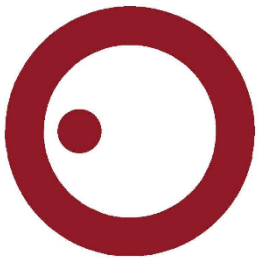


escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão

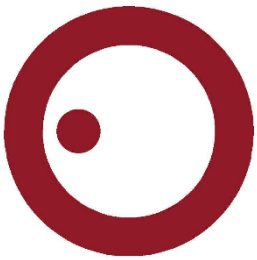
Departamento de Engenharia Informática

Mestrado em Cibersegurança e Informática Forense

ESTRATÉGIA INTEGRADA DE *CONTENT DISARM AND RECONSTRUCTION*

BRAIMA DJALÓ

Leiria, Março de 2025



escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão

Departamento de Engenharia Informática

Mestrado em Cibersegurança e Informática Forense

ESTRATÉGIA INTEGRADA DE *CONTENT DISARM AND RECONSTRUCTION*

BRAIMA DJALÓ

2220413

Dissertação realizada sob orientação da Professora Doutora Maria Micaela Gonçalves Pinto Dinis Esteves e da Professora Doutora Ângela Margarida de Sousa Pereira.

Leiria, Março de 2025

Agradecimentos

Gostaria de agradecer às muitas pessoas que nestes tempos me deram muito auxílio e confiança. Citar nomes pode parecer injusto, pois corro o risco de esquecer alguns, no entanto algumas pessoas foram tão importantes que não agradecer explicitamente a elas seria um erro.

Primeiramente, agradeço a *Allah* e à minha mãe, que me acompanhou nos momentos mais difíceis, importantes e alegres da minha vida, sempre com palavras de carinho, apoio e estímulo.

As minhas orientadoras, pelos seus incentivos, disponibilidade, apoio que sempre demonstraram durante todo este processo.

Agradeço a minha irmã Mariama Safa Baldé, pelo seu incentivo incondicional durante todo este caminho.

Ao meu tio Mamadu Adama Djalo, pelo seu apoio incondicional e por todas as ajudas feitas, porque sem ele seria muito difícil concretizar o meu sonho.

Aos meus colegas que me incentivaram e ajudaram na busca de informações para realização deste trabalho, em especial Prosper Badji.

Para finalizar, gostaria de agradecer a todos os meus professores de mestrado em cibersegurança e informática forense pelos conhecimentos transmitidos no decorrer do curso.

Resumo

A cibersegurança refere-se ao conjunto de práticas, tecnologias e processos utilizados para proteger os sistemas informáticos contra diversos tipos de ciberataques, incluindo *worms*, cavalos de Troia (*trojans*), *ransomware*, *spyware*, entre outros programas ou ficheiros, que podem apresentar-se sob a forma de código executável. Neste contexto, as soluções de segurança digital são aplicadas para proteger os sistemas contra ameaças cibernéticas. Por exemplo, um ficheiro pode estar infetado com *malware* incorporado, sendo que, ao ser aberto, pode desencadear a execução, em segundo plano, de um script que explora o *malware* para infetar o sistema do utilizador. Contudo, nem todos os utilizadores da internet possuem conhecimento suficiente sobre como se protegerem destes tipos de ataques. Neste contexto, surge a tecnologia *Content Disarm and Reconstruction* (CDR), que permite prevenir ataques realizados através de ficheiros potencialmente perigosos. A tecnologia CDR inclui métodos para eliminar objetos potencialmente perigosos incorporados nos ficheiros, incluindo aqueles utilizados em ataques de dia zero, preservando a sua funcionalidade. Esta tecnologia neutraliza o ficheiro ao remover quaisquer elementos potencialmente nocivos, reconstruindo-o posteriormente como um ficheiro seguro e mantendo a sua estrutura e formato original.

Neste estudo foram analisadas diversas tecnologias de CDR, tais como *Metadefender Cloud*, *Exefilter*, VirusTotal, *Glasswall*, *Docbleach* e *Odix*, entre outras, que disponibilizam soluções para análise de ficheiros em tempo real e *offline*. Para a realização da análise, efetuou-se um levantamento das tecnologias CDR existentes, selecionaram-se algumas destas e realizaram-se testes utilizando ficheiros potencialmente perigosos em diversos formatos, tais como PDF, RTF, HTML e DOC. Os resultados obtidos evidenciaram a eficácia das tecnologias CDR analisadas, especialmente quando utilizadas em conjunto para a neutralização e recuperação segura de ficheiros potencialmente infetados.

Palavras-Chaves: Cibersegurança, ciberataques, CDR, *malware*, ficheiros infetados

Abstract

Cybersecurity refers to the set of practices, technologies, and processes employed to protect computer systems against various types of cyberattacks, including worms, Trojan horses (trojans), ransomware, spyware, and other programmes or files that may appear in the form of executable code. In this context, digital security solutions are implemented to safeguard systems from cyber threats. For instance, a file may be infected with embedded malware, which, when opened, could trigger the execution of a background script that exploits the malware to infect the user's system. However, not all internet users have sufficient knowledge on how to protect themselves from these types of attacks. Therefore, the Content Disarm and Reconstruction (CDR) technology has emerged to prevent attacks conducted via potentially harmful files. CDR technology includes methods to eliminate potentially dangerous objects embedded in files, including those utilised in zero-day attacks, preserving the file's functionality. This technology neutralises the file by removing any potentially harmful elements and subsequently reconstructs it into a secure file, maintaining its original structure and format.

In this study, various CDR technologies were analysed, including Metadefender Cloud, Exefilter, VirusTotal, Glasswall, Docbleach, and Odix, among others, which offer solutions for real-time and offline file analysis. To carry out this analysis, existing CDR technologies were surveyed, selected technologies were tested, and potentially harmful files in various formats, such as PDF, RTF, HTML, and DOC, were used. The obtained results demonstrated the effectiveness of the analysed CDR technologies, particularly when combined to neutralise and safely recover potentially infected files.

Keywords: Cybersecurity, cyberattacks, CDR, malware, infected files

Índice

Lista de Figuras

Lista de Tabelas

Lista de Gráficos

Lista de Abreviaturas

ABNT	Associação Brasileira de Normas Técnicas

API	Application Programming Interface
AVI	Audio Video Interleave
AWS	Amazon Web Services
BFSI	Banking, Financial Services and Insurance
BMP	Windows Bitmap
CAGR	Compound Annual Growth Rate
CDR	Content Disarm and Reconstruction
CIP	Critical Infrastructure Protection
COM	Component Object Model
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DOC	Documento do Microsoft Word
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
HTML	HyperText Markup Language
IBM	International Business Machines
ICDR	Image Content Disarm and Reconstruction
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IEC	International Educational Consultants
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
LAMEA	Latin America, Middle East and Africa
MitM	Man-in-the-Middle
MotW	Mark of the Web
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OLE	Object Linking and Embedding

PDF	Portable Document Format
PdfCDR	Portable Document Format Content Disarm and Reconstruction
PNG	Portable Network Graphics
RAR	Roshal Archive
RTF	Rich Text Format
TAP	Transportes Aéreos Portugueses
TI	Tecnologias da Informação
URL	Uniform Resource Locator
VBA	Visual Basic for Applications
XML	Extensible Markup Language
XMP	Extreme Memory Profile

1. Introdução

As transações realizadas através da internet estão constantemente expostas a múltiplas ameaças cibernéticas, devido à ação de uma rede de *hackers* que se mantém vigilante para roubar dados de empresas e clientes, além de violar a privacidade dos utilizadores. Durante a pandemia da COVID-19, as empresas tiveram de se adaptar rapidamente a novos modelos de trabalho, como o teletrabalho, acelerando a transformação digital dos seus processos e respondendo ao aumento da procura por serviços online, o que ampliou significativamente as oportunidades para os *hackers* atacarem os seus alvos.

Na segunda metade do século XX, a cibersegurança surgiu como resposta ao crescimento exponencial da utilização de sistemas informáticos e das redes de comunicação. Com a proliferação de tecnologias digitais, especialmente a partir da década de 70, um conjunto alargado de ameaças e vulnerabilidades colocaram em risco a integridade, confidencialidade e disponibilidade dos dados e sistemas digitais. Consequentemente, tornou-se imprescindível implementar práticas e tecnologias capazes de proteger os sistemas contra ciberataques e salvaguardar informações sensíveis contra acessos não autorizados, ataques maliciosos e outras formas de crime digital [1].

Atualmente, a cibersegurança conta com ferramentas avançadas capazes de mitigar vulnerabilidades exploradas por *hackers*, que podem comprometer sistemas empresariais, roubar dados pessoais de clientes, aceder indevidamente a informações confidenciais de indivíduos ou obter ilegalmente informações financeiras de organizações. Esta evolução contínua das tecnologias e práticas de segurança digital é fundamental para enfrentar os desafios e ameaças de um cenário digital cada vez mais complexo e em permanente transformação [1].

Ciberataques ou ataques cibernéticos referem-se à exploração das vulnerabilidades existentes nos sistemas informáticos para obter acesso não autorizado a um computador ou sistema informático, causando danos e aproveitando-se das falhas de segurança ou de sistemas proporcionados pelos próprios *hackers* [2].

Entre os diversos tipos de ciberataques, destaca-se o *phishing,* uma forma de ataque cibernético que surgiu na década de 1990 e é amplamente utilizado por *hackers,* como parte de técnicas de engenharia social, para obter informações confidenciais de utilizadores. Este tipo de ataque consiste em induzir as vítimas a revelar dados sensíveis, como informações bancárias, palavras-passe ou outros dados pessoais, através de comunicações fraudulentas

que se fazem passar por entidades confiáveis [2]. Outro método, amplamente, utilizado pelos *hackers* para comprometer sistemas informáticos é o *malware* que consiste num *software* criado para infetar sistemas e causar danos, tornando-os inoperantes. Esses programas podem se manifestar de diversas formas, como vírus, *worms*, cavalos de Troia, *spywares*, entre outros. O *ransomware*, uma forma específica de *malware*, foi detetado, pela primeira vez, no início de fevereiro de 2017. Este *software* malicioso bloqueia o acesso aos sistemas e encripta todos os dados, tornando-os inacessíveis aos utilizadores. Nesta situação, os *hackers* exigem o pagamento de um resgate para restaurar o acesso aos dados, geralmente em criptomoedas, sob ameaça de perda permanente das informações. Um exemplo deste tipo de ciberataque, ocorreu à escala mundial, em maio de 2017, desencadeado pela disseminação de um vírus designado *WannaCry, que* infetou mais de 230 mil sistemas em todo o mundo, atingindo empresas de transporte, órgãos públicos, bancos e universidades. O ataque ocorreu porque muitos utilizadores clicaram em ficheiros infetados, permitindo que o vírus se instalasse e bloqueasse o acesso aos dados, levando os atacantes a exigir o pagamento de um resgate para a recuperação das informações [3].

O ataque *Distributed Denial of Service* (DDoS) representa uma ameaça crítica no atual panorama da cibersegurança, consistindo numa técnica baseada na sobrecarga intencional de recursos ou sistemas, dispensando a necessidade de recorrer a métodos de engenharia social. Estes ataques são perpetrados inundando servidores com um volume desmedido de tráfego gerado por dispositivos infetados com *malware*, comprometendo a capacidade de acesso dos utilizadores a serviços e sites *online*. A consequência direta desses ataques é a paralisação dos sistemas, o que pode criar falhas para invasões adicionais ou comprometer a integridade dos produtos digitais oferecidos pelas empresas. Assim, a proteção contra DDoS tornou-se uma prioridade essencial para a segurança cibernética, exigindo estratégias robustas para mitigar seus impactos e garantir a continuidade dos serviços digitais.

O ataque do tipo *Man-in-the-Middle* (MitM) constitui outra grave ameaça cibernética, na qual os cibercriminosos intercetam as comunicações entre duas partes com o objetivo de aceder a informações sensíveis. Ao explorarem vulnerabilidades em protocolos web inadequadamente protegidos, estes atacantes podem obter dados valiosos, comprometendo tanto a segurança da informação como a confiança nas interações digitais. A prevalência deste tipo de ataque reforça a necessidade urgente de adotar protocolos robustos, investir na formação em segurança digital e implementar medidas rigorosas de encriptação, garantindo assim a integridade e privacidade das comunicações na era digital.

Com a diversidade e a sofisticação destes ciberataques, tem se tornado cada vez mais desafiador garantir a segurança total dos sistemas informáticos, especialmente quando estão ligados à internet. A maioria dos utilizadores não possui um conhecimento aprofundado sobre como se proteger contra essas ameaças, o que os torna alvos fáceis para os atacantes. Dessa forma, os *hackers* exploram a fragilidade dos indivíduos em relação a conhecimentos técnicos para aproveitar as vulnerabilidades dos sistemas e obter acesso a dados confidenciais, seja de indivíduos ou organizações.

Atualmente, os programas antivírus têm como principal objetivo garantir a proteção dos equipamentos, detetando, filtrando e removendo automaticamente ficheiros infetados. No entanto, esta abordagem nem sempre é a mais eficaz. Muitas vezes, apenas uma parte dos ficheiros está realmente infetada, pelo que, ao eliminar integralmente esses ficheiros, pode-se acabar por perder informações importantes. Para ultrapassar esta limitação dos antivírus, surgiu uma abordagem alternativa denominada *Content Disarm and Reconstruction* (CDR), que visa proteger os sistemas informáticos contra ciberataques através da remoção de elementos maliciosos, sem comprometer a integridade ou funcionalidade dos ficheiros.

O CDR é uma tecnologia de segurança projetada para eliminar qualquer código malicioso presente em ficheiros que não estejam em conformidade com as políticas de segurança definidas pelo sistema, garantindo assim a entrega segura destes ficheiros aos destinatários. Ao contrário das técnicas tradicionais dos antivírus, que dependem de bases de dados com assinaturas conhecidas para detetar *malware*, o CDR não se baseia em assinaturas, partindo do princípio de que todos os ficheiros podem representar uma ameaça. Em vez de identificar ou analisar a funcionalidade do *malware,* esta tecnologia desconstrói os ficheiros suspeitos, removendo os componentes maliciosos e devolvendo um ficheiro limpo, seguro e funcional. Este método, que surgiu nos últimos anos, tem sido amplamente adotado por empresas que operam na área da cibersegurança, oferecendo uma camada adicional de proteção contra ameaças. O CDR proporciona medidas robustas de segurança para proteger os sistemas contra ataques diversos, incluindo ficheiros infetados, ataques de dia zero (que ocorrem quando um atacante explora uma vulnerabilidade antes que seja disponibilizada uma correção pelos programadores) e infeções por *malware* (situações em que o sistema é comprometido por software malicioso) [4], [5].

As grandes empresas de tecnologia têm reconhecido a importância do processo de CDR como uma estratégia eficaz para mitigar ameaças cibernéticas e prevenir o roubo de dados [6]. Esta consciencialização tem impulsionado a adoção e integração da tecnologia CDR nas

operações das organizações, garantindo que todos os tipos de ficheiros recebidos, incluindo imagens, ficheiros áudio e vídeo, PDFs e documentos nos formatos DOC e XLS, sejam analisados e livres de potenciais ameaças, como *malware* ou outros elementos nocivos. A implementação da tecnologia CDR protege não só os dados sensíveis das organizações, como também reforça a segurança num contexto digital cada vez mais complexo, evidenciando a importância de uma abordagem proativa na mitigação e prevenção de vulnerabilidades [6].

O mercado de CDR tem emergido como um pilar fundamental na cibersegurança, surgindo diversas empresas dedicadas à proteção de sistemas contra os crescentes riscos de ataques baseados em ficheiros. Nos últimos anos, com a intensificação dos ciberataques, a procura por soluções inovadoras e seguras tem se ampliado. As empresas especializadas em CDR não só desenvolvem produtos e serviços que mitigam vulnerabilidades, mas, também, promovem uma abordagem proativa na defesa cibernética, evidenciando a necessidade urgente de proteger informações sensíveis e garantir a integridade dos sistemas digitais.

Neste contexto, em julho de 2022, a OPSWAT, uma empresa de cibersegurança especializada na proteção de infraestrutura crítica (CIP) por meio de soluções avançadas de prevenção de ameaças e segurança, anunciou ter obtido a competência de segurança da *Amazon Web Services* (AWS) na categoria de proteção de dados. A OPSWAT comprovou sua capacidade de oferecer aos clientes conhecimentos em cibersegurança e proteção de dados para apoiá-los no alcance de seus objetivos de segurança na nuvem, cumprindo com sucesso os requisitos técnicos e de qualidade da AWS [7]. Também, em março de 2022, a empresa *Glasswall*, fornecedora de tecnologia de CDR, disponibilizou uma ferramenta para *desktop*. Esta tecnologia foi desenvolvida para ajudar a proteger as organizações dos setores público e privado contra os perigos de ataques baseados em ficheiros, como *malware* e *ransomware*. Em junho do mesmo ano, a empresa lançou um novo plug-in que permite integrar a ferramenta CDR aos *firewalls* de próxima geração da *Palo Alto Networks*. Este *plug-in* garante que os utilizadores estejam protegidos contra ameaças baseadas em ficheiros [7].

Recentemente, a Inteligência Artificial passou a ser utilizada na prevenção e na defesa contra ciberataques. Ao antecipar possíveis falhas, corrigir vulnerabilidades e mitigar automaticamente os danos, procura-se garantir que interrupções de comunicação, recuperação de dados e restabelecimento de serviços ocorram com a maior agilidade possível, minimizando prejuízos e reduzindo o tempo de inatividade [87].

1.1. Objetivos

O CDR tornou-se uma tecnologia de grande relevância na proteção contra ameaças à segurança dos sistemas informáticos, respondendo à constante inovação dos *hackers* em desenvolver novas formas de ataque. Para mitigar os riscos associados à cibersegurança, a tecnologia CDR proporciona uma camada adicional de proteção, identificando e neutralizando código malicioso incorporado nos ficheiros. Quando um ficheiro está infetado, a tecnologia CDR decompõe-no em vários componentes, como anexos, *scripts*, *hiperlinks* e campos de formulário (por exemplo, um e-mail com um *link* para *download* de *software* malicioso), analisando cada segmento na procura de códigos maliciosos e eliminando todos os elementos que representem risco. De seguida, o ficheiro é reconstituído em uma versão segura e completamente livre de ameaças. Ao realizar a inspeção automática de todos os ficheiros recebidos, estas ferramentas eliminam a necessidade de verificações manuais individuais, economizando tempo e recursos, enquanto fornecem proteção contra vírus e outras formas de *malware*. Além disto, as ferramentas CDR contribuem para a eficiência operacional das empresas [8].

Neste contexto, pretende-se com este estudo aprofundar o conhecimento sobre CDR, identificar e analisar algumas tecnologias existentes no mercado, examinar diferentes vulnerabilidades e estudar a forma de neutralizar as potenciais ameaças, incorporadas nos diferentes tipos de ficheiros.

O presente estudo tem como objetivos específicos:

- ✓ Apresentar o conceito de CDR, vantagens e desvantagens, bem como, o âmbito de aplicação;
- ✓ Identificar algumas soluções CDR existentes no mercado;
- ✓ Identificar e analisar as principais vulnerabilidades e estudar a forma de neutralizar as potenciais ameaças;
- ✓ Realizar testes a um conjunto de ficheiros infetados, apresentando e analisando os resultados obtidos.

1.2. Estrutura do Trabalho

Este relatório de dissertação está organizado em seis (6) capítulos:

No capítulo 1, Introdução, faz-se um enquadramento do tema, apresentam-se os objetivos do estudo e a estrutura do trabalho.

No capítulo 2, Conceitos Fundamentais, são introduzidos os conceitos associados ao tema da cibersegurança.

No capítulo 3, *Content Disarm and Reconstruction* (CDR), é apresentado o referencial teórico sobre a tecnologia CDR.

No capítulo 4, Soluções da tecnologia CDR, apresenta diversas opções disponíveis, assim como a respetiva comparação entre elas.

No capítulo 5, Testes e Análise dos Resultados Obtidos, são apresentados os resultados alcançados e inclui uma reflexão crítica sobre os mesmos.

No capítulo 6, Conclusão e Trabalho Futuro, apresenta-se a conclusão e o trabalho futuro.

2. Conceitos Fundamentais

2.1. Cibersegurança

A cibersegurança, também designada por segurança cibernética, refere-se à proteção de redes, dispositivos móveis e *software* contra-ataques maliciosos, como Cavalos de Tróia, vírus, *worms, ransomware, phishing*, ataques de dia zero, engenharia social, *spoofing,* entre outros. Estes ataques podem comprometer a segurança dos sistemas informáticos. A cibersegurança preocupa-se, também, em garantir que pessoas não autorizadas não consigam aceder remotamente aos servidores nem obter acesso aos dados dos sistemas. O principal objetivo da cibersegurança é prevenir ciberataques, que exploram falhas nos sistemas para invadir computadores, roubar informações, manipular dados e tornar indisponíveis diversos ficheiros [9].

Os três pilares fundamentais da cibersegurança – Confidencialidade, Integridade e Disponibilidade – são amplamente reconhecidos como a base para a proteção eficaz de sistemas de informação e dados sensíveis. Este modelo, conhecido como a Tríade CIA (*Confidentiality, Integrity, Availability*), é essencial para compreender as áreas principais de risco e desenvolver estratégias robustas de segurança.

A **confidencialidade** visa garantir que a informação é acessível apenas a indivíduos ou sistemas devidamente autorizados. Este princípio é crucial para proteger dados sensíveis, como informações pessoais, segredos comerciais ou comunicações confidenciais, de acessos não autorizados. Para assegurar a confidencialidade, implementam-se diversas medidas, como a criptografia, que protege os dados em trânsito e em repouso, tornando-os ilegíveis para quem não possui as credenciais apropriadas. Adicionalmente, utilizam-se controlos de acesso, que definem quem pode visualizar, editar ou partilhar informações, frequentemente suportados por mecanismos como a autenticação multifator. Outra prática comum é a segregação de dados, que minimiza os riscos de exposição ao armazenar informações sensíveis em ambientes protegidos ou isolados.

O segundo pilar, a **integridade**, garante que a informação se mantém exata, completa e consistente, assegurando que não foi alterada de forma não autorizada ou acidental. Este princípio é vital para garantir a fiabilidade dos dados utilizados na tomada de decisões e na execução de processos operacionais. Para proteger a integridade da informação, recorrem-se a ferramentas como assinaturas digitais e *hashes* criptográficos, que validam que os dados

não foram alterados desde a sua criação. Paralelamente, os registos de auditoria desempenham um papel importante ao monitorizarem alterações nos sistemas e dados, permitindo a identificação de atividades suspeitas. Outro mecanismo frequentemente utilizado é o controlo de versões, que preserva o histórico de alterações, protegendo contra a perda de dados ou alterações inadvertidas em contextos colaborativos.

Por fim, a **disponibilidade** assegura que a informação, os sistemas e os recursos estão acessíveis e operacionais sempre que necessário. Este princípio é particularmente crítico em setores onde interrupções podem causar consequências graves, como nas áreas da Saúde, das Finanças ou em infraestruturas críticas. Medidas de proteção da disponibilidade incluem a realização de *backups* regulares e a implementação de redundância, que permitem a recuperação de dados e sistemas em caso de falhas ou desastres. Além disso, é fundamental adotar estratégias de mitigação contra ataques de negação de serviço distribuído (DDoS), que visam sobrecarregar os sistemas, tornando-os inacessíveis. A manutenção regular e a monitorização contínua também desempenham um papel essencial, garantindo a funcionalidade dos sistemas e permitindo a deteção precoce de problemas ou ataques.

Embora cada um destes pilares desempenhe um papel distinto, eles estão interligados e dependem uns dos outros para oferecer uma proteção abrangente. Por exemplo, garantir a confidencialidade sem assegurar a integridade pode levar à proteção de informação que está corrompida ou desatualizada. Da mesma forma, a disponibilidade é imprescindível para que a confidencialidade e a integridade tenham valor prático, uma vez que informações inacessíveis não podem ser utilizadas. Assim, a abordagem integrada destes três pilares é indispensável para proteger as organizações contra as crescentes ameaças no ambiente digital e para garantir a resiliência dos sistemas de informação num mundo cada vez mais conectado [10].

A cibersegurança pode ser aplicável a uma variedade de contextos, desde negócios até a computação móvel, e pode ser dividido em algumas categorias comuns:

- ✓ **Segurança de rede:** esta categoria está relacionada com a proteção de redes de computadores contra acessos não autorizados ou intrusões maliciosas. Pode envolver a defesa contra invasores direcionados que procuram explorar vulnerabilidades específicas, bem como contra *malware* oportunista que tenta infetar sistemas de forma automática e indiscriminada. Para alcançar esta proteção, utilizam-se ferramentas como *firewalls,* sistemas de deteção de intrusão (IDS), sistemas de prevenção de intrusões

(IPS), e técnicas de segmentação de rede, que ajudam a limitar o impacto de possíveis ataques.

- ✓ **Segurança Operacional:** Foca-se nos processos e decisões relacionados com o tratamento e proteção de dados armazenados e manipulados pelos sistemas. Inclui a definição de permissões de acesso que regulam quem pode visualizar, editar ou partilhar dados dentro de uma rede. Além disso, contempla os procedimentos que determinam como os dados devem ser armazenados, partilhados e removidos de forma segura. Exemplos incluem o uso de políticas de gestão de privilégios, criptografia de dados em repouso, e estratégias para prevenir o armazenamento de dados sensíveis em dispositivos ou locais não seguros.
- ✓ **Segurança de Informação:** Esta categoria foca-se na proteção da integridade e da confidencialidade dos dados, tanto no momento em que estão armazenados, como durante a sua transmissão entre sistemas. O objetivo é garantir que a informação permaneça confidencial, intacta e acessível apenas a utilizadores ou sistemas autorizados. Para alcançar esse nível de proteção, são utilizados métodos como a criptografia de dados em repouso e em trânsito, bem como, o controlo rigoroso de acessos, assegurando que as informações sensíveis estão sempre protegidas contra acessos não autorizados ou adulterações.
- ✓ **Segurança das Aplicações:** Envolve a proteção de *software* e dispositivos contra ameaças que possam comprometer o seu funcionamento ou a segurança dos dados que processam. Aplicações vulneráveis podem ser uma porta de entrada para cibercriminosos acederem a sistemas críticos ou a informações sensíveis. O sucesso da segurança das aplicações começa na fase de desenvolvimento, onde se implementam práticas como a análise de código para identificar e corrigir vulnerabilidades, a utilização de *frameworks* de segurança robustos e a realização de testes rigorosos antes do lançamento. Além disso, a atualização contínua de *software* para corrigir vulnerabilidades emergentes é essencial para manter a proteção a longo prazo.
- ✓ **Recuperação de desastres e continuidade dos negócios:** Esta área define como uma organização deve reagir a incidentes de cibersegurança ou outros eventos que resultem na perda de operações ou dados. As políticas de recuperação de desastres estabelecem os procedimentos necessários para restaurar operações e informações, permitindo que a organização retorne à sua capacidade operacional anterior ao evento de forma eficiente.

Paralelamente, a continuidade dos negócios refere-se ao plano que a organização adota para manter as atividades essenciais em funcionamento, mesmo com a indisponibilidade de determinados recursos. Esta categoria inclui medidas como *backups* regulares, redundância de sistemas críticos e testes de simulação para garantir a prontidão em caso de desastres.

- ✓ **Educação do utilizador final:** Esta categoria aborda um dos elementos mais imprevisíveis da cibersegurança, os utilizadores. Mesmo os sistemas mais seguros podem ser comprometidos se os utilizadores não seguirem as melhores práticas de segurança. Assim, a formação dos utilizadores finais é essencial para reduzir os riscos associados a erros humanos. Ensinar os colaboradores a identificar e excluir anexos de e-mails suspeitos, evitar a utilização de dispositivos USB desconhecidos e adotar senhas fortes são exemplos de boas práticas a adotar para a segurança organizacional. Além disso, campanhas de sensibilização, simulação de ataques e programas de formação contínuos devem ser implementados para criar uma cultura de cibersegurança dentro da organização [11].

As soluções de Cibersegurança, como antivírus, *firewalls*, antimalware são utilizados para proteger contra *softwares* maliciosos. Por exemplo o *malware* incorporado em itens de documentos é projetado para ser completamente invisível para o utilizador de modo que quando o ficheiro é aberto, o utilizador pode estar completamente inconsciente de um *script* em execução em segundo plano, assim sendo o *malware* aproveita para infetar o sistema, assim como a rede. O CDR inclui tecnologias para eliminar códigos maliciosos incorporados nos ficheiros, e preservando a utilização do ficheiro.

A maioria dos problemas de segurança são criados por pessoas maliciosas que tentam ganhar algum benefício com isso [9].

Os problemas de segurança na área de cibersegurança podem surgir por diversos motivos, dependendo dos atores envolvidos e das suas intenções. A tabela 1 ilustra alguns exemplos de perfis de indivíduos ou organizações que podem causar problemas de segurança, bem como os respetivos objetivos ou motivações. Encontra-se uma explicação detalhada para cada caso apresentado na tabela 1.

Hacker	Motivo
Terrorista	Para roubar projetos de armas biológicas
Estudantes	Para se divertir a bisbilhotar e-mails
Cracker	Para testar o sistema de segurança ou roubar dados
Empresa	Para descobrir o plano estratégico de uma empresa
Contabilista	Para desviar dinheiro de uma empresa
Governo	Para descobrir segredos militares de um inimigo
Ladrão	Para roubar números de cartões bancários

Tabela 1- Motivos que podem causar problema de segurança [9]

Os terroristas utilizam técnicas de ciberataque para aceder a informações altamente sensíveis, como projetos relacionados com armas biológicas. Este tipo de atividade representa um risco elevado para a segurança global, dado o potencial para ser utilizado em ações que colocam vidas humanas em perigo e ameaçam a estabilidade internacional.

Já os estudantes, frequentemente impulsionados pela curiosidade ou pela busca de desafios, podem explorar sistemas e aceder a *e-mails* ou informações privadas sem considerar as consequências das suas ações. Embora estas práticas possam parecer inofensivas, podem comprometer a privacidade de dados e expor informações sensíveis a terceiros.

Os *crackers*, em contraste com os *hackers* éticos, realizam ataques intencionais para testar sistemas de segurança, identificar vulnerabilidades ou roubar dados. Estas ações maliciosas podem resultar em perdas significativas, como a exposição de informações confidenciais, prejuízos financeiros e danos à reputação de organizações.

No contexto corporativo, algumas empresas recorrem a práticas de espionagem para obter informações estratégicas dos seus concorrentes. Estas ações, que envolvem frequentemente o acesso não autorizado a sistemas de informação, têm como objetivo obter vantagens competitivas, comprometendo a ética empresarial e a confiança no mercado.

No caso de atores internos, como contabilistas, o acesso privilegiado a sistemas financeiros pode ser explorado para desviar dinheiro de uma organização. Estas ameaças internas são particularmente preocupantes, pois podem permanecer indetetadas durante longos períodos, amplificando os danos financeiros e operacionais.

Os governos, por sua vez, utilizam frequentemente ciberataques como ferramentas estratégicas para descobrir segredos militares ou políticos de países rivais. Estas atividades de ciberespionagem representam uma ameaça à segurança nacional e podem desestabilizar relações geopolíticas.

Por fim, os ladrões são frequentemente motivados por objetivos financeiros, utilizando cibercrimes para roubar informações bancárias, como números de cartões de crédito. Estas ações têm impacto direto sobre indivíduos, resultando em perdas financeiras e questões relacionadas com a proteção de dados pessoais.

A análise dos diferentes perfis de atores e das suas motivações revela que os problemas de segurança são diversos e complexos, variando significativamente em função do contexto e dos objetivos. Compreender estas dinâmicas é crucial para desenvolver estratégias de cibersegurança eficazes, que permitam mitigar os riscos e proteger sistemas e informações contra as ameaças mais variadas.

2.2. Ciberataques

Os ciberataques representam uma das maiores ameaças à segurança e à estabilidade no mundo digital atual. Com o crescimento exponencial da conectividade e da dependência tecnológica, os sistemas informáticos e as redes tornaram-se alvos preferenciais de indivíduos, organizações e estados que procuram explorar vulnerabilidades para alcançar objetivos maliciosos. Estes ataques variam em sofisticação e alcance, podendo comprometer informações pessoais, estratégias empresariais, infraestruturas críticas e até mesmo a segurança nacional [12].

O termo "ciberataque" refere-se a qualquer ação deliberada que vise perturbar, danificar ou obter acesso não autorizado a sistemas, dispositivos, redes ou dados. A evolução das técnicas de ataque, combinada com o aumento do número de atores envolvidos – desde *hackers* individuais a grupos organizados e governos – tem ampliado a escala e o impacto destas ameaças. A motivação por detrás dos ciberataques é diversificada, podendo incluir ganhos financeiros, espionagem, sabotagem ou até a promoção de ideologias específicas [13].

Há quatro tipos principais de ciberataques: os ataques passivos, os ataques ativos, os ataques internos e os ataques externos [12]. Os ataques passivos ocorrem quando os criminosos cibernéticos procuram agir de forma discreta, evitando qualquer ação que possa levar à sua deteção. O objetivo principal destes ataques é roubar dados e informações confidenciais, como credenciais de acesso, informações financeiras ou segredos empresariais. Exemplos

comuns incluem escutas de comunicações digitais *(sniffing*) e análise de tráfego de rede para capturar informações sensíveis. Apesar de não causarem interrupções diretas no funcionamento dos sistemas, os ataques passivos podem resultar em prejuízos graves devido à exposição de dados críticos.

Diferentemente dos ataques passivos, os ataques ativos têm como objetivo causar danos significativos e frequentemente irreparáveis aos sistemas informáticos. Estes ataques podem incluir ações como a manipulação ou destruição de dados, interrupções em serviços ou até mesmo o colapso completo de redes organizacionais. Exemplos de ataques ativos incluem injeção de código malicioso, ataques de DDoS e a disseminação de *malware.* O impacto destes ataques pode ser devastador, comprometendo a integridade e a disponibilidade dos sistemas e gerando grandes prejuízos operacionais e financeiros.

Os ataques internos são realizados por indivíduos que fazem parte da própria organização e que têm algum nível de acesso aos sistemas. Estes atacantes podem ser funcionários, colaboradores ou prestadores de serviços que utilizam os seus privilégios para comprometer a segurança. As motivações podem incluir vingança, ganhos financeiros ou cooperação com atores externos. Este tipo de ataque é particularmente perigoso, pois os atacantes já têm acesso direto ao ambiente interno, muitas vezes conseguindo evitar mecanismos de segurança externos. Exemplos incluem o roubo de dados confidenciais, manipulação de transações ou sabotagem de sistemas.

Por fim, os ataques externos são realizados por indivíduos ou grupos que não pertencem à organização e que não possuem acesso direto aos seus sistemas. Estes atacantes recorrem a métodos como a exploração de vulnerabilidades, *phishing,* força bruta para comprometer credenciais ou engenharia social para enganar utilizadores internos. A sua principal motivação pode ser o roubo de dados, a interrupção de serviços ou a obtenção de ganhos financeiros. Por serem originados fora da organização, estes ataques exigem sistemas de defesa robustos, como *firewalls*, sistemas de deteção de intrusões e políticas de segurança eficazes [12].

Em Portugal, a incidência de ciberataques em diversos setores, incluindo Telecomunicações, Transporte, Educação e Saúde, evidencia a crescente vulnerabilidade das infraestruturas críticas do país frente a ameaças digitais. Esses ataques não apenas comprometem a segurança e a integridade das informações sensíveis, mas também podem causar interrupções significativas nos serviços essenciais, afetando a vida cotidiana dos cidadãos e

a eficiência das operações empresariais. A necessidade urgente de fortalecer as medidas de cibersegurança e promover uma cultura de proteção digital destaca-se como uma prioridade, visando mitigar os riscos associados a essas ameaças e garantir a resiliência dos sistemas em face de futuros incidentes.

No dia 7 de fevereiro de 2022, a Vodafone Portugal foi alvo de um dos maiores ciberataques registados no país, causando um impacto significativo tanto em clientes particulares como empresariais. O ataque resultou numa interrupção generalizada dos serviços da operadora, afetando redes móveis e fixas, televisão e outros serviços baseados em redes de dados. Os serviços de voz em redes móveis, particularmente 2G e 3G, sofreram graves interrupções, enquanto as redes 4G e 5G, que dependem de dados, ficaram praticamente inoperacionais. Além disso, os serviços de televisão deixaram de estar acessíveis a muitos clientes, e funcionalidades essenciais, como mensagens de texto e sistemas digitais, foram severamente comprometidas. Empresas que dependiam de terminais de pagamento e sistemas de gestão baseados em redes de dados também enfrentaram dificuldades significativas.

Embora os detalhes técnicos exatos do ataque não tenham sido divulgados, foi confirmado que se tratou de uma ação deliberada e altamente sofisticada. A Vodafone garantiu que não houve acesso ou roubo de dados pessoais dos clientes, mas o impacto operacional foi extenso, exigindo uma resposta imediata. Equipas especializadas em cibersegurança e engenheiros técnicos foram mobilizados para mitigar os danos e restaurar os serviços. A recuperação total ocorreu de forma faseada, priorizando serviços essenciais, como a rede móvel de voz e os sistemas empresariais críticos. O ataque motivou uma investigação por parte das autoridades nacionais, destacando a crescente ameaça às infraestruturas críticas [14].

No mesmo dia, os Laboratórios Germano de Sousa foram alvo de um ataque informático que causou significativos transtornos operacionais. Suspeita-se que tenha sido um ataque do tipo *ransomware*, um dos métodos mais comuns e disruptivos utilizados por cibercriminosos. Este tipo de ataque envolve a encriptação dos dados da vítima, bloqueando o acesso aos sistemas até que um resgate seja pago. Como resultado, a rede dos laboratórios foi comprometida, afetando a comunicação com vários hospitais parceiros, incluindo os hospitais do Grupo Mello e do Grupo CUF.

Apesar do impacto operacional, os responsáveis pelos Laboratórios Germano de Sousa afirmaram que os dados dos clientes não foram comprometidos, assegurando que nenhuma

violação de informações sensíveis ocorreu. Este facto é particularmente relevante, considerando o tipo de dados tratados pela instituição, que incluem informações médicas e laboratoriais de extrema sensibilidade.

O ataque destacou a vulnerabilidade de instituições de saúde face a ciberameaças e sublinhou a necessidade de implementar medidas robustas de cibersegurança. Num setor onde a continuidade das operações é crítica, os efeitos de um ataque informático podem ser amplamente sentidos, desde a interrupção de serviços até à possível perda de confiança por parte dos pacientes e parceiros [15], [16].

No dia 30 de março de 2022, foi detetado um ataque à Sonae MC, uma das maiores empresas de retalho em Portugal. Este incidente afetou o funcionamento da plataforma Continente Online e da aplicação do Cartão Continente, dois serviços amplamente utilizados pelos clientes. A empresa confirmou que o ataque resultou na indisponibilidade temporária destes sistemas, causando transtornos tanto para os consumidores como para as operações internas.

De acordo com a Sonae MC, o ataque foi identificado como uma ação maliciosa direcionada aos seus sistemas informáticos. Apesar da gravidade da situação, a empresa assegurou que não houve comprometimento dos dados pessoais ou financeiros dos clientes, sublinhando que a proteção da privacidade dos seus utilizadores permaneceu intacta durante o incidente.

A Sonae MC reagiu de forma célere, ativando os seus protocolos de segurança e contando com a colaboração de equipas especializadas em cibersegurança para mitigar os impactos do ataque. Paralelamente, a empresa cooperou com as autoridades competentes para investigar a origem e a natureza do ataque, reforçando o compromisso em garantir a segurança dos seus sistemas e a confiança dos clientes. A resposta da Sonae MC demonstra o papel crítico de estratégias proativas de cibersegurança na mitigação dos danos e na rápida recuperação dos serviços, num contexto em que ataques deste tipo se tornam cada vez mais frequentes e sofisticados [17].

