INSTITUTO FEDERAL DE CIÊNCIA E TECNOLOGIA DE PERNAMBUCO

Recife

Departamento Acadêmico de Sistemas Eletrônicos

Tecnologia em Análise e Desenvolvimento de Sistemas

DANILO PEREIRA DA SILVA

ANÁLISE DE MÉTODOS DE DETECÇÃO DE ATAQUES DE RANSOMWARE EM DISPOSITIVOS IOT EM REDES TCP/IP

Recife
2020

DANILO PEREIRA DA SILVA

ANÁLISE DE MÉTODOS DE DETECÇÃO DE ATAQUES DE RANSOMWARE EM DISPOSITIVOS IOT EM REDES TCP/IP

Monografia apresentada ao Curso de Tecnólogo em Análise e Desenvolvimento de Sistemas do Instituto Federal de Pernambuco, como requisito parcial para obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Orientador: M.Sc. Anderson Luiz Souza Moreira.

Recife
2020

S586a Silva, Danilo Pereira da.

2020 Análise de Métodos de Detecção de Ataques de Ransomware em Dispositivos IoT em Redes TCP/IP / Danilo Pereira da Silva. – Recife: O Autor, 2020.

50 f.: il.

TCC (Curso de Tecnólogo em Análise e Desenvolvimento de Sistemas) – Instituto Federal de Pernambuco, Departamento Acadêmico de Sistemas Eletrônicos, 2020.

Inclui Referências

Orientador: Prof. M.e Anderson Luiz Souza Moreira

1. Ransomware. 2. IoT. 3. Segurança. I. Moreira, Anderson Luiz Souza, (orientador). II. Instituto Federal de Pernambuco. III. Título.

CDD 005.8

Catalogação na fonte: Bibliotecário Cristian do Nascimento Botelho CRB4/1866

Trabalho de Conclusão de Curso apresentado por **Danilo Pereira da Silva** à coordenação de Análise e Desenvolvimento de Sistemas, do Instituto Federal de Pernambuco, sob o título de **“ANÁLISE DE MÉTODOS DE DETECÇÃO DE ATAQUES DE RANSOMWARE EM DISPOSITIVOS IOT EM REDES TCP IP”**, orientado pelo Prof. **Anderson Luiz Souza Moreira** e aprovada pela banca examinadora formada pelos professores:

Recife, 17 de dezembro de 2020

_____

Prof. M.Sc. Anderson Luiz Souza Moreira
CSIN/DASE/IFPE

_____

Prof. M. Sc. Renata Freire de Paiva Neves
CSIN/DASE/IFPE

_____

Prof. M. Sc. Lizandro Nunes Silva
CELN/DASE/IFPE

Recife
2020

Este trabalho é dedicado a minha família
Pelo apoio, dedicação e superação.

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus por ter me ajudado me dando conhecimento e estratégias para chegar aqui, e concluir minha graduação.

Bem sei que não foi fácil o caminho até este dia, muitos problemas enfrentados dificuldades para chegar até aqui, mas ele chegou e estou muito feliz por isto. Também gostaria de agradecer a minha cunhada Mayara Lima que me auxiliou na construção de minha pesquisa escrita; aos meus pais, Antônio Carlos Gerôncio e Maria Ângela, por sempre estarem ao meu lado em minhas escolhas e decisões que precisei tomar o quando necessário, a minha esposa Tamyres de Oliveira, outra pessoa muito especial em minha vida que ajudou em diversas vezes que até pensei em desistir nesta caminhada. Mayara Kelly Lima, por sempre me incentivar e me dar o suporte sempre que necessário e ao meu orientador Anderson Moreira por ter me auxiliado, por ter tido enorme paciência comigo para desenvolver este trabalho. Também gostaria de agradecer a todo corpo docente pelos ensinamentos e conhecimento ministrado e para finalizar ao meu avô, Antônio Gerôncio da Silva que partiu antes de ver a entrega e conclusão do meu curso, mas que sempre me incentivou nos estudos desde muito jovem e a não desistir, eu o agradeço de coração.

Muito obrigado a todos.

“Até aqui nos ajudou o senhor" (1Sm 7:12)

RESUMO

Este trabalho, faz de uma análise documental que aborda estudos sobre vulnerabilidades a quais dispositivos *Internet of Things* (*IoTs)* estão expostos e métodos de detecção contra ataques de *ransomwares*, em redes *Transmission Control Protocol / Internet Protocol* (*TCP/IP)*. Para isto foram realizados dois métodos. Foi realizada uma simulação com o software *RanSim*, que realiza testes de ataques *ransomwares,* com demonstração de cenários de infecção para 20 tipos diferentes e 1 cenário onde os dados do dispositivo são cifrados. O segundo método adotado foi uma análise estática, explorando a estrutura de um arquivo *portable executable*, buscando palavras chaves que identificassem se o arquivo estava infectado com o *ransomware,* a partir disto possibilitar a criação de ferramentas para a prevenção de ataques.

Através deste trabalho foi possível observar alguns aspectos de segurança ainda pouco explorados no setor. Que podem ser melhorados através da utilização de *softwares* de identificação de vulnerabilidades. Ao concluir a análise foi observado que apesar dos métodos disponíveis, estes isoladamente não são totalmente eficazes, abrindo espaço para a criação de uma ferramenta que unifique esses métodos e aumente a eficácia de detecção e prevenção de ransomware.

Palavras-chaves: *Ransomware*. *IoT*. Segurança.

ABSTRACT

This paper is a documentary analysis that addresses studies on vulnerabilities to which *Internet of Things* (IoT) devices are exposed and methods of detection against ransomware attacks in *Transmission Control Protocol / Internet Protocol* (TCP/IP) networks. For this, two methods were performed. A simulation was executed with RanSim software, which performs tests for ransomware attacks, and demonstration of infection scenarios for 20 different types and 1 scenario where the device data is encrypted. The second method adopted was a static analysis, exploring the structure of a portable executable file, looking for keywords that would identify if the file was infected with ransomware, from this to enable the creation of tools for the prevention of attacks.

Through this work it was possible to observe some aspects of security that remain a little explored in the sector. That can be improved through the use of vulnerability identification software. At the end of the analysis, it was observed that despite the available methods, these alone are not fully effective, making room for the creation of a tool that unifies these methods and increases the effectiveness of detection and prevention of ransomware.

Keywords: Ransomware. *IoT*. Security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNICOS, ABREVIATURAS E SIGLAS

TI: Tecnologia da Informação

IOT: Internet of Things

TCP/IP: Transmission Control Protocol / Internet Protocol

CLP: Controlador Lógico Programável

CPU: Central Process Unit

RAM: Random Access Memory

TOR: The Union Routing The Union Routing

RAAS: Ransomware com um serviço

AES: Advanced Encrytion Algorithm

SO: Sistema Operacional

C&C: Controle e Comando

PE: Portable Executable

DOS: Disk Operation System

DDOS: Distributed Denial of Service

DLL: Dynamic-link Library

.NET: DotNet

SUMÁRIO

1 INTRODUÇÃO

O relevante crescimento do mercado de Tecnologia da Informação (TI) no mundo, envolvendo *Internet of Things* (IoT) ou simplesmente Internet das Coisas, foi a principal motivação para iniciar esta pesquisa. De acordo com (COMPUTERWORLD, 2020) em 2020 em junho 48% das empresas brasileiras estavam tinham perspectivas de fechar o ano negativo, porém em setembro do mesmo ano este número caiu para 14% e segue caindo. Com a chegada do 5g, o crescimento da utilização de *IoT*, terá grande avanço nos setores de carros autônomos, cidades inteligentes, saúde conectada, vídeos imersivos. Com projeção para 2023 de crescimento com conexões máquina a máquina (M2M), com suporte a dispositivos *IoT,* representará cerca de 50% (14,7 bilhões) do total mundial de dispositivos e conexões. (CISCO, 2020)

Observa-se o crescente número de dispositivos que estão sendo integrados nas nossas casas diariamente, o *IoT* vem ganhando força em todo mundo por seus benefícios e facilidades, porém as vulnerabilidades existentes, não são bem abordadas. (NIžETIć *et al*, 2020).

Leva-se em consideração a grande expansão dos dispositivos *IoT*, este trabalho visa realizar um estudo comparativo sobre diversos métodos de detecção contra ataques envolvendo *ransomware*. Análises de possíveis ações preventivas, apresentando vulnerabilidades desta tecnologia em redes *TCP/IP* e sugerindo algumas soluções de como identificar tais problemas, através de padrões apresentados e ferramentas para detecção. (HUMAYUN *et al.*, 2020).

Como é possível observar nas pesquisas de (UNISYS, 2017) o Brasil está cada vez mais envolvido com os dispositivos inteligentes, e apoiam a sua utilização para segurança. Este foi um dos motivos que foi levado em consideração para dar seguimento a pesquisa.

Inicialmente o trabalho visa demonstrar as possíveis vulnerabilidades dos dispositivos conectados em redes *Transmission Control Protocol / Internet Protocol (TCP/IP).* Focando mais precisamente em dispositivos *IoT*, tais quais: aplicativos de saúde, aplicativos de trânsito, aplicativos de segurança, que estão cada vez mais

inseridos no cotidiano. Levando-se em consideração foram realizadas análises através de softwares para identificar vulnerabilidades de dispositivos *IoT*.

1.1 Objetivo

O presente estudo tem como objetivo criar uma análise documental que aborda o crescimento de ataques de ransomware em dispositivos *IoT* em redes *TCP/IP*, estudando métodos de detecção e prevenção contra ataques. Realizando uma análise documental de vulnerabilidades de dispositivos *IoT*, entender o funcionamento dos ataques de *ransomware*, realizar simulação de ataque ransomware em ambiente controlado e analisar ransomware *Jigsaw* em arquivo de formato *portable executable.*

1.2 Organização do texto

Neste capítulo foi realizada considerações importantes que serão abordados no transcorrer deste trabalho. No capítulo 2 são apresentados conceitos para fundamentação da pesquisa. Conceitos básicos de segurança, *IoT*, e *ransomware* com foco em suas vulnerabilidades e métodos de detecção. No capítulo 3 é realizada análise de estudos que viabilizaram essa pesquisa, servido de base de estudo. No capítulo 4, foram empregados os métodos e conceitos para a realização de simulação e análise de *ransomware.* No capítulo 5 foi feita a discussão e comparação entre os estudos e seus métodos apresentados, com minha pesquisa e análise. Capitulo 6 conclui este trabalho.

2 CONCEITOS PARA ESTUDO

2.1 Segurança da Informação

A segurança da informação tem como principal pilar, a proteção de dados de valores, para empresas e ou indivíduos, isto define as características da segurança da informação. Com isso, parte de algumas características importantes, como: (GOMES, 2017).

Confidencialidade: refere-se aos dados só estarem disponíveis às pessoas devidamente autorizadas a terem acesso às mesmas.

Integridade: refere-se a consistências dos dados, uma vez que o dado foi criado e salvo, deve permanecer desta forma até que o seu criador o altere.

Disponibilidade: refere-se ao fato do dado estar sempre disponível quando necessário para os usuários devidamente autorizados.

Autenticidade: É a garantia de quem criou ou manipulou determinada informação, garantindo assim o rastreamento de quem realizou determinadas ações.

Todos esses pilares são de suma importância para a segurança nos dispositivos. (HINTZBERGEN *et al*., 2018).

2.2 Política de Segurança

A política de segurança parte do princípio de que a informação é um dos ativos mais valiosos nos dias atuais e que deve ser protegido (CASTILHO; FONTE, 2012). Tendo conhecimento disto as organizações priorizam cada vez mais a privacidade de suas informações. A engenharia social que pode ser considerada uma arte, para obter informações pessoais de indivíduos é uma técnica que vem sendo muito utilizada. (RODRIGUES, 2019).

