Revista Terra & Cultura: Cadernos de Ensino e Pesquisa
ISSN 2596-2809

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]
Robson de Lacerda Zambroti[2]

RESUMO

O presente artigo analisa a segurança entre o Windows e Linux, o Windows com suas inovações contínuas apresenta dominância no mercado, o mesmo apresenta muitas vulnerabilidades, como evidenciado pelo estudo de caso DART, que detalha um ataque em uma grande empresa que preferiu se manter anônima. Por outro lado, o Linux, com sua natureza de código aberto, oferece flexibilidade, mas também enfrenta desafios de padronização de segurança. O cenário de cibersegurança está em constante evolução, com profissionais sempre buscando brechas e sistemas operacionais tentando tapar essas lacunas. A crescente ameaça dos ataques *ransomware* é enfatizada, e a prevenção e a conscientização sendo cruciais para a segurança cibernética. A análise concluída reforça a importância das boas práticas, como atualizações regulares e cautela ao interagir com e-mails e links, e destaca a necessidade de sistemas operacionais robustos e adaptáveis em um mundo digital em constante mudança.

Palavras-chave: ataques cibernéticos; *ransomware*; segurança de dados; sistemas operacionais.

ABSTRACT

This article analyzes the security between Windows and Linux. Windows, with its continuous innovations, is dominant in the market and has many vulnerabilities, as evidenced by the DART case study, which details an attack on a large company that preferred to remain anonymous. On the other hand, Linux, with its open source nature, offers flexibility, but also faces security standardization challenges. The cybersecurity landscape is constantly evolving, with professionals always looking for loopholes and operating systems trying to plug them. The growing threat of ransomware attacks is emphasized, with prevention and awareness being crucial to cybersecurity. The concluded analysis reinforces the importance of good practices, such as regular updates and caution when interacting with emails and links, and highlights the need for robust and adaptable operating systems in an ever-changing digital world.

Keywords: cyber attacks; ransomware; data security; operational systems.

[1] Acadêmico do curso de Ciência da Computação da UniFil. Email: joao159@edu.unifil.br
[2] Professor Orientador da UniFil. Email: robson.zambroti@unifil.br

1 INTRODUÇÃO

Ataques *ransomwares*, 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 (Narain, 2018). Com seu potencial massivo de causar danos financeiros, os ataques *ransomware* se tornaram uma das principais preocupações no campo da segurança da informação.

Nos últimos anos, os ataques *ransomware* têm 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 evitar 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 (O'kane et. al, 2018).

De acordo com 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. Embora os ataques *ransomware* datem desde 1989 e desde então sua evolução tem sido notória.

Segundo o relatório X-Force da IBM publicado em 2023, em 2020 foi visto uma escalada exponencial da tenacidade destes ataques, a JBS USA, que em maio de 2021 foi vítima de um ataque *ransomware* que gerou um prejuízo de 11 milhões de dólares (Keary, 2021).

Foi relatado que um ataque *ransomware* em 2019 conseguiram implementar o programa malicioso em 60 dias ou mais, já em 2020 o tempo caiu para 9,5 dias, no ano seguinte em 2021 houve uma queda para 3,85 dias IBM (2023). É um indicador preocupante que apresenta uma variação abrupta de um ano para outro, logo a resposta imediata a estes ataques são cruciais.

A escolha do SO ou sistema operacional impacta diretamente a estabilidade, desempenho, facilidade de uso, confiabilidade, recursos disponíveis e os custos associados à infraestrutura. Independentemente da escolha entre Windows ou Linux, é importante atentar-se aos ataques *ransomware*, ambos estão expostos a essas ameaças, que costumam explorar vulnerabilidades. Portanto, a segurança é um ponto

crítico para qualquer organização ou usuário, independentemente do SO escolhido.

Segundo a pesquisa realizada por Awan e Khan (2023), em seu artigo é relatado que 54,5% dos usuários entrevistados utilizam Windows como sistema operacional padrão no trabalho ou casa, 27,3% Linux e apenas 18,2% MacOS. Tendo em vista que os dados se tornam relevantes e então a pesquisa é direcionada à sistemas Windows e Linux.

