Uma análise comparativa entre linux e windows em um contexto de ransomware

A comparative analysis between Linux and Windows in the context of ransomware

João Paulo Carnellossi dos Santos[1]
Igor Elias da Silva[2]

Resumo

Esta pesquisa examina o histórico de ataques cibernéticos em sistemas Linux e Windows e as políticas adotadas em resposta a esses ataques, com foco no comportamento frente a ameaças ransomware.
Os ataques ransomware são uma ameaça significativa no ambiente corporativo, causando interrupções e perdas de serviços, e afetando diretamente o sistema operacional.
Com base em uma revisão bibliográfica sistemática, o objetivo é determinar o Linux mais efetivo na proteção contra ransomware, através da análise de pesquisas e estudos de casos. Esperam-se contribuições para a segurança cibernética e políticas de seguranças.

Palavras-chave: Ataques Cibernéticos; Ransomware; Segurança de Dados; Sistemas Operacionais.

Abstract

This research examines the history of cyber attacks on Linux and Windows systems and the policies adopted in response to these attacks, with a focus on behavior in the face of ransomware threats.
Ransomware attacks pose a significant threat in the corporate environment, causing disruptions and service losses, directly affecting the operating system.
Based on a systematic literature review, the objective is to determine the most effective Linux in protecting against ransomware through the analysis of research and case studies. Contributions to cybersecurity and security policies are expected.

Keywords: Cyber attacks; Ransomware; Data Security; Operational systems.

[1]Centro Universitário Filadélfia de Londrina - UniFil
[2]Centro Universitário Filadélfia de Londrina - UniFil

1 INTRODUÇÃO

Atualmente sistemas operacionais (SO's) são indispensáveis no meio corporativo, e a segurança é um aspecto crucial para o bom funcionamento, pois uma violação pode resultar em danos irreparáveis para as organizações e até mesmo usuários domésticos. Embora existam muitos SO's disponíveis, majoritariamente o mercado corporativo se concentra em duas opções: Windows e Linux.

Segundo (Tanembaum e Boss 2016), lançado em 1991 o Linux é um SO código aberto distribuído sob uma variedade de licenças, incluindo a GNU General Public License, destaca-se como um importante competidor no mundo de servidores corporativos, também é utilizado como desktops corporativos e pessoais. o Windows foi originalmente lançado em 1985, inicialmente uma interface gráfica sobre o SO MS-DOS e ao longo dos anos evoluiu com várias versões, chegando ao que temos hoje, o Windows 11 para desktops e para servidores o Windows Server 2022.

E estes sistemas estão constantemente expostos à ameaças ransomware, uma ameaça cibernética cada vez mais comum, com capacidades devastadoras para indivíduos e empresas. Ele criptografa os dados de um usuário ou sistema e exige um pagamento em troca da chave de descriptografia. Com seu potencial massivo de causar danos financeiros, os ataques ransomware se tornaram uma das principais preocupações no campo da segurança da informação.

Segundo (Zavarsky e Lindskog 2016), o primeiro ransomware para Windows começou a se espalhar em 1989 disseminado em um ataque chamado PC Cyborg, que utilizava chaves simétricas para criptografia dos dados da vítima.

A escolha do SO impacta diretamente a estabilidade, desempenho, facilidade de uso, confiabilidade, recursos disponíveis e os custos associados a infraestrutura. Independentemente da escolha entre Windows ou Linux, é importante atentar-se aos ataques ransomware ambos estão expostos à estas ameaças. Malwares costumam explorar vulnerabilidades. Portanto, a segurança é um ponto crítico para qualquer organização ou usuário, independentemente do SO escolhido.

Nos últimos anos, osataques ransomware tem evoluído significativamente em termos de sofisticação e variedade. Táticas mais avançadas, como criptografia com par de chaves assimétricas, ofuscação de código e uso de canais de comunicação cifrados para evadir a detecção. O ransomware também se tornou mais direcionado e

personalizado, com alvos específicos com base em informações coletadas por meio de engenharia social ou outras técnicas.

A resposta imediata mediante a estes ataques são cruciais, possibilitando uma mitigação do dano, segundo um estudo realizado pela X-Force (IBM 2023), foi relatado que um ransomware em 2019 conseguiam implementar o programa malicioso em 60 dias ou mais na maioria dos casos, já em 2020 o tempo caiu para 9.5 dias, no ano seguinte em 2021 houve uma queda para 3.85 dias, é um indicador que apresenta uma variação abrupta de um ano para outro.