A NBR ISO/IEC 27002, que fornece diretrizes para padrões de segurança, conceitos que ajudam no gerenciamento da informação, que leva em consideração ambiente possíveis riscos. A NBR ISO/IEC 27002 cita alguns requisitos para estabelecer segurança da informação: é papel da organização fazer uma análise de riscos, através disto é possível identificar possíveis vulnerabilidades. Outra sugestão é um conjunto particular de objetivos e requisitos. O objetivo da norma é dar uma

direção, fornecendo caminhos para iniciar, implementar, manter e melhorar as políticas de segurança. (ABNT, 2013)

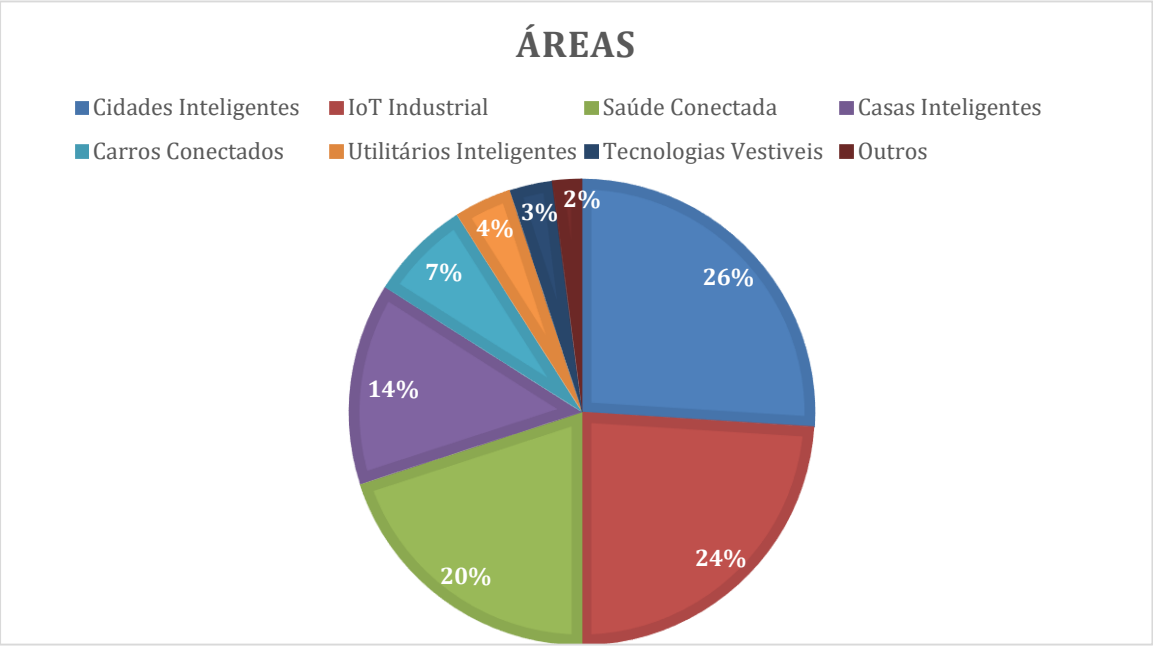
2.3 IoT e Suas Aplicabilidades

Internet das coisas refere-se à rede interconectada de dispositivos, sensores, atuadores, software, etc. que armazenam e trocam informações (AZMOODEH *et al.*, 2017).

O principal fator da utilização é sua integração com diferentes tecnologias, que cria diversas possibilidades e aplicabilidades. Como nas áreas de saúde, educação, indústrias, escritórios, residências, comércio entre outras. O crescimento da busca pela utilização dos dispositivos para automatizar casas e até mesmo carros inteligentes. No setor negocial, o destaque vai para as indústrias, que obteve um crescimento nos setores de qualidade e produção. (POOPER, 2018).

A Figura 1 mostra a perspectiva de distribuição e áreas de atuação onde os *IoT* estarão inseridos atualmente, onde é possível ver que a maioria do mercado está forcada nos setores das cidades inteligentes e *IoT* industrial. (NIžETIć *et al*, 2020).

Figura 1 - Estrutura de mercado geral de tecnologias IoT.



Fonte: (NIžETIć et al, 2020).

Tendo uma ideia do planejamento mostrado na figura 1. Áreas onde o *IoT* está sendo empregado. Esse mercado de dispositivos inteligentes tem previsão de crescimento de 7,3% com um faturamento de $ 123 bilhões no ano de 2021. (FORBES, 2018). O setor da saúde, que é o terceiro, vem se destacando com dispositivos que estão presentes desde em hospitais como em residências, em aparelhos que ajudam o monitoramento de pacientes e no envio de dados diretamente para hospitais ou pessoas responsáveis por monitorar pacientes, também vem sendo utilizada para monitoramento de doenças silenciosas como: diabetes e doença de Parkinson. (BAKER; XIANG; ATKINSON, 2017).

As indústrias também se inserem na inovação tecnológica, com o que se chama de Indústria 4.0. “Produção industrial será altamente flexível em volume de produção e personalização, extensa integração entre clientes, empresas, fornecedores e, acima de tudo, sustentável. ” (SHROUF; ORDIERES; MIRAGLIOTTA, 2014). As indústrias hoje partem do princípio do aumento, tanto de sua produção efetiva, quanto da qualidade, a utilização de monitoramento do processo, sistema de supervisão de tudo o que acontece dentro das fábricas, a facilidade no armazenamento de dados através dos dispositivos de Internet das Coisas, tem aumentado a procura pela implantação dos mesmos nestes ambientes, a perspectiva é que áreas de atuação desses dispositivos conectados à rede cresça.

Assim como também é possível observar o crescimento de sua utilização em automóveis que não precisam de motoristas, casas que podem ser controladas e monitoradas remotamente através desta tecnologia, que está inserida cada dia mais em nossa sociedade.

2.3.1 O mundo atual com os pagamentos digitais e IoT

Como pode ser visto até aqui ao longo do presente trabalho foi possível ver as aplicabilidades de dispositivos *IoT* e os pagamentos digitais estão inclusos nesse meio, algumas empresas como a Visa desenvolveram setores específicos para estudar mais sobre a aplicabilidade dos assuntos para resolver questões de pagamentos com segurança.

> O programa Visa *ready* tem como objetivo o estudo de soluções inteligentes e seguras para pagamentos. Nesse programa criado pela visa é possível que os fabricantes consigam fazer com que os seus dispositivos conectados possam realizar pagamentos de forma segura, desta forma permitindo que qualquer coisa desde um relógio como um carro possa ser utilizado para realizar pagamentos. (VISA, 2018).

Isto já está sendo posto em prática pela a empresa, para isso a Visa tem em mente utilização de recursos já criados como o visa *token* service, esse serviço garante que os pagamentos sejam efetuados de maneira segura em qualquer local, sendo assegurado pela própria empresa, basta apenas ter uma *Internet* próxima e um dispositivo compatível para a realização do pagamento. E para garantir a segurança eles determinam que para participar do programa Visa *ready* é necessário seguir alguns passos mínimos tais como: padrões funcionais e de segurança da visa. Assim com o Visa outras empresas buscam se inserir neste mercado estudando as possíveis maneiras de se utilizar dos dispositivos conectados para a realização de tarefas corriqueiras de nosso dia a dia.

2.4 Segurança e IoT

Nos últimos anos o crescimento de dispositivos *IoT* é evidente como já foi mostrado ao longo deste trabalho, mas juntamente como o crescimento de suas aplicabilidades cresce a necessidade de cautela com a sua segurança, já que estes dispositivos estão cada vez mais inseridos em setores que requerem um maior cuidado como transporte inteligente, cuidados médicos, industriais entre outros. (SUO, *et al*, 2012). O fato é que por sempre estarem conectados à *Internet,* isto oferece algumas vulnerabilidades. (SMITH, 2018).

2.5 Vulnerabilidades em Dispositivos *IoT*

Os dispositivos *IoT,* interligados em uma rede são muito mais vulneráveis, pois apresenta uma gama de problemas que podem ser explorados, tais como: infraestrutura, privacidade e indisponibilidade. (POOPER, 2018).

Existem alguns desafios que precisam ser levados em consideração quando é falado de segurança em *IoT,* comunicações feitas em redes sem fio, possibilitando

interceptação de tráfego de dados. A possibilidade de acesso físico, cria um ponto de atenção que necessita ser levado em consideração. Necessidade de zelar pela integridade dos dados trafegados e confidencialidade dos mesmos. (RIBEIRO, 2018).

Outro ponto que pode ser destacado é a utilização de rede *TCP/IP* que já deixa vulnerável a possíveis ataques, devido a miniaturização dificulta a construção de mecanismos complexos de segurança, pode causar gasto excessivo de consumo de energia e possíveis atrasos de comunicação, o que pode atrapalhar os propósitos dos dispositivos conectados. (M.SADEEQ, *et al*. 2018). Em uma rede de dispositivos inteligentes existem diversos objetos conectados a eles, que necessita de uma segurança mais reforçada, pois se um for infectado, isso pode ser prejudicial a toda a rede. (RIBEIRO, 2018).

Estes dispositivos possuem algumas vulnerabilidades que dão brechas na segurança. Muitos desses dispositivos não possuem um *hardware* robusto, os quais muitas das vezes não possuem um Sistema Operacional (*SO*), muito menos um *firewall* para criar defesas contra ataques de *hackers*, a utilização de periféricos como sensores entre outros pode ser prejudicada, ainda não existe um tipo de protocolo único para utilização de tráfego de dados para estes dispositivos e muito menos um padrão. (M.SADEEQ, *et al*. 2018).

A seguir é possível ver alguns dos protocolos de rede e tecnologias de comunicação, normalmente utilizados: (RIBEIRO, 2018).

- **Protocolos**: *Zigbee, 6LoWPAN, RPL, TCP/IP.*
- **Tecnologias de Comunicação**: *Bluetooth, Wi-fi, Thread.*

Será dado a seguir, ênfase no protocolo *TCP/IP*, foi adotado esse padrão porque é amplamente utilizado por diversas aplicações, é de fácil compreensão, e fácil utilização, dependendo de qual seja objetivo da construção de sua rede *IoT*, não é necessário utilizar outros protocolos nos quais você não use todos os recursos que eles proporcionam. O *TCP/IP* é conhecido como um conjunto de protocolos, ou uma pilha de protocolos. Você pode muito bem criar um protocolo exclusivo seu para tentar deixar mais segura a comunicação entre os dispositivos. Tendo como base a pesquisa

de (ZAHRA; SHAH, 2017) onde é proposta a utilização de uma lista negra para identificação de dispositivos confiáveis.

2.6 Malware

Um *malware* é um termo abreviado para “Software Malicioso” (Malicious Software), esse tipo de software foi criado especificamente para obter acesso ou danificar um computador, sem conhecimento do seu proprietário. Existem vários tipos de *malwares* como: *spyware, keyloggers, worms* ou qualquer outro código malicioso que queira se infiltrar em um computador. (NORTON, 2020).

Existem diversas classificações para eles, alguns deles são denominados como *Rootkits*, Cavalos de Tróia e o outro tipo que será discutido neste trabalho é o *ransomware*. (ZAKARIA, *et al*, 2017).

2.7 Ransomware

Ransomware é um *malware* que emprega criptografia para manter as informações da vítima em resgate. Os dados críticos de um usuário ou organização são criptografados para que eles não possam acessar arquivos, bancos de dados ou aplicativos. Um resgate é então exigido para fornecer acesso. O *ransomware* é frequentemente projetado para se espalhar por uma rede e por bancos de dados de destino e servidores de arquivos e, portanto, pode paralisar rapidamente uma organização inteira. É uma ameaça crescente, gerando bilhões de dólares em pagamentos a cibercriminosos e infligindo danos e despesas significativas para empresas e organizações governamentais. (MCAFEE, 2021)

Existe uma certa variedade deste *malware* mas a seguir será relatado dois dos principais tipos que estão em alta, são eles:

- *Locky ransomware*
- *Crypto ransomware*

***Locky ransomware*:** É um tipo de *ransomware* que não permite o acesso do usuário ao seu computador. Normalmente ele bloqueia o acesso do usuário de acessar a interface de seu computador ou outro dispositivo, como *smartphone*, e como um

ataque de *ransomware* depois do bloqueio ele solicita o pagamento de um determinado valor pelo usuário para que o mesmo volte a ter acesso ao seu dispositivo, estabelecendo um canal de comunicação com o mesmo para a efetivação do pagamento. Desta forma ele não é tão eficiente com o *Crypto*, pelo fato de não danificar os arquivos do computador, nem ao menos criptografá-los, caso o usuário formate o dispositivo ou voltar ao estado anterior, tem grande chance de removê-lo. Por isso é considerado não tão eficiente como *crypto*. *Locky* é bastante utilizado e mais eficiente para os casos de engenharia social, se disfarçando de autoridades como polícia que se utiliza disso para obter informações do usuário. Mas quando falamos de *locky* para dispositivos de *internet* das coisas, ele possui um grande potencial a nível de periculosidade. (SYMANTEC, 2015).