No dia 26 de abril de 2022, o Hospital Garcia de Orta enfrentou um ataque informático de grande impacto, do tipo *ransomware,* que comprometeu todos os seus sistemas informáticos. O incidente paralisou as operações digitais da unidade hospitalar, deixando indisponíveis os sistemas essenciais para o registo e gestão de informações clínicas, agendamentos e comunicação interna, elementos indispensáveis para o funcionamento eficaz de uma instituição de saúde.

Os atacantes encriptaram os dados da unidade e exigiram o pagamento de um resgate em *bitcoins* para restaurar o acesso aos sistemas. Este tipo de ataque é caracterizado pela utilização de criptomoedas como forma de pagamento, devido à sua natureza descentralizada e difícil rastreabilidade, o que complica a identificação dos autores do crime. A exigência de pagamento em *bitcoins* reflete uma estratégia comum entre cibercriminosos para maximizar os lucros enquanto minimizam o risco de serem detetados.

A interrupção dos sistemas teve repercussões graves na prestação de cuidados médicos, obrigando os profissionais de saúde a recorrerem a métodos manuais para gerir as operações, desde o registo de pacientes até à coordenação de tratamentos. A ausência de sistemas digitais representou um desafio significativo para a equipa hospitalar, que teve de lidar com atrasos e dificuldades acrescidas na prestação de cuidados de saúde [18]. Este caso evidencia as vulnerabilidades das instituições de saúde perante ciberataques, sobretudo face à sua crescente dependência de infraestruturas tecnológicas.

Em novembro de 2022, a Segurança Social de Portugal foi alvo de um ciberataque que comprometeu a segurança das suas redes informáticas. Este ataque, descrito como uma intrusão intencional e maliciosa, teve como alvo as contas de 14 mil funcionários, expondo vulnerabilidades nos sistemas internos da instituição. Apesar da gravidade da situação, as autoridades garantiram que os dados pessoais de cidadãos, contribuintes e empresas não foram comprometidos, um aspeto fundamental para preservar a confiança pública na instituição.

O ataque teve como principal consequência o acesso não autorizado a contas de utilizadores internos, o que poderia ter facilitado a exploração de sistemas ou informações sensíveis. No entanto, a resposta rápida e a implementação de medidas de contenção impediram danos mais extensos, preservando a integridade dos dados pessoais dos cidadãos e das empresas que dependem dos serviços da Segurança Social [19].

Em agosto de 2023, a companhia aérea Transportes Aéreos Portugueses (TAP) foi alvo de um ataque informático de grande dimensão, atribuído a um grupo de *hackers* especializado em r*ansomware*. Este tipo de ataque, caracterizado pela encriptação de dados e pela extorsão de resgates, resultou na divulgação pública de dados pessoais de 1,5 milhões de clientes da companhia. Entre as informações expostas estavam nomes, moradas e até alegados acordos comerciais da TAP, gerando sérias preocupações quanto à privacidade e segurança dos clientes afetados.

O impacto financeiro deste incidente foi igualmente significativo, com o CEO da companhia a estimar uma perda total de 5,7 milhões de euros. Estes prejuízos incluem os custos diretos relacionados com a mitigação do ataque e a recuperação de sistemas, bem como as repercussões operacionais e reputacionais para a TAP [20].

Os casos apresentados demonstram a crescente sofisticação e frequência dos ciberataques, que afetam setores críticos como saúde, retalho, aviação e serviços públicos. Estes incidentes sublinham a vulnerabilidade das organizações, independentemente da sua dimensão ou área de atuação, e evidenciam o impacto significativo que os ciberataques podem ter na operacionalidade, privacidade de dados e confiança dos utilizadores. A diversidade de ataques analisados, desde *ransomware* a intrusões maliciosas, destaca a necessidade de estratégias de cibersegurança robustas, que incluam medidas preventivas, monitorização contínua e respostas rápidas a incidentes. Para além da proteção tecnológica, é essencial promover a colaboração entre organizações e autoridades competentes, bem como investir na sensibilização e formação de colaboradores, de modo a criar resiliência num ambiente digital cada vez mais desafiante. Estes exemplos servem de alerta e reforçam a urgência de uma abordagem integrada à cibersegurança, essencial para mitigar os riscos e garantir a continuidade e a confiança nos sistemas digitais.

2.3. Malware

O termo *malware*, abreviatura de "*malicious software*", refere-se a qualquer programa ou código desenvolvido com o objetivo de executar ações prejudiciais ou atividades maliciosas num computador, dispositivo ou rede. Este tipo de *software* é projetado para infiltrar, danificar ou obter controlo não autorizado sobre sistemas, explorando vulnerabilidades tecnológicas ou humanas. O *malware* é uma das principais ameaças à cibersegurança e tem evoluído em complexidade e sofisticação, acompanhando o crescimento da dependência das infraestruturas digitais [21].

O *malware* apresenta-se sob várias formas. Seguem-se alguns tipos comuns:

- ✓ ***Vírus:*** é um programa do computador que infecta os computadores através da propagação de ficheiros em suportes removíveis ou recebidos através de *e-mails* ou páginas de internet.
- ✓ ***Worm:*** é um tipo de *malware* que propaga automaticamente na rede, e cria cópias de si mesmo em diferentes locais dos sistemas e se espalhe para outras máquinas. Os *worms*

propaga através da exploração automática de vulnerabilidades existentes em programas instalados em computadores.

- ✓ ***Cavalo de Tróia:*** é um tipo de *malware* que permite que o criminoso cibernético obtenha acesso aos sistemas das vítimas. Os utilizadores são enganados de alguma forma para realizarem um *download* de um programa ou para abrirem um anexo de *e-mail*, após isso o *malware* é instalado na máquina do utilizador.
- ✓ ***Spyware:*** é um *software* malicioso que permite controlar as atividades dos utilizadores e transmitir os seus dados sem o consentimento do utilizador.
- ✓ ***Ransomware*****:** é um tipo de *malware* que infeta os sistemas das vítimas, encriptando todos os dados da vítima tornando os dados inacessíveis. Depois do ataque o *hacker* pede um resgate à vítima para permitir que a vítima consiga recuperar os seus dados. A grande maioria das infeções por *ransomware* ocorrem por *e-mail* através de campanhas de *Phishing*, que nada mais são do que *e-mails* falsos, estruturados de maneira que a vítima pense que são *e-mails* verdadeiros. Esses *e-mails* sempre solicitam alguma ação do utilizador como clicar no anexo ou num *link* para fazer *download* de um ficheiro infetado após a ação o *ransomware* se instala e se conecta com o *hacker* que originou o ataque, o *malware* inicia o ataque encriptando todos os dados da vítima e, por fim, pede um resgate à vítima, conforme ilustrado na figura 1.

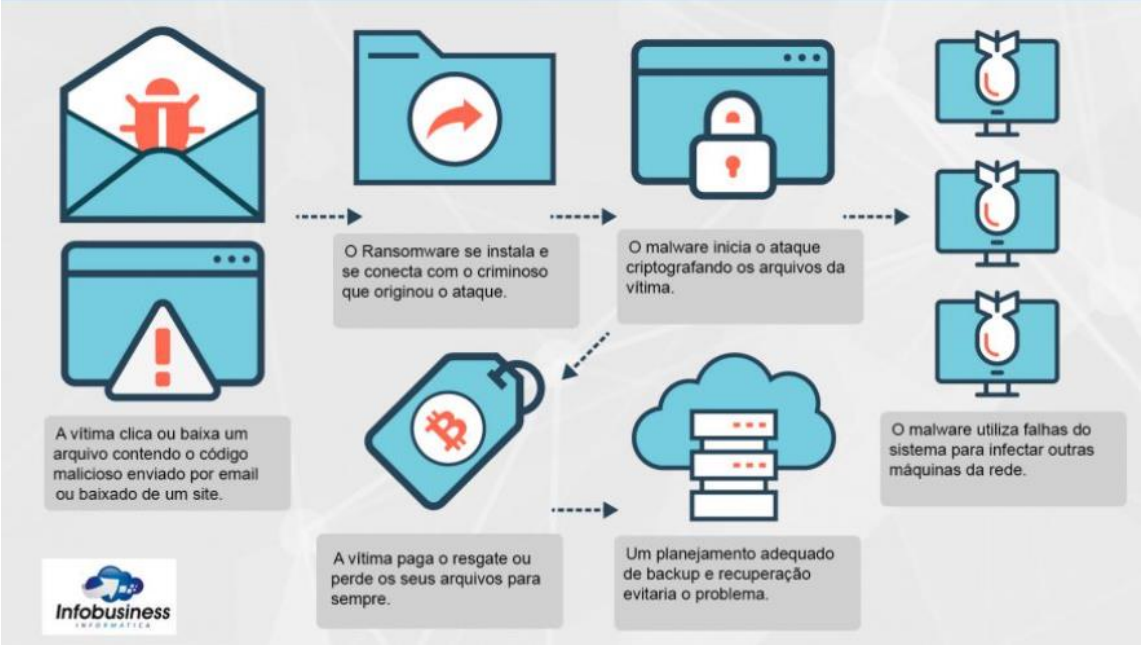


Figura 1- Funcionamento de um ataque do tipo *ransomware* [83]

- ✓ ***Backdoor:*** é uma falha de segurança que os cibercriminosos utilizam para comprometer a segurança dos sistemas informáticos das organizações, facilitando o acesso não autorizado aos recursos do sistema. Este tipo de vulnerabilidade é frequentemente explorado através de *trojans,* que são *softwares* maliciosos disfarçados de programas legítimos. Estes *trojans* são especialmente perigosos porque permitem que os cibercriminosos realizem uma série de ações prejudiciais, incluindo a modificação ou eliminação de ficheiros importantes. Além disso, possibilitam a execução de programas maliciosos que podem comprometer ainda mais o sistema. Estes programas podem ser utilizados para distribuir grandes quantidades de *e-mails* infetados, o que facilita a propagação de *malware* para outros sistemas. Outro risco associado às *backdoors* é a instalação de ferramentas maliciosas adicionais, que podem manter o acesso dos cibercriminosos ao sistema, mesmo após as vulnerabilidades iniciais serem corrigidas. Este acesso contínuo pode ser usado para recolher dados sensíveis, monitorizar atividades ou causar danos mais graves ao sistema e à organização como um todo [22].
- ✓ ***Rootkit:*** é um software malicioso que permite que os cibercriminosos tenham acesso não autorizado a um computador, uma aplicação ou uma rede. O *rootkit* é um *malware* que é muito difícil de ser detetado, pode ficar oculto por muito tempo num sistema infetado. Várias vezes os *rootkit* podem aparecer como uma única peça de *software* legítimo, só que são geralmente compostas por uma coleção de ferramentas que permitem os cibercriminosos o controle a nível de administrador sobre o sistema que é alvo do ataque. Os *rootkits* funcionam perto ou dentro do *kernel* do sistema operativo. Ele consegue executar comandos com certa facilidade. Também pode ocultar *keyloggers* para saber quais teclas foram pressionadas e, consequentemente ter acesso a cartão de crédito, dados pessoais, bancários ou qualquer outra informação sensível [94].
- ✓ ***Botnet:*** é uma rede de computadores infetados por *malware* que estão sob controlo de cibercriminosos e podem ser operados remotamente. Estes *malwares* são desenvolvidos com o objetivo de serem difíceis de detetar, permanecendo ativos em segundo plano e agindo apenas quando recebem instruções específicas do controlador da *botnet*. Este tipo de rede é utilizado para realizar diversas atividades maliciosas, como ataques de negação de serviço distribuído (DDoS), envio de *spam* em massa, roubo de dados ou disseminação de outros tipos de *malware.* A capacidade de operar de forma discreta e coordenada faz das *botnets* uma ferramenta poderosa e perigosa para cibercriminosos,

que conseguem mobilizar recursos de forma eficaz sem o conhecimento dos utilizadores dos computadores infetados [23].

- ✓ ***Adware:*** é um *software* malicioso projetado para redirecionar o navegador dos utilizadores para uma grande quantidade de anúncios, sem a sua permissão. Este tipo de s*oftware* é frequentemente exibido na forma de *pop-ups,* que aparecem de forma invasiva durante a navegação, e pode realizar d*ownloads* de forma secreta no dispositivo do utilizador. Além disso, esses anúncios muitas vezes contêm URLs que direcionam para *software* de terceiros, potencialmente malicioso, que pode comprometer ainda mais a segurança do sistema. Os *adwares* perturbam a experiência do utilizador e podem expor os dispositivos a riscos adicionais, como infeções por *malware* ou roubo de dados sensíveis [24].
- ✓ ***Phishing:*** são programas maliciosos ou técnicas de engenharia social projetados para enganar as pessoas a partilharem informações confidenciais, como senhas, dados bancários ou números de cartões de crédito. O objetivo principal do *phishing* é obter essas informações através de métodos enganosos, como o envio de *e-mails* fraudulentos ou mensagens aparentemente legítimas, que direcionam os utilizadores para páginas falsas. Essas páginas fraudulentas são frequentemente projetadas para imitar sites de instituições confiáveis, induzindo os utilizadores a fornecer os seus dados de forma involuntária. O *phishing* representa uma ameaça significativa à segurança, pois explora a confiança dos utilizadores e pode resultar em perdas financeiras e comprometimento da privacidade [25].
- ✓ ***Exploits:*** é um termo utilizado para descrever *softwares* ou códigos maliciosos que têm como objetivo assumir o controlo dos sistemas ou roubar dados de uma rede. Estes códigos são projetados para explorar pontos fracos em *softwares*, aproveitando vulnerabilidades específicas para comprometer a segurança dos sistemas. Os *exploits* são particularmente perigosos porque atuam de forma direcionada, utilizando métodos específicos para tirar proveito de falhas conhecidas, e podem causar danos significativos às redes e infraestruturas afetadas. Além disso, são frequentemente utilizados como parte de ataques maiores, como a instalação de *malware* adicional ou o acesso não autorizado a dados sensíveis, amplificando o seu impacto [26].

2.3.1. Resumo comparativo dos tipos de *malwares*

Em síntese, cada tipo de *malware* é distintivo em suas características, incluindo métodos de obtenção, instalação, propagação e ações maliciosas que realizam nos sistemas comprometidos. A análise dessas particularidades é essencial para a compreensão e mitigação dos riscos associados, e a tabela 2 serve como uma ferramenta ilustrativa que resume essas diferenças, facilitando a identificação e a resposta adequadas a cada ameaça cibernética. Esta comparação é fundamental para profissionais de segurança que buscam desenvolver estratégias eficazes de defesa contra um panorama de *malware* em constante evolução.

Tipos de *Malwares*	Vírus	*Worms*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Modo de obtenção							
Recebido automaticamente pela rede		Sim	Sim				
Recebido por e-mail	Sim	Sim	Sim	Sim	Sim		
Transferido de web sites	Sim	Sim	Sim	Sim	Sim		
Partilha de Ficheiros	Sim	Sim	Sim	Sim	Sim		
Uso de unidades removíveis	Sim	Sim	Sim	Sim	Sim		
Redes sociais	Sim	Sim	Sim	Sim	Sim		
Mensagens instantâneas	Sim	Sim	Sim	Sim	Sim		
Inserido por um invasor		Sim	Sim	Sim	Sim	Sim	Sim
Acção de outro código malicioso		Sim	Sim	Sim	Sim	Sim	Sim
Como ocorre a instalação:							
Execução de um ficheiro malicioso	Sim						
Execução explicita de outro código malicioso		Sim	Sim	Sim	Sim		

Tipos de *Malwares*	Vírus	*Worms*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Via execução de outro código malicioso						Sim	Sim
Exploração de vulnerabilidades		Sim	Sim			Sim	Sim
Como se propaga:							
Inseri uma cópia de si próprio nos ficheiros do sistema	Sim						
Envia uma cópia de si próprio automaticamente pela rede		Sim	Sim				
Não se propaga				Sim	Sim	Sim	Sim
Acções maliciosas mais comuns:							
Altera ou remove ficheiros	Sim			Sim			Sim
Consome grande quantidade de recursos		Sim	Sim				
Rouba informações sensíveis			Sim	Sim	Sim		
Instala outros códigos maliciosos		Sim	Sim	Sim			Sim
Possibilita o retorno do invasor						Sim	Sim
Envia spam e phishing			Sim				
Aplica ataques na Internet		Sim	Sim				
Procura manter-se escondido	Sim				Sim	Sim	Sim

Tabela 2- Tabela comparativa dos softwares maliciosos [84]

2.3.2. Métodos para Deteção e Prevenção de Malware

Existem diversos métodos de deteção e prevenção de *malware* para identificar a presença de *software* malicioso num sistema. Seguem-se os principais métodos de deteção e prevenção de *malware*:

- ✓ **Método Baseado em assinatura:** O *malware* é um programa que permite causar danos num sistema informático, ele pode ser extraído naturalmente da sua assinatura. No entanto, quando um sistema está infetado por *malware* é preciso realizar uma análise para obter o resultado de amostra do *malware*, após obter o resultado a assinatura é registada e inserida no base de dados. Quando um sistema for infetado os antivírus utilizam este base de dados para procurar a assinatura deste *malware* e notificar o utilizador se o ficheiro correspondente a esta assinatura no base de dados do antivírus. Um problema pode acontecer quando um *malware* não for identificado, ou seja, não está no base de dados do antivírus, pode não ser identificado pelo antivírus neste caso o sistema pode ser infetado com este *malware* [27].
- ✓ **Método SandBox:** *Sandboxing* é um meio de isolar aplicações, códigos potencialmente maliciosos ou sistemas operativos para realizar testes. Ele é muitos utilizado para prevenir de ataques de *ransomware, trojan e spyware*. O *Sandboxing* limita os recursos disponíveis para o item isolado, isto permite que o item seja utilizado para avaliação, evitando quaisquer danos ou prejuízos ao sistema ou dispositivo de armazenamento [28]. O *sandboxing* é utilizado em vários contextos, para a área de segurança de informação é utilizada para testar códigos maliciosos, também serve para testar códigos para prevenir de erros de programação. O *sandboxing* tem grandes vantagens porque permite manter sistemas seguras, bloqueia códigos maliciosos, previne de ameaças de dia zero.
- ✓ **Inteligência artificial:** A Inteligência Artificial (IA) pode ser utilizada para prevenir dos ciberataques. Este método permite que os sistemas aprendam de forma automática identificar características dos *malwares* [27]. Por outro lado, a IA ajuda a detetar, evitar e diminuir ciberameaças devido à autenticação inteligente e à resposta automatizada a possíveis ciberataques. Com a capacidade de analisar grandes volumes de dados em tempo real, a IA pode identificar padrões e comportamentos na anômalos que indicam possíveis ameaças. A IA não depende exclusivamente de regras pré-definidas, tornando-lhe mais adaptável e eficaz diante de novos tipos de ciberataques. Além disso, pode ser utilizada na análise de ficheiros suspeitos em busca de comportamentos maliciosos. A IA

pode examinar o conteúdo de ficheiros em busca de indícios de atividades maliciosas como códigos maliciosos embutidos ou comportamentos suspeitos [29]. Uma das maiores vantagens da IA na cibersegurança é a sua capacidade de automatizar as tarefas. Os algoritmos de aprendizagem de máquina podem ser treinados para identificar padrões e anomalias no tráfego da rede, permitindo detetar e responder a ameaças em tempo real. Por exemplo os sistemas de deteção de intrusão (IDS) baseado em IA podem detetar e bloquear automaticamente o tráfego de rede mal-intencionado, sem intervenção humana [30].

A par destes métodos, outros têm sido citados na literatura. A literatura recente tem apresentado uma série de métodos inovadores relacionados com o CDR, destacando aplicações específicas para diferentes formatos de ficheiros, que são frequentemente explorados por cibercriminosos para ataques a dados confidenciais.

De acordo com o artigo de Eli Belkind, Rand Dubin e Amit Dvir [31], publicado em julho de 2023, o sistema *Image Content Disarm and Reconstruction* (ICDR) foi desenvolvido para lidar com a crescente ameaça de códigos maliciosos ocultos em imagens. Os atacantes utilizam este método para esconder códigos maliciosos ou dados confidenciais em imagens legítimas, tanto para atacar os seus alvos como para exfiltrar informações sensíveis de dispositivos comprometidos. O sistema ICDR foi projetado para identificar e remover esses códigos maliciosos, garantindo que as imagens fiquem seguras antes de serem utilizadas. Esta abordagem representa um avanço significativo na proteção contra um vetor de ataque frequentemente negligenciado.

No artigo publicado por Ran Dubin [32], em fevereiro de 2023, foi apresentado o sistema DeepCDR, especificamente desenvolvido para o desarmamento e reconstrução de ficheiros no formato *Rich Text Format* (RTF). Este formato, amplamente utilizado por ser compatível com várias plataformas e aplicações, tornou-se um alvo comum para cibercriminosos que escondem códigos maliciosos em documentos aparentemente inofensivos. O sistema DeepCDR permite proteger organizações ao eliminar estas ameaças, garantindo que ficheiros RTF infetados não entrem em sistemas corporativos. Além disso, este método reforça o conceito de Zero *Trust*, onde nenhum ficheiro é considerado seguro até ser inspecionado e reconstruído.

Num outro artigo publicado por Ran Dubin [33], em abril de 2023, foi explorado o desarmamento e reconstrução de ficheiros PDF, um dos formatos mais explorados pelos

hackers devido às suas características flexíveis e amplamente utilizadas. Uma vez que os PDFs estão entre os ficheiros maliciosos mais comuns, um exemplo mencionado foi o uso do *Snake Keylogger,* que incorporava um ficheiro DocX malicioso num PDF para enganar o utilizador e evitar a deteção. Os PDFs podem incluir elementos como imagens atrativas, *hiperlinks*, componentes ativos e *exploits*, tornando-os alvos privilegiados para ataques.

O artigo apresentou a ferramenta PdfCDR para desarmar ficheiros PDF. O sistema identifica o tipo de ficheiro, aplica as regras do CDR, e, caso o ficheiro não possa ser desarmado, ele é compactado com proteção por senha e enviado para quarentena. Os resultados mostraram que 90% dos ficheiros maliciosos foram limpos com sucesso, enquanto os restantes 10%, que apresentavam estruturas anormais, foram colocados em quarentena. Esta abordagem reforça a proteção de sistemas industriais e corporativos que não podem depender apenas de antivírus [33].

Ainda Ran Dubin apresentou o primeiro sistema CDR desenvolvido para lidar com ficheiros no formato OLE (*Object Linking and Embedding*), utilizado por aplicações da *Microsoft Office*, como Word (DOC), Excel (XLS) e PowerPoint (PPT). Este formato é conhecido pela sua complexidade e pelo número significativo de vetores de ataque que pode incluir, como objetos incorporados, comandos ocultos, *links* externos e elementos de engenharia social.

O sistema proposto automatiza a conversão de regras de deteção em regras de desarmamento e reconstrução, neutralizando ameaças antes que possam ser exploradas. O formato OLE, devido à sua ampla utilização e natureza complexa, é um alvo de alto risco para cibercriminosos. Estudos demonstram que este tipo de ficheiro pode ser utilizado para incorporar imagens enganosas, comandos maliciosos e outros *exploits* sofisticados. A introdução deste sistema reforça a proteção contra ameaças frequentemente associadas a ficheiros OLE [34].

Os avanços na tecnologia CDR destacam a necessidade de soluções específicas para diferentes formatos de ficheiros, dado que os cibercriminosos continuam a explorar vulnerabilidades em formatos amplamente utilizados. Desde imagens e ficheiros PDF até documentos em formatos RTF e OLE, cada sistema desenvolvido oferece uma camada adiciona de proteção, garantindo que apenas ficheiros seguros sejam utilizados, independentemente do contexto. Estas inovações sublinham a importância do CDR como uma ferramenta indispensável no combate às ameaças cibernéticas modernas.

2.4. Ameaças

Uma ameaça representa qualquer ação que comprometa a segurança de um sistema informático, podendo resultar em danos significativos para a integridade, confidencialidade ou disponibilidade dos dados. As ameaças podem ser categorizadas como acidentais ou intencionais, dependendo da sua origem e motivação. As ameaças acidentais são aquelas que ocorrem sem qualquer intenção premeditada de causar danos. Exemplos comuns incluem falhas de *hardware*, erros de s*oftware*, interrupções causadas por desastres naturais ou até mesmo erros humanos inadvertidos. Estas situações podem surgir de vulnerabilidades previamente desconhecidas ou da falta de manutenção adequada dos sistemas, causando interrupções nos serviços ou perda de dados críticos. Por outro lado, as ameaças intencionais são ações deliberadas, realizadas com o objetivo claro de comprometer a segurança de sistemas informáticos. Estas ameaças são frequentemente motivadas por interesses financeiros, espionagem corporativa, ativismo político ou simplesmente a intenção de causar danos [35]. Entre os exemplos mais comuns estão os ciberataques, como roubo de informações sensíveis, destruição ou eliminação de dados, modificação de registos importantes, revelação de informações confidenciais e manipulação de dados para deturpação de fatos. Independentemente da sua origem, as ameaças podem ter impactos profundos nas operações das organizações, incluindo perdas financeiras, danos à reputação, compromissos legais e perda de confiança dos clientes e parceiros. Para mitigar esses riscos, é essencial que as organizações adotem estratégias de segurança robustas, como a implementação de sistemas de *backup*, monitorização contínua de atividades suspeitas, formação dos colaboradores para lidar com ameaças potenciais e a aplicação de atualizações regulares de segurança nos sistemas utilizados. A identificação e compreensão das diferentes formas de ameaças são passos cruciais para proteger os ativos digitais e assegurar a continuidade dos negócios num ambiente tecnológico cada vez mais desafiador [36].

Segundo o Índice Global de Ameaças para 2023 publicado pelo *Check Point*, os investigadores descobriram uma campanha substancial *malspam Qbot* que é distribuída através de ficheiros PDF malicioso, anexados a *e-mails* vistos em várias línguas [36].

O *malware Qbot* surgiu em 2008 como um *malware* bancário que foi desenvolvido com o objetivo de roubar senhas, *e-mails* e informações de cartão de crédito. O *Qbot* é instalado no dispositivo quando o utilizador receber um *e-mail* com um anexo que contém o ficheiro PDF [37].

De acordo com os dados de *Check Point,* o *AgentTesla* foi o *malware* mais dominante com um impacto de 10% em organizações mundiais compromete os sistemas dos alvos através de entrega de *e-mails* anexados com ficheiros .zip, .gz, .msi, .img e documentos de Microsoft Office [38]. De seguida, segue-se o *Qbot* com um impacto de 7%, e o *Formbook* com um impacto de 6% que é um *malware* que coleta e rouba dados sensíveis da máquina dos alvos, como por exemplo dados de *login*, captura de telas outras informações e depois estas informações são enviadas para um servidor que é controlado por cibercriminosos [39], conforme ilustrado no gráfico 1.

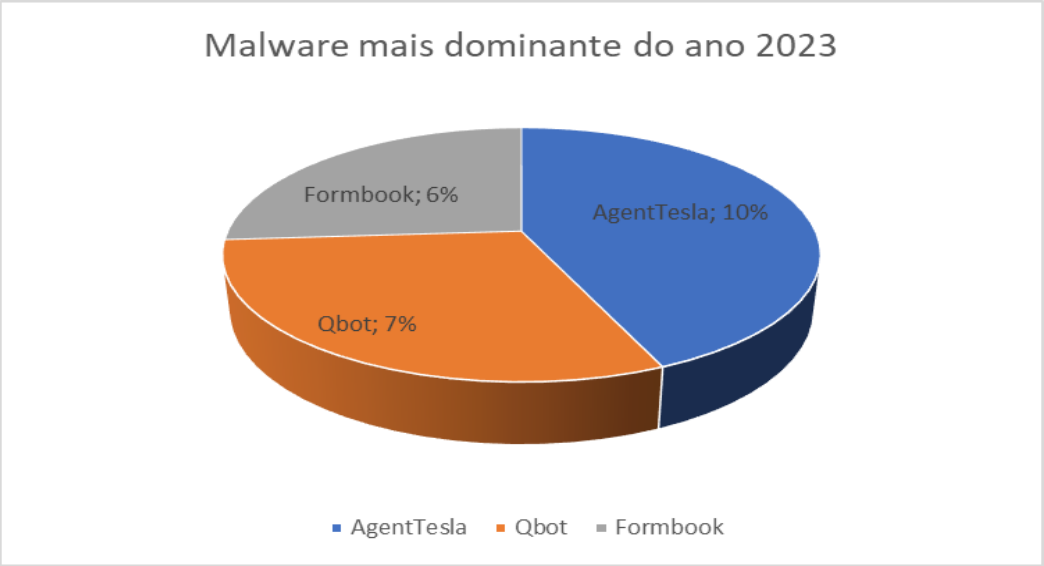


Gráfico 1- Malwares mais dominantes em 2023

2.5. Tendências em Ciberataques: Dados e Números

O relatório de Cibersegurança em Portugal referente ao ano 2022, publicado em junho de 2023 pelo Centro Nacional de Cibersegurança (CNCS), revela as vítimas de incidentes de cibersegurança mais relevantes em Portugal durante o ano 2022 foram os seguintes setores: Banca, Educação e Ciências, Tecnologias e Ensino Superior, Transportes, Saúde e Comunicação Social [40]. O documento evidência a prevalência de incidentes cibernéticos que afetaram essas áreas em particular, sugerindo uma necessidade urgente de estratégias de mitigação e resposta eficazes para proteger infraestruturas essenciais. A análise também sublinha a importância de um enfoque colaborativo entre instituições e órgãos governamentais para fortalecer a resiliência do país contra ameaças digitais e garantir a segurança da informação em um ambiente cada vez mais digitalizado.

O relatório de 2024 evidencia um aumento significativo nos ciberataques em Portugal, destacando o *ransomware*, *phishing* e *smishing*, burlas *on-line* e comprometimento de contas como as ameaças mais comuns enfrentadas [41]. Em 2023, as autoridades policiais registaram 2.512 casos de cibercrime, representando um crescimento superior a 13% em relação a 2022, com especial atenção ao aumento de 33% em casos de acesso/interceção ilegítimos e falsidade informática. Esses dados ressaltam a crescente necessidade de vigilância e medidas de proteção cibernética, uma vez que as táticas dos criminosos continuam a evoluir, ameaçando a segurança digital e a confidencialidade das informações dos cidadãos e organizações [42].

Em 2023, os ciberataques mais impactantes tiveram como alvo a administração pública local. No entanto, quem mais sofreu com a criminalidade digital foram indivíduos e pequenas e médias empresas (PME), frequentemente vítimas de esquemas de *phishing, smishing* e outras fraudes [42].

Segundo dados da equipa nacional de resposta a incidentes de segurança informática (CERT.PT), foram registados 2.025 incidentes de cibersegurança ao longo de 2023, representando um ligeiro aumento de dois casos face ao ano anterior. Verificou-se um crescimento particularmente significativo no número de incidentes reportados por entidades do setor privado. Os tipos de incidentes mais frequentemente registados em 2023 foram:

- Phishing e smishing, com 35%
- Tentativas de acesso não autorizado (login), com 19%
- Engenharia social, com 10%.

As marcas mais frequentemente utlizadas em campanhas de *phishing* e *smishing* foram as instituições bancarias 37%, serviços de e-mail, transporte e logística [42].

Em comparação com 2022, houve uma diminuição nos incidentes de alta visibilidade no ciberespaço nacional em 2023. Apesar disso, a atividade maliciosa se manteve intensa, resultando em um aumento contínuo no número de ciberataques, embora em menor escala do que no ano anterior. O relatório da Check Point Research [41] indicou que, no primeiro semestre de 2023, o número médio de ataques de *ransomware* por organização foi de 1.095, um aumento de 9% em relação ao mesmo período de 2022.

No primeiro semestre de 2023, 48 grupos de *ransomware* violaram mais de 2.200 vítimas, sendo o *Lockbit3* o mais ativo, registando um aumento de 20% nas vítimas em comparação com o primeiro semestre de 2022. O surgimento de novos grupos como: *Royal* e *Play* está

associado ao término dos grupos *Hive* e *Conti Ransomware-as-a-Service* (RaaS). Em termos de geografia, 45% das vítimas estão nos Estados Unidos de Améria (EUA), com um aumento inesperado nas entidades russas devido ao novo actor *MalasLocker*, que substitui os pedidos de resgate por doações de caridade. Os setores da indústria transformadora e do retalho foram os que registaram mais vítimas, o que sugere uma mudança na estratégia de ataque do *ransomware* [41].

Face ao crescente aumento de ciberataques a nível global, os dados apresentados no relatório da *Check Point* revelam que determinados setores são significativamente mais afetados do que outros (Gráfico 2). Entre os mais visados estão os setores da Educação, Administração Pública/Defesa, Saúde, Comunicações e Retalho, demonstrando a diversidade de alvos e a complexidade das ameaças que enfrentam [43].

O setor da Educação e Investigação destacou-se como o mais impactado, registando uma média de 2.046 ataques por semana em 2023. Apesar de elevado, este número representa uma diminuição de 12% em relação ao ano anterior, possivelmente refletindo esforços acrescidos de cibersegurança ou mudanças nas estratégias dos atacantes. Este setor continua, no entanto, a ser um alvo preferencial, dado o seu vasto volume de dados sensíveis e a potencial vulnerabilidade das infraestruturas tecnológicas utilizadas, conforme ilustrado no gráfico 2.

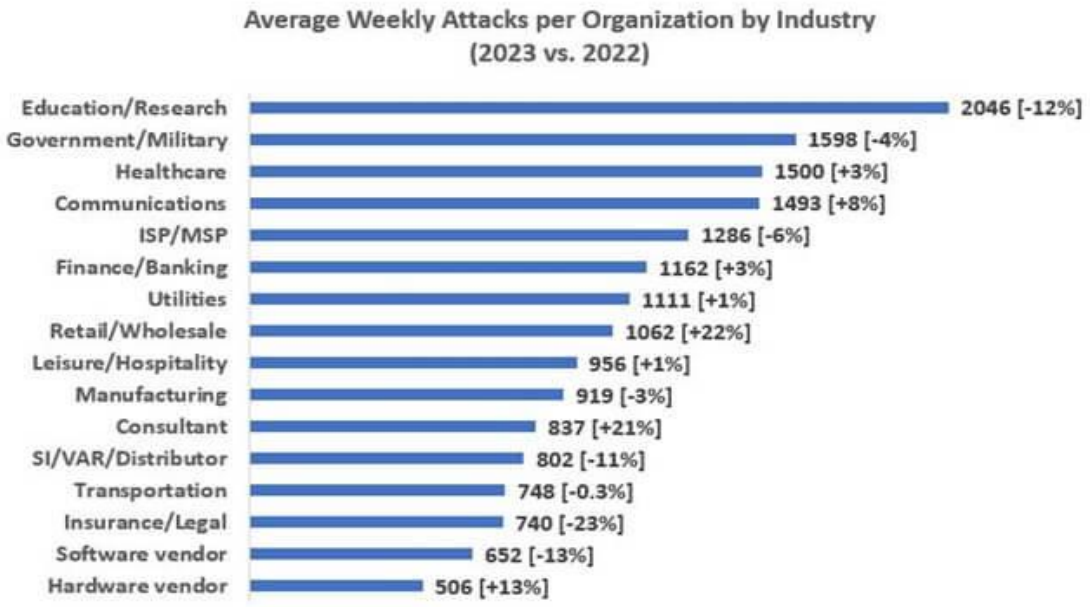


Gráfico 2- Média global de ataques semanais por organização do ano 2023 em relação ao ano 2022 [43]

O setor de Administração Pública e Defesa ocupou o segundo lugar, com uma média semanal de 1.598 ataques em 2023, registando uma ligeira redução de 4% face a 2022. A natureza crítica deste setor, que envolve informações estratégicas e de segurança nacional, mantém-no como um alvo prioritário para cibercriminosos e atores estatais maliciosos.

No setor da Saúde, os ataques continuam a crescer, com uma média de 1.500 ataques por semana em 2023, representando um aumento de 3% em comparação com 2022. Este crescimento evidencia a crescente vulnerabilidade de sistemas hospitalares e de saúde pública, que frequentemente lidam com dados altamente sensíveis e sistemas tecnológicos nem sempre atualizados.

O setor das Comunicações também registou um aumento expressivo, com uma média semanal de 1.493 ataques em 2023, o que representa um crescimento de 8% em relação ao ano anterior. Este aumento reflete a importância das infraestruturas de comunicação no mundo digital e a sua exploração por cibercriminosos para causar interrupções em grande escala ou roubar dados de utilizadores.

Por fim, o setor do Retalho registou o maior aumento percentual entre os setores analisados, com um crescimento de 22%, alcançando uma média de 1.062 ataques semanais em 2023. Este aumento pode estar associado à digitalização crescente no comércio, incluindo sistemas de pagamento online e armazenamento de dados de clientes, que representam um atrativo significativo para os atacantes [43].

O continente africano registou o maior número médio de ciberataques semanais por organização nos primeiros três meses de 2023, com uma média de 1.983 ataques. Este valor, embora elevado, representa uma ligeira redução de 2% em relação ao mesmo período de 2022, indicando uma estabilização parcial, possivelmente resultado de medidas de segurança mais eficazes em algumas organizações. Contudo, a dimensão e diversidade de vulnerabilidades no continente continuam a torná-lo um alvo atrativo para cibercriminosos. Na região da Ásia-Pacífico, verificou-se um aumento significativo na média de ataques semanais por organização, atingindo 1.835 ataques em 2023, o que representa um crescimento de 16% em relação ao ano anterior. Este aumento evidencia a intensificação das atividades maliciosas na região, que inclui economias emergentes e altamente digitalizadas, tornando-se um foco de interesse tanto para cibercriminosos quanto para atores estatais. A América do Norte registou um aumento anual de 9% no número médio de ciberataques semanais, alcançando uma média de 950 ataques por organização no primeiro trimestre de

2023. Este crescimento reflete a crescente sofisticação e frequência dos ataques dirigidos a uma região com alta densidade de organizações críticas e tecnologicamente avançadas, muitas das quais lidam com dados sensíveis e operações de alcance global. Estes dados sublinham a variabilidade regional no panorama de cibersegurança, onde fatores como infraestrutura tecnológica, capacidade de resposta e prioridades estratégicas influenciam as tendências de ataque. A necessidade de soluções adaptadas ao contexto regional, aliada à cooperação internacional em matéria de cibersegurança, é essencial para reduzir a incidência e o impacto dos ciberataques em escala global [43].

De acordo com os dados da *Kaspersky*, os *hackers* criaram, em média, 411 mil novos *malwares* por dia durante o ano de 2023, representando um aumento de 3% em relação a 2022. Além disso, foram detetados cerca de 380 mil *malwares* diariamente. Outros tipos de ameaças, como *ransomware, phishing* e ataques envolvendo documentos da *Microsoft Office*, também registaram um aumento significativo, na ordem dos 53%. Os cibercriminosos recorreram frequentemente à técnica de *backdoors* para se infiltrarem em sistemas de forma furtiva, evitando a deteção e comprometendo a segurança dos mesmos [44].

Os ataques baseados em *e-mail* continuam a ser o vetor de ataque mais dominante 88% de todas as entregas de ficheiros malicioso ocorrem por *e-mail*, com o restante baixado diretamente da internet. Os agentes de ameaças adaptaram-se às estratégias de protecção de *e-mail* e estão a explorar técnicas de entrega inovadoras. Após as restrições da *Microsoft* sobre macros VBA do *office* em ficheiros de fontes externas denotadas com a marca da Web (MotW), houve uma queda acentuada na prevalência de ficheiros maliciosos do *Office*, de quase 50% em 2022 para 2% em 2023 [43]. Esses dados sublinham a eficácia das medidas de segurança e a necessidade contínua de adaptação das estratégias de defesa frente às evoluções nas táticas dos cibercriminosos, conforme ilustrado no gráfico 3.

