Instituto Superior
de Contabilidade
e Administração
Politécnico de Coimbra

Instituto Superior
de Contabilidade
e Administração
Politécnico de Coimbra
COIMBRA BUSINESS SCHOOL
ISCAC.pt

Jorge Fernando da Cunha Coelho

Segurança em transferências de arquivos – A importância da limpeza de arquivos na sua transferência através de uma tecnologia Content Disarm and Reconstruction e a sua implementação

Coimbra, abril de 2024

Segurança em transferências de arquivos
Jorge Fernando da Cunha Coelho
ISCAC | 2024

Instituto Superior de Contabilidade e Administração
Politécnico de Coimbra
COIMBRA BUSINESS SCHOOL ISCAC.pt

Jorge Fernando da Cunha Coelho

Segurança em transferências de arquivos – A importância da limpeza de arquivos na sua transferência através de uma tecnologia Content Disarm and Reconstruction e a sua implementação

Trabalho de projeto submetido ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de **Mestre em Sistemas de Informação de Gestão**, realizada(o) sob a orientação do Professor Mário João Gonçalves Antunes e coorientação da Professora Isabel Maria Mendes Pedrosa.

Coimbra, abril de 2024

TERMO DE RESPONSABILIDADE

Declaro ser a autor deste projeto, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação do presente projeto.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

DEDICATÓRIA

Este trabalho é dedicado, com muito amor, ao meu filho Duarte, que nasceu após o término do primeiro ano letivo do mestrado, e à minha mulher Diana, que sem ela eu não seria metade do que sou hoje.

Para terminar o projeto, tive de prescindir de imenso tempo familiar que nunca mais será recuperado, por isso, se hoje termino este trabalho e se há alguém que merece esta dedicatória, porque um agradecimento não chega, é o meu filho e a minha mulher.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

AGRADECIMENTOS

A realização deste projeto e consequente conclusão do percurso académico em que ela está inserida, não seria possível sem o contributo de uma extensa lista de pessoas, ao qual eu deixo aqui presente um eterno agradecimento.

Primeiramente, à Professora Isabel Pedrosa e ao Professor Mário Antunes por me motivarem e encorajarem a terminar este projeto numa altura que o tempo era escasso, pela disponibilidade, simpatia e flexibilidade sempre demonstrada.

Agradecer à Loop pela flexibilidade e pelo apoio que proporcionaram. Depois aos meus colegas de trabalho, Francisco Nora e Jorge Pinheiro, por serem uns mentores para mim. Os vossos conselhos e ajuda em partes técnicas do projeto, na parte motivacional e gestão de tempo foram fundamentais.

Agradecer também aos meus amigos da Banda do Cercal, pela força e conselhos que me foram dando durante a realização do projeto.

Por fim, agradecer à minha família. Aos meus pais e irmão pelos esforços e sacrifícios que fizeram durante os meus percursos académicos, e que sempre que preciso me ajudam no que podem. Aos meus sogros e à minha cunhada Inês, pela ajuda que dão a mim e à Diana, para conseguirmos ter tempo para concretizar os nossos objetivos. À minha mulher Diana, que me dá a força que preciso para conseguir ir com tudo até ao fim e me mostrar que tenho mais valor dentro de mim do que julgo ter.

A todos, um obrigado é pouco.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

RESUMO

A cibersegurança tem um impacto, em crescendo, no quotidiano dos utilizadores dos sistemas de informação, pelo que, considera-se essencial conhecer, constantemente, o modo de proceder na sua defesa perante ataques de *ransomware*, *malware* ou *phishing*. As empresas assumem, de forma fulcral, a defesa dos sistemas de informação da gestão para o normal funcionamento e credibilidade no mercado, atendendo a que, é através destes sistemas que se processam todos os movimentos da atividade operacional, financeira e do pessoal, informação considerada crítica para os responsáveis pela área da cibersegurança. Os dados inseridos nos sistemas de informação são acessíveis aos utilizadores credenciados, existindo, amiúde, a necessidade de efetuar a sua transmissão entre diferentes sistemas, nomeadamente, através de envio de ficheiros pela Internet, facilitando o aumento do risco de violação e da probabilidade do seu desvio para entidades exteriores à rede, sem que qualquer dos utilizadores do sistema tome conhecimento da ocorrência. Acresce que, a receção de emails pelas empresas apresenta um sério risco de intrusão de terceiros na sua atividade, nomeadamente, na receção de um *curriculum vitae*, na realização de *download* de ficheiros e de programas alojados em repositórios não fidedignos. No sentido de facilitar a proteção, apresentam-se várias aplicações associadas à tecnologia Content Disarm and Reconstruction (CDR), que tem por finalidade a limpeza de ficheiros, integrando padrões potencialmente perigosos, antes da sua disponibilização aos utilizadores.

No presente projeto são testadas as capacidades da aplicação disponibilizada pela OPSWAT, o MetaDefender Cloud, para limpar um variado tipo de ficheiros e a sua disponibilização aos utilizadores, assegurando, que estes se encontram completamente limpos de potenciais fontes maliciosas. Visando permitir aos utilizadores dos sistemas de informação um acesso mais simples à aplicação, MetaDefender Cloud, foi criada uma interface gráfica de acesso à mesma, facilitando, assim, a admissão de vários utilizadores, em simultâneo, sem que nenhum deles tenha conta no MetaDefender Cloud.

Palavras-chave: Cibersegurança, CDR, *Malware*, Transferência de Ficheiros

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ABSTRACT

Cybersecurity has a growing impact on the daily lives of information systems users, so it is essential to constantly know how to defend against ransomware, malware, or phishing attacks. Companies take on the central role of defending their management information systems to ensure their normal functioning and credibility in the market, given that it is through these systems that all operational, financial and personnel movements are processed, information that is considered critical by those responsible for cybersecurity. The data entered the information systems is accessible to accredited users, and there is often a need to transmit it between different systems, namely by sending files over the Internet, which increases the risk of violation and the likelihood of it being diverted to entities outside the network, without any of the system's users being aware of it. In addition, the receipt of emails by companies poses a serious risk of third parties intruding on their business, particularly when receiving a curriculum vitae, downloading files and programs hosted in unreliable repositories. To facilitate protection, several applications associated with Content Disarm and Reconstruction (CDR) technology are presented, the purpose of which is to clean files of potentially dangerous patterns before they are made available to users.

This project tests the capabilities of the application provided by OPSWAT, MetaDefender Cloud, to clean a variety of files and make them available to users, ensuring that they are completely clean of potential malicious sources. To allow users of information systems simpler access to the MetaDefender Cloud application, a graphical interface was created for accessing it, thus making it easier to admit several users simultaneously, without any of them having a MetaDefender Cloud account.

Keywords: Cybersecurity, CDR, Malware, File Transfer

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ÍNDICE GERAL

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ÍNDICE DE FIGURAS

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ÍNDICE DE TABELAS

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Lista de abreviaturas, acrónimos e siglas

API – Application Programming Interface

ATP – Advanced Threat Protection

CDR – Content Disarm and Reconstruction

CNCS – Concelho Nacional de Ciber Segurança

CSPs – Cloud Service Providers

DFA – Deep File Analysis

EUA – Estados Unidos da América

HTML - HyperText Markup Language

ICAP – Internet Content Adaptation Protocol

IoT – Internet of things

MSPs – Managed Service Providers

OSS – Open Source Software

OT – Operational Technology

RPA – Robotic Process Automation

SaaS – Service-as-a-Service

SI – Sistemas de informação

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

INTRODUÇÃO

Ao longo dos anos, as mudanças nas tecnologias de informação têm levado a um aumento gradual da sua utilização por parte das pessoas. Tal pode ser constatado na Figura 1 com dados relativos a janeiro de 2024 (Kemp, 2024), onde mostra que em a esta data, havia cerca de cinco mil trezentos e quarenta e sete milhões de utilizadores em todo o mundo que usavam Internet, número mais alto registado desde 1990.

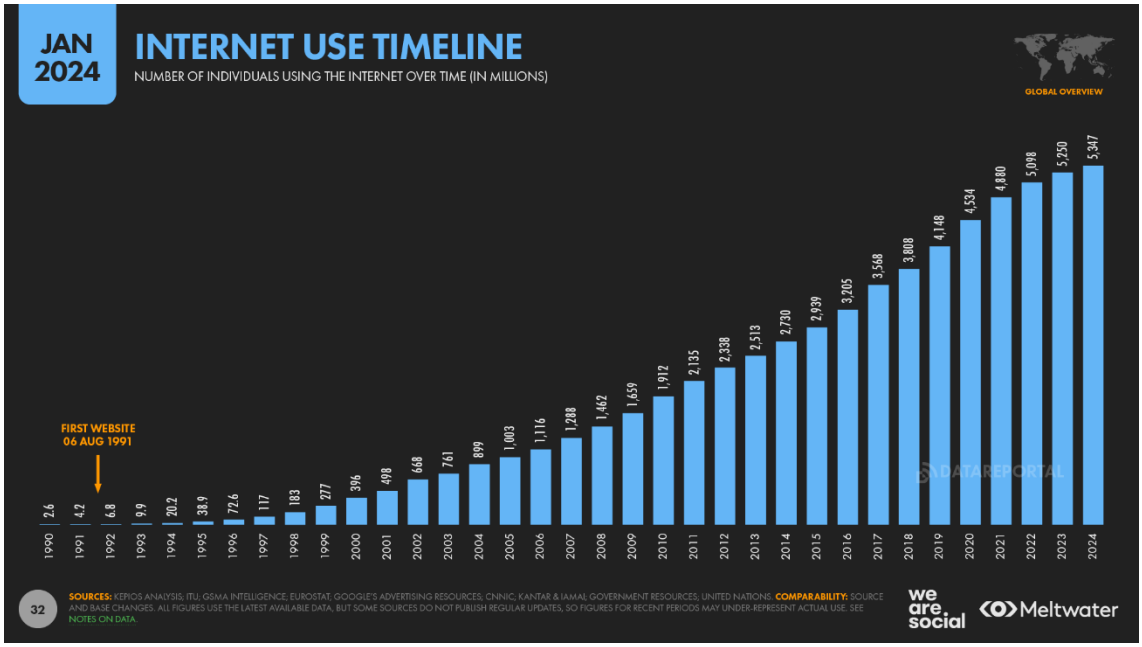

Figura 1 - Internet use timeline January 2023 DataReportal (Kemp, 2024)

Observando a Figura 2, podemos retirar algumas conclusões que ajudam a compreender o crescimento da utilização dos sistemas de informação (SI) e entender a importância da Internet para a população mundial. Os factos são demonstrados através das percentagens inscritas sob os tópicos da figura, mostrando o seguinte:

- Aproximadamente, dois terços da população mundial têm acesso à Internet.
- Mais de dois terços da população mundial tem, pelo menos, um telemóvel.
- Mais de metade da população mundial são utilizadores ativos de redes sociais.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