***Crypto Ransomware*:** *Crypto* tem como principal objetivo procurar e criptografar dados valiosos no computador, e o usuário só pode reaver os dados com uma chave para descriptografar os arquivos, porém isso só será possível caso o usuário pague um valor de resgate. Ele é projetado por procurar tipos específicos, como: (jpeg, pdf, .doc.). Diferentemente do *locky ransomware*, o usuário ainda pode usar seu dispositivo normalmente, porém sem ter acesso aos arquivos criptografados pelo *malware*. (SYMANTEC, 2015).

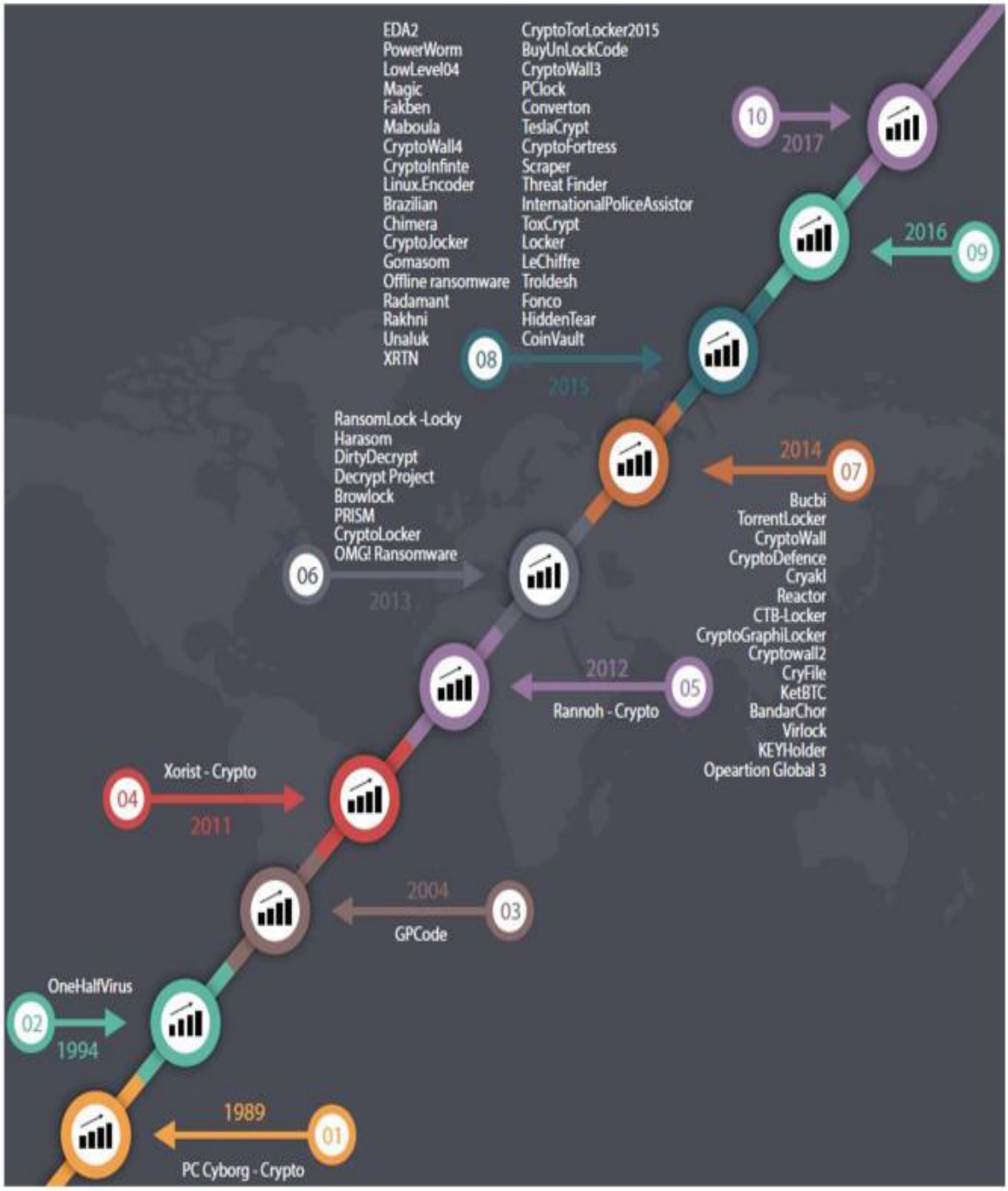
2.7.1 O Surgimento do Ransomware e sua Evolução.

O *ransomware* foi uma maneira encontrada pelos criminosos virtuais de ganhar fama e dinheiro. O crescimento da utilização de moedas virtuais aumentou de maneira considerável os ataques com o *malware*, sendo a principal forma de pagamento aos criminosos. (ZAKARIA, *et al,* 2017).

A figura 2 mostra a evolução em um curto período de tempo dos *ransomware* e sua família. O primeiro ataque de *ransomware* ocorreu no ano de 1989 com um *malware* chamado de *“PC cyborg”*, após cinco anos em 2004 outro ataque de expressão foi detectado com o nome de *“GPCode*” e o mesmo marcou sua época, de lá pra cá todos os anos novos tipos de *ransomware* são criados todos os anos e cada vez mais inteligentes. Ainda observando a figura 2, é possível notar o aumento de *ransomwares,* a evolução com o passar dos anos e o nome de alguns *malwares* mais

populares, tais como: *TorrentLocker, CryptoDefence, CryFile, KetBTC, Virlock, Cryptowall2, Cryakl, Reactor.* (CHITTOOPARAMBIL *et al*, 2018).

Figura 2- Linha do Tempo dos Ransomware.



Fonte: (CHITTOOPARAMBIL *et al*, 2018).

2.7.2 Características de um Ransomware:

Através das características listadas a seguir é possível diferençar o *ransomware* de outros tipos de *malwares,* são elas:

- Criptografia forte, o que faz com que você não consiga descriptografar os dados sem utilizar uma ferramenta específica para obter os dados.
- Possui Habilidade para criptografar diversos tipos de arquivos, como áudio, documentos, certificados, imagens.
- Ele faz um embaralhamento dos dados criptografados e isso faz com que seu sistema fique vulnerável.
- Muda os tipos de extensões de arquivos.
- Apresenta uma imagem solicitando resgate dos dados encriptados, normalmente na tela principal do sistema operacional.
- Pagamentos de resgate dos dados normalmente são realizados através de *Bitcoin*, moeda virtual.

Normalmente se utilizam do *The Union Routing* (TOR) que proporciona uma navegação anônima de criptografia, através deste navegador os invasores podem esconder-se da vigilância de rede, fornece também o *ransomware* com um serviço *(RaaS)*, esta plataforma pode ser personalizada e tratada pelos invasores.

Utiliza-se técnicas de evasão através de ofuscação complexa, dificultando que antivírus os detectem. Causa perda das credenciais do usuário do dispositivo.

Através destes pontos podemos conhecer um pouco mais de características que podem ser utilizadas para identificação de um *ransomware* e possivelmente prevenir aos usuários de dispositivos *IoT*. (SYMANTEC, 2015).

2.7.3 Como pode ser infectado

Existem diversas maneiras de ataque, como: engenharia social, *emails* de *spam*, distribuição de *botnets*.

> Um *botnet* é uma rede de computadores que foram infectados por *softwares* maliciosos e podem ser controlados remotamente, obrigando-os a enviar *spam*, espalhar vírus ou executar ataques de Distribute Denial of Service (*DDos)* sem o conhecimento ou o consentimento dos seus donos. O processo de infecção é rápido, e pode ser feito através do que eles chamam de recrutamento, ao executar um programa malicioso, pode ser infectado,

> também através de vulnerabilidades do navegador, downloads de *softwares* maliciosos. (AVAST, 2019).

Que podem direcionar as vítimas para sites maliciosos, onde podem ser utilizados códigos *exploits*, explorando as vulnerabilidades dos sistemas contra ataques de ransomware, permitindo que ele seja baixado no dispositivo. (ZAKARIA, *et al,* 2017).

2.7.4 Etapas de um Ataque Ransomware

Existem algumas fases que o *ransomware* passa até chegar ao momento da extorsão ao usuário, abaixo estão detalhadas tais etapas:

1º Exploração e infecção do ransomware:

Neste processo ele se instalará em uma pasta onde ele adiciona um arquivo com um nome aleatório e remove todos os executáveis do sistema. Em seguida ele cria um novo arquivo e atualiza a chave do registro. Desta forma ele garante que quando o arquivo for executado ele tenha total controle sobre ele, como variáveis locais, parâmetros de ajustes e outros. Executando de maneira segura, para que não possa ser descoberto e tenha controle sobre a aplicação. (BREWER, 2016).

2º Entrega e execução:

Começa a agir buscando os arquivos pessoais do usuário. Se faz necessário que o *malware* se conecte a um servidor de controle e comando, para ele estabelecer essa comunicação é usada uma rede que o deixe praticamente invisível. Usando o The Union Routing The Union Routing (*Tor)*, (TOR, 2021). Um navegador que fornece esse acesso a essa rede que permita que ele fique camuflado. Desta forma ele pega a chave criptográfica que é enviada pelo servidor, com a chave em mãos agora o *ransomware* pode criptografar os dados da vítima. (BREWER, 2016).

3º Apropriação de backup:

O *malware* realiza busca por arquivos de *backup* e pastas dos sistemas e removendo-os, desta maneira tentando dificultar a restauração do sistema através de um *backup*, e isso acontece com mais ênfase em sistemas *windows*, que é um dos sistemas mais atacado pelo *ransomware*. (BREWER, 2016).

4º Criptografia dos Arquivos:

Onde é realizada a criptografia dos arquivos, deixando os arquivos no computador do usuário, porém inacessíveis. Ele usa tags específicas para cada ataque, desta forma ele consegue diferenciar, com o aumento do conhecimento dos cybers criminosos, eles começaram a usar chaves com base na criptografia Advanced Encrytion Algorithm (AES) AES 256, considerada um tipo forte, dificultando que um usuário comum quebre por conta própria. Mas nem sempre a criptografia é realizada em servidores externos, existem tipos de ransomware que realizam a criptografia localmente, como no caso no *malware* SamSam. (BREWER, 2016).

> Este ransomware tem um comportamento muito peculiar se diferenciando dos outros, sua forma de ataque é mais objetiva, não sendo atacada através de e-mails (maneira mais comum de ser atacado por um ransomware). Seu método de ataque é manual, os harckers invadem o sistema manualmente através do conhecimento prévio sobre sua vítima e se esquivando de sistemas de segurança. O seu nível de periculosidade é bastante alto, justamente pelo fato de seu ataque ser feito de maneira manual pelo atacante, ele certifica-se de que os arquivos e máquinas estão realmente sendo criptografados e impedindo o processo de backup do dispositivo. Esse tipo de ataque é mais comum em organizações de grande porte. (SYMANTEC,2018).

