* execute os ataques determinados.

No capítulo 4, esses ataques serão apresentados de forma mais detalhada. Na figura 3.5, encontra-se o trecho do código responsável pela declaração dos ataques.

Figura 3.5: Ataques no arquivo ataque.h

```
1  struct attack_target {
2          struct sockaddr_in sock_addr;
3          ipv4_t addr;
4          uint8_t netmask;
5  };
6
7  struct attack_option {
8          char *val;
9          uint8_t key;
10 };
11
12 void attack_udp_generic(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
13 void attack_udp_vse(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
14 void attack_udp_dns(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
15 void attack_udp_plain(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
16 void attack_tcp_syn(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
17 void attack_tcp_ack(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
18 void attack_tcp_stomp(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
19 void attack_gre_ip(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
20 void attack_gre_eth(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
21 void attack_app_http(uint8_t, struct attack_target *, uint8_t, struct attack_option *);
```

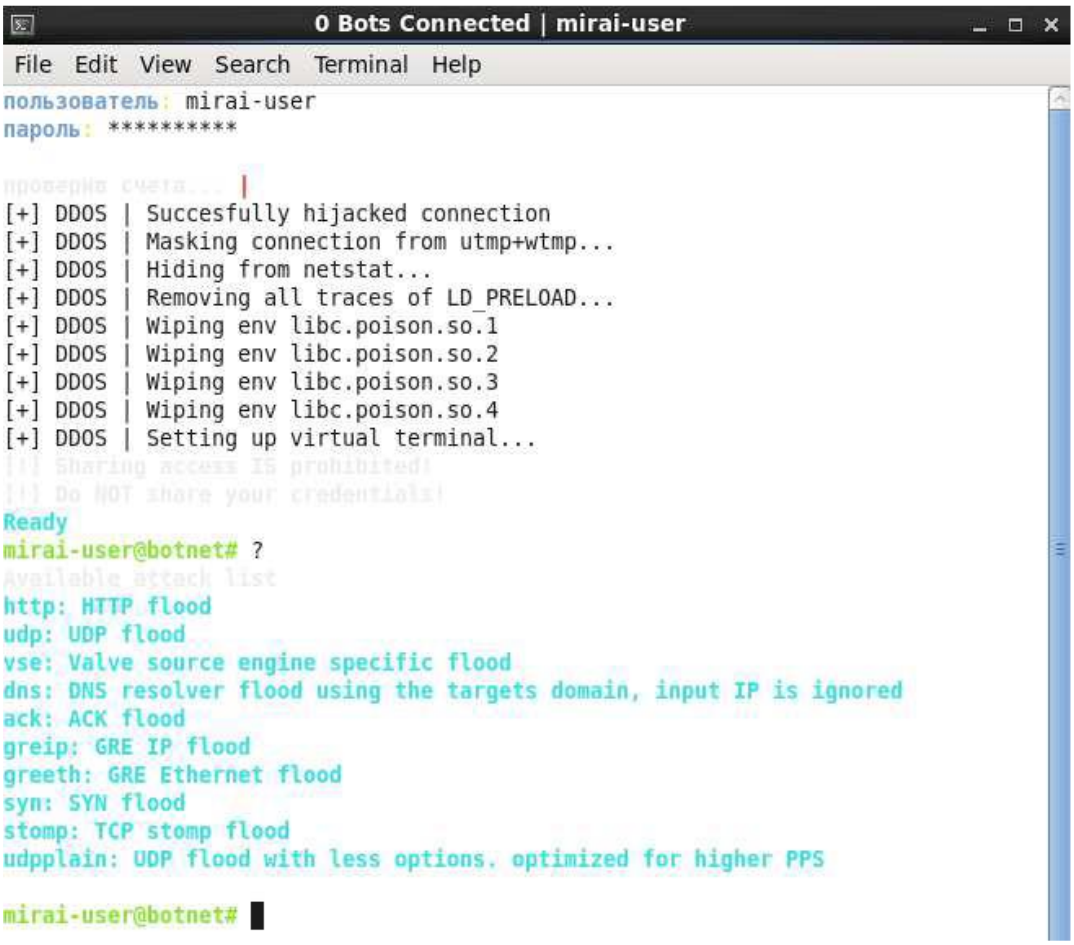
Fonte: Prado (2018)

3.2.2. Servidor de Comando e Controle

O servidor de C&C realiza três funções cruciais no sistema do Mirai: manter o registro dos bots pertencentes à botnet, oferecer o serviço de DDoS, mediante pagamento, para usuários interessados e enviar os comandos de ataques para os bots. (CAMARGO, 2018).

Através da figura 3.6, é possível ver o módulo do administrador, onde percebe-se que além de enviar os comandos de ataques aos bots, também controla a criação de usuários, assim como a quantidade máxima de bots permitida, duração dos ataques e os tempos de espera entre ataques. (PRADO, 2018)

Figura 3.6 – Interface do usuário administrador no C&C



Fonte: Prado (2018)

3.2.3. *Loader*

O Loader (Carregador) foi escrito utilizando a linguagem C com o propósito de disseminar o Mirai recrutando novos dispositivos vulneráveis encontrados. Ele pertence a um módulo separado do servidor C&C e dos bots, pois enviar o binário do malware para infectar novos dispositivos é uma tarefa que demanda uma grande quantidade de recursos e não seria eficiente caso realizada por equipamentos IoT de baixo poder computacional

A conexão entre o *Loader* e o potencial *bot* é estabelecida via *Telnet*, e então feita uma análise sobre a arquitetura do dispositivo, de forma a baixar o binário correspondente. A transferência do binário para o dispositivo é feita usando *wget* ou *tftp*. O wget é combinação de *World Wide Web* e a palavra *get* é uma ferramenta criada pelo *GNU Project* para recuperar conteúdos de arquivos de servidores na Internet, suportando downloads via FTP, SFTP, HTML e HTTPS (HOSTINGER, 2018, *apud* PRADO 2018).

Após verificar quais dessas ferramentas de transferência de arquivos o dispositivo possui, o binário do Mirai é baixado e o novo *bot* é inicializado.

