FACULDADE DE TECNOLOGIA ALCIDES MAYA
TECNÓLOGO EM REDES DE COMPUTADORES

Fernando Antônio Stark Candido

DDoS em IOT: uma revisão da literatura

Porto Alegre
2019

Fernando Antônio Stark Candido

DDoS em IOT: uma revisão da literatura

Trabalho de conclusão de curso de graduação apresentado à Faculdade de Tecnologia Alcides Maya, como requisito parcial para a obtenção do título de Tecnólogo em Redes de Computadores.

Orientador(a): Fagner Coin Pereira

RESUMO

Com a evolução da tecnologia, temos cada vez mais dispositivos IoT disponíveis no mercado, embalados por uma onda de necessidade de automatização dos mais variados equipamentos para facilidade do cotidiano. Porém, justamente por essa facilidade de obtermos dispositivos conectados, temos os riscos de abrirmos nossa rede para usuários mal intencionados. Será apresentada uma revisão da literatura publicada referente a Ataques de Negação de Serviço através do uso de malwares, como botnets em dispositivos conectados (IoT). Este é um estudo de revisão bibliográfica, e por se tratar de um assunto bastante discutido no exterior, foram utilizados em sua maioria artigos publicados na língua inglesa. Analisaremos os principais malwares responsáveis por esses ataques e identificaremos os principais métodos utilizados pelos demais autores para que seja possível a proteção da rede.

Palavras-chave: IoT. Internet das Coisas. DDoS. Denial Of Service. Botnet. Malware.

ABSTRACT

With the evolution of technology, we have increasingly IoT devices available in the market, rocked by a wave of need for automation of various equipment for everyday ease. But precisely because of this ease of obtaining connected devices, we have the risk of opening our network to malicious users. It will be presented a review of the published literature on Denial of Service attacks through the use of malware, such as botnets, to connected devices (IoT). This is a bibliographic review study, and because it is a subject widely discussed abroad, most articles published in the English language were used. We will analyze the main malware responsible for these attacks and identify methods for securing the network.

Keywords: IoT. Internet Of Things. DDoS. Denial Of Service. Botnet. Malware.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CERT	Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores
CFTV	Circuito Fechado de Televisão
CIAC	Computer Incident Advisory Capability
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
DVR	Digital Video Recorder
GRE	Generic routing encapsulation
IoT	Internet of Things
IP	Internet Protocol
LISP	Locator/Identifier Separation Protocol
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
NVR	Network Video Recorder
PTZ	Pan, Tilt, Zoom
TBps	Terabytes per second
TCP	Transmission Control Protocol
RFID	Radio-Frequency Identification
UDP	User Datagram Protocol
UTP	Unshield Twisted Pair
W3C	World Wide Web Consortium

SUMÁRIO

1 INTRODUÇÃO

Com a popularização dos dispositivos IoT (*Internet of Things*), ou em português Internet das Coisas, é cada vez mais comum nos depararmos com cenas que antes achávamos possíveis apenas em filmes de ficção científica, como por exemplo, a possibilidade de controlarmos a temperatura do ar-condicionado e a iluminação da sala de estar diretamente por um aplicativo através de um smartphone.

De acordo com a Gartner[1], estima-se que até o ano de 2020 teremos mais de 20 bilhões de dispositivos conectados, pois hoje encontram-se cada vez mais acessíveis ao público em geral, porém com a popularização dos dispositivos sendo implantados em larga escala.

Devido a esses dispositivos mais acessíveis, percebemos o surgimento de diversos problemas que podemos relacionar principalmente a dispositivos mais baratos de entrada, que estão disponíveis no mercado para o usuário comum e não possuem uma arquitetura definida com uma boa segurança implantada de fábrica, como por exemplo, em uma instalação mais simplificada de CFTV (Circuito Fechado de Televisão), ao utilizarmos um DVR (*Digital Video Recorder*), equipamento onde são conectadas as câmeras de segurança para gravação das imagens obtidas, o equipamento já vem pré configurado para o acesso a internet, possibilitando visualizar em tempo real das imagens das câmeras através de um smartphone ou computador.

Em diversos casos, a segurança não é aplicada principalmente por falta de conhecimento técnico do usuário. No exemplo do DVR, ao instalar o equipamento e já ter algumas funcionalidades pré configuradas, o usuário assume então, por ingenuidade ou por falta de conhecimento, que nenhuma ação precisa ser tomada em relação a segurança do acesso nestes dispositivos tecnológicos, tornando-o vulnerável a falhas, violações e ataques cibernéticos.

