FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Paulo Gusttavo Tognato

Ransomware em IoT

Americana, SP

2020

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Paulo Gusttavo Tognato

Ransomware em IoT

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: colocar apenas uma (01) área temática identificada na ficha de inscrição do curso.

Americana, SP

2020

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

T576r TOGNATO, Paulo Gusttavo

Ransomware em IoT. / Paulo Gusttavo Tognato. – Americana, 2020. 52f.

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

Orientador: Profa. Dra. Maria Cristina Aranda

1 Internet das coisas 2. Segurança em sistemas de informação I. ARANDA, Maria Cristina II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518

Paulo Gusttavo Tognato

Ransomware em IoT

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana

Americana, 30 de junho de 2020.

Banca Examinadora:

_____
Maria Cristina Aranda (Presidente)
Doutora
Fatec Americana

_____
Rogério Nunes de Freitas (Membro)
Mestre
Fatec Americana

_____
Daniela Dal Fabbro Amorim (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Inicialmente, de um modo especial, meus sinceros agradecimentos a Profa. Orientadora Dra. Maria Cristina Aranda, pelo apoio, incentivo e confiança depositada em minha pessoa para a realização deste trabalho, compartilhando com parte de sua sabedoria e conduzindo de maneira firme, porém amigável, todas as fases para o desenvolvimento desta pesquisa que serviu como uma contribuição importante e positiva nesta fase de minha vida acadêmica.

A todos os Professores que contribuíram para o meu enriquecimento cultural ao longo destes quatro anos de graduação.

Por fim, gostaria de agradecer pelos incentivos de todos os colegas e amigos da Faculdade de Tecnologia de Americana (FATEC - Americana) e, pelos vários momentos que compartilhamos juntos, os quais sempre foram especiais, restando disso certeza única de que essa convivência resultou em frutos de amizades que se prolongaram por muitos anos.

RESUMO

O constante desenvolvimento tecnológico vem revolucionando e transformando o cotidiano das pessoas como nunca se viu antes. Diante disso, surge então os dispositivos interconectados também conhecidos como Internet das Coisas – IoT. No entanto com a constante revolução e modernização da tecnologia, muitos problemas que se acreditava já estarem resolvidos, voltam a causar pânico na comunidade tecnológica. A escolha do presente assunto é referida ao constante desenvolvimento de novas tecnologias e a importância quanto ao tratamento da segurança das informações em um âmbito geral pelos fabricantes desenvolvedores, empresas e consumidores de novas tecnologias, principalmente devido ao constante crescimentos de ataques do tipo *ransomware*, que possuem capacidade de sequestrar, bloquear e cobrar taxas de resgate sobre os equipamentos infectados. Tendo como tema principal destacar a importância quanto ao tratamento sobre segurança da informação na era da Internet das Coisas, o presente estudo objetivou-se nos pilares da segurança da informação, bem como suas vulnerabilidades, ameaças e suas principais causas de quebra de segurança. Também se objetivou em analisar o contexto histórico, bem como os principais riscos e ameaças relacionados a invasão e sequestro de dados e *hardwares*, causados por ataques e *softwares* maliciosos, principalmente do tipo *ransonwares*, em dispositivos que utilizam da tecnologia da Internet das Coisas e, identificar possíveis soluções para minimizar os riscos e problemas encontrados. Com base na análise dos referenciais bibliográficos, foi aceitável compreender a importância de tratar da segurança da informação associadas ao desenvolvimento de novas tecnologias emergentes, além também de ter sido possível elencar soluções para tratativa e remediações de problemas comuns destes novos dispositivos, que de certa forma, já são comuns no cotidiano dos desenvolvedores de novas tecnologias, das empresas e pessoas que também consomem esses dispositivos.

Palavras-Chave: IoT, ransomware, segurança.

ABSTRACT

The constant technological development is revolutionizing and transforming the people's daily routine like never happened before. In view of that, interconnected devices appear, also known as Internet of Thing – IoT. However, with the constant technological revolution and modernization, so many problems that should be solved, came back to cause panic at technological community. The choice of the present subject is due to the constant development of new technologies and the importance of the treatment of information security in general by developers, companies, and customers of new technologies. Mainly due the constant increase in ransomware attacks, which have the capacity to hijack, block, and charge ransom fees on infected equipment. Taking as its mainly theme to emphasize the importance as the treatment about information security on the Internet of Things age, the present study aimed on the information security pillars, as well as vulnerabilities, threats, and main causes security breaches. It also aimed in to analyze the historical context, as well as the main risks and threats related to invasion and hijacking of data and hardware's, cause by attacks and malicious software's, mainly of ransomware types, into device that using Internet of Things technology and, to identify possible solutions to minimize the risks and problems found. Based in bibliography analyses, it is accepted to understand the importance of treat information security associated to development of new technologies. Besides, it was possible to list solutions to treat and remediating the common problems in these new devices, which are somehow common to new developers of new technologies, companies, and costumers of these devices.

Keywords: IoT, ransomware, security.

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO

Por diversos anos, a preocupação com a segurança dos recursos de Tecnologia da Informação (TI) das organizações não foi um assunto que alarmasse as companhias ou até mesmo os usuários finais, tendo em vista que o acesso a esses recursos computacionais era limitado e por muitas vezes manuseados somente por especialistas técnicos. Além disso, esses recursos, por muitas vezes, ficavam concentrados em um único computador central, ou em salas confinadas, e com isso todo o sistema computacional estava protegido contra possíveis ataques externos.

Entretanto, com a constante evolução dos recursos de TI, trazendo o surgimento dos computadores pessoais, difusão de equipamentos de redes de computadores, e consequentemente nos últimos anos o surgimento de dispositivos e sensores inteligentes capazes de se conectar com a Internet, houve uma expansão exponencial no compartilhamento de informações ou recursos tecnológicos. Com isso a necessidade da implementação de técnicas e políticas de segurança da informação para proteção destes novos recursos de TI se tornou um assunto cada vez mais discutido nas gestões das empresas.

A escolha do tema do presente trabalho se deve a importância em que a segurança da informação alcançou em todo o mundo e o constante crescimento e inclusão de novos dispositivos inteligentes. Tendo em vista a grande capacidade de compartilhamento de dados por esses novos dispositivos interconectados com a Internet, tratar sobre segurança nesse contexto é algo essencial para prover confiabilidade tanto para os usuários finais quanto para as empresas que utilizam estes dispositivos.

O objetivo geral deste trabalho é especificar o quão importante é tratar sobre segurança da informação na era da Internet das Coisas.

Como objetivos específicos estão a apresentação dos principais riscos e ameaças relacionados a invasão e sequestro de dados e *hardwares*, causados por *softwares* maliciosos, principalmente do tipo *ransonwares*, em dispositivos que utilizam da tecnologia da Internet das Coisas e, a identificação de possíveis soluções para enfrentar os riscos levantados.

O **método científico** de pesquisa utilizado foi baseado em uma pesquisa exploratória que visa expor uma base fundamentada em teorias e conceitos acerca

do tema de estudo, tendo como técnica empregada a pesquisa em livros, *sites* especializados, artigos e relatórios técnicos.

O trabalho foi estruturado da seguinte forma:

O primeiro capítulo descreve a histórico e conceitos, expansão, principais aplicações e os perigos relacionados ao crescimento exponencial da fabricação e uso dos dispositivos IoT.

O segundo capítulo descreve os conceitos de segurança da informação, seus pilares, vulnerabilidades e ameaças. Além da apresentação das principais causas de quebra de segurança da informação.

A partir do segundo capítulo, o terceiro capítulo é estruturado com o intuito de fornecer informações complementares e específicos sobre os tipos, formas de infecção e legislações que permeiam os ataques com *ransomware*.

Com base nos capítulos anteriores, o quarto capítulo trata sobre as preocupações do crescimento dos ataques *ransomwares* em dispositivos IoT. Além disso, é exposto também o porquê de os ataques estarem serem direcionados a dispositivos IoT e o que pode ser feito, tanto por empresas, quanto por usuários finais em casa de percepção de uma invasão.

Já o último capítulo trata sobre a considerações finais do trabalho, reunindo informações de aprendizado e sugestões de desenvolvimento por parte das indústrias de dispositivos IoT de possíveis mecanismos, ferramentas e soluções para os problemas apresentados durante o estudo.

2 INTERNET DAS COISAS (IoT)

A Internet das Coisas, ou *IoT*, está influenciando o estilo de vida da humanidade desde como reagem até como se comportam. Desde o ar-condicionado que pode ser controlado com um *smartphone*, até carros inteligentes que conseguem entregar com a melhor e menor rota, ou um relógio inteligente o qual está controlando atividades pessoais e monitorando funções vitais.

Kevin Ashton (2009), utilizou pela primeira vez em 1999 o termo IoT (acrônimo de *Internet of Things*, ou, Internet das Coisas), enquanto trabalhava e estudava os dispositivos por identificação por rádio frequência (RFID) e realizava apresentações de sistemas de sensores, que começavam então a conectar o mundo físico com a Internet. A partir disso, o termo IoT começou a ser utilizado e novas pesquisas foram desenvolvidas, levando a criação de novos padrões internacionais. Com isso, parcerias de empresas para a criação de novos dispositivos também começaram a aumentar em larga escala.

Santos (2016), definiu resumidamente o significado da terminologia dos dispositivos de IoT.

> “A Internet das Coisas, em poucas palavras, nada mais é que uma extensão da Internet. Esta extensão é feita ao proporcionar que objetos do dia a dia (quaisquer que sejam) se conectem à Internet. A conexão com a rede mundial de computadores viabiliza, 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 muitas oportunidades tanto no âmbito acadêmico quanto no industrial. Todavia, estas possibilidades apresentam riscos e acarretam amplos desafios técnicos e sociais.”

Ou seja, IoT é uma rede gigante, com uma plataforma que tem a capacidade de receber, analisar e compartilhar dados, e interconectar dispositivos físicos através da Internet. Estes dispositivos capturam e compartilham dados, mensurando como são utilizados e o ambiente em que estão sendo operados. Tudo isso com a utilização de sensores que são integrados em cada dispositivo físico.

Esses dispositivos físicos são os telefones móveis, eletrodomésticos, semáforos, carros inteligentes e quase tudo que se vê durante o dia a dia. Os sensores que estão integrados nesses dispositivos emitem dados continuamente, monitorando a forma que tais dispositivos estão operando.

A IoT provê uma plataforma comum para que todos esses dispositivos depositem seus dados, em uma linguagem comum, para que todos os dispositivos possam se comunicar com eles mesmos. Mas a principal questão é como os dispositivos compartilham essa grande quantidade de dados e como esses dados são usados.

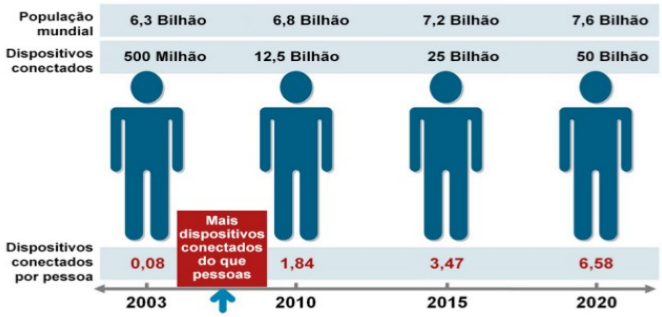
Como os dados são emitidos de vários sensores, através de *softwares* embarcados nos dispositivos físicos, os dados podem ser enviados para a plataforma de IoT. De forma segura, a plataforma de IoT captura os dados de diferentes fontes e consegue analisar e extrair informações valiosas conforme as necessidades. Finalmente, o resultado pode ser compartilhado com outros dispositivos para obter uma melhor experiência dos usuários, automações e melhorias de eficiência de processos e dos próprios dispositivos e sensores.

2.1 Expansão da IoT

Nos últimos anos, percebe-se que houve um crescimento exponencial no desenvolvimento e comercialização de novos dispositivos, e principalmente a capacidade destes dispositivos serem interconectados. Essa nova era de interconectividade de objetos e dispositivos com a Internet, teve sua primeira terminologia criada por um pioneiro em tecnologia britânico chamado Kevin Ashton.