4 ATAQUES UTILIZADOS NO MIRAI

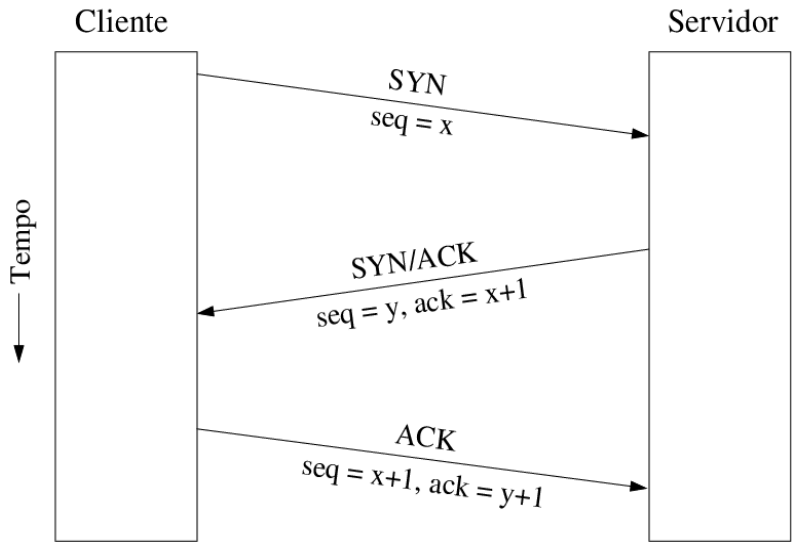
Este capítulo tem o propósito de apresentar em mais detalhes as ferramentas utilizadas nos ataques de negação de serviço do Mirai

4.1. ATAQUES BASEADOS EM PROTOCOLO TCP

O TCP é um protocolo orientado a conexão e com garantia de entrega de segmentos TCP fim a fim por causa dos controles de sequenciamento, erro e fluxo.

Para manter a confiabilidade, o TCP faz uso do *Three Way Handshake*, onde para que se inicie uma conexão entre dois *hosts*, o primeiro envia um segmento SYN (para sincronização); quando o segundo *host* recebe esse pacote, responde com o segmento SYN-ACK, que significa que está pronto para a conexão e com recursos alocados e por fim, o primeiro *host* envia o segmento ACK (para concluir o estabelecimento da conexão). A figura 4.1 resume o funcionamento do protocolo TCP.

Figura 4.1 - Protocolo TCP

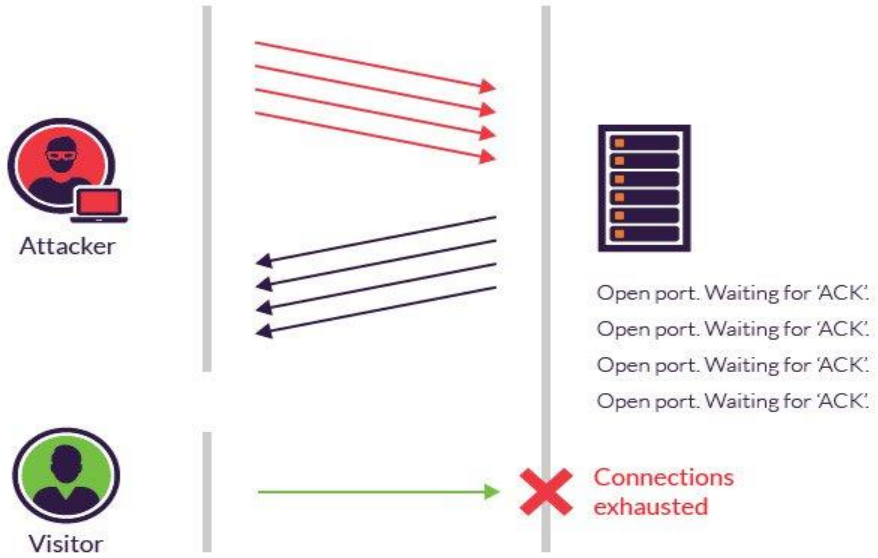


Fonte: Laufer *et al.* (2005)

4.1.1.SYN *FLOOD*

Em um ataque SYN *Flood*, a entidade maliciosa envia sucessivos segmentos SYN para o servidor, que age conforme o protocolo TCP determina, ou seja, responde com um segmento SYN-ACK, porém o servidor nunca obtém resposta e seus recursos ficam alocados ao atacantes até que haja o time out da conexão, porém durante esse período, qualquer usuário legítimo fica impedido de usar os serviços. A figura 4.2 resume o processo.

Figura 4.2 – Ataque SYN *FLOOD*



Fonte: Imperva (2019a)

4.1.2.ACK *FLOOD*

Em um ataque ACK, os invasores enviam segmentos TCP ACK falsificados (aproveitando-se da característica do protocolo TCP de garantir a entrega de todos os segmentos) a taxas muito altas de transmissão que não pertencem a nenhuma sessão atual da tabela de estados do *firewall* e/ou da lista de conexões do servidor.

A inundação do ACK esgota os *firewalls* de uma vítima, forçando pesquisas na tabela de estados e esgotando os recursos do servidor usados para corresponder esses segmentos recebidos a um fluxo existente. (CORERO, 2019).

4.1.3.TCP STOMP *FLOOD*

Segundo Breslaw e Bekerman (2016), STOMP é um protocolo baseado em texto *(SimpleText Oriented Messaging Protocol)* e permite a comunicação de clientes com programas intermediários de mensagem. O ataque STOMP de Mirai pode ser dividido nos seguintes estágios:

1. Um dispositivo botnet usa o STOMP para abrir um handshake TCP autenticado com um aplicativo direcionado.
2. Uma vez autenticados, os dados indesejados disfarçados de solicitação STOMP TCP são enviados ao destino.
3. A enxurrada de solicitações falsas de STOMP leva à saturação da rede.
4. Se o destino estiver programado para analisar solicitações STOMP, o ataque também poderá esgotar os recursos do servidor. Mesmo que o sistema descarte os pacotes de lixo eletrônico, os recursos ainda serão utilizados para determinar se a mensagem está corrompida.