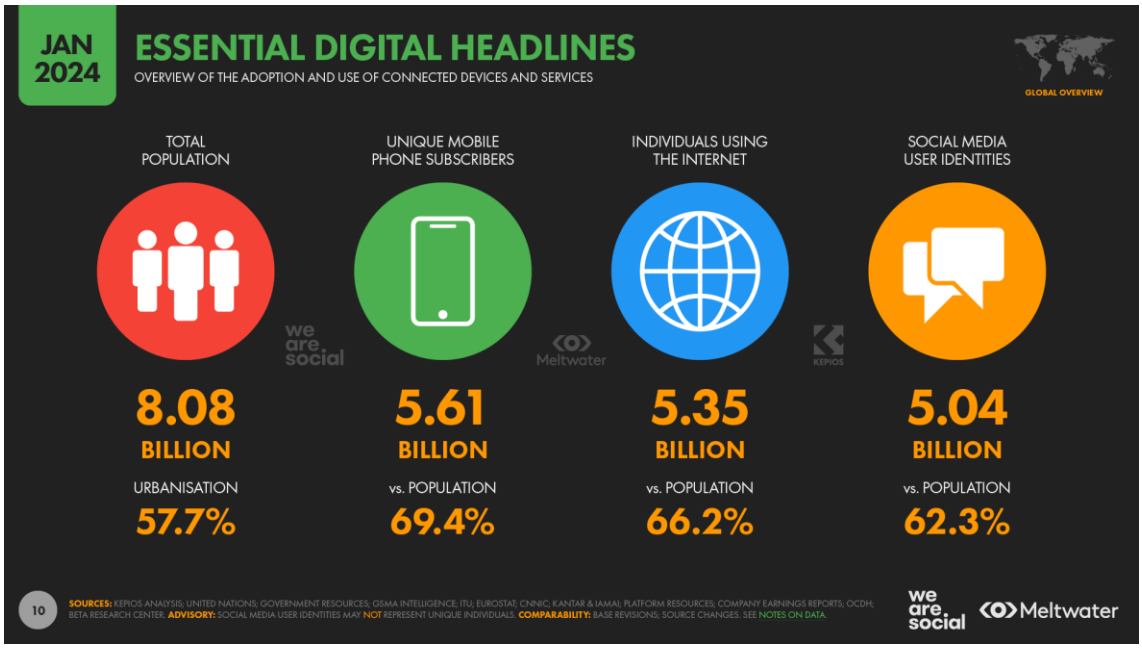

Figura 2 - Global digital headlines January 2024 DataReportal (Kemp, 2024)

Como em todas as vertentes da humanidade, no mundo cibernético também há quem tente, de um modo pouco ortodoxo, dificultar a vida às pessoas e às empresas, procurando contornar as leis para seu benefício, situação que se torna mais vulnerável e facilitada com o aumento da quantidade de utilizadores de Internet em todo o mundo, fator que induz a um aumento das falhas de segurança. Como forma de tentar combater esta variedade crescente de intrusos e intrusões, são postas em prática todos os dias várias normas de mitigação das tentativas de intrusão e exploração de vulnerabilidades por parte dos cibercriminosos.

O cibercrime, como um crime tradicional, é descrito pelo triangulo do crime (Lallie et al., 2021), especificando que para um cibercrime ocorrer têm de existir três fatores: uma vítima, um motivo e uma oportunidade. Estes fatores estão em sintonia e podem traduzir-se num ataque que prejudique, de qualquer forma, um indivíduo ou uma empresa.

Nos dias de hoje é fácil encenar uma oportunidade para explorar as fragilidades da vítima, sem saber que está a ser trapaceada. Este facto foi particularmente relevante durante a pandemia provocada pelo COVID19, em que os ataques aumentaram cerca de 300% (Wetzig, 2022), e que obrigou a que o trabalho remoto fosse exigido em grande parte das empresas. Isto deve-se à reduzida literacia em cibersegurança e à falta de perceção do

risco cibernético em grande parte das empresas e pelos utilizadores de SI. A literacia em cibersegurança foi estudada por (Mee et al., 2021), onde foram analisados quarenta e nove países e a União Europeia, situando Portugal em 25º no contexto geral, identificado na Figura 3 extraída do estudo.

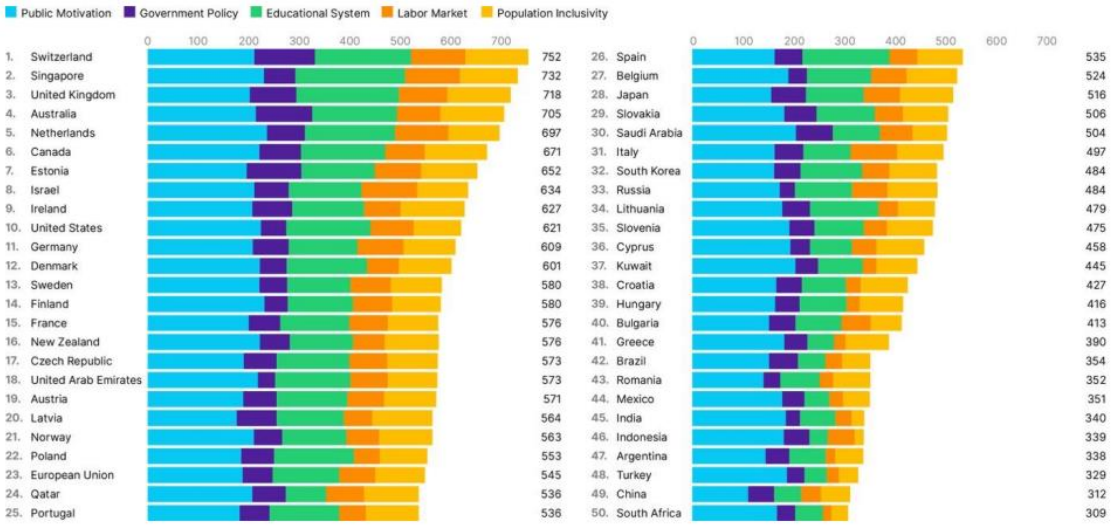

Figura 3- Ranking de literacia sobre Cyber Risk (Mee et al., 2021)

Face ao apresentado, pode ser extraído o parecer que no âmbito da cibersegurança, Portugal ainda tem imenso trabalho a desenvolver para atingir um nível de desenvolvimento que permita uma diminuição acentuada do risco na utilização dos SI. Neste contexto, revela-se necessário que os utilizadores tenham a noção que um simples clique num *link* ou o *download* de um ficheiro adulterado pode ter consequências nefastas tanto para o próprio, como para a organização onde se insere.

O cibercrime está dividido em dois tipos de crime (*Cps.Gov.Uk*, 2019), o crime *cyber-dependent* e o crime *cyber-enabled*, como se demonstra através da Figura 4 e se sumariza de seguida.

Os crimes *cyber-dependent* são cometidos apenas pelo meio do uso de Tecnologia da Informação e Comunicação (TIC), onde o dispositivo serve tanto como ferramenta para cometer o crime, como de arma para o crime. Ou seja, são ataques aos próprios computadores, tornando-os incapazes para certas tarefas ou até mesmo bloqueando-os.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Os crimes *cyber-enabled* são os crimes mais tradicionais. Este tipo de crime pode ser realizado quer em larga como em curta escala ou alcance, com o recurso a ferramentas apropriadas para o efeito e que procuram causar crimes contra as pessoas e não necessariamente com impacto nos computadores como por exemplo a extorsão, o uso de códigos bancários e o roubo de identidade.

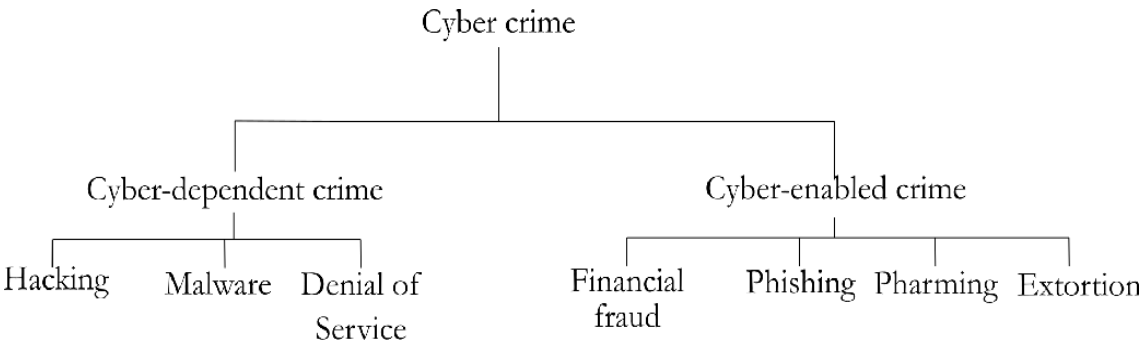

Figura 4- cyber-dependent and cyber-enabled crimes (Lallie et al., 2021)

Estes crimes podem ser originados através do *download* de ficheiros que se encontram disponíveis na Internet, sendo de fácil acesso para quem os quer aceder. Aqui é criada uma oportunidade para que os crimes sejam cometidos através do *malware* injetado no ficheiro. Nesta circunstância, também é possível a sua origem resultar de cliques em *links* não fidedignos que podem ser enviados por email, por mensagens SMS e ainda através das redes sociais, mais conhecidos como *spam,* no caso de serem contactos não solicitados e evasivos, ou *scam* no caso de tentarem defraudar quem recebe este contacto.

Malware é um acrónimo que deriva de duas palavras inglesas: "*malicious"* e *"software*" que na sua tradução, entendemos como software malicioso. A transferência deste tipo de ficheiros é um dos métodos mais comuns, e uma das mais sérias ciberameaças, utilizadas pelo cibercriminoso para efetuar um ciberataque (Gibert et al., 2021). O método consiste em enviar num programa uma parte do código que corresponde ao que, na gíria, se designa por vírus informático. Esta parte do código, quando executada, provoca, normalmente, situações ameaçadoras à integridade do computador e dos seus programas, sem que o utilizador se aperceba que o está a executar.

Grande parte dos ficheiros que provêm de *third party applications*, como por exemplo *secure file transfers*, portais *web* ou soluções de isolamento, podem pôr em risco o nosso

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

computador, a partir do momento em que são considerados como confiáveis e ultrapassam, assim, as camadas de segurança da empresa (Sasa Software, n.d.).

Em Portugal, os cibercrimes registados têm evoluído a uma velocidade incrível, não obstante, muitos desses escaparem à condição de registo. O Centro Nacional de Cibersegurança (CNCS), criou o CERT.PT (CNCS, 2023), cujos dados relativos aos registos que esta entidade teve entre os anos de 2015 e 2022, são detalhados na Figura 5. Estes dados mostram que os incidentes têm vindo, constantemente, a aumentar. A partir do ano de 2020, o CERT.PT começou a contar como incidente não só o incidente em si, como as vulnerabilidades detetadas por eles.