A Cisco (2011), divulgou no *Cisco Internet Business Solutions Group* (IBSG), estimando que até 2020, teríamos cerca de 50 bilhões de dispositivos de IoT ao redor do mundo. A Figura 1 a seguir, mostra que nesse período, a Cisco havia apresentado que já existiam cerca de 12,5 bilhões de dispositivos IoT ao redor do mundo.

Figura 1 - Crescimento de Dispositivo IoT até 2020.

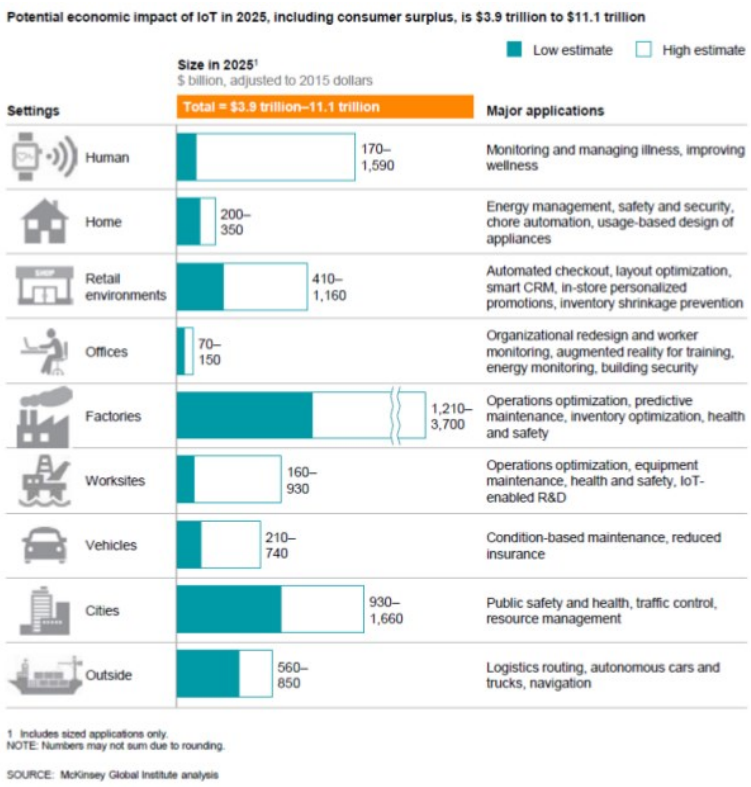


Fonte: Cisco IBSG (2011)

De acordo com McKinsey (2015), foi estimado que, das nove áreas em que a IoT está sendo aplicada constante nessa pesquisa, o valor de impacto econômico,

entre gastos e receitas, nessas áreas será de 3,9 a 11,1 trilhões de dólares por ano em 2025, conforme mostrado na Figura 2 a seguir.

Figura 2 - Gráfico econômico de aplicações de IoT



Fonte: McKinsey Global Institute (2015)

Segundo a Security Today (2020), foi identificado que os dispositivos de IoT, alcançariam uma marca histórica de mais de 31 bilhões de dispositivos em 2020. Um crescimento de aproximadamente 18%, se levado em conta os cerca de 26 bilhões de dispositivos já registrados em 2019. Além disso, foi identificado que o mercado norte alcançou aproximadamente 83,9 bilhões de dólares em receitas com dispositivos IoT.

Essa rápida expansão da utilização destes dispositivos interconectados por todo o mundo, já facilitam e continuarão facilitando a comunicação e desenvolvimento de soluções para as pessoas e organizações.

2.2 Aplicação da IoT

A tecnologia IoT já está embarcada em muitos dispositivos, e promete equipar bilhões de dispositivos com inteligência e conectividade. Alguns dos principais domínios na qual a IoT já está sendo utilizada em larga escala, são: indústrias, residências, saúde, dispositivos vestíveis e agricultura.

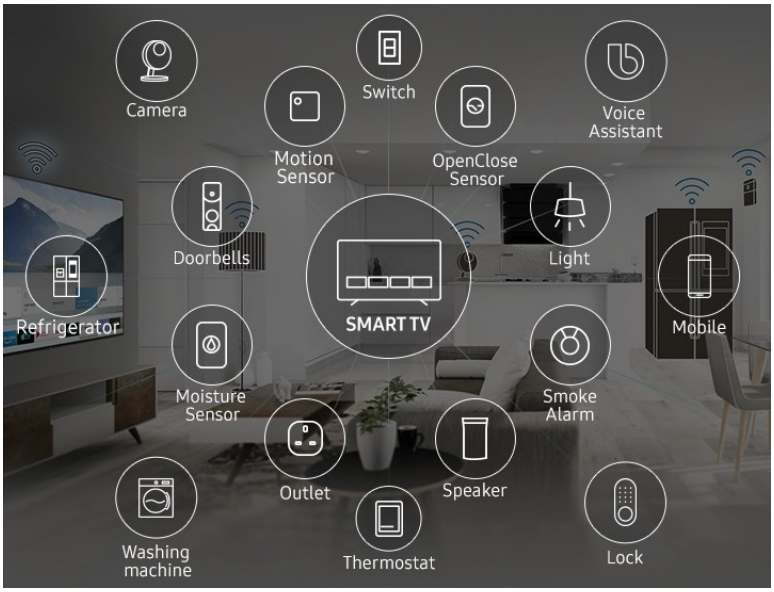
2.2.1 Aplicações Industriais

Esse é um dos domínios em que a IoT tem maior capacidade de expansão, assim como na qualidade do desenvolvimento dos produtos, tendo em vista a criticidade dos negócios e da necessidade de um maior retorno sobre o investimento em novas tecnologias. De acordo com a Hawlett Packard Enterprise (HPE), com a inclusão de dispositivos IoT na indústria, passou a existir a possibilidade de dimensionar os produtos em suas embalagens, oferecendo um melhor desempenho para a otimização de uso de matérias prima, redução de custos em processos e otimização de experiencias do cliente. Além disso, a utilização da IoT é capaz de otimizar a logística e cadeia de suprimentos, realizar gestão automática de inventário, realizar o controle de qualidade, prover segurança e proteção, e de forma mais completa digitalizar os processos industriais das plantas fabris.

2.2.2 Aplicações Residenciais (*Smart Home*)

De acordo com a Smarthome (2020), *Smart Home* é o termo utilizados para os dispositivos conectados com a Internet, usados para automatizar, monitorar e gerenciar as aplicações e sistemas residenciais. A Figura 3 mostra que os dispositivos mais comuns são: Sistemas de Iluminação, Sistemas de Câmeras, Sistemas de Segurança e Controle de Acesso, Sistemas de Entretenimento, *Smartphones,* Sistemas de Controle de Temperatura e Climatização, Eletrodomésticos e Sistemas de Irrigação.

Figura 3 - Casa inteligente com Dispositivos IoT

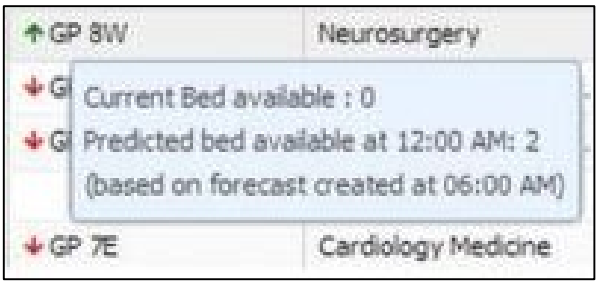


Fonte: Samsung (2020)

2.2.3 Saúde (*Healthcare*)

Além de melhorar os processos de negócios industriais, a IoT pode também salvar vidas. De acordo com uma publicação de Kim Gittleson (2013), o MT. Sinal Medical Center diminuiu o tempo de espera dos seus pacientes em torno de 50%. Isto foi devido a adoção de dispositivos IoT em colaboração com a empresa GE *Healthcare*, neste caso com uma solução conhecida como *AutoBed,* conforme interface gráfica mostrada na Figura 4, que é um algoritmo que monitora a ocupação de mais de 1000 unidades/leitos considerando cerca de 15 fatores diferentes.

Figura 4 – Interface gráfica do sistema Autobed.



Fonte: Kim Gittleson, BBC (2013)

Outros exemplos comuns de equipamentos de IoT para o ramo de *Healthcare* são os marcapassos e bombas de infusões de medicamentos.

2.2.4 Dispositivos Vestíveis

Os dispositivos vestíveis, também conhecidos como *wearables*, são os produtos de IoT mais comuns nos dias de hoje. Relógios, peças de roupas, pulseiras ou até mesmo óculos inteligentes tem se tornado cada vez mais presentes no nosso cotidiano. Esses dispositivos trabalham na maioria das vezes integrados aos smartphones, mas também possuem características de trabalhos individuais, que vão desde a integração de sensores de GPS, bem como o registro de atividades esportivas, monitoramento de batimentos cardíacos e quantidade de calorias.

Mas para que esses dispositivos sejam de fato conhecidos como wearables na definição de IoT, é necessário que estes dispositivos estejam conectados a outros aparelhos inteligentes ou à Internet.

2.2.5 Agricultura

A IoT está sendo utilizada na agricultura em diversas áreas, sendo que uma das técnicas aplicadas é conhecida como *Smart Greenhouse*, desenvolvida pela empresa Postscapes (2020). Essa técnica é utilizada para o cultivo em estufas, capaz

de aumentar o rendimento das culturas pelo controle de parâmetros ambientais. Além disso, essa técnica utiliza os dispositivos de IoT não apenas para o controle dos fatores climáticos, mas também, através de sensores, é permitido medir e controlar fatores de acordo com os requisitos de cada tipo de cultura, e de acordo com o processamento dos dados, é iniciado tomadas de decisões e definido ações para que outros mecanismos possam efetuar a colheita, rega ou distribuição de adubos e fertilizantes em pontos específicos do cultivo.

Outro uso que está sendo aplicado em larga escala, é a utilização da IoT em maquinários agrícolas pesados, como plantadeiras, colhedeiras, entre outros. Neste processo, os maquinários são operados remotamente por GPS [1](*Global Positioning System*) e permitem o controle total das ações e ambiente na qual os equipamentos estão trabalhando, assim como, os dados de terreno, rota, quantidade de produção (seja colheita ou plantio), níveis de combustível, estado de manutenção da frota de equipamentos, entre outros aspectos. Além disso, um único operador remoto pode controlar e monitorar diversos equipamentos através da utilização de pilotos automáticos providos pelos equipamentos e através da sincronização dos dados fornecidos pelo GPS e demais sensores instalados (VALTRA, 2020).

2.3 Perigos do crescimento exponencial da IoT

Por conta deste vasto campo que vem se abrindo no mundo da IoT, diversas companhias e startups vem se posicionando com o intuito de abraçar uma parte da fatia desse enorme mercado em desenvolvimento. Com isso, a criação de plataformas e *frameworks* diferentes ajudam os desenvolvedores de IoT a acelerar o processo de desenvolvimento dos produtos, na qual englobam diferentes bibliotecas já existentes.

Alguns dos mais populares frameworks utilizados, são: *Eclipse Kura, The Physical Web, IBM Cloud, Lelylan, Thing Speak, Bug Labs, The Thing System, Open Remote, OpenHAB, Eclipse* IoT*, Node-Red, Flogo, Kaa* IoT*, Macchina.io, Zetta, GE Predix, DeviceHive, Distributed Services Architecture, Open Connectivity Foundation*.

Essa é apenas uma fração da imensa quantidade de plataformas e *frameworks* populares que pode ser encontrada no mundo da IoT. Além disso, há também uma gama de protocolos sendo utilizados pelos fabricantes para suas soluções de IoT,

[1] GPS (*Global Positioning System*) é um sistema de rádio navegação que permite que seus usuários determinem e monitorem a exata localização e velocidade em tempo real de equipamentos, em quaisquer condições climáticas e em qualquer lugar no mundo.

sendo os mais comuns: *Wi-Fi, BLE, Cellular / Long Term Evaluation (LTE), ZigBee, ZWave, 6LoWPAN, LoRA, CoAP, SigFox, Neul, MQTT, AMQP, Thread, LoRaWAN*.

Embora a grande diversidade de plataformas e protocolos facilite muito a vida dos desenvolvedores e empresas, há uma outra perspectiva, normalmente negligenciada pela mentalidade dos desenvolvedores estarem utilizando ferramentas populares de mercado, que é o descuido na avaliação da segurança dessas estruturas. Existem muitas soluções e produtos comercializados hoje sob o rótulo IoT que não possuem arquiteturas básicas e imaturas de segurança, e por consequência disso, não somente os dispositivos residenciais estão sob risco, mas também todos os equipamentos que trabalham para automatização de edifícios, carros, ônibus, aeroportos, serviços de saúde, aplicações de logística e de industrias ficam vulneráveis a ataques (WAHER, 2015), e para tanto se torna necessário criar contramedidas para proteger suas soluções de IoT.