Uma das principais razões da necessidade de nos preocuparmos com a devida configuração de dispositivos é mitigar riscos de ataques cibernéticos de

[1] Empresa atuante no ramo de pesquisas e consultorias voltadas para TI.

inutilização temporária da rede de computadores e equipamentos conectados à ela, este tipo de ataque é definido como DDoS (*Distributed Denial of Service*), ou em português ataque de negação de serviço. Segundo Criscuolo (2000), citado por Zargar, Joshi e Tipperque (2013), esse tipo de ataque é uma evolução do DoS, (*Denial of Service*), ou apenas negação de serviço, que são tentativas de impedir que usuários acessem algum recurso de rede, que surgiu por volta da década de 1980 e tem sua primeira ocorrência documentada em 1999, pelo Computer Incident Advisory Capability (CIAC).

O DDoS, segundo Deshmukh e Devadkar (2015) consiste em inutilizar um determinado serviço por esgotamento de recursos de processamento da máquina através da escravização de diversos outros dispositivos, que são chamados de zumbis, fazendo-os atacar um determinado recurso realizando diversas requisições para seu alvo.

Nas seções a seguir serão apresentadas informações sobre as origens do IoT e históricos de ataques DDoS ocorridos em dispositivos conectados, através de pesquisas anteriores de outros autores sobre os assuntos abordados. Serão avaliados ainda os resultados obtidos nas pesquisas, a fim de identificar as possibilidades de defesas e métodos existentes para que seja possível a proteção da rede.

1.1 Problema

Com a crescente onda de dispositivos conectados, aumentam os riscos de abrirmos nossa rede para usuários mal intencionados. Diversos ataques DDoS ocorrem diariamente e se não protegermos nossa rede, podemos nos tornar parte dessa estatística.

1.2 Justificativa

A presente pesquisa se justifica com base na crescente demanda por automação dos equipamentos domésticos, onde os usuários conseguem fácil acesso a equipamentos IoT e acabam deixando de lado a preocupação com a segurança da rede, tornando cada vez mais frequentes casos de invasão e de

indisponibilidade por ataques DDoS, inclusive tendo repercussão na mídia de acordo com o impacto causado. Esperamos que a pesquisa contribua para que possamos mitigar possíveis ataques DDoS a partir dos métodos avaliados com base nas pesquisas dos autores estudados.

1.3 Objetivos

Com base no problema apresentado, os objetivos do presente estudo dividem-se em: Objetivo Geral e Objetivos Específicos, conforme listados a seguir:

1.3.1 Objetivo Geral

Analisar riscos de ataques DDoS e intrusão em dispositivos IoT e métodos de defesas disponíveis no mercado.

1.3.2 Objetivos Específicos

- Analisar ataques DDoS que ocorreram com a utilização de Malwares;
- Entender os danos ocorridos;
- Catalogar métodos de defesas.

1.4 Delimitação do Trabalho

Esta pesquisa limita-se a pesquisarmos malwares capazes de criarem botnets e identificarmos métodos eficazes na proteção tanto da infecção desses malwares, assim como também a detecção e proteção de ataques DDoS gerados a partir dessas botnets. Como esses malwares seguem em constante evolução, manipulados por pessoas más intencionadas, não é possível precisarmos que os métodos avaliados nessa pesquisa manter-se-ão eficazes em um futuro breve.

1.5 Organização Textual

Esta pesquisa foi organizada em quatro capítulos. O segundo capítulo contém toda a estrutura base da pesquisa, a revisão bibliográfica, que foi ordenada em diversos subcapítulos para melhor estruturar a pesquisa.

No primeiro subcapítulo abordaremos um dos objetos da pesquisa, os dispositivos IoT. No segundo subcapítulo buscamos entender as origens dos ataques DDoS. No quarto subcapítulo veremos alguns dos principais malwares utilizados para esses ataques. Por fim, no quinto subcapítulo veremos métodos de defesas para tais ataques propostos por outros autores.

No capítulo 3 será apresentado a metodologia científica utilizada para o desenvolvimento da pesquisa, detalhando a natureza do estudo e as técnicas de coleta e a análise de dados empregados.

No capítulo 4 apresentaremos as considerações finais do estudo e as perspectivas para futuras pesquisas.

2 REVISÃO BIBLIOGRÁFICA

2.1 IoT

A partir do avanço tecnológico que vivenciamos na área da tecnologia da informação e mais especificamente na área de redes de computadores, é comum hoje presenciarmos a utilização de dispositivos IoT[2] em nosso dia a dia, seja na rua, em estabelecimentos comerciais e também na indústria.

2.1.1 Surgimento

De acordo com Pessoa et al. (2015, p. 3 apud Zambarda, 2014), “a ideia de conectar objetos é discutida desde 1991, quando a conexão TCP/IP e a Internet, como é conhecida hoje, começou a se popularizar.”

Segundo Ashton (2009), o termo Internet das Coisas foi criado por ele mesmo, como o título de uma apresentação realizada por ele em 1999, para falar sobre a utilização da tecnologia RFID[3] na Procter & Gamble[4].