Figura 5- Incidentes registados pelo CERT.PT entre 2015 e 2022 (CNCS, 2023)

Todos os dias existem novas variantes de *malware*, que são desenhadas de acordo com o seu alvo (Sim, 2018). Algumas variantes podem ser reconhecidas pelos antivírus tradicionais, porém outras não são detetadas, o que faz com que a aposta em tecnologias com a filosofia de "*zero trust"* seja o caminho certo a trilhar para a segurança dos utilizadores de SI e das empresas.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Contextualização do Problema

Em 2020, mais de 70% de anexos de emails maliciosos ou *links*, e cerca de 30% dos *downloads* maliciosos foram distribuídos através de PDF, Word, Excel e PowerPoint (*What Is Content Disarm and Reconstruction*, 2024), fatores que induzem à necessidade de aumentar o nível da investigação para que este tipo de ameaça não afete o quotidiano dos utilizadores de SI e das empresas.

Outro dado relevante apresenta que, em 2016, estimava-se que 95% das violações de dados eram causadas por erro humano, principalmente através de cliques em *links* existentes em email relacionados com burlas ou *scam* (Wetzig, 2022). Apesar da contínua educação dos colaboradores das empresas e dos utilizadores de SI, cerca de 27% destes ainda são vítimas de ataques de *phishing* ou engenharia social (Votiro, 2022). Segundo (Wetzig, 2022), 43% de todos os ciberataques são direcionados a pequenas empresas, que são porventura as que têm menos capacidade para investir na sua segurança.

Perante o comportamento inapropriado que se manifesta no universo dos utilizadores de SI, a segurança da empresa passa a ser um grande desafio, cuja garantia não se apresenta sólida somente pela utilização dos antivírus tradicionais. Ao longo do tempo, vão sendo criadas, novas variantes de vírus e novas metodologias de ataque que os antivírus não identificam e não conseguem detetar, gerando, assim, uma janela de oportunidade para os ataques cibercriminosos.

Estas ameaças geram, indiscutivelmente, uma grande preocupação quando se trata de aspetos de cibersegurança. O rápido crescimento do volume de dados e a evolução dos ciberataques determinam a exigência de respostas rápidas para a salvaguarda das informações pessoais e dos negócios (Goutam, 2015). Ao longo do tempo, o ciberespaço, irá continuar a evoluir e os utilizadores dos SI tendem a tornar-se, cada vez mais, dependentes dos serviços e das conveniências que estes fornecem (McDuffie & Piotrowski, 2014). Esta situação causa, quer às empresas como aos utilizadores de SI, uma dependência obrigatória da cibersegurança para proteção das infraestruturas críticas, das quais dependemos no dia a dia. Os serviços financeiros são os principais alvos de

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ciberataques através de *malware*, porém, qualquer utilizador de SI pode ser vítima destes ataques (Phạm et al., 2021).

O website `transparencymarketresearch.com` disponibiliza dados relativos a um questionário efetuado, pela empresa Ponemon, a três mil empresas, onde cerca de metade delas admitem que sofreram algum tipo de exfiltração de dados nos últimos dois anos. Cerca de 34% das que sofreram estes ataques, tinham conhecimento da ocorrência, contudo, nada fizeram para resolver a questão. A esta mentalidade, exige-se que seja alterada para que as empresas um dia possam ter sucesso e não serem mal vistas pelos seus *stakeholders* (*Global Content Disarm and Reconstruction (CDR) Market*, 2023).

Motivação para o estudo

Após quatro anos de experiência no desenvolvimento de várias soluções para empresas como a Gesfrota, The Loop Co., Worten e atualmente Millenium BCP, como Full Stack Developer, e uma pós-graduação em cibersegurança, concluída com sucesso na Coimbra Business School, considera-se pertinente trabalhar no envolvimento e enquadramento de ambas as áreas, no sentido de acrescentar valor aos trabalhos realizados, quer individualmente, quer em equipa. Este desiderato visa incrementar a valorização da segurança nas várias aplicações que são desenvolvidas por mim e pela minha equipa.

Atualmente, encontro-me a prestar serviço na modalidade de *outsoursing* ao banco Millenium BCP, integrando o quadro de pessoal da empresa The Loop Co. De momento, as fontes de conhecimento e o investimento em cibersegurança por parte da Loop são essenciais, integrando, esta área de ação, um dos pontos do plano anual da empresa, tendo por objetivo incutir uma melhoria nas infraestruturas de defesa nas redes atuais e no conceito de cibersegurança nos colaboradores. Com exíguo conhecimento no âmbito de redes de SI, procuro sempre incutir o reforço de cibersegurança através de técnicas ou aplicações que ajudam a melhorar as defesas da empresa e dos seus projetos. A criação de um plano para eventuais ataques e o incremento da formação dos colaboradores na área da cibersegurança, apresenta-se como uma âncora para evitar situações menos agradáveis, face ao aumento do número de colaboradores e das tipologias de projetos existentes.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Como sempre procurei desenvolver mais o conceito de cibersegurança, pode ser para mim uma aposta trabalhar numa área que gosto e na qual apresento o presente projeto.

Objetivos do Projeto

Os custos reputacionais de uma falha de segurança resultam, normalmente, em mudanças persistentes nas políticas e operações das empresas, que só podem ser apanhadas pela observação da reação dos mercados no longo prazo (Tosun, 2021). Esta é uma das ideias para que todo o agente que tenha contacto direto com uma empresa deve ter presente. O impacto das ações de cada um dos colaboradores pode ter um grande impacto na empresa, independentemente da sua dimensão. Em 2012, milhões de emails e passwords foram exfiltrados do LinkedIn, e apenas em 2016 esse facto foi descoberto. No entanto, ao contrário das boas normas de cibersegurança, a maior parte dos utilizadores proprietários das contas envolvidas no caso, ainda tinham a mesma password (Lallie et al., 2021). O resultado desta ação adveio da enorme quantidade de pessoas que foram expostas à receção de mails de *phishing, blackmail* e contas comprometidas com publicações de *phishing*.

Em 2016, cerca de 95% das violações de dados foram causadas por erro humano (Wetzig, 2022), o que faz com que as empresas tenham de investir ainda mais na qualificação dos seus colaboradores. Apesar das lutas organizacionais com a educação e qualificação dos colaboradores, cerca de 27% dos funcionários de uma organização falham em ataques de *phishing* ou engenharia social (Votiro, 2022).

Algumas tendências como IoT, *cloud*, redes sociais, ou *Big Data* estão fortemente implementadas no mundo digital, o que faz com que o cibercriminosos tenham oportunidade de explorar e expor vulnerabilidades que não são protegidas nem identificadas pelos utilizadores (Hussain et al., 2020). Atualmente, cerca de 80% das violações bem-sucedidas são de "*zero-day exploits*", que não são reconhecidas pelas tradicionais soluções de deteção baseadas em assinaturas (Phạm et al., 2021). Como prevenção para este problema as empresas podem contratar ou implementar no seu contexto empresarial *white hats*, ou *ethical security hackers*. Estes *hackers* usam

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

habilidades de *hacking* para identificar vulnerabilidades de segurança em *hardware*, *software* ou redes(Caldwell, 2011).

Visando contribuir para a pesquisa de uma melhor solução para as nossas empresas, e que estas se apresentem bem cotadas na tendência para a eliminação e obstrução ao erro dos colaboradores, na vertente relativa à defesa em ambiente digital, pretende-se desenvolver uma investigação ao CDR e em que âmbito este pode ajudar na defesa de uma empresa e das pessoas. Contudo, o presente estudo não irá evitar em pleno que os colaboradores, visitantes e outros intervenientes na atividade da empresa cometam o erro de abrir um *website* malicioso, mas, pretende-se que tenda a ajudar a prevenir que uma pessoa faça um *download* de um ficheiro malicioso, mesmo que este ficheiro não seja suspeito à primeira vista.

O objetivo específico assenta em aprofundar o conhecimento sobre a tecnologia de segurança CDR, identificar e explorar algumas aplicações existentes no mercado, e saber em que ambientes as mesmas funcionam. No desenvolvimento do trabalho, procura-se determinar quais as aplicações que melhor se adaptam a ambientes locais ou se já existem integrações destas em micro serviços para ambientes *cloud*, se alteram muito os ficheiros quando os desconstrói para remover potenciais vírus, e se resultam de uma implementação viável para as empresas.

O desenvolvimento do projeto incide, também, numa pesquisa sobre aplicações que funcionam em tecnologia *open source* e que se manifestem úteis para a utilização de pessoas singulares, tendo assim, uma ferramenta de defesa contra os ficheiros provenientes da *web* ou do *email*, caracterizando-se por serem programas que não têm custo para o utilizador.

Metodologia

Para a realização do presente projeto, promoveu-se um estudo sobre a temática para averiguar e entender quais os problemas que apresentavam neste âmbito. Tendo por base o problema encontrado, foi proposto desenvolver uma aplicação que assumisse a condição de solução para o problema.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Após se identificar que a transferência de ficheiros pode sobrevir num problema para as empresas e utilizadores comuns dos SI, efetuou-se a escolha das tecnologias que contribuem para a resolução do problema emergente da pesquisa. Estas tecnologias foram executadas, no caso do CDRFileCleanApp, e desenvolvida a sua comunicação com a aplicação MetaDefender Cloud.

Para a sua conclusão, foi necessário proceder à recolha de ficheiros com algum tipo de vírus, a fim de criar um ambiente de testes. Os testes apresentam-se necessários para garantir que a interface desenvolvida e a comunicação com a aplicação MetaDefender Cloud, se encontra em conformidade com o pretendido.

Os testes realizados reproduziram vários resultados que foram recolhidos e analisados, averiguando assim a viabilidade, tanto da interface que criámos, como da aplicação que estamos a usar para limpar os ficheiros.

Contributos esperados

Com a realização deste projeto pretende-se contribuir, de forma positiva, para a implementação de boas práticas na área da cibersegurança em ambiente empresarial e ambiente pessoal. No final do projeto espera-se que seja mais fácil a integração de uma ferramenta de segurança na transferência de ficheiros como é o CDR.

Será desenvolvida uma interface em Blazzor, que tem como propósito dar acesso a mais que uma pessoa à mesma API Key disponibilizada para uma conta da aplicação MetaDefender Cloud. Neste ambiente, uma pequena empresa não tem de estar a criar várias contas para cada um dos utilizadores.

Os desenvolvimentos aplicados poderão, futuramente, receber melhorias, tanto no desempenho, como na experiência do utilizador, podendo ainda, ser sujeito a uma melhoria na sua automatização, sendo, nesse sentido, necessário entregar o ficheiro para *upload*, e sem mais nenhuma ação complementar, haver uma devolução do ficheiro por parte da aplicação, assim como, uma apresentação dos resultados quando estes estiverem disponíveis na API.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Organização do Documento

O presente projeto encontra-se parcelado em quatro capítulos. O primeiro capítulo irá apresentar o desenvolvimento do estado da arte para conhecer melhor a metodologia em que vamos trabalhar, criar linhas para nos guiarmos durante o projeto e entender o básico do seu funcionamento.

No segundo capítulo, será tratado o cerne da metodologia que pretende estudar, concetualizando e desenvolvendo a metodologia CDR, os seus princípios, que componentes integram os programas que seguem esta metodologia, e como é a sua integração nos sistemas de segurança. O estudo irá também incidir sobre desenvolvimentos das técnicas que existem, as vantagens e desvantagens de um CDR, analisar alguns programas OSS e outros que existam no mercado para empresas.