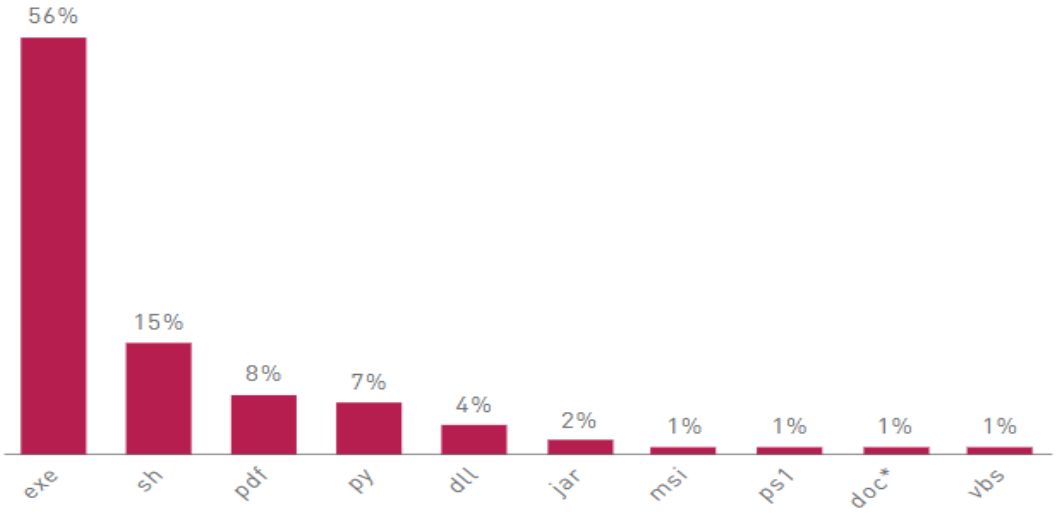


Gráfico 3- Web- principais tipos de ficheiros maliciosos em 2023 [43]

Paralelamente, vetores de ataques alternativos começaram a ganhar destaque, incluindo ficheiros HTML e vários tipos de ficheiros compactados. Em particular, a exploração de ficheiros HTML registou um aumento significativo, sendo responsável por 69% de todos os anexos de ficheiros maliciosos detetados. Esta tendência demonstra a capacidade dos cibercriminosos em adaptar as suas estratégias para contornar medidas de proteção existentes, reforçando a necessidade de vigilância contínua e de medidas de cibersegurança inovadoras [43], conforme ilustrado no gráfico 4.

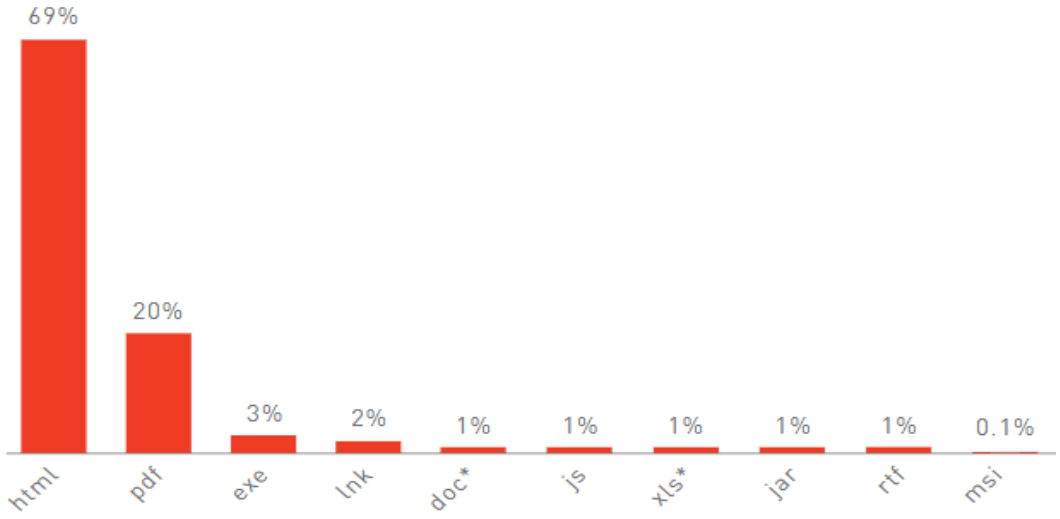


Gráfico 4- E-mail: principais tipos de ficheiros maliciosos em 2023 [43]

A utilização de vários tipos de ficheiros também tem aumentado, particularmente aqueles protegidos por senhas, apresenta um desafio de segurança significativo, pois esses ficheiros

geralmente não são detetados por muitos serviços de segurança, criando vetores de ataque eficazes. Formatos como .img e .iso também são vulneráveis, pois sua capacidade de propagar a funcionalidade *Mark of the Web* (MotW) depende muito do *software* de extração empregado. Embora a *Microsoft* tenha feito esforços para resolver esse problema por meio de atualizações, outros fornecedores de software, como o 7-zip, exibem vários graus de adesão aos protocolos de segurança, diminuindo a eficácia do mecanismo de proteção MotW. Esse cenário ressalta a necessidade de vigilância e medidas de segurança robustas para neutralizar as ameaças emergentes associadas aos processos de gerenciamento e extração de ficheiros, conforme ilustrado no gráfico 5.

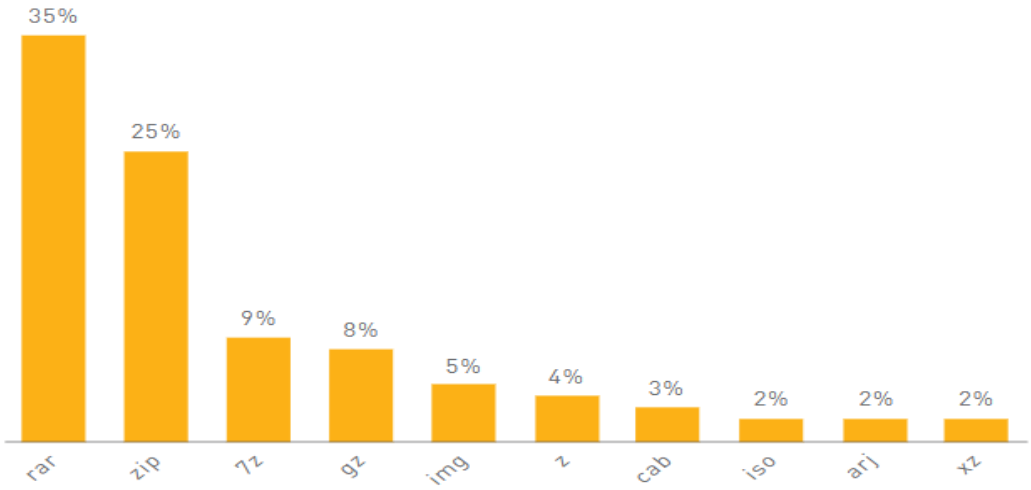


Gráfico 5- Tipos de ficheiros maliciosos entregues por e-mail em 2023 [43]

2.6. Vulnerabilidade

O conceito de vulnerabilidade, amplamente debatido na área da cibersegurança, é definido de várias formas, mas, em essência, refere-se a qualquer falha ou fraqueza presente num sistema informático ou no código de *software* que pode ser explorada por *hackers* para obter acesso não autorizado. Estas falhas comprometem a integridade, confidencialidade e disponibilidade dos sistemas e dados, representando um risco significativo para organizações e indivíduos.

De acordo com o relatório *Risk Management Framework for Information Systems and Organizations*, publicado pelo *National Institute of Standards and Technology* (NIST), as vulnerabilidades são descritas como pontos fracos que os atacantes podem explorar para causar danos a sistemas de informação ou aos dados armazenados nesses sistemas. Estes pontos fracos podem estar presentes em várias camadas de um sistema, desde falhas no

design de software até configurações incorretas de segurança ou práticas inadequadas de gestão de acesso [45].

A norma ABNT ISO/IEC 27005 (2011), por sua vez, apresenta uma definição complementar, descrevendo vulnerabilidade como a fragilidade de um ativo ou de um conjunto de ativos que pode ser explorada por uma ou mais ameaças. Esta abordagem enfatiza a importância de compreender as vulnerabilidades no contexto mais amplo da gestão de ativos e da análise de risco, fornecendo um enquadramento estruturado para avaliar e mitigar os riscos associados [46].

Um dos métodos mais comuns utilizados por atacantes para explorar vulnerabilidades é o *spear phishing*, uma técnica de engenharia social direcionada. Neste tipo de ataque, o atacante envia mensagens de *e-mail* personalizadas, destinadas a um indivíduo ou grupo específico, que contêm anexos ou *links* maliciosos. Estas mensagens são cuidadosamente elaboradas para parecerem legítimas, explorando a confiança ou descuido das vítimas. Quando o destinatário abre o anexo ou clica no *link,* o *malware* é instalado no sistema, iniciando o ataque. Este método destaca a sofisticação dos atacantes e também demonstra como uma vulnerabilidade técnica pode ser explorada em combinação com falhas humanas, aumentando a eficácia dos ataques [45].

No primeiro semestre de 2023, o panorama de ameaças relacionadas com fraquezas e falhas nos sistemas de *software*, designadas como vulnerabilidades, registou um aumento significativo em comparação com o mesmo período de 2022. Dados publicados pelo *National Institute of Standards and Technology* (NIST)*,* através da *National Vulnerability Database* (NVD), indicam que foram identificadas e divulgadas um total de 13.683 vulnerabilidades, classificadas de acordo com a norma *Common Vulnerability Scoring System* (CVSS) *v3.X.* Este número representa um aumento de aproximadamente 3% em relação às 13.243 vulnerabilidades reportadas no segundo semestre de 2022, evidenciando uma tendência de crescimento contínuo no número de falhas exploráveis em sistemas informáticos [47].

As vulnerabilidades podem assumir diferentes formas e manifestar-se em várias etapas do ciclo de vida de um sistema, desde o desenvolvimento inicial até à implementação e manutenção. Independentemente do tipo de vulnerabilidade, todas merecem atenção cuidadosa, uma vez que cada uma requer abordagens específicas para mitigação e resolução. A diversidade destas fragilidades sublinha a necessidade de estratégias de segurança

abrangentes que considerem a complexidade dos ambientes tecnológicos atuais. Seguem-se alguns exemplos de vulnerabilidades comuns que devem ser monitorizadas e tratadas: CVE-2023-38831: Zero-Day no WinRAR, CVE-2023-34362, CVE-2023-2868 e CVE-2023-21716 da RTF.

A primeira vulnerabilidade, CVE-2023-38831: Zero-Day no WinRAR, tem sido explorada ativamente desde abril de 2022 e permite o comprometimento de contas de negociação de criptomoedas e ações [48]. Esta vulnerabilidade foi identificada nas versões do *RARLabs WinRAR* anteriores à 6.23, permitindo que os atacantes criassem ficheiros maliciosos por meio de ficheiros ZIP e RAR que aparentavam conter ficheiros inofensivos, como PDFs, documentos de texto ou imagens JPG. Os atacantes podem ocultar código malicioso dentro de ficheiros, mascarando os formatos e criando um ficheiro "armado". Quando os utilizadores abrem esses ficheiros considerados inofensivos, um *script* é automaticamente executado, permitindo a instalação de *malware* nos sistemas comprometidos. Para mitigar este tipo de ameaça, é essencial que os utilizadores mantenham sempre os seus *software*s atualizados, eliminando o risco de exploração por ficheiros falsificados. Adicionalmente, recomenda-se que realizem verificações regulares nos seus sistemas, com ferramentas de segurança adequadas, para identificar e corrigir potenciais vulnerabilidades [49].

A segunda vulnerabilidade, CVE-2023-34362, é uma vulnerabilidade de injeção de SQL que foi encontrada na aplicação web do *MOVEit Transfer* (Software de transferência segura de ficheiros) que poderia permitir que um atacante não autenticado obtivesse acesso ao base de dados do *MOVEit Transfer*. Dependendo do mecanismo de base de dados que está a ser utilizado (MySQL, Microsoft SQL Server ou SQL do Azure), um atacante pode inferir inserir informações sobre a estrutura e o conteúdo de base de dados e executar instruções SQL que alteram ou eliminam elementos de base de dados. Esta vulnerabilidade foi explorada em maio e junho de 2023, a exploração de sistemas não corrigidos pode ocorrer via HTTP ou HTTPS [50].

Depois, a vulnerabilidade CVE-2023-2868 trata-se de uma vulnerabilidade de injeção de comando remoto no produto Barracuda *E-mail Security Gateway* que afeta as versões 5.1.3.001-9.2.0.006. A vulnerabilidade surge de uma falha em limpar de forma abrangente o processamento do ficheiro .tar. A vulnerabilidade decorre da validação de entrada incompleta de um ficheiro .tar fornecido pelo utilizador no que se refere aos nomes dos ficheiros contidos no ficheiro. Como consequência, um atacante remoto pode formatar especificamente esses nomes de ficheiros de uma maneira especifica que resultará na

execução remota de um comando do sistema através do operadora qx do Perl com os privilégios do produto *E-mail Security Gateway*. Esse problema foi corrigido como parte do *patch BNSF-36456*. Este *patch* foi aplicado automaticamente a todos os dispositivos do cliente [51].

A vulnerabilidade CVE-2023-21716 da RTF foi divulgada pela *Microsoft* através do seu pesquisador Joshua Drake em novembro de 2022. Corresponde a uma vulnerabilidade de corrupção de *heap* encontrada no analisador *Rich Text Format* (RTF) do *Microsoft Office Word* ao processar uma tabela de tipos de letra (fonttbl) que contém um número excessivo de tipos de letra (f###). Esta vulnerabilidade pode ser explorada pelos atacantes através da criação de um ficheiro RTF malicioso enviando uma mensagem de *e-mail* malicioso incentivar o utilizador a abrir o ficheiro. Depois que o ficheiro é aberto o atacante ganha o acesso ao sistema permitindo que o atacante execute comandos arbitrários com os privilégios do alvo por meio de ficheiros RTF mal-intencionados. Esta vulnerabilidade CVE-2023-21716 recebeu uma pontuação de *Common Vulnerability Scoring System (CVSS)* de 9,8 críticas [52].

Os produtos afetados pela vulnerabilidade CVE-2023-21716 incluem uma variedade de aplicações e sistemas que utilizam versões vulneráveis das tecnologias identificadas. Esta vulnerabilidade, amplamente divulgada pela comunidade de cibersegurança, pode comprometer a segurança dos sistemas ao explorar falhas específicas presentes nas versões não atualizadas dos produtos. Para melhor visualização e compreensão, os produtos foram organizados numa tabela, que detalha os nomes dos sistemas, versões afetadas e possíveis impactos associados. Esta estrutura permite uma análise clara e objetiva, ajudando organizações e utilizadores a identificar rapidamente os riscos e a tomar medidas corretivas para mitigar a exposição à vulnerabilidade, conforme ilustrado na tabela 3.

Produtos Afetados	
Microsoft 365 Apps	Para Empresas: ✓ Edições de 32 e 64 bits
Microsoft Office	Office 2019: ✓ Para Mac, edições de 32 e 64 bits ✓ Servidor on-line do Office ✓ Servidor do Office Web Apps 2013 Service Pack1
Microsoft Word	Word 2013: ✓ Para edições RT SP1, de 32 bits e SP1 de 64 bits Word 2016: ✓ Para edições de 32 e 64 bits

Produtos Afetados	
SharePoint	✓ Servidor Corporativo 2013 Service Pack 1 ✓ Servidor Corporativo 2016 ✓ Pacote de Serviços 1 da Fundação 2013 ✓ Servidor 2019 ✓ Edição de assinatura de servidor ✓ Pacote de idiomas da edição de assinatura do servidor

Tabela 3- Tabela de produtos afetados pela vulnerabilidade CVE-2023-21716 [53]

A vulnerabilidade CVE-2017-11882, descoberta em 14 de novembro de 2017, explora uma falha no *software Equation Editor* do *Microsoft Office* [54]. Os atacantes utilizam a vulnerabilidade CVE-2023-21716 para comprometer a segurança dos sistemas, explorando falhas presentes em documentos do *Microsoft Office*. Para explorar esta vulnerabilidade, os cibercriminosos criam ficheiros maliciosos, como documentos Word ou Excel, que contêm código embutido em formato RTF. Estes ficheiros são projetados para incluir todas as instruções necessárias para explorar a vulnerabilidade e comprometer o sistema do alvo. De acordo com a *Microsoft*, num cenário típico de ataque baseado em *e-mail*, o atacante envia o ficheiro malicioso por *e-mail* para a vítima, utilizando técnicas de engenharia social para convencê-la a abrir o ficheiro. Assim que o utilizador interage com o documento, o código malicioso é ativado, explorando a vulnerabilidade para ganhar acesso ao sistema ou executar ações maliciosas, comprometendo a integridade e a segurança do dispositivo. Este tipo de ataque reforça a importância de práticas seguras no manuseio de anexos e a necessidade de atualizações regulares de *software* para prevenir tais ameaças. Num ataque com base na web o atacante pode hospedar um site e usar o ficheiro malicioso que preparado para explorar a vulnerabilidade (54). Assim que o ficheiro é aberto, o *Equation Editor* processa o ficheiro RTF e executa o código malicioso. Para se proteger contra essa vulnerabilidade o *Microsoft* lançou atualizações para edições afetadas de *Microsoft Office*, como *Microsoft Office 2007* e *Microsoft Office 2010* [55].

A vulnerabilidade CVE-2018-4990 do *Acrobat Reader* DC permite que os atacantes executem códigos maliciosos nas máquinas dos alvos permitindo assim assumir o controle dos sistemas baixar e executar *malware* neles. Esta vulnerabilidade é explorada por meio da criação de um ficheiro PDF malicioso que incorpora um código *JavaScript* que manipula o objeto *Button1*. Este objeto contém uma imagem JPEG2000 criada, que é projetada para ativar uma dupla vulnerabilidade no *Adobe Reader* [56].

3. *Content Disarm and Reconstruction* (CDR)

O CDR foi inicialmente desenvolvido pelas unidades militares de segurança cibernética e, posteriormente, adaptado para uso civil com o objetivo de proteger dados confidenciais contra infiltrações de *malware* [57]. Esta tecnologia introduz uma abordagem inovadora e proativa no combate a ameaças digitais, operando de forma distinta das soluções tradicionais de cibersegurança.

Enquanto os métodos convencionais, como análises de *malware* e antivírus, dependem de bases de dados de assinaturas conhecidas para identificar ameaças, o CDR assume que todos os ficheiros são potencialmente maliciosos, independentemente da sua origem. Este conceito elimina a necessidade de identificar a funcionalidade exata do *malware* antes de o neutralizar. Em vez disso, o CDR atua eliminando componentes suspeitos de ficheiros, como códigos embutidos ou macros, e substituindo-os por versões limpas e reconstruídas que preservam a funcionalidade original sem comprometer a segurança [32].

A capacidade do CDR de desarmar ficheiros é baseada numa análise profunda das especificações dos formatos de ficheiro. A tecnologia identifica padrões permitidos e remove elementos que não estão em conformidade com esses padrões ou com as políticas de segurança definidas. Após esta etapa, o ficheiro é reconstruído para garantir que esteja livre de ameaças e pronto para utilização segura. Este processo não apenas protege contra infeções por *malware,* mas também evita a propagação de códigos maliciosos dentro de redes organizacionais [31].

Adicionalmente, o CDR é altamente eficaz contra uma vasta gama de ameaças, incluindo aquelas associadas a ficheiros de uso comum, como documentos Word, Excel, PDFs e imagens. A sua aplicação é particularmente relevante no combate a ameaças distribuídas por *e-mail*, que continuam a ser o vetor dominante para entrega de *malware*. Mais de 90% dos ataques cibernéticos envolvem ficheiros anexados a mensagens de *e-mail* ou descarregados da internet, muitos dos quais se escondem em tipos de ficheiros aparentemente inofensivos. O CDR é, portanto, uma solução eficaz para prevenir esses ataques ao eliminar o risco antes mesmo de os ficheiros serem abertos [58].

Além de proteger contra *malware* conhecido, o CDR também se destaca na mitigação de ameaças *zero-day*, em que os atacantes exploram vulnerabilidades desconhecidas para introduzir código malicioso. Ao reconstruir os ficheiros com base em padrões seguros, o

CDR reduz significativamente a possibilidade de que *exploits* desconhecidos sejam usados para comprometer sistemas.

A versatilidade do CDR permite a sua aplicação em diversos contextos, incluindo proteção de sistemas de *e-mail*, navegadores da web, servidores de ficheiros e dispositivos removíveis. A sua utilização melhora significativamente a resiliência cibernética das organizações, protegendo dados confidenciais e assegurando a continuidade das operações num ambiente digital cada vez mais desafiador [32], [57].

Um dos principais pesquisadores da tecnologia *Gartner*, reconheceu o CDR como uma solução de alto valor para a segurança dos sistemas. A pesquisa mostrou que as soluções baseadas em deteção são insuficientes para uma defesa contra ameaças ocultas. Por isso, o CDR é uma solução viável porque vai permitir higienizar todos os ficheiros e será capaz de eliminar códigos mal-intencionados escondidos em ficheiros [59].

O CDR pode ser utilizado como uma medida eficaz para prevenir diversas ameaças cibernéticas em diferentes contextos tecnológicos. A sua aplicação é ampla, abrangendo as seguintes áreas críticas:

- ✓ E-mail: o CDR protege contra ficheiros maliciosos enviados como anexos em mensagens de *e-mail*, uma das formas mais comuns de distribuição de *malware.* Ele remove componentes suspeitos e reconstrói os ficheiros para garantir a segurança antes de serem abertos pelos utilizadores.
- ✓ Navegadores da Web: Pode ser usado para prevenir o *download* de ficheiros maliciosos provenientes de *websites* comprometidos, protegendo os utilizadores enquanto navegam na internet e minimizando o risco de infeções.
- ✓ Servidores de ficheiros: o CDR protege os servidores de ficheiros ao inspecionar e desarmar qualquer ficheiro carregado ou partilhado, assegurando que apenas conteúdos limpos e seguros são disponibilizados dentro da rede organizacional.
- ✓ Programas de e-mail na nuvem: na era das soluções baseadas em nuvem, o CDR oferece proteção adicional para programas de *e-mail* como o *Gmail* ou o *Outlook* Web, garantindo que os anexos enviados ou recebidos são processados e reconstruídos sem elementos maliciosos.
- ✓ Dispositivos removíveis: o CDR pode ser aplicado para proteger contra ficheiros maliciosos armazenados em dispositivos removíveis, como *pen drives* ou discos

externos, ao garantir que estes dispositivos não introduzam ameaças no sistema ao serem conectados.

A tecnologia CDR permite efetuar análise dos principais tipos de formato de ficheiros tais como: Imagens, .HTML, PDF, Documentos de Office, RFT, Formato de ficheiros de áudio, ficheiro de vídeo entre outros.

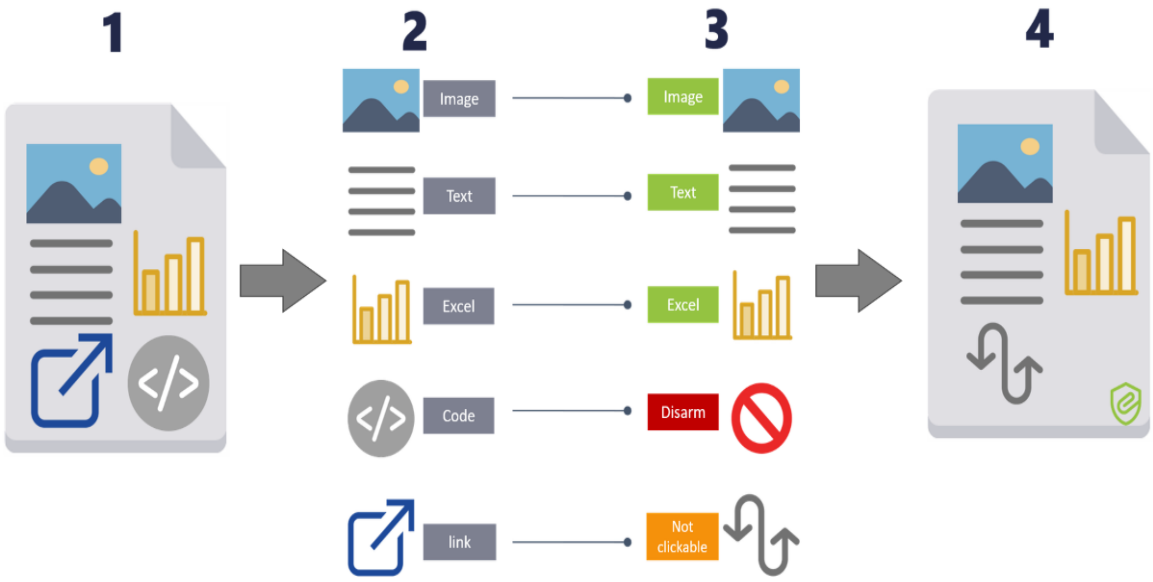


Figura 2- Tecnologia *Content Disarm and Reconstruction* [76]

A figura 2 ilustra o funcionamento da tecnologia CDR, detalhando as etapas principais envolvidas no processo de desarmamento e reconstrução de ficheiros para garantir a sua segurança. O processo inicia-se com a análise de um ficheiro original (Etapa 1), que pode conter vários elementos, como imagens, texto, tabelas Excel, código embutido e *links* clicáveis. Este ficheiro é considerado potencialmente perigoso, pois pode incluir componentes maliciosos disfarçados.

Na Etapa 2, o ficheiro é descomposto nos seus diferentes componentes, com cada elemento (como imagens, texto ou código) a ser identificado e processado separadamente. Este passo permite uma análise granular dos conteúdos do ficheiro, determinando quais os componentes que representam um risco para a segurança.

A Etapa 3 foca-se no desarmamento e verificação dos componentes. Elementos considerados seguros, como imagens e texto, são mantidos no ficheiro. No entanto, componentes potencialmente perigosos, como código embutido (exemplo: scripts maliciosos), são desarmados e removidos. Além disso, *links* clicáveis são desativados para impedir que os utilizadores sejam redirecionados para sites maliciosos.

Por fim, na Etapa 4, o ficheiro é reconstruído utilizando apenas os componentes seguros. O resultado é um ficheiro funcional, contendo elementos como texto, imagens e tabelas, mas agora livre de qualquer ameaça maliciosa. Este processo assegura que o ficheiro é seguro para utilização sem comprometer a integridade ou a funcionalidade dos dados.

A imagem demonstra de forma clara e eficaz como o CDR transforma um ficheiro potencialmente perigoso num ficheiro seguro, eliminando ameaças proactivamente sem depender de métodos tradicionais de deteção. Este sistema reforça a proteção contra ataques baseados em ficheiros, oferecendo uma solução inovadora para os desafios da cibersegurança moderna.

3.1. Evolução da tecnologia CDR

A tecnologia CDR evoluiu ao longo dos tempos e permitiu melhorar as suas capacidades em tratamento de ficheiros maliciosos. Existem três tipos de CDR, os quais são explicados nos subcapítulos seguintes.

3.1.1. CDR tipo 1: Converter ficheiros em PDF

O CDR Tipo 1 baseia-se na conversão de ficheiros para o formato PDF como uma forma de neutralizar ameaças e proteger os utilizadores contra código malicioso contido em documentos. Este método consiste em transformar o ficheiro original, independentemente do seu formato inicial (como documentos Word, Excel ou apresentações PowerPoint), numa versão em PDF, o que impede a execução de código malicioso embutido quando o documento é aberto. Esta abordagem aproveita a natureza estática dos PDFs, que geralmente não permitem a execução de *scripts* ou macros, tornando o ficheiro mais seguro para o utilizador final.

Uma das principais vantagens deste tipo de CDR é a sua simplicidade e rapidez, uma vez que a conversão ocorre quase instantaneamente, reduzindo a superfície de ataque de forma eficaz. É particularmente útil em cenários onde a prioridade é a segurança imediata, como na análise de ficheiros recebidos por *e-mail* ou transferidos através de dispositivos removíveis. A eliminação de código embutido durante a conversão assegura que potenciais *scripts* ou macros maliciosos não sejam executados, prevenindo ataques antes que estes possam causar danos [59].

Contudo, este método apresenta algumas limitações significativas, especialmente no que diz respeito à funcionalidade dos ficheiros convertidos. Durante o processo de conversão,

elementos legítimos do documento, como macros, campos de formulário e *hiperlinks*, são eliminados. Isto pode resultar em ficheiros que, embora seguros, se tornam inutilizáveis para os seus propósitos originais. Por exemplo, um ficheiro Excel com fórmulas interativas ou um formulário Word com campos editáveis perde toda a sua funcionalidade, sendo transformado num documento estático que apenas pode ser visualizado.

Além disso, a conversão para PDF pode não ser apropriada para ficheiros que requerem interação do utilizador, como documentos que dependem de *hiperlinks* para navegação ou de macros para cálculos automatizados. Estes desafios tornam este tipo de CDR mais adequado para situações onde a prioridade é a segurança sobre a funcionalidade, como na proteção de ficheiros recebidos de fontes desconhecidas ou potencialmente perigosas.

Apesar das suas limitações, o CDR Tipo 1 continua a ser amplamente utilizado, especialmente em ambientes empresariais, devido à sua eficácia na eliminação de ameaças cibernéticas antes que estas possam ser ativadas. No entanto, a sua implementação deve ser cuidadosamente avaliada com base nas necessidades específicas do utilizador ou da organização, garantindo que a segurança não comprometa a produtividade ou a funcionalidade essencial dos ficheiros [60].

3.1.2. CDR tipo2: Remover código Ativo e objetos incorporados

O CDR Tipo 2 é uma abordagem mais avançada em comparação com a conversão para PDF, focando-se na remoção de código ativo e objetos incorporados que possam representar riscos de segurança. Este método elimina elementos potencialmente perigosos do ficheiro original, como macros, *scripts*, e objetos embutidos (por exemplo, ficheiros executáveis ou objetos OLE). Após este processo, o ficheiro é reconstruído no seu formato original, preservando a maior parte da usabilidade e garantindo que o utilizador ainda possa interagir com o documento de forma funcional.

A principal vantagem deste método é a sua capacidade de manter o formato original do ficheiro, o que é essencial para utilizadores que precisam de trabalhar com documentos que exigem interatividade limitada, como tabelas Excel ou documentos Word com conteúdos estáticos. Apesar de remover *links* clicáveis, macros e outros elementos dinâmicos que possam ser explorados por atacantes, o ficheiro reconstruído ainda oferece uma experiência de utilizador mais próxima do documento original, diferentemente do que ocorre na conversão direta para PDF.

A reconstrução do ficheiro no formato original garante que os utilizadores não enfrentem dificuldades significativas ao lidar com documentos importantes. Por exemplo, relatórios ou formulários que dependem de gráficos, tabelas ou imagens permanecem utilizáveis, embora funcionalidades dinâmicas, como *hiperlinks* ou automações, sejam desativadas por razões de segurança. Este equilíbrio entre segurança e usabilidade torna o CDR Tipo 2 uma solução ideal para organizações que lidam frequentemente com ficheiros partilhados entre diferentes partes, como documentos recebidos por e-mail ou descarregados da internet.

Contudo, é importante destacar que, mesmo com o processo de reconstrução, o ficheiro perde algumas funcionalidades críticas, como macros automatizadas, *scripts* personalizados e *links* clicáveis, o que pode limitar a sua utilidade em cenários específicos. Por exemplo, um documento que contenha *links* de navegação interna ou cálculos automáticos configurados em macros terá essas funcionalidades removidas, podendo exigir ajustes manuais por parte do utilizador.

O CDR Tipo 2 é especialmente útil em ambientes empresariais que precisam de proteger os seus sistemas sem comprometer totalmente a produtividade. É uma solução eficaz para mitigar riscos associados a ficheiros dinâmicos provenientes de fontes externas, oferecendo um nível elevado de proteção enquanto mantém uma experiência de utilizador satisfatória. Contudo, a sua implementação deve ser avaliada com base na criticidade das funcionalidades do ficheiro original, garantindo que a segurança e a usabilidade sejam equilibradas de forma adequada [60].

3.1.3. CDR tipo 3: Tecnologia de Seleção Positiva

O CDR Tipo 3, baseado na tecnologia de Seleção Positiva, representa uma evolução significativa no tratamento de ficheiros, abordando as limitações dos métodos anteriores (CDR Tipo 1 e CDR Tipo 2). Este método tenta preservar a funcionalidade completa dos ficheiros originais ao reconstruí-los de forma mais precisa e com maior atenção aos detalhes, utilizando modelos de segurança predefinidos como referência.

Ao contrário dos métodos anteriores, que removem ou desativam automaticamente elementos suspeitos, a tecnologia de Seleção Positiva opera com base no princípio de "copiar apenas o que é seguro". Durante o processo de reconstrução, a tecnologia analisa detalhadamente o ficheiro, identificando e copiando exclusivamente os elementos que se encontram em boas condições e que correspondem a modelos seguros de referência. Assim,

componentes potencialmente perigosos são completamente excluídos, enquanto elementos seguros são mantidos sem comprometer a integridade ou funcionalidade do ficheiro.

Uma das principais vantagens do CDR Tipo 3 é a sua capacidade de preservar a funcionalidade total dos documentos após a reconstrução. Este método é particularmente eficaz em ficheiros complexos que contêm macros, *links*, ou outros elementos interativos, permitindo que o ficheiro final seja utilizado de forma idêntica ao documento original, mas sem os riscos associados a código ou objetos maliciosos.

Além disso, a tecnologia de Seleção Positiva garante que cada ficheiro que entra numa organização seja 100% seguro, eliminando completamente qualquer código ou objeto malicioso que possa ser usado para comprometer os sistemas. Este nível de proteção é alcançado sem sacrificar a usabilidade, tornando o método ideal para organizações que necessitam de lidar com documentos dinâmicos e interativos, como formulários, relatórios automatizados ou ficheiros com *scripts* integrados.

Embora o CDR Tipo 3 apresente uma abordagem mais avançada e eficiente, a sua implementação requer maior capacidade computacional e conhecimento técnico, dado que o processo de análise e reconstrução com base em modelos seguros pode ser mais complexo e demorado. No entanto, esta desvantagem é amplamente compensada pela combinação única de segurança total e preservação da funcionalidade, posicionando este método como a solução mais robusta e adaptada às exigências do ambiente corporativo moderno.

A tecnologia de Seleção Positiva é especialmente recomendada para organizações que lidam com grandes volumes de documentos e que necessitam de garantir a máxima segurança sem comprometer a produtividade. Este método proporciona uma abordagem equilibrada, permitindo a reconstrução precisa de ficheiros enquanto assegura a eliminação completa de quaisquer riscos associados a vulnerabilidades exploráveis [61].

3.2. Comparação entre Tipos de CDR

De forma a comparar os tipos de CDR, é apresentado na tabela 4, a comparação dos três (3) tipos de CDR existentes.

	CDR Tipo 1	CDR Tipo 2	CDR Tipo 3
Utilização e Experiência do Utilizador	Converte ficheiros em PDF tornando-os estáticos e inutilizáveis	Remove conteúdo ativo, a fim de garantir a segurança de cada ficheiro	Mantém a usabilidade, a funcionalidade e a fidelidade completa dos ficheiros
Ficheiros protegidos comprimidos por senhas	Não higieniza ficheiros ZIP ou protegidos por senha	Não higieniza ficheiros ZIP ou protegidos por senha	Higieniza ficheiros ZIP e protegidos por senha
Bloqueio de ficheiros	Bloqueia ficheiros com ameaças conhecidas	Bloqueia ficheiros com ameaças conhecidas	Nenhum ficheiro é bloqueado; Todos os ficheiros são higienizados de ameaças conhecidas e desconhecidas
Modelos	Modelo original é potencialmente malicioso mantido	Modelo original é potencialmente malicioso mantido	A reconstrução baseada em modelo coloca o conteúdo em um modelo novo, limpo e seguro
Conteúdo ativo	O ficheiro é nivelado	Remove todo o conteúdo ativo	Retém conteúdo ativo, apenas remove elementos maliciosos
Falsos Positivos	Alta taxa de falsos positivos	Alta taxa de falsos positivos	0% de taxa de falsos positivos
Manutenção	Manutenção envolvida	Manutenção envolvida	Não requer manutenção; Plug e Play
Latência	Segundos a minutos	Segundos a minutos	Milissegundos; os funcionários recebem ficheiros seguros instantaneamente

Tabela 4- Tabela comparativa dos tipos de CDR [61]

3.3. Princípios de Funcionamento de CDR

O funcionamento do CDR consiste em realizar uma análise detalhada do ficheiro para identificar a presença de código malicioso. Após esta identificação, o código malicioso é eliminado, e o ficheiro é reconstruído para garantir a sua segurança. Ao final deste processo, o ficheiro torna-se completamente inofensivo, mantendo apenas os elementos seguros e legítimos.

A figura 3 ilustra o funcionamento do CDR, detalhando as etapas principais desde a receção do ficheiro até à entrega de um ficheiro seguro e funcional. O processo inicia-se com a receção do ficheiro original (*Input*), que é introduzido no sistema para análise. Este ficheiro pode conter potenciais ameaças e, por isso, é submetido a uma validação inicial da sua estrutura.

Na etapa de validação da estrutura do ficheiro, o sistema analisa se o ficheiro cumpre os padrões e as políticas de segurança estabelecidos. Caso a estrutura do ficheiro não esteja em conformidade, ele é colocado em quarentena, impedindo o seu processamento e protegendo os sistemas contra possíveis riscos. Apenas os ficheiros que passam nesta validação avançam para as etapas seguintes.

O passo seguinte envolve o desarmamento de ameaças potenciais, onde o sistema identifica e remove elementos maliciosos ou potencialmente perigosos. Entre os componentes analisados estão macros, campos de formulários, vídeos, imagens, *scripts,* objetos incorporados, *links (hyperlinks*) e documentos anexados. Os macros são eliminados para evitar a execução de *scripts* maliciosos, enquanto os campos de formulários são achatados, tornando-os inativos. Os vídeos e imagens são higienizados para remover quaisquer códigos embutidos, e os *scripts* são completamente removidos. São analisados objetos incorporados e, dependendo do risco, podem ser higienizados ou removidos. Os *links* são processados para garantir que não redirecionam os utilizadores para conteúdos maliciosos, e quaisquer documentos anexados passam por um processo de sanitização.

Após o desarmamento, o ficheiro é submetido à reconstrução, onde é reconstituído no seu formato original, mas sem os elementos perigosos que possam comprometer a segurança. Este processo assegura que o ficheiro reconstruído está em conformidade com os padrões de segurança, ao mesmo tempo que mantém a sua usabilidade.

Finalmente, na etapa de output, o ficheiro reconstruído é disponibilizado ao utilizador como um documento seguro e livre de ameaças, mas com plena funcionalidade. Este método de funcionamento do CDR destaca-se pela sua abordagem proativa, garantindo que ficheiros

potencialmente perigosos sejam desarmados antes de representarem qualquer risco, proporcionando assim uma proteção robusta contra ameaças cibernéticas.

Sucintamente, o funcionamento de CDR são baseados em quatro (4) etapas principais:

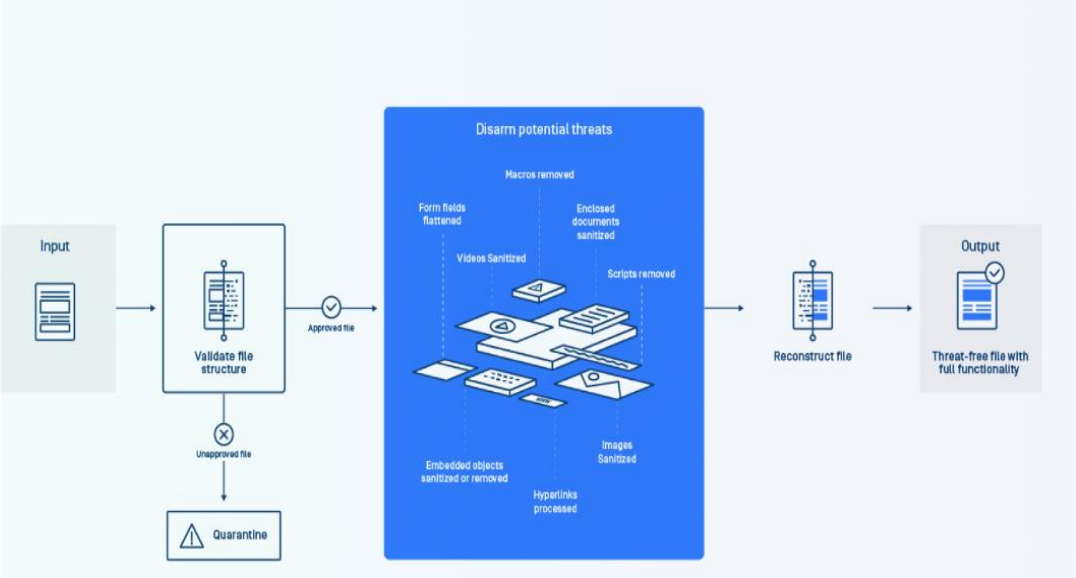


Figura 3- Funcionamento de CDR [95]

- ✓ **Extração de ficheiro:** Esta etapa permite verificar o ficheiro em busca de código malicioso. Essa etapa normalmente envolve o uso de *software* especializado, que examina o ficheiro segmentando-o em seus componentes constituintes, como textos, imagens e código.
- ✓ **Verificação do tipo de ficheiro:** Esta etapa é muito importante para o processo de CDR porque permite verificar o tipo de ficheiro que está sendo tratado, porque existe diferentes extensões de ficheiro e também cada ferramenta suporta uma determinada extensão de ficheiro.
- ✓ **Desarme e reconstrução de conteúdo:** O processo de Desarme e Reconstrução é a etapa 3 é o processo que permite desarmar o ficheiro dividindo em seus componentes distintos e executar uma análise em busca de ameaças, depois de tudo reconstruir o ficheiro eliminando todo o código malicioso e deixar o ficheiro seguro para o seu uso.
- ✓ **Entrega de Ficheiro:** Esta etapa os ficheiros são recompilados, renomeados e entregues, mantendo a integridade do ficheiro e permitir os utilizadores acessarem os ficheiros de uma forma segura [62].