4.2. ATAQUES BASEADOS EM PROTOCOLO UDP

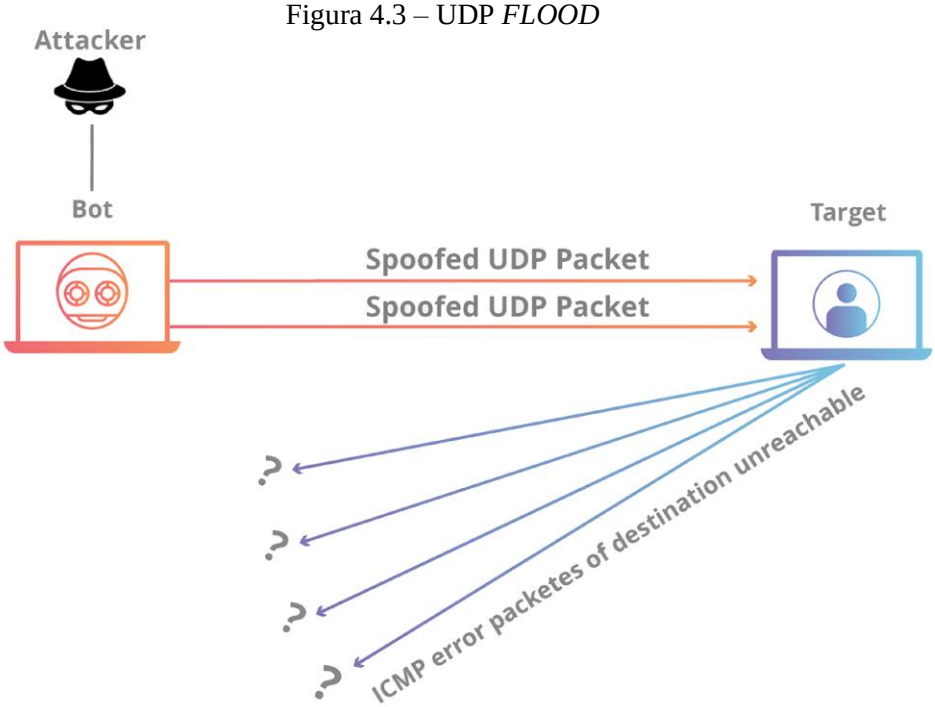
4.2.1.UDP *FLOOD*

Segundo Cloudflare (2018, *apud* PRADO 2018)

> Uma inundação UDP é um tipo de ataque de negação de serviço no qual um grande número de pacotes UDP (*User Datagram Protocol*) é enviado para um servidor de destino com o objetivo de sobrecarregar a capacidade desse dispositivo de processar e responder. O *firewall* que protege o servidor de destino também pode ficar esgotado como resultado da inundação UDP, resultando em uma negação de serviço para tráfego legítimo.
> Uma inundação UDP funciona principalmente explorando as etapas que um servidor executa quando responde a um pacote UDP enviado para uma de suas portas. Sob condições normais, quando um servidor recebe um pacote UDP em uma porta específica, ele executa duas etapas em resposta:
>
> - O servidor primeiro verifica se há algum programa em execução que esteja atendendo solicitações no momento na porta especificada.
> - Se nenhum programa estiver recebendo pacotes nessa porta, o servidor responderá com um pacote ICMP (*ping*) para informar ao remetente que o destino estava inacessível. (CLOUDFLARE, 2018, *apud* PRADO 2018)

A figura 4.3 demonstra a execução do ataque de forma simplificada

Figura 4.3 – UDP *FLOOD*



Fonte: Cloudflare (2018, *apud* PRADO 2018)

4.2.2. *PLAIN* UDP *FLOOD*

O *Plain* UDP *Flood* é um ataque com as mesmas características que o UDP *Flood* visto anteriormente, porém com uma especificidade que o permite ser mais rápido e otimizado. Nesta variação, a porta de origem do ataque é uma porta fixa na qual o *bot* se liga antes que o ataque de *loop* seja executado (BING, 2017, *apud* PRADO 2018).

4.2.3. VSE *FLOOD*

O ataque de inundação *Valve Source Engine* (VSE) é um ataque de amplificação UDP desenvolvido para consumir os recursos de um servidor de jogos através do envio de requisições *TSource Engine Query*, provocando atrasos e até mesmo interrupção do serviço (JAIN, 2016, *apud* PRADO, 2018).

4.3. HTTP *FLOOD*

"O HTTP é a base de solicitações de Internet baseadas em navegador e é comumente usado para carregar páginas da *Web* ou para enviar conteúdo de formulários pela Internet." (CLOUDFLARE, 2018)

Existem duas variedades de ataques de inundação HTTP:

- Ataque HTTP *GET*- nessa forma de ataque, vários computadores ou outros dispositivos são coordenados para enviar várias solicitações de imagens, arquivos ou algum outro ativo de um servidor de destino;
- Ataque HTTP *POST*- normalmente quando um formulário é enviado a um site, o servidor deve lidar com a solicitação recebida e enviar os dados para uma camada de persistência, geralmente um banco de dados. O processo de manipulação dos dados do formulário e execução dos comandos necessários do banco de dados é relativamente intensivo comparado à quantidade de poder de processamento e largura de banda necessária para enviar a solicitação *POST*. (CLOUDFLARE, 2018)

4.4. GRE *FLOOD*

O GRE é um protocolo de comunicação usado para estabelecer uma conexão ponto a ponto direta entre dois nós na rede. É um método efetivo usado para transportar informações entre dois pares sem sofrer interceptações no caminho, ele representa um túnel entre o emissor e o receptor (LEYES; BRESLAW, 2016, *apud* PRADO 2018).

Ao fazer uso deste protocolo de forma amplificada por seus bots, o Mirai pode rapidamente esgotar os recursos de seu alvo devido à carga de processamento necessária para desencapsular os pacotes.