No terceiro capítulo, objetiva-se a implementação da solução, que deverá recair sobre a que apresente maior viabilidade, em resultado do seu estudo efetuado no capítulo anterior, sendo explicado os critérios usados para a sua escolha e fazendo a sua instalação.

No quarto capítulo, serão apresentados os testes à aplicação, será efetuada a recolha dos resultados e a análise dos mesmos.

Conclui-se o estudo com a enunciação dos contributos orientados para o trabalho, das limitações emergentes durante o seu desenvolvimento e projetando a realização de trabalhos futuros esperados para o desenvolvimento da temática tratada.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

1 ESTADO DA ARTE

Tendo por objetivo fundamentar perceção sobre a problemática da transferência de ficheiros e da segurança no meio cibernético das pessoas e daquilo que as rodeia, e com o objetivo de alicerçar o pilar principal do estudo que serve de base ao presente projeto, foi efetuada uma pesquisa bibliográfica sobre o foco principal do projeto (CDR) na base de dados de artigos científicos SCOPUS.

Para a pesquisa dos documentos, construímos uma *query* que deu assim origem à seguinte pesquisa:

```
TITLE-ABS-KEY ("Content disarm and reconstruction")
```

O resultado da pesquisa não foi o esperado, pois apenas foram obtidos dois artigos, ambos do mesmo autor, o que impossibilita a realização de um debate sobre o estado da arte com a profundidade, objetividade e fiabilidade desejado.

Após as análises dos artigos encontrados na pesquisa anterior (Dubin, 2023a, 2023b), foi possível extrair duas *keywords*, servindo estas de base para a realização da investigação desejada. São elas:

- PDF
- *malware*

Nesta conjuntura, com estas *keywords*, utilizadas por Dubin em ambos os artigos relacionados com a tecnologia *Content Disarm and Reconstruction* e com o elemento da "Cibersegurança", um conceito que deve estar presente em todos os assuntos relacionados com a transferência de ficheiros *online* e na sua proteção contra infeções, que possam resultar deste procedimento. Foi realizada, deste modo, a pesquisa na plataforma SCOPUS com a seguinte *query*:

```
TITLE-ABS-KEY((("Content Disarm and reconstruction") OR PDF OR malware) AND Cybersecurity)
```

Com esta *query* de pesquisa foram obtidos um total de mil setecentos e setenta documentos, situação que contribui e possibilita a realização de um estudo mais aprofundado do estado da arte. Esta conjugação de pesquisas permite que a discussão não

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

se restrinja estritamente ao tema CDR, tendo em consideração a falta de bibliografia sobre este tópico, conforme notado anteriormente, incluindo estes novos elementos no estudo, PDF e *malware*, introduzem-se novos componentes que carreiam para a discussão matéria suficiente e significativa para o tema a desenvolver, contribuindo assim, para uma dissertação mais abrangente da temática.

Após a extração do ficheiro RIS dos documentos encontrados na pesquisa, utilizou-se o programa VOSviewer para estudar a ligação entre os termos mais frequentes dos artigos que foram selecionados.

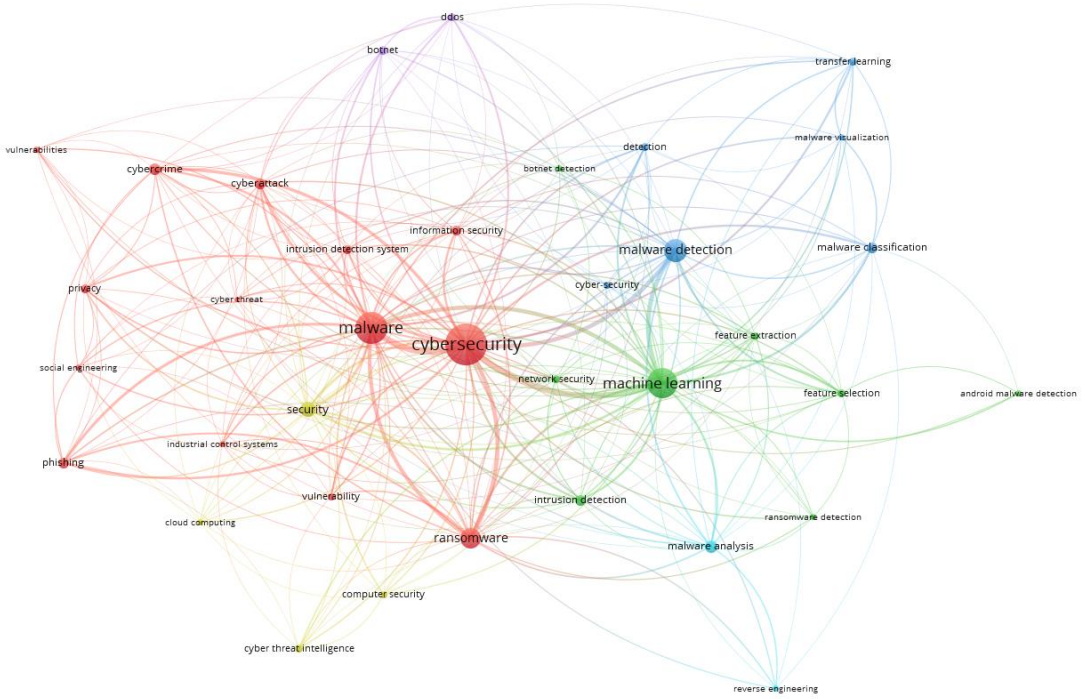

Figura 6- Resultado de pesquisa VOSViewer

Após a análise do grafismo fornecido pelo VOSviewer presente na Figura 6, constata-se que a palavra "*Cybersecurity*" é o conceito mais vezes reiterado nos artigos em questão, sendo o vocábulo que denota maior importância nos artigos analisados. A cibersegurança é o conjunto de ferramentas, políticas, conceitos, salvaguardas, diretrizes, abordagens na gestão de risco, treino, boas práticas, garantia e tecnologias que podem ser usadas para proteger o ciberambiente, a organização e os seus ativos (Goutam, 2015; Von Solms & Van Niekerk, 2013).

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Desta enunciação é possível inferir quanto se reveste de importante o conceito de cibersegurança no contexto em que são tratados os temas relacionados com transferência de ficheiros através da Internet, principalmente, quando estes provêm de fontes inseguras.

A temática da segurança deve ser levada a sério pelos utilizadores de SI, para que o esforço dos elementos que desenvolvem a pesquisa focada na segurança dos sistemas, não resulte em vão. Casos como o *cyber-bulling*, fraudes *online*, pornografia, roubo de identidade, e o *gambling* aumentaram consideravelmente devido à falta de consciência e do mecanismo de proteção dos utilizadores de Internet (Rahman et al., 2020).

Revela-se pertinente retirar desta análise que os conceitos "*Malware*", "*Malware detection*", "*Machine learning*" e "*Ransomware*" se interligam de forma significativa com outros vocábulos utilizados nos artigos. Neste enquadramento, torna-se exequível conferir algum destaque ao conceito "*Malware Detection"* em razão deste se apresentar como um dos temas objeto de análise infra. A discussão do tema não se foca, inteiramente, na deteção de *malware*, porquanto, o modo de funcionamento do sistema não é na base da deteção, mas, da confiança, extraindo o *malware* sempre que este seja reconhecido no momento da limpeza dos ficheiros.

Salienta-se também o conceito "*Security"*, o qual, juntamente com os termos supramencionados, apresenta uma importância significativa na interligação que se produz entre o conjunto de conceitos manifestos em todos os *clusters*. O conceito "*Security*" apresenta-se nestes artigos, de modo constante, a par da palavra "*CyberSecurity*", denotando um natural entendimento sobre esta situação, na medida em que um conceito se encontra, parcialmente, interligado ao outro, pelo que um representa o ambiente como um todo e o outro encontra-se mais associado ao ambiente digital.

Após a análise do grafismo desenvolvido pelo VOSViewer, nota-se que apesar de não serem encontradas publicações com significado relevante sobre a tecnologia CDR, foi possível encontrar várias referências a outros temas, mais abrangentes e com considerável interesse para a elaboração do presente trabalho. Num determinado prisma, todos os conceitos supramencionados servem de fundamento à existência da tecnologia CDR,

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

conjugando-se para o combate ao *cybercrime* através da prevenção e limpeza de ficheiros, estejam eles contaminados ou não com algum *malware* ou *ransomware*.

Face ao exposto, pretende-se a realização de uma pesquisa mais alargada sobre o tema com base em artigos disponibilizados na plataforma Google Scholar, os quais, conjugados com os disponibilizados pelo SCOPUS, se manifestaram basilares para o início da discussão do tema. Também será realizada uma pesquisa a *websites* fidedignos, principalmente de empresas desenvolvedoras de CDR e fóruns destas, de modo a obter uma base sustentável para o desenvolvimento da investigação proposta.

O CDR é uma metodologia proativa que extrai ameaças aos vetores de ataque dos documentos e ficheiros *media* (Dubin, 2023b). Esta metodologia funciona como uma camada de segurança, baseada em confiança zero para o sistema onde está implementado, seja localmente ou na *cloud*. Para mitigar efetivamente o *malware* e o risco que se corre em MSPs e CSPs, é preciso incorporar métodos de deteção como antivírus e *firewalls*, bem como soluções de prevenção como as ATP, proteção de *endpoint* e o filtro através da tecnologia CDR (*Sunshine2021*, n.d.). Alguns testes de deteção dos melhores antivírus mostraram que a melhor solução de defesa do mercado não é o suficiente para que um sistema esteja totalmente protegido (*Malware Protection Test March*, 2023), reforçando assim a utilização desta camada em sistemas que tenham um grande fluxo de transferência de ficheiros.

Existe também uma grande importância na atualização destes programas, para melhorar *scripts* de reconhecimento que possam ser corridos para que os ficheiros que contenham *malware* sejam mais fáceis de detetar, no caso de não ser reconhecido no meio do ficheiro. Como o ficheiro é totalmente desmontado e lido pelo programa, este pode não estar suficientemente capaz de detetar algumas intrusões que estejam escondidas no meio do código, limitação que advém do grau de desenvolvimento do programa. Neste contexto, exige-se uma permanente atenção sobre as últimas versões de atualização, quer do gestor de transferências de ficheiros, quer dos antivírus que acumulem funções com o CDR.

No desenvolvimento da pesquisa, foi efetuada uma procura rápida em algumas bases de dados estatísticas, e no site Statista (Petrosyan, 2023), foi encontrado um relatório com

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

dados baseados no Software de deteção Checkpoint (*CheckPoint*, 2024), apresentado na Figura 7. Este relatório revela que os programas executáveis são os mais explorados (57%) para transmitir vírus através de *download* efetuados no browser, com os ficheiros PDF e .dll a ficarem bastante longe (com 10% e 8% respetivamente). Na utilização de email para envio de documentos, os ficheiros .doc destacam-se em primeiro lugar (35%), seguindo-se logo atrás os executáveis (26%) e os PDF (22%), e com uma percentagem significativa, surgem ainda os .xls (17%).