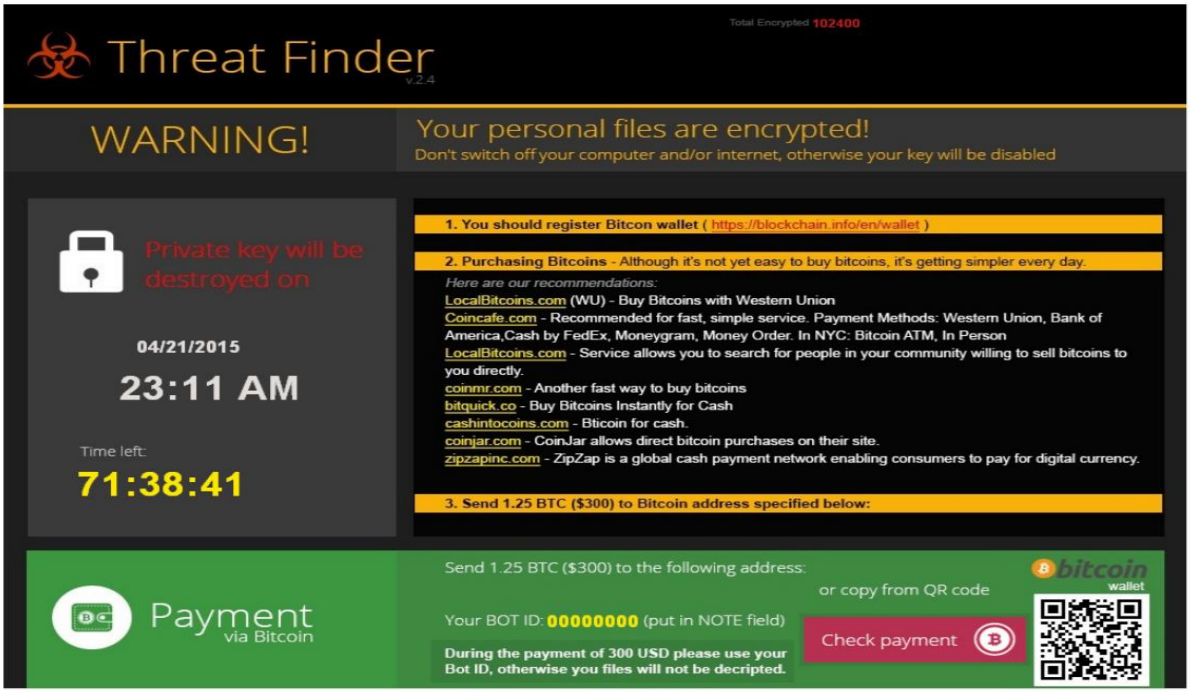
5º Notificação e Limpeza:

O usuário é notificado que foi infectado, e que precisa realizar o pagamento do valor caso queira reaver seus arquivos pessoais, dentro de um período de tempo determinado pelos criminosos. As instruções de como realizar o pagamento

normalmente aparecem em arquivos tipo texto nas pastas dos arquivos encriptados ou numa tela na área de trabalho do usuário, da mesma forma que diz qual o tipo de *ransomware* que o atacou. O pagamento que é realizado normalmente em uma conexão através de um navegador da *DeepWeb* onde seu rastreio é muito difícil. Após o pagamento o *malware* deixa o dispositivo sem deixar rastros do criminoso. (BREWER, 2016).

Na figura 3 é possível ver algumas das telas de como o dispositivo infectado mostra, nela é possível ver o aviso de que os arquivos do proprietário foram criptografados e que para reaver seus arquivos pessoais novamente (chave para decifrar os arquivos), será necessário realizar um pagamento, no caso da imagem em questão em *bitcoins* (moedas virtuais), que estão em alta.

Figura 3 - Um modelo de tela de notificação de ataque.



Fonte: (SYMANTEC, 2015).

3 ANÁLISE DE TRABALHOS

A análise documental é uma operação que se realiza sobre os documentos pertencentes a um determinado conjunto e tem como objetivo obter uma representação de cada um deles que permita encontrar e recuperar o documento de acordo com critérios previstos e informar sobre o mesmo por meio de uma interface adequada. Essas representações, mais manejáveis que o original, podem substituir o documento no processo documental (MATOS, 2015).

Díaz, Carmen e Lacruz (2010) corrobora com tal definição, entendendo que a análise documental tem como objetivo primordial a recuperação dos documentos a partir de distintos critérios morfológicos ou temáticos, geralmente normalizados. Analisa-se o documento, desta perspectiva, para que “apareça” quando seja necessário. A análise documental permite controlar os documentos por meio de suas representações, ou seja, informar sobre eles sem ir diretamente a eles.

3.1 Artigos Analisados

Os estudos analisados a seguir, constroem a base da minha pesquisa constatando o motivo da escolha do tema. Com dados quantitativos e qualitativos.

A primeira análise feita demonstra a insegurança dos usuários que possuem dispositivos *IoT,* por todo o mundo*.* Os demais trabalhos apresentam pontos de vulnerabilidades juntamente com métodos de detecção e prevenção de ataques.

3.1.1 O Futuro da Privacidade de Segurança de dados preocupa a internet das coisas.

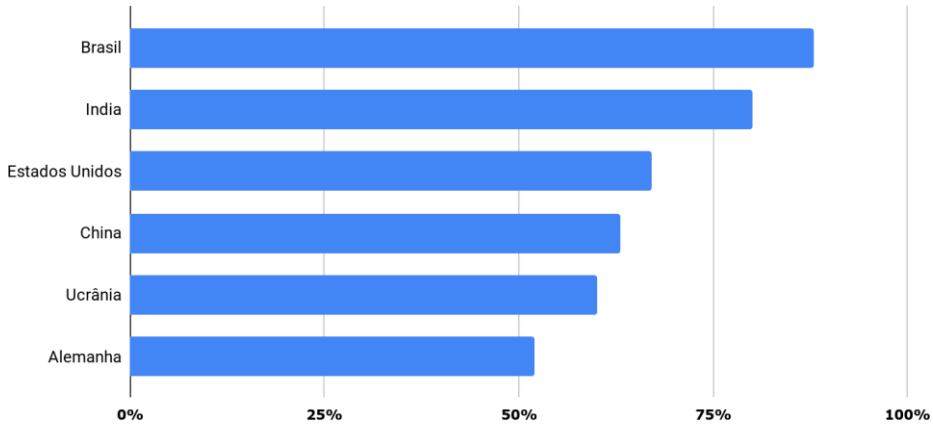
Será traçado a seguir uma análise sobre o estudo de (SOLANGI *et al*., 2018). No artigo são levantados pontos de vulnerabilidades e traz os conceitos de segurança ponta a ponta e questões de privacidades em ambientes distribuídos. A utilização de *IoT* para aplicações de assistência médica é algo que vai ser muito investido nas próximas décadas, a assistência à saúde reforça ainda mais o cuidado que será necessário com a segurança destes dispositivos. Sensores que mandam

informações de como está o estado atual do paciente, que pode ser monitorado de centrais médicas, ou até mesmo de monitoramento da tela de seu próprio *smartphone*.

O fato de estar no meio de uma rede não heterogênea permite questionar pontos como privacidade, vulnerabilidade e segurança, contra ameaças invisíveis. De acordo com o artigo, alguns pontos de vulnerabilidades como autenticação, integridade de dados, acesso não permitido aos dados são alguns dos desafios encontrados neste novo mundo criado dos dispositivos *IoT*. Um ponto levado em consideração é que os aparelhos *IoT* não são equipados com periféricos como computadores pessoais. Eles utilizam sensores, devido a isso, muitas pessoas acreditam ser confiável.

A seguir na figura 4, é possível observar uma crescente preocupação dos proprietários de dispositivos inteligentes, em países selecionados que estão preocupados com a invasão dos equipamentos

Figura 4 - Países onde proprietários estão preocupados com invasões em *IoTs*.



Fonte: (SOLANGI *et al.*, 2018)

De acordo com a pesquisa global sobre segurança do consumidor de dispositivos *IoT,* demonstra que cerca de 78% das pessoas que utilizam aplicações deste tipo de equipamentos. Tem receio de serem *hakeados* e 90% concordaram em ter algum tipo de dispositivo mecânico de segurança para evitar possíveis ataques cibernéticos. (IRDETO, 2017).

Outra problemática apresentada no estudo, é o grande quantitativo de dados gerados por estes mecanismos. Cerca de 500 bilhões destes dispositivos estarão em operação até 2025. (IRDETO, 2017). Como isto, o estudo exalta a preocupação de dados compartilhados e cita exemplos como: dados compartilhados entre médico e paciente, compartilhamento de dados de caminhada, o perfil público indesejado, isto significa o compartilhamento de informações pessoais dos usuários para análise de crédito por exemplo.

Contudo, os pontos frisados neste artigo têm ênfase na vulnerabilidade que as pessoas que se utilizam de dispositivos *IoT* estão expostas. Evidenciando assim, a importância de intensificar os padrões de segurança e privacidade para garantir que esse mercado cresça de maneira ordenada e mais segura possível.

O estudo supracitado, expõe vulnerabilidades e insegurança dos consumidores, devido ao compartilhamento de dados. Devido a isto, foi proposto que os próximos sistemas possuam a capacidade de relatar possíveis problemas em relação aos princípios da segurança da informação. Outro aspecto para o aumento da segurança seria melhorar a identificação e reconhecimento dos donos ou responsáveis, pelos aparelhos inteligentes.

O estudo conclui, frisando a importância de se investir em segurança para estes dispositivos. De forma que a responsabilidade não seja apenas do desenvolvedor, mas toda a sociedade envolvida, mesmo que seja de maneira direta ou indireta.

3.1.2 Internet of Things Security: A Survey.

Na pesquisa de (M.SADEEQ, *et Al*. 2018) ele traz 2 algoritmos propostos no estudo de (ATZORI, 2017), que podem solucionar o problema de performance em sistemas *IoT,* ambos visam ter alto desempenho para dispositivos que não possuam um *hardware* robusto como por exemplo, microcontroladores. Um dos algoritmos implementado é de alto desempenho e necessita de consumo de memória mais elevado. Que necessita de uma codificação maior e de mais recursos para sua execução. Enquanto o segundo algoritmo é um pouco mais lento, porém não necessita de tantos recursos para poder ser executado. Ambos algoritmos podem funcionar em tempo de execução, os dois tem capacidade para defender contra ataques de temporização e *SPA*. O autor monta uma tabela descritiva citando alguns

algoritmos e suas aplicabilidades. Na tabela1 é possível observar alguns algoritmos, bem como objetivos alcançados.

Tabela 1 - Áreas de ataques em IoT, e algoritmos eficazes para estes ataques.

Pesquisador	**Campo Aplicação**	**Ferramenta Usada**	**Algoritmos de Segurança**	**Objetivos satisfatórios**
Liu, Z., et al.	Cuidados com saúde	---------	MOTE-ECC, cryptography-RSA	família emergente de curvas elípticas leves adequadas para IoT.
Zhou, R., et Al.	Industrial	IND-sF-CKA, IND-sF-KGA	Keygen	Sistema Fc-MKA-KSE para compartilhamento de dados IIoT e pesquisa de dados autorizada.
Cheng, C., et Al.	Commercial	Public & private key	Cryptosystem	quantum resistant algorithms for securing communication in the IoT.
Xu, R., et al.	Industrial	----------	Cryptography, quantum computers	criptografia baseada em treliça é uma escolha adequada para IoT inteligente.

Fonte: (M.SADEEQ, et Al. 2018).

Os pesquisadores citam o estudo de (GAJ, 2018), que sugere uma alternativa de segurança utilizando o conceito de *blockchain.* O termo *blockchain* diz respeito a ter vários registros de transações espalhadas por diversos computadores, isso faz com que exista uma maior dificuldade trabalho para obter os dados. Como o próprio nome diz, no *blockchain* os dados são armazenados em blocos e estes blocos possuem chaves de ligações que são “*hash*” de uma maneira mais simples são códigos criptografados, que são “chaves” que servem para ter acesso aos blocos. Permitindo desta maneira, realizar transações complexas de maneira segura através de técnicas criptográficas. (SILVA, 2017).