Figura 4.4 – Protocolo GRE

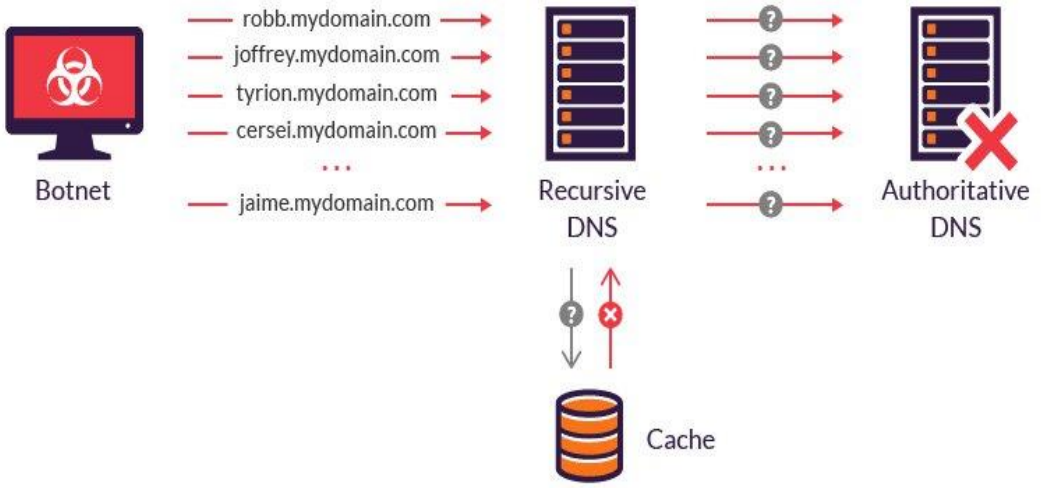
Fonte: O autor

4.5. DNS *FLOOD*

Segundo Imperva (2019b):

> Em um ataque de inundação de DNS, o agressor tenta sobrecarregar um determinado servidor DNS (ou servidores) com tráfego aparentemente válido, sobrecarregando os recursos do servidor e impedindo a capacidade dos servidores de direcionar solicitações legítimas para recursos da zona. O servidor DNS gasta todos os seus recursos procurando esses registros, seu cache é preenchido com solicitações incorretas e, eventualmente, não possui recursos para atender a solicitações legítimas. (IMPERVA, 2019b)

Figura 4.5 DNS *FLOOD*



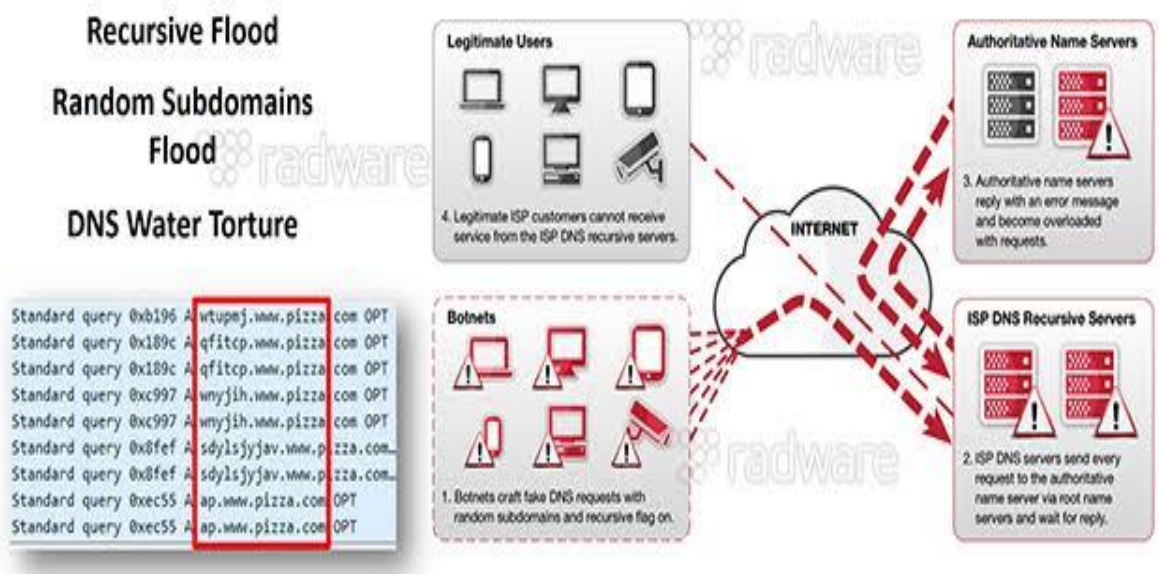
Fonte: Imperva (2019b)

Uma outra forma de ataque de DNS chamada de *Water Torture* é mencionada no trabalho de Camargo (2018) ligando esse tipo de ataque também ao Mirai. Segundo Camargo (2018):

> O ataque DDoS chamado de DNS*Water Torture* é um dos ataques utilizados pelo *malware* Mirai, sendo considerado novo, dado que a verificação de sua utilização na rede tem sido relativamente recente, um dos primeiros ataques sendo registrado no ano de 2014. Desde então, mais ataques deste tipo têm sido registrados na rede, estudos para identificar a sua assinatura sendo realizados. A ideia principal deste tipo de ataque é a indisponibilização de um serviço de forma indireta. Um alvo torna-se inalcançável não porque ele não consegue mais responder às requisições de seus clientes, mas ao invés disso, porque o servidor DNS autoritativo responsável por resolver o seu nome de domínio para clientes enviando requisições legítimas fica sobrecarregado respondendo milhares de requisições falsas vindas de *bots* pertencentes à uma rede *botnet* que em nosso caso é a rede *botnet* Mirai. Às vezes as requisições feitas durante a realização deste tipo de ataque chegam a ser tantas que até servidores DNS recursivos, pertencentes à ISPs e referenciados por roteadores de redes locais, sofrem de forma secundária

com a realização deste ataque. Isso ocorre pois eles precisam constantemente ficar alocando recursos para responder às requisições, porém, nunca recebem a resposta do servidor DNS autoritativo que permitiria a desalocação destes recursos, o que faz com que eles próprios também fiquem sobrecarregados e sofram como alvos de um ataque de negação de serviço. Esse efeito dominó mostra como este ataque pode ser eficiente, sendo capaz de afetar mais de um alvo de uma vez sem sequer enviar um único pacote de dados para este alvo. (CAMARGO, 2018)