Acredita-se que uma revisão bibliográfica comparativa pode trazer luz ao campo, permitindo uma análise sistemática e abrangente das pesquisas já existentes, fornecendo insights valiosos sobre tendências, técnicas e estratégias adotadas mediante estes ataques em ambos os sistemas. Demonstrando como os ataques ransomware evoluíram ao longo dos últimos anos e como eles atuam, é possível uma conscientização da nocividade destes ataques.

A partir do estudo apresentado, os resultados podem embasar melhores adoções de políticas e práticas de segurança no campo da informação. Compreendendo diferenças e semelhanças entre abordagens de segurança adotadas pelos sistemas operacionais, assim é possível desenvolver melhores estratégias de defesa para cada ambiente.

2 RESULTADOS ESPERADOS

Busca-se analisar os sistemas Linux e Windows sob um contexto de ameaças ransomware, abordando pontos específicos, como a eficácia das medidas de segurança, taxa de infecção, capacidade de retomada de serviços apos um ataque e mitigação de danos após o conhecimento do ataque.

Pretende-se identificar estratégias na prevenção, detecção e mitigação de danos mediante estes ataques, analisando casos passados, pesquisas e livros já existentes na área, serão analisadas, políticas de acesso, criptografias, capacidade da detecção frente a comportamentos maliciosos e medidas protetivas existentes. É esperado concluir que o sistema Linux possui um leque menor de vulnerabilidades, e documentar o que faz o sistema menos vulnerável.

Por fim, a capacidade de recuperação após um ataque ransomware também

será um aspecto analisado neste estudo. Será investigada a eficácia dos recursos e ferramentas de recuperação oferecidos por cada sistema operacional, bem como a velocidade e eficiência na restauração de dados e sistemas comprometidos.

Espera-se que essa abordagem mais específica na análise comparativa dos sistemas operacionais forneça insights valiosos sobre a segurança de dados em cada um deles, permitindo uma escolha informada e embasada na seleção do sistema operacional mais seguro em ambientes corporativos.

3 Estado da arte

3.1 A internet e a informação

No decorrer da internet, houve um avanço significativo tanto para usuários domésticos quanto para empresas, e os cibercriminosos não deixam de se beneficiar disto. Crimes tradicionais, como chantagem, extorsão e roubo, são conhecidos, porém com o crescimento da informação na internet é aberto um novo ambiente para atuação destes criminosos, os mesmos podem automatizar seus ataques, atingindo muito mais vítimas, esse novo ambiente tornou os crimes cibernéticos ubíquos.(O'KANE et al., 2018), o tema de segurança da informação (SI) tem cada vez mais tomado o espaço, seja por regulamentações visando a proteção de dados, responsabilização por eventuais vazamentos, tornando a segurança da informação, um desafio cada vez maior nas empresas.

3.2 Ransomware

O ransomware é projetado e desenvolvido com intuito de desabilitar o computador da vítima ou o acesso aos seus dados. Os criminosos, então, chantageiam a vítima para recuperar o equipamento ou os dados. O ransomware exibe uma mensagem sobre os termos do resgate (nota de resgate) e, nos primeiros dias, alguns criminosos tentavam alegar que eram policiais ou autoridades no assunto. Alguns ataques exibiam imagens ilícitas pretendendo destacar a devastação na vida da vítima se fosse processada em tribunal aberto. Essas técnicas de intimidação, projetadas para encorajar as vítimas a pagar. Joseph Popp, o fundador do primeiro ransomware, criou o programa em 1989, chamado 'AIDS' (PC Cyborg), que foi implantado como

um Trojan. O Trojan AIDS foi espalhado usando disquetes. Ao inserir o disquete, o programa AIDS criptografava os arquivos no disco C: e depois exigia um pagamento de 189 dólares para uma caixa postal no Panamá.(O'KANE et al., 2018).

Segundo (O'Kane, et al.,2018), a evolução da internet e da computação em nuvem criou um terreno fértil para ransomware, o crescimento do ransomware viu um aumento de 600% no número de famílias de ransomware dentre os mais conhecidos estão Cerber, Locky, CryptoWall e WannaCry, segundo o autor a criação das moedas digitais como o BitCoin e Ethereum, contribuíram para o avanço, pois possibilitaram o pagamento anônimo. Existem duas classes principais cujo podemos classificar o ransomware, elas são Locker Ransomware e Crypto Ransomware.