Levando-se em consideração a grande variedade de aparelhos criados em um curto período de tempo. O controle de segurança e de identificação de riscos, não

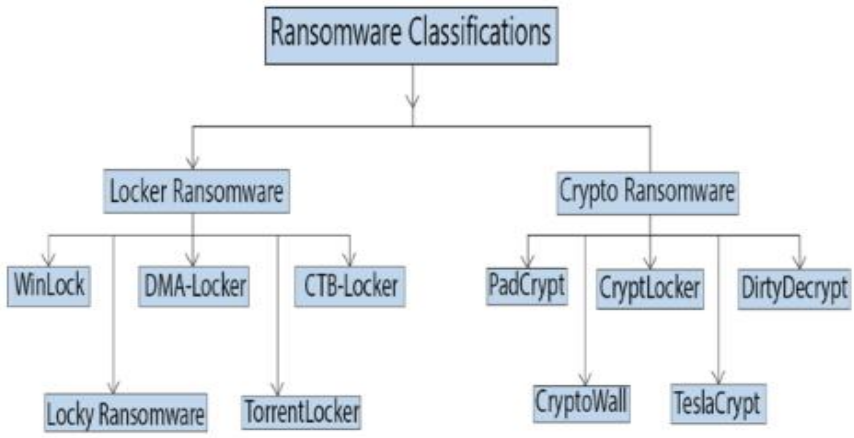
conseguem acompanhar de forma hábil. Um outro desafio apresentado é a criação de um algoritmo de criptografia leve e eficaz para ser utilizado nos dispositivos, tendo em consideração que normalmente os dispositivos *IoT* tem algumas limitações como: poder de processamento, energia, memória. (M.SADEEQ, *et Al.* 2018).

Com isso são apresentados estudos de algoritmos que podem ser utilizados em aplicações inteligentes, tendo foco a proteção dos dispositivos. Contudo, ainda são encontradas dificuldades para que essa disseminação de algoritmos seja amplamente utilizada.

3.1.3 IoT Based Ransomware Growth Rate Evaluation and Detection Using Command and Control Blacklisting.

O próximo trabalho analisado é de (ZAHRA; SHAH, 2017) onde é enfatizada a importância de reforço na segurança e um estudo mais aprofundado sobre o tema. Esta pesquisa tem como foco a prevenção contra ataques de *ransomware* aos dispositivos de internet das coisas. Ele apresenta dados que demonstram que cerca de 70% dos dispositivos conectados à internet são vulneráveis a ataques. Na figura 5 é observado a classificação da família do *ransomware.*

Figura 5 - Árvore de Classificação da família de Ransomware.



Fonte: (ZAHRA, SHAH, 2017).

Como observado na figura acima os *ransomware são classificados em dois grupos, sendo eles: Locker ransomware, Crypto ransomware*.

(ZAHRA; SHAH, 2017) descreve em partes como os hackers podem acessar um dispositivo que esteja dentro de uma rede *IoT*, na rede *TCP/IP*:

Primeiro o invasor manda requisições ao servidor proxy hacker, com o intuito de descobrir o *ip* da vítima, após receber o *ip* ele envia essa informação como um identificador único ao servidor de controle e comando.

O autor relata que o servidor Controle e Comando (C&C) desempenha o papel de um *backbone*[1] na comunicação. Após receber o *ip* enviado pelo *hacker* o servidor de controle e comando estabiliza a comunicação com o dispositivo *IoT,* o qual ele tem o seu endereço, em seguida o serviço de *C&C* manda uma chave pública com o objetivo de criptografar os dados que estão no dispositivo.

Após todos os passos anteriores serem executados com sucesso, o servidor de *C&C* envia um *link* com um endereço na *deepweb,* onde é enviado instruções de como pode ser realizado o pagamento para obter resgate dos dados criptografados por ele. Sua ideia é que no momento em que o servidor *C&C* estabelece comunicação com o dispositivo da vítima, o seu modelo extrai o cabeçalho *TCP/IP* de todas as solicitações recebidas, juntamente ao extrair o cabeçalho ele extrai os *ips* de destino e origem. Em seguida os armazena temporariamente em uma lista negra do servidor *C&C* para combinar o *ip*, se um dos *ips* de destino ou origem estiverem na lista negra do servidor de controle e comando a conexão será cortada.

Um problema relatado pelo autor é que para que a detecção e o controle seguro funcionem, é necessário ter os endereços adicionado à lista negra. Desta forma novas requisições ou *ips* desconhecidos poderão ser tratados, não permitindo um acesso indevido ao mesmo.

Concluindo o autor mostra que houve uma taxa de crescimento de cerca 670% para o *cryptowall*, 350% para o *locky ransomware*, 179% para o *CBT-Locker*, 7% para o *ceber*. Estas são algumas das ameaças que vem se destacando com o passar dos anos e merecem ser estudadas com mais atenção.

[1] O *Blackbone*, que significa espinha dorsal, utilizado para identificar a principal rede pela qual todos os dados de um cliente passa.

4 TÉCNICAS DE PREVENÇÃO

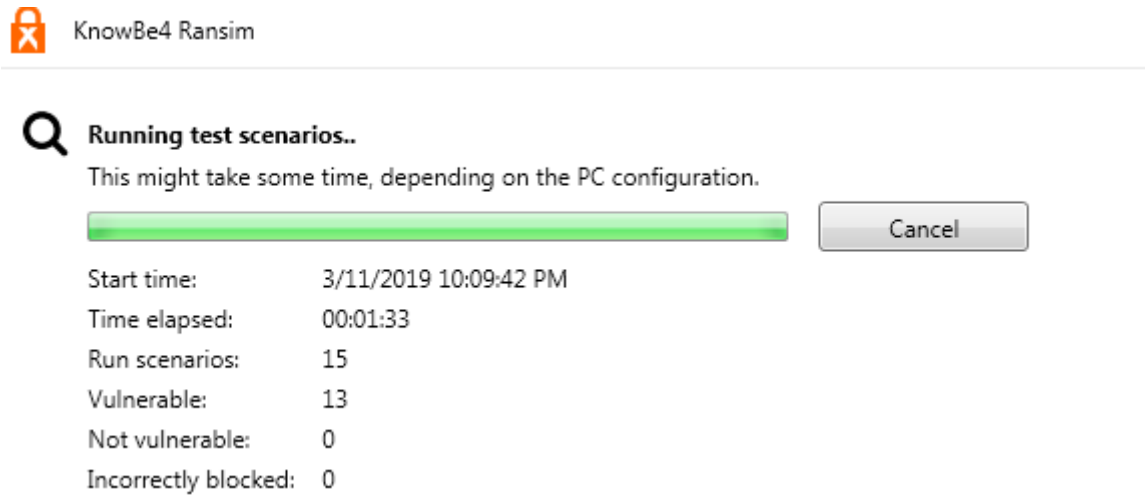
Neste capítulo serão explicadas as principais tecnologias e ferramentas utilizadas para detectar e prevenir possíveis ataques de *ransomware* em dispositivos *IoT.* Para análise foi realizada a busca por métodos de detecção, como *softwares* capazes de realizar verificação de pontos de vulnerabilidades e através disso ver qual método se aplica para realizar a prevenção contra tal problema, além de utilizar as informações disponibilizadas pelo software para auxílio na análise de um *ransomware.*

4.1 Ransim

É um *software* gratuito que pode verificar a rede onde o dispositivo está conectado e traçar os pontos onde o *malware* pode atacar. Este *software* é responsável por realizar simulação de ataques de *ransomware* e desta forma mostrar pontos de vulnerabilidades no dispositivo. É capaz de simular vinte cenários de infecção com *ransomware* e um cenário de criptografia, totalizando 21 cenários. Listando através de sua interface as brechas encontradas em sua rede. (KNOWBE4, 2020).

A seguir na figura 6 é possível ver o seu funcionamento e as vulnerabilidades encontradas em um dispositivo. A simulação foi realizada dentro de um ambiente controlado para exemplificar os problemas.

Figura 6 - Simulação de cenários de vulnerabilidades com ataques *ransomware*.



Fonte: O Autor (2019).

Alguns dos cenários simulados e seus efeitos são:

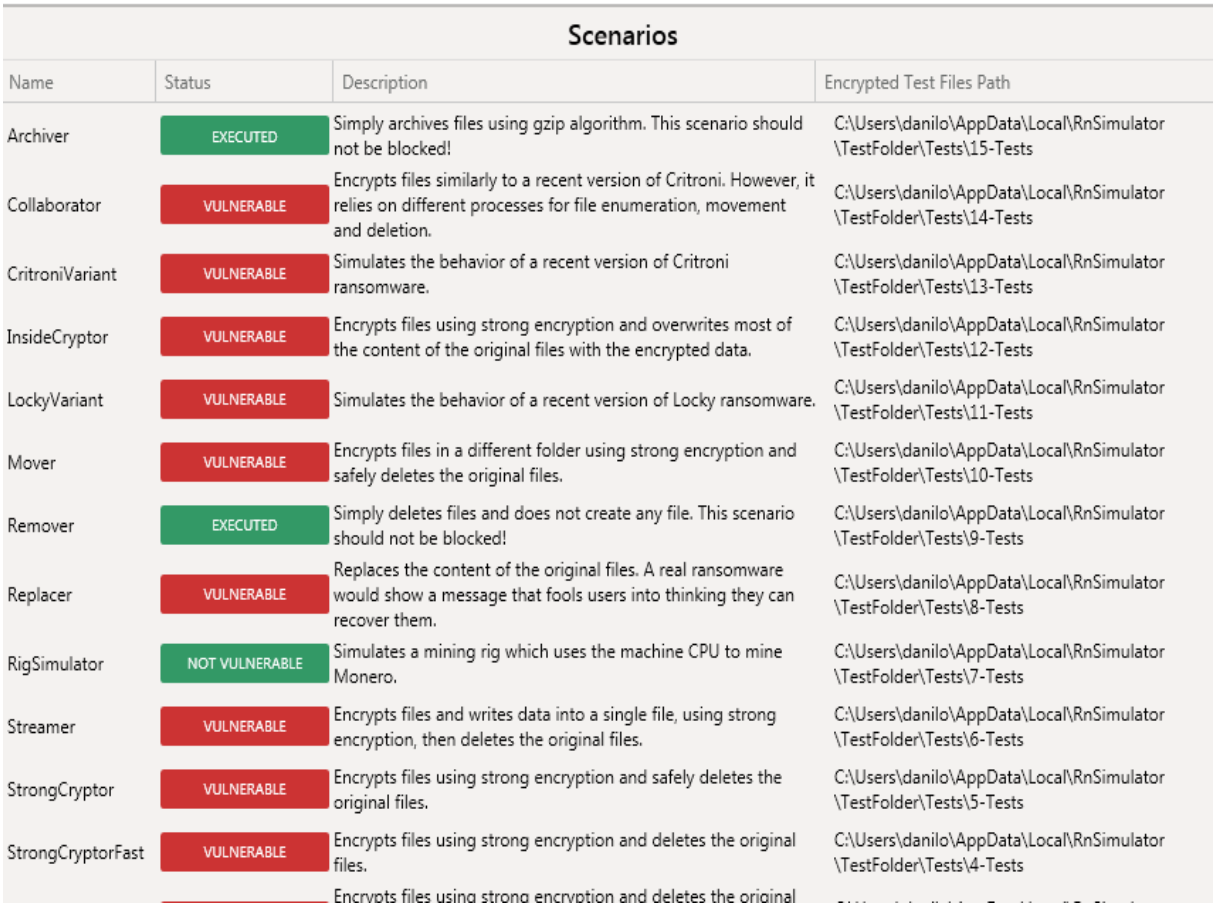
- *LockyVariant*: realiza a simulação da versão mais recente do *locky ransomware*, o qual tem como objetivo encriptar arquivos encontrados no dispositivo.
- Remover: um ataque que apenas remove os arquivos da vítima, não realizando sequer uma cópia criptografada, como é de costume de ataques deste m*alware.*
- *InsideCryptor:* Encripta os arquivos utilizando um tipo forte de criptografia, sobrescrevendo a maior parte do conteúdo original dos arquivos por dados criptografados.
- *Streamer*: Grava os dados do arquivo em um único arquivo em seguida criptografa o arquivo e remove o arquivo original.
- *Replacer:* Encripta o conteúdo dos arquivos originais, neste momento, um *ransomware* verdadeiro mostraria uma mensagem em seguida dizendo que os usuários poderiam recuperá-lo e que para isso precisam realizar o pagamento.
- *Collaborator*: Simula a encriptação de arquivos simulando uma recente versão do *Criptoni However* que realiza uma enumeração dos arquivos diferentes, movimenta e remove arquivos.

Esses são alguns dos ataques simulados pelo *software*. Possibilitando identificar onde existem vulnerabilidades e quis tipos ataques ele está suscetível.

Após identificar locais e tipos de ataques que o dispositivo está propenso, foi realizada uma análise estática com base nas informações apresentadas pela ferramenta, tais como nome do *malware*, sua família e perfil para estudo.