3.4. Vantagens da tecnologia

O CDR apresenta várias vantagens significativas no contexto da cibersegurança, posicionando-se como uma solução eficaz para a proteção contra ameaças baseadas em ficheiros mal-intencionados. A sua abordagem proativa, que elimina componentes maliciosos antes que os ficheiros sejam abertos pelos utilizadores, oferece uma camada de proteção robusta e confiável.

Uma das principais vantagens do CDR é a sua capacidade de realizar uma análise profunda dos ficheiros, inspecionando cada componente, como s*cripts*, macros, *links* e metadados, em busca de códigos maliciosos. Este processo não só remove ameaças conhecidas, mas também elimina elementos maliciosos ocultos que poderiam escapar aos métodos tradicionais de deteção, como os utilizados por *software* antivírus. Esta capacidade é particularmente útil para proteger contra ameaças baseadas em *malware* e ameaças baseadas em ficheiros, proporcionando uma segurança abrangente.

Outro ponto forte do CDR é a sua capacidade de automatizar o processo de análise e reconstrução de ficheiros, permitindo que grandes volumes de dados sejam processados em curtos períodos de tempo. Esta eficiência é crucial para organizações que lidam com fluxos contínuos de documentos e dados provenientes de diferentes fontes, como *e-mails*, servidores de ficheiros ou plataformas de armazenamento na nuvem.

Além disso, o CDR conta com um recurso de deteção aprimorada, capaz de identificar código mal-intencionado escondido em áreas pouco convencionais, como metadados ou secções internas de documentos que, geralmente, não são analisadas por *software* de segurança tradicional. Esta capacidade reduz significativamente o risco de ataques avançados, como as ameaças de dia zero, em que os atacantes exploram vulnerabilidades desconhecidas antes que sejam corrigidas.

A tecnologia CDR oferece ainda as seguintes vantagens específicas:

- ✓ **Proteção contra ameaças de dia zero**: O CDR elimina componentes potencialmente maliciosos antes que possam ser explorados, mesmo em ataques que utilizam vulnerabilidades ainda não descobertas.
- ✓ **Deteção de ameaças aprimorada**: A análise detalhada permite identificar códigos maliciosos sofisticados, incluindo aqueles ocultos em metadados ou partes menos acessíveis dos ficheiros.

- ✓ **Maior segurança de rede**: Ao garantir que apenas ficheiros seguros sejam partilhados ou utilizados dentro da rede, o CDR reduz significativamente o risco de comprometer sistemas críticos.
- ✓ **Redução do risco de violação de dados**: A remoção de componentes maliciosos e a reconstrução segura dos ficheiros ajudam a prevenir ataques que poderiam levar à exposição ou roubo de dados sensíveis.
- ✓ **Experiência de utilizador aprimorada**: Embora garanta segurança, o CDR preserva a funcionalidade dos ficheiros reconstruídos, permitindo que os utilizadores continuem a utilizá-los sem comprometer a produtividade.
- ✓ **Políticas de segurança personalizáveis**: A tecnologia permite ajustar as políticas de análise e reconstrução de ficheiros de acordo com as necessidades específicas de cada organização, proporcionando flexibilidade e adaptação ao ambiente corporativo [58] [59] [60].

Em suma, o CDR não só protege contra uma ampla gama de ameaças cibernéticas, mas também melhora a eficiência operacional e a resiliência de sistemas e redes. A sua combinação de segurança proativa, automatização e capacidade de personalização torna-o uma ferramenta indispensável no arsenal de cibersegurança de organizações modernas.

3.5. Desvantagens da tecnologia

Embora o CDR ofereça uma abordagem robusta para proteger sistemas contra ameaças cibernéticas, a tecnologia apresenta algumas desvantagens que devem ser consideradas, especialmente em contextos onde a funcionalidade total dos ficheiros é essencial.

Uma das principais desvantagens do CDR está relacionada com a eliminação de conteúdos ativos, como macros, campos de formulários e *hiperlinks*. Estes elementos, frequentemente utilizados para automatizar tarefas ou facilitar a navegação em documentos, são desativados ou removidos durante o processo de desarmamento. Como resultado, os utilizadores que esperam receber um ficheiro com toda a sua funcionalidade original podem, em vez disso, obter um documento simplificado, com funcionalidades essenciais desativadas.

Além disso, mesmo com a implementação da tecnologia de seleção positiva (um método avançado que tenta reconstruir os ficheiros preservando a funcionalidade), alguns elementos podem ainda ser eliminados durante o processo, afetando a usabilidade do ficheiro final. Por exemplo, documentos que dependem de macros complexas para cálculos automatizados ou

formulários interativos com campos editáveis podem perder essas capacidades, o que pode comprometer tarefas importantes que dependem dessas funcionalidades.

Outro aspeto crítico é que, em alguns casos, a reconstrução do ficheiro pode torná-lo inalterável ou não editável, especialmente quando os componentes eliminados eram essenciais para a edição ou personalização. Esta limitação pode ser problemática em cenários onde o utilizador precisa de modificar o conteúdo do documento ou trabalhar com ele de forma dinâmica.

Adicionalmente, a dependência do CDR em políticas de segurança predefinidas pode levar à remoção de elementos que, embora inofensivos, sejam identificados como potenciais ameaças. Isto pode resultar em perdas desnecessárias de funcionalidade, especialmente em organizações que utilizam formatos de ficheiros específicos ou personalizações que não estão contempladas nas definições de segurança padrão do sistema.

Finalmente, outra desvantagem está relacionada com o custo e a complexidade da implementação do CDR em ambientes corporativos. A integração da tecnologia requer infraestruturas avançadas e, em muitos casos, formação especializada para equipas de TI, o que pode ser um obstáculo para organizações com recursos limitados [62].

Em resumo, apesar da sua eficácia na eliminação de ameaças cibernéticas, o CDR apresenta desafios significativos, principalmente no que diz respeito à preservação da funcionalidade completa dos ficheiros e à compatibilidade com fluxos de trabalho que dependem de conteúdos dinâmicos. Assim, a sua utilização deve ser cuidadosamente ponderada, considerando o equilíbrio entre a segurança e a usabilidade exigidas por cada organização ou contexto.

3.6. Mercado de *CDR*

Prevê-se que o mercado global de CDR apresente um crescimento significativo nos próximos anos, com uma Taxa Composta de Crescimento Anual (CAGR) projetada de 18,3% entre 2023 e 2032. Em 2022, o mercado foi avaliado em 274,8 milhões de dólares e está estimado para atingir um impressionante 1,4 mil milhões de dólares até 2032, refletindo a crescente importância desta tecnologia no panorama global de cibersegurança [63].

Este crescimento acelerado é impulsionado por vários fatores chave. Um dos principais motores é o aumento exponencial das violações de dados, que representam um risco crescente para organizações em todo o mundo. À medida que os cibercriminosos

desenvolvem métodos mais sofisticados para comprometer redes e sistemas, as empresas reconhecem a necessidade de implementar soluções como o CDR, que oferece uma defesa proativa contra ameaças baseadas em ficheiros.

Outro fator determinante é o aumento das regulamentações e conformidades mais rígidas em relação à segurança de conteúdo. Os governos e organizações internacionais estão a introduzir leis e normas cada vez mais rigorosas para proteger dados sensíveis e garantir a privacidade. Esta pressão regulatória está a impulsionar a adoção de tecnologias avançadas como o CDR, que ajuda as organizações a cumprir essas exigências enquanto minimizam os riscos associados a ataques cibernéticos [63].

Além disso, o crescimento do mercado de CDR é alimentado pelo aumento do número de ameaças avançadas, como ataques de dia zero, *ransomware* e *malware*, bem como ataques baseados em ficheiros. Estas ameaças, muitas vezes difíceis de detetar com métodos tradicionais de segurança, destacam a necessidade de soluções como o CDR, que elimina componentes maliciosos de ficheiros antes que estes possam causar danos. O aumento de ataques baseados em ficheiros, em particular, reforça a relevância do CDR, uma vez que mais de 90% dos ataques cibernéticos utilizam ficheiros como vetor de entrada.

O mercado também é impulsionado pela adoção crescente de soluções baseadas na nuvem e pelo trabalho remoto, que aumentaram a troca de ficheiros digitais e, consequentemente, a exposição a ameaças. Organizações em setores críticos, como saúde, finanças, governo e tecnologia, estão a investir significativamente em tecnologias de CDR para proteger os seus sistemas e dados contra potenciais ataques.

Com uma combinação de fatores económicos, regulamentares e tecnológicos a impulsionar a procura, o mercado de CDR está preparado para um crescimento contínuo e sustentado. Esta evolução sublinha a crescente consciencialização sobre a importância da cibersegurança proativa, destacando o papel do CDR como uma solução indispensável na luta contra ameaças cibernéticas [63].

O aumento de incidentes de ciberataques e violações de dados e o aumento da conformidade governamental e dos padrões regulatórios sobre cibersegurança estão a impulsionar o crescimento do mercado. Alem disso, o aumento na adoção de soluções e serviços de segurança baseados em nuvem está alimentando o crescimento do mercado de CDR. No entanto, o alto custo de implementação da solução de CDR e a escassez de profissionais qualificados em cibersegurança e planeamento estratégico limitam o crescimento do

mercado de CDR. Por outro lado, espera-se que o aumento dos investimentos em soluções de segurança de *big data* e o aumento das iniciativas de transformação digital em diferentes setores forneçam inúmeras oportunidades para a expansão do mercado durante o período de previsão.

O CDR é uma estratégia de segurança que envolve a eliminação de elementos potencialmente perigosos dos ficheiros recebidos e a reconstrução com conteúdo não contaminado. Essa técnica pode ser utilizada para mitigar o risco de ataques de *malware* em redes corporativas e garantir que todos os ficheiros sejam seguros para uso. Além disso, vários setores, como saúde, finanças, e entre outros sectores, têm regulamentos sobre privacidade e segurança de dados. O CDR pode ajudar as organizações a atender a esses requisitos de conformidade, fornecendo uma camada adicional de proteção contra ataques baseados em ficheiros.

O mercado global de CDR é segmentado por diversos critérios, incluindo componentes, área de aplicação, modo de implantação, tamanho da organização (gráfico 6), vertical e região geográfica. Os componentes são categorizados entre soluções e serviços, enquanto as áreas de aplicação incluem *e-mail*, *web*, Protocolo de Transferência de Ficheiros (FTP) e dispositivos removíveis. O modo de implantação divide-se em ambientes locais e em nuvem, e no que diz respeito ao tamanho da organização, há uma distinção entre grandes empresas de telecomunicações e pequenas e médias empresas, com segmentos específicos para o setor de *Banking, Financial Services and Insurance* (BFSI), Tecnologia da Informação (TI) e telecomunicações, energia e serviços públicos, manufatura e saúde. Finalmente, a análise regional abrange as regiões da América do Norte, Europa, Ásia-Pacífico e LAMEA, oferecendo uma perspetiva abrangente sobre a estrutura e dinâmica do mercado de CDR. [63].

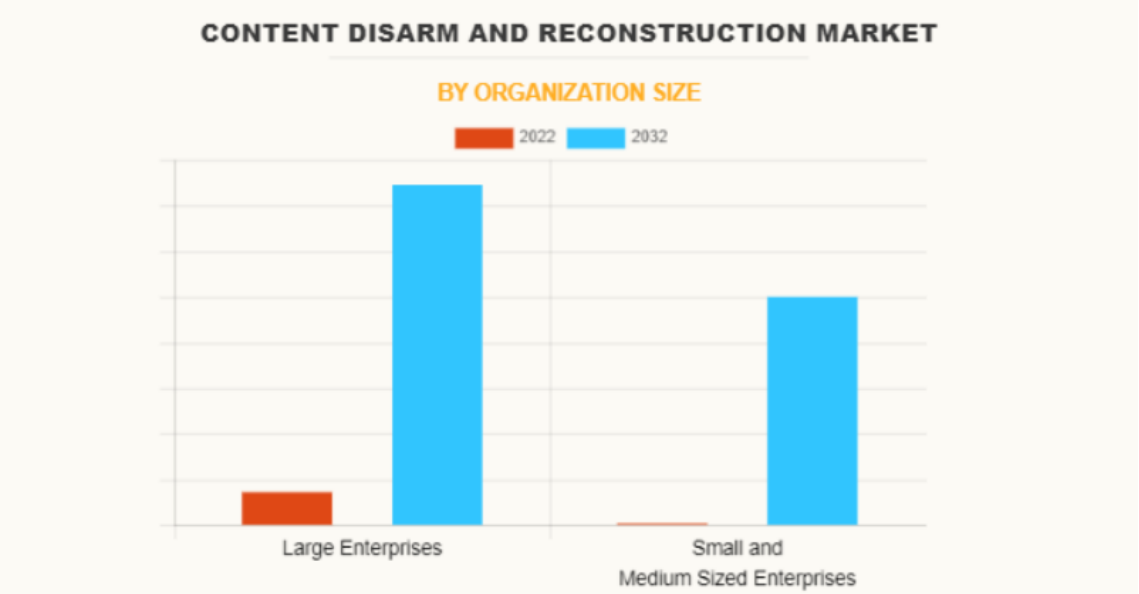


Gráfico 6- Mercado de Content Disarm and Reconstruction (CDR) [63]

Em 2022, o segmento de grandes empresas dominou a participação no mercado de CDR, uma tendência que deve persistir ao longo do período de previsão devido às infraestruturas de TI mais complexas e à necessidade de proteger grandes volumes de dados sensíveis. Contudo, o segmento de pequenas e médias empresas está previsto para experimentar um crescimento substancial nos próximos anos, impulsionado pelo aumento das ameaças cibernéticas e pela adoção de políticas de trabalho remoto. A crescente consciencialização sobre a segurança digital levará essas empresas a integrar soluções de CDR em suas operações, indicando uma evolução significativa no panorama de segurança cibernética para todos os segmentos [63].

3.6.1. Principais Empresas que atuam na área de *CDR*

O mercado de CDR tem vindo a crescer rapidamente, com várias empresas a destacarem-se como líderes no fornecimento de soluções inovadoras para proteger organizações contra uma ampla gama de ameaças cibernéticas, incluindo *malware, ransomware* e ataques de dia zero. Estas empresas desenvolvem tecnologias avançadas que ajudam a identificar, remover e reconstruir ficheiros potencialmente perigosos antes que possam comprometer os sistemas. Encontram-se algumas das principais empresas que atuam nesta área, cada uma com especializações e abordagens distintas:

- ✓ Check Point Software Technologies Lts.
- ✓ Fortinet, Inc
- ✓ Broadcom
- ✓ OPSWAT, Inc

- ✓ Perton
- ✓ Deep Secure
- ✓ Votiro
- ✓ Resec
- ✓ Sasa Software
- ✓ Glasswall

Check Point é uma empresa norte-americana, fundada em 1993, reconhecida no setor de cibersegurança e oferece soluções abrangentes que incluem tecnologias de CDR. A empresa integra o CDR nas suas soluções de *firewall* e proteção de *e-mail*, permitindo que as organizações desarmem ficheiros maliciosos antes que estes entrem nas redes internas. A *Check Point* foca-se na proteção contra ataques avançados, incluindo ameaças de dia zero [88].

A Fortinet é uma empresa conhecida pelas suas soluções de segurança integradas, incluindo o uso de CDR para complementar os seus sistemas de *firewall* e proteção de *endpoints*. As suas tecnologias permitem uma análise profunda e reconstrução de ficheiros, protegendo organizações contra-ataques baseados em ficheiros em ambientes corporativos e na nuvem [88].

A Broadcom, que adquiriu a Symantec, utiliza soluções baseadas em CDR como parte do seu portefólio de segurança cibernética. Estas tecnologias são integradas em plataformas de segurança de *e-mail* e na proteção de *endpoints*, garantindo que ficheiros maliciosos sejam neutralizados antes de atingirem os utilizadores finais [88].

A OPSWAT oferece ferramentas de CDR que se destacam pela sua eficácia em ambientes industriais e corporativos. As suas soluções são amplamente utilizadas em setores críticos, como saúde e energia, onde a segurança de ficheiros é essencial. A OPSWAT foca-se na deteção e remoção de ameaças ocultas, incluindo códigos embutidos em documentos [88].

A Peraton é uma empresa focada em soluções de cibersegurança para setores governamentais e industriais. Utiliza CDR como parte da sua abordagem integrada para proteger sistemas críticos contra-ataques sofisticados, incluindo aqueles que envolvem ficheiros maliciosos [97].

A Deep Secure é especializada em tecnologias de CDR que oferecem proteção avançada contra ameaças baseadas em ficheiros. A empresa utiliza métodos inovadores para desarmar

e reconstruir documentos, garantindo a segurança dos dados sem comprometer a funcionalidade dos ficheiros [88].

A Votiro é uma empresa americana, fundada em 2010, e é especializada em oferecer soluções avançadas de deteção e prevenção de ameaças para proteger as organizações contra ataques cibernéticos. Sua tecnologia, reconhecida e amplamente utilizada nos setores financeiro e empresarial, oferece uma camada robusta de proteção, especialmente em relação a *e-mails* e transferências de ficheiros, contribuindo significativamente para a segurança cibernética das empresas. A eficácia das soluções da *Votiro* demonstra a importância da inovação tecnológica na mitigação de ameaças digitais, impulsionando as práticas de segurança robustas e confiáveis nas organizações [88].

A Resec [88] oferece soluções de CDR que permitem proteger redes corporativas contra-ataques baseados em ficheiros, com especial foco na eliminação de ameaças *zero-day*. As suas ferramentas integram-se facilmente com sistemas de segurança existentes, oferecendo uma camada adicional de proteção.

A Sasa Software [88] fornece ferramentas de CDR para proteção contra ficheiros maliciosos em múltiplos canais, incluindo *e-mails*, transferências de ficheiros e dispositivos removíveis. A sua tecnologia é amplamente utilizada por organizações que necessitam de proteção robusta contra ataques cibernéticos.

A Glasswall [96] é uma empresa de segurança cibernética das empresas mais inovadoras no campo do CDR, focando-se na reconstrução segura de ficheiros sem comprometer a funcionalidade. As suas soluções são reconhecidas pela rapidez e precisão, tornando-se uma escolha popular em setores que exigem alta segurança.

Estas empresas lideram o desenvolvimento de soluções de CDR, oferecendo ferramentas indispensáveis para organizações que enfrentam ameaças cibernéticas complexas. A integração destas tecnologias em sistemas corporativos permite uma proteção mais eficaz contra uma vasta gama de ataques, garantindo que ficheiros maliciosos sejam desarmados antes de poderem comprometer a integridade dos sistemas. Cada empresa traz uma abordagem única, adaptada às necessidades específicas de diferentes setores e ambientes organizacionais.

3.6.2. Aplicação de *CDR*

O CDR pode ser aplicado em diversos contextos, tornando-se uma ferramenta versátil e indispensável para a segurança cibernética. As suas funcionalidades permitem proteger sistemas e redes contra ameaças provenientes de diferentes fontes, como:

- ✓ E-mail;
- ✓ Web
- ✓ FTP;
- ✓ Dispositivos removíveis

O CDR desempenha um papel crucial na proteção contra ameaças transmitidas por *e-mail*, que continuam a ser o vetor de ataque mais comum. Nesta aplicação, o CDR verifica e limpa todos os anexos de ficheiros recebidos por *e-mail*, eliminando componentes maliciosos, como macros, *scripts* ou *links* embutidos. Assim, garante que os utilizadores recebam ficheiros livres de códigos maliciosos, reduzindo significativamente o risco de infeções por *malware* ou *ransomware*. Esta abordagem é particularmente importante, dado que mais de 90% dos ataques de *malware* utilizam o *e-mail* como canal de entrada [89].

Na navegação na Web, o CDR atua ao desarmar s*cripts* maliciosos e códigos ocultos incorporados em ficheiros transferidos de websites. Esta aplicação protege os utilizadores contra-ataques que exploram downloads automáticos ou vulnerabilidades em navegadores. Por exemplo, quando um utilizador descarrega um documento de um site potencialmente comprometido, o CDR remove todos os elementos maliciosos antes de permitir que o ficheiro seja aberto, garantindo uma navegação mais segura.

No caso de transferências de ficheiros por FTP (*File Transfer Protocol*), o CDR protege as organizações contra a transmissão de ficheiros infetados. Ao inspecionar e desarmar ficheiros enviados ou recebidos através deste protocolo, o CDR assegura que apenas ficheiros seguros entram ou saem da rede. Esta aplicação é essencial em ambientes corporativos onde o FTP ainda é amplamente utilizado para partilhar dados sensíveis entre diferentes localizações.

Os dispositivos de armazenamento removível, como *pen drives* e discos rígidos externos, representam outro canal comum para a disseminação de *malware*. O CDR higieniza os ficheiros acedidos por meio destes dispositivos, removendo qualquer código malicioso ou objetos embutidos antes que os ficheiros sejam abertos nos sistemas. Este processo é

particularmente útil em ambientes onde dispositivos externos são frequentemente utilizados, reduzindo o risco de infeção e propagação de *malware* dentro da rede.

Além dos contextos mencionados, o CDR também pode ser integrado em sistemas de partilha de ficheiros na nuvem, plataformas colaborativas e servidores de ficheiros corporativos. Estas integrações garantem uma proteção contínua contra ameaças baseadas em ficheiros em todos os pontos de interação digital, oferecendo uma camada de segurança consistente em infraestruturas tecnológicas complexas.

A aplicação do CDR em diferentes contextos demonstra a sua eficácia e versatilidade na proteção contra ameaças cibernéticas. Ao garantir que ficheiros provenientes de e-mails, sites, FTP ou dispositivos removíveis sejam inspecionados, desarmados e reconstruídos antes de serem utilizados, o CDR oferece uma solução robusta para mitigar riscos e reforçar a segurança de sistemas e redes em vários ambientes.

4. Soluções da tecnologia CDR

4.1. Docbleach

Docbleach é uma ferramenta de código aberto que serve para desarmar e reconstruir conteúdos, com o intuito de eliminar potenciais ameaças nos documentos dos utilizadores. A *Docbleach* não é uma ferramenta tão perfeita para proteger os sistemas contra-ataques dos ficheiros maliciosos, mas foram tomadas algumas decisões para proteger os sistemas contra a maior parte dos ataques deste género. Muitas tecnologias comuns de segurança cibernética, como *antimalware* e antivírus, só podem detetar ameaças conhecidas e não podem detetar ou proteger os sistemas de ataques secretos ou de dia zero. Na verdade, 80% das violações bem-sucedidas são ataques do dia zero que não são reconhecidos pelas soluções tradicionais de deteção baseadas em assinatura. Hoje em dias os utilizadores não têm forma de se protegerem contra as várias variantes de vírus que surge diariamente e que chegam a caixa de *e-mail* dos utilizadores [64].

A ferramenta *Docbleach* suporta os seguintes formatos de ficheiros:

- ✓ Documentos do Office (.doc, .docx, .xls, .xlsx. etc)
- ✓ Ficheiro de PDF (.pdf)
- ✓ Ficheiros RTF (.rtf)

Os documentos do *Microsoft Office* são alguns dos ficheiros mais utilizados em ambientes empresariais e, simultaneamente, um dos vetores de ataque mais explorados pelos *hackers*. Estes ficheiros podem conter macros, *scripts* maliciosos ou objetos incorporados que representam uma ameaça para os sistemas. O *Docbleach* inspeciona e remove esses componentes perigosos, garantindo que os documentos sejam seguros antes de serem abertos ou partilhados.

O formato PDF é amplamente utilizado para a partilha de documentos, mas também tem sido explorado para ocultar códigos maliciosos, objetos ativos ou *hiperlinks* maliciosos. A ferramenta *Docbleach* aplica técnicas avançadas de desarmamento em ficheiros PDF, eliminando elementos suspeitos, como macros ou objetos incorporados, enquanto preserva o conteúdo necessário para o utilizador. Esta funcionalidade é particularmente importante para prevenir ataques baseados em ficheiros PDF, como aqueles que utilizam *exploits* para explorar vulnerabilidades.

O formato RTF, conhecido pela sua compatibilidade com várias plataformas, é frequentemente utilizado para partilhar documentos simples, mas também é explorado para ataques cibernéticos. Os ficheiros RTF podem conter comandos maliciosos ocultos que podem ser acionados quando abertos em editores de texto. O *Docbleach* deteta e remove estes comandos perigosos, garantindo que os ficheiros RTF são seguros para uso.

A ferramenta remove conteúdos perigosos e também preserva a funcionalidade essencial dos ficheiros, garantindo que os utilizadores possam continuar a trabalhar com eles sem interrupções significativas. A capacidade de suportar múltiplos formatos de ficheiros torna o *Docbleach* uma solução versátil, adequada para diferentes cenários de utilização. Além disso, o *Docbleach* pode ser integrado em fluxos de trabalho automatizados, permitindo que organizações processem grandes volumes de ficheiros de forma eficiente e segura. Esta ferramenta é especialmente valiosa em ambientes onde a troca de ficheiros é constante, como setores de saúde, financeiro, governamental e educativo [90].

O suporte a formatos amplamente utilizados, como documentos do *Office*, ficheiros PDF e ficheiros RTF, faz do *Docbleach* uma solução essencial para organizações que desejam proteger os seus sistemas contra ameaças cibernéticas associadas à partilha de ficheiros. A sua capacidade de desarmar e reconstruir ficheiros garante um equilíbrio entre segurança e funcionalidade, tornando-o uma ferramenta confiável no contexto da cibersegurança moderna [90].

4.2. Oletools

Oletools é um conjunto de ferramentas *python* para analisar ficheiro *Microsoft OLE2* (também chamado de Armazenamento Estruturado, Formato Binário de Ficheiro Composto ou Formato de Ficheiro de Documento Composto) como documentos do *Microsoft Office* ou Mensagem do *Outlook*, é utilizado principalmente para analise de *malware*, perícia e depuração. Ele é baseado no analisador *olefile* [66] porque permite analisar, ler e gravar ficheiros *Microsoft OLE2*.

A ferramenta *Oletools* possui as seguintes ferramentas:

- ✓ ***Oleid:*** Oleid é um *script* para analisar o ficheiro OLE, como documentos do Office, para detectar características específicas que poderiam indicar que o ficheiro é suspeito ou malicioso, em termos de segurança, ele pode detectar macros VBA, objectos Flash incorporados [65].
  Exemplo: $: oleid nome_ficheiro.extensão

- ✓ ***Olevba:*** Olevba é um *script* para analisar ficheiro OLE e OpenXML, como documentos de *MS Office*, para detetar macros VBA, extrair o seu código-fonte em texto não encriptado e detetar padrões relacionados à segurança como macros executáveis automaticamente, palavras-chaves VBA suspeitas usadas por malware, anti-sandboxing e antivirtualização [65].
  Exemplo: $: olevba nome_ficheiro.extensão

Para extrair macros VBA no ficheiro para uso posterior utiliza-se o seguinte comando:
$: olevba -c nome_ficheiro.extensão > nome_ficheiro.vba

A ferramenta *Oletools* é um conjunto de utilitários projetado para a análise de ficheiros que utilizam o formato OLE (*Object Linking and Embedding*), amplamente utilizado em documentos do *Microsoft Office,* como *Word, Excel e PowerPoint*. Esta ferramenta é especialmente útil para identificar e neutralizar potenciais ameaças, como macros maliciosas, códigos ocultos e indicadores de ataque cibernético. *Oletools* é amplamente utilizada em investigações de cibersegurança para a análise de ficheiros suspeitos e permite uma análise detalhada de vários elementos relacionados com *malware*. A seguir, são destacadas as suas principais funções:

1. Análise Completa da Estrutura Binária de Projetos VBA

- ✓ Oletools realiza uma análise aprofundada da estrutura binária de projetos VBA (*Visual Basic for Applications*), permitindo determinar a localização exata de macros comprimidas em ficheiros maliciosos.
- ✓ A ferramenta pode extrair os projetos VBA, incluindo páginas de código específicas, como a página de código 1251, utilizada para caracteres cirílicos.

2. Extração e Análise de Código-Fonte

- ✓ Oletools permite a extração e análise do código-fonte de macros e *scripts* embutidos nos ficheiros, ajudando a identificar comportamentos suspeitos ou maliciosos que possam comprometer a segurança de sistemas.

3. Deteção de Palavras-Chave Suspeitas

- ✓ A ferramenta é capaz de detetar palavras-chave frequentemente associadas a *malware*, permitindo identificar rapidamente padrões utilizados em ataques cibernéticos, como funções ou comandos conhecidos por serem explorados por atacantes.

4. Deteção de Macros Autoexecutáveis

- ✓ Oletools identifica macros configuradas para autoexecução, um método comumente utilizado por cibercriminosos para ativar *scripts* maliciosos assim que um ficheiro é aberto pelo utilizador.

5. Desofuscação de Cadeias de Caracteres

- ✓ A ferramenta inclui capacidades avançadas de desofuscação para interpretar cadeias de caracteres codificadas ou ocultas, que são frequentemente usadas para mascarar comandos ou dados maliciosos. Isso inclui técnicas como:
  - Hexadecimal (Hex);
  - Base64;
  - StrReverse;
  - Combinações como Dridex Hex + StrReverse.

6. Extração de Indicadores de Comprometimento (IOC)

- ✓ *Oletools* pode extrair vários Indicadores de Comprometimento (IOC), como:
  - Endereços IP;
  - URLs;
  - Endereços de correio eletrónico;
  - Nomes de ficheiros executáveis.
- ✓ Estes indicadores podem estar presentes em texto claro ou oculto dentro de macros ou ficheiros comprimidos.

7. Análise em Modo Triagem

- ✓ A ferramenta oferece um modo de triagem que permite analisar rapidamente uma coleção de ficheiros de uma só vez, tornando-a eficiente para lidar com grandes volumes de documentos suspeitos.

8. Alternativas à *Oletools*

- ✓ Existem outras ferramentas que complementam ou oferecem funcionalidades semelhantes à *Oletools*, incluindo:
  - *Oledump*: Focado na extração e análise de objetos OLE.
  - *OfficeMalScanner*: Especializado na análise de documentos do *Office* em busca de malware [66].

A *Oletools* é uma ferramenta poderosa para a análise de ficheiros OLE, especialmente em contextos de cibersegurança, onde a deteção precoce de ameaças pode fazer a diferença. As suas funcionalidades, como análise de estrutura binária, extração de código-fonte, deteção de macros autoexecutáveis e indicadores de compromissos, tornam-na indispensável para investigadores e profissionais de segurança cibernética que lidam com ficheiros maliciosos. Além disso, a sua capacidade de triagem de múltiplos ficheiros simultaneamente aumenta a eficiência em cenários de grande escala, complementando outras ferramentas, como *Oledump* e *OfficeMalScanner*.

A ferramenta *Oletools* destaca-se pela sua flexibilidade e eficiência na análise de ficheiros que utilizam o formato OLE. Esta solução foi projetada para detetar, analisar e neutralizar ameaças embutidas em ficheiros do *Microsoft Office* e outros documentos que utilizam objetos incorporados. Entre as suas principais características funcionais, incluem-se as seguintes:

1. Opções para Digitalizar Vários Ficheiros

- ✓ Uma das funcionalidades mais práticas da *Oletools* é a sua capacidade de analisar múltiplos ficheiros simultaneamente. Esta opção é particularmente útil em cenários onde grandes volumes de documentos precisam de ser inspecionados, como em auditorias de segurança ou investigações forenses.
- ✓ Este recurso permite aos utilizadores poupar tempo e otimizar o processo de análise, garantindo que potenciais ameaças em múltiplos ficheiros sejam identificadas de forma rápida e eficiente.

2. Saída em Formato CSV

- ✓ A ferramenta oferece a possibilidade de exportar os resultados da análise em formato CSV (*Comma-Separated Values*), um formato amplamente utilizado para processamento de dados.
- ✓ Esta funcionalidade permite que os resultados sejam facilmente organizados, analisados e integrados em relatórios de segurança ou sistemas de gestão de incidentes.
- ✓ Além disso, o formato CSV é compatível com diversas aplicações, como *Microsoft Excel* e ferramentas de visualização de dados, facilitando a análise de padrões e tendências em ataques.

3. Verificação de Ficheiros ZIP Encriptados

- ✓ A *Oletools* inclui suporte para verificar ficheiros ZIP encriptados, uma funcionalidade essencial para lidar com ficheiros compactados que podem conter documentos maliciosos.
- ✓ Este recurso permite que os utilizadores inspecionem ficheiros ZIP protegidos por senha, identificando possíveis ameaças embutidas nos documentos contidos no arquivo.
- ✓ Em casos onde a senha para o ficheiro ZIP é conhecida, a *Oletools* pode abrir e inspecionar os documentos, oferecendo uma camada adicional de segurança em situações onde os atacantes utilizam compactação e encriptação para ocultar *malware.*

As características funcionais da *Oletools* tornam-na uma ferramenta versátil no combate a ameaças cibernéticas [66]. A sua capacidade de digitalizar múltiplos ficheiros simultaneamente, exportar resultados em formato CSV e verificar ficheiros ZIP encriptados aumenta significativamente a sua utilidade em ambientes corporativos e de segurança cibernética. Estas funcionalidades permitem uma abordagem sistemática e eficiente para a identificação e mitigação de ameaças, consolidando a *Oletools* como uma solução essencial no arsenal de ferramentas de análise e defesa contra ataques cibernéticos.

A ferramenta *Oletools* é amplamente reconhecida no setor de cibersegurança pelas suas diversas vantagens que a tornam uma solução indispensável para a análise de ficheiros no formato OLE. Abaixo estão detalhadas as suas principais vantagens, que abrangem tanto a

funcionalidade quanto a acessibilidade, facilitando o trabalho de profissionais e organizações na deteção e mitigação de ameaças cibernéticas:

1. Múltiplas Opções para Cada Tipo de Dados

- ✓ A *Oletools* destaca-se pela sua capacidade de oferecer opções adaptadas a diferentes tipos de dados analisados.
- ✓ Seja na análise de macros, cadeias de texto ocultas, objetos incorporados ou metadados, a ferramenta disponibiliza métodos especializados para tratar cada tipo de conteúdo.
- ✓ Esta flexibilidade garante resultados precisos e uma análise personalizada, permitindo aos utilizadores focar-se em aspetos específicos de cada ficheiro, com maior controlo sobre os dados que estão a ser inspecionados.

2. Apresentação em Vários Tipos de Interfaces

- ✓ Uma das grandes vantagens da *Oletools* é a versatilidade das suas interfaces, adaptando-se a diferentes necessidades dos utilizadores. A ferramenta suporta:
  - o GUI (Interface Gráfica do Utilizador): Ideal para utilizadores menos experientes ou para aqueles que preferem uma interface visual mais intuitiva.
  - o CLI (Interface de Linha de Comando): Dirigida a utilizadores avançados e profissionais de cibersegurança, permitindo automatizar tarefas e integrar *a Oletools* em fluxos de trabalho através de *scripts.*
  - o Browser: Algumas funcionalidades da ferramenta podem ser acedidas diretamente a partir de um navegador, oferecendo uma solução prática para análises rápidas sem necessidade de instalação de *software*.

3. Suporte para Análise de Imagens

- ✓ A ferramenta suporta a análise de imagens incorporadas em documentos, detetando possíveis códigos maliciosos ou dados ocultos embutidos nas imagens.
- ✓ Esta funcionalidade é particularmente relevante, dado que os *hackers* utilizam frequentemente imagens como um vetor para mascarar ameaças ou exfiltrar dados, aproveitando o facto de que muitos *softwares* tradicionais de cibersegurança não analisam imagens em profundidade.

4. Facilidade de Utilização

- ✓ Apesar da sua complexidade técnica, a *Oletools* foi concebida para ser fácil de utilizar, independentemente do nível de experiência do utilizador.
- ✓ A interface intuitiva e a documentação abrangente tornam a ferramenta acessível tanto para profissionais de cibersegurança como para utilizadores menos experientes.
- ✓ Além disso, a simplicidade de configuração e a disponibilidade de várias opções de interface garantem que a ferramenta pode ser rapidamente integrada em fluxos de trabalho sem necessidade de longos períodos de adaptação.

As vantagens da *Oletools*, como a sua capacidade de lidar com múltiplos tipos de dados, a disponibilidade de diferentes interfaces, o suporte para análise de imagens e a facilidade de utilização, tornam-na uma ferramenta essencial no campo da cibersegurança. Esta versatilidade permite que a ferramenta atenda às necessidades de diferentes utilizadores, desde profissionais avançados até utilizadores ocasionais, consolidando-a como uma das soluções mais eficientes e adaptáveis para a análise de ficheiros no formato OLE e a deteção de ameaças cibernéticas [66].

4.3. ExeFilter

Exefilter é uma ferramenta que foi desenvolvida pela DGA/CELAR (Ministério da Defesa Francês) desde 2004, é escrito em *Python,* e foi lançado como código aberto em 2008. *Exefilter* é uma ferramenta de código aberto para filtrar formatos de ficheiros em e-mails, páginas da web ou ficheiros. O *Exifilter* deteta muitos formatos de ficheiros comuns e pode remover conteúdos ativos como (scrips, macros, etc.) de acordo com uma política definida.

Muitos sistemas informáticos não estão protegidos contra ameaças de conteúdos maliciosos, e estes conteúdos maliciosos podem entrar nos sistemas através de *e-mail*, *web* ou dispositivos removíveis.

Os códigos maliciosos podem ser escondidos na maioria dos formatos de ficheiro comuns como por exemplo: documentos de OFFICE, PDF, HTML, XML, RTF, JPEG etc.

Atualmente, são aproveitadas as recentes vulnerabilidades descobertas em vários formatos de ficheiro para atacar os sistemas dos alvos. Por isso esta ferramenta foi projetada para ser incluído em *gateways* (e-mail, web, serviços web) ou em estações de trabalhos dos utilizadores para filtrar os dispositivos removíveis [67]. A figura 4 ilustra a interface gráfica do *Exefilter*.