File type	Web	Email
exe	57%	26%
pdf	10%	22%
dll	8%	-
xls	5%	17%
lnk	4%	2%
ps1	3%	-
jar	2%	-
doc	1%	35%
xlsb	1%	-
html	1%	0.8%
vbs	-	0.6%
xlsm	-	9%
ppt	-	1%

Figura 7- Rating de ficheiros maliciosos recebidos via email em 2022(Petrosyan, 2023)

Os dados presentes na Figura 7, podem indicar que a maior parte dos executáveis que estão disponíveis na *web* são maliciosos, o que não é totalmente correto, pois se o *download* do executável for feito através de distribuidores autorizados para o efeito, a percentagem é mais reduzida.

Quanto aos ficheiros recebidos através do email, a sua diversificação e origem são mais amplas, situação que pode dificultar a ação dos utilizadores dos SI, por motivos de desconhecimento ou perceção sobre o carácter fidedigno do remetente, confiando no que

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

lhes foi enviado e acabando por abrir uma porta ao cibercrime quando fizer o download daquele ficheiro.

A deteção de *malware* nestes ficheiros por um antivírus está limitada ao nível de desenvolvimento dos mesmos. Contudo, o que os antivírus não reconhecem, eles não são capazes de defender nem transmitir a informação de que o ficheiro está corrompido ou não (Dubin, 2023a). Desta forma seria preciso uma primeira linha de segurança baseada em confiança zero para evitar a infeção de sistemas através de vírus que são desconhecidos dos antivírus.

Porém, a perfeição ainda não é um atributo do sistema de CDR, devido à existência de um código malicioso embutido nos ficheiros que pode não ser executável. Esta situação pode motivar a que a limpeza do ficheiro não seja executada em pleno quando o código malicioso se encontre presente, levando o CDR a pensar que este seja código passivo, determinando que esta tecnologia não seja totalmente eficaz (Wiseman, 2023).

Autor	**Título do Artigo**	**Contributos**
Yehudah Sunshine	The rise of MSP & CSP vulnerabilities	Estudo sobre defesas e mitigação de risco dos *service providers*
Ran Dubin	Content Disarm and Reconstruction of PDF Files	Descrição pormenorizada sobre CDR de ficheiros PDF, como são construídos e os perigos existentes, através de um estudo sobre a aplicação PdfCDR.
Ran Dubin	Content Disarm and Reconstruction of RTF Files a Zero File Trust Methodology	Introdução à metodologia *zero trust*, o que representa para um CDR, e como a aplicação pode atuar num ficheiro RTF.

Tabela 1 - Tabela de principais contribuidores do estado da arte

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Na Tabela 1, mencionam-se os autores que mais contribuíram para este estado da arte, por terem desenvolvido trabalhos sobre uma aplicação que se encontra embrionária no seu estudo, contribuindo de forma meritória para impulsionar o avanço na investigação sobre o CDR, e para incrementar a vontade de investigação deste tema a uma comunidade científica mais alargada.

Em suma, o CDR é reconhecido como sendo um dos grandes meios de segurança para as empresas, não se encontrando dependente da deteção de algum tipo de *malware* existente num ficheiro, este irá ser na maioria das vezes limpo pela aplicação. Com base na revisão apresentada anteriormente, considera-se que ainda existem desafios a considerar para um maior desenvolvimento desta ferramenta científica, salientando-se a investigação sobre a presença do código passivo que não é removido por não ser reconhecido como malicioso.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

2 FUNDAMENTOS DE CDR

O *Content Disarm and Reconstruction* (CDR) é uma tecnologia avançada de limpeza de ficheiros e prevenção de ameaças que não se baseia na deteção, pois segue a filosofia de confiança zero. Segundo o CISA(Security Agency, 2023), o modelo confiança zero tem cinco pilares, que podem ser constatados na Figura 8, e no qual as organizações se podem basear, adaptando-os às suas necessidades de proteção. São eles:

- **Identidade** – refere-se aos atributos que unicamente descrevem os utilizadores ou entidades que podem introduzir risco se não forem geridos adequadamente. Neste caso é preciso limitar acessos conforme a identidade do utilizador para haver um menor risco de exposição do sistema.
- **Dispositivo** - que inclui *hardware*, *software* e outros componentes que possam auxiliar um potencial ataque. A ligação entre estes componentes deve ser segura para que a superfície de ataque seja limitada.
- **Rede** – são potenciais canais de risco para intrusões no sistema se não forem controlados adequadamente. Esta deve ter várias camadas de segurança para que seja mais difícil efetivar qualquer ataque que seja tentado.
- **Aplicação** – Aplicações ou áreas de trabalho que inclui sistemas, programas e serviços em execução permanente, serviço móvel e a *cloud* podem conter vulnerabilidades que põe em risco os dados se estes não forem geridos apropriadamente. Estes devem ser seguros, com várias camadas e limitação de acessos para que a superfície que possa ser afetada seja limitada.
- **Dados** – Qualquer tipo de dados num sistema, em rede, aplicações, bases de dados, infraestruturas e *backups* com metadata associada pode introduzir risco, como acesso não autorizado se a devida proteção não for aplicada. Deve haver o mínimo de privilégios para ter acesso a estes dados críticos e aplicar uma boa segurança para o acesso a estes.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

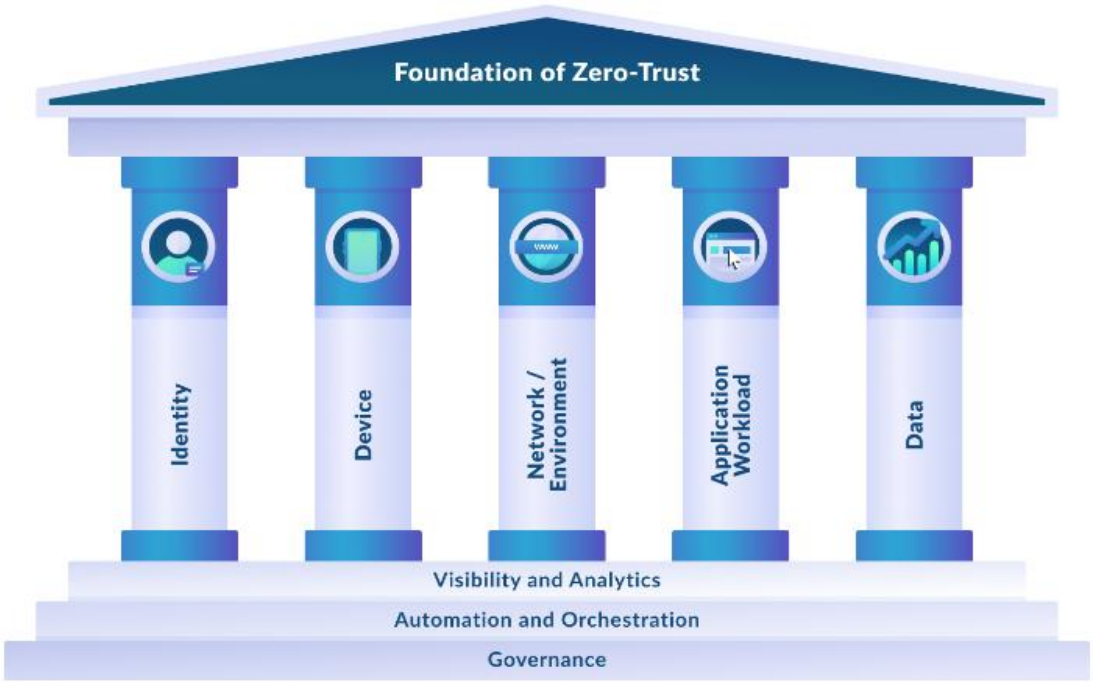

Figura 8- Foundation of zero-trust (David Tutin, 2023)

Com base neste tipo de confiança, o CDR assume que todos os ficheiros são maliciosos (David Tutin, 2023), desconstrói o ficheiro convertendo-o para código binário, limpa todo o código que possa conter agentes maliciosos e volta a reconstruir o ficheiro, garantindo plena utilização com conteúdo seguro (OPSWAT, 2020). Este fundamento, é a solução base oferecida pelo CDR e com o aumento do número de utilizadores tem-se vindo a revelar muito eficaz no que toca a boas práticas na segurança de empresas, atendendo a que muitas delas apresentavam um deficiente sistema de segurança motivado pela falta de limpeza nos ficheiros que recebiam.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

2.1 Funcionamento e Arquitetura do CDR

2.1.1 Princípios de Funcionamento

Encaminhar um ficheiro para um destinatário pode representar um risco elevado para o utilizador recetor. O ficheiro que é enviado pode ser extraviado para incubar um vírus que ficará pronto para atuar assim que o ficheiro for aberto, caso este não seja detetado pelo antivírus ou pela *firewall* que protege o computador. Face à situação supra, a não abertura dos ficheiros também não se apresenta como uma solução razoável, considerando que o utilizador que recebe os ficheiros pode estar a perder informações importantes, caso alguma intrusão seja detetada por um antivírus. A alternativa pode passar pela utilização de um CDR para a proteção de um computador que receba muitos ficheiros de fontes desconhecidas. Esta ferramenta visa remover potenciais fontes de código malicioso existente nos ficheiros e que pode implicar infeções nos sistemas, causando o mínimo transtorno ao seu utilizador.

O CDR funciona de uma forma muito eficaz, removendo tudo o que entende como suspeito de conter elementos que infetem um computador, tal como *links* num Word, código escondido dentro de um PDF ou executável, Macros num Excel e também imagens nestes documentos. Estas volatilidades são todas removidas para não dar azo a um possível incidente.

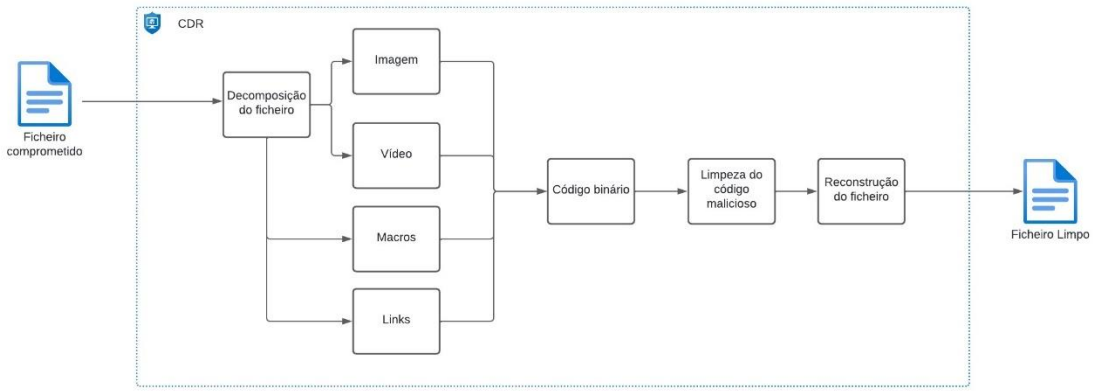

Figura 9 - Ciclo do CDR

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

O CDR é uma ferramenta que segue a metodologia de confiança zero que vem ganhando popularidade nos Sistemas de controlo da Indústria, na proteção de *upload* e *download* de ficheiros e na segurança de email (Dubin, 2023b, 2023a). Tem como finalidade desmontar um ficheiro em blocos de código e voltar a montar o mesmo, na forma inicial, mas, sem qualquer tipo de ameaças para o utilizador que vai usufruir daquele ficheiro. Este desmantelamento, como exemplificado na Figura 9, tem como objetivo separar imagens, vídeos, formulários, texto, tabelas e *hiperlinks* de um ficheiro, transformando esses componentes em binários e retirando *scripts*, macros, *exploits* escondidos e objetos maliciosos incorporados.