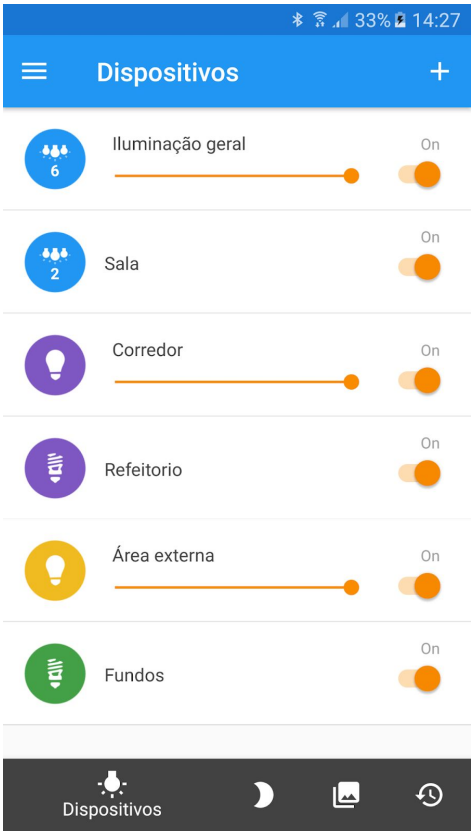
2.1.2 Atualmente

A partir da evolução da tecnologia existente e a necessidade de inovação, surgem as possibilidades de automação de dispositivos que antes utilizávamos para apenas funcionalidades simples e hoje, ao conectarmos o dispositivo à rede, adquirimos a capacidade de termos um maior controle sobre eles, como por exemplo, acendermos a luz da nossa residência a partir do uso de um smartphone, com um aplicativo.

---

[2] IoT (Internet of Things) acrônimo em Inglês para Internet das Coisas.
[3] RFID (Radio Frequency Identification) tecnologia para identificação por rádio frequência.
[4] P&G, empresa multinacional do setor de bens de consumo.

Figura 1 - Aplicativo Bluelux



Fonte: Bluelux (2019)

Essa é apenas uma das inúmeras possibilidades que um dispositivo conectado nos traz, Porém a Internet das Coisas vai muito além do que apenas o controle da iluminação, como resumido por Santos et al.

> A Internet das Coisas, em poucas palavras, nada mais é que uma extensão da Internet atual, que proporciona aos objetos do dia-a-dia (quaisquer que sejam), mas com capacidade computacional e de comunicação, se conectarem à Internet. A conexão com a rede mundial de computadores viabilizará, primeiro, controlar remotamente os objetos e, segundo, permitir que os próprios objetos sejam acessados como provedores de serviços. Estas novas habilidades, dos objetos comuns, geram um grande número de oportunidades tanto no âmbito acadêmico quanto no industrial. Todavia, estas possibilidades apresentam riscos e acarretam amplos desafios técnicos e sociais. (SANTOS et al., 2016, p. 2).

Para Atzori et al (2010), a Internet das Coisas já uma realidade e está crescendo rapidamente no cenário de tecnologia e tráfego de dados wireless, permitindo que vários objetos do cotidiano possam se comunicar e ter uma interação através de chips e sensores. Também afirma que de acordo com o NIC[5], até o ano de 2025 teremos sensores IoT em todos objetos que interagimos no dia a dia, tais

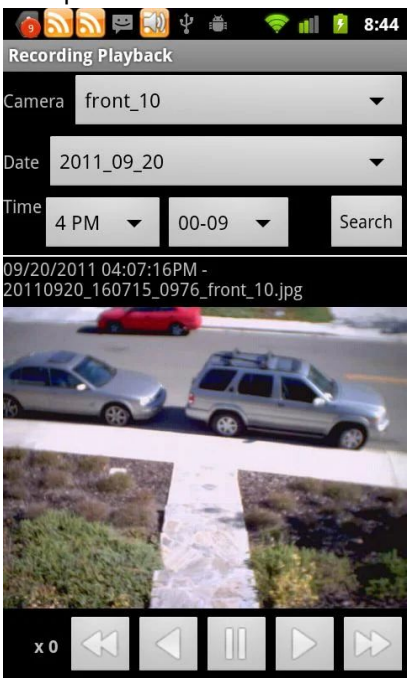
[5] Conselho Nacional de Inteligência dos Estados Unidos da América.

como pacotes de alimentos, móveis, documentos, entre outros. Justamente por essa previsão de grandiosidade próxima, o NIC lista a IoT como uma das seis maiores tecnologias promissoras desenvolvida por civis, gerando um grande impacto no cotidiano dos usuários.

2.2 Câmeras de monitoramento e Circuito Fechado de TV (CFTV)

A evolução das câmeras de monitoramento e circuitos fechados de TV permitem hoje que esses dispositivos sejam conectados também a Internet, tornando-se parte de IoT. Essa conexão é feita para que possamos visualizar a área monitorada pelas câmeras de forma remota, através de um aplicativo em nosso smartphone.