Figura 4.6 – DNS *Water Torture*



Fonte: Radware (2017)

5 VULNERABILIDADES IoT E BOAS PRÁTICAS DE SEGURANÇA

5.1.Vulnerabilidades em IoT

Com base no trabalho de Alharbi e Aspinall (2018), pode-se apontar as seguintes vulnerabilidades nos dispositivos estudados pelos autores (smart câmeras):

- Fluxo de dados não criptografados;
- Fluxo de dados com criptografia fraca;
- Segurança fraca nas redes onde se inseriam os dispositivos IoT;
- Uso de senhas padrão.

5.2.Boas práticas de segurança

Altlan e Wills (2002), elencam um conjunto de boas práticas para elevar a segurança em redes IoT, são elas:

- Resistência à adulteração de hardwares: deve-se manter os dispositivos isolados e apenas pessoas autorizadas devem ter acesso físico a eles. Além disso, bloquear portas não utilizadas.
- Autenticação forte: muitos usuários usam senhas fracas ou mesmo não alteram a padrão, o que como foi apresentado anteriormente como uma vulnerabilidade explorada pelo Mirai. Cabe aos usuários, portanto, a política de senhas fortes e a não utilização das senhas padrão;
- Atualizações de firmware: os dispositivos IoT devem possuir um firmware atualizável, de modo a sempre estarem sempre com o último pacote de segurança instalado; e
- Identificação de nós falsos na rede: os dispositivos de envio e recebimento devem ser identificados como legítimos, além disso, cabe ao administrador da rede implementar mecanismos de controle para que dispositivo em sua rede seja identificado de forma única. Evitando assim que aparelhos maliciosos sejam implantados em sua rede assim como efetuar varreduras frequentes para verificar anormalidades na operação de seus dispositivos.

6 IoT: O BRASIL E A MARINHA

"A popularização da Internet das Coisas provocou uma crescente oportunidade para a criação de aplicações em diversas áreas, através da combinação do uso de sensores e/ou atuadores." (CARVALHO, 2017).

Neste contexto, foi criado pelo Governo Federal um plano de ação estratégico, em IoT, para o país liderado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) em parceria com o Ministério da Ciência, Tecnologia, Inovação e Comunicações (MCTIC).

De acordo com esse plano de ação (BRASIL, 2017), o objetivo da implementação da IoT é promover um desenvolvimento sustentável da sociedade brasileira, capaz de aumentar a competitividade da economia, fortalecer as cadeias produtivas nacionais e promover a qualidade de vida dos brasileiros.

Este plano comtempla os seguintes temas:

- Cidades: elevar a qualidade de vida nas cidades e soluções que possibilitem um aumento da segurança pública e uso eficaz dos recursos hídricos e energéticos;
- Saúde: melhoria da eficiência das unidades de saúde;
- Rural: Aumentar a produtividade e colocar o Brasil no cenário mundial de exportador de soluções IoT para agropecuária tropical; e
- Indústria: Aumentar a eficiência e flexibilidade dos processos industriais.

Analisando os objetivos da implementação da IoT no Brasil de maneira ampla, pode-se extrapolar aplicações para o meio militar e para a Marinha, devido à grande variedade de Organizações Militares (OM) existentes, inclusive de caráter industrial e hospitalar.

Dentre os exemplos de possíveis aplicações de IoT na Marinha do Brasil, pode-se ressaltar:

- Uso das soluções IoT para um monitoramento do consumo de recursos hídricos e energéticos, de modo a evitar desperdícios e reduzir as despesas de manutenção das OM;
- Soluções em controle de estoques e gerenciamento de ativos, contribuindo para um sistema de abastecimento mais eficiente; e

- Em relação à segurança orgânica das OM e dos militares pode-se empregar soluções dessa tecnologia para:
  - Implementar uma rede de sensores e câmeras de modo a construir um perímetro que possibilite um alarme antecipado para uma eventual ocorrência de segurança; e
  - Implementar uma solução através de etiquetas RFID descaracterizadas do meio militar de modo que substituam os atuais selos de estacionamentos (que expõem nosso pessoal como militares, colocando em risco sua segurança e de seus familiares, já que o contexto atual é de extrema hostilidade por parte de criminosos para com os militares)

Para essas e outras aplicações sejam implementadas, é necessário que um cuidadoso estudo seja feito com o objetivo de buscar as melhores formas de emprego, sem que a da segurança cibernética e da informação sejam ameaçados.

7 CONCLUSÃO

O trabalho apresentou uma tecnologia que vem crescendo exponencialmente no mercado: os dispositivos IoT. No entanto, com a corrida causada pela concorrência do mercado, diversos dispositivos foram postos à venda sem a devida preocupação com a questão da segurança.

O custo dessa inundação de dispositivos vulneráveis conectados foi explorado largamente pelo Mirai, para execução de ataques de negação de serviço.

No entanto, a tecnologia IoT também se apresenta como uma grande ferramenta para diversos fins, uma vez que, mesmo entre os grandes autores, não há um consenso sobre o que são as ‘coisas’. Pode-se, contudo, generalizar para coisas como sendo qualquer dispositivo capaz de se conectar com a Internet. Sendo assim, as possibilidades para seu emprego são inúmeras.

Considerando o emprego em gerência de recursos e segurança, os dispositivos IoT são uma alternativa com um grande potencial em ajudar a administração pública, contribuindo para um uso mais eficiente dos recursos da União, melhorando a gestão e aumentando a segurança física das OMs e do pessoal.

Porém, esta tecnologia ainda carece de uma padronização sobre requisitos de segurança. Cabendo, atualmente, aos seus utilizadores fazer o uso de boas práticas para obter uma rede bem estruturada e com o mínimo de segurança aceitável.