Várias empresas e residências já conviveram com ataques de *crackers* e *softwares* com intuitos maliciosos desde o surgimento das primeiras páginas da web, e por isso a comunidade tecnológica deve se preocupar ainda mais com o desenvolvimento de produtos para uso em IoT, impedindo que criminosos possam tentar invadir e tomar o controle de possíveis dispositivos vulneráveis conectados à Internet.

Por consequência do rápido crescimento dos dispositivos IoT no mercado, Balaguer (2015), diz que houve um aumento na disseminação de vulnerabilidades e ameaças para todos os tipos de *hardwares* e *softwares*, e por isso, a segurança da informação nestes dispositivos deve ser mantida entre as principais prioridades de melhorias da indústria da tecnologia de dispositivos IoT. Por sua vez, Maressa Urbano (2017), complementa que as vulnerabilidades a ataques chegam também as empresas:

> “[...] Como milhões de novos dispositivos passam a estar conectados, é inevitável que algumas pessoas levem seu gadgets para o ambiente de trabalho. Caso se conectem à rede da empresa, é natural que aquele objeto passe a ser mais um *endpoint*, ou seja, mais uma porta de entrada para vírus e malwares”.

Portanto, proteger a Internet das Coisas será uma tarefa complexa e difícil, tendo em vista que, sua população estimada em bilhões de objetos, que irão interagir uns com os outros e com outras entidades, como seres humanos ou entidades virtuais, criam muitas possibilidades de ataques disponíveis à pessoas mal-intencionadas,

ataque a vários canais de comunicações, ameaças físicas, negação de serviço, fabricação de identidade entre outras (BABAR; MAHALLE, 2010).

3 SEGURANÇA DA INFORMAÇÃO

A SI (Segurança da Informação) é um dos temas mais abordados e estudados dentro dos processos para gestão de TI (Tecnologia da Informação) das organizações e da comunidade tecnológica.

Para Peixoto (2006), o termo Segurança da Informação é a definição de uma área do conhecimento que protege os chamados ativos da informação contra possíveis acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade.

De forma mais ampla, o termo Segurança da Informação abrange todas as políticas, procedimentos e metodologias técnicas e operacionais que são usadas para impedir acessos não autorizados, alterações, roubos ou danos físicos a equipamentos ou sistemas de informação. Ela pode ser composta por um conjunto de técnicas e ferramentas, destinadas a salvaguardar *hardwares*, *softwares*, redes de comunicação, informações e dados. (LAUDON; LAUDON, 2004)

Fontes (2010), de maneira simplista e objetiva, define o significado de Segurança da Informação:

> "[...] Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada".

Diante disso, propor modelos e novos estudos de melhorias e modernização dos processos de segurança da informação é fundamental, principalmente enxergando o crescimento da transmissão de dados devido a produção de novos dispositivos interconectados, do desenvolvimento de novas tecnologias de computação (por exemplo a computação quântica e computação em nuvem), e também da necessidade de proteção dos dados de uma forma geral.

3.1 Pilares de Segurança da Informação

A Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização (ROSA, 2010).

Segundo a Norma ISO 27001 (ABNT, 2006), que gerencia a segurança da informação no mundo, a "Segurança da Informação é a proteção da informação de

vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

> "Nenhuma área da informática é tão vasta e apreciada como a segurança da informação; o ponto principal da segurança leva a um ponto principal, o ser humano, todo o processo de segurança inicia e tem seu término em um ser humano. Não adianta nada gastarmos fortunas em equipamentos e sistemas de segurança se não conhecermos quem utilizará nossos sistemas, e quem pode ter acesso a eles mesmos sem autorização" (OLIVEIRA, 2001, p. 3).

Os principais pilares da segurança da informação, de acordo com a NBR ISO/IEC 27002 (ABNT, 2005) está definida em três princípios básicos. Também conhecidos como CID, esses princípios visam propor Confidencialidade (C), Integridade (I) é Disponibilidade (D) para toda a infraestrutura, aplicações e dispositivos. A definição de cada um dos pilares, pode ser dada como:

3.1.1 Confidencialidade

A confidencialidade dos dados significa que somente os receptores desejados e autorizados poderão acessar e ler os dados. Para Campos (2007), a quebra da Confidencialidade é:

> "[...] Quando uma informação é acessada por pessoa não autorizada, intencionalmente ou não, seja pela descoberta de uma senha, pelo acesso a documentos ou de qualquer outro modo, então isto é um incidente de Segurança da Informação por quebra de confidencialidade".

3.1.2 Integridade

Integridade dos dados significa ter a certeza de que a informação não é alterada durante a transmissão da origem ao destino. Para Campos (2007), a quebra da Integridade é:

> "[...] Quando uma informação é indevidamente alterada, intencionalmente ou não, tal como pela falsificação de um documento, da alteração de registros em um banco de dados, ou qualquer coisa que altere a informação original de maneira indevida, configura um incidente de Segurança da Informação por quebra de integridade".

3.1.3 Disponibilidade

Disponibilidade de dados significa assegurar o acesso confiável e no tempo certo a serviços de dados para usuários autorizados. Para Campos (2007), a quebra da Disponibilidade é:

> “[...] Quando a informação não é acessível nem mesmo por quem é de direito, como no caso da perda de documentos, quando há sistemas de computador “fora do ar” ou, ainda, em função de ataques de negação de serviço a servidores de rede ou servidores Web, ou seja, quando esses servidores estão inoperantes em resultado de ataques e invasões, então isto é um incidente de Segurança da Informação por quebra de disponibilidade. Mesmo as “quedas” de sistemas não provocadas, ou seja, não intencionais, configuram quebra de disponibilidade”.

3.2 Vulnerabilidades

No contesto de SI, a vulnerabilidade é classificada como pontos fracos ou falhos na qual podem ser explorados por uma ameaça, interna ou externa, para obter acesso a um ativo.

Para exemplificar o contexto de ativo, pode-se entender que, ativos são as pessoas (funcionários, clientes, visitantes, convidados), propriedades intelectuais, projetos, desenhos, máquinas, equipamentos de informática, sensores, celulares, informações (*softwares*, banco de dados, arquivos e registros) e até a reputação e imagem que é atribuída para uso no cotidiano de uma empresa.

Oliveira (2018), classifica as vulnerabilidades como, quaisquer características de fraqueza de um ativo da informação. Ou seja, características de modificação e de captação na qual os bens, ativos, ou recursos intangíveis de informática, respectivamente, softwares, ou programas de bancos de dados, ou informações, ou ainda a imagem corporativa ou pessoal, podem ser alvos de um possível ataque. De forma sucinta, é a fragilidade que um ativo de informação por ser explorado por uma ameaçam para que um ataque possa ser concretizado.

3.3 Ameaças

No contesto de SI, ameaças todas as coisas que podem explorar as vulnerabilidades, de forma intencional ou acidental, e geralmente ela vai obter acesso ao ativo com o intuído de danificar, destruir, ou fazer uso destes ativos para obtenção de informações de forma não autorizada.

> “A ameaça pode ser definida como qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e consequentemente gerando um determinado impacto. As ameaças apenas existem se houverem vulnerabilidades, sozinhas pouco fazem” (LAUREANO, 2005, p. 15).

Segundo Oliveira (2018), ameaças são eventos ou atitudes indesejáveis que potencialmente remove, desabilitam, danificam ou destroem um ativo de informação.

A ameaça pode ser também a expectativa de acontecimentos acidentais ou propositais, causada por um agente que pode afetar um ambiente, sistema ou ativo de informação.

Para Sêmola (2014), as ameaças podem ser dos tipos:

- **Involuntárias**: São as ameaças inconscientes, quase sempre causadas por desconhecimento, descuido ou negligência. Podem ser causadas, por exemplo, por acidentes, erros ou falta de energia.
- **Voluntárias**: Ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.
- **Naturais**: Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremoto, aquecimento, poluição, entre outros fatores climáticos.

3.4 Principais causas de quebra de Segurança da Informação

Dentre as principais causas de quebra de segurança da informação, enquadra-se: as pessoas, os engenheiros sociais ou *crackers,* os ataques e os códigos maliciosos (*malwares*).

3.4.1 Pessoas

Segundo pesquisa da PWC (2018), foi constatado a principal causa de incidentes de segurança da informação são as pessoas dentro das organizações. Sendo destas causas, cerca de 30% dos funcionários atuais e cerca de 28% de ex-funcionários das organizações. Neste caso, normalmente essas pessoas não respeitam as normas e políticas de segurança ou não está contente com a companhia e vai de alguma forma causar algum dano aos ativos da companhia. Essas pessoas de certa forma estão imunes aos mecanismos de segurança, tendo em vista que eles possuem conhecimentos quanto aos possíveis pontos de fraqueza que a empresa possui, facilitando a sua ação e potencializando os danos que podem ser causados à empresa.

3.4.2 Engenheiros Sociais

Também são pessoas, mas normalmente externas às organizações. Esses, da mesma forma, conhecidos como *hackers* do mal ou *crackers*, buscam utilizar dos seus

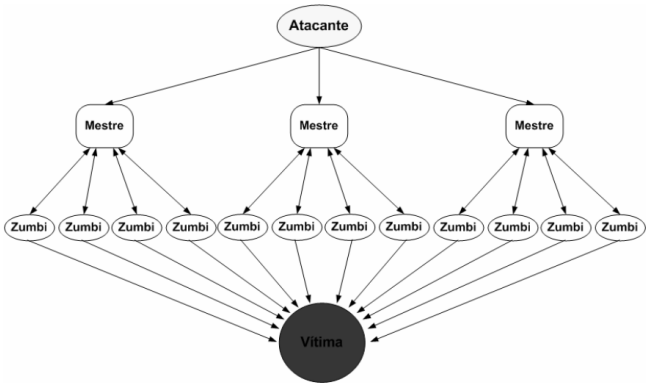
conhecimentos para detectar, ampliar falhas e explorar as vulnerabilidades emocionais e ignorância das pessoas, ou sistemas e serviços mal configurados e expostos à rede mundial de Internet, com o intuído de obter, danificar ou destruir um ativo do alvo que será explorado.

3.4.3 Ataques

Dentre os principais ataques cita-se: Negação de Serviços (DoS/DDoS), *Phishing*, *Pharming*, *Spoofing*, *Snnifing*,

a. Negação de Serviços (DoS/DDoS): Segundo a Avast (2020), o ataque de Negação de Serviços (*DoS – Denial of Service*) ou ataque Distribuído de Negação de Serviços (*DDoS – Distributed Denial of Service*), são formas de tentativas mal-intencionadas de sobrecarregar um serviço, servidor ou rede. O *DOS/DDOS* atua com o intuito de causar lentidão ou a interrupção da conexão do alvo do ataque. De forma simples, esse tipo de ataque causa um engarrafamento da rede alvo, na qual esse alvo passa a receber uma quantidade de dados superior ao que consegue processar, e por isso, os seus serviços começam a não mais responder, e passam a ser negados. Esses ataques utilizam uma grande quantidade de tráfego da Internet, normalmente obtidos através da infecção de vários sistemas ou redes de computadores invadidos e comprometidos, e através desses, o atacante consegue redirecionar o tráfego de dados para atingir um alvo em específico ou a infraestrutura ao seu redor. A diferença entre *Denial of Service* (DoS) e *Distributed Denial of Service* (DDoS), é que, enquanto o DDoS utiliza a distribuição em diversas máquinas para realizar o ataque, o DoS se concentra em apenas uma máquina atacante para envio dos pacotes de dados pela Internet. A Figura 6 a seguir, demostra a estrutura de um ataque de negação de serviço distribuído (DDoS).