3.2.1 Locker Ransomware

O Ransomware Locker bloqueia a interface do usuário do computador ou dispositivo e depois pede ao usuário que pague uma taxa para restaurar o acesso. Os computadores bloqueados permanecerão com capacidades limitadas. O Ransomware Locker não afeta o sistema subjacente nem os arquivos. Esse tipo de ransomware muitas vezes se disfarça de autoridades policiais e alega emitir multas aos usuários por supostas indiscrições online ou atividades criminosas. Como é possível remover a maioria das ameaças ransomware Locker de forma limpa, os cibercriminosos costumam se esforçar muito para incorporar técnicas de engenharia social para pressionar as vítimas a pagar.(NARAIN, 2018)

3.2.2 Crypto Ransomware

Tem por objetivo encontrar e criptografa dados valiosos armazenados no disco, tornando os dados inacessíveis a menos que o usuário obtenha a chave de descriptografia. Seu objetivo é passar despercebido apenas até encontrar e criptografar todos os arquivos que possam ser importantes e valiosos para o usuário. Com infecções de Ransomware Crypto, na maioria das vezes, o computador afetado continua funcionando normalmente, e os usuários ainda podem usar o computador, exceto para acessar os dados criptografados. A chave de descriptografia é armazenada no servidor do atacante, portanto, as vítimas não podem recuperar seus arquivos sem pagar o resgate. Existe um risco adicional com esse tipo de ransomware em termos de pos-

síveis backdoors sendo criados e espalhando a infecção para vários arquivos que podem ser trocados pela rede de e para o sistema comprometido.(NARAIN, 2018)

3.2.3 Familias de ransomware

Além das classes, podemos classificar um ransomware em familias, que se distinguem pela estratégia de propagação, data de aparecimento, técnicas de criptográfia, e técnicas para controle do ransomware após sua propagação.(SUBEDI, BUDHATHOKI e DASGUPTA, 2018).

3.2.3.1 Reveton

O Reveton foi um ransomware notório, conhecido por exibir mensagens falsas de agências governamentais alegando atividades ilegais do usuário e exigindo o pagamento de multas. Era propagado principalmente mediante kits de exploração e usava o método de pagamento MoneyPak.(SUBEDI, BUDHATHOKI e DASGUPTA, 2018).

3.2.3.2 CryptoLocker

O CryptoLocker foi um dos primeiros ransomware a ganhar destaque, sendo ativo entre 2013 e 2014. Ele se espalhava por via de anexos de e-mail maliciosos e sites comprometidos. Utilizava criptografia forte e exigia o pagamento em Bitcoin para a recuperação dos arquivos.(SUBEDI, BUDHATHOKI e DASGUPTA, 2018).

3.2.3.3 CryptoWall

O CryptoWall foi uma variante do CryptoLocker, também muito difundido no período de 2013 a 2014. Ele utilizava técnicas semelhantes de propagação e criptografia, exigindo resgate em Bitcoin através da rede Tor.(SUBEDI, BUDHATHOKI e DASGUPTA, 2018).

3.2.3.4 Cerber

O Cerber é uma família de ransomware que tem sido ativa desde 2016. É conhecida por utilizar criptografia forte e por exigir o pagamento do resgate em Bitcoin. Ele se espalha principalmente por meio de anexos de e-mail e sites comprometidos.(SUBEDI, BUDHATHOKI e DASGUPTA, 2018).

3.2.3.5 Petya

O Petya foi um ransomware de alto impacto que surgiu em 2016. Ele se propagava por meio de e-mails de phishing e explorava vulnerabilidades em sistemas, como a exploração da falha EternalBlue. O Petya usava criptografia forte e exigia o pagamento em Bitcoin.(SUBEDI, BUDHATHOKI e DASGUPTA, 2018).

3.2.3.6 WannaCry

Surgiu em 2017, e explorava uma vúlnerabilidade no protocolo de compartilhamento de arquivos SMB do Windows. O ransomware segue o padrão Crypto Ransomware. O WannaCry atacou hospitais, empresas, universidades e organizações governamentais, afetando cerca de 150 países, afetando mais de 200.000 vítimas, o ransomware se instalava na rede de várias formas, o maior acumulo de casos se deu pelo phishing de emails (envio de emails contendo softwares maliciosos). (MOHURLE e PATIL, 2017).