As dificuldades na implementação e vulnerabilidades destes dispositivos não devem ser encaradas como fatores impeditivos para um salto tecnológico, mas sim como um incentivo para a busca de soluções para sua implementação de forma eficiente e eficaz.

O tema IoT é bem extenso e no escopo deste trabalho não pôde ser abordado todos os assuntos atinentes a este tema, sendo assim, fica como sugestão para trabalhos futuros o estudo sobre a implantação da IoT nas diversas instituições da Marinha do Brasil.

REFERÊNCIAS

AKAMAI. **Threat Advisory**: Mirai botnet. 2016. Disponível em: https://www.akamai.com/br/pt/resources/our-thinking/threat-advisories/akamai-mirai-botnet-threat-advisory.jsp. Acesso em: 20/11/2019

ALHARBI, R.; ASPINALL, D. **An IoT Analysis Framework:** An Investigation of IoT Smart Cameras' Vulnerabilities. in Living in the Internet of Things: Cybersecurity of the IoT - 2018. London, UK. 2018

ALOMARI, E. *Et al*. **A Survey of Botnet-Based ddos Flooding Attacks of Application Layer**: Detection and mitigation approaches. *In:*Gupta, B. *Et al*. **Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security**. Information Science, 2016. p. (55)-(82)

ATLAM, H. F.; WILLS, G. B. **IoT Security, Privacy, Safety and Ethics**.*In:* Farsi M. *Et al* **Digital Twin Technologies and Smart Cities**, **Internet of Things.** Springer, Cham. Suíça. 2020

BRASIL. Presidência da República. Gabinete de Segurança Institucional**. Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018: versão 1.0.** Gabinete de Segurança Institucional. Secretaria-Executiva. Departamento de Segurança da Informação e Comunicações. Brasília-DF, 2015.

_____. Diretoria Geral do Material da Marinha. **DGMM-0540: Normas de tecnologia da informação da Marinha.** Rio de Janeiro-RJ, 2019

_____. Estado Maior da Armada. **EMA-416: Doutrina de tecnologia da informação da Marinha.** Brasília-DF, 2007.

_____. Banco Nacional de Desenvolvimento Econômico e Social (BNDES). **Estudo "Internet das Coisas: um plano de ação para o Brasil"**. Brasília-DF, 2017.

BRESLAW, D.; BEKERMAN, D. **Como o Mirai usa o protocolo STOMP para lançar ataques DDoS.** 2016. Disponível em: https://www.imperva.com/blog/mirai-stomp-protocol-ddos/. Acessado em 30/01/2020

CAMARGO, C. I. **Mirai:** um estudo sobre botnets de dispositivos IoT. Universidade de Brasília. Brasília-DF, 2018.

CARVALHO, F. O. **Descoberta contínua de serviços em IoT**. Pontifícia Universidade Católica do Rio de Janeiro (PUC-RJ). Rio de Janeiro-RJ, 2017.

CORERO. **O que é um ataque de inundação SYN-ACK?** 2019. Disponível em: https://www.corero.com/resource-hub/syn-ack-flood-attack/. Acessado em 02/02/2020

CLARKE, R. A.; KNAKE, R. K. **Guerra Cibernética**: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro-RJ. Editora Brasport Livros e Multimídia LTDA, 2015.

CLOUDFLARE. O que é um ataque DDoS de inundação HTTP? 2018
Disponível em: https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/. Acessado em: 02/02/2020.

EXAME. **Os mais famosos ataques DDoS da história e o que podem nos ensinar sobre segurança na web.** 2019. Disponível em: https://exame.abril.com.br/negocios/releases/os-mais-famosos-ataques-ddos-da-historia-e-o-que-podem-nos-ensinar-sobre-seguranca-na-web Acessado em: 20/11/2019

FIGUEIRA, V. P. **"Internet das coisas"**: Um estudo sobre questões de segurança, privacidade e infraestrutura. Universidade Federal Fluminense. Niterói-RJ, 2016.

GIL, A. C. **Como elaborar projetos de pesquisa**, 4ª edição. São Paulo -SP. Editora Atlas, 2002.

HINTZBERGEN, J. *Et al*. **Fundamentos da segurança da informação**. Rio de Janeiro-RJ. Editora Brasport Livros e Multimídia LTDA, 2015.

IMPERVA**. O que é um ataque de inundação SYN**. 2019a. Disponível em: https://www.imperva.com/learn/application-security/syn-flood. Acessado em : 30/01/2020.

IMPERVA. O que é um ataque de inundação DNS.2019b. Disponível em: https://www.imperva.com/learn/application-security/dns-flood/. Acessado em 02/02/2020.

JUNIOR, J. S. P; SILVA, C. S; XAVIER, D. D. **Segurança em Internet das Coisas:** Um Survey de Soluções *Lightweight*. Universidade do Estado de Mato Grosso, UNEMAT. Alto Araguaia. Revista de Sistemas e Computação, Salvador, v. 7, n. 2, p. 365-384, jul./dez. 2017. Disponível em: http://www.revistas.unifacs.br/index.php/rsc. Acessado em 11/01/2020.

LAKATOS E. M., MARCONI M. **A. Fundamentos de metodologia científica**, 5ª edição. São Paulo- SP. Editora Atlas, 2003.

LAUFER, R. *ET al*. **Negação de Serviço**: Ataques e contramedidas. Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Florianópolis-SC, 2005.

MACINI, M. **Internet das Coisas:** História, Conceitos, Aplicações e Desafios**.** 2018 Disponível em: https://www.researchgate.net/publication/326065859

MIGRANI, E. **A internet das coisas** Rio de Janeiro-RJ**.** Editora FGV, 2018.

JUNIOR, A. A. J. e Edward David MORENO, E. D. **Segurança em Infraestrutura para Internet das Coisas**. Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 370-380. Disponível em: http://www.revista.ufpe.br/gestaoorg. Acessado em 29/12/2019

OLIVEIRA, S. I. C. **Estudo sobre o impacto de dispositivos IoT em ataques DDoS.** Universidade Federal De Uberlândia. Uberlândia-MG, 2018.