Acredita-se que a pesquisa qualitativa, pode trazer luz ao tema pois se trata de uma análise de acontecimentos, permitindo conscientização do público alvo destes sistemas operacionais, apoiada a um estudo de caso e pesquisas bibliográficas, fornecerá *insights* valiosos, que auxiliarão na identificação da evolução vertiginosa, e metodologia destes ataques *ransomwares* ao longo dos últimos anos, assim é possível uma conscientização da nocividade destes ataques, embasar posteriormente tomada de decisões durante a prevenção ou mitigação dos danos.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 A INTERNET E A INFORMAÇÃO

Com o avanço do mundo digital, houve uma melhoria significativa tanto para usuários domésticos quanto para empresas, e os cibercriminosos não deixam de se beneficiar disto. Crimes tradicionais, como chantagem, extorsão e roubo, com o crescimento da informação na internet abre-se um novo ambiente para atuação desses criminosos, os mesmos podem automatizar seus ataques, atingindo 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.

2.2 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 tentaram 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 como *ransomware*, elas são Locker *ransomware* e Crypto *ransomware*.

2.2.1 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).

2.2.2 Crypto ransomware

Tem por objetivo encontrar e criptografar 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 possíveis backdoors sendo criados e espalhando a infecção para vários arquivos que podem ser trocados pela rede de e para o sistema comprometido. (Narain, 2018)

2.2.3 Famílias de ransomware

Além das classes, podemos classificar um *ransomware* em famílias, que se distinguem pela estratégia de propagação, data de aparecimento, técnicas de criptografia, e técnicas para controle do *ransomware* após sua propagação. (Subedi; Budhathoki; Dasgupta, 2018).

Os autores Hull, John e Arief (2019) mencionam que *ransomwares* geralmente se espalham através de anexos de e-mail maliciosos, aplicativos de software infectados, dispositivos de armazenamento externo infectados ou sites comprometidos. Além disso, é destacado que os ataques de phishing são a principal causa de ativação de *ransomware* em um computador da vítima. Abaixo os autores Mohurle e Patil (2017), descorrem sobre algumas famílias de ransomware.

- 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.
- O CryptoLocker foi um dos primeiros *ransomware* a ganhar destaque, sendo ativo

entre 2013 e 2014. Ele se espalhava por e-mails maliciosos e sites comprometidos. Utiliza criptografia forte e exigia o pagamento em Bitcoin para a recuperação dos arquivos.

- 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 mediante a rede Tor.
- 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.
- 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 Eternal Blue. O Petya usava criptografia forte e exigia o pagamento em Bitcoin.
- O Wanna Cry surgiu em 2017 e explorava uma vulnerabilidade no protocolo de compartilhamento de arquivos SMB (Server Message Block) do Windows, que é um protocolo de compartilhamento de arquivos em rede. 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 textit{ransomware} se instalava na rede de várias formas, o maior acúmulo de casos se deu pelo phishing de e-mails (envio de e-mails contendo softwares maliciosos). (Mohurle e Patil, 2017).

2.2.4 Caso JBS USA

Em 2023, uma das principais companhias alimentícias dos EUA enfrentou um ataque ransomware que paralisou suas operações, impactando a produção e distribuição de carne tanto nos EUA quanto no Canadá. Esse ataque causou uma elevação imediata nos preços das carnes, evidenciando as falhas na segurança cibernética das infraestruturas empresariais americanas. Mesmo com consideráveis investimentos em tecnologia e segurança, a empresa teve que desembolsar 11 milhões de dólares para o grupo de *hackers* russos REvil. Esse evento ressaltou o quão suscetíveis grandes corporações estão a ameaças cibernéticas e sublinhou a

urgência de reforçar medidas de proteção.

2.3 SISTEMAS OPERACIONAIS

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

2.3.1 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 computadores baseados em Intel na época.

Os autores Adekotujo et al. (2020) dizem que o Windows possui quase 90% de participação de mercado sobre outros sistemas operacionais. No entanto, essa afirmação é acreditada como não sendo mais tão precisa devido ao crescente interesse das pessoas em sistemas operacionais de código aberto.

2.3.1.1 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), 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), 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.