Na Figura 7, pode ser visto como o programa apresenta o resultado ao usuário. Enumerando as vulnerabilidades onde a simulação não obteve sucesso e onde a simulação conseguiu danificar os dados do usuario, quantidade de arquivos que estão vulneráveis e quais tipos de arquivos são estes. Sejam eles documentos, imagens, vídeos entre outros arquivos, bem como através dos nomes dos *malwares* identificar sua família e com base nisso traçar um padrão de análise para criação de métodos de prevenção.

Figura 7- Simulação de ataques de *ransomware*.



Scenarios

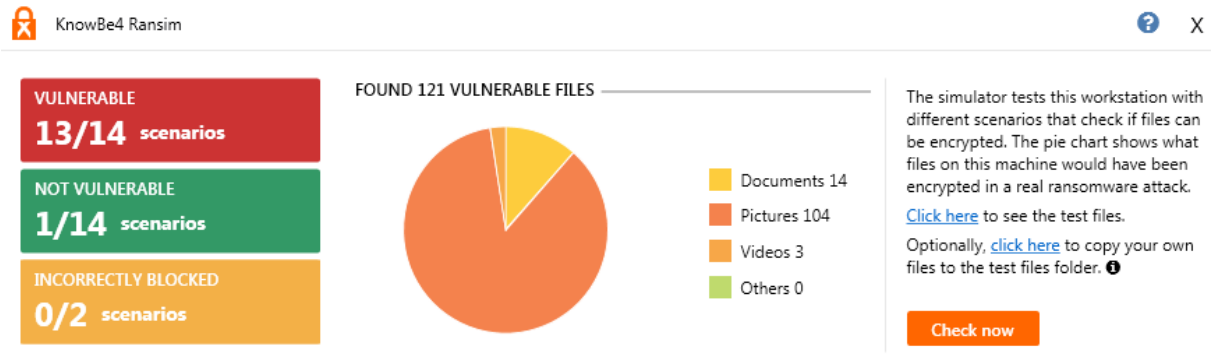
Name	Status	Description	Encrypted Test Files Path
Archiver	EXECUTED	Simply archives files using gzip algorithm. This scenario should not be blocked!	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\15-Tests
Collaborator	VULNERABLE	Encrypts files similarly to a recent version of Critroni. However, it relies on different processes for file enumeration, movement and deletion.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\14-Tests
CritroniVariant	VULNERABLE	Simulates the behavior of a recent version of Critroni ransomware.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\13-Tests
InsideCryptor	VULNERABLE	Encrypts files using strong encryption and overwrites most of the content of the original files with the encrypted data.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\12-Tests
LockyVariant	VULNERABLE	Simulates the behavior of a recent version of Locky ransomware.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\11-Tests
Mover	VULNERABLE	Encrypts files in a different folder using strong encryption and safely deletes the original files.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\10-Tests
Remover	EXECUTED	Simply deletes files and does not create any file. This scenario should not be blocked!	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\9-Tests
Replacer	VULNERABLE	Replaces the content of the original files. A real ransomware would show a message that fools users into thinking they can recover them.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\8-Tests
RigSimulator	NOT VULNERABLE	Simulates a mining rig which uses the machine CPU to mine Monero.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\7-Tests
Streamer	VULNERABLE	Encrypts files and writes data into a single file, using strong encryption, then deletes the original files.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\6-Tests
StrongCryptor	VULNERABLE	Encrypts files using strong encryption and safely deletes the original files.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\5-Tests
StrongCryptorFast	VULNERABLE	Encrypts files using strong encryption and deletes the original files.	C:\Users\danilo\AppData\Local\RnSimulator \TestFolder\Tests\4-Tests
		Encrypts files using strong encryption and deletes the original	

Fonte: O Autor (2019) sobre ferramenta específica

Uma grande vantagem do *software* é sua fácil utilização, não necessitando de um conhecimento aprofundado do mesmo para poder utilizá-lo.

Na Figura 8, pode ser observado como o programa apresenta o resultado ao usuário. Enumerando as vulnerabilidades onde a simulação não obteve sucesso e onde a simulação conseguiu danificar os dados do usuário, a quantidade de arquivos que estão vulneráveis e quais tipos de arquivos são estes, sejam eles documentos, imagens, vídeos entre outros.

Figura 8 - Resultado da Simulação de ataques de *ransomware*.



Fonte: O Autor (2019) sobre ferramenta Ransim.

4.2 Análise Estática

É o processo de análise de estrutura de um código ou programa onde é possível encontrar pontos que possam auxiliar na detecção e prevenção contra ataques. Esse tipo de análise serve para que possamos identificar padrões que possam auxiliar na detecção de *malwares* e de alguma maneira proteger os dispositivos contra ataques. Esse tipo de análise é bastante segura pois não está executando o código propriamente dito. (AISAWA, *et al*, 2019).

Após esta análise, foi feita a avaliação do tipo dinâmica, ou seja em “tempo de execução”, onde podemos ir dando comandos para avaliação do código.

Foi realizada uma análise de estrutura, através do *Portable Executable* (PE), que possui as seguintes estruturas: (MICROSOFT, 2020).

- Cabeçalho Mark Zbikowski (MZ) DOS;
- Fragmento (stub) DOS do arquivo PE;
- Cabeçalho da imagem opcional;
- Tabelas de seções (que possui uma lista de cabeçalhos de seção);
- Diretório de dados (onde ficam os ponteiros para as seções);
- Sessões propriamente ditas.

Toda essa estrutura que compõe o arquivo, foi analisada que para ser um arquivo executável. Existe uma informação importante que pode ser encontrada no cabeçalho *Disk Operation System* (*DOS*), os dois primeiros *bytes* do cabeçalho

constam a assinatura que identifica o tipo de arquivo, para um tipo executável sempre tem início com “MZ” que hexadecimal seria (4D 5A), o *MZ* é uma referência ao Mark Zbikowski criador do executável *DOS*. (SOUZA, 2016).

O *PE Header* contém a assinatura do arquivo executável, desta maneira é possível identificar em qual sistema ele poderá ser executado. Na nossa análise iremos partir para as sessões, pois aqui é onde ficam os dados dos arquivos. As sessões podem conter o código compilado do arquivo ou chamadas a programas específicos, instruções em binário. As sessões podem ser divididas em etapas como: *TEXT/CODE, RDATA, DATA, RSRC*. (ANDERSON, ROTH, 2018).

A seguir foi realizado uma análise em alguns *malwares* dentro de um ambiente controlado para identificar algumas características que possam ser utilizadas como base para criar algoritmos de defesa ou até mesmo adotar outras medidas a fim de, proteger os dispositivos contra possíveis ataques.

Na figura 9, é possível ver alguns *malwares* analisados como o locky e jigsaw.

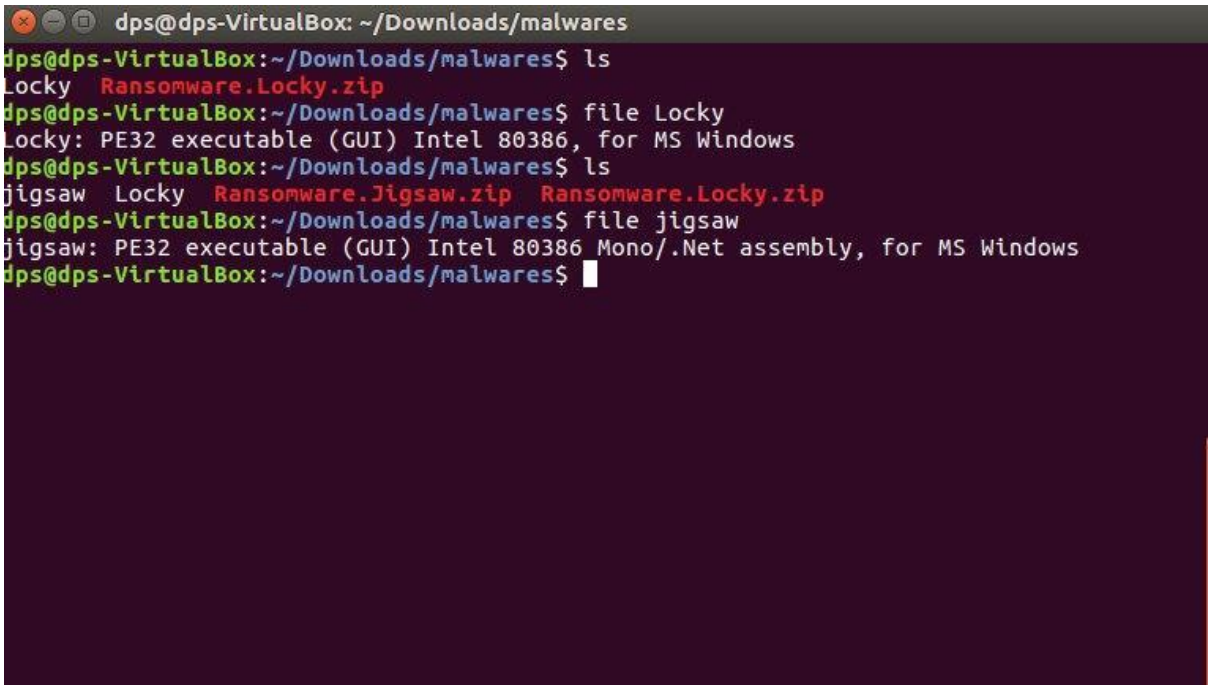
Foi utilizado o comando de acordo com a seguinte sintaxe:

```
file <nome do malware>
```

Ao executar o comando acima é possível identificar qual tipo de arquivo. Se é um executável, uma *Dynamic-link library (DLL), txt* ou qualquer outro tipo. Nesta análise iremos apenas trabalhar com arquivos do formato *PE*. A execução da instrução retorna o tipo do arquivo, o processador onde o mesmo foi projetado para ser executado e para qual sistema foi criado. Neste caso usado para um dispositivo que tenha o sistema *windows*.

Através desta instrução é possível observar alguns pontos importantes tais quais os vistos na análise do *ransomware Jigsaw*. O nome deste *ransomware* se dá a uma referência ao filme conhecido aqui no Brasil como Jogos Mortais, pelo fato de quando o *malware* se estabelece coloca a imagem do palhaço, um personagem do filme de terror o qual seu nome faz referência. Na instrução é possível ver que o arquivo *PE* tem uma instrução de *DotNet* (.NET) em *assembly.*

Figura 9 – Análise de *malware* Jigsaw.



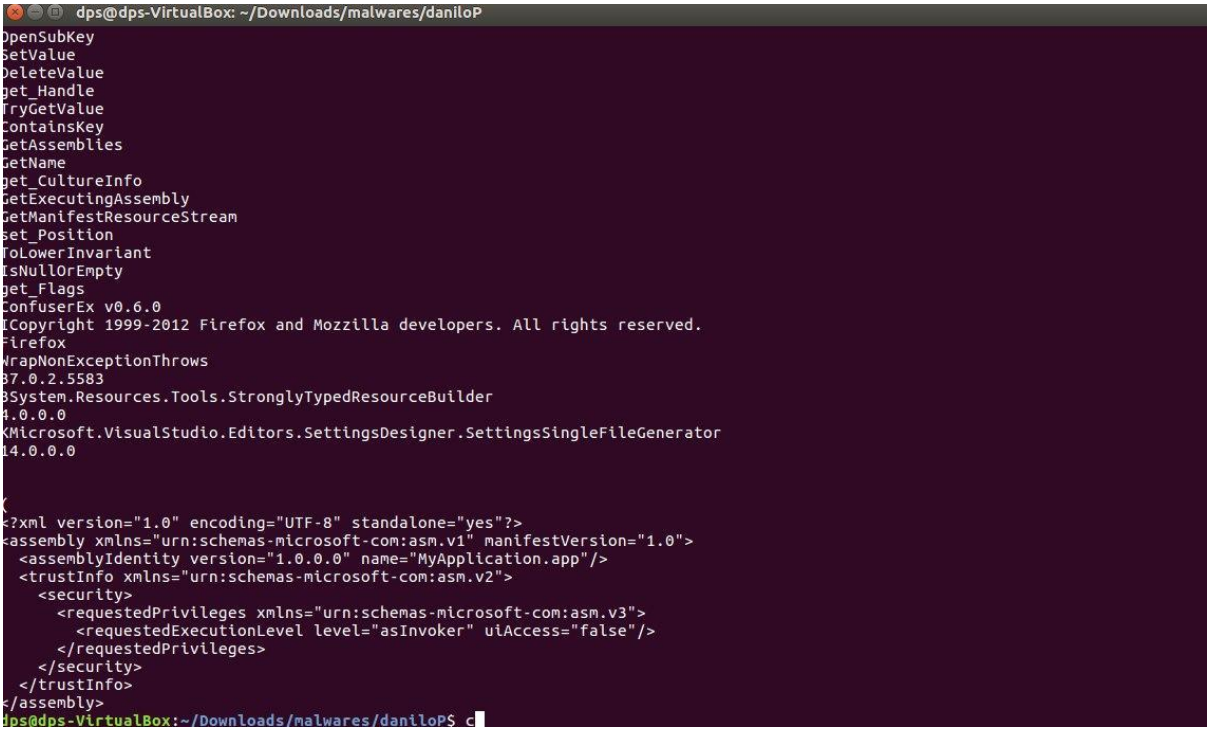
Fonte: O Autor (2019).