Figura 2 - Aplicativo IP Cam Viewer Lite



Fonte: Google Play (2019)

2.2.1 Topologia de um Circuito Fechado de TV

Os circuitos fechados de TV podem ser analógicos ou digitais, isso influenciará na topologia principalmente na escolha dos equipamentos a serem utilizados, além de impactar diretamente no custo do projeto.

Ao utilizarmos um CFTV com câmeras analógicas, será conectado na rede um DVR para centralizarmos as câmeras, que serão conectadas através de cabos coaxiais. Esse sistema, por ser mais básico permite que seja possível apenas visualizarmos as imagens captadas pelas câmeras.

Já para um sistema mais tecnológico, geralmente de maior porte e consequentemente mais custoso, utilizaremos câmeras com sinal digital conectadas através de cabos de rede UTP diretamente em um NVR (*Network Video Recorder*) ou até mesmo passando antes por um switch, e com isso, conseguiremos ter um controle maior da instalação, podendo gerenciar através da própria rede a qualidade das imagens das câmeras, medir o tráfego de dados e até mesmo manipular a câmera, caso ela seja do tipo PTZ[6].

2.3 DDoS (Distributed Denial of Service)

Conforme Douligeris e Mitrokotsa (2004), ataques DoS (Denial of Service - acrônimo em inglês para Negação de Serviço) hoje são uma das maiores ameaças de segurança presentes na Internet, especificamente ataques DDoS (acrônimo em inglês para Ataque Distribuído de Negação de Serviço), em que o impacto é de maior escala e com maiores danos ao alvo, principalmente por eles ocorrerem sem nenhum tipo de sinal ou aviso, em que no momento que o ataque é iniciado, as capacidades computacionais do alvo acabam comprometidas ou até mesmo são anuladas muito rapidamente.

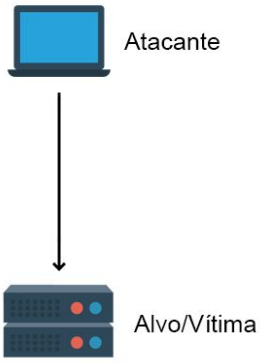
2.3.1 Definição de DDoS

Para entendermos como funciona um ataque DDoS, primeiro devemos compreender um ataque DoS. De acordo com a W3C[7] em sua página de perguntas mais frequentes sobre segurança, a WWW Security FAQ, o DoS é um ataque direcionado a um alvo com objetivo de torná-lo incapaz. O ataque mais comum é aquele em que para inutilizar o alvo, é consumida toda a largura de banda disponível para aquele determinado alvo, causando o que seria uma ‘inundação’ da rede, com

[6] Sigla que une três funcionalidades da câmera (Pan, Tilt e Zoom):
[7] World Wide Web Consortium (W3C) é a principal organização de padronização da Internet.

pacotes falsos trafegando dados a fim de não permitir que dados legítimos trafeguem na rede.

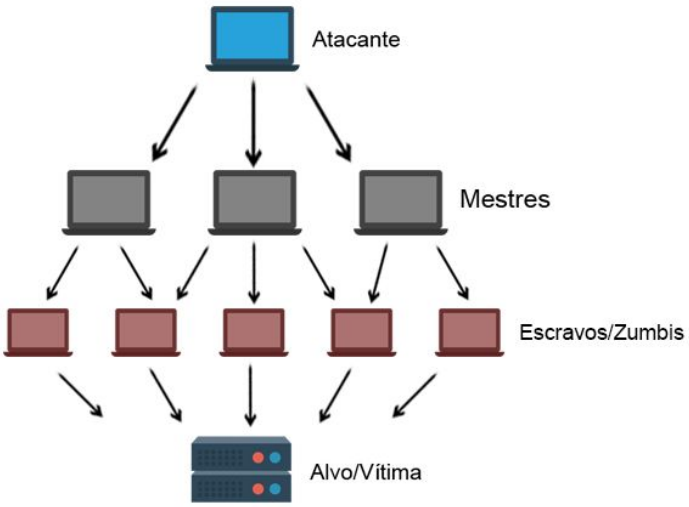
Figura 3 - Ataque DoS



Fonte: Elaborado pelo autor (2019)

Já o ataque DDoS é uma evolução do ataque DoS, conforme a W3C diz em sua página, o ataque distribuído utiliza diversos computadores ou dispositivos para lançar um ataque coordenado em direção a um alvo, portanto o tamanho do ataque é muito maior, com diversos dispositivos escravizados, ou zumbis, lançando esses pacotes ao alvo, multiplicando a efetividade da incapacitação do dispositivo.

Figura 4 - Ataque DDoS



Fonte: Elaborado pelo autor (2019)

2.4 Botnets

De acordo com a CERT, “Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.”.