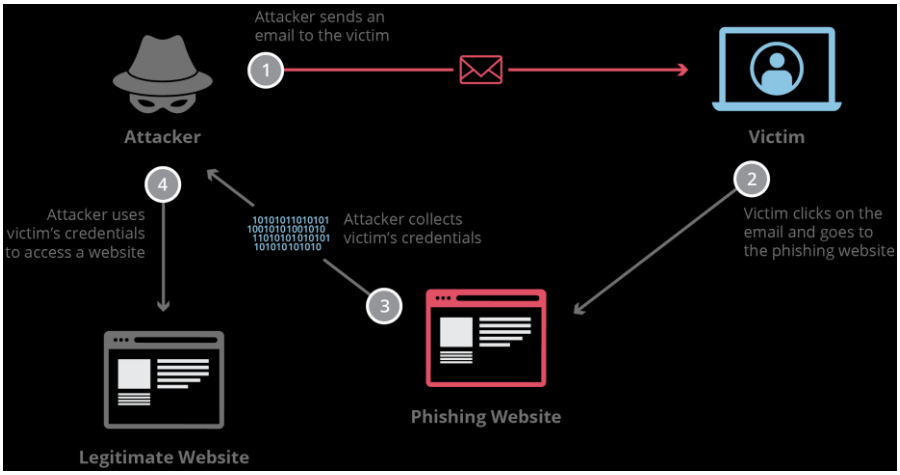
Figura 3 - Estrutura de um ataque de negação de serviço distribuído



Fonte: Researchgate (2020)

b. ***Phishing***: Segundo a Avast (2020), *phishing* e uma forma de ataque que enganam pessoas com o intuído de roubar dados sensíveis, como senhas e números de CPF, números de cartões de créditos, entre outros. A forma mais comum do ataque de *phishing* e através de iscas enviada via *e-mail*, ou seja, o atacante envia um *e-mail* com uma mensagem de texto que imita uma pessoa ou uma organização na qual a pessoa possui alguma relação de confiança, como por exemplo, um amigo, um banco, ou algum órgão do governo. A partir do momento que a vítima acessa o *e-mail*, ela encontrara uma mensagem para amedrontá-la ou informando que alguma ação muito importante precisa ser tomada, e que para acessar o conteúdo detalhado das informações ela precisa clicar em um *link*, em uma imagem no corpo da mensagem, ou em um arquivo que esteja anexo ao *e-mail*. Ambos as opções irão exigir que a vítima tome alguma ação, seja acessar um *site*, clicar em um *link* ou arquivo, para que o ataque seja efetivado. A partir do momento em que a vítima cai na armadilha e acessa as opções do atacante, o atacante consegue ter acesso ou instalar algum outro *software* malicioso na máquina da vítima. A Figura 7 demostra a estrutura de um ataque de *Phishing*.

Figura 4 - Estrutura de um ataque de Phishing

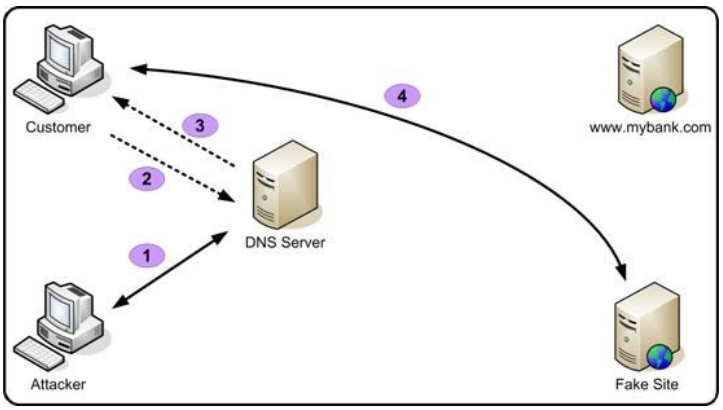


Fonte: Cloudflare (2020)

c. ***Pharming***: Segundo a Avast (2020), se você já acessou a sua conta bancária online, percebeu que as suas informações estavam comprometidas e que seu dinheiro foi roubado, provavelmente você foi vítima de um ataque do tipo *pharming*. Uma das táticas do ataque de *pharming* é da clonagem do tráfego de *sites* legítimos encaminhando os usuários para *sites* falsos. Esse processo de clonagem e falsificação é realizado normalmente através do envenenamento do sistema de nomes de domínios (DNS *poisoning*), na qual um criminoso ao conseguir acessar e

comprometer as tabelas e arquivos de configuração dos servidores do sistema de nomes de domínio, modifica os dados destes documentos, resultando no direcionamento dos usuários para *sites* maliciosos ao invés dos *sites* legítimos. Assim, quando o usuário digita seus dados, como por exemplo, dados de cartão de crédito, CPF, informações bancárias ou senhas nestes sites fraudulentos, os usuários têm suas informações e identidades roubadas como resultado do ataque. A Figura 8 abaixo, demostra a estrutura de um ataque do tipo *Pharming*.

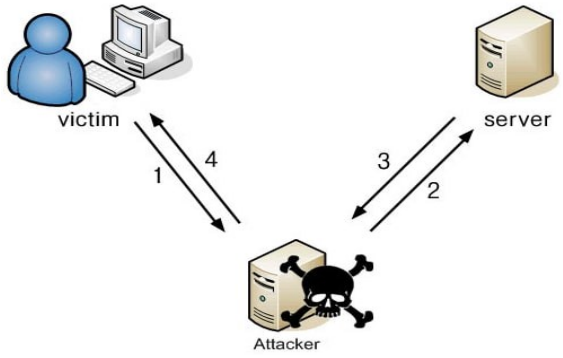
Figura 5 - Estrutura de um ataque de Pharming



Fonte: Technical Info (2020)

d. ***Spoofing***: Segundo a Avast (2020), a técnica de *spoofing* é realizada para enganar dispositivos, usuários ou sistemas de computadores, através da ocultação ou falsificação da identidade destes elementos, seja do endereço MAC (*Midea Access Control Address*), dos endereçoes de *e-mail* de um usuário ou dos dados de *login* dos sistemas de computadores. Embora a Internet seja um local de fácil acesso e ótimo para se comunicar com outras pessoas, é também um local que facilita muito a falsificação de identidades. Outra técnica de *spoofing* muito realizada é a falsificação de endereços IP (*Internet Protocol*), e com isso é possível mascarar o endereço de IP de um determinado dispositivo, tornando muito difícil a identificação por parte de outros dispositivos a origem da transferência dos dados enviados a eles. A Figura 9 demostra a estrutura de um ataque do tipo *Spoofing*.

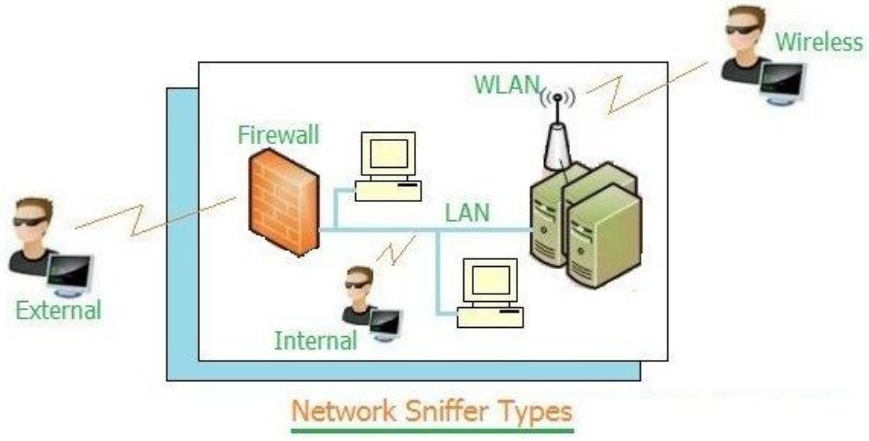
Figura 6 - Estrutura de um ataque de Spoofing



Fonte: Springboard (2018)

e. ***Snnifing***: Segundo a Avast (2020), o ataque do tipo *snnifing* utilizam de softwares chamados de *snnifers* para captura do tráfego de dados que entra e sai de um determinado dispositivo ou da rede que este dispositivo está conectado. Essa técnica normalmente é utilizada pelos administradores de redes para diagnosticar problemas ou detectar falhas de segurança em sua rede. No entanto, essa técnica também pode ser utilizada por criminosos para obterem informações como, senhas e usuários, ou mensagens que estão sendo transmitidas na rede sem mecanismos de criptografia, a assim os criminosos podem capturar essas mensagens e ganhar acesso aos dispositivos e sistemas conectados na rede através das senhas e dos usuários capturados. A Figura 10 demostra os tipos de ataques de rede que podem ser realizados com *Snnifers*.

Figura 7 - Tipos de ataques com Snnifers de Rede



Fonte: RF Wireless World (2012)

3.4.4 Códigos Maliciosos (Malwares)

Segundo o CERT.br (2020), o *malware*, ou *malicious softwares*, é um termo geral utilizado para todos os tipos de códigos maliciosos, na qual os atacantes podem

utiliza-los para enfraquecer, destruir ou ganhar acesso aos dados e informações de um ativo.

A Kapersky (2019), define os códigos maliciosos como:

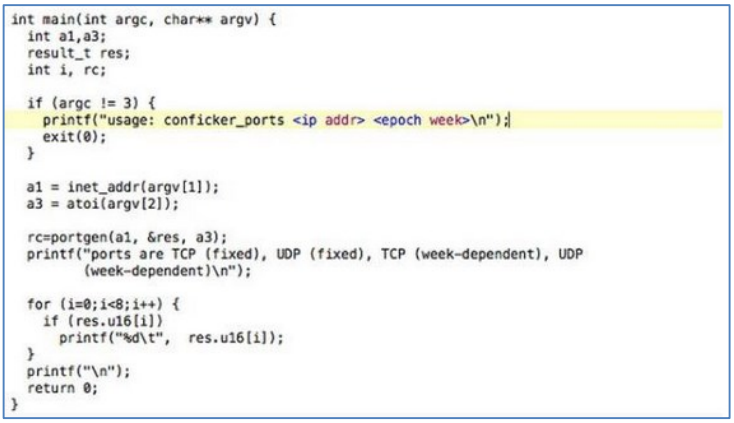
> “Código malicioso é um tipo de código de computador ou script da Web nocivo que tem como objetivo criar vulnerabilidades no sistema, gerando *backdoors*, violações de segurança, roubo de dados e informações, além de outros danos possíveis em sistemas de arquivos e computadores. É um tipo de ameaça que o software antivírus pode não conseguir bloquear sozinho. De acordo com a Kaspersky Lab, nem todas as proteções antivírus conseguem lidar com determinadas infecções causadas por código malicioso, que é diferente de malware. Malware se refere especificamente a software malicioso, mas código malicioso inclui scripts de sites que podem explorar vulnerabilidades para fazer upload de malware”.

Há muitos tipos e diferentes formas que uma *malware* pode infectar um alvo, seja através da conexão destes computadores com páginas da *web*, *e-mails*, *links* e documentos infectados, ou também pela instalação destes códigos de forma manual pelos próprios atacantes, uma vez que eles consigam ganhar acesso físico aos ativos.

Uma vez esses códigos instalados nos ativos, eles podem corromper, copiar, ou alterar as informações de um ativo, além também de serem capazes de se propagarem dentro de uma rede de ativos interconectados, tudo isso dependendo das condições na qual foram programados para serem executados. Os tipos mais comuns de *malwares* são: Vírus, *Worms*, Cavalo de Tróia (*Trojan Horse*), *Spyware*, *Backdoor*, *Rootkit*, *Ransomware*.

a. **Vírus**: São fragmentos de códigos de computadores, que os inserem dentro de outros programas hospedeiros, forçando os programas hospedeiros quando executados a tomar ações maliciosas e compartilharem esses fragmentos maliciosos entre outros programas. Os vírus normalmente são propagados em *e-mails*, *scripts*, macros, redes *bluetooth* e mensagens de textos de celulares. A Figura 11 demostra o código fonte do vírus Conficker.

Figura 8 - Código fonte do Vírus Conficker (2008)



```
int main(int argc, char** argv) {
  int a1,a3;
  result_t res;
  int i, rc;

  if (argc != 3) {
    printf("usage: conficker_ports <ip addr> <epoch week>\n");
    exit(0);
  }

  a1 = inet_addr(argv[1]);
  a3 = atoi(argv[2]);

  rc=portgen(a1, &res, a3);
  printf("ports are TCP (fixed), UDP (fixed), TCP (week-dependent), UDP
         (week-dependent)\n");

  for (i=0;i<8;i++) {
    if (res.u16[i])
      printf("%d\t",  res.u16[i]);
  }
  printf("\n");
  return 0;
}
```

Fonte: Nagy, 2013.

b. ***Worms***: São fragmentos de softwares maliciosos que se reproduzem e se espalham sozinhos de computador para computador. Segundo o CERT.br (2020), diferente do vírus, o *worm* não precisa ser executado por um programa hospedeiro, mas sim pela execução direta de suas próprias cópias ou através de vulnerabilidades encontradas nos ativos dentro de uma rede de computadores. A Figura 12 demostra um alerta de worm encontrado detectado por um programa *antispyware* em um *e-mail*.