PRADO, M. A. **Análise experimental da botnet IoT Mirai**. Universidade Federal de Uberlândia. Uberlândia-MG, 2018

SANTOS S. **Introdução à IoT**: Desvendando a internet das coisas. Joinville -SC. Editora Clube dos Autores, 2018.

SANTOS P. M. P. **Internet das coisas:** O desafio da privacidade. Instituto Politécnico de Setúbal. Escola Superior de Ciências Empresariais. Setúbal, Portugal. 2016

ANEXO I

EXEMPLOS DE USO DO ESPAÇO CIBERNÉTICO PARA FINS BÉLICOS

No caso do ataque da Força Aérea Israelense à Síria, observou-se que mesmo com o moderno sistema de defesa aérea sírio, ocorreu um bombardeio a instalações no território sírio, sem que as aeronaves Eagles e Falcons (empregadas no ataque) fossem detectadas.

Com o sucesso do ataque israelense, os sírios concluíram de forma relutante, lenta e dolorosa que seu sistema de defesa antiaérea havia sido "dominado" ciberneticamente e não pôde sequer disparar seus mísseis de defesa antiaérea, porque não existiam alvos no sistema para que eles pudessem seguir;

Na segunda guerra contra o Iraque, bem antes da fase inicial de bombardeio americano, os militares iraquianos já sabiam que sua rede militar privada, segura e fechada havia sido comprometida, pois já haviam sido alertados pelos próprios americanos

Pouco antes da guerra, milhares de oficiais iraquianos receberam e-mails de dentro do Ministério da Defesa iraquiano dizendo, em resumo, que se eles quisessem que suas tropas ficassem ilesas, eles deveriam ir para casa e deixar os tanques e outros blindados, sob seu comando, em formação e os abandonassem e que as tropas iraquianas seriam reconstituídas após a alteração do regime. Os oficiais iraquianos obedeceram às instruções do Comando Central e quando as tropas americanas chegaram, encontraram os veículos ordenadamente estacionados e nenhuma tropa para fazer resistência.

Ainda segundo Clarke e Knake (2015) a segunda guerra contra o Iraque e o ataque israelense à Síria demonstraram duas formas diferentes de uso da Guerra Cibernética. Uma é o uso para facilitar um ataque convencional. A outra, é o uso para o envio de propagandas e desmoralizar o inimigo (semelhante à antiga prática de soltar panfletos de aviões com mensagens para desmoralizar a tropa e incentivar a rendição).

Porém o uso do ciberespaço não parou por aí, mais uma vez os guerreiros cibernéticos entraram em ação, dessa vez na Rússia.

Segundo Clarke e Knake (2015) em um conflito envolvendo a Rússia e a Geórgia no ano de 2008, os russos, enquanto suas tropas avançavam, usaram um ataque de DDoS contra as comunicações da Geórgia, com isso, perdeu acesso aos meios de comunicação, sites do governo e o acesso aos sites da CNN e BBC, ficando "cega" quanto as movimentações russas.

A Geórgia se conecta à internet através da Rússia e da Turquia. A entrada da maioria dos roteadores da Rússia e da Turquia que enviava tráfego para a Geórgia foi tão inundada com os ataques que nenhum tráfego de saída poderia passar. Os *hackers* assumiram o controle direto do resto dos roteadores que suportavam o tráfego para a Geórgia. Como consequência, os georgianos não conseguiam se conectar a qualquer fonte de notícia ou informação externa e não podiam enviar e-mails para fora do país. A Geórgia efetivamente perdeu o domínio '.ge' da nação e foi forçada a mudar muitos sites de seu governo para servidores fora do país.

Os georgianos bem que tentaram defender seu ciberespaço utilizando 'soluções alternativas' para frustar os ataques DDoS, mas os russos rebateram cada movimento. A Geórgia tentou bloquear todo o tráfego vindo da Rússia. Os russos então redirecionaram seus ataques para parecerem pacotes vindo da China. Além de um servidor mestre em Moscou para controlar todas as botnets usadas nos ataques, servidores no Canadá, Turquia e Estônia também foram usados.

A Geórgia transferiu a página da internet do presidente para um servidor no *Blogspot* do *Google*, localizado na Califórnia. Os russos então configuraram falsos sites presidenciais e direcionaram o tráfego para eles. O setor bancário georgiano desligou seus servidores e planejou superar os ataques, imaginando que a perda temporária do sistema bancário on-line seria mais tranquila do que correr o risco de roubo de seus dados críticos ou danos internos aos sistemas.

Sem poder atingir os bancos da Geórgia, os russos fizeram suas botnets enviarem uma exurrada de tráfego para a comunidade bancária internacional, fingindo serem ataques cibernéticos da Geórgia. Esses ataques desencadearam uma resposta automática da maioria dos bancos estrangeiros, que encerraram suas conexões com o setor bancário georgiano. Sem acesso ao sistema de compensação europeu, as operações bancárias da Geórgia ficaram paralisadas. O sistema de cartões de crédito também foi abaixo, seguido do sistema de telefonia móvel.

No auge do conflito, os ataques DDoS vinham de seis *botnets* diferentes, utilizando tanto computadores de usuários da internet desinformados como através de

voluntários que baixaram o *software hacker* a partir de vários sites anti Geórgia. Depois de instalar o *software*, o voluntário poderia se juntar à guerra cibernética apenas clicando em um botão chamado *Start Flood*.

Neste episódio, na verdade, os russos demonstraram bastante moderação no uso das armas cibernéticas e, provavelmente, salvaguardaram suas melhores armas cibernéticas para quando realmente precisarem delas, em um conflito em que a OTAN e os Estados Unidos estiverem envolvidos.

ANEXO II

COMUNICAÇÕES EM DISPOSITIVOS IOT

O texto adiante é um extrato do trabalho de dissertação de mestrado de Santos (2016). O propósito deste anexo é apresentar alguns modos de comunicação entre dispositivos IoT. O fato de ser possível várias formas de comunicação, sem um padrão propriamente dito reforça a ideia de complexidade e heterogeneidade existente em redes IoT.

