**CENTRO UNIVERSITÁRIO SAGRADO CORAÇÃO**

**Ana Carolina de Oliveira**

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

BAURU

2021

**Ana Carolina de Oliveira**

**CYBERATAQUES 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](#_Toc66978106)

[2. OBJETIVOS 5](#_Toc66978107)

[2.1. OBJETIVO GERAL 5](#_Toc66978108)

[2.2. OBJETIVOS ESPECÍFICOS 5](#_Toc66978109)

[3. REFERENCIAL TEÓRICO 5](#_Toc66978110)

[3.1. SEGURANÇA DA INFORMAÇÃO 5](#_Toc66978111)

[3.2. CYBERATAQUES 6](#_Toc66978112)

[3.3. RANSOMWERE 6](#_Toc66978113)

[3.4. MECANISMOS DE DEFESA 6](#_Toc66978114)

[4. MATERIAIS E MÉTODOS 6](#_Toc66978115)

[4.1. HARDWARE 6](#_Toc66978118)

[5. CRONOGRAMA 7](#_Toc66978119)

[6. REFERÊNCIAS 8](#_Toc66978120)

# 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 cyberataques 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, cyberataques, cyberataques com o ransomwere Ekans e mecanismos de defesas;
* Verificar histórico de cyberataques com o ransomwere Ekans;
* Determinar os principais tipos de alvos do ransomewere Ekeans;
* Identificar o modo como o ransomwere opera;
* 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, 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 é manter a proteção dos dados de um indivíduo ou de alguma empresa.

Devido ao avanço tecnológico, tudo está conectado, por conseguinte se algum elemento conectado ao sistema é comprometido, todo o sistema pode estar comprometido, então para a segurança da informação é necessario se preocupar tanto com a segurança fisica dos dados quanto com a digital.

Com a facilidade de uso aumentando gradativamente, a necessidade de conhecimento de alto nível para realizar ataques avançados também diminui.

Quanto maior o parque computacional, mais difícil se torna seu gerenciamento, e disso surgem inúmeros problemas graves, de consequências desastrosas.

A área de SI possui três pilares básicos com o acréscimo de mais duas, que permitem a troca segura de informação, desde que nenhum deles seja violado. São eles:

– Confidencialidade

– Integridade

– Disponibilidade

– Autenticidade

– Legalidade

Confidencialidade

• Esse pilar é o responsável pelo controle de acesso à informação apenas por aquelas pessoas ou entidade que tenham permissão compatível com sua função e determinada pelo dono daquela informação.

Integridade

• Aqui, através dessa propriedade, é determinada a necessidade de garantir que a informação mantenha todas as suas características originais como determinadas pelo proprietário da informação.

Disponibilidade

• Essa propriedade define que determinada informação esteja sempre disponível para o acesso quando necessário, de maneira íntegra.

• Alguns dos ataques conhecidos buscam justamente derrubar a disponibilidade, e para algumas empresas o simples fato de não ter suas informações disponíveis durante determinado período de tempo, isso pode acarretar prejuízos estrondosos.

Autenticidade

• Propriedade responsável por garantir que a informação vem da origem informada, permitindo a comunicação segura e garantia de que a informação a qual tem acesso é correta e de fonte confiável.

Legalidade

• É a propriedade que define se determinada informação, ou operação, está de acordo com as leis vigentes no país. As mesmas leis que regem um país podem ser completamente diferentes em outro, o que pode ocasionar uma série de problemas, caso o sistema de gestão não seja adaptável.

# CYBERATAQUES

# RANSOMWERE

# MECANISMOS DE DEFESA

# MATERIAIS E MÉTODOS



# 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. (Cyberataques, Mecanismos de Defesa, Ramsomwere Ekans) |  |  |  |  |  |  |  |  |  |  |  |  |
| **2** | Verificação de cyberataques 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

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.

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