**CENTRO UNIVERSITÁRIO SAGRADO CORAÇÃO**

**Ana Carolina de Oliveira**

**CIBERATAQUES COM O RANSOMWERE EKANS E MECANISMOS DE DEFESA**

BAURU

2021

**Ana Carolina de Oliveira**

**CIBERATAQUES COM O RANSOMWERE EKANS E MECANISMOS DE DEFESA**

Pré-Projeto de Iniciação Científica apresentada à Pró-Reitoria de Pesquisa e Pós-Graduação como parte dos pré-requisitos para aprovação do conselho, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU

2021

**RESUMO**

A integração tecnológica é exponencial e coopera para melhorar diversas áreas do cotidiano da sociedade como um todo. Contudo, juntamente as facilidades, surgem grandes ameaças que colocam empresas e indivíduos em riscos. Baseando-se nisso, o objetivo desta pesquisa é determinar como um dos mais recentes ransomweres descobertos, o Ekans, opera e de que forma as empresas – em especial – podem se proteger da ameaça.

**Palavras chave:** Segurança da Informação, Ransomwere, Ekans, Mecanismos de Defesa.

**SUMÁRIO**

[1. INTRODUÇÃO 4](#_Toc67320123)

[2. OBJETIVOS 5](#_Toc67320124)

[2.1. OBJETIVO GERAL 5](#_Toc67320125)

[2.2. OBJETIVOS ESPECÍFICOS 5](#_Toc67320126)

[3. REFERENCIAL TEÓRICO 5](#_Toc67320127)

[3.1. SEGURANÇA DA INFORMAÇÃO 5](#_Toc67320128)

[3.2. CIBERATAQUES 7](#_Toc67320129)

[3.3. RANSOMWERE 8](#_Toc67320130)

[3.4. MECANISMOS DE DEFESA 8](#_Toc67320131)

[4. MATERIAIS E MÉTODOS 8](#_Toc67320132)

[4.1. FERRAMENTAS UTILIZADAS – VIRTUALBOX 8](#_Toc67320133)

[4.2. HARDWARE 8](#_Toc67320136)

[5. CRONOGRAMA 9](#_Toc67320137)

[6. REFERÊNCIAS 10](#_Toc67320138)

# INTRODUÇÃO

A integração da computação na sociedade moderna se torna cada vez mais presente e cada vez mais profunda. Com isso várias novas possibilidades se tornam visíveis. Há inúmeras forma de usar o setor da Tecnologia da Informação para se maximizar lucros, automatizar tarefas cotidianas, gerenciar grandes quantidades de informações com uma eficiência jamais vista antes na história e entre outros. Em suma, é inegável que a tecnologia – de uma forma geral – trouxe grandes auxílios para a sociedade como um todo, no entanto, é igualmente inegável que juntamente com as novas possibilidades também vieram novas ameaças.

Assim como no mundo físico, o então nomeado “mundo virtual” possui ameaças tão perigosas – senão mais perigosas. Quanto mais integrado fica o mundo físico ao mundo virtual, maiores são as chances de um cyberataque ter efeitos gigantescos e prejudiciais, não somente a grandes empresas, mas também aos usuários dos sistemas de informação de forma geral.

Companhias multinacionais deixam a serviço da tecnologia processos de todos os escopos, desde serviços de contabilidade básicos, até linhas de produção inteiras. Obviamente, isso atrás – como já mencionado – grandes vantagens para as corporações, porém também as expõe a novos riscos. É possível hoje para linhas de montagem inteiras com algumas linhas de código; roubar dados confidenciais de funcionários, clientes, projetos; inutilizar servidores e entre outros.

Por esses motivos, as empresas precisam se preocupar e investir em tecnologias e politicas afim de garantir a máxima segurança. Entre as tecnologias, estão os softwares de antivírus, chaves de criptografia, backups e etc. As politicas, por sua vez, consistem em normas de boas práticas para os funcionários, como regras de acesso a internet, acesso a recursos do sistema e etc.