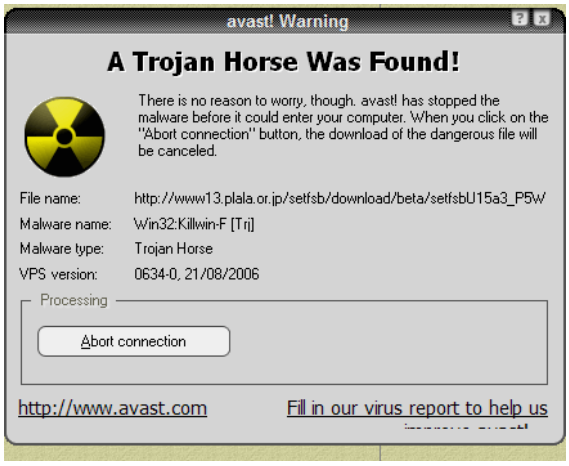
Figura 9 - Alerta de Worm em e-mail.

Fonte: Security-Wire (2010)

c. **Cavalo de Troia (*Trojan Horse*)**: Esse tipo de *malware* não se reproduz ou executa suas finalidades sozinhos. Normalmente esse *software* é instalado e mascarado em outros programas, arquivos baixados ou arquivos recebidos pela Internet. Esse tipo de *malware* executa suas funções somente quando o programa mascarado é de fato executado pelo usuário, podendo então fazer *download* de novos programas, criar uma *backdoor*, apagar, alterar, copiar, coletar e espionar os dados

dos ativos em que ele foi executado. A Figura 13 demostra um alerta de cavalo de troia detectado por um programa de antivírus em um arquivo.

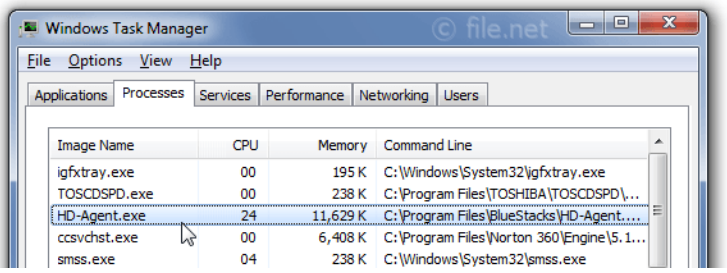
Figura 10 - Cavalo de Troia baixado pela Internet



Fonte: Alves (2017)

d. ***Spyware***: São *softwares* maliciosos usados com a finalidade de obter dados de forma que o usuário não tenha nenhuma suspeita. Ou seja, ele possibilita a espionagem do comportamento, do uso dos recursos computacionais, do envio e recebimento de arquivos, além de compartilhar todas essas informações com o atacante. *Keyloggers* são exemplos específicos de *spywares* que gravam o que foi digitado no teclado do alvo afetado, como por exemplo usuários e senhas, e compartilham esses dados com o atacante. A Figura 14 demonstra um spyware camuflado em um processo detectado no gerenciador de tarefas do sistema operacional Windows.

Figura 11 - Spyware em computador infectado.

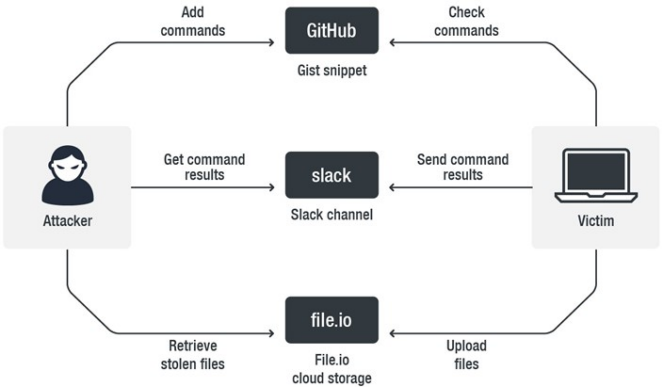


Fonte: File.net (2020)

e. ***Backdoor***: É um tipo de *malware* que é usado para abrir uma “porta dos fundos” no equipamento que foi previamente afetado por um outro tipo de *malware* ou pela exploração de falhas em *softwares* ou aplicações instaladas que estejam vulneráveis. A sua função é garantir que o atacante possa futuramente retornar a invadir o

computador comprometido, permitindo uma conexão através de acesso remoto, sem que seja necessário um novo ataque com métodos de invasão ou infecção que foram utilizados para comprometer o equipamento da primeira vez. A Figura 15 demonstra o fluxo de trabalho de um backdoor que atingiu as aplicações GitHub e Slack.

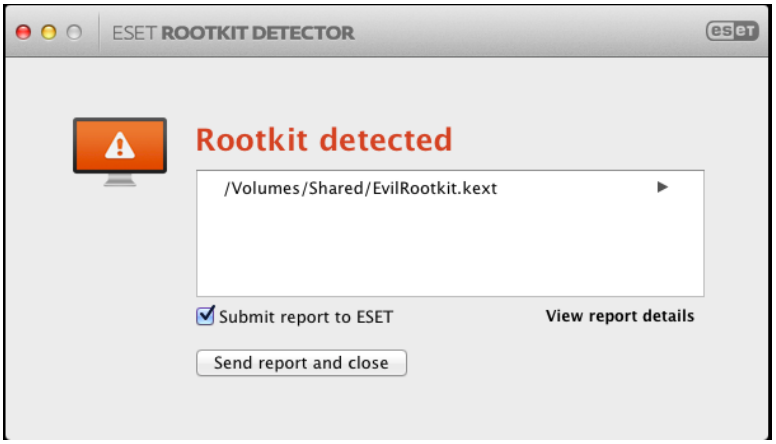
Figura 12 - Workflow de um Backdoor que atingiu o GitHub e Slack



Fonte: Tecmundo (2019)

f. Rootkit: É um tipo de *malware* que permite *crackers* criarem *backdoors* a ganharem acesso completo, inclusive com privilégios administrativos, em computadores ou em redes de computadores. Ele tem uma grande capacidade de camuflagem, pois se escondem de *softwares* de segurança, ocultando suas chaves de registro (CARVALHAL, 2012). Além desse *malware* afetar *softwares* e sistemas operacionais, eles podem também afetar os *hardwares* e *firmwares* de recursos computacionais, e por conta disso consegue realizar diversas ações maliciosas, como por exemplo o envio de *spams* para outros usuários ou utilização do dispositivo afetado para realização de ataques “DoS” (SANTOS DIAS, 2013*).* A Figura 16 demonstra um alerta de *Rootkit* detectado por um programa de detecção de *Rootkits*.

Figura 13 - Alerta de Rootkit



Fonte: Léveillé (2013)

g. Ransomware: São tipos de *malwares* utilizados para sequestrar parte ou todo o sistema de arquivos da vítima. Esse tipo de código malicioso, além de sequestrar, pode também utilizar técnicas de criptografia para criptografar os dados e exigir uma taxa de resgate para que a vítima volte a acessar a esses dados. Esse tipo de *ransomware* com a utilização de técnicas de criptografia é conhecido como *crypto-ransomware*. Os criminosos para devolverem os dados sequestrados exigem uma taxa de resgate, que pode ser o fornecimento de senhas ou de dinheiro, normalmente em moedas virtuais, como o *bitcoin* (NOVAES, 2014). Segundo a Trend Micro (2016);

> "[...] A maneira mais simples de descrever o ransomware é que ele é uma ameaça online que pode deixar os arquivos e/ou sistemas de sua empresa completamente inúteis. A vítima é então forçada a pagar um resgate para recuperar o acesso. As primeiras versões de ransomware foram feitas para bloquear a máquina da vítima até que o pagamento fosse feito. Mas, o mais perigoso nessa nova classe do assim chamado "crypto-ransomware" é que ele irá buscar extensões de arquivos específicos (muitas vezes comuns) como .doc ou .pdf, inutilizando-os com uma criptografia forte. Isso deixa os chefes de TI com poucas opções a não ser pagar por uma chave de decodificação."

A Figura 17 demonstra a tela de um computador infectado pelo ransomware FBI.

Figura 14 - Tela de computador infectado pelo ransomware FBI

Fonte: Defesanet (2012)

4 RANSOMWARES

Como citado no parágrafo anterior, *ransomware* é um termo que descreve um conjunto de malwares que tem como finalidade o bloqueio de dispositivos, captura e criptografia de informações e principalmente a extorsão digital das vítimas que tiveram seus dispositivos infectados por esse *software* malicioso.

4.1 Tipos de ransomware

O *ransomware* pode ser dividido em duas categorias segundo CERT.br (2020), os *ransonware* pode ser classificado como *Locker e Crypto.*

4.1.1 Ransomware Locker:

Esse tipo de ransomware, que costuma ser menos complexo, mas que não necessariamente é mais fácil de mitigar, realiza a criptografia de um conjunto de arquivos importantes, e desta forma bloqueiam e impedem o acesso do usuário ao dispositivo ou sistema infectado.

4.1.2 Ransonware Crypto:

Esse é o tipo de *ransomware* mais comum atualmente. O *ransomware crypto* também utiliza de mecanismos de criptografia, mas apenas para encriptar e impedir o acesso aos dados e arquivos do dispositivo infectado. Dessa forma, para acessar os arquivos é necessária uma chave criptográfica, que fica em posse dos criminosos. Os criminosos utilizam esta técnica como uma forma de extorsão para cobrar um valor, normalmente em bitcoins, para entregar a chave e permitir as vítimas decriptar e recuperar os arquivos. Outro ponto crítico, é que mesmo que a vítima tente abrir esse arquivo em outro sistema operacional, o arquivo continuará criptografado, e portanto ainda haverá a necessidade da chave criptográfica para liberar o acesso aos arquivos, forçando assim as vítimas a pagarem o resgate, caso não tenham nenhum tipo de mecanismo de backup com uma cópia destes arquivos.

4.2 Formas de infecção

Os ransonwares normalmente são distribuídos por técnicas de engenharia social, na qual se utilizam de ataques do tipo phishing para propagar arquivos maliciosos ocultos em links de páginas da Internet ou anexo a e-mails. No entanto, conforme observado na cartilha de segurança do CERT.br (2020), os ramsonware

podem também se espalhar através da exploração de vulnerabilidades em sistemas de informação e dispositivos que não tenham ou que não estejam com suas barreiras de segurança corretamente configuradas e atualizadas.

4.3 Ransonwares mais conhecidos

Alguns dos *ransomwares* mais conhecidos, são: Locky, WannaCry, BadRabit e Petya.

4.3.1 Locky

Segundo a Kapersky (2020), esse *ransomware* ficou conhecido por este nome, devido a extensão dos arquivos encriptados serem “.locky”. Esse ransomware era transmitido principalmente usando técnicas de engenharia social, na qual os criminosos enviavam e-mails de phishing para as vítimas, e quando a vítima abre e executa o link ou arquivo anexo ao e-mail são infectadas. Teve suas primeiras aparências em 2016, e se espalhou rapidamente por algumas regiões do mundo, incluindo a América do Norte, Europa e Asia. Pesquisas indicam que os valores cobrados pelas chaves variam entre e, dependendo da quantidade de arquivos afetados.

4.3.2 WannaCry

Segundo a Kapersky (2020), esse *ransomware* ficou conhecido mundialmente depois de infectar mais de 230 mil computadores com o sistema operacional Windows em mais de 150 países em um único dia. Esse *ransonware* foi distribuído em larga escala devido a exploração de uma vulnerabilidade no sistema operacional Windows referenciada como MS17-010. Os criminosos cobravam 300 dólares convertido em bitcoin como resgate para cada dispositivo infectado. Estima-se que a origem desse *ransonware* seja a Coreia do Norte.