Este tipo de tecnologia pode ser utilizado localmente (método mais antigo) num computador. O seu processo em *background* consume os ficheiros descarregados da Internet, dos quais tem o formato de leitura compatível para limpeza. Segundo a Forcepoint (*ForcePoint*, 2024), esta ação pode ser prejudicial nestes sistemas antigos. Eles podem conter código malicioso passivo, que não precisa de ser executável e pode estar escondido em falhas que possam ocorrer nos ficheiros(Wiseman, 2023). Atualmente já poucas empresas trabalham com CDR localmente, por ser algo que pesa bastante no sistema do computador.

O mercado dos CDR evoluiu, em conformidade com outros mercados, na área da segurança, sendo atualmente, disponibilizadas várias alternativas desta ferramenta, principalmente, através de aplicações localizadas num servidor físico, ou de integrações através de APIs acedidas através dos seus *endpoints*, e que podem ter ou não associadas uma aplicação *frontend* para os utilizadores.

O CDR pode ser usado em vários tipos de soluções, apresentando-se a transferência de ficheiros como principal tarefa, como por exemplo nas soluções entre domínios (CDS), portais de *upload* de arquivos, migração para a *cloud* ou em redes isoladas na transmissão de ficheiros.

Os benefícios do desarme e da reconstrução dos ficheiros traduz-se assim numa proteção e otimização destes, e menor risco e maior produtividade para os utilizadores, através de uma fácil implementação no sistema.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

2.1.2 Componentes básicos de um CDR

Para a construção desta solução é preciso ter componentes para tratar os vários estágios do documento. A Figura 10, apresenta a análise a arquitetura de um programa CDR procurando demonstrar os passos que os documentos percorrem dentro do programa e como se percebe se os documentos estão salvaguardados ou não.

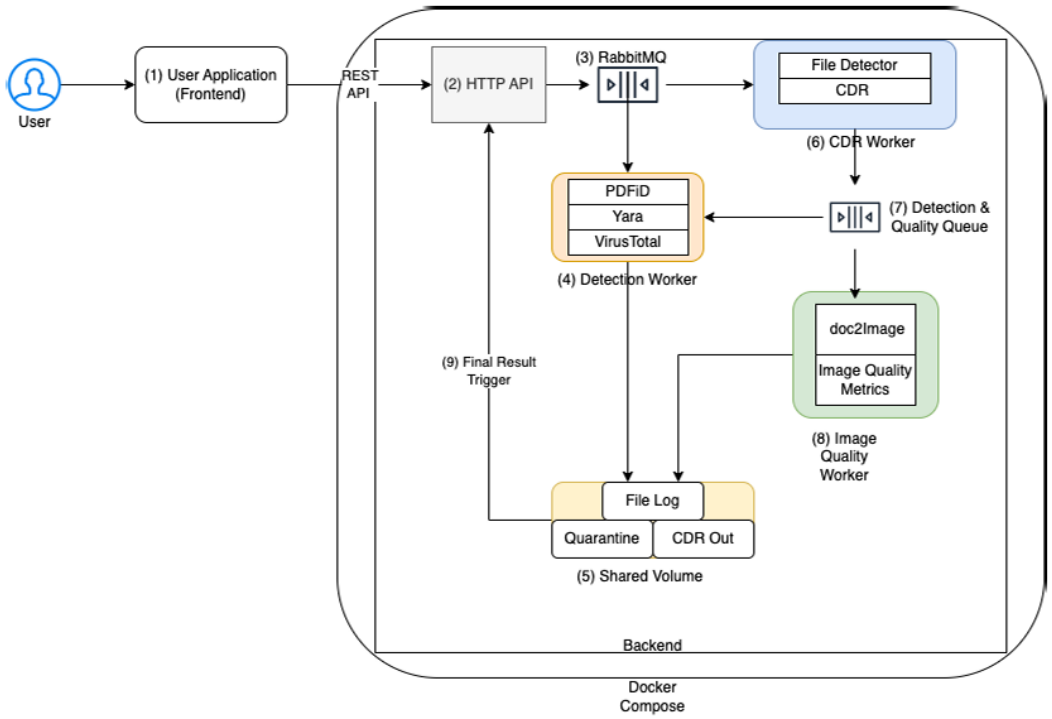

Figura 10 - Arquitetura do programa PdfCDR (Dubin, 2023a)

O exemplo utilizado é da aplicação PdfCDR (Dubin, 2023a), que foi desenvolvida para os utilizadores fazerem o *upload* do ficheiro que querem limpar. Esta aplicação é desenvolvida em microsserviços e constituída por sete *containers*. Estes *containers* são utilizados para virtualizar aplicações, principalmente na gestão de aplicações em nuvem e podem conter neles um serviço, uma *framework*, uma base de dados ou um repositório de ficheiros (Pahl et al., 2019). A arquitetura em microsserviços evita a paragem completa da aplicação, no caso de um dos serviços estar em baixo, o que permite ao utilizador continuar a utilizar a mesma.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

No caso do PdfCDR, após o *upload* para a API do serviço, o ficheiro é inserido no *container* RabbitMQ (3). Após ser tratado pelo RabbitMQ, o ficheiro é enviado para duas zonas de trabalho, a de deteção (4), e ao mesmo tempo para a zona de trabalho CDR (6).

O *output* da zona de trabalho de deteção é guardado no volume partilhado (5), no File Log, onde podemos comparar os resultados com os resultados provenientes de outras zonas de trabalho.

A zona de trabalho CDR depois de receber o ficheiro, analisa-o e identifica o seu tipo. Conforme o seu tipo, a aplicação CDR vai aplicar os algoritmos necessários para limpar o ficheiro. Caso algum ficheiro falhe ao ser desmontado, o ficheiro é enviado para um ficheiro Zip e remetido para a pasta de "quarentena" no volume partilhado. Se houver sucesso no desmantelamento do ficheiro, este é enviado para a fila de deteção e qualidade (7).

Na fila de deteção e qualidade existe uma divisão do ficheiro, sendo que uma cópia do ficheiro é para o *container* de deteção (4), após a aplicação do CDR ao ficheiro, e a outra cópia é para a zona de comparação de imagem (8). No *container* de deteção (4) verifica-se se o ficheiro é malicioso ou não. Caso seja malicioso repete os passos anteriormente descritos, em que comprime e envia o ficheiro em formato Zip para a Quarentena. Caso seja seguro vai enviar o ficheiro para a pasta CDR Out, que também está no volume partilhado.

A zona de trabalho de qualidade de imagem recebe o ficheiro da fila de deteção e qualidade e compara com o ficheiro original. Os resultados são expostos na secção de resultados do volume partilhado. Após esta análise ao ficheiro a aplicação recebe o status e os *logs* de todos os procedimentos por onde o ficheiro passou, sendo estes disponibilizados na API juntamente com o ficheiro limpo.

2.1.3 Integração com sistemas de segurança

Os sistemas OT, muitas das vezes são os sistemas que mais preocupações dão ao gestor de redes de uma empresa em questões de cibersegurança. Estes sistemas referem-se à tecnologia, sistemas e protocolos utilizados nas operações industriais para controlar,

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

monitorizar e operar sistemas industriais (Akailvi et al., 2023). Conformam-se em sistemas que podem sofrer ataques e invasões, através dos ficheiros que possam existir em trânsito e que estes sistemas necessitem para a sua tarefa. Para evitar estes incidentes, a evolução nos sistemas de informação permitiu a integração de CDR em sistemas OT. Assim sempre que haja transmissão de ficheiros, estes são depurados para aumentar a segurança do sistema.

Na maioria das vezes, as integrações são feitas sobre aplicações que estão alojadas em *cloud* e a trabalhar em ambiente remoto. Na sua maioria são *web application programming interfaces* (APIs) que fornecem vários *endpoints* para servirem diferentes propósitos.

As APIs são componentes que fornecem diversas funcionalidades e que na gíria se denominam de servidores, para os componentes que utilizam essas funcionalidades, mais conhecidos como clientes (Maalej & Robillard, 2013). Estas funcionalidades podem ser distribuídas por vários clientes, através de ligações que estes têm com o servidor, como é possível constatar através da Figura 11. Estas ligações designam-se de *endpoints*, e a sua arquitetura consiste no URI, no método HTTP que a define, no HTTP status, no HTTP *header* que normalmente leva a informação para a ligação à API, e no HTTP *body* que contém recursos que podem ser exigidos no pedido.

Figura 11 - Esquema de ligação cliente com servidor

Do mesmo modo que existe o tipo de integração nos sistemas OT, também podemos ter a integração do sistema CDR em qualquer outra plataforma através de uma API disponibilizada. Esta plataforma poderá ser um antivírus como temos por exemplo o caso

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

do CDR da Check Point (*CheckPoint*, 2024) que pode ser integrado nas suas soluções de proteção, garantindo assim, melhor serviço aos seus clientes. Como este caso, temos outros fornecedores de outros CDR tal como a Fortinet (*Fortinet*, 2024), que disponibiliza aos seus clientes o FortiGate.

A Forcepoint (*ForcePoint*, 2024), por sua vez, tem um produto que integra tecnologias *Zero Trust* e *Security Service Edge* numa única plataforma em *cloud*. Este é provido de uma consola que disponibiliza vários *endpoints*, garantindo a sua integração com outras aplicações, sistemas ou redes, assim como pode ser implementado num servidor fixo em detrimento da *cloud*.

2.2 Técnicas de Desarmamento e Reconstrução de Conteúdo

As técnicas de desarme são diversificadas conforme o produto desenvolvido por cada empresa, podendo, dentro da mesma empresa pode haver diferentes CDR disponíveis. No entanto, com a digitalização tem havido uma migração para o desarme através da *cloud*, aumentando e diversificando os produtos que existem no mercado e indo ao encontro das reais necessidades das empresas.

Existem alguns programas bastante eficazes que continuam a trabalhar em servidores físicos, tal como o *Zero Trust CDR* da Forcepoint. Este CDR é implementado separadamente em dois servidores distintos, um interno que apenas recebe e disponibiliza os ficheiros dos utilizadores, e, também, envia e recebe os ficheiros que são para limpar para um servidor externo, através de uma rede protegida que tem comunicação, apenas, com o exterior. Este pode ser atacado no momento da execução do ficheiro e quando após a sua limpeza, ative algum *script* que seja passivo e não tenha sido detetado. Caso o servidor não detete a existência de *malware*, este retorna o ficheiro e a limpeza efetuada (Wiseman, 2023). Esta técnica também pode apresentar falhas caso o *firmware* da placa de interface não se encontre devidamente protegido, pois, esta interface é muito mais simples que a do primeiro servidor. Quando ocorre a situação supra mencionada, pode acontecer a intrusão de um invasor, facilitando o seu acesso a todos os servidores. Porém, no caso do *Zero Trust CDR*, existe uma verificação independente que é enviada com o

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

objetivo de passar a mensagem de que está tudo a funcionar corretamente, garantindo assim que o ficheiro só passa pela interface se for válido.