2.3.1.2 Sticky Keys

É relatado pelo autor Saleem, 2022 que o Sticky Keys é uma funcionalidade destinada a ajudar usuários com mobilidade limitada. Os Sticky Keys em outras palavras, permite que as teclas de modificação (como Ctrl, Alt, Shift) sejam "fixadas" ou "aderidas", de modo que não precisem ser pressionadas ao mesmo tempo que outras teclas, e também permite gravar padrões para acesso, facilitando

autenticações.

2.3.1.3 Mimikatz

É uma ferramenta que foi desenvolvida em 2011 por Benjamin Delpy, ele demonstrou e confirmou como os protocolos usados para autenticação da Microsoft estavam gravemente vulneráveis a ataques. Os invasores exploram essa vulnerabilidade no sistema Windows para acessar o armazenamento interno (Shairoze e Erej, 2021). Os autores citam que o Mimikatz oferece vários módulos para coletar e usar credenciais do Windows em sistemas alvo. A partir do Windows XP em diante, o Mimikatz funciona em todas as versões do Windows.

2.3.1.4 Advanced IP Scanner

É um software que segundo a empresa desenvolvedora (Farmatech, 2023) , possibilita escanear a rede local e identificar dispositivos conectados, podendo-se realizar ações nos dispositivos escaneados, segundo o autor (Roslan, 2023), o Advanced IP scanner utiliza técnicas de escaneamento semelhantes ao NMAP, porém não com a mesma eficiência e força.

2.3.1.5 Protocolo de desktop remoto (RDP)

É um protocolo desenvolvido pela Microsoft que proporciona acesso e exibição remotos por via de uma conexão de rede para aplicações baseadas em Windows que estão sendo executadas em um servidor. Especificamente, ele oferece acesso a computadores remotos que executam desde o Windows 2000 Server até versões mais recentes, incluindo o Windows XP (Kerai, 2010).

2.3.2 Linux

É um sistema operacional baseado em Unix, composto por um kernel Linux originalmente desenvolvido por Linus Torvalds e posteriormente expandido 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, os autores Silberschatz, Galvin e Gagne (2018), dizem que 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.

2.3.2.1 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.

- A biblioteca PAM (Pluggable Authentication Modules), 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.
- O 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.

3 METODOLOGIA

A metodologia da presente pesquisa foi estruturada a fim de abordar a escalada dos ataques *ransomware* ao longo dos últimos anos, visando abranger sistemas Windows e Linux, dada a sua prevalência no mercado. Fornecendo uma análise qualitativa pois foram analisados além dos dados, fatos históricos de ataques, faz uso de um estudo de caso aliado a uma revisão de literatura para obter uma compreensão objetiva e clara do tema.

Uma revisão da literatura foi realizada para coletar informações sobre a evolução dos ataques *ransomware* desde sua primeira aparição em 1989 até os desenvolvimentos mais recentes. Relatórios, como o X-Force da IBM (2023), foram consultados para obter dados sobre a tenacidade e rapidez desses ataques ao longo dos anos. Além disso, artigos acadêmicos e publicações de especialistas no campo da segurança da informação foram revisados para entender as táticas avançadas empregadas por *ransomwares* e as vulnerabilidades exploradas em diferentes sistemas operacionais.

Foi analisado um estudo de caso específico de ataque à uma organização que utilizava o sistema operacional Windows, e então foi feito um paralelo com o referencial coletado sobre o Linux, a fim de simular conceitualmente o comportamento mediante este ataque. Esta análise ajuda a identificar técnicas de ataque, possíveis medidas de mitigação, informações sobre como as organizações responderam a esses ataques, consequências enfrentadas e aprendizados.

O cenário atual e os ataques de *ransomware* operados por humanos foram investigados em profundidade através de um estudo de caso específico. A Microsoft, através de sua equipe DART, foi analisada para entender como grandes organizações respondem a ataques de *ransomware* e quais estratégias são empregadas para mitigar tais ameaças.

