**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 os alvos podem se proteger da ameaça. Para fins de coleta e analise de dados, serão realizadas simulações com maquinas virtuais

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

**SUMÁRIO**

[1. INTRODUÇÃO 4](#_Toc67581613)

[2. OBJETIVOS 5](#_Toc67581614)

[2.1. OBJETIVO GERAL 5](#_Toc67581615)

[2.2. OBJETIVOS ESPECÍFICOS 5](#_Toc67581616)

[3. REFERENCIAL TEÓRICO 5](#_Toc67581617)

[3.1. SEGURANÇA DA INFORMAÇÃO 5](#_Toc67581618)

[3.2. CIBERATAQUES 7](#_Toc67581619)

[3.3. RANSOMWERE 8](#_Toc67581620)

[3.4. MECANISMOS DE DEFESA 8](#_Toc67581621)

[4. MATERIAIS E MÉTODOS 9](#_Toc67581622)

[4.1. DESENVOLVIMENTO PRÁTICO 10](#_Toc67581623)

[4.2. FERRAMENTAS UTILIZADAS – VIRTUALBOX E KALI LINUX 10](#_Toc67581624)

[4.3. HARDWARE 11](#_Toc67581627)

[5. CRONOGRAMA 12](#_Toc67581628)

[6. REFERÊNCIAS 13](#_Toc67581629)

# 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 ciberataque 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 (Central 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 ciberataque.

# 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;
* Simular o ataque do ransomwere Ekans utilizando VirtualBox;
* 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, 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 ransomwere como um software malicioso com a finalidade de bloquear os dados de um sistema, exigindo aos proprietários deste um pagamento para a recuperação das informações. Os primeiros ataques com ransomwares relatados ocorreram na Rússia no ano de 2005. Desde então, o esse modo operante de ataque se propagou pelo mundo.

Esse malware pode se instalar no sistema de diversas formas: través de sites maliciosos, links enviados por e-mail e redes sociais e instalação de aplicativos vulneráveis. Após a infecção o software pode bloquear a tela do computador e/ou tornar arquivos importantes inacessíveis por meio de criptografia.

No ano de 2013, por exemplo, houve um ataque de grande proporção atingindo diversas versões do sistema operacional Microsoft Windows causando danos a milhares de usuários e empresas.

A remoção de um ransomwere é complexa, já que o acesso do usuário ao sistema é comprometido. A melhor alternativa tanto para usuários pessoais, quanto para empresariais é a prevenção e utilização de mecanismos de defesa.

# MECANISMOS DE DEFESA

O único sistema verdadeiramente seguro é aquele que está desligado, desplugado, trancado num cofre de titanium, lacrado, enterrado em um bunker de concreto, envolto por gás nervoso e vigiado por guardas armados muito bem pagos. Mesmo assim, eu não apostaria minha vida nisso. (SPAFFORD).

Deste modo é possível verificar a importância dos mecanismos de defesa para proteger as informações, portanto é necessário técnicas de defesa. Estas variam de acordo com a necessidade e o modelo do sistema dividindo-se em três categorias: física, administrativa e lógica

A proteção física é referente a manutenção da integridade física (hardware) do sistema contra catástrofes naturais como incêndios, alagamentos, raios e entre outros. Como exemplo pode-se citar o sistema de refrigeração de um servidor. A função deste é a de manter os dispositivos sempre um uma temperatura favorável ao bom funcionamento, evitando a paralização por super aquecimento.

A proteção administrativa refere-se a organização do núcleo da empresa, como por exemplo selecionar a equipe responsável pela segurança.

A proteção lógica retrata o controle de acessos a informações. Um exemplo seria a utilização de usuários, senhas e níveis de acesso diferentes. Assim, pessoas externas não conseguem acesso nenhum aos dados e pessoas internas somente acessam os conteúdos que lhes são úteis para suas respectivas funções. Com abordagens como essa o rastreamento em casos de invasões, ou vazamento, também se torna uma tarefa mais simples, já que pelas informações vazadas é possível deduzir qual grupo de pessoas teria acesso a elas.