De acordo com os dados fornecidos pelo site da CERT.br (Cental de Estudos, Resposta e Tratamento de Incidente de Segurança no Brasil) a quantidade de ciberataques reportados em 2010 foi de 142.844 e em 2019 foi de 875.327, um aumento de aproximadamente 900% em menos de dez anos. Isso evidencia o impacto que esses ataques geram na sociedade como um todo. Por mais que alguns incidentes sejam “menores” e não tenham um escopo global, a relevância do tema não se perde. O mundo virtual ganha cada vez mais importância e cada vez mais espaço, se tornando cada vez mais fundamental e – consequentemente – perigoso.

# OBJETIVOS

# OBJETIVO GERAL

Explanar sobre o funcionamento do ransomewere Ekans e constatar as melhores formas de defesa contra esse tipo de cyberataque.

# OBJETIVOS ESPECÍFICOS

* Pesquisar sobre, ciberataques, ciberataques com o ransomwere Ekans e mecanismos de defesas;
* Verificar histórico de ciberataques com o ransomwere Ekans;
* Determinar os principais tipos de alvos do ransomewere Ekans;
* Identificar o modo como o ransomwere opera;
* Simular o ataque do ransomwere Ekans utilizando VirtualBox;
* Constatar melhores mecanismos de defesa para o ransomwere Ekans.

# REFERENCIAL TEÓRICO

A seguir serão tratados alguns aspectos teóricos principais referentes à esta pesquisa.

# SEGURANÇA DA INFORMAÇÃO

Aspirando- se que segundo o Dicionário Aurélio da Língua Portuguesa (2010, p. 689), entre as definições da palavra “segurança” há a “Estado, qualidade ou condição de seguro”, e, segundo o Dicionário Aurélio da Língua Portuguesa (2010, p. 426), entre as definições da palavra “informação” há a “Fatos conhecidos ou dados comunicados acerca de alguém ou algo”, portanto, pode-se concluir que segurança da informação consiste em proteger dados de indivíduos, empresas, governos e etc.

Atualmente, diversos sistemas são integrados e dependentes uns dos outros. Por isso é necessário que todas partes estejam seguras, já que o comprometimento de uma única parte, compromete o todo.

Existem cinco pilares básicos para a segurança da informação, sendo eles:

– Confidencialidade

– Integridade

– Disponibilidade

– Autenticidade

– Legalidade

Confidencialidade consiste no controle de acesso à informação apenas por aqueles que tenham permissão compatível com sua função, isto é, não deve existir acesso absoluto em um sistema. O acesso deve ser fragmentado de tal forma que não haja como um único individuo conhecer tudo.

Integridade se define como a garantia de que a informação será sempre completa e verdadeira, ou seja, sem que haja partes faltantes.

Disponibilidade, como o próprio nome sugere, é manter as informações sempre disponíveis de forma que estas nunca fiquem inacessíveis quando necessárias.

A autenticidade é a propriedade que assegura que toda informação está correta, em outras palavras, que não há falsificação

Por fim, a legalidade define que toda a informação e toda e qualquer manipulação referente a ela, estará de acordo com a legislação determinada pelo país.

# CIBERATAQUES

Pode-se definir ciberataques como a invasão de sistemas com o intuito de evidenciar, modificar, anular, destruir, ou roubar informações de empresas, pessoas, organizações, nações e etc. Os autores desse tipo de delito podem ser desde indivíduos únicos agindo de forma autônoma, até grupos, sociedades, organizações e nações.

De acordo com o CERT.br os ciberataques são feitos de varias formas, são eles:

* Worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
* Dos (DoS -- Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
* Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede
* Web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
* Scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
* Fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem. (CERT.br, 2020)

O impacto de um ciberataque é sempre imprevisível. As consequências podem ser: um profundo abalo na reputação da empresa - por si só gera falta de confiança por parte dos investidores e perda de clientes; interrupção na produção; exposições de informações sensíveis e aplicação de punições legais, como multas e prisões.

# RANSOMWERE

Consolida-se que ransomwere é um software malicioso cuja a intenção é bloquear os dados do sistema e exigir pagamento em dinheiro, geralmente com uma moeda não ratreavel, como por exemplo a moeda virtual bitcoin.