4.3.3 BadRabit

Segundo a Kapersky (2020), esse ransomware ficou conhecido mundialmente em 2017, após ser detectado inicialmente na Rússia e Ucrânia. Afetou o aeroporto ucraniano de Odessa, agências de meio de comunicação da Rússia e o sistema de metrô em Kiev, na Ucrânia. No Brasil, o BadRabbit também foi detectado em empresas do setor de comunicação e de outras áreas. Esse *ransonware* foi distribuído

através de um falso instalador do software Adobe Flash Player, portanto, quando as vítimas baixavam o instalador e executavam o arquivo de instalação, os seus computadores eram infectados. Os criminosos cobravam 280 dólares, convertidos em bitcoin, como resgate para cada dispositivo infectado.

4.3.4 Petya

Segundo a Kapersky (2020), o Petya se tornou um dos principais assuntos tratados em segurança cibernética em 2017. Ele foi detectado inicialmente na Ucrânia, antes de ser detectado também na Europa e Estados Unidos. O Petya se espalhou através de anexos de e-mails maliciosos, que quando baixados e executados manualmente, infecta o computador da vítima e criptografa a tabela de arquivos mestre (MFT), que é o guia de onde os arquivos ficam salvos no HD, e sem acesso ao MFT o computador não consegue encontrar nenhum arquivo.

4.4 Legislação

Devido o *ramsonware* ser uma técnica disseminada mundialmente a pouco tempo, esse tipo de ataque não está tipificado em leis, com exceção do Código Penal do Texas, que possui a Seção 33.023, em vigor desde 1 de janeiro de 2017, para tratar exclusivamente sobre o termo *ransomware* (TEXAS, 2017).

No entanto, MASSENO e WENDT (2017), definem que:

> “Assim, no que se refere a Portugal, temos à disposição o Código Penal (de 1995, com múltiplas atualizações), a Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro) e, também, a Lei da Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de outubro). A este propósito, é necessário ter em atenção que, desde a Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de agosto), o conteúdo do Direito português resulta essencialmente da aplicação ou transposição de Instrumentos Normativos de origem europeia, os quais relevam também para a interpretação das Leis nacionais. Nomeadamente, nos importam a Convenção do Conselho da Europa sobre o Cibercrime, adotada em Budapeste, a 23 de novembro de 2001, e a Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa aos ataques contra os sistemas de informação.”

Além disso, no que se diz respeito a legislação brasileira, MASSENO e WENDT (2017) também definem que:

> “Por seu turno, no Brasil as fontes têm evoluído mais lentamente e com uma influência externa apenas indireta, pelo que podemos encontrar apoios no Código Penal (de 1942), tal como alterado pela Lei Carolina Dieckmann (Lei 12.737/2012, de 30 de novembro). O Brasil não é signatário da Convenção do Conselho da Europa sobre o

Cibercrime, denominada de Convenção de Budapeste, apesar de a mesma estar aberta à adesão de outros países e de, na América Latina, tal já ser o caso do Chile, do Panamá e da República Dominicana, enquanto os Estados Unidos, o Canadá, o Japão e a República da África do Sul participaram mesmo na negociação da Convenção."

5 INTERNET DAS COISAS E RANSOMWARES

Levando em conta os dados da Sonicwall (2019), em seu Relatório de Ameaças Cibernéticas, o *ransomware* se tornou um dos mais preocupantes ataques cibernéticos dos últimos anos, principalmente com relação aos dispositivos IoT, uma vez que, nesses dispositivos os criminosos não se preocupam somente com o sequestro de dados e informações, mas também simplesmente programar esse tipo de *malware* para bloquear ou obter controle completo sobre os dispositivos vulneráveis, podendo desta forma afetar redes inteiras de dispositivos IoT. Foi observado também, um aumento de 55% em ataques de dispositivos IoT. Esses dados foram baseados na análise de cerca de 1 milhão de sensores espalhados por mais de 200 países e o número de ataques já superam os dois primeiros trimestres de 2018.

Hoje, usuários domésticos, governos e grandes corporações estão tentando se proteger de todos os tipos de *malwares*. Contudo, ainda se ignora esses tipos de ataques na nova onda tecnológica de dispositivos IoT e isso pode ser muito perigoso dado à quantidade e diversidade dos dispositivos que vem sendo desenvolvidos. Além do mais, deve-se levar em conta que IoT *ransomware* possui aspectos e objetivos diferentes dos *ransomware* tradicionais.

5.1 O crescimento de dispositivos IoT afetados por ransomwares

Como os consumidores e empresas continuam comprando e conectando os dispositivos na Internet, geralmente sem medidas básicas de segurança, os criminosos virtuais cada vez mais podem ser aproveitar e distribuir esse tipo de *malware* pela Internet.

Segundo o levantamento da Sonicwall (2019), os dispositivos de IoT têm sido cada vez mais aproveitados pelos criminosos virtuais para distribuir *payloads* (código malicioso com forte capacidade de destruição). Além disso para aumentar a eficácia do ataque, os criminosos estão separando o *payload* do vetor de infecção (credencias padrão, exploração conhecidas de vulnerabilidades de serviços e protocolos, entre outros). Com isso, evita-se a detecção e facilita-se a disseminação do *malware*.

O presidente da TrendMicro, Willian Malic (2018), em uma entrevista à revista eletrônica Olhar Digital, esclarece que a Internet das Coisas foi desenhada com dois princípios. O primeiro seria a segurança física, ou seja, se um dispositivo falhar ele

não irá comprometer a vida ou o bem estar das pessoas. O segundo seria a disponibilidade, ou seja, se um dispositivo falhar o restante dos recursos poderão seguir em uso. Contudo, nesses princípios não há nenhuma definição relacionada a segurança da informação, que é o ponto mais sensível da Internet das Coisas atualmente. Malic, ressalta ainda que:

> "A mentalidade de um engenheiro industrial é muito diferente da de um especialista em segurança da informação. São duas culturas diferentes. Fora isso, ainda há o problema dos usuários – que não estão exatamente habituados com todos os recursos que um aparelho conectado à internet pode trazer. Nós continuamos adotando novos produtos sem entender as implicações deles, as pessoas instalam as tecnologias e não têm ideia do que elas fazem"

Os dispositivos de IoT, possuem características e arquiteturas bastante diferentes dos computadores, servidores e recursos computacionais que a maioria dos usuários costumam utilizar. Ainda que, uma característica comum seja o uso do Wi-Fi, normalmente não existe grande poder de processamento ou uma interface de controle do usuário diretamente com o dispositivo. Em concordância disso, Palmer (2018), faz a seguinte colocação:

> "Embora os dispositivos de IoT tenham muito menos poder de processamento que até mesmo os mais básicos PCs, eles trazem as vantagens – para os hackers – de, primeiro, raramente ter um sistema de cibersegurança adequado e, segundo, os usuários não darem muita atenção a eles, geralmente instalando os dispositivos e não mais pensando neles depois"

Segundo um estudo da revista Convergência Digital (2018), não é difícil quebrar a segurança de um dispositivo IoT, principalmente levando em consideração que os usuários normalmente não trocam as senhas padrão dos dispositivos, o que leva a massiva tentativa do ataque de força bruta nesses dispositivos, que é usado em cerca de 93% dos ataques detectados. Além disso, também há o agravante dos usuários não saberem exatamente como o equipamento se comporta quando conectado à Internet, trazem a possibilidade desses dispositivos serem explorados também com o uso de *exploits* (softwares maliciosos que exploram determinadas vulnerabilidades conhecidas de um sistema ou equipamento) conhecidos em meio a comunidade tecnológica. Tudo isso aumenta a probabilidade dos ataques a dispositivos IoT serem massivos, afetando grandes quantidades de dispositivos, e com o agravante dos potenciais danos que podem ocorrer devido ao tempo de indisponibilidade e falta de controle sobre os dispositivos, além disso, os criminosos podem exigir quantias de

resgate muito maiores e tempos de resgate cada vez menores se baseando no tipo do ataque e do tipo de dispositivo sequestrado.

5.2 Por que ransomware em IoT?

No modelo mais comum de *ransomware,* o *ransomware crypto*, o sucesso do ataque deve-se a irreversibilidade, ou seja, quando um *desktop* ou servidor é afetado, parte ou todos os arquivos são sequestrados e normalmente criptografados. Devido a isso, ao menos que se possua em mãos os *backups* de todos os dados sequestrados, a única possibilidade de obter os arquivos após esse tipo de ataque é através da chave privada em posse dos criminosos, que normalmente exigem taxas, como a cobrança de valores em *bitcoins ou* informações privilegiadas, para liberação dos dados.

Na RSA Conference de 2019, a Symantec (2019), questionou os participantes se eles pagariam um resgate de 100 dólares para um dispositivo que custa apenas 10 dólares, no caso uma lâmpada inteligente. Diante desse questionamento, foi possível perceber que, esse tipo de ataque não terá efeito significativo a todos os dispositivos IoT, pois, como a maioria dos dados de dispositivos IoT normalmente são enviados e armazenados em plataformas na nuvem para serem processados, poucos ou nenhum dado sensível fica armazenado nestes dispositivos, e por isso os dados passam a não ser algo tão valioso para os atacantes quando se fala desse tipo de tecnologia. Além disso, os valores cobrados dos ataques em ralação aos valores dos dispositivos IoT, passam a ser outro fator a ser pensado pelos criminosos.

Por conta disso, os criminosos voltam a se concentrar no método antigo de ataque *ransomware*, o *ransomware locker*, o qual consiste em sequestrar e ou bloquear os dispositivos infectados, e não mais na avaliação da quantidade ou qualidade dos dados que a vítima possui para exigir um resgate ou se concentrar em novos ataques. Diante disso, o foco dos criminosos passa a ser então na quantidade de dispositivos afetados ou qual a finalidade deste dispositivo IoT.

Do ponto de vista dos ataques massivos a equipamentos com as mesmas vulnerabilidades, os criminosos virtuais podem reduzir o valor a ser cobrado pelo resgate, e se concentrarem no montante total de pagamento de todos os dispositivos afetados, ou simplesmente utilizam dos equipamentos para suas próprias finalidades, como é o caso do *ransomware* Mirai, que possui uma estimativa de afetar mais de 24 bilhões de dispositivos IoT em 2020, sequestrando e transformando esses dispositivos em zumbis a disposição dos criminosos.

Por outro lado, o maior perigo seria quando os criminosos focam na empregabilidade dos equipamentos, se atentando para o que esse determinado dispositivo possui finalidade. Ou seja, em um contexto residencial, os criminosos se preocupariam, por exemplo, em descobrir as rotinas dos usuários pelos dispositivos sequestrados, a fim de bloquear o controle do termostato de uma residência enquanto o usuário está fora de casa, e exigir o pagamento do resgate imediato para liberar a refrigeração da casa. Neste mesmo contexto, os criminosos poderiam obter o controle das câmeras de segurança, e desta forma poderia monitorar os usuários e até expor a vida intima deles na Internet, além também de terem esses equipamentos e tráfego de rede disponíveis para a realização de um ataque DDoS. No contexto de veículos com sistemas inteligentes, os criminosos se preocupariam com bloqueio do veículo em locais com pouco movimento ou remotos, e fariam a exigência do resgate enquanto o usuário está dentro do veículo, sem opções próximas de socorro. Além disso, enquanto a Internet das Coisas expande as possibilidades de criação de dispositivos de suporte à vida, como marcapassos e bombas de infusões de medicamentos, ou em organizações que usam a Internet das Coisas em sistemas de controle industrial como estações de bombeamento, usinas de energia elétrica e linhas de produções totalmente automatizadas, as consequências pela perda do controle ou do bloqueio destes dispositivos IoT e os danos da resposta tardia a este incidente, aumentariam exponencialmente de acordo com o tempo em que o dispositivo está fora do controle das vítimas.

Pode-se observar então que, neste novo cenário, percebe-se que os atacantes não se concentram mais em somente um contexto tecnológico, mas devido ao uso da IoT como solução para diversas aplicações, ataques *ramsonware* podem ser usados para controlar quantidades enormes de dispositivos e usá-los como fonte para ataques DDoS. Podem também ser usados para desligar ou controlar câmeras de vigilância, equipamentos domésticos, veículos com sistemas inteligentes, sistema de indústria de energia ou até mesmo linhas de produção industriais inteiras.