A seguir uma outra instrução utilizada para analisar arquivos *PE* seria utilizando o comando:

`strings -a  nome do arquivo analisado`

Desta forma é possível identificar também na figura 9, alguns pontos que podem auxiliar na identificação do *malware*. O comando auxilia para explorar o que é contido dentro das seções do *PE* e através disso é possível descobrir chamadas a instruções específicas e ver se o *malware* chama alguma *dll* ou algo que possa nos ajudar na análise. Muitos *ransomwares* utilizam-se desta técnica de tentar mascarar algumas chamadas de instruções dentro das seções com o intuito de não serem descobertos por programas de segurança como antivírus.

Figura 10 – Análise de Arquivo PE, buscando por palavras chaves.



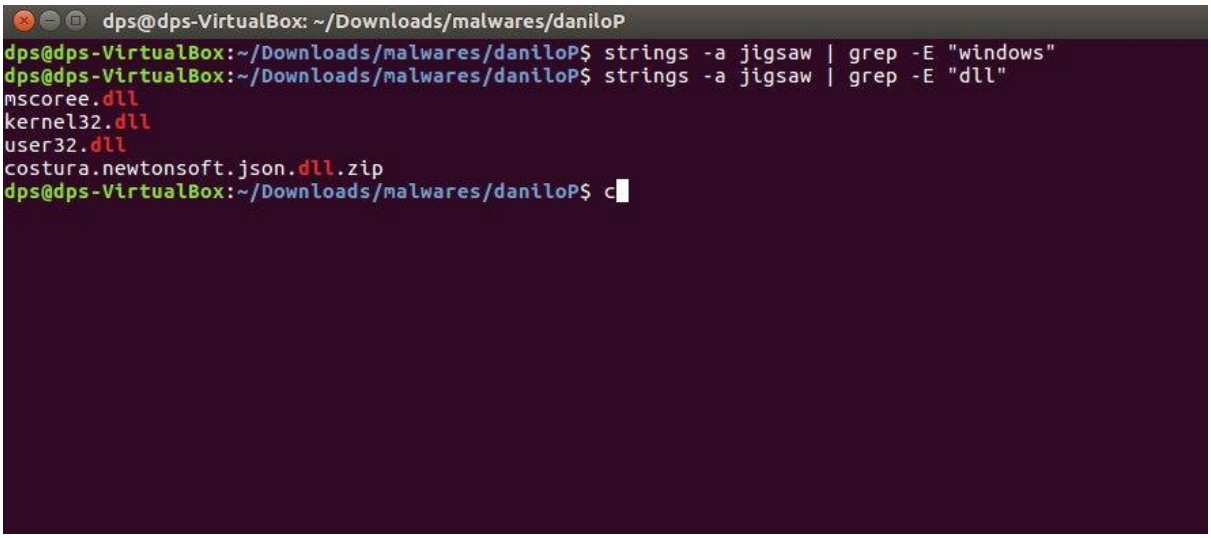
Fonte: O Autor (2019).

A partir disso, podemos utilizar um novo comando:

```
strings -a nome do ransomware  | grep -E "o que você está procurando"
```

Na figura 10, é possível ver pesquisa sendo realizada com a utilização de palavras chaves. Na primeira pesquisa não foi encontrado nada relacionado ao *windows* ou nenhuma chamada a alguma instrução, porém ao digitarmos *dll*, é possível identificar alguns arquivos sendo referenciados dentro do conteúdo apresentado. Dentre os achados, o que chama atenção é a *dll* costura.newtonsoft.dll.zip. Sendo um arquivo *dll* com um *.zip* no final, uma das formas utilizadas por *harckers* para mascarar instruções e chamadas maliciosas que resultem na danificação do dispositivo sem o antivírus ou qualquer outro *software* de análise de *malware detectar*. Também é importante mencionar as outras *dlls* que aparecem que são *dlls* importantes na execução do *windows*, o sistema para o qual este *ransomware* foi desenvolvido.

Figura 11– Busca e análise de instruções dentro do PE infectado.



Fonte: O Autor (2019).

As instruções apresentadas acima na figura 11, são de grande valia para analisar e conhecer um pouco mais sobre os *ransomwares*. Após um estudo mais aprofundado sobre suas estruturas e comportamentos através dos métodos apresentados durante o estudo, seria possível a criação de rotinas nos dispositivos que pudessem realizar buscas através de artefatos suspeitos com essas informações. Podendo auxiliar em possíveis ataques com base nos padrões estudados. É importante ressaltar que, ambos os pontos de análises são utilizados para o estudo analítico dos *malwares* em dispositivos.

5 DISCUSSÃO E COMPARAÇÃO

Este capítulo tem como objetivo realizar a discussão dos dados analisados através dos métodos adotados e ferramentas utilizadas para análise. E traçar um breve comparativo sobre qual método poderia ser utilizado em uma futura prevenção contra possíveis ataques de *ransomwares* a dispositivos *IoT*. Na simulação realizada pelo *Ransim* podemos constatar o quanto nossos dispositivos estão propensos e vulneráveis a ataques. Os testes foram todos realizados em ambientes controlados, tanto a simulação de ataques, com o intuito de identificar a quais vulnerabilidades que o dispositivo estava propenso, quanto a análise de *malware*, para tentarmos entender o seu comportamento e perfil. E a partir disso abrir margens para elaboração futura de um algoritmo para prevenção contra os ataques.

Os métodos apresentados no capítulo anterior demonstram a grande variedade de tipos de *ransomware* e algumas maneiras que podem ser utilizadas para sua identificação. Os dois métodos partem do princípio analítico, coletando informações para poder entender um pouco mais sobre o comportamento dos *malwares* e assim utilizar métodos eficazes para sua prevenção.

Os mesmos não deveriam ser utilizados de maneira isolada para a prevenção contra ataques, porém podem ser bastante eficazes se utilizados em conjunto e dependendo do que o usuário deseja realizar.

Com a lista de arquivos gerada pelo *ransim*, é possível identificar o tipo de *malware* que pode infectar aquela pasta, ou aquele arquivo. Desta maneira é possível providenciar soluções, como utilizar *softwares* de monitoramento e ferramentas de segurança. Atualmente é possível encontrar diversas ferramentas no mercado, com este propósito.

Porém como já abordado no decorrer da pesquisa. Existem muitos dispositivos que não possuem hardware com capacidade suficiente para utilizá-los.

O segundo método de análise apresentado mostra um pouco das estruturas de arquivos *PE*, que são utilizados para ataques aos dispositivos que o possuem. Desta maneira, também foi possível compreender melhor como um *ransomware* se comporta. Foi utilizado o conceito de *sandbox*, realizando testes e simulações em um ambiente controlado, o que possibilitou uma análise um pouco mais minuciosa.

Os arquivos *PE,* são utilizados por dispositivos que possuem o sistema operacional *windows*. Onde foi possível demonstrar que mesmo sistemas operacionais consolidados no mercado estão suscetíveis.

Após entender como funcionam os tipos de arquivos e o comportamento dos *ransomwares* é possível criar rotinas de execução com base em tais comandos para serem executados após a instalação de novos *softwares*, atualizações e downloads. A fim de detectar algum ponto suspeito na execução. A ação poderia ser finalizada através da rotina criada. Lembrando que este método por si só, não seria 100% eficaz, a chegada a esta conclusão é a criação de novos tipos diferentes de *ransomwares* em um curto período de tempo, como pode ser observado na pesquisa de (CHITTOPARAMBIL, *et al*. 2018).

(ZAHRA; SHAH, 2017) apresenta uma proposta de um outro método para a detecção de possíveis ataques na rede. Que pode ser utilizado em dispositivos em redes *TCP/IP*. Que é a criação de uma lista negra, propondo um método de detecção com base na análise de tráfego do *cryptowall*. Sua proposta é extrair o cabeçalho *TCP/IP* de todas as solicitações recebidas, fazendo isso para ambos os lados, tanto host de origem quanto o destino, armazenados temporariamente na lista negra. Caso um dos *ips* estejam na lista do servidor controle e comando a comunicação seria finalizada. Porém, esse método possui um problema, para que ele bloqueie a comunicação é necessário saber os endereços dos servidores *C&C*, caso esses *ips* sejam de novos servidores controle e comando ou sejam desconhecidos a técnica não seria aplicada da maneira correta. Não finalizando a comunicação e expondo o dispositivo atacado, porém isto não o torna inviável, mas para ter uma melhor eficiência teria que ser utilizado de maneira conjunta com algum outro tipo de método.

(BREWER, 2016) Cita mais algumas outras maneiras de detecção de *ransomwares,* os estudos com base no *cryptowall* e *locky*, o autor recomenda, criação de métodos de busca através da extensão .*locky* por exemplo, com o intuito de encontrar arquivos que estão sendo infectados no sistema. O mesmo pode ser utilizado para o *cryptowall*, porém desta maneira, já seria tarde porque diversos arquivos poderiam ter sido infectados. Além disto é necessário conhecer sobre os *malwares* previamente para que desta forma possa ser utilizado o conhecimento sobre os mesmos para realizar a busca. Seria necessário, por exemplo, saber o tipo de

criptografia utilizada para saber como e qual algoritmo seria mais eficiente. Falhas ou pontos de atenção que devem ser levados em consideração na análise.

No método de análise estática, apresentado por (BREWER, 2016) o autor defende o constante monitoramento da rede onde os dispositivos estão inseridos, utilizando os conhecimentos sobre as fases do ataque de um *ransomware*. Na etapa onde é realizada a criptografia de arquivos. Onde existe a troca de chaves entre o dispositivo e o servidor de controle e comando, podem ser detectadas através das assinaturas de rede e interceptadas. Além da mudança no nome de arquivos específicos e alterações de registro dos dispositivos dentro de uma mesma rede.

O *software ransim* juntamente com o método da lista negra apresentado por (ZAHRA; SHAH, 2017), apresentam propostas mais eficazes. Pois ambos permitem identificar ataques e vulnerabilidades antes de um possível ataque. Um dos problemas encontrados é que o *ransim* necessita de um sistema operacional em um dispositivo *IoT* onde sabemos que são mínimos.

6 CONCLUSÃO

Com o crescimento dos avanços tecnológicos na sociedade atual, o crescimento de dispositivos inteligentes passa a estar em todos os locais. A partir disto é necessário pensarmos na importância da segurança destes dispositivos. A fim de aprimorar e fortalecer o conhecimento no setor para prevenir ataques específicos quando necessário.

O estudo sobre os ataques de *ransomwares* em redes *TCP/IP*, não foi trivial. Foi necessário adquirir conhecimento sobre as vulnerabilidades dos dispositivos. A análise de *malwares* específicos são complexas, devido a sua constante evolução acarretando na necessidade de atualização contínua.