# MATERIAIS E MÉTODOS

Pesquisas com propósitos acadêmicos propendem, em primeira instância, a deter o caráter de pesquisa exploratória, tendo em vista que raramente o pesquisador terá um conhecimento a cerca do assunto retratado na pesquisa.

Segundo Gil (2010), as pesquisas exploratórias têm por finalidade proporcionar maior familiaridade com o problema, com o intuito de torná-lo mais explícito ou a construir hipóteses.

Á vista disso, este projeto trata-se de uma pesquisa exploratória com o objetivo é compreender como o ransomwere Ekans opera. Usando para tal, simulações em máquinas virtuais. Como resultado, espera-se identificar os melhores mecanismos de defesa para esse ransomwere.

O projeto será desenvolvido em duas etapas: na primeira serão realizadas pesquisas, estudos e desenvolvimento do embasamento teórico; na segunda serão feitos testes com a ferramenta VirtualBox com o objetivo de gerar conhecimento sobre os dados estudados.

Para o desenvolvimento do embasamento teórico e a descrição das atividades, haverá a necessidade de realizar pesquisas sobre:

1. Conceituação de segurança da informação;
2. Conceitos e casos de ciberataques;
3. Caracteristicas de ransomweres;
4. Conceitos de mecanismos de defesa;
5. Características e funcionamento da ferramenta de virtualização de máquinas VirtualBox;
6. Testes com a ferramenta VirtualBox para simulação de ciberataques com o ransomwere Ekans;
7. Identificação de melhores mecanismos de defesa.

# DESENVOLVIMENTO PRÁTICO

Serão feitas simulações utilizando duas maquinas virtuais sendo uma a atacante e outra o alvo. A maquina atacante terá como sistema operacional o Kali Linux enquanto a maquina alvo terá instalado o sistema operacional Microsoft Windows 10 Home.

A atacante usará o ransomwere Ekans e realizara ataques a maquina alvo. Com os resultados obtidos pela maquina alvo será analisado o comportamento do ransomwere. Depois que a analise estiver concluída, espera-se então identificar os melhores mecanismos de defesas contra a ameaça.

# FERRAMENTAS UTILIZADAS – VIRTUALBOX E KALI LINUX

O Oracle VM VirtualBox, software de virtualização de plataforma cruzada de código aberto mais popular do mundo, permite que os desenvolvedores forneçam código mais rápido executando vários sistemas operacionais em um único dispositivo. (ORACLE).

“Kali Linux é uma distribuição Linux [...] de código aberto voltada para várias tarefas de segurança da informação, como teste de penetração, pesquisa de segurança, computação forense e engenharia reversa.” (KALI LINUX, tradução nossa).

A escolha da ferramenta VirtualBox deveu-se a:

1. Ser uma ferramenta de código aberto.
2. Possibilidade de utilização de mais de uma maquina virtual ao mesmo tempo.
3. Possibilidade de usar sistemas operacionais diferentes.
4. Ser de conhecimento prévio da pesquisadora.

A escolha do sistema operacional Kali Linux deveu-se a:

1. Possuir código aberto.
2. Possuir ferramentas nativas que auxiliam na simulação de invasão.
3. Ser de conhecimento prévio da pesquisadora.

# 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. |  |  |  |  |  |  |  |  |  |  |  |  |
| **5** | Simulação do ataque com o ransomwere Ekans utilizando o VirtualBox. |  |  |  |  |  |  |  |  |  |  |  |  |
| **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.

CARDOSO, P. O que é um ramsomwere?.TechTudo, 2017. Disponível em: < https://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html>. Acesso em: 22 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.

GIL. A. C.; Como Elaborar Projetos de Pesquisa. 5.ed. São Paulo: Atlas, 2010.

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.

A DISTRIBIÇÃO DE TESTE MAIS AVANÇADA. Disponível em: < https://www.kali.org/>. Acesso em: 25 de mar. de 2021.

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.

ORACLE VM VIRTUALBOX. Oracle. Disponível em: < https://www.oracle.com/br/virtualization/virtualbox/>. Acesso em: 25 de mar. de 2021.

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

SPAFFORD, G.; Diretor de Operações de Computador, Auditoria e Tecnologia da Segurança, Purdue University/France.

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.