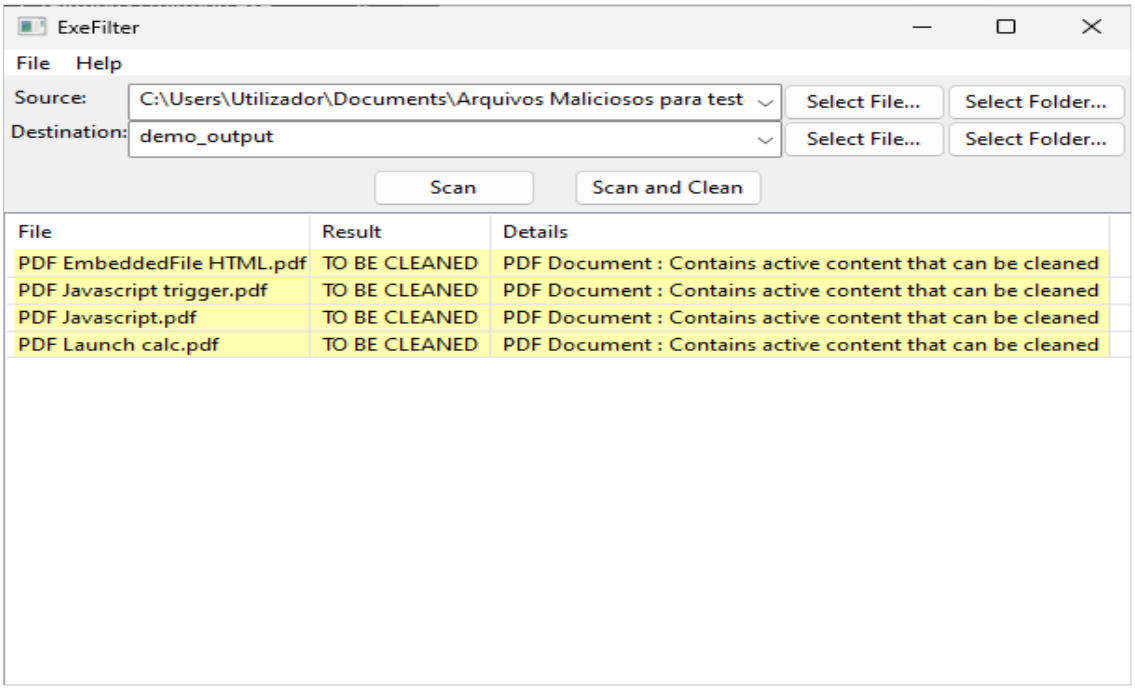


Figura 4- Interface Gui do Exefilter

O *Exefilter* é uma ferramenta desenvolvida com o objetivo de fortalecer a segurança de redes sensíveis e proteger sistemas contra ameaças cibernéticas associadas a ficheiros, mensagens de e-mail e conteúdos ativos. Os seus objetivos específicos refletem a sua capacidade de atuar de forma proativa na defesa contra ataques baseados em ficheiros maliciosos e conteúdos não confiáveis provenientes de fontes externas. Abaixo são detalhados os principais objetivos do *Exefilter:*

1. Proteger Redes Sensíveis Contra-Ataques Baseados em Ficheiros e Conteúdos Ativos

- ✓ O E*xefilte*r foi projetado para proteger redes sensíveis, como aquelas usadas em organizações empresariais, governamentais ou de infraestruturas críticas, contra ameaças cibernéticas que exploram ficheiros maliciosos, mensagens de *e-mail* e conteúdos ativos, como macros ou *scripts* embutidos.
- ✓ Este objetivo garante que ficheiros com potenciais ameaças sejam bloqueados antes de atingirem os sistemas, protegendo contra-ataques que possam comprometer dados sensíveis ou a estabilidade da rede.

2. Filtrar Todos os Conteúdos Ativos Indesejados das Fontes Externas

- ✓ O *Exefilter* atua como um filtro avançado, eliminando conteúdos ativos indesejados provenientes de fontes externas, como *e-mails*, transferências de ficheiros e dispositivos removíveis.

- ✓ Conteúdos ativos, como macros em documentos do Microsoft Office, *scripts* embutidos ou objetos incorporados, são frequentemente utilizados por cibercriminosos para lançar ataques. O *Exefilter* identifica e bloqueia esses elementos antes que possam representar uma ameaça.
- ✓ Este objetivo é essencial para prevenir infeções de *malwar*e e reduzir o risco de violações de segurança causadas por conteúdos não verificados.

3. Garantir a Entrada Apenas de Ficheiros Conhecidos e Controlados

- ✓ O *Exefilte*r assegura que apenas formatos de ficheiros conhecidos e controlados sejam permitidos dentro do sistema, garantindo que os ficheiros aprovados sejam analisados e cumpram os padrões de segurança estabelecidos.
- ✓ Este objetivo é alcançado através de uma abordagem baseada em políticas, onde os administradores podem definir quais tipos de ficheiros são permitidos. Ficheiros desconhecidos, incomuns ou potencialmente perigosos são automaticamente bloqueados ou enviados para quarentena para análise adicional.
- ✓ Essa funcionalidade reduz drasticamente o risco de ataques que utilizem formatos de ficheiros menos comuns ou manipulados para explorar vulnerabilidades.

Os objetivos do *Exefilter* refletem o seu papel como uma ferramenta essencial para organizações que procuram fortalecer a sua segurança contra-ataques cibernética baseada em ficheiros e conteúdos ativos. Ao proteger redes sensíveis, filtrar conteúdos indesejados e garantir que apenas ficheiros confiáveis entrem no sistema, o *Exefilter* proporciona uma camada adicional de proteção, reduzindo significativamente o risco de infeções e violações de dados. A sua abordagem proativa permite que organizações mantenham ambientes seguros e protegidos contra uma ampla gama de ameaças modernas.

A ferramenta *Exefilter* é uma solução inovadora concebida para filtrar e monitorizar ficheiros, garantindo maior segurança e conformidade com políticas predefinidas. As suas principais características incluem:

1. Filtragem Personalizável

- ✓ O *Exefilter* permite a aplicação de políticas específicas para o processamento de ficheiros. Estas políticas são definidas de acordo com as necessidades do utilizador ou da organização, assegurando um elevado grau de personalização.

2. Algoritmo Exclusivo de Filtragem

- ✓ A ferramenta utiliza um algoritmo avançado que filtra ficheiros com base em:
  - Extensão do ficheiro: Análise automatizada para identificar formatos específicos.
  - Conteúdo do ficheiro: Verificação do conteúdo interno, independentemente da extensão.
  - Deteção e remoção de conteúdo ativo: Proteção contra *scripts* e códigos potencialmente maliciosos.

3. Reconhecimento Abrangente de Formatos

O *Exefilter* reconhece uma ampla variedade de formatos de ficheiros, incluindo:

- ✓ Ficheiros de texto e documentos: Documentos do *Microsoft Office* (Word, Excel, PowerPoint), RTF e outros formatos de texto.
- ✓ Ficheiros multimédia: Imagens (JPEG, BMP, PNG, GIF), vídeos (AVI) e áudio (MP3, WAV).
- ✓ Ficheiros compactados: ZIP.
- ✓ Outros formatos: HTML, PDF.

4. Deteção e Remoção de Conteúdos Ativos

A ferramenta é especialmente eficaz na identificação e remoção de conteúdos ativos em ficheiros que possam comprometer a segurança. Exemplos incluem:

- ✓ HTML: JavaScript, VBScript, objetos como Flash e iFrames.
- ✓ PDF: JavaScript, ações de inicialização e ficheiros incorporados.
- ✓ Documentos do Office: Macros VBA, objetos de pacote OLE.
- ✓ RTF: Objetos de pacote OLE.

5. Interfaces Intuitivas

O *Exefilter* oferece duas opções de interface:

- ✓ Interface gráfica do utilizador (GUI): Ideal para utilizadores que preferem um ambiente visual interativo.
- ✓ Interface de linha de comando (CLI): Para utilizadores avançados que necessitam de maior controlo e automação.

6. Geração de Relatórios

- ✓ A ferramenta pode produzir relatórios detalhados nos formatos HTML e XML, fornecendo informações valiosas sobre os processos de filtragem e deteção.

7. Compatibilidade Multiplataforma

- ✓ O *Exefilter* é compatível com os seguintes sistemas operativos:
  - Windows;
  - GNU/Linux;
  - Mac OSX.

8. Licença de Código Aberto

- ✓ Disponibilizado sob uma licença *open source*, o *Exefilte*r promove a colaboração e a melhoria contínua pela comunidade de desenvolvedores.

9. Integração com Python API

- ✓ Para utilizadores e programadores que pretendem integrar ou personalizar o *Exefilter* em aplicações específicas, a ferramenta disponibiliza uma API em *Python.*

Com estas funcionalidades, o *Exefilter* posiciona-se como uma ferramenta essencial para organizações que necessitam de soluções eficazes e flexíveis para a gestão e segurança de ficheiros [67].

A ferramenta *Exefilter* apresenta diversas vantagens que a tornam uma solução robusta e eficiente para a proteção contra ameaças digitais e gestão de conteúdos. Entre as principais vantagens destacam-se:

- ✓ Proteção contra conteúdos ativos maliciosos: A ferramenta é eficaz na remoção de vírus, *worms* e cavalos de Troia, que frequentemente dependem de conteúdos ativos. Esses conteúdos maliciosos são propositadamente identificados e eliminados, minimizando o risco de infeções no sistema.
- ✓ Motor de filtragem genérico e de código aberto: O *Exefilter* utiliza um motor de filtragem genérico baseado em *software* de código aberto. Essa característica promove a transparência no funcionamento da ferramenta e também facilita a sua personalização e integração em diferentes sistemas, adaptando-se às necessidades específicas de cada utilizador ou organização.

- ✓ Remoção ativa de conteúdos e mitigação de ataques direcionados: A capacidade de remoção ativa de conteúdos potencialmente perigosos permite que o *Exefilter* atue como uma camada adicional de proteção contra ataques direcionados, garantindo maior segurança no tratamento e manuseio de dados.
- ✓ Correspondência rigorosa entre extensões de ficheiros e conteúdos: A ferramenta oferece um elevado grau de precisão na correspondência entre extensões de ficheiros e os seus conteúdos reais. Isso reduz significativamente a possibilidade de execução de ficheiros maliciosos disfarçados sob extensões aparentemente inofensivas.
- ✓ Filtragem baseada em listas brancas: Ao contrário da abordagem tradicional de filtragem por listas negras, o *Exefilter* adota uma estratégia de filtragem baseada em listas brancas. Este método limita a aceitação apenas a formatos de ficheiros previamente aprovados, proporcionando maior controle e segurança no processamento de dados. Esta abordagem é especialmente útil em ambientes corporativos onde a conformidade e a integridade dos dados são cruciais.
- ✓ A combinação dessas características posiciona o *Exefilter* como uma solução inovadora e eficaz no domínio da segurança digital, promovendo a proteção ativa e inteligente contra ameaças cibernéticas [68].

Embora a ferramenta *Exefilter* ofereça diversas vantagens no contexto da segurança digital, apresenta também algumas limitações que podem impactar a sua aplicação em determinados cenários. Estas desvantagens incluem:

- ✓ Necessidade de atualização constante dos filtros: Os formatos de ficheiros e métodos de exploração estão em constante evolução. Por isso, é necessário atualizar regularmente os filtros da ferramenta para acompanhar as mudanças e garantir que novas ameaças ou variantes de ficheiros maliciosos sejam detetadas e bloqueadas. Este processo exige recursos contínuos e pode ser moroso em ambientes com grandes volumes de dados.
- ✓ Impossibilidade de detetar todas as explorações desconhecidas: Apesar da sua eficácia, a ferramenta não é capaz de identificar todas as ameaças, especialmente aquelas que utilizam técnicas inéditas ou formatos totalmente novos. Essa limitação reflete um desafio comum em soluções de segurança baseadas em assinaturas ou listas pré-definidas, deixando o sistema vulnerável a ameaças de dia zero e explorações não documentadas.

- ✓ Dependência de *scripts* HTML e Flash em muitos *websites*: A filtragem rigorosa implementada pelo *Exefilter* pode ser problemática para utilizadores que precisam aceder a websites que utilizam *scripts* em HTML, Flash ou outras tecnologias interativas. A restrição desses conteúdos pode comprometer a funcionalidade esperada de algumas páginas web ou bloquear acessos necessários, reduzindo a eficiência e a produtividade dos utilizadores.
- ✓ Restrição para os utilizadores finais: A ferramenta é mais adequada para administradores de sistemas ou profissionais com conhecimentos técnicos, o que pode dificultar o seu uso por utilizadores finais com menos experiência. Essa barreira técnica pode limitar a adoção do *Exefilter* em ambientes onde a utilização por utilizadores comuns é uma necessidade.
- ✓ Essas desvantagens destacam a necessidade de avaliar cuidadosamente o uso do *Exefilter* em diferentes contextos, garantindo que as suas limitações sejam mitigadas por medidas complementares de segurança ou adaptações às necessidades específicas dos utilizadores [67].

4.4. Yara

A *Yara* é uma ferramenta de código aberto amplamente utilizada no domínio da cibersegurança para a análise e identificação de *malware.* Desenvolvida para facilitar a tarefa dos administradores de sistemas e investigadores de segurança, a *Yara* oferece uma linguagem poderosa e flexível para criar assinaturas de dados que permitem a classificação e identificação de amostras de *malware* com base em características específicas.

As regras *Yara* são o principal componente da ferramenta e permitem que os investigadores definam padrões específicos, como textos binários, padrões hexadecimais, *hashes* ou outras características observáveis em ficheiros ou processos suspeitos. Essas regras podem ser criadas para descrever detalhadamente famílias de *malware* e os seus comportamentos, permitindo uma análise detalhada e proativa.

Por exemplo, as regras podem ser utilizadas para:

- ✓ Identificar CVEs (*Common Vulnerabilities and Exposures*): As assinaturas podem ser criadas para detetar vulnerabilidades conhecidas em ficheiros ou sistemas.
- ✓ Reconhecer metodologias de ataques comuns: As regras ajudam a identificar padrões de ataques, como técnicas de *phishing, ransomware* ou injeções de código.

- ✓ Monitorizar atividades suspeitas: Os administradores podem usar *Yara* para detetar comportamentos incomuns em sistemas ou ficheiros, que podem ser indicativos de uma intrusão ou de *malware* ativo.

É bastante versátil e tem como benefícios:

- Linguagem flexível e poderosa: *Yara* permite a criação de regras complexas para descrever famílias de *malware* de forma precisa. A flexibilidade da linguagem também facilita a descrição de comportamentos e características detalhadas.
- Comunidade ativa e regras de código aberto: Existem diversas regras de *Yara* disponíveis publicamente, muitas delas criadas por especialistas em segurança. Essas regras oferecem uma visão abrangente sobre comportamentos maliciosos detetados em ficheiros e sistemas.
- Integração com outras ferramentas: A *Yara* pode ser integrada em sistemas de deteção de intrusões (IDS), soluções de antivírus, plataformas de resposta a incidentes e outras ferramentas de segurança.

Apesar de ser uma ferramenta poderosa, a eficácia da Yara depende diretamente da qualidade e manutenção das suas regras. Regras desatualizadas ou mal definidas podem levar a falsos positivos ou a falhas na deteção de ameaças recentes.

A Yara é uma ferramenta essencial para profissionais de segurança da informação que procuram soluções eficazes e detalhadas para a análise de *malware*. A sua capacidade de descrever comportamentos e características de *malware*, aliada a uma comunidade ativa que contribui com regras de qualidade, torna-a uma ferramenta indispensável na luta contra as ameaças cibernéticas [69] [70].

4.5. VirusTotal

VirusTotal é uma ferramenta online que foi criada em 2004 por uma equipe de desenvolvedores espanhóis e, atualmente é mantida pela empresa Google [91]. Esta ferramenta permite aos utilizadores verificar ficheiros e URLs potencialmente perigosos, identificando a presença de *malware* e conteúdos maliciosos através da utilização de múltiplos mecanismos de antivírus e serviços de análise de sites [92]. Além de suas funcionalidades intuitivas de análise, o serviço também oferece uma API robusta, permitindo que os desenvolvedores integrem as informações geradas pelo Vírus Total em suas próprias

aplicações e fluxos de trabalho, aumentando assim a segurança e proatividade na proteção contra ameaças digitais [71].

O VirusTotal se destaca como uma ferramenta essencial na identificação de ameaças virtuais, oferecendo uma combinação notável de eficácia, facilidade de uso e acesso a uma vasta base de dados que abrange informações de diversos fornecedores de segurança. Essas características fazem do VirusTotal uma escolha privilegiada tanto para profissionais de segurança cibernética quanto para utilizadores comuns que buscam proteger seus dispositivos e informações. A capacidade de integrar e analisar dados de múltiplas fontes é um ativo valioso no combate a um cenário de ameaças em constante evolução, consolidando a posição do VirusTotal como uma solução indispensável na defesa contra *malware* e outras vulnerabilidades digitais.

As principais características do VirusTotal são:

- ✓ Execute vários mecanismos antivírus.
- ✓ Atualizações automáticas de assinaturas de vírus em tempo real.
- ✓ Resultados detalhados de cada mecanismo antivírus.
- ✓ Estatísticas globais em tempo real.
- ✓ Automação de análise de API.
- ✓ Comunidade de pesquisa de *malware*

O funcionamento do VirusTotal permite que utilizadores identifiquem possíveis ameaças em ficheiros, PDFs e sites, oferecendo uma solução confiável para monitorar e proteger sistemas contra riscos cibernéticos.

Para utilizar o VirusTotal, o processo é simples e direto: o utilizador deve acessar o site e optar pela análise de ficheiro ou URL. No caso de ficheiros, a plataforma permite o upload direto, bem como o envio por *e-mail* para análise. Para avaliar URLs, basta inserir o endereço na caixa de texto e clicar em “Analisar”. Com essa abordagem intuitiva, o VirusTotal torna-se uma ferramenta acessível e eficaz para verificar a segurança de ficheiros e *links* na internet, contribuindo para a proteção contra ameaças cibernéticas, conforme ilustrado na figura 5.

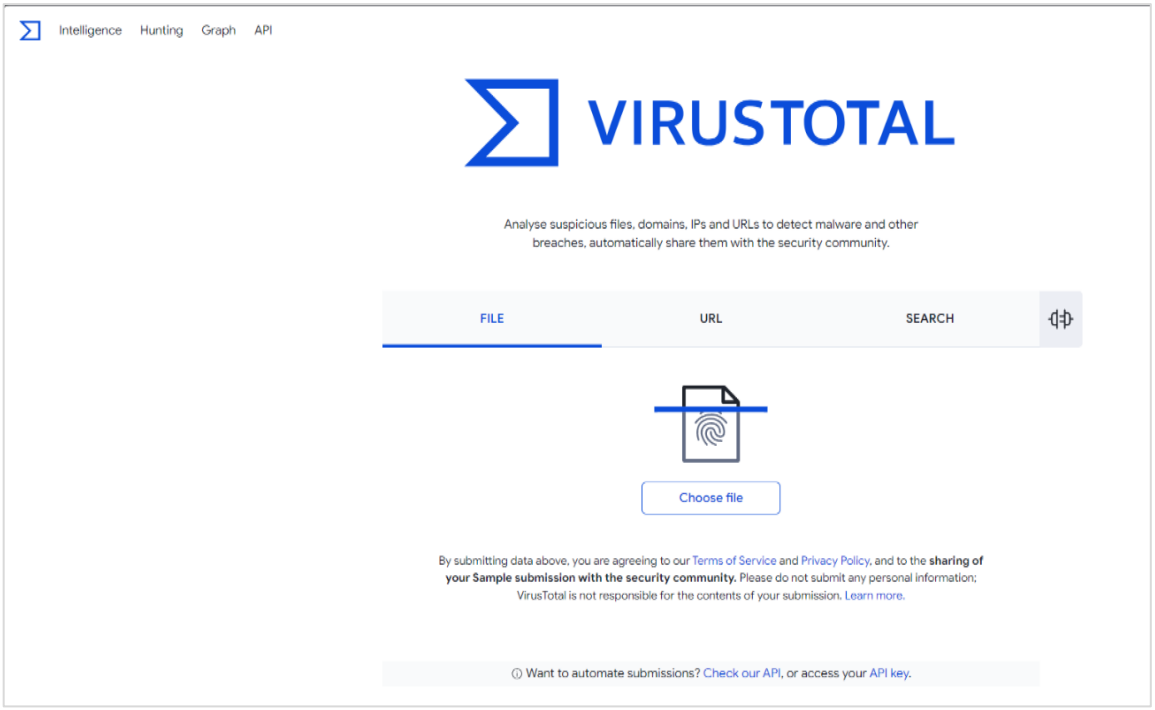


Figura 5- Interface de VirusTotal [71]

O VirusTotal se destaca como uma ferramenta essencial para a deteção de ameaças cibernéticas, oferecendo uma ampla cobertura de análise por meio da utilização de diversos mecanismos antivírus e ferramentas de deteção de *malware*. Sua capacidade de fornecer informações detalhadas sobre a reputação e os comportamentos de ficheiros e URLs permite que os utilizadores compreendam melhor as ameaças potenciais. A integração fácil com outras ferramentas de segurança e sistemas de gerenciamento a torna ainda mais útil em ambientes corporativos e de TI, otimizando a proteção contra riscos online. Além disso, o acesso gratuito à plataforma democratiza a segurança cibernética, permitindo que tanto indivíduos quanto organizações aprimorem suas defesas online, tornando o VirusTotal uma solução valiosa e acessível para todos os utilizadores.

Entretanto, o VirusTotal apesar de ser uma ferramenta útil para detetar ameaças cibernéticas, possui algumas desvantagens significativas que os utilizadores devem considerar. Sua dependência de bancos de dados de assinaturas pode limitar a sua capacidade de identificar novas e desconhecidas ameaças, enquanto a possibilidade de falsos positivos pode comprometer a confiabilidade dos resultados. Embora forneça análises detalhadas, o VirusTotal pode não ser suficiente por si só para análises avançadas de *malware*, demandando o uso de ferramentas suplementares para uma avaliação completa. Além disso, o envio de ficheiros para a plataforma levanta preocupações relacionadas à privacidade e confidencialidade dos dados, já que informações podem ser partilhadas com terceiros.

Portanto, é essencial que os utilizadores adotem uma abordagem cautelosa e considerem esses fatores ao utilizar o VirusTotal como parte de sua estratégia de segurança cibernética.

O VirusTotal oferece a capacidade de detetar uma ampla gama de ameaças à segurança de computadores, identificando diversos tipos de *malware*. Entre os componentes detetados estão vírus, *worms*, cavalos de tróia, *adware*, *spyware* e *ransomware*, cada um representando um método distinto de ataque cibernético. Os vírus replicam-se e infetam ficheiros, enquanto os *worms* se espalham sem a necessidade de infeção direta de outros ficheiros. Os cavalos de tróia enganam os utilizadores ao se disfarçarem como programas úteis, e o *adware* exibe anúncios indesejados. Por outro lado, o *spyware* coleta informações dos utilizadores sem consentimento, e o *ransomware* encripta dados, demandando pagamento para a recuperação.

Além de detetar diversos tipos de *malware*, também é capaz de identificar ameaças como *phishing*, *exploits* e vulnerabilidades. Sua análise detalhada é realizada por mais de 70 scanners antivírus e serviços de lista de bloqueio de URL e domínio, utilizando uma variedade de ferramentas para extrair sinais relevantes do conteúdo analisado. Essa multifuncionalidade torna o VirusTotal como uma ferramenta essencial na luta contra as ameaças cibernéticas, promovendo uma navegação online mais segura e protegida.

4.6.Metadefender Cloud (OPSWAT)

O *Metadefender Cloud* é uma ferramenta que permite examinar os ficheiros em busca de *malware* após a conclusão limpa o ficheiro eliminando todo o conteúdo malicioso e no final cria uma versão limpa e disponibiliza o ficheiro para *download*.

O *Metadefender* Cloud API fornece aos investigadores de *malware*, equipas de respostas a incidentes e fornecedores de tecnologia, APIs abrangentes para alavancar tecnologias avançadas de deteção e prevenção de ameaças [72].

A ferramenta se destaca como uma solução robusta e gratuita que permite aos utilizadores identificar e mitigar vulnerabilidades através da análise de múltiplos motores antivírus e tecnologias avançadas de deteção de ameaças. Com sua capacidade de oferecer uma deteção precisa e eficaz de *malware*, a plataforma não apenas assegura a integridade dos dados dos utilizadores, mas também contribui significativamente para a proteção de dispositivos contra ciberataques.

Para iniciar o *scan* do ficheiro com o *Metadefender Cloud,* o utilizador tem de selecionar o "Deep CDR" no menu de análise, seguidamente selecionar o ficheiro pretendido e clicar em processo, conforme ilustrado na figura 6.

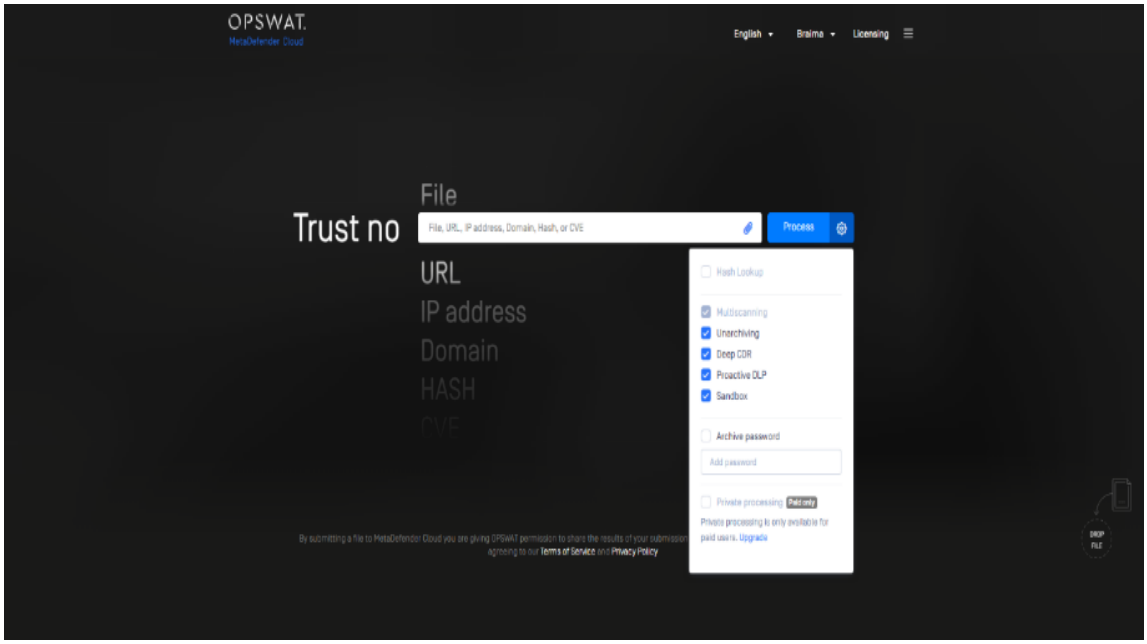


Figura 6- Interface de Metadefender Cloud

O *MetaDefender Cloud* destaca-se no domínio da segurança cibernética ao empregar vários mecanismos de verificação para a deteção de ameaças, ao contrário da abordagem tradicional que se concentra num único mecanismo antivírus. Esta estratégia multifacetada não só aumenta a probabilidade de identificar ficheiros potencialmente perigosos, como também se complementa com a tecnologia de *sandboxing,* que analisa ficheiros suspeitos num ambiente seguro e isolado. Como resultado, o *MetaDefender Cloud* oferece uma proteção aprimorada, conseguindo identificar ameaças que outros programas antivírus podem inadvertidamente ignorar. Esta combinação de verificações abrangentes e ambientes seguros demonstra a eficácia do *MetaDefender Cloud* na proteção contra ameaças cibernéticas.

O *MetaDefender Cloud* combina várias características que reforçam a proteção contra ameaças digitais. A sua abordagem de proteção multimecanismo permite a deteção de ameaças por meio de múltiplas verificações, ao passo que a tecnologia de *sandboxing* garante que ficheiros suspeitos sejam analisados num ambiente controlado e seguro. Além disso, o sistema consegue identificar vulnerabilidades em dispositivos e sistemas, evitando possíveis explorações por cibercriminosos. Outro aspeto importante é a funcionalidade de desinfeção de ficheiros, que trata e elimina infeções por vírus e outras ameaças. Por fim, a integração fluida com outras soluções de segurança e ferramentas de gestão de TI torna o

MetaDefender Cloud uma escolha eficaz para reforçar as defesas cibernéticas de qualquer organização.

A *MetaDefender Cloud* representa um avanço significativo na deteção e segurança de ficheiros, utilizando a tecnologia *Deep Content Disarm and Reconstruction* (Deep CDR) para proteger os ambientes contra explorações de dia zero que possam ser introduzidas através de ficheiros. Este processo desarma e reconstrói documentos, garantindo que apenas o conteúdo seguro criado pelo utilizador é mantido, ao mesmo tempo que elimina potenciais ameaças, como macros, *JavaScript* e ligações maliciosas. Com esta abordagem inovadora, a *MetaDefender Cloud* não só reforça as defesas de cibersegurança, como também adiciona uma camada de proteção, promovendo um ambiente digital mais seguro e confiável [93].

4.7. Glasswall CDR

A *Glasswall Halo* [98] é uma ferramenta desenvolvida pela empresa *Glasswall* que utiliza a tecnologia CDR para oferecer uma proteção contra ficheiros maliciosos, adotando uma abordagem de confiança zero. Isso significa que apenas os ficheiros que foram verificados e limpos pela plataforma são considerados seguros, efetivamente eliminando qualquer ameaça antes que possa afetar os sistemas empresariais. Ao implementar a *Glasswall*, as organizações podem fortalecer a sua defesa cibernética, garantir a integridade dos seus dados e proteger-se contra ficheiros maliciosos.

A *Glasswall* apresenta 4 etapas para proteger agências governamentais e empresas contra ameaças baseadas em ficheiros infetados:

- ✓ Inspeção: O ficheiro é dividido nos seus componentes constituintes, e a estrutura dos ficheiros é validada em relação à sua especificação.
- ✓ Reconstrução: Nesta etapa, as estruturas desconhecidas ou inválidas do ficheiro são reparadas de acordo com a especificação definida para o tipo de ficheiro em questão.
- ✓ Limpeza: Elimina estruturas de ficheiros consideradas de alto risco, especialmente aquelas que contêm conteúdos ativos, seguindo as políticas de segurança configuradas.
- ✓ Entrega: Na fase final, são realizadas verificações semânticas no documento, assegurando a integridade visual e garantindo a usabilidade do ficheiro [73].

Em resumo, a *Glasswall Halo* foi concebida para fornecer às organizações uma defesa robusta contra ameaças baseadas em ficheiros. Ao combinar a regeneração de ficheiros,

a inspeção profunda de ficheiros e a integração de inteligência de ameaças, a *Glasswall* oferece uma solução abrangente que ajuda as organizações a proteger os seus dados sensíveis e a manter uma postura de segurança forte perante a evolução das ameaças cibernéticas.

4.8. Votiro

A Votiro é uma ferramenta desenvolvida pela empresa votiro que utiliza a tecnologia CDR, permitindo que todas as empresas estejam seguras contra-ataques de dia zero e não revelado [74]. A tecnologia CDR da votiro permite identificar *malware,* desarmar e reconstruir o ficheiro mantendo a integridade e a funcionalidade do ficheiro garantindo que o ficheiro esteja 100% seguro [75].

A Votiro protege as empresas contra todas as tentativas de exploração de ficheiros, incluindo ataques realizados através de *e-mail*, partilha de ficheiros e *downloads* na web. A solução implementa um mecanismo de segurança de múltiplas camadas, integrando vários componentes para eliminar ameaças cibernéticas que tentam infiltrar-se numa empresa ou organização [75].

4.9. ODIX

A *Odix* é uma ferramenta desenvolvida pela empresa Odix, que utiliza tecnologias avançadas como *Deep Files Analaysi*s (DFA) e TrueCDR^{TM} para proteger ficheiros contra-ataques baseados em ficheiros maliciosos. Diferente dos métodos antivírus e *sandbox* que verificam ameaças, detetam e bloqueiam um subconjunto de *malware*. O processo principal de CDR concentra-se na validação da estrutura dos ficheiros no nível binário. Esse processo permite neutralizar tanto ameaças conhecidas assim como desconhecidas, incluindo *malwares* de dia zero, garantindo que o utilizador receba uma cópia segura do ficheiro original infetado [76].

O DFA complementa esta abordagem ao tratar cada ficheiro como um "iceberg": embora possa parecer inofensivo à superfície, o processo examina profundamente o conteúdo interno para detetar e eliminar *malware* incorporado. Esta análise vai além das capacidades das soluções tradicionais, como as ferramentas ligadas da *Microsoft.*

O processo de análise de ficheiros na Odix envolve quatro etapas principais:

- ✓ Aplicação das Políticas: As políticas de segurança são aplicadas para determinar quais ações tomar com base nas características do ficheiro e nas configurações da organização.

✓ Verificação de Antivírus: Apesar de complementar a abordagem de CDR, a verificação de antivírus garante uma camada adicional de proteção ao identificar padrões de ameaças conhecidas.

✓ Validação do Tipo de Ficheiros: Verifica se o tipo de ficheiro corresponde à sua estrutura e especificação, identificando potenciais anomalias.

✓ TrueCDR^{TM}: Este método desarma conteúdos maliciosos e reconstrói o ficheiro, preservando sua integridade e usabilidade para o utilizador.

Combinando o DFA e o TrueCDR^{TM}, a Odix oferece uma solução robusta e eficaz para proteger as organizações contra ameaças cibernéticas baseadas em ficheiros, garantindo segurança sem comprometer a produtividade, conforme ilustrado na figura 7.

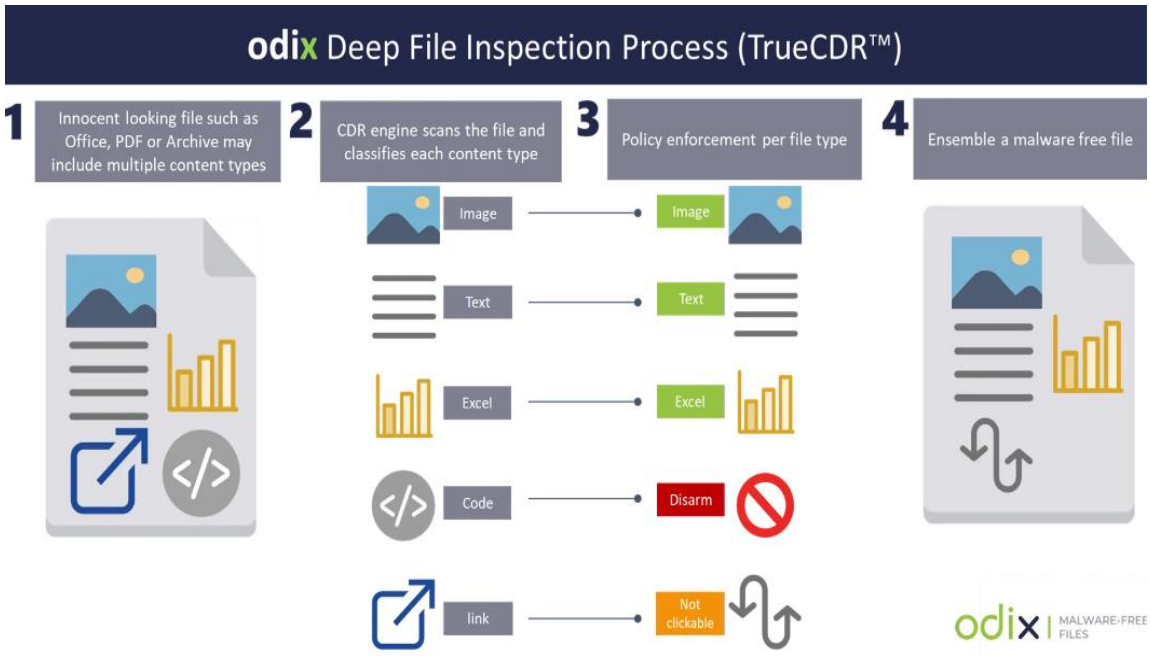


Figura 7- Funcionamento de ODIX [76]

4.10. GateScanner

GateScanner é uma ferramenta desenvolvida pela empresa *Sasa Software* [77]. O principal produto da empresa, é amplamente utilizado por empresas para se defenderem contra ameaças baseadas em ficheiros. Esta tecnologia parte do princípio de que todos os ficheiros devem ser tratados como suspeitos, realizando um processo rigoroso de desarmamento e reconstrução. Durante este processo, o *GateScanner* elimina *malwares* conhecidos e desconhecidos, incluindo ameaças de dia zero, *ransomware* e ataques avançados e persistentes, independentemente de terem ou não assinatura.

Os ficheiros processados pelo *GateScanner* são transformados em cópias seguras, neutralizadas e confiáveis, eliminando ameaças indetetáveis e preservando a total usabilidade e funcionalidade dos documentos originais. Este método garante que as organizações possam utilizar os ficheiros sem comprometer a segurança dos seus sistemas [78]. A eficácia desta abordagem pode ser visualizada na figura 8.

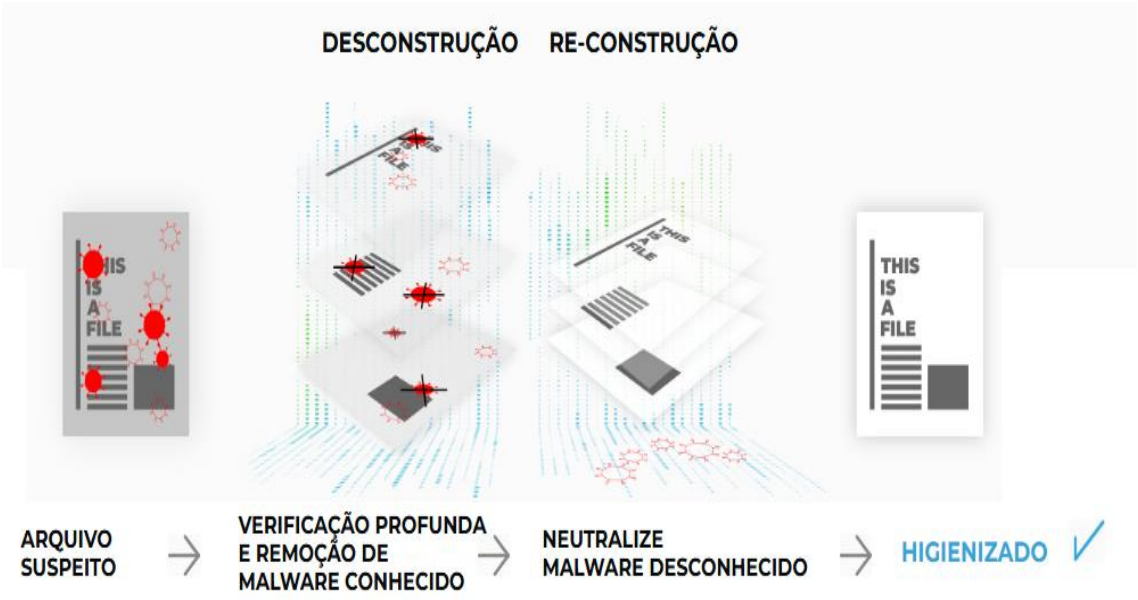


Figura 8- Funcionamento de *GateScanner* [85]

4.11. Comparação das soluções CDR

A tabela 5 apresenta uma análise comparativa de várias aplicações CDR, destacando os custos, a disponibilidade de código aberto, suporte a relatórios de análise, características principais do sistema e as plataformas suportadas. Estas ferramentas desempenham um papel crucial na proteção contra ficheiros maliciosos, utilizando técnicas de desarmamento e reconstrução para eliminar ameaças cibernéticas. Abaixo, descreve-se brevemente cada ferramenta e suas características:

Aplicações CDR	Custo	Código Aberto	Relatório de Analise	Características do sistema	Plataformas
Dockbleach	Gratuito	Sim	Não	✓ Desarme e Reconstrução de Conteúdos; ✓ Detecta ameaças conhecidas ✓ Não detecta ameaças do dia zero ✓ Ficheiros Suportados: Documentos de Microsoft Office, PDF, RTF	✓ Linux ✓ Windows
Oletools	Gratuito	Sim	Não	✓ Opções para digitalizar vários ficheiros ✓ Saída CVS ✓ Opções para verificar ficheiros de ficheiros ZIP encriptados ✓ Extração e analise de código-fonte ✓ Detecção de palavras-chave suspeitas tipicamente utilizadas em *malware* ✓ Detecção de macro autoexecutável	✓ Windows ✓ Linux

Aplicações CDR	Custo	Código Aberto	Relatório de Analise	Características do sistema	Plataformas
				✓ Ficheiros Suportado: Ficheiro OLE, OpenXML	
Exefilter	Gratuito	Sim	Sim	✓ Desarme e Reconstrução de Conteúdos; ✓ Filtra ficheiros de acordo com a política definida; ✓ Pode detectar, remover conteúdos activos em alguns formatos: HTML, PDF, Word; Excel, RTF	✓ Windows ✓ GNU/Linux ✓ MAC
Yara	Gratuito	Sim	Não	✓ Identificar CVEs (*Common Vulnerabilities and Exposures*); ✓ Reconhecer metodologias de ataques comuns; ✓ Monitorizar atividades suspeitas	✓ Linux ✓ Windows
VirusTotal	Gratuito	Sim	Sim	✓ Execute vários mecanismos antivírus. ✓ Atualizações automáticas de assinaturas de vírus em tempo real. ✓ Resultados detalhados de cada mecanismo antivírus. ✓ Estatísticas globais em tempo real. ✓ Automação de análise de API.	✓ MacOS ✓ Windows ✓ Linux

Aplicações CDR	Custo	Código Aberto	Relatório de Analise	Características do sistema	Plataformas
				✓ Comunidade de pesquisa de malware	
OPSWAT (Metadefender Cloud)	✓ Pago ✓ Versão Gratuita	Não	Sim	✓ Desarme e Reconstrução de Conteúdos ✓ Analise comportamentais; ✓ Gerenciamento de Endpoint; ✓ Análise de Vulnerabilidades ✓ Analise de *Malware*; ✓ Gerenciamento de *Patches*; ✓ Scan ✓ Ficheiros Suportados: PDF, RTF, Documentos do Microsoft, TXT, HTML, EXE, JPEG, PNG, XML	✓ Saas ✓ Windows
Glasswall	✓ Pago ✓ Versão Gratuita	Não	Não	✓ Desarme e Reconstrução de conteúdos ✓ Segurança de E-mail	✓ Windows
Votiro	✓ Pago ✓ Versão Gratuita	Não	Sim	✓ Desarme e Reconstrução de Conteúdos ✓ Segurança Informática; ✓ Gateway de e-mail seguro	✓ SaaS ✓ Windows; ✓ Mac
GateScanner	✓ Pago ✓ Versão Gratuito	Não	Sim	✓ Desarme e Reconstrução de Conteúdos; ✓ Segurança de Redes	✓ SaaS ✓ Windows ✓ No Local
Odix (FileWall)	✓ Pago; ✓ Versão Gratuito	Não	Sim	✓ Desarme e Reconstrução de Conteúdos; ✓ Segurança Cibernética; ✓ Segurança de E-mail;	✓ SaaS; ✓ Windows

Aplicações CDR	Custo	Código Aberto	Relatório de Analise	Características do sistema	Plataformas
				✓ Analise de *Malware* ✓ NSPM (Network Security Policy Management) ✓ Analise de Malware;	

Tabela 5- Tabela comparativa dos sistemas CDR

5. Testes e Análise dos Resultados Obtidos

Após a pesquisa de soluções *open source* e de aplicações gratuitas disponíveis, foi identificado o *MetaDefender Cloud*, desenvolvido pela empresa OPSWAT, como uma alternativa viável para este trabalho. Esta aplicação, baseada na tecnologia OPSWAT Deep CDR, disponibiliza um plano gratuito adequado à carga de testes prevista, embora apresente algumas limitações em cenários de utilização mais intensiva, incluindo restrições específicas. Para aceder a esse plano, é necessário criar uma conta na plataforma OPSWAT e, caso se verifique a necessidade de ultrapassar os limites estabelecidos, existem opções de subscrição facilmente integráveis. Deste modo, estão reunidas as condições para iniciar os testes com o *MetaDefender Cloud*, tirando partido das suas capacidades de proteção e análise.