3.3 Sistemas Operacionais

São softwares que gerenciam os recursos físicos do computador (hardware), trazendo um ambiente de execução para o usuário.

> "Um sistema operacional é um software que atua como intermediário entre o usuário e o hardware de um computador. Ele fornece um ambiente de execução para os programas de aplicativos e controla os recursos do sistema, como processadores, memória, dispositivos de entrada e saída, e arquivos."(SILBERSCHARTZ, GALVIN e GAGNE, 2018, p. 10).

Os sistemas operacionais gerenciam os recursos, balançeando o uso de processadores, memória, dispositivos, gerenciamento de processos, seja execução de processos, que são instâncias de programas em execução, como a criação, término, escalonamento e comunicação entre os processos, gerenciamento de memória, eles alocam e desalocam memória para os processos, garantindo o compartilhamento seguro e eficiente da memória entre os programas em execução, gerenciamento de sistemas de arquivos, os sistemas operacionais gerenciam o armazenamento e organização dos arquivos em sistemas de arquivos, gerenciamento de dispositivos, eles controlam a comunicação entre o computador e os dispositivos periféricos (TANEMBAUM e BOSS, 2016).

3.3.1 Windows

Segundo (Bassil, 2012), O Windows, incluindo todas as suas versões, estima-se ter uma participação total de mercado de 92,03% tornando-o o maior sistema operacional dominante para computadores pessoais. O sistema é projetado pela Microsoft Corporation, que o originou em 1985 como um complemento para o MS-DOS, que era o sistema operacional padrão enviado na maioria dos PCs baseados em Intel na época.

3.3.1.1 Modelo de Segurança

O modelo de segurança do Windows é uma coleção de processos em modo de usuário e modo de kernel que fornecem, monitoram e gerenciam os diferentes componentes de segurança do sistema operacional Windows, coordenando entre eles, (Bassil, 2012) disserta sobre alguns dos componentes de segurança do windows.

Monitor de Referência de Segurança (SRM):

O SRM é um componente em modo de kernel que fica no diretório system32 nomeado de Ntoskrnl.exe, que impõe políticas de segurança no computador. Ele protege os diversos recursos do sistema operacional, realizando proteção e auditoria de objetos em tempo de execução, além de manipular privilégios de segurança, frequentemente conhecidos como direitos de usuário.

Subsistema de Autoridade de Segurança Local (Lsass):

O Lsass é um processo em modo de usuário localizado no diretório System32 nomeado Lsass.exe, responsável pela política de segurança do sistema local, autenticação de usuários e envio de mensagens de auditoria de segurança para o registro de eventos. Na verdade, o Lsass implementa a maioria de suas funcionalidades em uma biblioteca de vínculo dinâmico dentro do mesmo diretório no arquivo Lsasrv.dll.

Gerenciador de Contas de Segurança (SAM):

É um serviço combinado a um banco de dados. O serviço SAM consiste em um conjunto de sub-rotinas responsáveis por gerenciar o banco de dados que contém

os nomes de usuário e grupos definidos na máquina local. Ele é implementado como uma biblioteca de vínculo dinâmico no diretório System32 no arquivo Samsrv.dll, e é executado no processo Lsass. Por outro lado, o banco de dados SAM é usado em sistemas que não funcionam como controladores de domínio e contém os usuários e grupos locais definidos, juntamente com suas senhas e outros atributos. O banco de dados SAM é armazenado no registro em HKLM/SAM.

3.3.2 Linux

É um sistema operacional baseado em Unix, composto por um kernel Linux originalmente desenvolvido por Linus Torvalds e posteriormente estendido e aprimorado por uma grande comunidade de desenvolvedores em todo o mundo, e o GNU, que é uma coleção de software composta por partes de software, programas de sistema e ferramentas utilitárias originalmente concebidas por Richard Stallman para criar um sistema operacional completamente livre e aberto usando o kernel Linux. Basicamente, o GNU/Linux é de código aberto e, portanto, qualquer pessoa pode ler e modificar seu código-fonte e criar o que são chamadas de distribuições Linux, como Red Hat, Debian e Ubuntu.(BASSIL, 2012).