Os dados foram coletados através de relatórios publicados, artigos acadêmicos, estudos de caso e entrevistas com especialistas em segurança cibernética. A análise destes dados permitiu identificar tendências e técnicas comuns empregadas por atacantes. Após a coleta, os dados foram analisados para identificar metodologias de ataque, tendências e *insights* valiosos sobre a natureza e evolução dos ataques *ransomware*. Esta análise ajudou a formular recomendações e estratégias para mitigar tais ameaças no futuro.

4 ANÁLISE DO ESTUDO DE CASO DART

O cenário cibernético atual tem visto um aumento significativo nos ataques de ransomware operados por humanos. Estes ataques, muitas vezes devastadores, têm como alvo organizações com vulnerabilidades de segurança específicas, causando danos significativos e interrupções.

Uma grande organização, que preferiu permanecer anônima, foi recentemente comprometida por um ataque de ransomware. A Microsoft, por meio de sua equipe DART, foi chamada para investigar e mitigar o incidente.

4.1 DETALHES DO INCIDENTE

- No ponto de entrada, o profissional identificou um dispositivo vulnerável com a porta TCP 3389 aberta, permitindo o acesso RDP, por via de técnicas de força bruta, o atacante conseguiu acesso inicial ao sistema.
- Fase de Reconhecimento, uma vez dentro, o atacante buscou mapear a rede, identificando pontos críticos e coletando informações. Utilizou ferramentas como o Advanced IP Scanner para obter uma visão detalhada da infraestrutura da rede.
- Com intuito de coletar credenciais e visando aprofundar seu acesso, o atacante usou a ferramenta Mimikatz, credenciais foram extraídas, permitindo ao atacante um acesso mais amplo à rede.
- A movimentação na rede, foi possível utilizando as credenciais obtidas, então o atacante navegou pela rede, acessando sistemas críticos, a movimentação foi discreta, aproveitando-se de ferramentas e processos legítimos para evitar detecção. Para garantir sua permanência, o atacante implementou várias técnicas

de evasão, isso incluiu a desativação de certos recursos de segurança e a abertura de portas específicas para garantir a comunicação contínua.

- O profissional implementou o *hack* Sticky Keys (uma funcionalidade), garantindo que, mesmo se detectado, ele pudesse acessar o sistema. Então finalmente, foi lançado o ransomware, criptografando dados críticos, uma nota de resgate foi deixada, exigindo pagamento em troca da descriptografia dos dados.
- O responsável pelo ataque iniciou remotamente um Script PowerShell interativo a partir de vários compartilhamentos remotos. Esse método de ataque randomiza os pontos de distribuição e torna a correção mais difícil durante a fase final do ataque de ransomware (Dart, 2023).
- A primeira ação da equipe DART foi isolar os sistemas afetados para evitar uma propagação adicional do *ransomware*. Eles desconectaram rapidamente os servidores comprometidos da rede principal.
- Com sistemas isolados, a equipe iniciou uma avaliação detalhada para determinar a extensão do dano. Isso inclui identificar quais sistemas foram criptografados, quais backups estavam intactos e quais dados haviam sido comprometidos.
- A equipe DART focou em restaurar os sistemas críticos. Felizmente, alguns backups off-line estavam disponíveis, permitindo uma recuperação parcial dos dados. No entanto, dados recentes que não foram incluídos nos backups tiveram que ser considerados perdidos ou retidos até o pagamento do resgate.

4.2 PARALELO COM LINUX

E como o Linux se comportaria mediante este ataque, com base no referencial bibliográfico coletado é possível traçar um paralelo e definir o comportamento, desde a fase de invasão até o estágio final de dispersão na rede.

- No ponto de entrada, o Linux não possui um protocolo nativo equivalente ao RDP, logo não seria possível nativamente a invasão, mas ferramentas não licenciadas como o VNC (*Virtual Network Computing*) podem fornecer funcionalidades semelhantes para acesso remoto ao ambiente.
- As técnicas de exploração utilizadas no ataque Windows, não seriam efetivas no Linux pelo seu modelo de segurança, como citado por BASSIL (2017) o Linux

mantém uma árvore de permissões robustas, com diferentes grupos e políticas de segurança. Logo precisam ser adaptadas para o ambiente Linux.