A pesquisa não tinha objetivo de criar um método de prevenção contra ataques, mas sim de realizar um estudo para entender melhor, como eles se comportam, seu crescimento, áreas onde estão inseridos, como pode ser infectado e como proteger os dispositivos em redes *TCP/IP*. Foi apresentado neste trabalho, ferramentas que possam auxiliar na identificação de alguns tipos de *ransomwares*, traçando um comparativo com outras pesquisas a fim de juntar em um trabalho futuro os conhecimentos adquiridos para criação e ou auxílio de ferramentas de segurança para dispositivos inteligentes.

Nenhum dos métodos citados são 100% eficazes. Podendo obter um melhor resultado através da unificação dos métodos. Criando uma ferramenta que possa auxiliar na detecção e prevenção de *ransomware,* com maior eficiência. Acredito que esta seria a maneira mais eficiente de se prevenir contra ataques, além de resolver problemas de vulnerabilidades e desafios nos dispositivos, como a criação de uma rede mais segura, utilização de *SO,* para que esses tipos de algoritmos sejam utilizados com eficácia.

REFERÊNCIAS

ABNT (Brasil). **Norma Técnica**. 2013. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306582. Acesso em: 18 maio. 2019.

AISAWA, A. A. *et al*. **Breve Comparação de Ferramentas para Análise Estática e Código Malicioso.** Acesso em: 10 jan. 2021.

ANDERSON, S. H. ROTH. P. 2018. **EMBER: An Open Dastaset for training static PE Malware Machine Learning Models.** Disponível em: https://arxiv.org/abs/1804.04637. Acesso em: 08 abr. 2020.

ATZORI, M. **Blockchain-based architectures for the internet of things: a survey**, 2017.

AZMOODEH, Amin *et al*. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. **J Ambient Intell Human Comput.** pp. 1-12. 23 ago. 2017. Disponível em: https://core.ac.uk/download/pdf/84653993.pdf. Acesso em: 5 jan. 2021.

BAKER, Stephanie B.; XIANG, Wei; ATKINSON, Ian. Internet of Things for Smart Healthcare Technologies, Challenges, and Opportunities. **Ieee Access**, [S.L.], v. 5, p. 26521-26544, 29 nov. 2017. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/access.2017.2775180. Disponível em: https://ieeexplore.ieee.org/document/8124196. Acesso em: 7 maio. 2019.

CASTILHO, Sérgio Duque; FONTE, Miguel Feitoza da. **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO APLICADA EM UMA INSTITUIÇÃO DE ENSINO MEDIANTE ANÁLISE DE RISCO**. 2012. 5 f. TCC (Graduação) - Curso de Análise e Desenvolvimento de Sistemas, Faculdade de Tecnologias de Ourinhos, Ourinhos, 2012. Disponível em: https://www.fatecourinhos.edu.br/retec/index.php/retec/article/download/99/144. Acesso em: 8 fev. 2019.

CISCO, **Cisco Annual Internet Report prevê que 5G será responsável por mais de 10% das conexões móveis no mundo em 2023.** 2020. Disponível em: https://news-blogs.cisco.com/americas/pt/2020/02/19/cisco-annual-internet-report-preve-que-5g-sera-responsavel-por-mais-de-10-das-conexoes-moveis-no-mundo-em-2023/ Acesso em: 15 dez. 2020.

COMPUTERWORLD, **Mercado Brasileiro de Ti está mais otimista e caminha para recuperação em 2021.** 2020 Disponível em:

https://computerworld.com.br/negocios/mercado-brasileiro-de-ti-esta-mais-otimista-e-caminha-para-recuperacao-em-2021/. Acesso em: 20 nov. 2020.

CHITTOOPARAMBIL, Helen Jose *et al*. A Review of Ransomware Families and Detection Methods. **Advances In Intelligent Systems And Computing**, [S.L.], v. 843, p. 588-597, 9 set. 2018. Springer International Publishing. http://dx.doi.org/10.1007/978-3-319-99007-1_55. Disponível em: https://link.springer.com/chapter/10.1007%2F978-3-319-99007-1_55. Acesso em: 05 jan. 2020.

DÍAZ, Raquel Gómez; CARMEN, María del; LACRUZ, Agustín. **Polisemias visuales. Aproximaciones a la alfabetización visual en la sociedad intercultural**. 167. ed. Salamanca: Colección Aquilafuente, 2010. 234 p. Disponível em: https://ur.b-ok.global/book/5576142/62f8fc. Acesso em: 06 jan. 2021.

FORBES, 2018. **10 Charts That Will challenge your perspective of IoT's growth.** Disponível em: https://www.forbes.com/sites/louiscolumbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/?sh=46a0b55e3ecc#79c388e3ecce,%20(accessed,%20March%2021,%202020). Acesso em: 07 de jan. 2021.

GAJ, K.: **Challenges and Rewards of Implementing and Benchmarking Post-Quantum Cryptography in Hardware, in Editor (Ed.)^(Eds.): Book Challenges and Rewards of Implementing and Benchmarking Post-Quantum Cryptography in Hardware** (ACM, 2018, edn.), pp. 359-364.

GOMES, Thales de Oliveira. **Segurança da Informação - Conceitos Fundamentais**. 2017. Disponível em: https://www.linkedin.com/pulse/seguran%C3%A7a-da-informa%C3%A7%C3%A3o-conceitos-fundamentais-de-oliveira-gomes/?originalSubdomain=pt. Acesso em: 30 maio. 2018.

HINTZBERGEN, Jule *et al***. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.** Rio de Janeiro: Brasport, 2018.

HUMAYUN, Mamoona *et al*. Internet of things and ransomware: Evolution, mitigationand prevention. **Egyptian Informatics Journal.** [S.I.]., p. 1-1. 28 maio 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S1110866520301304. Acesso em: 06 jan. 2021.

IRDETO, organization. **IRDETO GLOBAL CONSUMER PIRACY SURVEY**, 2017.

KNOWBE4. 2020. **Find out how vulnareble yout network is against ransomware and cryptomining attaks.** Disponível em: https://www.knowbe4.com/ransomware-simulator. Acesso em: 09 ago. 2020.

MATOS, Júlia Silveira. **ANÁLISE DOCUMENTAL**. [S.I.]., 2015. Color. Disponível em:http://repositorio.sead.furg.br/bitstream/123456789/1739/1/An%C3%A1lise_documental.pdf. Acesso em: 8 jan. 2021.
MCAFEE. 2021**.** **What is Ransomware**. Disponível em: https://www.mcafee.com/enterprise/pt-br/security-awareness/ransomware.html#how-it-works Acesso em: 06 jan. 2021.

MICROSOFT. 2020. **PE format**. Disponível em: https://docs.microsoft.com/en-us/windows/win32/debug/pe-format Acesso em: 08 de jan. 2021.

M.SADEEQ, Mohammed A. *et al*. Internet of Things Security A Survey. **2018 International Conference On Advanced Science And Engineering (Icoase)**, [S.L.], p. 1-1, out. 2018. IEEE. http://dx.doi.org/10.1109/icoase.2018.8548785. Disponível em: https://ieeexplore.ieee.org/document/8548785/authors#authors. Acesso em: 02 fev. 2020.

NIžETIć, Sandro, *et al*. Internet of Things (IoT): Opportunities, issues and challenges towardsa smart and sustainable future. **Journal Of Cleaner Production**, [S.L.], v. 274, 19 jul. 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S095965262032922X#undfig1. Acesso em: 06 jan. 2021.

NORTON, 2020. **Malware**. Disponível em: https://br.norton.com/internetsecurity-malware.html Acesso em: 02 maio. 2020.

POPPER, Marcos Antonio. **INTERNET DAS COISAS: POTENCIALIDADES E PERIGOS**. 2018. 20 f. TCC (Graduação) - Curso de Curso de Especialização em Gestão da Segurança da Informação, Universidade do Sul de Santa Catarina, Santa Catarina, 2018. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/3703/1/Marcos_Popper%5B48190-49065%5DAD6_versao_final_publicacao.pdf. Acesso em: 28 dez. 2020.

RIBEIRO, Raquel Maria Oliveira. **Segurança em IoT: simulação de ataque em uma rede RPL utilizando Contiki.** 2018. 70 f. TCC (Graduação) - Curso de Engenharia Eletrônica e Telecomunicações, Universidade Federal de Uberlândia Faculdade de Engenharia Elétrica Engenharia Eletrônica e de Telecomunicações, Patos de Minas, 2018.

RODRIGUES, Renato. **Brasil é o País com mais usuários atacados por phishing**. 2019. Disponível em: https://www.kaspersky.com.br/blog/brasil-ataques-phishing/11826/. Acesso em: 12 jun. 2019.

SILVA, Carlos Henrique Duarte da (Ed.). **Blockchain: o que é e como funciona?** Disponível em: https://www.ibm.com/blogs/systems/br-pt/2017/06/05/blockchain-o-que-e-e-como-funciona/ . Acesso em: 05 jun. 2017.

SOUZA, Victor Hugo de. **TÉCNICAS E FERRAMENTAS DE ANÁLISE VISUAL DE MALWARES**. 2016. 62 f. TCC (Graduação) - Curso de Engenheiro de Redes de Comunicação, Departamento de Engenharia Elétrica, Universidade de Brasilia,

Brasilia, 2017. Disponível em: https://bdm.unb.br/handle/10483/17092. Acesso em: 02 jan. 2021.

SUO, Hui, *et al*. Security in the Internet of Things A Review. **2012 International Conference On Computer Science And Electronics Engineering**, [S.L.], online, mar. 2012. IEEE. http://dx.doi.org/10.1109/iccsee.2012.373. Disponível em: https://ieeexplore.ieee.org/document/6188257/authors#authors. Acesso em: 11 ago. 2020.

SHROUF, F.; ORDIERES, J.; MIRAGLIOTTA, G.. Smart factories in Industry 4.0 A review of the concept and of energy management approached in production based on the Internet of Things paradigm. **2014 Ieee International Conference On Industrial Engineering And Engineering Management**, [S.L.], online, dez. 2014. IEEE. http://dx.doi.org/10.1109/ieem.2014.7058728. Disponível em: https://ieeexplore.ieee.org/abstract/document/7058728. Acesso em: 15 fev. 2020.

SMITH, Dave. **Say Hello to Android Things 1.0.** 2018. Disponível em: https://android-developers.googleblog.com/2018/05/say-hello-to-android-things-10.html Acesso em: 07 abr. 2018.

SYMANTEC**,** 2015. **The revolution of ransomware**. Disponível em: https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf. Acesso em: 20 abr. 2018.

SYMANTEC, 2018. **"Samsam: Target Ransomware Attacks Continue"**. Disponível em: https://symantec-blogs.broadcom.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks Acesso em: 03 mar. de 2020

TOR. 2021. **Navegue com Privacidade**. Disponível em: https://www.torproject.org/pt-BR/. Acesso em: 08 jan. 2021;

UNISYS (São Paulo). **Maioria dos brasileiros apoia utilização de dispositivos IoT para alerta de emergências, rastreamento de bagagem, meio de pagamento e monitoramento da saúde, de acordo com o Unisys Security Index**. 2017. Disponível em: https://www.unisys.com.br/offerings/security-solutions/News%20Release/BR-Maioria-dos-brasileiros-apoia-utiliza%C3%A7%C3%A3o-de-dispositivos-IoT. Acesso em: 14 mar. 2018.

VISA, **Visa brings Secure Payment Solutions to the Internet of Things.** 2020. Disponível em: https://usa.visa.com/visa-everywhere/innovation/visa-brings-secure-payments-to-internet-of-things.html Acesso em: 12 dez. 2018.

ZAHRA, A.; SHAH M. A. **IoT Based Ransomware Growth Rate Evaluation and Detection Using Command and Control Blacklisting.** Huddersfield, 2017. DOI 10.23919/IConAC.2017.8082013. Disponível em: https://ieeexplore.ieee.org/abstract/document/8082013. Acesso em: 20 jan. 2019.

ZAKARIA, Wira Zanoramy A, *et al*. The Rise of Ransomware. **Proceedings Of The 2017 International Conference On Software And E-Business - Icseb 2017**, [S.L.],

p. 66-70, dez. 2017. ACM Press. http://dx.doi.org/10.1145/3178212.3178224. Disponível em: https://dl.acm.org/doi/10.1145/3178212.3178224. Acesso em: 11 set. 2020.