Esse malware pode se instalar no sistema de diversas formas, través de sites maliciosos, links suspeitos por e-mail, ou instalação de apps vulneráveis, também por meio de links enviados por redes sociais, meio muito utilizado para espalhar vírus atualmente, podendo bloquear a tela do computador ou utilizada criptografia para tornar inacessível arquivos importantes.

(Não sei se da pra fazer uma citação direta aqui!!)Os primeiros ataques, com ransomwares, relatados foram na Russia em 2005, porém esse tipo de ataque se espalhou pelo mundo e em 2013 houve um ataque que conseguiu atingir todas as versões do Sistema Operacional Windows e atingiu milhares de usuários, tanto pessoais quanto empresariais.

Quando um sistema ou computador é infectado ele é bloqueado instataneamente, tornando muito difícil a remoção do ransomware, pelo fato que o usuário não consegue sequer acessar seu o sistema. Portanto,é necessário utilizar dos mecanismos de defesa para prevenção.

# MECANISMOS DE DEFESA

# MATERIAIS E MÉTODOS

# FERRAMENTAS UTILIZADAS – VIRTUALBOX



# HARDWARE

O projeto será desenvolvido utilizando como principal ferramenta um computador pessoal (PC), com o sistema operacional Windows 10 Pro – 64 bits, processador Intel® Core™ i5 CPU 650 @ 3.20GHz com memória RAM de 4 GB. O fundamento da escolha do computador se deve pela razão de pertencer à pesquisadora, além de, em primeiro momento, suprir as necessidades da pesquisa.

# CRONOGRAMA

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ETAPAS** | | **Mês de execução** | | | | | | | | | | | |
|  | | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| **1** | Levantamento Bibliográfico: Fichamento de Livros, Periódicos, Vídeos, CD Rom, Pesquisas Internet etc. (Ciberataques, Mecanismos de Defesa, Ramsomwere Ekans) |  |  |  |  |  |  |  |  |  |  |  |  |
| **2** | Verificação de ciberataques com o ransomwere Ekans |  |  |  |  |  |  |  |  |  |  |  |  |
| **3** | Determinação dos principais tipos de alvos do ransomwere Ekans. |  |  |  |  |  |  |  |  |  |  |  |  |
| **4** | Identificação de como o ransomwere opera. |  |  |  |  |  |  |  |  |  |  |  |  |
| **5** | Constatação de melhores mecanismos de defesa contra o ransomwere Ekans |  |  |  |  |  |  |  |  |  |  |  |  |
| **6** | Redação preliminar do projeto de pesquisa. |  |  |  |  |  |  |  |  |  |  |  |  |
| **7** | Considerações finais do projeto de pesquisa, revisão e entrega. |  |  |  |  |  |  |  |  |  |  |  |  |

# REFERÊNCIAS

BASÍLIO, A. L.. O que é um ciberataque?. CartaCapital, 2017. Disponível em: < https://www.cartacapital.com.br/carta-explica/o-que-e-um-ciberataque/>. Acesso em: 19 de mar. de 2021.

ESTATÍSTICAS DOS INCIDENTES REPORTADOS AO CERT.BR. CERT.br, 2020. Disponível em: < https://www.cert.br/stats/incidentes/>. Acesso em: 18 de mar. de 2021.

INCIDENTES REPORTADOS AO CERT.BR. CERT.br, 2020. Disponível em: < https://cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html >. Acesso em: 19 de mar. de 2021.

INFORMAÇÃO. In: DICIONÁRIO Aurélio da Língua Portuguesa. 8. ed. Curitiba: Editora Positivo, 2010. v. 2, p. 426.

O QUE É UM RANSOMWERE?. Kaspersky. Disponível em: < https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware >. Acesso em: 22 de mar. de 2021.

SEGURANÇA. In: DICIONÁRIO Aurélio da Língua Portuguesa. 8. ed. Curitiba: Editora Positivo, 2010. v. 2, p. 689.

ZEFERINO, D. O que são ciberataques, como acontecem e como prevenir?. Certifiquei, 2020. Disponível em: < https://open.spotify.com/collection/tracks >. Acesso em: 19 de mar. de 2021.