- A permanência do invasor no sistema e na rede, não seria um problema, pois o Linux apesar de robusto com as políticas de segurança, uma vez que o sistema seja invadido, é possível a cópia das chaves de criptografia dupla que permitem o acesso a vários recursos e softwares.
- Uma vez que o invasor consiga acesso direto à máquina, de mesmo modo que o ransomware é liberado no Windows ele é no Linux, e sua propagação é similar, porém no Linux o módulo de segurança responsável por registrar toda a movimentação na rede, é mais robusto que o Windows, logo sua movimentação tem mais chances de ser percebida, caso aja ações fora do padrão.
- Como citado anteriormente, Linux mantém registros detalhados de atividades do sistema. O que pode auxiliar na fase de isolamento, identificando de onde partiu o ataque e quais os dispositivos afetados.

4.3 CONCLUINDO A ANÁLISE

Este incidente serve como um lembrete crítico da importância da cibersegurança proativa. A rápida intervenção da equipe DART fez o possível para mitigar o impacto, mas a prevenção é sempre a melhor forma de defesa.

O paralelo com o Linux, evidenciou como o Windows é mais visado pelos invasores, acredita-se que por conta da predominância majoritária no mercado, e seu modelo de segurança deixa a desejar nos registros de auditoria, estruturas de permissões e até mesmo nas funcionalidades para acessibilidade que como visto no caso do StickyKeys pode abrir uma brecha de segurança.

Organizações são aconselhadas a revisar e fortalecer regularmente suas posturas de segurança para evitar tais comprometimentos, o DART realça, casos desta natureza raramente conseguem êxito na tentativa de restaurar os dados sem ceder ao resgate.

5 CONCLUSÕES GERAIS

Mediante as análises, o sistema operacional é a base de um computador

(Silberschatz, Galvin e Gagne, 2018), regulando a comunicação entre hardware e software. Este artigo explorou a dinâmica dos dois sistemas operacionais predominantes: Windows e Linux, com ênfase especial em suas características de segurança e desafios associados.

O Windows estabelece sua dominância no mercado, ocupando a parcela de 90% de usuários (Adekotujo *et al*., 2020), com suas contínuas inovações e compromissos com a acessibilidade, não está isenta de vulnerabilidades.

Apesar de oferecer um ambiente familiar e amigável para muitos, suas vulnerabilidades intrínsecas, como evidenciado pela exploração por meio de ferramentas como Mimikatz, textit{hack} StickyKeys visto no caso DART, destacam a necessidade contínua de aprimoramento em seu modelo de segurança.

É notório que o Windows tem sido o maior alvo dos ataques textit{ransomware}, tendo em vista que as famílias de textit{ransomware} majoritariamente atuam invadindo sistema por envio sistemático de e-mails maliciosos (Narain, 2018), e então se propaga na rede por via de falhas nos protocolos de compartilhamento de arquivos exclusivos do Windows como SMB, que só podem ser acessados no Linux mediante software de terceiros (Dart, 2023).

Por outro lado, o Linux, com sua natureza de código aberto, fornece uma flexibilidade inigualável. No entanto, essa mesma abertura também pode ser uma faca de dois gumes, já que a diversidade de distribuições pode apresentar desafios de padronização de segurança, e quando utilizamos programas de terceiros ou drivers não licenciados oficialmente o risco se eleva (Awan e Khan, 2023), como visto na análise do caso DART, o Linux quando utiliza serviços de terceiros que simulam o RDP, abre uma brecha possibilitando o ataque que anteriormente afetava apenas o Windows.

Foi possível concluir que o Linux se torna mais seguro em diversos aspectos, as famílias de ransomwares existentes, não são voltadas para os módulos nativos do sistema operacional, e sua estrutura de permissões o favorece na prevenção destes ataques, às políticas de segurança são mais restritas sendo necessário uma customização do responsável do sistema.

O estudo de caso DART ilustra o mundo real de ataques de *ransomware*, lembrando a todos os usuários e administradores de sistemas da importância da prontidão e resiliência em cibersegurança. O cenário de cibersegurança está em

constante evolução, com atacantes sempre buscando brechas e sistemas operacionais sempre se esforçando para tapar essas lacunas. O caso auxilia a ver que a mitigação e recuperação dos dados é trabalhosa e tende a não ser completa, havendo perda de parte destes dados.