3.3.2.1 Modelo de Segurança

O modelo de segurança do Linux é uma coleção de vários processos ativos, serviços de daemon e bibliotecas que fornecem um framework seguro para o kernel Linux. O autor (Bassil, 2017), detalha alguns destes recursos.

Biblioteca PAM (Pluggable Authentication Modules):

A biblioteca PAM fornece a interface e as funções necessárias para desenvolver aplicativos compatíveis com PAM. A biblioteca PAM é essencial para permitir a autenticação de usuários no sistema operacional Linux.

Arquivo de Configuração PAM:

É um arquivo de texto onde o administrador do sistema pode especificar qual esquema de autenticação é usado para um aplicativo específico. No sistema Linux, essas informações de configuração podem ser armazenadas em um arquivo dentro

do diretório /etc/pam ou como uma linha no arquivo de configuração /etc/conf. Após a inicialização da biblioteca PAM, o arquivo de configuração do PAM é lido para carregar os módulos de autenticação correspondentes.

Módulo de Autenticação:

É um módulo que contém vários procedimentos de autenticação, usados para criar credenciais de autenticação, autenticar usuários e conceder privilégios a usuários autenticados.

Módulo de Gerenciamento de Contas:

Rege contas de usuários e determina se um usuário autenticado tem permissão para acessar o sistema. Cria uma sessão de login após uma autenticação bem-sucedida e é responsável por validar a data de expiração do nome de usuário e/ou senha.

Módulo de Gerenciamento de Senhas:

Administra as senhas dos usuários, incluindo definição, redefinição e alteração de senhas. Em outras palavras, define ou altera os dados de autenticação do usuário.

Módulo de Gerenciamento de Sessão:

Controla o início e o término de uma sessão de login. Também lida com a criação das entradas de log apropriadas para cada sessão inicializada.

REFERÊNCIAS

BASSIL, 2012 BASSIL, Y. Windows And Linux Operating Systems From A Security Perspective **Journal of Global Research in Computer Science** Beirut, Líbano, v. 3, n. 2, fev. 2012. Documento eletrônico. Disponível em <https://doi.org/10.48550/arXiv.1204.0197> Acesso em 2 de junho de 2023

IBM, 2023 IBM – International Business Machines. **IBM Security X-Force Threat Intelligence Index 2023.** IBM, 2023. Disponível em: <https://www.ibm.com/reports/threat-intelligence>. Acesso em: 4 maio. 2023.

MOHURLE e PATIL, 2017 MOHURLE, S.; PATIL, M. A brief study of Wannacry Threat: Ransomware Attack 2017. **International Journal of Advanced Research in Computer Science**, Pune, India , v. 8, n. 5, p. 1938-1940, junho. 2017

NARAIN, 2018 NARAIN, P. **Ransomware - Rising Menace to an Unsuspecting Cyber Audience.** Houston, Texas, USA 2018, 64 p. Tese (Mestre em Ciência Segurança de Sistemas de Informação) - University of Houston. Documento eletrônico. Disponível em <http://hdl.handle.net/10657/3145>. Acesso em 25 de maio de 2023.

O'KANE et. al, 2018 . O'KANE, P.; SEZER, S.; CARLIN, D. Evolution of ransomware. **IET Networks**, Belfast, Irlanda, v. 7, p. 321-327, 2018

SUBEDI, BUDHATHOKI e DASGUPTA, 2018 SUBEDI, K. P.; BUDHATHOKI, D. R.; DASGUPTA, D. Forensic Analysis of Ransomware Families Using Static and Dynamic Analysis. **2018 IEEE Security and Privacy Workshops (SPW)**, San Francisco, CA, USA p. 180-185, 2018. Documento eletrônico. Disponível em <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=8424649> Acesso em 25 de maio de 2023

SILBERSCHATZ, GALVIN e GAGNE, 2018 SILBERSCHATZ, A.; GALVIN, P.; GAGNE, G.; **Operating system concepts.** ed. 10. Hoboken, NJ: Wiley, 2018

TANENBAUM e BOSS, 2016 TANENBAUM, A.S.; BOSS, H. **Sistemas Operacionais Modernos**. Tradução: Daniel Vieira e Jorge Ritter. São Paulo: Pearson Education do Brasil, 2016.

ZAVARSKY e LINDSKOG, 2016 ZAVARSKY, P.; LINDSKOG, D.; Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization. **Procedia Computer Science**, Edmonton, Canadá, v. 94, p. 465-472, março. 2016.