5.3 O que fazer no caso de uma invasão?

Essa questão varia muito do tipo de dispositivo e o local na qual ele está aplicado, podendo ser uma empresa ou uma residência. Desta forma, se defender de uma invasão causada por um *ransomware* pode não ser algo tão fácil, e diante disso um programa de antivírus e sempre manter o backup de seus dados atualizados, que

são metodologias fundamentais da segurança da informação, podem não ser o suficiente para garantir a segurança dos seus dispositivos IoT e da rede que eles estão conectados.

Em empresas, normalmente quando um dispositivo é afetado por um *ransomware*, normalmente a equipe responsável pela segurança digital é acionada e através do conhecimento técnico desses profissionais, eles conseguem isolar os equipamentos, identificar o tipo de ataque realizado e trabalhar para mitigar os problemas ocasionados pelo ataque.

Porém, se um dispositivo residencial é invadido, normalmente a vítima não terá conhecimento suficiente para agir e mitigar o problema. Para estes casos de ataques a dispositivos na qual as vítimas possuem nenhum ou pouco conhecimento sobre segurança da informação, Popper (2018) propõe as seguintes diretrizes:

> “Na suspeita que pode ter acontecido uma invasão ou contaminação por vírus em um ou até em todos os dispositivos da Internet das Coisas, o primeiro passo é isolar aquele ou aqueles dispositivos dos demais, retirando-o da rede. Em seguida contate um técnico capacitado que possa identificar a vulnerabilidade e se possível, a origem do ataque ou contaminação. Em casos mais extremos será necessário formatar os dispositivos e configurá-los novamente. Após os dispositivos estarem “limpos”, independente de violado ou não, troque todas as senhas de todos os dispositivos e procure inserir novas senhas seguras.”

6 CONSIDERAÇÕES FINAIS

Como os dispositivos de IoT são em sua maioria de natureza e arquitetura extremamente complexa, a melhor maneira de aprender sobre a segurança desses dispositivos é observar o que aconteceu no passado. Ao aprender sobre os erros de segurança que outros desenvolvedores de produtos cometeram no passado, outros desenvolvedores podem entender que tipo de problemas de segurança esperar no produto que estão avaliando e repensar como proteger seus próprios os dispositivos.

A seguir estão alguns dos exemplos mais comentados sobre falhas de segurança e vulnerabilidades de dispositivos IoT.

a) **Philips Hue**: DHANJANI (2013), criou uma técnica que causava apagões permanentes através de repetidos ataques para obter o controle dos dispositivos Philips Hue, que é uma lâmpada inteligente. Ele descobriu essa técnica após perceber que os dispositivos utilizavam apenas a criptografia MD5 do endereço MAC (controle de acesso a mídia) para validar a autenticidade das mensagens trocadas com o dispositivo. Com isso, era possível aprender facilmente os endereços MAC dos dispositivos, criar pacotes de dados maliciosos e enviar comandos para desligar os dispositivos. Isso causava um apagão permanente nos dispositivos, exigindo que os proprietários substituíssem o equipamento.

b) **Google NEST**: Segundo HERNANDEZ et al. (2016), havia uma falha de segurança no Google Nest em que permitia a instalação de um *firmware* malicioso no dispositivo. Isso era possível quando se pressionava o botão NEST por aproximadamente 10 segundos para acionar a opção de redefinição global do dispositivo. Neste momento, era possível conectar o Google NEST á uma mídia USB contendo um *firmware* malicioso para que fosse instalado no dispositivo.

c) **Jeep Hack**: O *Jeep Hack* é um dos ataques mais conhecidos contra dispositivos de IoT. Esse ataque foi desenvolvido por dois pesquisados de segurança Charlie Miller e Chris Valasek, e demostrado em 2015. O ataque consistia em uma complexa engenharia reversa de binários e protocolos individuais, na qual tirou proveito de muitas vulnerabilidades diferentes, sendo a principal no sistema UCONECT da Chrysler, que permitia o acesso e controle remoto dos veículos Jeep equipados com esse sistema. A Figura 18 a seguir, demonstra o código fonte utilizado para explorar o sistema da Jeep. Essa vulnerabilidade resultou em um *recall*

(chamada para manutenção e recuperação) de aproximadamente 1,4 milhão de veículos (MILLER; VALASEK, 2015).

Figura 15 - Código fonte utilizado para explorar o sistema da Jeep

```
#!python
import dbus
bus_obj=dbus.bus.BusConnection("tcp:host=192.168.5.1,port=6667")
proxy_object=bus_obj.get_object('com.harman.service.NavTrailService','/com/ha
rman/service/NavTrailService')
playerengine_iface=dbus.Interface(proxy_object,dbus_interface='com.harman.Ser
viceIpc')
print playerengine_iface.Invoke('execute','{"cmd":"netcat -l -p 6666 |
/bin/sh | netcat 192.168.5.109 6666"}')
```

Fonte: MILLER; VALASEK (2015)

d) **Fechaduras Inteligentes**: Os pesquisadores de segurança Anthony ROSE e Ben RAMSEY, realizaram durante a DEF CON 24 (um dos maiores eventos de segurança da informação mundial) uma apresentação intitulada "*Picking Bluetooth Low Energy Locks from a Quarter Mile Away*" na qual eles expuseram vulnerabilidades em diversos produtos que utilizavam fechaduras inteligentes. Dentre as vulnerabilidades, foram exploradas transmissões de senhas em texto plano (sem proteções criptográficas), os aplicativos móveis eram suscetíveis a reversão possibilitando captura, distorção ou falsificação de informações confidenciais do dispositivo.

e) **Armas Inteligentes e Rifles**: Além dos dispositivos comuns conhecidos e utilizados pelas pessoas, dispositivos utilizados pelas forças armadas como rifles e armas de fogo também estão ficando inteligentes. Um aplicativo móvel do fabricante tecnologias de rifles inteligentes *TrackingPoint*, foi considerado vulnerável a alguns problemas de segurança. Os pesquisadores Runa SANDVIK e Michael AUGER, identificaram que era possível explorar o aplicativo móvel, e assim, o invasor conseguia alterar parâmetros como velocidade do vento, direção, peso da bala, entre outros, que são necessários para a preparação do disparo. Ou seja, o atirador não saberia que essas alterações foram realizadas, quando esses parâmetros fossem modificados.

Pode se perceber então que, todos os casos acima seriam passíveis de invasão e sequestro dos equipamentos por criminosos mal-intencionados através de *ransonwares*, e que o grande desafio dos dispositivos IoT é que eles são desenvolvidos em sua grande maioria por empresas que antes fabricavam apenas *hardwares*, na qual a mentalidade dos engenheiros industriais são totalmente diferente de especialistas em segurança da informação, conforme foi citado por Malic (2018), no capitulo 5.

Com a evolução do conceito de IoT e a facilidade de tornar os equipamentos interconectados com a Internet, essas empresas começaram a embarcar *softwares* inteligentes dentro de seus próprios *hardwares*. Porém, esse tipo de empresa possui pouco ou nenhuma preocupação com a segurança destes dispositivos tendo em vista que, a segurança não é a prioridade do negócio delas, e por conta disso, pontos críticos relacionados a essas empresas, como a falta de maturidade dos processos de segurança e nas metodologias de desenvolvimento de dispositivos IoT, agregados a falta de padrões e arquiteturas de referência no mercado, e a falta de profissionais de segurança especializados para o desenvolvimento seguro destes dispositivos, devem ser observados pela comunidade técnica.

Outro aspecto importante é se tornar obrigatório a criação de um Grupo de Resposta a Incidentes de Segurança (CSIRT) dentro das empresas fabricantes desses dispositivos. A criação de um CSIRT dos vendedores, que representam os fabricantes de hardwares ou softwares e que tratam das vulnerabilidades existentes nos seus produtos, devem auxiliar a ampliação da identificação e avaliação de possíveis riscos e vulnerabilidades no desenvolvimento e lançamento de novos dispositivos IoT. Com isso, juntamente com o departamento de pesquisa e desenvolvimento das empresas deveriam criar metodologias e ferramentas para a implantação de melhorias nos dispositivos IoT, tais como:

- Implantação de atualização do *firmware* dos dispositivos de forma obrigatória e remota, através de canais seguros e com pacotes criptografados, a fim de manter os equipamentos sempre atualizados diretamente pelo fabricante.
- Criação de mecanismos confiáveis de autenticação, inibindo a falsificação de dispositivos, que abrem brecha quando estes dispositivos estão conectados a servidores com diversas máquinas conectadas em sua rede, pois os dispositivos falsificados podem se passar como autênticos dentro dessas redes.
- Unificação da base de códigos de segurança.
- Ferramentas de gerenciamento do ciclo de vida dos certificados de segurança habilitados, para que estes certificados sejam revogados periodicamente, e que assim estes sejam atualizados para manter a segurança dos equipamentos e de futuras autenticações nas redes na quais são operados.
- Atendimento das legislações vigentes de segurança e proteção de dados.

Outro fator extremamente importante para minimizar possíveis vulnerabilidade e riscos é a orientação e conscientização dos usuários, que também está diretamente ligada a segurança desses equipamentos. Quando os dispositivos são vendidos no mercado, os consumidores simplesmente implantam os produtos com ambientes inseguros, o que pode tornar esses dispositivos alvos fáceis de ataques de criminosos cibernéticos. Boas práticas, já implementadas ao decorrer da evolução da web para garantir a segurança dos usuários finais, devem ser aplicadas também no contexto da IoT para minimizar os riscos por conta da falta de conhecimento dos usuários, sendo necessário:

- Nunca permitir a utilização de senhas fracas;
- Sempre exigir a troca das senhas padrão dos dispositivos;
- Desativas as funções de *plug-and-play* universal para que os dispositivos não se conectem em qualquer lugar;
- Sempre revisar as configurações de segurança e principalmente as diretrizes de acesso remoto e acesso administrativo dos equipamentos;
- Sempre manter os equipamentos atualizados de acordo com os lançamentos de novos pacotes de atualização dos fabricantes;

Percebe-se então que, todos os fatores relacionados acima estão diretamente ligados a distribuição massiva de malwares e aos ataques e sequestro de dispositivos IoT em ritmo recorde. Tendo em vista que à medida que as empresas fabricam e que os consumidores continuam utilizando esses dispositivos sem as medidas mínimas de segurança adequadas, os criminosos se aproveitam cada vez mais de falhas e brechas de segurança para invadirem e sequestrarem os dispositivos e seus dados.

Obviamente, proteger a Internet das Coisas continua sendo uma tarefa árdua, pois o setor está apenas procurando um caminho a se tornar estável e, os criminosos *online* estão apenas começando a conhecer os cenários e avaliar as oportunidades e a lucratividade potencial do novo mercado. Mas, como visto nos casos acima, as empresas já devem buscar metodologias e ferramentas para proteção destes dispositivos, além de mapear e avaliar os seus riscos e possíveis impactos, e prever políticas de segurança da informação e governança para garantir o controle e segurança destes dispositivos.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Norma ABNT NBR ISO/IEC 27001:2013**: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisito. 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Norma ABNT NBR ISO/IEC 27001-2006**: Sistemas de Gestão da Segurança da Informação – Requisito, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Norma ABNT NBR ISO/IEC 27002:** Tecnologia da Informação -Técnicas de Segurança – Código de prática para a gestão da segurança da informação (conteúdo técnico idêntico ao da ABNT NBR ISO/IEC 17799), 2005.

ALVES, Gilvan. **What is the difference between malware, a virus and a Trojan?**. 2017. Disponível em: https://www.dicasecuriosidades.net/2017/03/qual-e-diferenca-entre-malware-um-virus.html. Acesso em: 05 mar. 2020.

ASHTON, Kevin. **That 'Internet of Things' Thing**: In the real world, things matter more than ideas. 22 jun. 2009. Disponível em: https://www.rfidjournal.com/articles/view?4986. Acesso em: 05 mar. 2020.

AVAST. **DDoS** – Ataque Distribuído de Negação de Serviço. Disponível em: https://www.avast.com/pt-br/c-ddos. Acesso em: 06 jan. 2020.

AVAST. **Pharming**. Disponível em: https://www.avast.com/pt-br/c-phishing. Acesso em: 06 jan. 2020.

AVAST. **Phishing**. Disponível em: https://www.avast.com/c-pharming. Acesso em: 28 fev. 2020.

AVAST. **Spoofing**. Disponível em: https://www.avast.com/c-spoofing. Acesso em: 28 fev. 2020.