Segundo os autores Awan e Khan, a melhor estratégia sempre será a prevenção, cursos de conscientização no âmbito de segurança da informação e boas práticas tanto no ambiente corporativo quanto no doméstico, a efetividade dos ataques *ransomware* crescem de maneira exponencial, em 2020 a 2023 esse salto se tornou assustador como já citado (IBM, 2023).

Em resumo, enquanto avançamos em direção a um futuro ainda mais digitalizado, a necessidade de sistemas operacionais robustos, seguros e adaptáveis torna-se cada vez mais crucial. As partes interessadas, sejam desenvolvedores, administradores ou usuários finais, devem se manter informadas, atualizadas e, acima de tudo, vigilantes em um cenário digital que está em constante mudança e desafio.

A análise não visa apenas informar e conscientizar sobre a crescente ameaça *ransomware* no mundo digital, mas também procura reforçar a importância das boas práticas na hora de abrir e-mails acessar sites, tendo em vista que as famílias *ransomware* responsável pelos ataques mais danosos no mundo digital, ocorrem por links maliciosos em e-mails.

Bem como se mostra crucial manter as atualizações de sistema em dia, é válido mencionar o caso da família WannaCry em 2017 atacou inúmeros computadores, o mesmo ocorreu por uma falha no protocolo SMB que já havia sido corrigida pela Microsoft no ano em questão, porém havia muitos computadores não atualizados (Mohurle e Patil, 2017). Ambos sistemas operacionais atualmente possuem uma estrutura de segurança robusta e diversificada, cabe aos usuários e administradores do sistema, seguirem as boas práticas de segurança citadas anteriormente.

REFERÊNCIAS

ADEKOTUJO, A.; Odumabo A.; Ademola A.; Aiyeniko O. A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS. **International Journal of Computer Applications** v. 176, p. 16-23, 2020.

FARMATECH Advanced IP Scanner. **Advanced IP Scanner - About** FARMATECH, 2023. Disponível em: https://www.advanced-ip-scanner.com/br/help/. Acesso em: 20

out. 2023.

AWAN , M. T.; KHAN, K. Linux vs. Windows: A Comparison of Two Widely Used Platforms. **Journal of Computer Science and Technology Studies**, v. 4, n. 1, p. 41–53, 2022.

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.

DART, Equipe de Detecção e Resposta da Microsoft. **Estudo de caso do ransomware Microsoft,** DART. 2023. Disponível em: https://learn.microsoft.com/pt-br/security/ransomware/dart-ransomware-case-study. Acesso em: 12 out. 2023.

HULL, G.; JOHN, H.; ARIEF, B.; ransomware deployment methods and analysis: views from a predictive model and human responses. **Crime Sci 8, 2 (2019)**. Disponível em: https://doi.org/10.48550/arXiv.1204.0197. Acesso em: 2 out. 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.

KEARY, J. Rebuffing Russian. ransomware: How the United States Should Use the Colonial Pipeline and JBS USA Hackings as a Defense Guide for ransomware. **eReposity Setton Hall**. Seton Hall University, 2022.

KERAI, P. Remote access forensics for VNC and RDP on Windows platform. **Research Online of Edith Cowan University**. Edith Cowan University, novembro de 2011.

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, jun. 2017.

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 maio 2023.

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

ROSLAN, F. H. A Comparative Performance of Port Scanning Techniques. **Journal of Soft Computing and Data Mining**, v. 4, n. 2, p. 43–51, 2023.

SALEEM Y.. Windows INTERFACE FOR DISABLED PERSON. **Pakistan Journal of Science**, v. 66, n. 1, 2022.

SUBEDI, K. P.; BUDHATHOKI, D. R.; DASGUPTA, D. Forensic Analysis of

\textit{ransomware} Families Using Static and Dynamic Analysis. **2018 IEEE Security and Privacy Workshops (SPW)**, San Francisco, CA, USA p. 180-185, 2018.

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

SHAIROZE M. e EREJ A. The Secrets to MIMIKATZ - The Credential Dumper. **International Journal for Electronic Crime Investigation,** Lahore, Paquistão, v. 5, n. 4, 2021.

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

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