Por outro lado, temos exemplos como a Opswat (OPSWAT, 2024) que se rege pela técnica mais convencional, onde o seu CDR recebe o ficheiro e valida se este tem uma estrutura válida. Caso não manifeste essa estrutura, o ficheiro é enviado para quarentena, devendo ser eliminado de imediato. Ao invés, se este ficheiro for válido, o mesmo vai ser desmontado permitindo a remoção do código malicioso de todas as suas partes. Após esta ação, o ficheiro é reconstruído e devolvido ao utilizador, podendo voltar a ser usado sem qualquer tipo de risco.

2.3 Vantagens e Limitações do CDR

2.3.1 Vantagens

Considerando as vantagens que este que este produto nos fornece, revela-se interessante perceber que tipo de problemas e o risco que ele acarreta, na área da cibersegurança, principalmente ao nível do tecido empresarial onde existe uma maior troca de ficheiros e uma grande oportunidade para a intrusão. O objetivo é o foco na transmissão de ficheiros, tanto internamente, como com o exterior, de onde pode existir um maior número de ameaças.

Basicamente, como já descrito anteriormente, o CDR é uma ferramenta muito poderosa e bastante eficaz na remoção de código malicioso que se encontra embutido num ficheiro para afetar o sistema, garantindo ao máximo preservar o conteúdo original do ficheiro. Representa um tipo de ação baseado no conceito de confiança zero, pelo que, remove tudo o que considera ser prejudicial para o sistema, elevando a taxa de sucesso de prevenção de infeção do mesmo para aproximadamente 100% de eficácia.

Atualmente, com a evolução da tecnologia, o CDR apresenta a vantagem de dispensar a existência de ter uma aplicação dedicada a cada tipo de ficheiro, atendendo a que existem várias soluções no mercado que já cobrem maior parte dos tipos de ficheiros existentes. Esta evolução permitiu uma significativa redução dos custos com tecnologia de segurança informática.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Outra das vantagens que o CDR apresenta, traduz-se na sua contribuição para melhores políticas de segurança das empresas, que, por vezes, é exigida por uma tutela que coordena a atividade ou setor da empresa / entidade.

O CDR, como maior parte de outras ferramentas e técnicas, produz a redução de custos das empresas através da supressão ou bloqueio de possíveis ataques. A ausência destas ações poderia redundar em custos avultados para as empresas ou para os utilizadores dos SI, quer em tempo despendido para solucionar o problema, quer no dinheiro que se possa despender para o resolver.

A implementação destas soluções exige, efetivamente, o dispêndio de dinheiro para garantir a defesa da empresa, no entanto, caso não seja esta a decisão, os custos poderão ser muito superiores com a resolução de problemas de segurança, nas situações em que as empresas se encontram sujeitas a ataque e não possuem ferramentas para se defender. Com o aumento da defesa e o conhecimento tecnológico, as entidades que possuem as ferramentas de defesa, conseguem aumentar o desempenho e a produtividade, por sentirem maior segurança no desenvolvimento da atividade e que o nível de risco é diminuto no momento da utilização do seu SI.

2.3.2 Desvantagens

Como todos os sistemas de segurança informática, o CDR não é perfeito e apresenta algumas desvantagens. A principal desvantagem encontra-se associada ao custo que uma solução destas tem para quem a pretende implementar. Acrescendo, que depois de implementada, é necessário o investimento na manutenção, na atualização permanente da aplicação para garantir o nível de defesa contra as ameaças emergentes, na remoção de vulnerabilidades que possam vir a ser detetadas com o tempo, nos recursos exigíveis de *hardware* e *software*, ou na aprendizagem e treino de pessoal para se dedicar ao modo de trabalho da ferramenta. Estes custos podem a vir ser significativos para as empresas e gerar um impacto grande nas suas contas.

O CDR também não garante à empresa uma taxa de sucesso na defesa de 100%, na defesa dos seus interesses, denotando que também tem falhas. Algumas podem ocorrer por falta

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

de manutenção e atualização, mas, podem ocorrer situações em que o CDR também não consiga reconhecer código malicioso dentro do ficheiro que está a ser analisado.

Para além das desvantagens supramencionadas, convém referir que a complexidade dos ficheiros condiciona o desempenho da aplicação, podendo o tratamento dos mesmos ser efetuado de forma mais rápida ou lenta, situação que pode causar transtorno à atividade empresarial. A execução de um ficheiro Word composto por mais de 100 páginas, contendo imagens e alguns *links*, revela-se naturalmente mais demorado que o processo de um ficheiro Word que tenha apenas 10 páginas, requerendo o primeiro um volume de tempo superior para o seu desarme. Esta condição pode impactar a utilização do CDR e na produtividade dos colaboradores da empresa.

2.4 CDR OSS

As bases da iniciativa Open Source data de 1998 e desde então as aplicações *open source* (OSS) têm tido um grande crescimento, quer no interesse, quer na sua popularidade, tanto na indústria como no ensino devido ao seu relativo baixo custo (Lenarduzzi et al., 2020).

Uma caracterização quase comum do OSS é a mítica, um pouco desatualizada, de um coletivo de talentosos *hackers* que oferecem livremente os seus serviços para produzir software de alta qualidade e de forma uniforme (Fitzgerald, 2006). Esta designação tinha algum sentido até estas aplicações começarem a ser desenvolvidas para serem viáveis a nível económico, denominada a era do OSS 2.0. Porém, atualmente o OSS continua a depender imenso do voluntariado dos programadores e da sua boa vontade em desenvolver softwares sem receber nada em troca.

Ao nível dos CDR OSS existem poucas aplicações, e com pouca diversificação em termos de uso. Efetuou-se uma pesquisa através do Github (plataforma open source de repositório para ferramentas de código aberto) pela string `content-disarm-reconstruction` e apenas foram encontrados seis projetos, dos quais podemos destacar o DocBleach, o DocBleachShell, CDR-Image, ICDR, AI-MODEL-CDR e CoDeRedlight.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Após mais algumas pesquisas, foi encontrado o Linux security Expert (Linux security Expert, 2021), que é um website que tem rating de ferramentas que podem ser utilizadas na segurança do Linux. Aqui também foi efetuada a pesquisa pela string `content disarm and reconstruction` do qual resultou apenas uma aplicação, o DocBleach. Para ir mais longe fizemos mais uma pesquisa por `data sanitizing` na qual foi encontrado um grupo de ferramentas que continha três tipos de CDR OSS diferentes, dos quais o já falado DocBleach, o CIRCLean e o Bleach da Mozzila.

Para um conhecimento mais pormenorizado destas ferramentas, foi feita uma pesquisa rápida para conhecer melhor que tipo de ferramentas CDR OSS temos disponíveis.

2.4.1 DocBleach

O DocBleach é um produto criado por Maxime Guerreiro, e com licença permissiva de uso comercial, modificação, distribuição e uso privado dada pelo MIT. Esta licença restringe a responsabilidade civil e a garantia a quem a usa.

Este produto é desenvolvido em Java e caracteriza-se como um software avançado para o desarme e reconstrução de conteúdo. O seu principal objetivo é a remoção de malware existente em arquivos de Office ou tudo que possa ser uma ameaça à segurança do computador (Maxime Guerreiro, 2016).

Mais aspetos interessantes à descrição do DocBleach está na fácil instalação do projeto para uso simples no computador pessoal. Esta instalação é efetuada através da linha de comandos do Windows ou em sistema operativo Linux, e para a sua construção é preciso utilizar o Maven. Depois de construído no computador basta correr a seguinte linha de comando:

```
java -jar docbleach.jar -in unsafe_document.doc -out safe_doc.doc
```

Este comando serve para enviar o documento para ser limpo e reconstruído, e receber como output o documento reconstruído.

Esta ferramenta, segundo o que já falámos anteriormente tem as suas desvantagens, pois é um CDR que está alojado no próprio computador e que pode não efetuar eficazmente a limpeza do ficheiro, podendo deixar passar blocos de código que contenha vírus, mas que

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

não foi reconhecido como tal. Outra desvantagem é que deixou de ser atualizada há cerca de 4 anos, estando depreciado e não sendo aconselhado o seu uso.

O DocBleach também tem um SaaS disponível no github para quem quiser contribuir e usar. Este serviço está disponibilizado numa API que é executado em Docker e disponibiliza os seus *endpoints* para a limpeza dos ficheiros. Este projeto também já não é atualizado há cerca de 5 anos.

No site Linux Security Expert tem um rating de 60 pontos, o que mostra que está a ficar pouco saudável, muito graças à idade que o projeto tem e da última data de lançamento.

2.4.2 CoDeRedlight

O CoDeRedlight (InterProbe, 2022) é um CDR escrito em Python, e que é executado através da linha de comandos do Sistema Operativo Linux. Este programa foi elaborado por uma equipa turca de investigação e desenvolvimento na área dos *Malwares* e das Vulnerabilidades, e tem licença GPL – 3.0 license.

Este CDR é muito simples e bastante fácil de utilizar, porém, talvez por ser um trabalho de investigação que teve pouca colaboração externa, também é muito limitado. Tem apenas suporte para ficheiros Word e para Excel, sendo que ficou por fazer o suporte para ficheiros PDF. Esta ferramenta não está presente no site Linux Security Expert.

2.4.3 Bleach

O Bleach (Mozilla, 2023) é uma ferramenta criada pela Mozilla em 2010 para a utilização no seu browser. Esta ferramenta diverge das anteriores porque apenas se foca na limpeza de HTML que possa conter algum tipo de *malware* embutido. Como exemplo, esta ferramenta efetua a substituição de caracteres especiais por carateres normais, como o caso do espaço normal, identificado como “ ”, mas que muitas das vezes vem como caracter especial e é usada a entidade no html como “ ”.

Esta ferramenta está obsoleta desde 23 de janeiro de 2023, mas ainda assim continua a receber *updates* de tempos a tempos, sendo que o último foi feito há cerca de 6 meses.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

No site Linux Security Expert tem um rating de 84 pontos, o que mostra que está algo saudável.

2.4.4 CIRCLean

O CIRCLean (Raphaël Vinot, 2019), é uma ferramenta criada para uma vertente completamente diferente das ferramentas anteriores, mas que não deixa de ter o mesmo objetivo, a limpeza de ficheiros de *pen drives*. A prática da infeção das *pen drives* foi utilizada durante muito tempo pelos *hackers*, mas com a evolução da *cloud* e da velocidade da Internet, estas estão cada vez menos em uso.

Esta solução converte os documentos com código potencialmente prejudicial em documentos desarmados e reconstruídos. O código desta solução é executado num Raspberry Pi, não sendo necessário conectar a *pen* com alguma unidade USB do computador.

Esta solução tem 78 pontos de rating, sendo que já não é atualizada há algum tempo, o que pode comprometer a segurança de quem a utilize.