Segundo Dietz et al. (2018), botnet é uma rede de computadores infectadas por um mesmo malware com o intuito malicioso, como roubar senhas ou enviar spam. Há uma variante da botnet, a IoT botnet, essa mais recente, que possui a capacidade de após infectar os alvos, dispositivos IoT, permite o atacante controlá-los de forma remota para realizarem diversas ações maliciosas, como por exemplo, a realização de um ataque DDoS de grandes proporções geradas a partir dos bots. Ainda segundo os autores, num geral, todos os IoT botnets possuem um comportamento similar, primeiro invadindo os dispositivos não seguros para posteriormente transformá-lo em um zumbi da botnet, capaz de gerar o ataque DDoS.

2.4.1 MIRAI

Podemos verificar que esse tipo de ataque vem sendo utilizados recentemente, principalmente com o malware Mirai, que surgiu em 2016 e utiliza como alvo dispositivos IoT vulneráveis, e seguem sendo utilizados a partir de variações do bot original, conforme a Kaspersky:[8]

> Recentemente, fomos confrontados com uma nova versão do Mirai (botnet de propagação própria que tem como alvo dispositivos IoT e foi responsável por um ataque DDoS massivo em servidores Dyn em 2016). Segundo os analistas, a botnet está equipada com mais exploits, o que a torna ainda mais perigosa e permite que se expanda mais rapidamente. O mais preocupante é que esta nova versão não só atende às suas vítimas habituais (roteadores, câmeras IP e outras coisas inteligentes), mas agora também vai contra dispositivos IoT das empresas. (KASPERSKY, 2019, p.1)

Ainda segundo a Kaspersky, o código-fonte do malware foi disponibilizado na Internet, ou seja, está aberto para todas as pessoas e qualquer usuário mal intencionado poderia utilizar dele para realizar novos ataques, pois “O código Mirai é

[8] Empresa russa produtora de softwares de segurança.

muito flexível e adaptável, por isso pode ser reprogramado com novos exploits para expandir seus objetivos" (KARSPERSKY, 2019).

Segundo Kolias et al. (2017), para possibilitar a contaminação dos alvos, o botnet age escaneando os IPs da rede pública através das portas TCP 23 ou 2323. Através do método de invasão por força bruta o Mirai age testando diversas senhas para concluir o acesso, pois ele possui em seu código-fonte as credenciais de 62 equipamentos IoT, a maioria câmeras de segurança e equipamentos DVR.

Em outro estudo, Antonakakis et al. (2017) monitoraram os ataques que ocorreram com a utilização do botnet e afirmam que durante o período monitorado, de setembro de 2016 até 28 de fevereiro de 2017, o Mirai foi responsável por 15.194 ataques DDoS.

Conforme o estudo de Dietz et al. (2018), basicamente todo IoT botnet possui um ciclo de vida de sete passos, que foram organizados na Tabela 1:

Tabela 1 - Ciclo de vida de um botnet

Passos	Instrução
1	Escanear a rede pública em busca de portas abertas nos dispositivos;
2	Realizar a penetração por força-bruta;
3	Eliminar possíveis malwares concorrentes que já tenham infectado o dispositivo;
4	Estabelecer comunicação com o dispositivo mestre;
5	Executar scripts maliciosos;
6	Repetir os passos anteriores, buscando novos alvos;
7	Realizar ataques DDoS conforme ordem do dispositivo Mestre

Fonte: DIETZ, Christian et al. (2018)

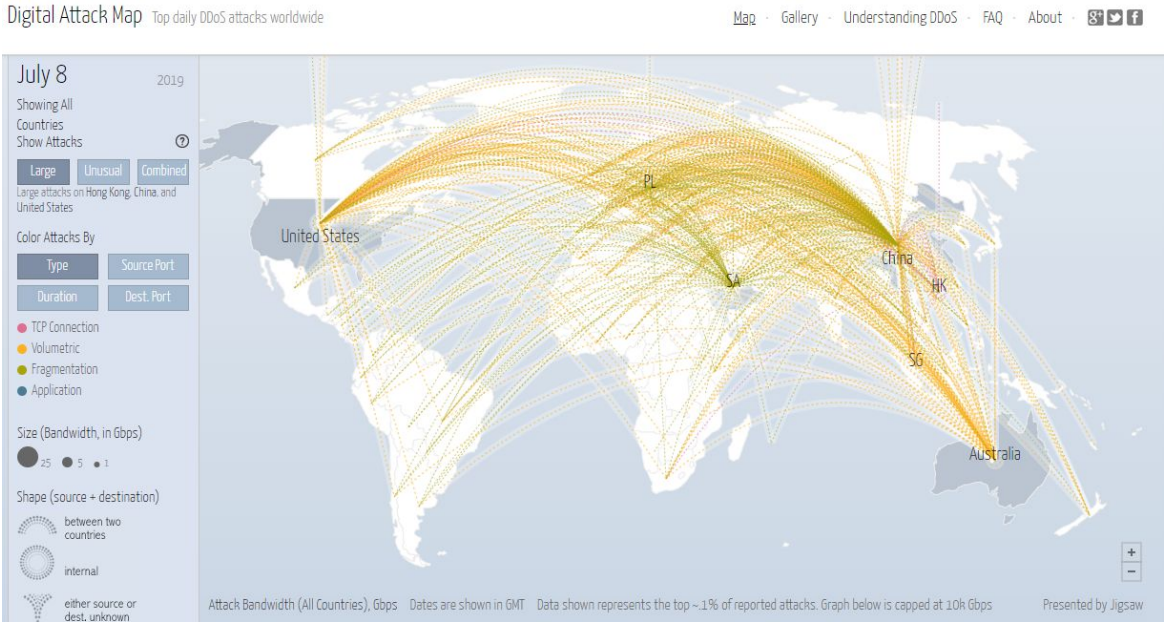
Os dados do ciclo de vida da Tabela 1 foram obtidos pelos autores com base no IoT botnet Mirai, porém como no estudo eles mencionam, o comportamento de todo IoT botnet é praticamente idêntico, portanto, os sete passos do ciclo de vida do Mirai servem para exemplificar qualquer outro botnet, principalmente porque,