- **Wi-fi**

A rede *Wi-fi* é uma rede local sem fios (*WLAN*) que transmite via ondas de rádio padronizadas segundo a norma IEEE 802.111, através de um alcance máximo de 50 metros e uma velocidade de conexão de 2,4GHz ou 5GHz de ultra frequência. Esta tecnologia é ótima para efetuar transferências de grandes quantidades de dados entre os dispositivos. No entanto, esta requer uma grande quantidade de energia para operar, ao passo que muitos dispositivos IoT requerem uma taxa de transferência de dados muito menor do que a usada pelo *Wi-fi*. Isto significa que as baterias dos dispositivos têm de ser mudadas numa base regular.

- **Bluetooth**

Introduzido pela Ericsson na década de 1990, a tecnologia *Bluetooth* é um pilar da comunicação de curto alcance. Transmite dados numa frequência de banda entre os 2,4 e os 2,485GHz. Opera em distâncias menores do que o *Wi-fi* e requer menos energia para operar. O novo *Bluetooth* v4.0, ou *Smart Bluetooth*, é um protocolo importante para a IoT, visto oferecer uma range de alcance similar ao *Bluetooth*, mas projetado para um consumo de energia significativamente reduzido. No entanto, o *Smart Bluetooth* não é realmente concebido para transferência de arquivos e é mais adequado para pequenos blocos de dados.

- **Zigbee**

A tecnologia *Zigbee* permite a dispositivos de baixa potência de operação, baixa taxa de transmissão de dados e baixo custo de implementação enviarem dados na rede, com cada dispositivo capaz de retransmitir os dados em direção ao seu destino pretendido. Resumidamente, é um chip que, por ser mais barato e gastar menos energia, tem vindo a ganhar adeptos no mercado. Para Strickland (2014, *apud* SANTOS, 2016), a única

desvantagem é o facto de o *standard Zigbee* existir em vários formatos, não sendo por isso um verdadeiro *standard*.

- **Z-Wave**

É uma tecnologia de baixo consumo, primariamente projetada para automação de residências, ou seja, para produtos como controladores de lâmpadas e sensores, entre outros. Otimizada para comunicação confiável e de baixa latência de pequenos pacotes de dados, com taxas de transferência entre os 100kbit/s, opera na faixa de sub-1GHz, não interferindo na largura de banda 2,4GHz, como o *Bluetooth* ou o *Z-Wave*. O *Z-Wave* utiliza um protocolo mais simples do que as outras tecnologias, que podem permitir um desenvolvimento mais rápido e simples, no entanto a única fabricante destes *chips* é a Sigma *Design*s, sendo uma desvantagem para as outras tecnologias *wireless* que apresentam múltiplos fabricantes (RS, 2015, *apud* SANTOS, 2016).

- **Thread**

O *Thread* visa solucionar as necessidades da IoT. Com base nas especificações atuais, o *Thread* é capaz de suportar uma rede de até 250 dispositivos. Cada casa pode ter a sua própria rede, ou seja, uma rede pode ter até 250 aparelhos que interagem com os seus habitantes numa base diária. Tal como acontece no *Zigbee*, tem uma topologia mesh, ou seja, todos esses dispositivos são capazes de retransmitir dados. Esta tecnologia procura evitar o problema de vários *standards* como acontece com o *Zigbee*, exigindo um programa de certificação para todos os que desejem incorporar esta tecnologia nos seus produtos, não permitindo a variação de *standards*.

Segundo Strickland (2014, *apud* SANTOS, 2016), se a *Thread* comprovar a sua utilidade, será uma plataforma sólida para a IoT. Mas para isso, os executivos da *Thread* vão necessitar de convencer tanto os utilizadores, como os fabricantes, de que irão resolver um problema, e não apenas adicionar o seu nome à lista de tecnologias em alternativa.

- **RFID**

A tecnologia de RFID (*radio frequency identification* – identificação por radiofrequência) é o termo dado às tecnologias que utilizam a frequência de rádio para captura de dados. Para isso existem diversos métodos de identificação, sendo que o mais utilizado é armazenar um número de série que identifique uma informação, num *microchip*. Tal tecnologia permite a captura automática de dados, para identificação de objetos com dispositivos eletrônicos, conhecidos como etiquetas eletrônicas, *tags* ou RF *tags*, que emitem

sinais de radiofrequência para leitores que recolhem estas informações. Esta tecnologia existe desde a década de 40 e complementa a tecnologia do código de barras, já ela bastante difundida. Segundo a RFID Center of Excellence (2013, *apud* SANTOS, 2016), esta tecnologia pode ter várias aplicações: segurança e controlo de acessos, controlo de tráfego de veículos, identificação pessoal, rastreio animal, identificação de objetos etc.

As suas áreas de aplicação são igualmente as mais variadas: setor público (controlo de passaportes, identificação de ativos em bibliotecas, farmacêutico (autenticidade de produtos), automotivo (imobilizador eletrônico de motor), aéreo (identificação e movimentação de bagagens em aeroportos), médico-hospitalar (identificação de pacientes, controlo da administração de medicamentos).

Barbin, M. (2015, *apud* SANTOS, 2016) afirma que a RFID uma das mais promissoras, visto as etiquetas para identificação de objetos serem baratas, e diferentemente do código de barras, têm processamento e memória, fornecendo alguma inteligência.

- **NFC**

O NFC (*Near Field Communication*) é uma tecnologia que permite a transferência de dados numa comunicação sem fios de curta distância, sendo apenas este fator de distância, a única diferença entre o NFC e o RFID. O NFC surgiu a partir do RFID, por isso muitos dos benefícios observados no ponto anterior são compartilhados por ambas as tecnologias. Tal como acontece no RFID, a comunicação é feita de maneira simples e intuitiva, bastando apenas aproximar dois aparelhos, ou o aparelho e uma *tag* passiva, a uma curta distância. A velocidade da taxa de transferência do NFC é de 424 kbits/s e opera na frequência de 13.56 Mhz.