BABAR, Sachin. MAHALLE, Parikshit. STANGO, Antonietta. PRASAD, Neeli. PRASAD, Ramjee. **Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)**. 3rd International Conference on Recent Trends in Network Security and Applications, Chennai, India, 2010.

BALAGUER, Adriano. **Segurança da Informação no mundo da Internet das Coisas**. Comércio Eletrônico – Vendas e Segurança na Internet. 2000. 69 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Centro Universitário do Triângulo, Uberlândia, 2000. Disponível em: http://www.computacao.unitri.edu.br/downloads/monografia/48761143224807.pdf. Acesso em: 20 nov. 2019.

CAMPOS, André. **Sistemas de Segurança da Informação**: Controlando os riscos. 2 ed. Florianópolis: Visual Books, 2007.

CARVALHAL, Aline. **O que é rootkit**? 25 jan. 2012. Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-rootkit.html. Acesso em: 22 nov. 2019.

CERT.br. **Cartilha de Seguranca para Internet**: Códigos Maliciosos (Malware). Disponível em: https://cartilha.cert.br/malware/. Acesso em: 09 jul. 2020.

CLOUDFLARE. **What is a Phishing attack**. Disponível em: https://www.cloudflare.com/learning/access-management/phishing-attack/. Acesso em: 05 mar. 2020.

CONVERGENCIA DIGITAL. Triplicam os ataques de malware via internet das coisas. 20 ago. 2018. Disponível em: http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=49012&sid=18. Acesso em: 10 jul. 2020.

DEFESANET. **Vírus que "sequestram" computadores aumentam 43 por cento em três meses, diz estudo**. 26 nov. 2012. Disponível em: http://www.defesanet.com.br/cyberwar/noticia/8770/Virus-que--sequestram--computadores-aumentam-43-por-cento-em-tres-meses--diz-estudo/. Acesso em: 05 mar. 2020.

DHANJANI, Nitesh. **Hacking Lightbulbs**: Security evaluation of the philipshue personal wireless lighting system. 2013. Disponível em: https://www.dhanjani.com/docs/Hacking%20Lighbulbs%20Hue%20Dhanjani%202013.pdf. Acesso em: 27 fev. 2019.

FILE.net. **What is HD-Agent.exe?**. Disponível em: https://www.file.net/process/hd-agent.exe.html. Acesso em: 05 mar. 2020.

GARTNER. **Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020**. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io. Acesso em: 05 maio 2020.

GITTLESON, Kim. **How tracking technology can better fill hospital beds**. BBC. 26 nov. 2013. Disponível em: https://www.bbc.com/news/business-25059166. Acessado em: 28 fev. 2020.

NAGY, Attila. **14 Infamous Computer Virus Snippets That Trace a History of Havoc**. Gizmodo. 05 jul. 2013. Disponível em: https://gizmodo.com/14-infamous-computer-virus-snippets-that-trace-a-histor-601745022. Acesso em: 05 mar. 2020.

HERNANDEZ, Grant. et al. **Smart Nest Thermostat**: A Smart Spy in Your Home. 2016. Disponível em: https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf. Acesso em: 27 fev 2019.

HPE, Hawlett Packard Enterprise. **O que é a Internet das Coisas Indústrial (IIOT)**. Disponível em: https://www.hpe.com/br/pt/what-is/indústrial-IoT.html. Acessado em: 28 fev 2020.

KAPERSKY. **O que é código malicioso?**. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/malicious-code. Acesso em: 12 nov 2019.

LAUDON, Kenneth C. LAUDON, Jane P. **Sistemas de Informação Gerenciais**: administrando a empresa digital. 5a ed. São Paulo: Person Pretice Hall, 2004.

LAUREANO, Marcos Aurelio Pchek. **Gestão da Segurança da Informação**. Apostila, 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em: 27 nov. 2019.

LÉVEILLÉ. Marc-Etienne M. **Known unknowns**: detecting rootkits under OS X. 23 set. 2013. Disponível em: https://www.welivesecurity.com/2013/09/23/known-unknowns-detecting-rootkits-under-os-x/. Acesso em: 05 mar. 2020.

MALIK, Willian. Entenda por que a internet das coisas ainda é tão insegura. Olhar Digital. 10 jul. 2020. Disponível em:

MANYIKA, James. et al. **The Internet of Things**: Mapping the Value Beyond the Hype. McKinsey Global Institute, 2015.

URBANO, Maressa. **Dia Mundial da Internet**: SVM alerta para os riscos que esse fenômeno está causando. 17 maio 2017. Disponível em: https://www.dicastreslagoas.com.br/dia-mundial-da-internet/. Acesso em: 05 mar. 2020.

MASSENO, Manuel David. WENDT, Emerson. **O ransomware na lei:** apontamentos breves de Direito Português e Brasileiro. 17 jul. 2017. Disponível em: http://direitoeti.com.br/artigos/o-ransomware-na-lei-apontamentos-breves-de-direito-portugues-e-brasileiro/#:~:text=chapeu%20branco%E2%80%9D)%3A-,1.,de%20multa%20at%C3%A9%20120%20dias%20. Acesso em: 09 jul. 2020.

MCKINSEY & COMPANY. **Industry 4.0**: How to navigate digitization of the manufacturing sector. abril 2015. Disponível em: http://www.forschungsnetzwerk.at/downloadpub/mck_industry_40_report.pdf. Acesso em: 07 maio 2020.

MILLER, Charlie. VALASEK, Chris. **Remote Exploitation of an Unaltered Passenger Vehicle**. August 10, 2015. Disponível em: http://illmatics.com/Remote%20Car%20Hacking.pdf. Acesso em: 27 fev. 2020.

NOVAES, Rafael. **Veja o que é um Ransomware, um tipo de malware muito perigoso**. 14 maio 2014. Disponível em:http://www.psafe.com/blog/ransomware/. Acesso em: 22 nov. 2019.

OLIVEIRA, Waldes. **Riscos, vulnerabilidade e ameaça em Segurança da Informação**. Disponível em: https://www.techtem.com.br/seguranca-da-informacao-riscos-vulnerabilidade-e-ameaca/. Acesso em: 29 nov. 2019.

OLIVEIRA, Wilson Jose de. **Segurança da informação**: técnicas e soluções. Florianópolis: Visual Books, 2001.

PALMER, Danny. **IoT security**: Is cryptocurrency-mining malware your next big headache?. ZDNet. 03 maio 2018. Disponível em: https://www.zdnet.com/article/iot-security-is-cryptocurrency-mining-malware-your-next-big-headache/. Acesso em: 10 jul 2020.

PEIXOTO, Mário César Pintaudi. **Engenharia Social & Segurança da Informação na Gestão Corporativa**. 1a ed. Rio de Janeiro: Brasport, 2006.

POPPER. Marcos Antonio. **Internet das coisas**: potencialidades e perigos. 2018. UNISUL, Santa Catarina, 2018. Disponível em: https://riuni.unisul.br/bitstream/handle/12345/4943/Marcos_Popper%5B48190-49065%5DAD6_versao_final_publicacao.pdf?sequence=1&isAllowed=n. Acesso em: 11 jul. 2020.

POSTSCAPES. **Smart Greenhouse Remote Monitoring Systems**. Disponível em: https://www.postscapes.com/smart-greenhouses/. Acessado em: 28 fev de 2020.

PWC. **The Global State of Information Security® Survey 2018**. Disponível em: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html. Acesso em: 29 nov. 2019.

RESEARCHGATE. **Estrutura de um ataque de negação de serviço distribuído**. Disponível em: https://www.researchgate.net/figure/Figura-31-Estrutura-de-um-ataque-de-negacao-de-servico-distribuido_fig1_228934014. Acesso em: 05 mar. 2020.

REUTER. Honda é alvo de ataque hacker e suspende parte da produção, incluindo no Brasil. 09 jun. 2020. Disponível em: https://br.reuters.com/article/internetNews/idBRKBN23G1VV-OBRIN. Acesso em: 09 jul. 2020.

RF WIRELESS WORLD. **Network Security Tutorial**. 2012. Disponível em: https://www.rfwireless-world.com/Tutorials/network-security-tutorial.html. Acesso em: 05 mar. 2020.

SAMSUNG. **Casa inteligente com dispositivos IoT. 2020.** Disponível em: https://www.samsung.com/africa_pt/tvs/smart-tv/smart-home-with-IoT-devices/. Acesso em: 10 mar. 2020.

SANDVIK, Runa. AUGER, Michael. **Hackers Can Disable a Sniper Rifle - Or Change Its Target**. 29 jul. 2015. Disponível em: https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/. Acesso em: 27 fev. 2020.

SANTOS DIAS, Juliana Costa. **O que são Rootkits e como enfrentá-los**. 13 jun. 2013. Disponível em: https://blog.kaspersky.com.br/o-que-sao-rootkits-ecomo-enfrenta-los/769/. Acesso em: 22 nov. 2019

SECURITY-WIRE. **How to Remove Email-Worm.JS.Gigger Virus?**. 17 maio 2010. Disponível em: http://security-wire.com/tag/delete-email-worm-js-gigger-virus. Acesso em: 05 mar. 2020.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: Uma visão executiva. Rio de Janeiro, RJ: Elsevier Editora, 2014. 2. ed. 46p.

SETHI, Pallavi e SARANGI, Smruti R. **Internet of Things**: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering. 26 Jan. 2017. Disponível em: https://www.hindawi.com/journals/jece/2017/9324035/. Acesso em: 10 jan 2020.

SILVA FILHO, A. M. **Segurança da Informação e Disponibilidade de Serviços na Era da Internet**. Revista Espaço Acadêmico, 07 jan. 2005.

SILVA FILHO, A. M. **Entendendo e Evitando a Engenharia Social**: Protegendo Sistemas e Informações. Revista Espaço Acadêmico, 07 dez. 2004.

SILVA FILHO, A. M. **Segurança da Informação**: Sobre a Necessidade de Proteção de Sistemas de Informações. Revista Espaço Acadêmico, 05 nov. 2004.

SMARTHOME. **What is a smart home?**. 2020. Disponível em: https://www.smarthome.com/what-is-a-smart-home. Acesso em: 10 mar. 2020.

SPRINGBOARD. **Spoofing Attacks**: Everything You Need to Know. 07 jun. 2018. Disponível em: https://www.springboard.com/blog/spoofing-attacks/. Acesso em: 05 mar. 2020.

STALLINGS, Willian. **Criptografia e segurança de redes**: Princípios e Práticas. 4. ed. São Paulo: Pearson Prentice Hall, 2008. 492 p.

SONICWALL. **Relatório de Ameaças Cibernéticas da SonicWall 2019**. 24 jul. 2019. Disponível em:https://www.sonicwall.com/news/sonicwall-2019-mid-year-threat-report/. Acesso em: 25 nov. 2019

TECHNICAL INFO. **The Pharming Guide**. Disponível em: http://www.technicalinfo.net/papers/Pharming2.html. Acesso em: 05 mar. 2020.

TECMUNDO. **Slack e GitHub têm malware backdoor que rouba documentos**. 11 mar. 2019. Disponível em: https://www.tecmundo.com.br/seguranca/139370-slack-github-tem-malware-backdoor-rouba-documentos.htm. Acesso em: 05 mar. 2020.

TEXAS, PENAL CODE (2017), Capítulo XXXIII – Computer Crimes, Sec. 33.023. Disponível em: https://statutes.capitol.texas.gov/Docs/PE/htm/PE.33.htm. Acesso em: 09 jul. 2020.

TREND MICRO. **Combater a epidemia de ransomware exige uma segurança em camadas**. 27 maio 2016. Disponível em:https://blog.trendmicro.com.br/combater-epidemia-de-ransomware-exige-uma-seguranca-em-camadas/. Acesso em: 22 nov. 2019.

THE GUARDIAN. **Traffic cameras in Victoria infected by WannaCry ransomware**. 22 jun. 2017. Disponível em: https://www.theguardian.com/australia-news/2017/jun/22/traffic-cameras-in-victoria-infected-by-wannacry-ransomware. Acessado em: 27 fev. 2020.

VALTRA. **Precision Farming**: Made Easy. Disponível em: https://www.valtra.com/our-insights/smart-farming/technology-solutions.html. Acesso em: 28 fev. 2020.

WAHER, Peter. **Learning Internet of Things**. Packt Publishing Ltd. Birmingham Mumbai, 2015.