segundo os autores, após o vazamento do código fonte do Mirai na internet, diversos IoT botnets variantes surgiram, como o Satori, Okiru, Persirai, Masuta e o Puremasuta.

2.5 Estratégias de proteção

Ataques DDoS ocorrem diariamente por todo o planeta, com diversos alvos e atacantes de diferentes países e com diferentes motivos. Como um ataque DDoS afeta a capacidade de banda de um determinado provedor, é possível mensurarmos e visualizarmos a grande maioria dos ataques que ocorrem, pois existem websites especializados nisso, como por exemplo o Digital Attack Map, que informa em seu guia de perguntas e respostas que obtém esses dados a partir de uma base de dados montada pela Arbor Networks ATLAS®, empresa global de inteligência em ameaças, que compila os dados obtidos através de acordos de compartilhamento anônimo de dados de tráfego de provedores de banda larga do mundo todo, somando mais de 130 Tbps de tráfego.

Figura 5 - Mapa de ataques DDoS



Fonte: Digital Attack Map (2019)

Justamente por esses ataques ocorrerem diariamente, é de extrema importância que sejam tomadas estratégias de proteção para que possamos evitar

indisponibilidades indesejadas em nossa rede. As proteções disponíveis vão desde firewalls a softwares exclusivamente direcionados à proteção e análise de ataques DDoS, com finalidade de prevenir, coibir ou até mesmo mitigar os danos causados por um possível ataque.

Tabela 2 - Estratégias de defesa pesquisadas

Estratégia	**Método**	**Resultado esperado**
Honeypot	Armadilha	Propositalmente se tornar um alvo para poder estudar o atacante e mitigar o ataque.
LISP	Prevenção de contaminação	O atacante não consegue identificar hosts vulneráveis.
Computação na Borda	Detecção e mitigação	Identificação rápida do ataque (0.62 segundos) e bloqueio do tráfego malicioso (cerca de 82%)
Detecção e Isolamento	Prevenção de contaminação	Identificar as vulnerabilidades e isolar os dispositivos antes da infecção pelo malware.

Fonte: Elaborado pelo autor (2019)

2.5.1 Honeypot

Em um artigo publicado no CERT[9], Hoepers, Steding-Jessen e Chaves (2007 apud SPITZNER, 2002) definem o método Honeypot como sendo "...um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido", ou seja, funciona como uma réplica do alvo com o intuito de enganar o atacante, que ignora o alvo e passa a atacar a réplica, permitindo que seja possível obter dados de sua origem a fim de mitigar o ataque.

2.5.2 Protocolo de Separação de Endereço e Identificação

Luo et al. (2013) propuseram uma abordagem de proteção a infecção dos botnets com a utilização do protocolo LISP, a fim de evitar que esses *hosts* tornem-se escravos e façam parte de um exército zumbi. O estudo diz que para qualquer método de invasão que o botnet utilizará, primeiro ele precisa descobrir se

[9] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

o host a ser acessado consegue receber pacotes, e para isso, é utilizado o IP público, porém ao utilizarmos o protocolo LISP, os caminhos para os hosts deixam de ser diretamente através do IP e são conhecidos apenas pelos roteadores através de mapas da rede. Quando uma solicitação de envio de pacote para um host é realizada, o roteador envia o mapa da rede para identificá-lo. Na proposta de Luo et al. (2013), ao receber diversas requisições em um curto período de tempo, o mapa é alterado e o roteador deixa de responder a essa solicitação, portanto o atacante não consegue identificar hosts vulneráveis.