Para validar a eficácia dessa aplicação, utilizou-se a plataforma VirusTotal como metodologia de suporte, o que permitiu avaliar de forma mais concreta se a ferramenta realmente elimina fontes maliciosas de maneira eficaz. Após a obtenção dos resultados, foi realizada uma análise detalhada dos dados provenientes dos testes, com o objetivo de oferecer uma avaliação crítica sobre o desempenho da aplicação testada e a sua capacidade de contribuir para um ambiente digital mais seguro.

Inicialmente, foi realizada uma análise detalhada de seis ficheiros distintos, incluindo formatos como PDF, HTML, RTF, DOC e XLS, com o objetivo de detetar e neutralizar potenciais ameaças de natureza cibernética. A tabela 6 apresenta informações detalhada sobre cada ficheiro analisado.

Nome dos Ficheiros	Formato	Hash	Tamanho do ficheiro	Conteúdo
EmbeddedFile HTML.pdf	.pdf	Sha 256: 73fb9d94156c360334fc28cfa1ab6639f4f5d1e675734f5f200ad028dc66007c	2.07 KB	JavaScript Embutido
Form W4-2016.pdf	.pdf	Sha 256: 225411b1b24709b4de40678e05ad591b343467c0b84ee0c0cd27c331126bb7db	105.97 KB	Campos de Formulário

Nome dos Ficheiros	Formato	Hash	Tamanho do ficheiro	Conteúdo
HTML Javascript obfuscated.html	.html	Sha 256: b71ebf3c71bf7695e41f6a6a0498d651023c1dc705b6aa4b0fef1ae9bcfecf4d	769 B	Hiperlinks
RTF OLE Package EXE.rtf	.rtf	Sha 256: 71cd5900a9d83d03d04ef6bc4f0b1a13b828e5cf519239115ceb92094aa61727	148.59 KB	Contém um ficheiro executável dentro de um objeto OLE
eicar-word-macro-cmd-echo.doc	.doc	Sha 256: 03d0985601b7b6e75036b48b9f835bf8b3d664a894f74e80b761627f4cd69749	32.50 KB	Objeto Macro
eicar-excel-macro-write-file.xls	.xls	Sha 256: 4e9f51d537e9bff3b502afdb117148dd2e52eaa1546df13996808c33601a091	31 KB	Objeto Macro

Tabela 6- Informações detalha dos ficheiros analisados

Os testes começaram com a utilização do VirusTotal para identificar a presença de códigos maliciosos, seguido pela aplicação da ferramenta *Metadefender Cloud* que não só analisou, bem como, desarmou e reconstruiu os conteúdos suspeitos, garantindo a remoção de quaisquer elementos maliciosos. Após este processo, os ficheiros tratados foram novamente submetidos ao VirusTotal, com o objetivo de confirmar que estavam limpos e livres de ameaças. Finalmente, os resultados das análises foram avaliados de forma detalhada para verificar a eficácia das ferramentas utilizadas e assegurar a integridade e segurança dos ficheiros processados, demonstrando a relevância das práticas de segurança digital na proteção contra ameaças cibernéticas.

5.1. Exemplo1- análise do ficheiro *PDF EmbeddedFile HTML.PDF*

O VirusTotal utiliza múltiplos motores antivírus para analisar os ficheiros de forma abrangente. Durante a análise do ficheiro EmbeddedFile HTML.pdf, verificou-se que, embora o formato PDF seja amplamente utilizado para a partilha de documentos, também tem sido frequentemente explorado para ocultar código malicioso, objetos ativos ou *hiperlinks* maliciosos. Com 60 análises realizadas, por múltiplos motores antivírus, por intermédio do VirusTotal, 10 deles designadamente os antivírus *Baidu, Kaspersky, McAfee, SentinetOne (Static ML), Xcitium, Gridinsoft (no Cloud), Kingsoft, NANO-Antivírus, Skyhigh (SWG)* e *ZoneAlarmbyCheckPoint* identificaram potenciais ameaças, conforme ilustrado na tabela 7. Os restantes, não sinalizaram comportamentos suspeitos, como ilustrado na figura 9. É relevante destacar que este ficheiro PDF continha *JavaScript* embutido, uma funcionalidade que, apesar de legítima em determinados contextos, pode ser explorada para fins maliciosos, aumentando o risco de segurança.

Além disso, foi identificada a presença da fonte Adobe Typo 1, um formato amplamente utilizado em aplicações de imagem digital. Embora não seja intrinsecamente malicioso, o uso dessa fonte em ficheiros manipulados pode levantar preocupações em contextos específicos. Adicionalmente, a análise revelou a presença de um processo associado a um navegador baseado no Chrome, identificado como um sequestrador de navegador generalizado. Este tipo de *malware* altera as definições do navegador da vítima e redireciona o tráfego para sites de publicidade. A infeção é geralmente introduzida através de um ficheiro ISO, que induz o utilizador a executá-lo ao disfarçar-se como um videojogo crackeado ou um filme pirateado. Posteriormente, o *malware* manifesta-se sob a forma de uma extensão do navegador. Este comportamento, ilustrado na figura 9, sugere que o ficheiro poderia estar associado a uma tentativa de execução de *scripts* ou extensões não autorizadas, o que reforça a necessidade de atenção redobrada.

Esta análise demonstra como elementos aparentemente inofensivos, como *JavaScript* embutido ou extensões personalizadas, podem ser explorados em ficheiros para ações potencialmente maliciosas, sublinhando a importância de uma inspeção detalhada em cada fase do processo de validação.

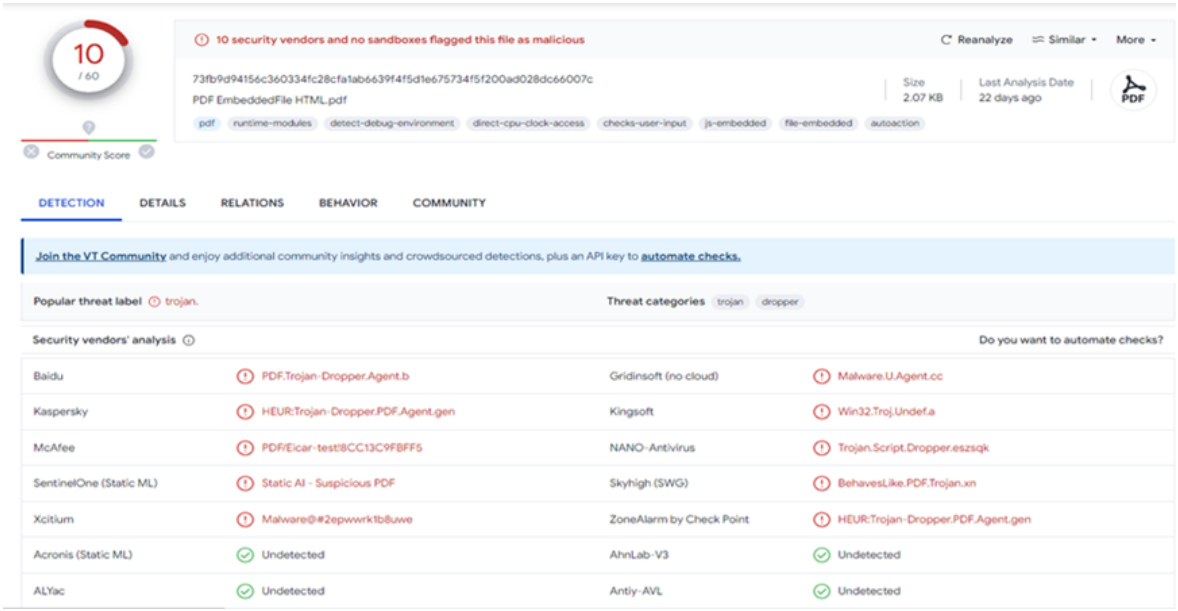


Figura 9- Resultado da análise do ficheiro "PDF EmbeddedFile HTML.pdf" através do VirusTotal

Antivírus	Ameaças Detetadas
Baidu	PDF.Trojan-Dropper.Agent.b
Kaspersky	HEUR:Trojan- Dropper.Agent.gen
McAfee	PDF/Eicar-test!8CC13C9FBFF5
SentinetOne (Static ML)	Static Al-Suspicious PDF
Xcitium	Malware@#2epwwrk1b8uwe
Gridinsoft (no Cloud)	Malware.U.Agent.cc
Kingsoft	Win32.Troj.Undef.a
NANO-Antivírus	Trojan.Script.Dropper.eszsqk
Skyhigh (SWG)	BehavesLike.PDF.Swrot.xn
ZoneAlarmbyCheckPoint	HEUR:Trojan-Dropper.PDF.Agent.gen

Tabela 7- Ameaças detetadas por diferentes motores antívirus através de VirusTotal

Conforme ilustrado na tabela 7, a análise das ameaças identificadas por diferentes soluções antivírus através de VirusTotal, revela a complexidade e sofisticação dos ataques

cibernéticos atuais, destacando a importância da vigilância contínua e da atualização das defesas de segurança. O antivírus Baidu expôs o *PDF.Trojan-Dropper.Agent.b*, que utiliza métodos enganosos para inserir *malware* em documentos PDF, colocando em risco a integridade dos dados dos utilizadores. A ameaça *HEUR:Trojan-Dropper.Agent.gen*, identificada pelo *Kaspersky*, demonstra um alto nível de complexidade ao comprometer sistemas e facilitar atividades ilícitas. Por sua vez, o *McAfee* destaca a utilidade do ficheiro de teste EICAR como uma ferramenta essencial para a avaliação da eficácia das medidas de segurança implementadas. O SentinelOne identificou um ficheiro PDF suspeito, potencialmente portador de conteúdos maliciosos, enquanto o Xcitium e o Kingsoft detetaram malware concebido para explorar vulnerabilidades específicas, evidenciando a capacidade dos cibercriminosos para manipular plataformas digitais de forma sofisticada. Além disso, foi identificado um *Trojan* pelo NANO-Antivírus que se disfarça como software legítimo para infiltrar-se nos sistemas e potencialmente roubar informações sensíveis. Já o *Skyhigh* destacou um perigo adicional, com PDFs maliciosos que enganam os utilizadores para abrir arquivos comprometidos. Diante dessas ameaças, é imperativo que as organizações implementem medidas de segurança robustas, como atualizações constantes, formação de utilizadores e planos eficazes de resposta a incidentes, para mitigar os riscos apresentados por estas entidades maliciosas e proteger a integridade dos dados.

Na figura 10 é apresentado o resultado da análise do ficheiro *EmbeddedFile HTML.pdf* utilizando a ferramenta Metadefender Cloud. Como evidenciado pelos dados, foram identificadas a presença de cinco (5) ameaças positivas em 24 análises realizadas consecutivamente por diferentes antivírus incorporados no Metadefender Cloud, com um tempo de análise de apenas 3 segundos. Durante o processo, o ficheiro foi desarmado e reconstruído, resultando na eliminação de dois (2) objetos de *JavaScript* embutidos no ficheiro, que representavam potenciais riscos de segurança. Os resultados destacam a eficácia da ferramenta Metadefender Cloud na deteção de ameaças e na mitigação de riscos associados a ficheiros potencialmente perigosos.

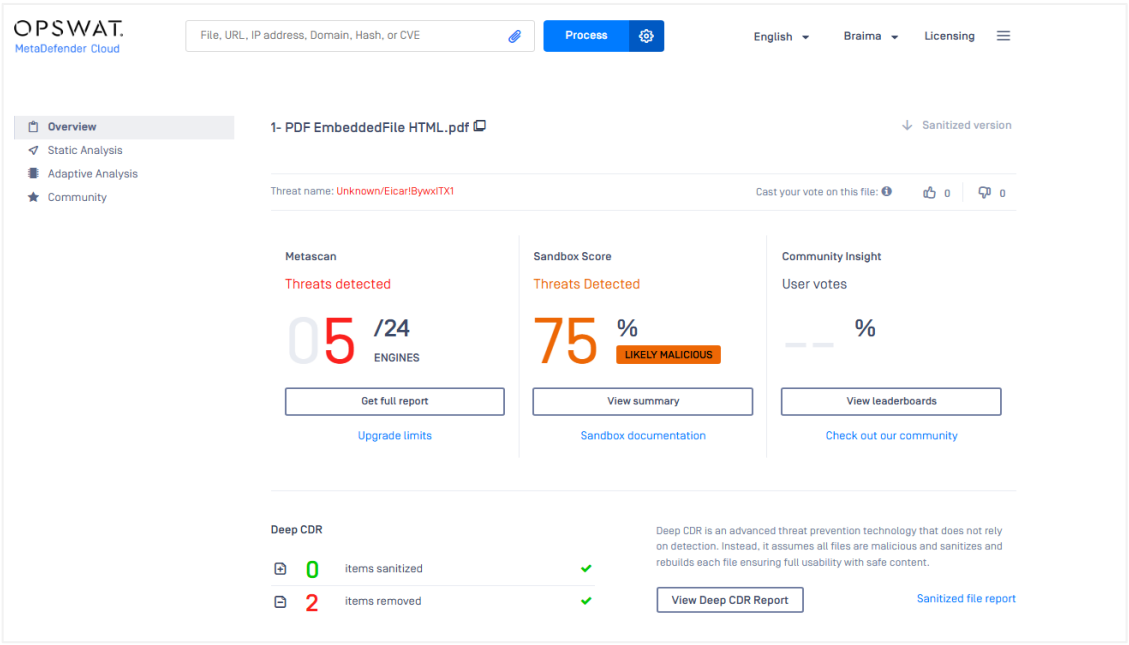


Figura 10- Resultado da análise do ficheiro "PDF EmbeddedFile HTML.pdf" através de Metadefender Cloud

Após o desarmamento, o ficheiro foi novamente submetido ao VirusTotal para uma nova análise, com o objetivo de verificar a sua limpeza e assegurar que estava completamente isento de quaisquer ameaças. Este procedimento reforça a eficácia da utilização de ferramentas especializadas, garantindo a segurança e a integridade do ficheiro tratado. Uma abordagem que se alinha com as teorias de autores como Ran Dubin [33], que destacam a sinergia entre tecnologias na mitigação de riscos. A combinação de diferentes ferramentas não apenas reforça a eficácia dos processos, mas também assegura que os dados manipulados permaneçam protegidos contra ameaças.

5.2.Exemplo 2: análise do ficheiro Form W4-2016.pdf

O ficheiro Form W4-2016.pdf foi submetido ao VirusTotal, onde foi analisado por 60 motores de antivírus distintos, não tendo sido identificada qualquer ameaça associada. Este resultado indica que o documento está livre de conteúdos maliciosos, reforçando a sua segurança e integridade para futuros usos, conforme ilustrado na figura 11.

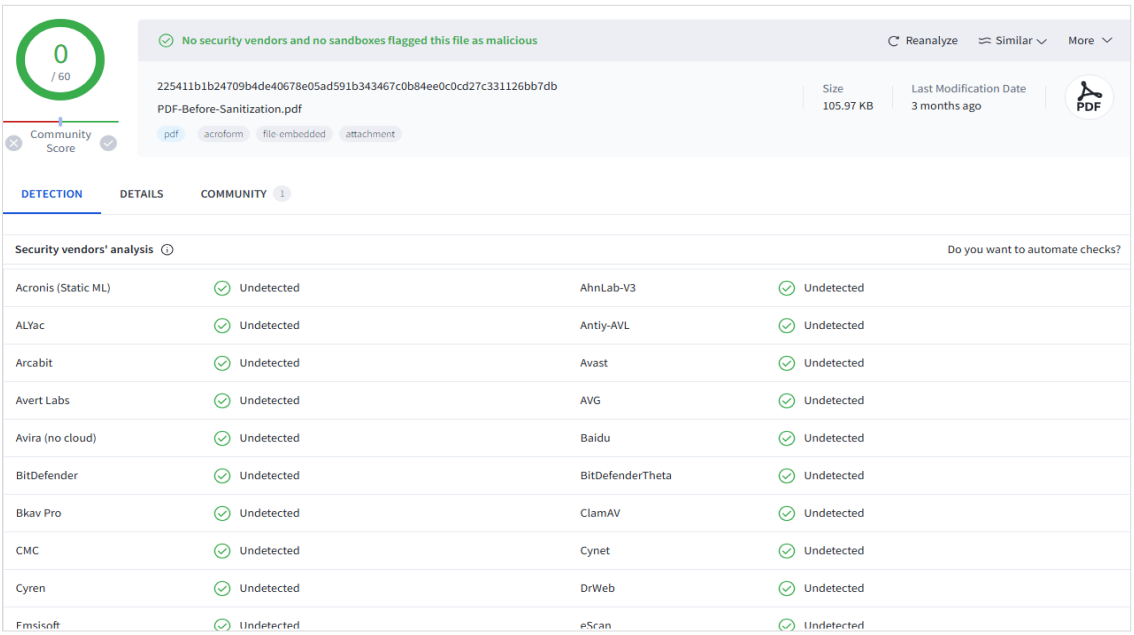


Figura 11- Resultado da análise do ficheiro "Form W4-2016.pdf" atráves do VirusTotal

Na Figura 12 é ilustrado o processo de análise do ficheiro Form W4-2016.pdf recorrendo à ferramenta Metadefender Cloud, a qual utilizou 24 motores de antivírus para identificar potenciais ameaças. Os resultados não evidenciaram qualquer atividade maliciosa, sugerindo que o ficheiro estava isento de componentes nocivos. No entanto, como medida adicional de segurança, o ficheiro foi sujeito a um processo de desarmamento (CDR), durante o qual foram removidos 56 elementos, incluindo 42 campos de formulário e 14 objetos não utilizados. Esta etapa é fundamental na área da cibersegurança, dado que elementos redundantes ou inativos podem constituir vetores de ataque, mesmo em documentos aparentemente inofensivos. Assim, o processo de desarmamento não só eliminou potenciais vulnerabilidades, como também mitigou de forma significativa a possibilidade de exploração de pontos de entrada por parte de um agente malicioso.

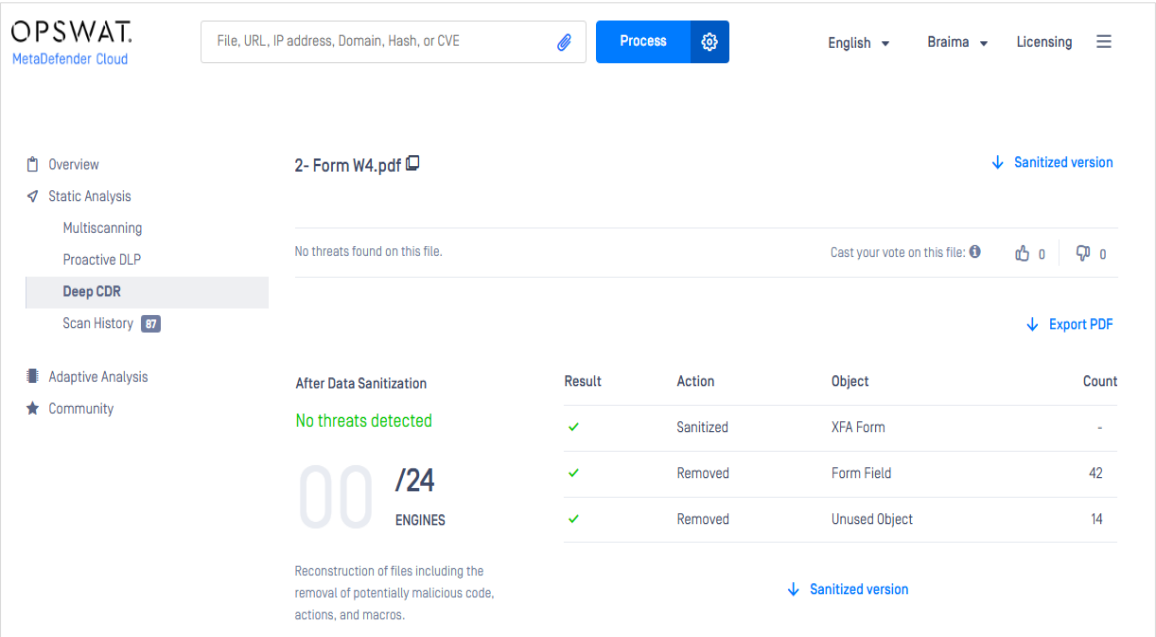


Figura 12- Resultado do ficheiro "Form W4-2016.pdf" através de Metadefender Cloud

Após o desarmamento, o ficheiro foi submetido novamente para análise no VirusTotal e no Metadefender Cloud, para validar a eficácia do processo e garantir que o ficheiro estava completamente limpo e livre de ameaças. Este procedimento reforça a importância da utilização das ferramentas de CDR, permitindo não apenas a identificação de ameaças conhecidas, mas também a mitigação de riscos associados a componentes potencialmente perigosos que podem não ser detetados em análises iniciais, conforme ilustrado nas figuras 23, 24 e 25 do anexo B.

5.3.Exemplo 3: análise do ficheiro HTML Javascript obfuscated.html

Na figura 13 é ilustrado o resultado obtido com a submissão do ficheiro *HTML Javascript obfuscated.html* para análise no VirusTotal. Foram realizadas 46 análises com diferentes motores de antivírus, não tendo sido detetada qualquer ameaça no ficheiro.

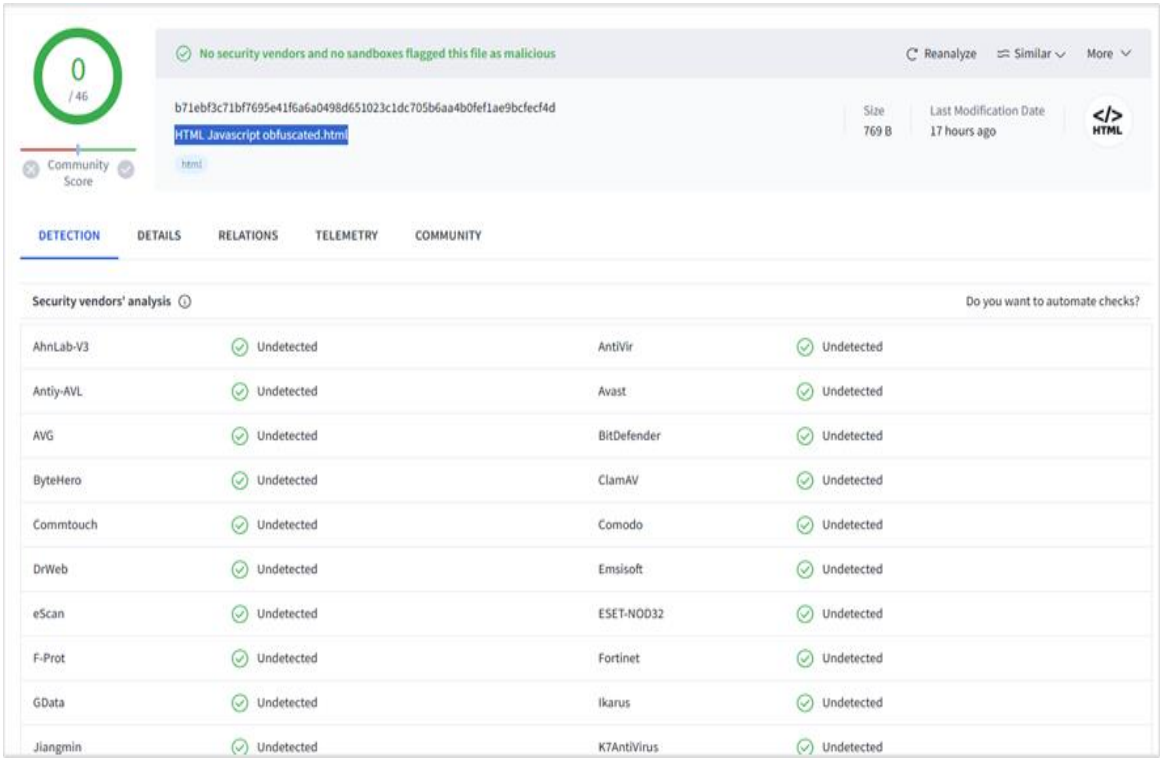


Figura 13- Resultado da análise do ficheiro "HTML JavascriptObfuscated.htm" atráves de VirusTotal

Na Figura 14 é apresentado o resultado da análise ao ficheiro HTML *Javascript obfuscated.html* através da ferramenta Metadefender Cloud. Durante o processo, foram realizadas 24 análises com diferentes motores de antivírus. Embora não tenha sido detetada qualquer ameaça por esses motores, a análise identificou a presença de três (3) *hiperlinks* incorporados no ficheiro. Apesar de não apresentarem, à partida, um comportamento explicitamente malicioso, os *hiperlinks* em ficheiros HTML representam potenciais vetores de ataque, especialmente quando associados a conteúdos externos ou a técnicas de ofuscação de código, práticas frequentemente utilizadas por cibercriminosos para ocultar atividades maliciosas.

Como medida preventiva, o ficheiro foi submetido a um processo de desarmamento e reconstrução, que resultou na remoção completa dos três *hiperlinks* identificados. Este procedimento contribui significativamente para a mitigação do risco de exploração futura, ao eliminar possíveis canais de ligação com conteúdos externos ou não autorizados. Apesar de esta ação ter implicado a perda de algumas funcionalidades do ficheiro, nomeadamente a desativação dos *hiperlinks*, tal compromisso é considerado aceitável face ao reforço da segurança global do documento.

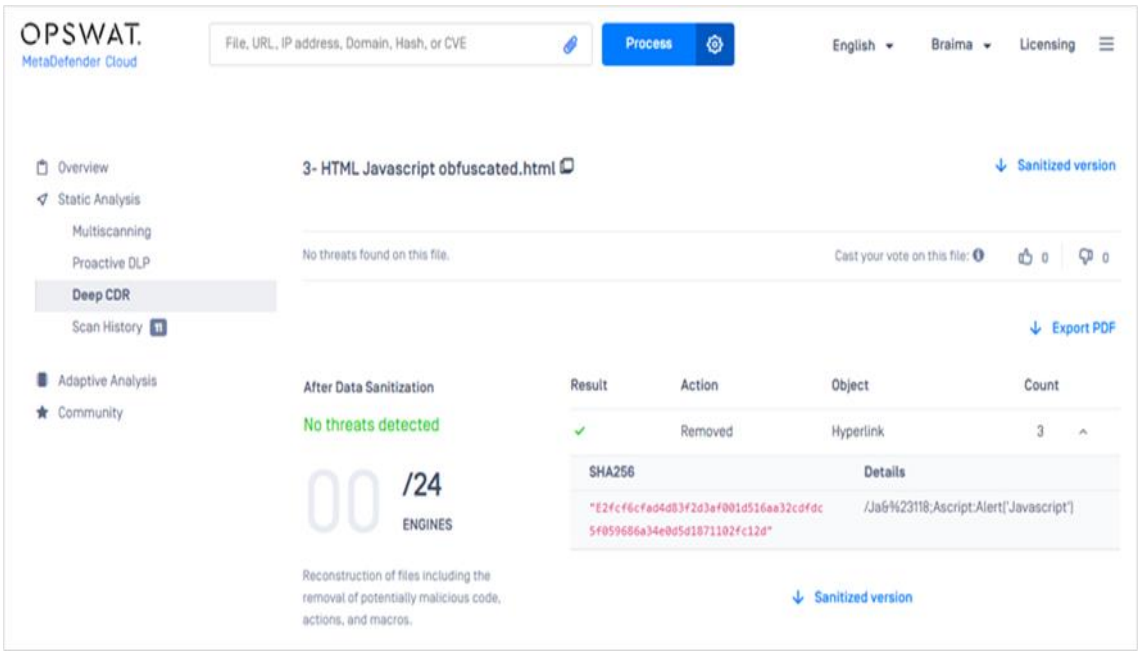


Figura 14- Resultado da análise do ficheiro "HTML Javascript Obfuscadet.html" através de Metadefender

Após o desarmamento, o ficheiro foi novamente analisado no *VirusTotal* e no Metadefender Cloud, com o objetivo de confirmar a eficácia das ações corretivas implementadas e assegurar que o ficheiro estava isento de quaisquer ameaças. Os resultados das análises pós-tratamento, validaram que o ficheiro reconstruído estava limpo e livre de componentes que pudessem comprometer a segurança, conforme ilustrado nas figuras 27, 28 e 29 do anexo C.

Este processo sublinha a importância de uma abordagem pró-ativa na gestão de ficheiros potencialmente inseguros, utilizando ferramentas avançadas para identificar e neutralizar riscos, mesmo quando as análises iniciais não indicam comportamentos maliciosos explícitos. A eliminação de *hiperlinks*, que costumam ser um dos pontos de vulnerabilidade, contribui significativamente para a segurança e integridade dos sistemas da organização, evidenciando a necessidade de protocolos rigorosos na análise e tratamento de ficheiros.

5.4. Exemplo 4: análise do ficheiro RTF OLE Package EXE.rtf

Na figura 15, é apresentado o resultado da análise do ficheiro *RTF OLE Package EXE.rtf* utilizando a ferramenta VirusTotal, onde foram realizadas 59 análises por diferentes motores de antivírus. Destes, 28 antivírus classificaram o ficheiro como malicioso (figura 15) como por exemplo: *Ad-Aware- Trojan.GenerickD.3570977*; *Avast- win32:Malware-gen*; *ESET-NOD32- AVariant Of Generik.IKPBEJJ*; *Aegislab- Trojan.RTF.Alien.4!C,* entre outros. Os

restantes antivírus, não identificaram a presença de qualquer ameaça. Este resultado destaca a disparidade na eficácia dos sistemas de deteção de *malware*, sublinhando a importância de considerar múltiplas ferramentas e abordagens na avaliação da segurança de ficheiros digitais.

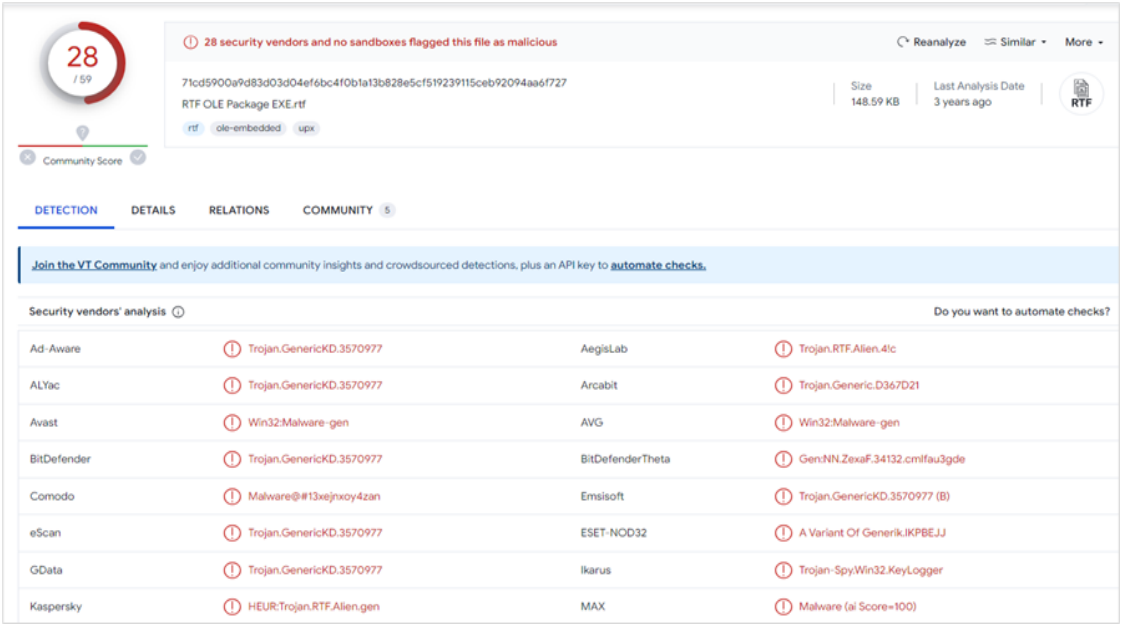


Figura 15- Resultado da análise do ficheiro " RTF OLE Packge EXE.rtf" atráves do VirusTotal

A análise do ficheiro *RTF OLE Package EXE.rtf*, realizada por meio da ferramenta Metadefender Cloud, revelou a presença de 5 ameaças identificadas por 24 motores antivírus, como por exemplo: *Comodo-Malware*; *IKARUS- Trojan.SuspectCRC*; *NANOAV-Trojan.Win32.Graftor.Dnqsup*; *Varist- W32/ABTrojan.OKTY-7934*; *Vir.IT Explorer-Trojan.Win32.Generic.AKLQ*. Essas ameaças indicam que o ficheiro continha elementos incorporados que são frequentemente utilizados como vetor de ataque para executar código malicioso ou instalar software não autorizado.

Após a identificação das ameaças, o ficheiro foi submetido a um processo de desarmamento e reconstrução, que resultou na criação de uma versão limpa, completamente isenta de elementos maliciosos. Este procedimento envolveu a remoção das cinco (5) ameaças detetadas, garantindo a eliminação dos objetos potencialmente perigosos incorporados no ficheiro, conforme ilustrado nas figuras 16 e 17.

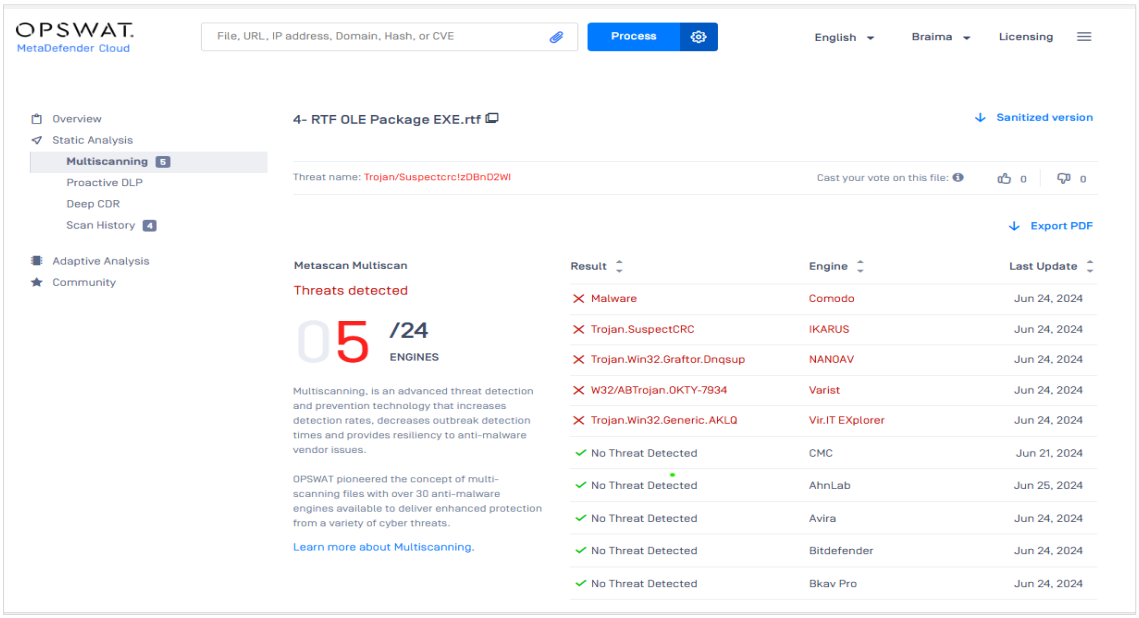


Figura 17- Resultado da análise do ficheiro "RTF OLE Package" através de *Metadefender Cloud*

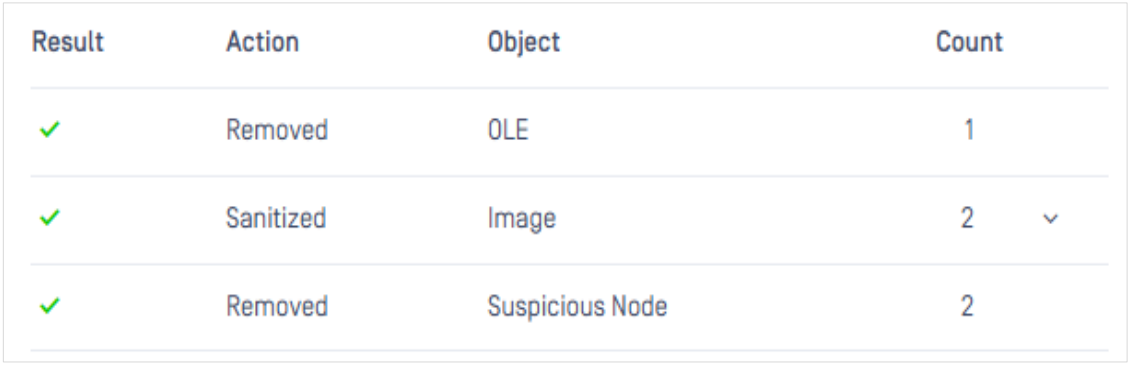


Figura 16- Resultado do ficheiro "RTF OLE Package EXE.rtf" através de *Metadefender Cloud*

Posteriormente, o ficheiro reconstruído foi novamente analisado no VirusTotal e no Metadefender Cloud, para validar a eficácia do processo de higienização e confirmar que o ficheiro estava completamente limpo e seguro. Os resultados das análises pós-tratamento, validaram que o ficheiro reconstruído estava limpo e livre de componentes que pudessem comprometer com a segurança do sistema, conforme ilustrado nas figuras 31 e 32 do anexo D.