2.5.3 Computação na borda

De acordo com a gigante de tecnología, Hewlett Packard Enterprise:

> A computação na borda é uma arquitetura de TI aberta e distribuída que apresenta poder de processamento descentralizado, capacitando tecnologias de computação móvel e Internet das Coisas (IoT). Na computação na borda, os dados são processados pelo próprio dispositivo, computador ou servidor local, em vez de serem transmitidos para um data center. (HEWLETT PACKARD, 2019, p. 1)

Bhardwaj, Miranda e Gavrilovska (2018) propuseram uma alternativa de defesa que consiste na utilização de *Edge functions* para a prevenção de ataques DDoS nos dispositivos IoT, rodando códigos de defesa diretamente no dispositivo de borda. Essa função, chamada de ShadowNet, nos testes realizados pelos autores, provou-se de certa forma eficaz.

Dentre os botnets utilizados para a simulação, um deles foi o Persirai, que realiza ataques de inundação de UDP gerados através de câmeras de segurança. Seus resultados mostraram que utilizando a função, foi possível identificar o ataque de inundação UDP em 0.62 segundos após o seu início, também bloqueando cerca de 82% do tráfego malicioso que tentou penetrar na rede.

Em contrapartida, como os próprios autores sugerem, deve-se ser avaliada a viabilidade do uso do *ShadowNet,* pois para que seja realmente eficaz, o software deverá rodar em diversos dispositivos, gerando altos custos, além disso, o software deve ser capaz de identificar ataques de múltiplas origens geográficas, pois em suas simulações, ele foi eficaz detectando apenas uma origem.

2.5.4 Detecção e Isolamento

Dietz et al. (2018) propuseram em seu estudo, um método de defesa para evitar a contaminação pelos malwares na rede, essa aplicação foi dividida em várias fases, em que a primeira delas consiste em um firewall aplicado diretamente no roteador da rede que realizará uma varredura a fim de identificar dispositivos IoT vulneráveis. Ao final desse escaneamento, todos os dispositivos vulneráveis identificados são catalogados e o firewall montará uma tabela com o endereçamento de todos eles. A partir dos endereçamentos da tabela, o firewall então age de forma similar ao malware, pois ele possui mais duas etapas: escanear por portas abertas e então testar as combinações de credenciais que os malwares utilizam.

Chega então o momento que foi chamado pelos autores de isolamento, em que com todos os endereçamentos dos dispositivos vulneráveis mapeado, aqueles que foram invadidos pelo firewall são colocados em regras de acesso para que não seja possível o acesso externo a eles sem antes passar pelo firewall.

Em seus testes, os autores comprovaram a eficácia da solução, realizando três testes com três dispositivos, em cada teste alterando os dispositivos vulneráveis na simulação. Em todas as vezes o firewall foi capaz de identificar as vulnerabilidades e isolar os dispositivos antes da infecção pelo malware.

3 METODOLOGIA

3.1 Pesquisa bibliográfica e documental

Como procedimento metodológico adotado para obtenção dos objetivos, foi realizado uma pesquisa bibliográfica e documental. Segundo Fachin (2001), “A pesquisa bibliográfica é, por excelência, uma fonte inesgotável de informações, pois auxilia na atividade intelectual e contribui para o conhecimento cultural em todas as formas do saber.“. A pesquisa considera informações de livros, artigos, teses e matérias jornalísticas em portais da internet. Para Fonseca (2002):

> A pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto. Existem porém pesquisas científicas que se baseiam unicamente na pesquisa bibliográfica, procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta (FONSECA, 2002, p. 31-32).

4 CONCLUSÕES E PERSPECTIVAS

Apesar de não ser um tema novo, ataques DDoS seguem acontecendo e não temos perspectiva de solução a curto prazo, pois como os malwares geralmente possuem código aberto, criminosos seguem desenvolvendo novas variantes para realizar tais ataques. Apesar disso, como visto na pesquisa, é possível tomarmos algumas ações para prevenirmos maiores consequências caso ocorra algum ataque tendo nossa própria rede como alvo de um ataque. Também é possível evitarmos que nossa rede seja contaminada com algum determinado malware, evitando assim de nossa rede tornar-se parte de um exército pertencente a uma botnet.

Também foi possível identificarmos alguns dos principais malwares responsáveis por ataques DDoS utilizando botnets. Esse passo é importante para que possamos perceber a evolução dos malwares e a necessidade de aplicarmos segurança na rede.

Na bibliografia pesquisada, vimos que DDoS é um assunto que não possui uma solução completamente eficaz, justamente pela evolução constante dos malwares, porém através dos métodos identificados torna-se possível a mitigação de alguns dos principais métodos de invasão e ataques que possamos sofrer.

Conforme já mencionado, os métodos para defesa identificados são válidos para os malwares estudados nas versões em que se encontram na presente data, porém é possível que em algum momento, os métodos que hoje possuem eficácia deixem de proteger para determinado malware.