Este caso reforça a importância do uso combinado de ferramentas de análise avançadas, como o Metadefender Cloud, que permite não apenas identificar e neutralizar ameaças, mas também assegurar a integridade e a segurança dos ficheiros processados. A remoção de objetos maliciosos em ficheiros RTF com OLE destaca-se como uma medida fundamental na prevenção de possíveis ataques, garantindo um ambiente digital mais seguro.

5.5. Exemplo 5: (eicar-word-macro-cmd-echo.doc)

A análise do ficheiro *eicar-word-macro-cmd-echo.doc*, efetuada através da ferramenta VirusTotal, revelou que 44 dos 65 motores de antivírus utilizados identificaram o ficheiro como malicioso, enquanto os restantes não detetaram qualquer ameaça. Este resultado evidencia a importância da utilização de múltiplos sistemas de deteção para uma avaliação mais abrangente de ficheiros potencialmente perigosos, destacando a variabilidade na eficácia dos diferentes softwares antivírus disponíveis no mercado. A disparidade nas deteções reforça a necessidade de uma abordagem proativa na proteção dos sistemas contra *malware*, bem como, a importância de manter atualizadas as definições dos antivírus, de forma a assegurar uma defesa robusta e eficaz contra ameaças emergentes, conforme ilustrado na Figura 18.

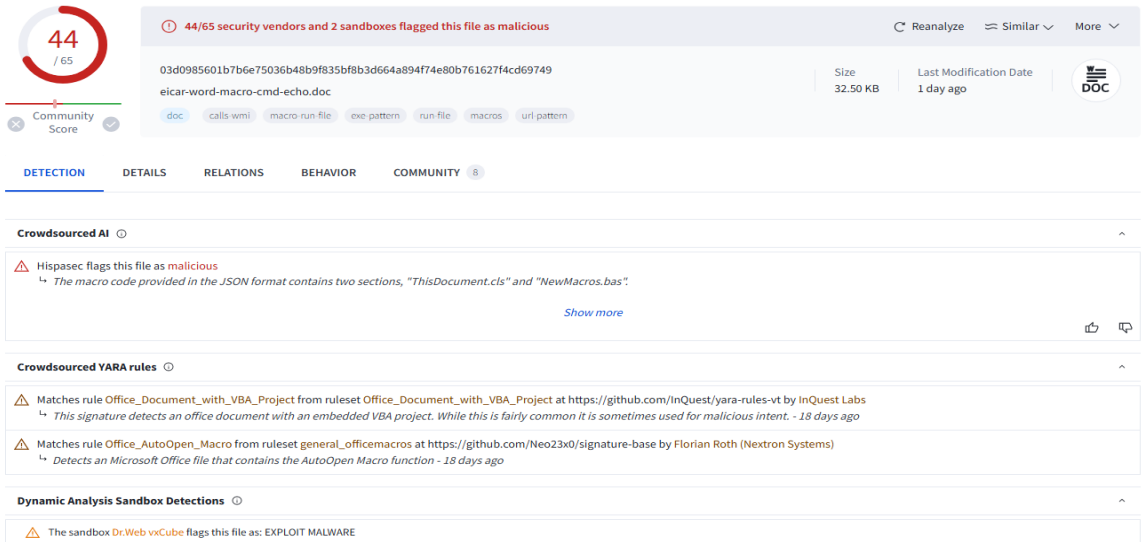


Figura 18- Resultado da análise do ficheiro "Eicar-word-macro-cmd-echo.doc" através do VirusTotal

Na figura 19 é apresentado o resultado da análise do ficheiro *eicar-word-macro-cmd-echo.doc* por meio da ferramenta Metadefender Cloud. Durante essa análise, 24 motores antivírus identificaram 15 ameaças, considerando o ficheiro como infetado ou potencialmente malicioso. Este elevado número de deteções aponta para a presença de uma ameaça significativa, associada a um objeto macro embutido no ficheiro.

Para mitigar os riscos, o ficheiro foi submetido a um processo de desarmamento e reconstrução, que resultou na remoção do objeto macro identificado como a principal fonte de ameaça. Este procedimento foi essencial para eliminar potenciais funcionalidades

maliciosas que poderiam comprometer a segurança dos sistemas, caso o ficheiro fosse executado.

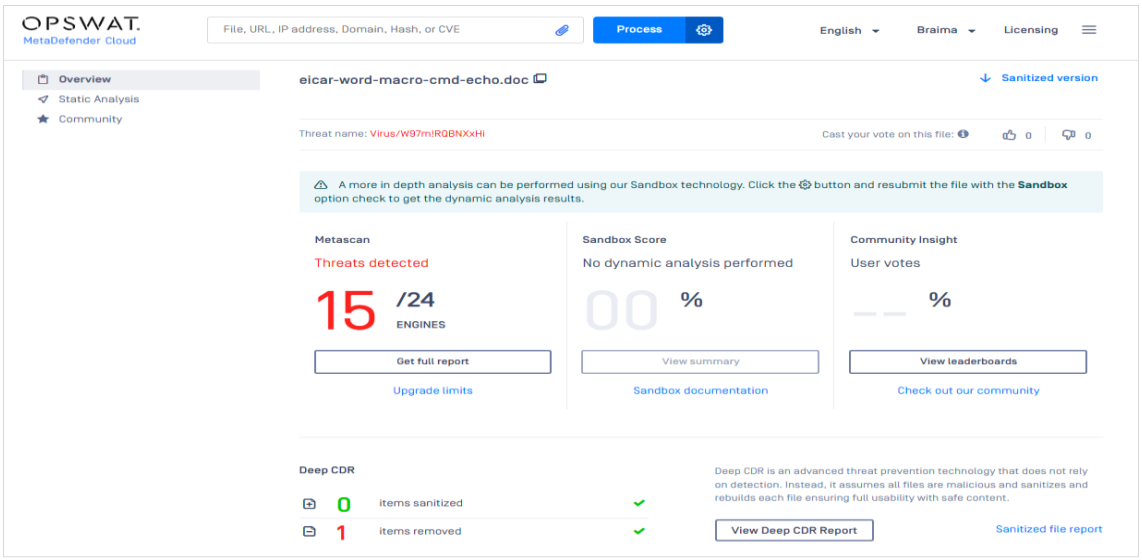


Figura 19- Resultado da análise do ficheiro "Eicar-word-cmd-echo.doc" através da Metadefender Cloud

Após a reconstrução, o ficheiro foi novamente analisado no VirusTotal e no Metadefender Cloud, com o objetivo de validar a eficácia do processo de limpeza e garantir que o ficheiro estava completamente isento de ameaças. Os resultados subsequentes confirmaram a ausência de qualquer comportamento malicioso ou componentes suspeitos no ficheiro tratado, atestando a segurança e a integridade do mesmo, conforme as figuras 33 e 34 do anexo E.

5.6.Exemplo 6: (eicar-excel-macro-write-file.xls)

A análise do ficheiro *eicar-excel-macro-write-file.xls*, realizada por meio da ferramenta VirusTotal, revelou resultados significativos, foram detetadas 27 ameaças entre os 65 motores antivírus. Destes, 27 foram capazes de reconhecer o ficheiro como malicioso, evidenciando a eficácia de uma parte considerável dos motores antivírus na deteção de potenciais ameaças. Esses resultados sublinham a importância de utilizar ferramentas de segurança robustas e atualizadas na proteção contra software malicioso, além de reforçar a necessidade de consciencialização sobre os riscos associados a ficheiros potencialmente inseguros, especialmente aqueles que incorporam macros, conforme ilustrado na figura 20.

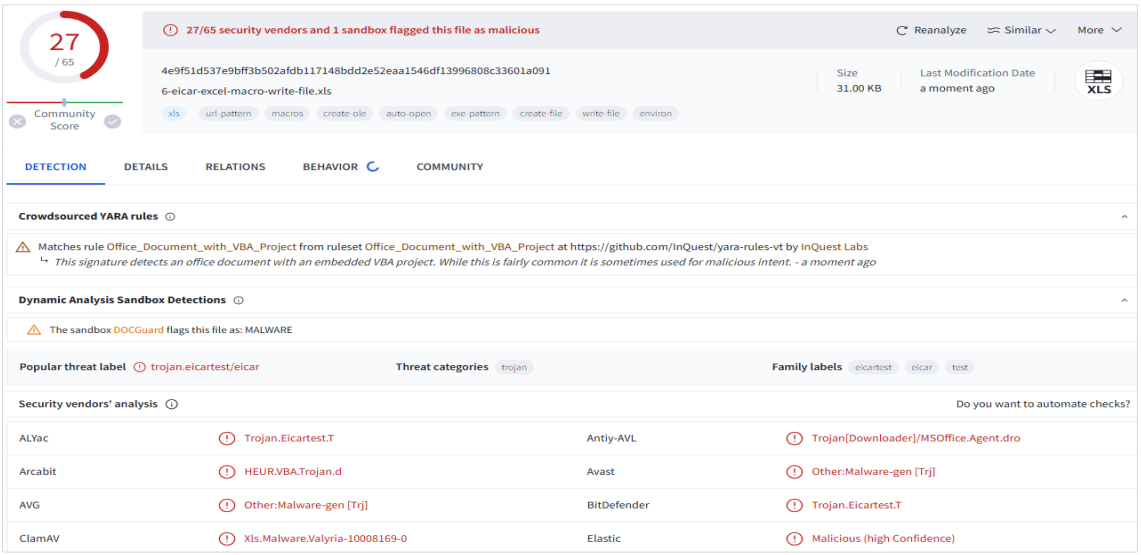


Figura 20- Resultado da análise do ficheiro "Eicar-excel-macro-write-fil.xls através do Vírus Total

A análise do ficheiro *eicar-excel-macro-write-file.xls* por meio da ferramenta *Glasswall* revelou a presença de componentes vulneráveis que podem ser explorados por *hackers* para comprometer a segurança do sistema do utilizador. Durante o processo, o ficheiro foi eficazmente desarmado e reconstruído, resultando na remoção de um objeto macro que poderia ser utilizado por *hackers* para executar ataques. Importante destacar que a análise foi realizada rapidamente, em apenas 1.17 segundos, demonstrando a eficiência da ferramenta na identificação e mitigação de ameaças potenciais. Essa intervenção é fundamental para reforçar a proteção dos sistemas contra o crescente número de ataques cibernéticos baseados em documentos maliciosos, conforme ilustrado na figura 21.

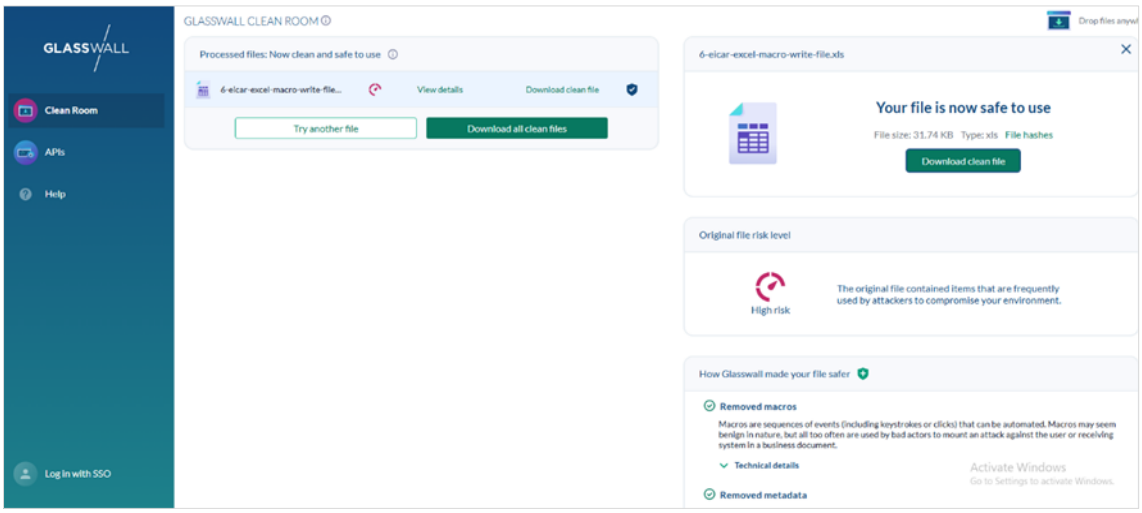


Figura 21- Resultado da análise do ficheiro Eicar-excel-macro-write-file.xls através de Glasswall

5.7.Resumo dos Resultados Obtidos

Nome dos Ficheiros Testados	Nº de Antivírus que Detetaram ameaças	Nº de Antivírus que não detetaram ameaças	Total de Scan
PDF EmbeddedFile HTML.PDF	10	50	60
Form W4-2016.pdf	0	60	60
HTML Javascript obfuscated.html	0	46	46
RTF OLE Package EXE.rtf	28	31	59
eicar-word-macro-cmd-echo.doc	44	21	65
eicar-excel-macro-write-file.xls	27	38	65

Tabela 8- Tabela de resumo dos resultados obtidos com o VirusTotal

Nome dos Ficheiros Analisados	Nº de Antivírus que Detetaram ameaças	Nº de Antivírus que não detetaram ameaças	Nº de Objetos Removidos	Tempo de Analise (Segundos)
PDF EmbeddedFile HTML.PDF	5	19	2	3
Form W4-2016.pdf	0	24	56	3
HTML Javascript obfuscated.html	0	24	3	3
RTF OLE Package EXE.rtf	5	19	5	3
eicar-word-macro-cmd-echo.doc	15	9	1	3
eicar-excel-macro-write-file.xls	6	18	1	1

Tabela 9- Tabela de resumo dos resultados obtidos com o Metadefender Cloud

A análise dos seis ficheiros submetidos a testes revelou que a maioria foi identificada como infetada por vários motores antivírus, conforme apresentado na Tabela 8, que reúne os resultados obtidos através da ferramenta VirusTotal. Dos ficheiros avaliados, quatro foram identificados como maliciosos, enquanto dois, nomeadamente o *Form W4-2016.pdf* e o *HTML Javascript obfuscated.html*, não apresentaram sinais de ameaça. Esses resultados destacam a importância da análise cuidadosa dos ficheiros digitais, uma vez que a deteção de potenciais ameaças pode variar entre diferentes programas antivírus, sublinhando a necessidade de uma abordagem abrangente na cibersegurança.

A análise dos ficheiros efetuada com recurso à ferramenta Metadefender Cloud revelou que, dos seis ficheiros avaliados, quatro continham ameaças significativas, evidenciando a presença de objetos potencialmente exploráveis para fins maliciosos. Os dois ficheiros restantes, *Form W4-2016.pdf* e *HTML Javascript obfuscated.html*, foram considerados seguros, não tendo sido detetadas quaisquer ameaças por nenhum dos 24 motores de antivírus utilizados. No entanto, continham, no total, 56 campos de formulário e 3 *hiperlinks* incorporados. O tempo médio de análise foi de 2,6 segundos, variando consoante o tamanho dos ficheiros. Estes resultados reforçam a importância da utilização de ferramentas especializadas na deteção de ameaças, como parte integrante de uma estratégia eficaz de cibersegurança.

Após realizar uma análise meticulosa dos ficheiros, procedeu-se ao envio dos mesmos para as plataformas VirusTotal e Metadefender Cloud, com o intuito de verificar a presença de quaisquer ameaças potenciais. Os resultados obtidos foram satisfatórios, confirmando que os ficheiros estão limpos e isentos de ameaças, reforçando a eficácia das ferramentas de deteção utilizadas nas análises realizadas. Esta validação é fundamental para garantir a segurança e a integridade dos dados manipulados.

Uma análise comparativa dos resultados obtidos com o Metadefender Cloud face às contribuições de outros autores revela uma convergência significativa nas abordagens de desarmamento de conteúdo, evidenciando a eficácia das técnicas de CDR na mitigação de ameaças cibernéticas. As conclusões indicam que, embora todas as ferramentas analisadas ofereçam mecanismos robustos para neutralizar conteúdo potencialmente malicioso, o seu desempenho varia consideravelmente consoante o caso de uso e o tipo de ficheiros processados.

O Metadefender Cloud destacou-se pela sua versatilidade e capacidade de lidar com uma ampla gama de formatos de ficheiros, demonstrando uma elevada adaptabilidade em diferentes contextos. Já o PdfCDR [33] apresentou um processo mais simplificado e direcionado para ficheiros no formato PDF, assegurando um desarmamento completo ao mesmo tempo que preserva a integridade do conteúdo original. Os resultados mostram que 90% dos ficheiros maliciosos foram limpos com sucesso, enquanto os restantes 10%, que continham estruturas anómalas, foram devidamente colocados em quarentena.

Por outro lado, o DeepPCDR [32] destacou-se pela utilização de algoritmos de deteção avançados, consolidando a sua posição como uma ferramenta particularmente eficaz para análises profundas de conteúdo. Estas evidências sublinham a importância de selecionar a ferramenta de CDR mais adequada, tendo em conta o contexto de utilização e os requisitos específicos de cada organização.

5.8. Limitações

As principais dificuldades enfrentadas na realização deste trabalho prenderam-se, em primeiro lugar, com a complexidade do tema abordado, que exige uma compreensão aprofundada de diversos marcos teóricos e da aplicação prática das estratégias de desarmamento e reconstrução de conteúdo.

Adicionalmente, a investigação foi significativamente limitada pelo acesso restrito a ferramentas essenciais, como Metadefender Core, Glasswall, Exefilter e GateScanner, cuja utilização está condicionada à aquisição de licenças pagas, frequentemente com custos elevados, e sem disponibilização de versões gratuitas para fins académicos.

A instalação do Sasa GateScanner revelou-se igualmente inviável, uma vez que requer credenciais de acesso que não foi possível obter, apesar das várias tentativas de contacto com o suporte técnico, que não obtiveram resposta.

Por fim, a situação foi agravada pela impossibilidade de utilizar o DocBleach, uma ferramenta *open source* relevante para este tipo de análise, mas que se encontra arquivada e sem manutenção ativa desde 9 de novembro de 2020, o que inviabilizou a sua integração no estudo.

6. Conclusão e Trabalho Futuro

Neste trabalho realizou-se uma análise detalhada das áreas da cibersegurança e das tecnologias de CDR, permitindo compreender melhor a relevância e aplicabilidade destas soluções na proteção contra ficheiros infetados.

No início do estudo, foram definidos objetivos claros, sendo o principal apresentar o conceito de CDR, incluindo as suas vantagens e desvantagens, identificar soluções CDR disponíveis no mercado, destacar as principais vulnerabilidades associadas, realizar testes práticos e apresentar os respetivos resultados.

O estudo destacou as principais contribuições do CDR para a segurança cibernética, comprovando a eficácia desta abordagem na neutralização de ameaças associadas a ficheiros potencialmente perigosos. Ao implementar técnicas avançadas de neutralização e reconstrução de conteúdos, o CDR demonstrou capacidade para proteger sistemas e informações sensíveis, mitigando significativamente o risco de infeção por *malware*. Os resultados obtidos não só comprovaram a viabilidade técnica desta metodologia, como, também, evidenciaram o seu impacto positivo na proteção de infraestruturas críticas, contribuindo para um ambiente digital mais seguro.

Os testes realizados com ferramentas como VirusTotal e Metadefender Cloud revelaram elevada eficácia na identificação de ameaças e na reconstrução segura dos ficheiros. Em casos específicos como o *HTML Javascript obfuscated.html* e o *EmbeddedFile HTML.pdf*, o CDR revelou-se uma solução robusta, removendo eficazmente elementos perigosos e permitindo a validação segura dos ficheiros reconstruídos.

No entanto, também se observaram limitações, nomeadamente a dependência do acesso à internet em determinadas ferramentas, como o VirusTotal e o Metadefender Cloud, o que pode representar um entrave em ambientes com restrições de conectividade ou requisitos elevados de segurança.

Adicionalmente, destaca-se a importância das empresas selecionarem soluções de CDR alinhadas com as suas políticas internas de segurança e necessidades específicas. Esta seleção deve considerar fatores como a capacidade de integração de análises em tempo real, compatibilidade com sistemas existentes e estratégias para ultrapassar limitações, como a dependência da conectividade.

Como sugestão para trabalho futuro, propõe-se uma análise mais detalhada dos algoritmos utilizados nas ferramentas de CDR, visando aprofundar o conhecimento sobre a sua eficácia em diferentes contextos. Além disso, o desenvolvimento de uma aplicação autónoma e personalizável representaria um avanço significativo, permitindo análises tanto em tempo real como offline, com processos adaptáveis às políticas de segurança específicas de cada organização. Sugere-se ainda o uso da inteligência artificial (IA) como ferramenta preventiva, reforçando a capacidade de antecipar e mitigar ataques cibernéticos.

Por fim, recomenda-se explorar estratégias de integração das soluções CDR com sistemas de monitorização contínua de redes e proteção de dispositivos finais (*endpoint protection*), aumentando a eficácia global destas tecnologias e promovendo um ecossistema mais robusto e integrado de segurança digital. Este trabalho reforça a relevância do CDR como componente essencial no atual panorama da cibersegurança, com potencial significativo para evoluir e responder eficazmente às necessidades dinâmicas do ambiente digital contemporâneo.

Referências Bibliográficas

[1] NordVPN. A História da cibersegurança. Publicado em: 20 de dezembro de 2022. https://nordvpn.com/pt/blog/historia-da-cibersegurança/?srsltid=AfmBOoqrXFUT_OxoH3lmP2HyeHVo_xrXWwuHpXDr2-U_v1za0SZI2MNs.

[2] Microsoft Security. (2024). What-is-a-cyberattack. https://www.microsoft.com/pt-pt/security/business/security-101/what-is-a-cyberattack

[3] HLTI. (2024). *O Que é Phishing*, Tipos E Exemplos. Publicado em: April 12, 2024. Disponível: https://www.hlti.com.br/phishing/

[4] Skillmine Technology Consulting. Content Disarm and Reconstruction (CRD) technology in cybersecurity: Safeguarding against evolving threats. [Online] 28 de fevereiro de 2024. [Citação: 30 de dezembro de 2024.] https://www.linkedin.com/pulse/content-disarm-reconstruction-crd-technology-cybersecurity-cwvac/.

[5] Boulevard, S. (2021). *What is Content Disarm and Reconstruction (CDR)? Everything You Need to Know*. Publicado em: 5 de Janeiro de 2021. Disponível: https://securityboulevard.com/2021/01/what-is-content-disarm-and-reconstruction-cdr-everything-you-need-to-know/

[6] Kiteworks. (n.d.). *content Disarm and Reconstruction (CDR): Zero-trust Threat Protection*. Disponível: https://www.kiteworks.com/risk-compliance-glossary/cdr-content-disarm-and-reconstruction/

[7] Mordor Intelligence. Tamanho do mercado global de desarme e reconstrução de conteúdo e análise de ações - tendências e previsões de crescimento (2024-2029). [Online] [Consultado em: 8 de julho de 2024.] Tamanho do mercado global de desarme e reconstrução de conteúdo e análise de ações – Tendências e previsões de crescimento (2024– 2029) Source: https://www.mordorintelligence.com/pt/industry-reports/content-disarm-and-reconstruction-market.

[8] Slashdot. Best Content Disarm & Reconstruction (CDR) Software of 2024. [Online] 15 de fevereiro de 2024. https://slashdot.org/software/content-disarm-reconstruction-cdr/.

[9] Tanenbaum, A. & Wetherall, D. Computer Networks (5th ed.). [Online] 20 de julho de 2024. https://csc-knu.github.io/sys-prog/books/Andrew%20S.%20Tanenbaum%20-%20Computer%20Networks.pdf.

[10] Iceberg Security. Os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade. [Online] 7 de novembro de 2024. [Consultado em: 30 de dezembro de 2024.] https://icebergsecurity.cloud/blog/artigo/os-tres-pilares-da-seguranca-da-informacao:-confidencialidade-integridade-e-disponibilidade/.

[11] Kaspersky. O que é cibersegurança? [Online] [Consultado em: 30 de dezembro de 2024.] https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security.

[12] Klusaité, Laura. O que é um ataque cibernético? [Online] 28 de julho de 2020. https://nordvpn.com/pt-br/blog/o-que-e-ataque-cibernetico/.

[13] *A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions.* Aslan, Ö., Aktug, S., Ozkan, M., Yilmaz, A. & Akin, E. 6, 2023, Electronics, Vol. 12, pp. 1-42.

[14] Vodafone. Vodafone Portugal alvo de ciberataque. [Online] 8 de fevereiro de 2022. https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html.

[15] Guerreiro, Catarina. Laboratórios Germano de Sousa alvo de ataque informático. *CNN Portugal.* [Online] 10 de fevereiro de 2022. https://cnnportugal.iol.pt/geral/laboratorios-germano-de-sousa-alvo-de-ataque-informatico/20220210/6204e4990cf2c7ea0f183aed.

[16] Correia, G. & Casanova, R. Laboratórios Germano de Sousa alvo de ataque informático. CUF alerta para "constrangimentos no acesso ao serviço de análises clínicas". [Online] 10 de fevereiro de 2022.

[17] Sonae. Notícias. Informação sobre ataque informático. [Online] 6 de abril de 2022. https://mc.sonae.pt/noticias/informacao-ataque-informatico/.

[18] Gomes, J. & Agência Lusa. Sistema informático do Hospital Garcia de Orta em baixo após ataque informático. Atividade clínica foi quase toda "mantida". [Online] 26 de abril de 2022. https://observador.pt/2022/04/26/sistema-informatico-do-hospital-garcia-de-orta-em-baixo-apos-ataque-informatico/.

[19] Agência Lusa. Segurança Social. Ciberataque sem evidência de acesso a dados. [Online] 23 de novembro de 2022. https://rr.sapo.pt/noticia/pais/2022/11/23/seguranca-social-ciberataque-sem-evidencia-de-acesso-a-dados/309256/.

[20] Nunes, Flávio. Ciberataque à TAP: o que disse a empresa (e o que aconteceu depois). [Online] 22 de setembro de 2022. https://eco.sapo.pt/2022/09/22/ciberataque-a-tap-o-que-disse-a-empresa-e-o-que-aconteceu-depois/.

[21] Lima, Gustavo. Sua assinatura do Scribd foi cancelada. Clique aqui para renová-la. [Online] 4 de junho de 2021. https://pt.scribd.com/document/510565144/Apresentacao-Aula-6-Codigo-Malicioso-Malware.

[22] Gugelmin, F. & Yuge, C. Entenda o que é backdoor e a diferença com os trojans. [Online] 4 de agosto de 2021. https://canaltech.com.br/seguranca/o-que-e-backdoor-em-computacao-191727/#google_vignette.

[23] Cidadão na Rede (n.d.). O QUE É BOTNET. Publicado October 7, 2022, Disponível: https://cidadaonarede.nic.br/pt/videos/o-que-e-botnet

[24] Shahzad, R., Lavesson, N. & Johnson, H. *Accurate Adware Detection Using Opcode Sequence Extraction. 2011 Sixth International Conference on Availability, Reliability and Security.* 2011, pp. 189-195.

[25] Neves, Raquel. *Vitimação por Phishing: um estudo empírico. Dissertação de Mestrado em Criminologia.* Faculdade de Direito da Universidade do Porto: s.n., 2022.

[26] *Exploit Prediction Scoring System (EPSS).* Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I. & Roytman, M. 3, 9 de julho de 2021, Digital Threats: Research and Practice, Vol. 2, pp. 1-17.

[27] Shaputra, Muhammad. [Online] 6 de outubro de 2023. https://www.itsecasia.tech/content-disarm-reconstruction-technology/.

[28] Gafety. Sandbox: o que é e como funciona. [Online] 22 de março de 2021. https://gatefy.com/pt-br/blog/sandbox-o-que-e-e-como-funciona/.

[29] *INTELIGÊNCIA ARTIFICIAL, DEFINIÇÕES E APLICAÇÕES: o uso de sistemas inteligentes em benefício da medicina.* Santos, A. & del Decchio, G. 1, julho de 2020, Revista Interface Tecnológica, Vol. 17, pp. 129-139.

[30] Devoteam Cyber Trust. 14 Tendências em cibersegurança para 2024. [Online] dezembro de 2023. https://www.integrity.pt/pdf/14tendenciascibersegurança_2024_PT.pdf.

[31] *Open Image Content Disarm And Reconstruction.* Belkind, E., Dubin, R. & Dvir, A. 2023.

[32] *Content Disarm and Reconstruction of RTF Files a Zero File Trust Methodology.* Dubin, Ran. 2023, IEEE Transactions on Information Forensics and Security, Vol. 18, pp. 1461-1472.

[33] *Content Disarm and Reconstruction of PDF Files.* Dubin, Ran. 2023, IEEE Access, Vol. 11, pp. 38399-38416. https://ieeexplore.ieee.org/document/10103531.

[34] *Content Disarm and Reconstruction of Microsoft Office OLE files.* Dubin, Ran. fevereiro de 2024, Computers & Security, Vol. 137.

[35] Ameaças e ataques aos Sistemas de Informação: prevenir e antecipar. Pinheiro, José. 5, dezembro de 2007, Cadernos UniFOA, pp. 11-21.

[36] *Cyber security: State of the art, challenges and future directions.* Admass, W., Munaye, Y. & Diro, A. 2024, Cyber Security and Applications, Vol. 2, pp. 1-9.

[37] IT Security. As principais ameaças para as organizações em abril de 2023. [Online] 15 de maio de 2023. https://www.itsecurity.pt/news/threats/as-principais-ameacas-para-as-organizacoes-em-abril-de-2023.

[38] Alhababy, A. What Is Agent Tesla Malware? [Online] 2016. https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/agent-tesla.

[39] Tavella, Fernando. Formbook: malware rouba dados de login salvos em navegadores. [Online] 21 de outubro de 2022. https://www.welivesecurity.com/br/2022/10/21/formbook-malware-rouba-dados-de-login-salvos-em-navegadores/.

[40] Centro Nacional de Cibersegurança . Relatório em 15 minutos. Cibersegurança em Portugal. [Online] junho de 2023. [Consultado em: 31 de dezembro de 2024.] https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs15m.pdf.

[41] IT Security. Relatório revela aumento de 8% de ciberataques a nível mundial. [Online] 28 de agosto de 2023. [Consultado em: 31 de dezembro de 2024.] https://www.itsecurity.pt/news/analysis/relatorio-revela-aumento-de-8-de-ciberataques-a-nivel-mundial.

[42] Centro Nacional de Cibersegurança. Relatório Cibersegurança em Portugal. [Online] julho de 2024. https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf.

[43] Check Point. 2024 Cyber Security Report. [Online] 2024. [Consultado em: 31 de dezembro de 2024.] https://www.checkpoint.com/resources/?fw=1b737.

[44] IT Security. Foram implementados mais de 400 mil ficheiros maliciosos por dia em 2023. [Online] 7 de dezembro de 2023. https://www.itsecurity.pt/news/analysis/foram-implementados-mais-de-400-mil-ficheiros-maliciosos-por-dia-em-2023.

[45] National Institute of Standards and Technology. Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy. [Online] dezembro de 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[46] ABNT/CB-21. Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. [Online] agosto de 2011. https://www.academia.edu/38380611/ISO_IEC_27005_Gestao_de_Riscos_TI.

[47] S21 Cyber Solutions by Thales. Threat Landscape Report 2023 - Ataques Relevantes. [Online] https://www.s21sec.com/wp-content/uploads/2023/07/S21sec_Thales_ThreatLandscapeReport_2023_ES.pdf.

[48] Reis, Leovan. CVE-2023-38831: Zero-Day no WinRAR. [Online] 28 de agosto de 2023. https://blog.ecotrust.io/cve-2023-38831-zero-day-no-winrar/.

[49] Github.com. CVE-2023-38831 PoC (Proof Of Concept). [Online] 2025. [Consultado em: 1 de janeiro de 2025.] https://github.com/HDCE-inc/CVE-2023-38831?tab=readme-ov-file.

[50] National Vulnerability Databse NVD. CVE-2023-34362 Detail Description. [Online] [Consultado em: 1 de janeiro de 2025.] https://nvd.nist.gov/vuln/detail/CVE-2023-34362.

[51] Common Vulnerabilities and Exposures (CVE). CVE-2023-2868. [Online] [Consultado em: 1 de janeiro de 2025]. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2868.

[52] Ngo, Nhut. CVE-2023-21716: Proteção maliciosa de arquivos RTF com desarmamento e reconstrução de conteúdo. [Online] 21 de março de 2023. [Consultado em: 1 de janeiro de 2025.] https://portugese.opswat.com/blog/malicious-rtf-file.

[53] Palazolo, Gustavo. CVE-2023-21716: Microsoft Word RCE Vulnerability. [Online] 27 de março de 2023. [Consultado em: 1 de janeiro de 2025.] https://www.netskope.com/pt/blog/cve-2023-21716-microsoft-word-rce-vulnerability.

[54] Ostec. CVE-2017-11882: vulnerabilidade explorada há cinco anos. [Online] 5 de setembro de 2023. [Consultado em: 1 de janeiro de 2025.] https://ostec.blog/geral/cve-2017-11882-vulnerabilidade-explorada-ha-cinco-anos/?cn-reloaded=1&cn-reloaded=1&cn-reloaded=1&cn-reloaded=1.

[55] Microsoft. Microsoft Office Memory Corruption Vulnerability. [Online] 29 de novembro de 2017. [Consultado em: 1 de janeiro de 2025.] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882.

[56] Kadam, Prashant. CVE-2018-4990 – Adobe Reader Double Free (Zero Day) vulnerability alert! [Online] 16 de maio de 2018. [Consultado em: 1 de janeiro de 2025.] https://blogs.quickheal.com/cve-2018-4990-adobe-reader-double-free-zero-day-vulnerability-alert/.

[57] Sunshine, Yehudah. How CDR improves file security. [Online] 23 de abril de 2021. [Consultado em: 1 de janeiro de 2025.] https://cyberprotection-magazine.com/how-cdr-improves-file-security.

[58] Chan, Kyle. 19 Most Common Types of Phishing Attacks in 2025. [Online] 30 de dezembro de 2024. [Consultado em: 1 de janeiro de 2025.] https://www.upguard.com/blog/types-of-phishing-attacks.

[59] Votiro. Gartner Recognizes Content Disarm and Reconstruction as a High-Benefit Solution. [Online] 22 de junho de 2023. [Consultado em: 1 de janeiro de 2025]. https://votiro.com/blog/gartner-recognizes-content-disarm-and-reconstruction-cdr-as-a-high-benefit-solution/.

[60] A Complete Guide to Content Disarm and Reconstruction (CDR). [Online] 18 de dezembro de 2020. [Consultado em: 2 de janeiro de 2024.] https://votiro.com/guides/what-is-content-disarm-and-reconstruction-cdr/.

[61] Voitiro. What is Content Disarm and Reconstruction (CDR)? Everything You Need to Know. [Online] 5 de janeiro de 2021. [Consultado em: 2 de janeiro de 2025.] https://securityboulevard.com/2021/01/what-is-content-disarm-and-reconstruction-cdr-everything-you-need-to-know/.

[62] Malwation Analysis Solutions. Content Disarm and Reconstruction (CDR): Nice-to-Have or Must Have? What is the Cost of No Action? [Online] 21 de dezembro de 2024. [Consultado em: 2 de janeiro de 2025.] https://www.malwation.com/blog/content-disarm-and-reconstruction-cdr-nice-to-have-or-must-have-what-is-the-cost-of-no-action.

[63] Allied Market Research. Content Disarm And Reconstruction Market Size, Share, Competitive Landscape and Trend Analysis Report, by Component, by Deployment Mode, by Organization Size, by Application, by End User : Global Opportunity Analysis and Industry Forecast, 2023-2032. [Online] junho de 2023. [Consultado em: 2 de janeiro de 2025.] https://www.alliedmarketresearch.com/content-disarm-and-reconstruction-market.

[64] Github.com. DocBleach. [Online] 9 de novembro de 2020. [Consultado em: 1 de janeiro de 2025.] https://github.com/docbleach/DocBleach.

[65] Samad, Abdul. Practical Guide to Malware Analysis and Reverse Engineering (Analyzing Malicious MS-Office Document — P1). [Online] 12 de maio de 2022. [Consultado em: 2 de janeiro de 2025.] https://systemweakness.com/practical-guide-to-malware-analysis-and-reverse-engineering-analyzing-malicious-document-p-1-b39b92704d1c.

[66] Github.com. decalage/oletools. [Online] [Consultado em: 2 de janeiro de 2025.] https://github.com/decalage2/oletools.

[67] Decalage2. [Online] [Consultado em: 2 de janeiro de 2025.] https://github.com/decalage2/exefilter.

[68] Lagadec, Philippe. ExeFilter. An open-source framework for active content filtering. [Online] 28 de março de 2008. https://www.decalage.info/files/CanSecWest08_Lagadec_ExeFilter.pdf.

[69] Yara. Welcome to YARA's documentation! [Online] [Consultado em: 2 de janeiro de 2025.] https://yara.readthedocs.io/en/stable/index.html.

[70] 70. Souza, Vinicius. Yara – Ferramenta de análise de Malwares. [Online] 27 de abril de 2021. [Consultado em: 2 de janeiro de 2025.] https://blog.ironlinux.com.br/yara-rules-ferramenta-de-analise-de-malwares/.

[71] VirusTotal. Virus Total. [Online] 2024. https://www.VirusTotal.com/gui/home/upload.

[72] RamsData. OPSWAT. MetaDefender Cloud. [Online] [Consultado em: 2 de janeiro de 2025.] https://ramsdata.com.pl/pt-pt/opswat/produtos/metadefender-cloud-ramsdata/.

[73] GlassWall. What is Content Disarm and Reconstruction (CDR)? [Online] [Consultado em: 2 de janeiro de 2025.] https://www.glasswall.com/cdr.

[74] Senetas. Votiro announces its first formal channel partner program. [Online] [Consultado em: 2 de janeiro de 2025.] https://www.senetas.com/votiro-announces-first-formal-channel-program/.

[75] Gore, Jo. Votiro Disarmer Technology. [Online] 1 de fevereiro de 2022. https://support.votiro.com/hc/en-us/articles/360014530138-Votiro-Disarmer-Technology.

[76] Odix. Proprietary Deep File analysis and TrueCDRTM algorithm for efficient Malware Prevention. [Online] [Consultado em: 2 de janeiro de 2025.] https://www.odix.com/odix-technology/.

[77] Sasa Software. Sasa Software. [Online] [Consultado em: 3 de janeiro de 2025]. https://www.sasa-software.com/about-sasa-software/.

[78] Sasa Software. (n.d.). Sasa Software Overview. última atualização: 21 de setembro de 2024, Disponível: https://finder.startupnationcentral.org/company_page/sasa-software

[79] ISO. ISO 32000-1:2008(en) Document management —Portable document format— Part 1: PDF 1.7. [Online] [Consultado em: 3 de janeiro de 2025.] https://www.iso.org/obp/ui/en/#iso:std:iso:32000:-1:ed-1:v1:en.

[80] IronMoon. PDF Malware: Part 1 Understanding PDF Files. [Online] 20 de maio de 2020. [Consultado em: 3 de janeiro de 2025.] https://ironmoon.net/2020/05/01/Understanding-PDF-Files.html.

[81] Microsoft Learn Challenge. [MS-DOC]: Word (.doc) Binary File Format. [Online] 15 de novembro de 2022. [Consultado em: 3 de janeiro de 2025]. https://learn.microsoft.com/en-us/openspecs/office_file_formats/ms-doc/ccd7b486-7881-484c-a137-51170af7cc22?redirectedfrom=MSDN.