Com a expansão das organizações e de suas redes, a alta disponibilidade é um requisito chave. Até mesmo curtos períodos de inatividade de uma rede podem gerar perdas de produtividade e grande impacto financeiro, como vimos na pesquisa grandes empresas tendo períodos de indisponibilidade, causando prejuízos enormes, seja em acessos a determinada plataforma, compras que deixam de ser realizadas, clientes que procuram a concorrência por não conseguir acessar o site de sua empresa e diversos outros problemas. Diante disso, o presente trabalho apresenta uma pesquisa bibliográfica contendo propostas de mecanismos de defesas para as redes, através da implantação de softwares específicos, protocolos,

monitoramento da rede. Os testes realizados pelos demais autores comprovam a necessidade de tais procedimentos e a sua determinada eficácia.

Como não é possível prevermos como os malwares se comportarão nas suas próximas evoluções, há uma limitação na pesquisa, onde podemos apenas estudar o que já ocorreu, portanto, uma das principais formas de nos defendermos de ataques futuros, além dos métodos implementados pelos outros autores, é a constante manutenção de todos os equipamentos instalados em nossa rede. Isso inclui atualizações de segurança fornecidos pelos fabricantes, utilização de senhas seguras, a troca das senhas de tempos em tempos, assim como também utilizarmos softwares específicos para isso, como firewalls.

No entanto, as limitações oportunizam uma continuidade ao estudo, possibilitando que a medida que novos malwares sejam lançados, novas formas de defesa mais eficazes também estão por vir, cabendo estudos para comprovação objetiva e de coleta e amostra de dados confiáveis de tais métodos.

REFERÊNCIAS

ANTONAKAKIS, Manos et al. Understanding the mirai botnet. In: **26th {USENIX} Security Symposium ({USENIX} Security 17)**. 2017. p. 1093-1110.

ASHTON, K. **That 'Internet of Things' Thing** Disponível em: <https://www.rfidjournal.com/articles/view?4986>. Acesso em: 12 de junho 2019.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. **Computer networks**, v. 54, n. 15, p. 2787-2805, 2010.

BHARDWAJ, Ketan; MIRANDA, Joaquin Chung; GAVRILOVSKA, Ada. Towards IoT-DDoS prevention using edge computing. In: **{USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 18)**. 2018.

DA SILVA, Thalita Bento et al. A INTERNET DAS COISAS: SERÁ A INTERNET DO FUTURO OU ESTÁ PRESTES A SE TORNAR A REALIDADE DO PRESENTE?. **Engenharias On-line**, v. 1, n. 1, p. 41-50, 2015.

DESHMUKH, Rashmi V.; DEVADKAR, Kailas K. Understanding DDoS attack & its effect in cloud environment. **Procedia Computer Science**, v. 49, p. 202-210, 2015.

DIETZ, Christian et al. IoT-Botnet Detection and Isolation by Access Routers. In: **2018 9th International Conference on the Network of the Future (NOF)**. IEEE, 2018. p. 88-95.

DIGITAL ATTACK MAP. Disponível em **<**http://www.digitalattackmap.com/>. Acesso em 20 de novembro de 2019.

DOULIGERIS, Christos; MITROKOTSA, Aikaterini. DDoS attacks and defense mechanisms: classification and state-of-the-art. **Computer Networks**, v. 44, n. 5, p. 643-666, 2004.

FACHIN, Odília. **Fundamentos de metodologia**. Saraiva Educação SA, 2001.

FONSECA, João José Saraiva. Metodologia da Pesquisa Científica. 2002.

GARTNER. **Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.** Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>. Acesso em 12 junho de 2019.

HEWLETT PACKARD ENTERPRISE. **O que é computação na borda?.** Disponível em <https://www.hpe.com/br/pt/what-is/edge-computing.html>. Acesso em 03 de dezembro de 2019.

HOEPERS, Cristine; JESSEN, Klaus S.; CHAVES, M. H. P. C. Honeypots e honeynets: Definições e aplicações. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, ver**, v. 1, 2007.

KASPERSKY. **Empresas são novo foco da botnet Mirai.** Disponível em <https://www.kaspersky.com.br/blog/mirai-enterprise/11616/> Acesso em 06 de novembro de 2019.

KOLIAS, Constantinos et al. DDoS in the IoT: Mirai and other botnets. **Computer**, v. 50, n. 7, p. 80-84, 2017.

LUO, Hongbin et al. Preventing DDoS attacks by identifier/locator separation. **IEEE network**, v. 27, n. 6, p. 60-65, 2013.

SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. **Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos**, p. 31, 2016.

SHOBANA, M.; RATHI, S. IOT Malware: An Analysis of IOT Device Hijacking. 2018.

W3C. **The World Wide Web Security FAQ.** Disponível em <https://www.w3.org/Security/faq/wwwsf6.html> Acesso em 29 de outubro de 2019.

ZARGAR, Saman Taghavi; JOSHI, James; TIPPER, David. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. **IEEE communications surveys & tutorials**, v. 15, n. 4, p. 2046-2069, 2013.