[82] FileFormat. O que é um arquivo RTF? [Online] [Consultado em: 3 de janeiro de 2025.] https://docs.fileformat.com/pt/word-processing/rtf/.

[83] Eduardo Passos. *Ransomware.* Publicado March 4, 2019, Disponível: https://infob.com.br/o-que-e-ransomware/

[84] FUNDAJ. (n.d.). *Códigos maliciosos (Malware).* [Online] 21 de dezembro de 2020. https://www.gov.br/fundaj/pt-br/centrais-de-conteudo/noticias-1/4-codigos-maliciosos-malware.

[85] Sasa Software. (n.d.). *How gatescanner works*. [Consultado em: 3 de janeiro de 2025.] https://www.sasa-software.com/

[86] João Emílio de Almeida. *Cybersecurity: from risk prevention to*

[87] *incident management*. [Online] setembro de 2021. [Consultado em: 3 de janeiro de 2025]. https://scielo.pt/pdf/rist/n43/1646-9895-rist-43-1.pdf

[88] Emergen Research. Top 10 Empresas no Mercado de Desarmamento e Reconstrução de Conteúdo (CDR) em 2023. [Online] 11 de julho de 2023. https://www.emergenresearch.com/blog/top-10-companies-in-content-disarm-and-reconstruction-market-in-2023

[89] Check Point. *what-is-email-security*. [Consultado em: 4 de janeiro de 2025] https://www.checkpoint.com/pt/cyber-hub/threat-prevention/what-is-email-security/why-email-security-is-important/

[90] Github. DocBleach. [Online] 29 de março de 2017. https://github-wiki-see.page/m/docbleach/DocBleach/wiki

[91] Camila Porto. Vírus Total. [Online] 5 de junho de 2024. https://pinkfireblog.com.br/VirusTotal/

[92] WebCatalog. VirusTotal. [Consultado em: 5 de janeiro de 2025] https://webcatalog.io/es/apps/VirusTotal.

[93] OPSWAT. OPSWAT lança MetaDefender Cloud na Austrália, garantindo a soberania dos dados na região APAC. [Online] 4 de abril de 2023 https://portugese.opswat.com/blog/opswat-launches-metadefender-cloud-in-australia-ensuring-data-sovereignty-in-the-apac-region

[94] Fortinet. (n.d.). What Is A Rootkit. [Consultado em: 1 de janeiro de 2025] https://www.fortinet.com/resources/cyberglossary/rootkit

[95] OPSWAT. *Content Disarm and Reconstruction (CDR) Selection Guide*. [Publicado] março de 2021.

https://info.opswat.com/hubfs/Demand%20Gen%20Assets/White%20Papers/OPSWAT_CDR_SelectionGuide_EN.pdf

[96] NUTANIX. Soluções *Glasswall*. [Consultado em: 5 de janeiro de 2025]. https://www.nutanix.com/en_sg/partners/technology-alliances/glasswall

[97] Peraton. Cibernético. [Consultado em: 3 de janeiro de 2025]. https://www.peraton.com/missions/cyber/

[98] Cybersecurity. *Glasswall Halo*. [Consultado em: 27 de dezembro de 2025]. https://cybersecurity-excellence-awards.com/candidates/glasswall-halo-an-advanced-content-disarm-and-reconstruction-cdr-solution-that-protects-organizations-against-file-based-security-threats-2025/

ANEXOS

Anexos

Anexo A: Exemplo 1 - PDF EmbeddedFile HTML.PDF

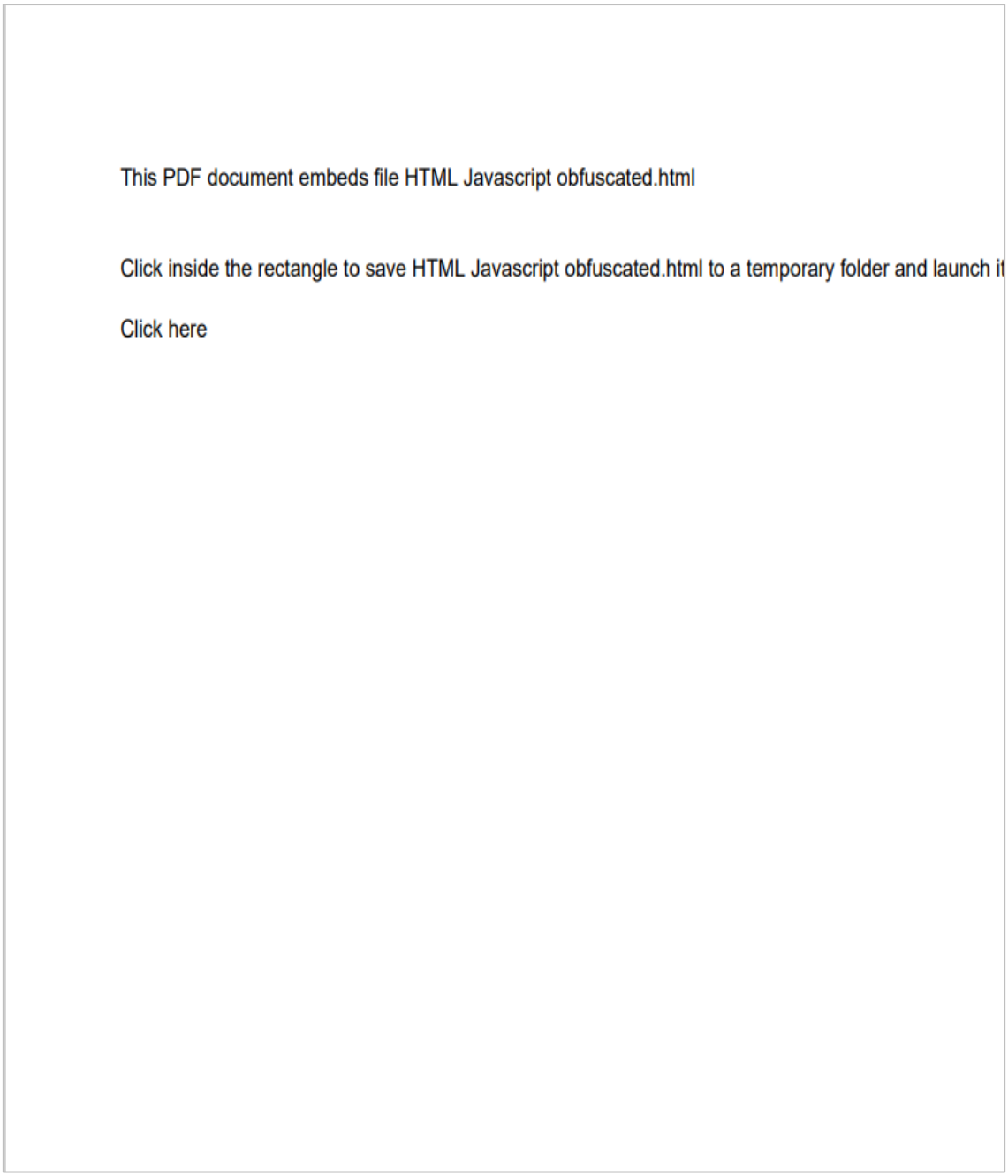
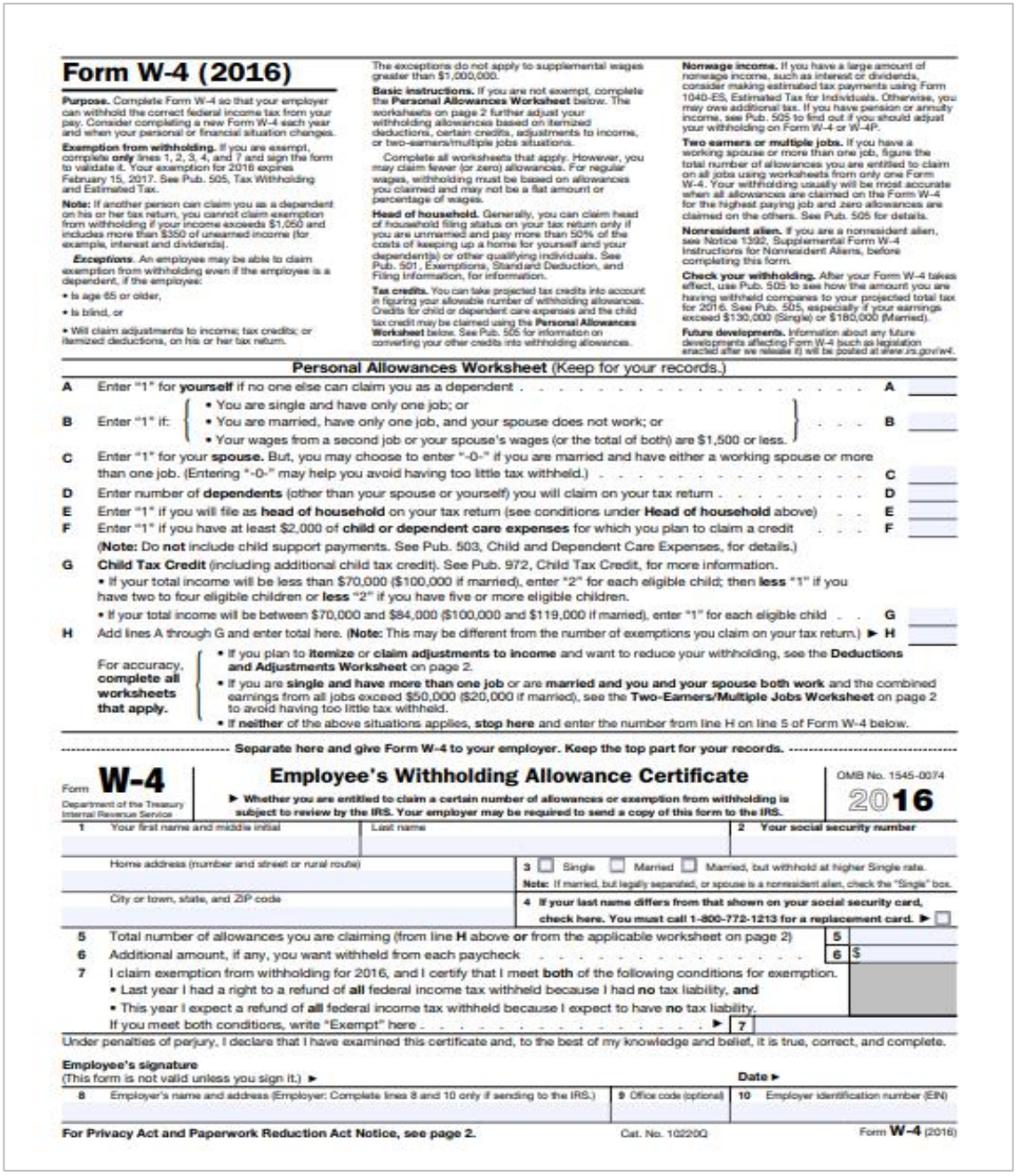


Figura 22- Ficheiro original infetado antes da análise

Anexo B: Exemplo 2 - Form W4-2016.pdf



Form W-4 (2016)

Purpose. Complete Form W-4 so that your employer can withhold the correct federal income tax from your pay. Consider completing a new Form W-4 each year and when your personal or financial situation changes.

Exemption from withholding. If you are exempt, complete **only** lines 1, 2, 3, 4, and 7 and sign the form to validate it. Your exemption for 2016 expires February 15, 2017. See Pub. 505, Tax Withholding and Estimated Tax.

Note: If another person can claim you as a dependent on his or her tax return, you cannot claim exemption from withholding if your income exceeds $1,050 and includes more than $350 of unearned income (for example, interest and dividends).

Exceptions. An employee may be able to claim exemption from withholding even if the employee is a dependent, if the employee:

- Is age 65 or older,
- Is blind, or
- Will claim adjustments to income; tax credits; or itemized deductions, on his or her tax return.

The exceptions do not apply to supplemental wages greater than $1,000,000.

Basic instructions. If you are not exempt, complete the **Personal Allowances Worksheet** below. The worksheets on page 2 further adjust your withholding allowances based on itemized deductions, certain credits, adjustments to income, or two-earners/multiple jobs situations.

Complete all worksheets that apply. However, you may claim fewer (or zero) allowances. For regular wages, withholding must be based on allowances you claimed and may not be a flat amount or percentage of wages.

Head of household. Generally, you can claim head of household filing status on your tax return only if you are unmarried and pay more than 50% of the costs of keeping up a home for yourself and your dependent(s) or other qualifying individuals. See Pub. 501, Exemptions, Standard Deduction, and Filing Information, for information.

Tax credits. You can take projected tax credits into account in figuring your allowable number of withholding allowances. Credits for child or dependent care expenses and the child tax credit may be claimed using the **Personal Allowances Worksheet** below. See Pub. 505 for information on converting your other credits into withholding allowances.

Nonwage income. If you have a large amount of nonwage income, such as interest or dividends, consider making estimated tax payments using Form 1040-ES, Estimated Tax for Individuals. Otherwise, you may owe additional tax. If you have pension or annuity income, see Pub. 505 to find out if you should adjust your withholding on Form W-4 or W-4P.

Two earners or multiple jobs. If you have a working spouse or more than one job, figure the total number of allowances you are entitled to claim on all jobs using worksheets from only one Form W-4. Your withholding usually will be most accurate when all allowances are claimed on the Form W-4 for the highest paying job and zero allowances are claimed on the others. See Pub. 505 for details.

Nonresident alien. If you are a nonresident alien, see Notice 1392, Supplemental Form W-4 Instructions for Nonresident Aliens, before completing this form.

Check your withholding. After your Form W-4 takes effect, use Pub. 505 to see how the amount you are having withheld compares to your projected total tax for 2016. See Pub. 505, especially if your earnings exceed $130,000 (Single) or $180,000 (Married).

Future developments. Information about any future developments affecting Form W-4 (such as legislation enacted after we release it) will be posted at *www.irs.gov/w4*.

Personal Allowances Worksheet (Keep for your records.)

A	Enter "1" for **yourself** if no one else can claim you as a dependent	A
B	Enter "1" if: • You are single and have only one job; or • You are married, have only one job, and your spouse does not work; or • Your wages from a second job or your spouse's wages (or the total of both) are $1,500 or less.	B
C	Enter "1" for your **spouse.** But, you may choose to enter "-0-" if you are married and have either a working spouse or more than one job. (Entering "-0-" may help you avoid having too little tax withheld.)	C
D	Enter number of **dependents** (other than your spouse or yourself) you will claim on your tax return	D
E	Enter "1" if you will file as **head of household** on your tax return (see conditions under **Head of household** above)	E
F	Enter "1" if you have at least $2,000 of **child or dependent care expenses** for which you plan to claim a credit (**Note:** Do **not** include child support payments. See Pub. 503, Child and Dependent Care Expenses, for details.)	F
G	**Child Tax Credit** (including additional child tax credit). See Pub. 972, Child Tax Credit, for more information. • If your total income will be less than $70,000 ($100,000 if married), enter "2" for each eligible child; then **less** "1" if you have two to four eligible children or **less** "2" if you have five or more eligible children. • If your total income will be between $70,000 and $84,000 ($100,000 and $119,000 if married), enter "1" for each eligible child	G
H	Add lines A through G and enter total here. (**Note:** This may be different from the number of exemptions you claim on your tax return.) ►	H

For accuracy, **complete all worksheets that apply.**

- If you plan to **itemize** or **claim adjustments to income** and want to reduce your withholding, see the **Deductions and Adjustments Worksheet** on page 2.
- If you are **single and have more than one job** or are **married and you and your spouse both work** and the combined earnings from all jobs exceed $50,000 ($20,000 if married), see the **Two-Earners/Multiple Jobs Worksheet** on page 2 to avoid having too little tax withheld.
- If **neither** of the above situations applies, **stop here** and enter the number from line H on line 5 of Form W-4 below.

Separate here and give Form W-4 to your employer. Keep the top part for your records.

Form **W-4** — Department of the Treasury, Internal Revenue Service

Employee's Withholding Allowance Certificate

► **Whether you are entitled to claim a certain number of allowances or exemption from withholding is subject to review by the IRS. Your employer may be required to send a copy of this form to the IRS.**

OMB No. 1545-0074 — **2016**

1	Your first name and middle initial / Last name	2 Your social security number
	Home address (number and street or rural route)	3 ☐ Single ☐ Married ☐ Married, but withhold at higher Single rate. Note: If married, but legally separated, or spouse is a nonresident alien, check the "Single" box.
	City or town, state, and ZIP code	4 If your last name differs from that shown on your social security card, check here. You must call 1-800-772-1213 for a replacement card. ► ☐
5	Total number of allowances you are claiming (from line **H** above **or** from the applicable worksheet on page 2)	5
6	Additional amount, if any, you want withheld from each paycheck	6 $
7	I claim exemption from withholding for 2016, and I certify that I meet **both** of the following conditions for exemption. • Last year I had a right to a refund of **all** federal income tax withheld because I had **no** tax liability, **and** • This year I expect a refund of **all** federal income tax withheld because I expect to have **no** tax liability. If you meet both conditions, write "Exempt" here	7

Under penalties of perjury, I declare that I have examined this certificate and, to the best of my knowledge and belief, it is true, correct, and complete.

Employee's signature (This form is not valid unless you sign it.) ► **Date** ►

8	Employer's name and address (Employer: Complete lines 8 and 10 only if sending to the IRS.)	9 Office code (optional) / 10 Employer identification number (EIN)

For Privacy Act and Paperwork Reduction Act Notice, see page 2. Cat. No. 10220Q — Form **W-4** (2016)

Figura 23- Ficheiro original infetado antes da análise

Figura 24- Resultado da análise do ficheiro Form w4-2016.pdf no VirusTotal depois da análise

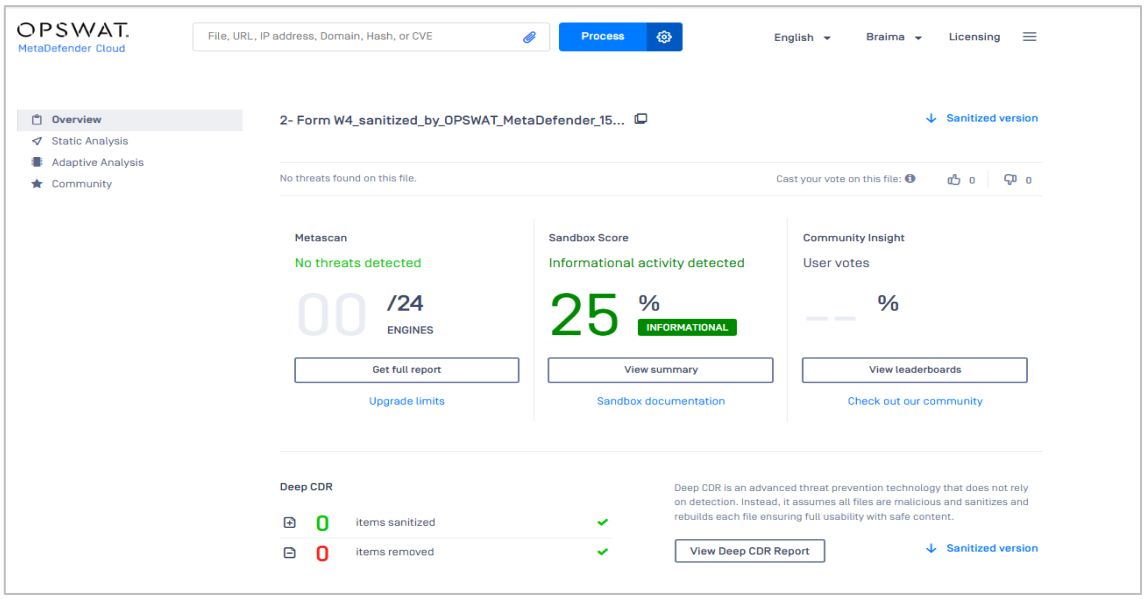


Figura 25- Resultado da análise do ficheiro Form w4-2016.pdf no Metadefender Cloud depois da análise

Anexo C: Exemplo 3 - HTML Javascript obfuscated.html

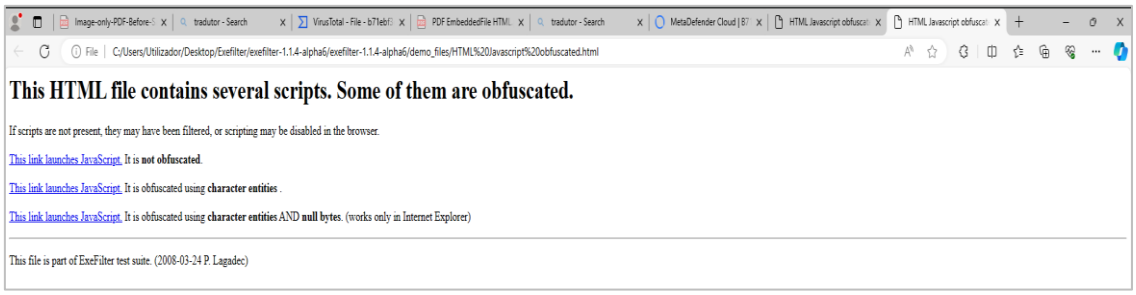


Figura 26- Ficheiro infetado antes da análise

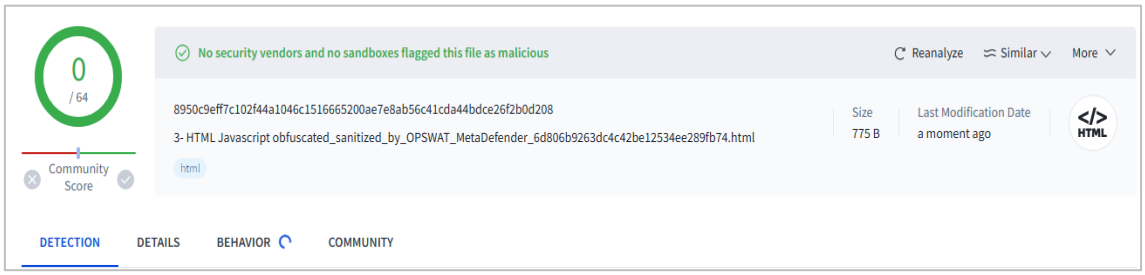


Figura 27- Resultado da análise do ficheiro HTML Javascript obfuscated.html no VirusTotal depois da limpeza

Figura 28- Resultado da análise do ficheiro Javascript obfuscated.html depois da limpeza

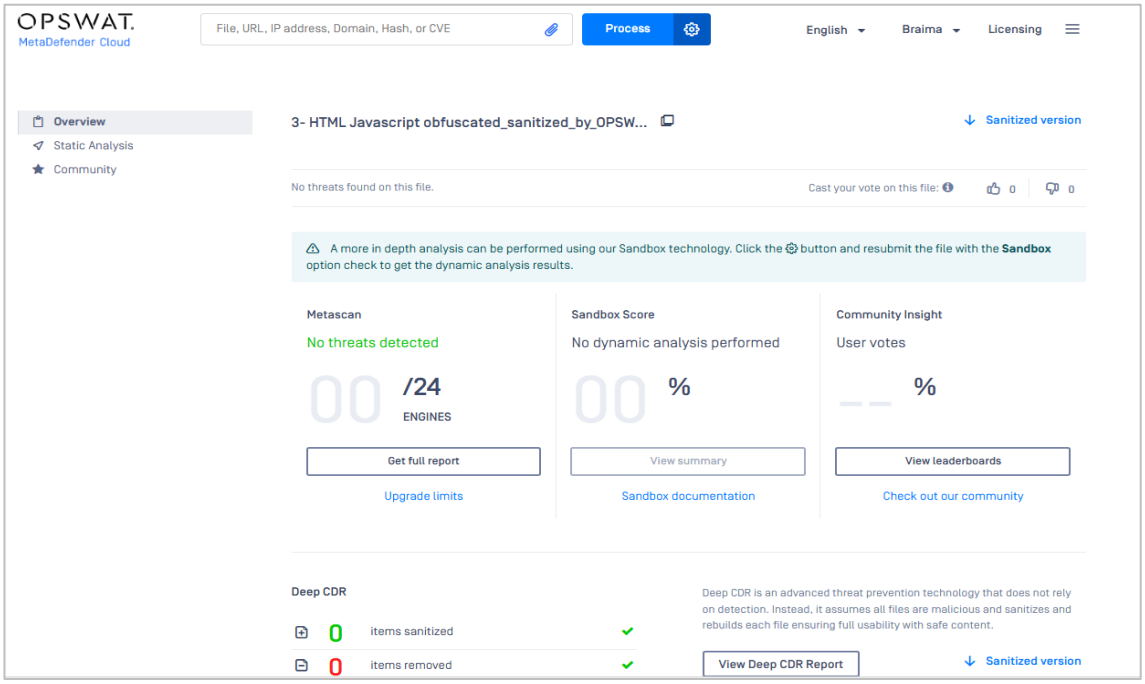


Figura 29- Resultado da análise do ficheiro Javascript obfuscated.html no Metadefender Cloud depois da limpeza

Anexo D: Exemplo 4 - RTF OLE Package EXE.rtf

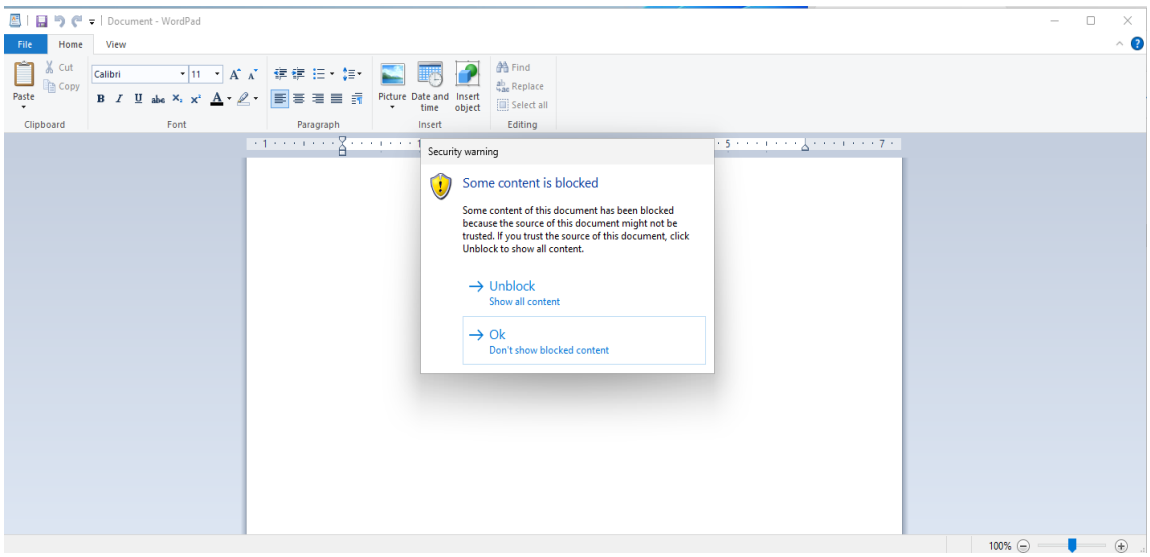


Figura 30- Ficheiro RTF Ole Package EXE.rtf infectado antes da análise

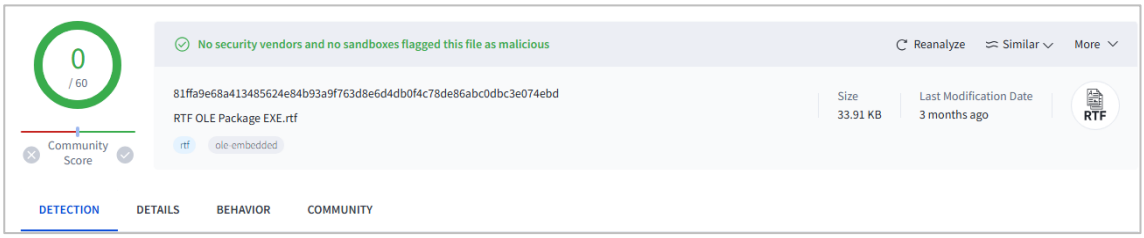


Figura 31- Resultado da análise do ficheiro RTF Ole Package EXE.rtf no VirusTotal depois da limpeza

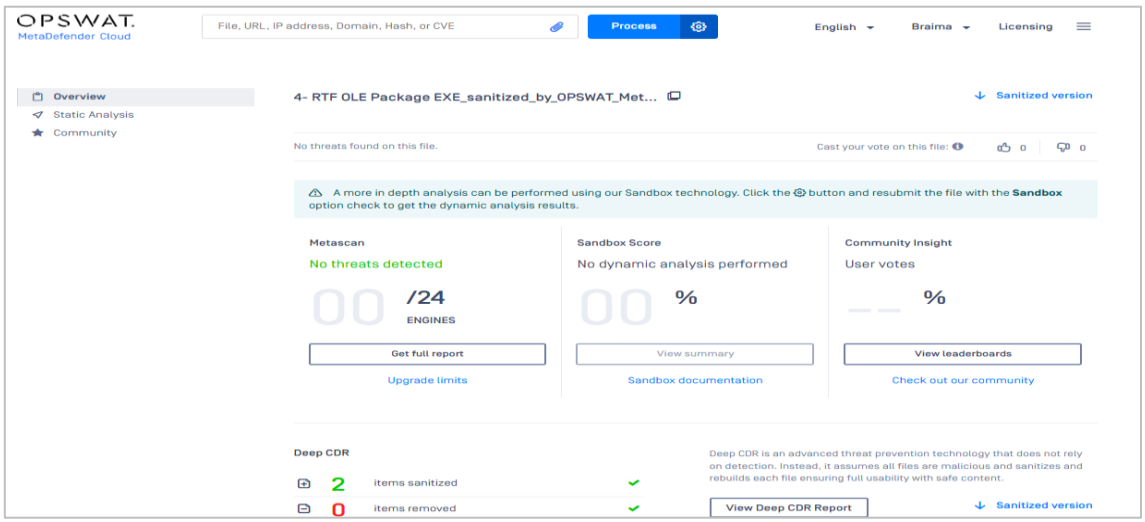


Figura 32- Resultado da análise do ficheiro RTF Ole Package EXE.rtf no Metadefender Cloud depois da limpeza

Anexo E: Exemplo 5 - eicar-word-macro-cmd-echo.doc

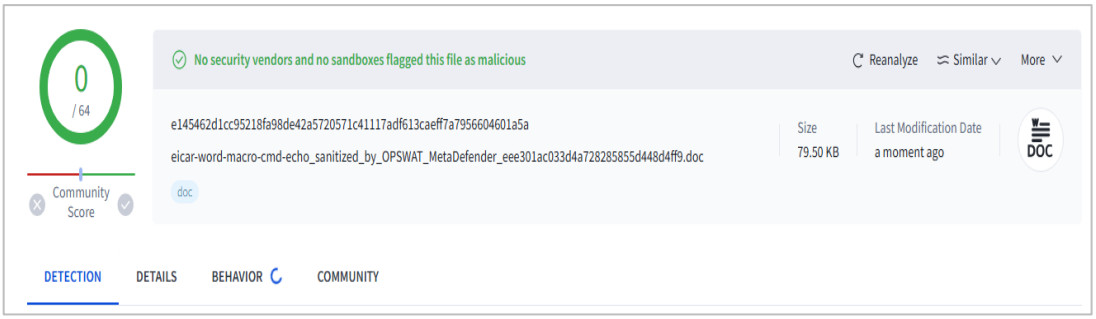


Figura 33- Resultado da análise do ficheiro Eicar-word-cmd-echo.doc no VirusTotal depois da limpeza

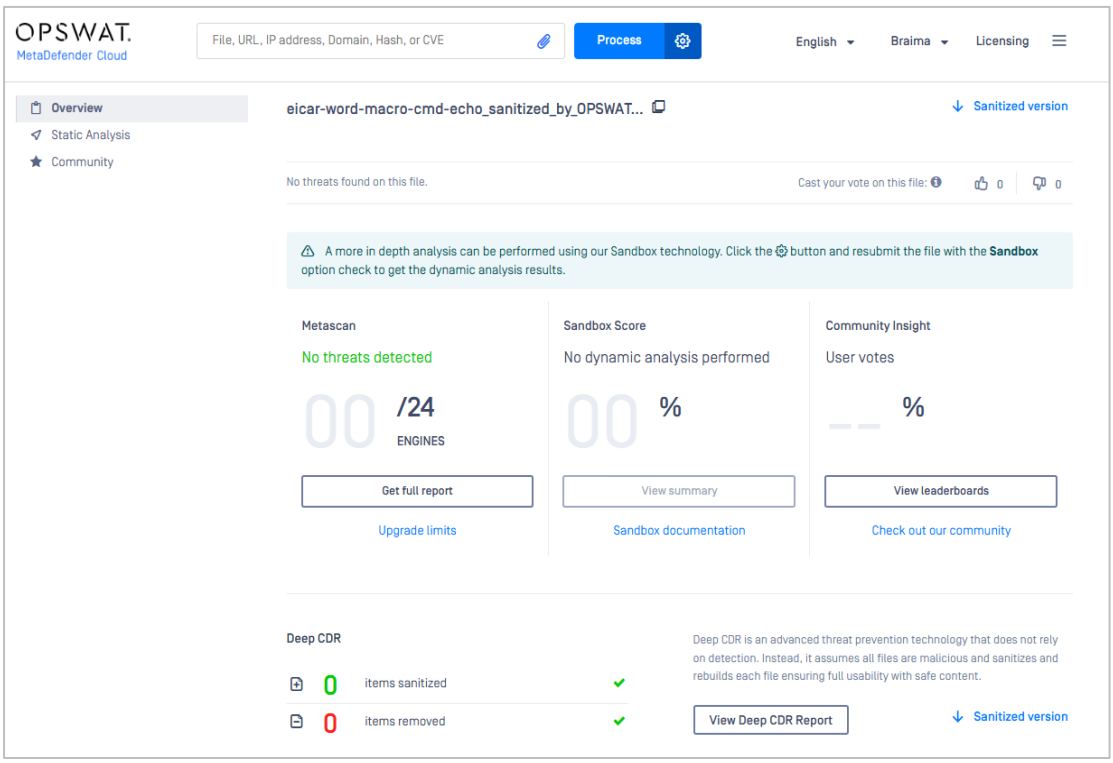


Figura 34- Resultado da análise do ficheiro Eicar-word-macro-cmd-echo.doc no Metadefender Cloud depois da limpeza

Anexo F: Exemplo 6 eicar-excel-macro-write-file.xls

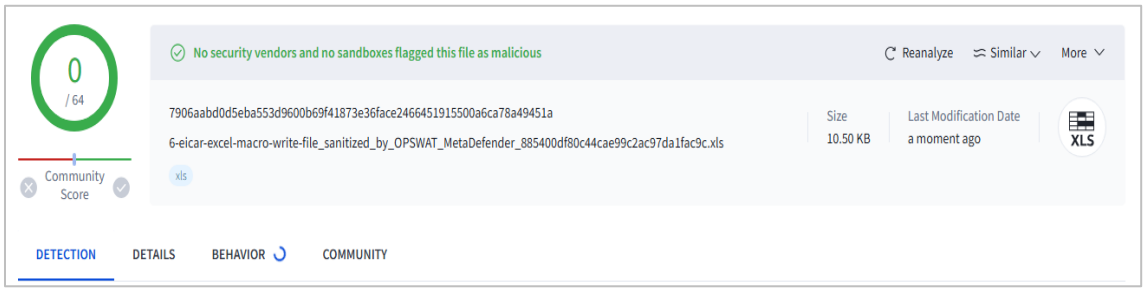


Figura 35- Resultado da análise do ficheiro Eicar-excel-macro-write-file.xls no VirusTotal depois da limpeza

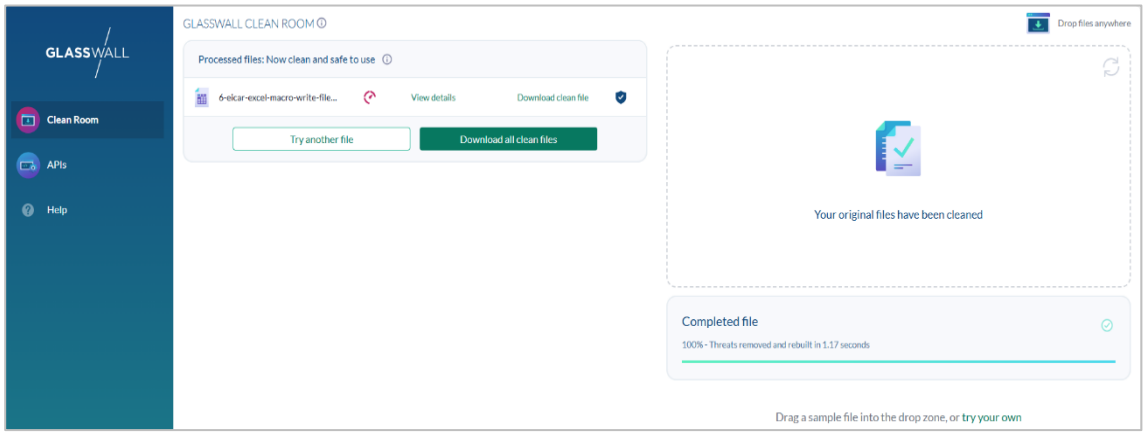


Figura 36- Resultado da análise do ficheiro Eicar-excel-macro-write.file.xls no Glasswall depois da limpeza

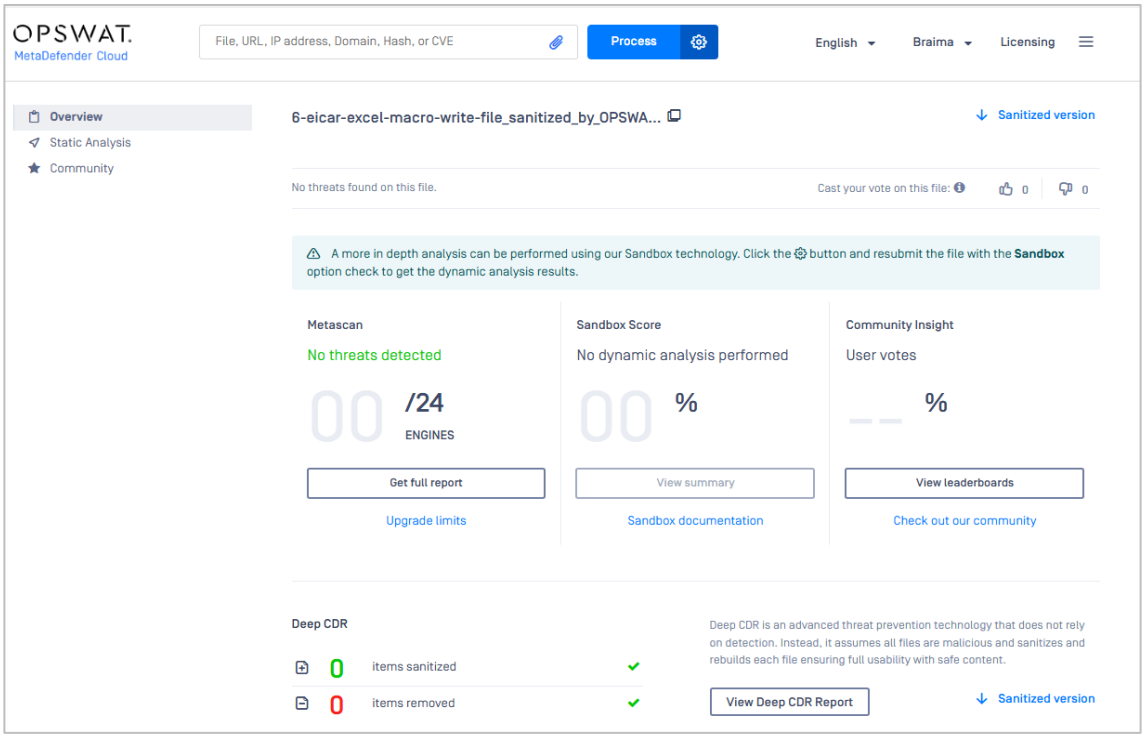


Figura 37- Resultado da análise do ficheiro Eicar-macro-write-file.xls no *Metadefender Cloud* depois da limpeza