2.5 CDR Proprietário

Este mercado é o mais avançado e desenvolvido. Qualquer que seja o cliente que pague um produto para sua segurança quer garantias, e tendo estes produtos bastante impacto nas contas de uma empresa, é sempre importante que a tecnologia que seja utilizada seja sempre tecnologia de ponta e que deixe o cliente mais seguro nas ações que toma.

As diferenças que existem entre estes dois tipos de *software* são enormes, o que leva as empresas que podem a escolher este tipo de *software*, mesmo apesar do modelo *open source* estar em constante crescimento, na área dos CDR estes ainda estão pouco desenvolvidos e muito pouco amigos do utilizador, difíceis de instalar por parte dos utilizadores ou então são muito limitados e alguns obsoletos. No modelo proprietário existe uma maneira diferente de pensar no produto e há a exigência de o cliente receber um produto na proporção do que paga.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Este tipo de modelo tem um tipo de desenvolvimento muito diferente, sendo de código fechado e feito por pessoas especializadas para o efeito, com ambiente gráfico amigo do utilizador facilitando as suas ações. Garante uma segurança mais apertada e por vezes desenvolvida à medida para cada empresa, com manutenções muito mais regulares, oferecendo segurança para novos tipos de *malware* que sejam detetados. Por norma a empresa proprietária deste tipo de software oferece um suporte constante, podendo ser 24 horas por dia. Claro que para uma empresa que oferece isto, o custo do produto, seja na compra ou na assinatura, pode ser bastante elevado(Andrew Park, 2023).

Grande parte das empresas do setor dos CDR apresenta produtos e soluções variadas o que permite ao utilizador escolher apenas o sistema que mais se adapte às suas necessidades, evitando assim gastar dinheiro com uma solução que não necessita. Neste mercado existem bastantes empresas, pelo que vamos identificar três e os seus produtos, mostrando que o CDR pode ser adaptado a vários tipos de situações.

2.5.1 Odix

A Odix é uma empresa israelita com sedes em Israel e nos EUA, e considerada uma das melhores no mercado dos CDR. Esta empresa é proprietária de um processo patenteado pela mesma, o Deep File Analysis que está presente nos seus serviços de CDR, e dentro do qual também detém a patente do algoritmo responsável pelo desarme e reconstrução dos ficheiros analisados, o TrueCDR™(Odix, 2024). O DFA considera um ficheiro como um iceberg em que procura vestígios na parte visível, mas mesmo encontrando algo na superfície, vai à parte não visível do documento procurar por algo que possa estar escondido nos restantes 80% do ficheiro.

Este processo tem na sua base a execução de quatro fases que são fundamentais para a proteção dos seus utilizadores:

1. Aplicação das políticas – Confere se o tipo e o tamanho estão dentro dos parâmetros para entrada no processo, e verifica a fonte e o canal pelo qual chegou ao utilizador são fidedignos.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

2. Scan do ficheiro – Efetua o *scan* de multi antivírus, podendo assim despistar algum vírus que seja reconhecido e que não esteja incorporado no código binário do ficheiro.
3. Validação do tipo de ficheiro – Neste passo efetua a validação do tipo de ficheiro para que ele possa ser verificado e se não existe alguma incongruência com o que foi validado na primeira fase, aquando da execução das políticas.
4. TrueCDR – aqui entra em ação a técnica de desarme e reconstrução do ficheiro para que sejam removidas todas as ameaças que existam no ficheiro, sejam elas reconhecidas ou não pelo CDR.

Este processo é utilizado em quatro serviços que são disponibilizados pela Odix, sendo todos eles para diferentes finalidades:

1. FileWall – É um produto adaptado ao Microsoft 365 e que pode ser facilmente integrado oferecendo a segurança de ponta contra os ataques com base em ficheiros. Este produto protege os utilizadores Microsoft 365 contra os ataques de *ransomware* e *malware* a que possam estar sujeitos nas trocas de ficheiros. Esta solução apresenta vários pontos favoráveis na sua escolha: a facilidade de implementação sem problemas, a segurança aos utilizadores internos e externos, a proteção contra o conhecido e contra o desconhecido e baixo tempo de execução do serviço.
2. Kiosk – Este produto disponibilizado pela Odix é dedicado à limpeza de ficheiros que estão presentes em suportes amovíveis tais como *pen drives*, CDs ou DVDs e disco rígidos externos. Estes canais de transmissão de ficheiros ainda são muito afetados para a execução de ataques. Esta é uma estação de trabalho de alta segurança e arquitetura baseada em Linux que está localizada fora da rede da empresa. Tem um grande portfólio de tipo de ficheiros a que pode executar a limpeza, fácil de instalar e amiga do utilizador.
3. NetFolder – Este é o serviço mais abrangente de todos, que é dedicado aos ficheiros comuns que podem ser partilhados entre colaboradores de uma empresa ou com pessoas externas. Este serviço também atua sobre os *downloads* que são

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

feitos para a rede, os *uploads* de ficheiros e anexos, e também pode ser utilizado num RPA em que se processem ficheiros.

4. FileDiligence – É um serviço *on-demand* que garante um processo de digitalização e limpeza com alta qualidade de ficheiros em massa em *data centers*. Este serviço consiste na configuração de instâncias do NetFolder de forma que seja escalável conforme necessário pela empresa. Estas instâncias podem ser implementadas no Microsoft Azure. Normalmente este serviço é utilizado para três casos específicos: empresas que precisem de mudar ou importar dados de outro *data center* porque foram adquiridas ou estão a adquirir uma outra empresa, para empresas que suspeitam que estão sobre ataque, e para empresas que estão sobre ataque. Isto pode acontecer porque o FiliDiligence corre na hora sobre todos os ficheiros da empresa, permitindo uma limpeza rápida e eficaz, capaz de parar o ataque, mas que não repara os danos causados nem recupera ficheiros que possam ter sido capturados aquando o ataque.

Estes são as soluções oferecidas pela Odix, e que mostra que tem soluções bastante abrangentes para qualquer que seja a necessidade das empresas.

2.5.2 OPSWAT Deep CDR

A OPSWAT é uma das empresas líderes em cibersegurança de infraestruturas críticas, e desenvolve imensos produtos para a segurança das empresas. No caso do mercado dos CDR apresenta o Deep CDR que ajuda na prevenção de ameaças baseadas em ficheiros, conhecidas e desconhecidas, protege de ataques de *malware* e ataques *zero-day*. Este CDR também apresenta uma segurança abrangente baseada na prevenção para aplicações *web*, onde deteta e neutraliza potenciais ameaças antes que elas possam causa algum dano ao utilizador (OPSWAT, 2024).

Esta tecnologia apresenta um processamento de arquivos de multinível, uma reconstrução precisa de ficheiros fazendo com que os ficheiros não percam a sua usabilidade e funcionalidade após a remoção do código malicioso, suporte para mais de 150 tipos de ficheiros, fornece informações aprofundadas sobre os ficheiros desarmados na sua interface para utilizador, podendo ser utilizada para limpar arquivos, ficheiros

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

incorporados, anexos de email e *hiperlinks*. É integrada com a OPSWAT Multiscanning para incluir uma avançada deteção de ameaças antes da limpeza.

A arquitetura deste CDR, presente na, divide-se em quatro partes que atuam de maneira diferente caso seja um ficheiro único, uma imagem, uma pasta de ficheiros ou um QR Code. No caso de um ficheiro, este é recebido pelo CDR que valida a estrutura do ficheiro e em caso de falha na validação da estrutura, este ficheiro é redirecionado para a Quarentena. Caso a validação seja efetuada com sucesso, o ficheiro é desmantelado e vai ser processado peça a peça e removido todo o código que seja detetado como potencialmente malicioso. Após esta fase é feita a reconstrução do ficheiro e devolvido para o utilizador, com todas as funcionalidades que ele tem.

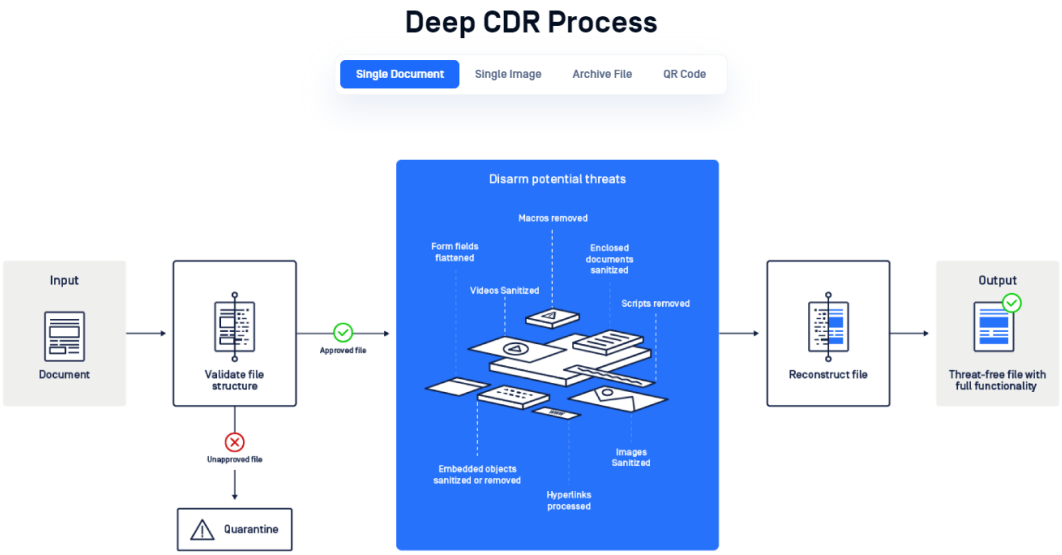

Figura 12- Processo OPSWAT Deep CDR (OPSWAT, 2024)

Este CDR é utilizado por várias empresas muito conceituadas a nível mundial, tal como a Bosch, Comcast, Paloalto ou American Express, o que podemos constatar que para o ser é porque é muito bom e cumpre com os requisitos que são exigidos pelos clientes.

2.5.3 Zero Trust Forcepoint

O Zero Trust CDR da Forcepoint (*ForcePoint*, 2024) é um serviço que pode ser aplicado em imensas situações e em diferentes camadas de proteção, sendo que pode ser ajustado

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

a cada situação concreta. Este serviço pode ser aplicado nos *gateways* de uma rede empresarial e em *web gateways*, ao seu email ou ao seu Microsoft 365, pode ser fornecido como um SaaS baseado em *cloud* através de API ou pode ser implementado num portal de proteção. Este serviço é muito flexível e ajusta-se a vários tipos de performance.

O Zero Trust CDR aplicado nos *gateways* da rede empresarial é criado para garantir que os *downloads* através da Internet não contenham nenhum tipo de ameaça maliciosa que possa danificar o sistema informático de uma empresa. O CDR, presente na Figura 13 é implementado através do GX Appliance da Forcepoint, e este é aplicado como uma extensão no *web security gateway* que suporta o ICAP, que foi concebido para alargar a capacidade dos servidores *proxy*, libertando os seus recursos para servidores externos e conseguindo assim efetuar outras tarefas como a verificações de antivírus e filtragem de conteúdos. Isto promove tanto *downloads* seguros como *uploads* seguros.

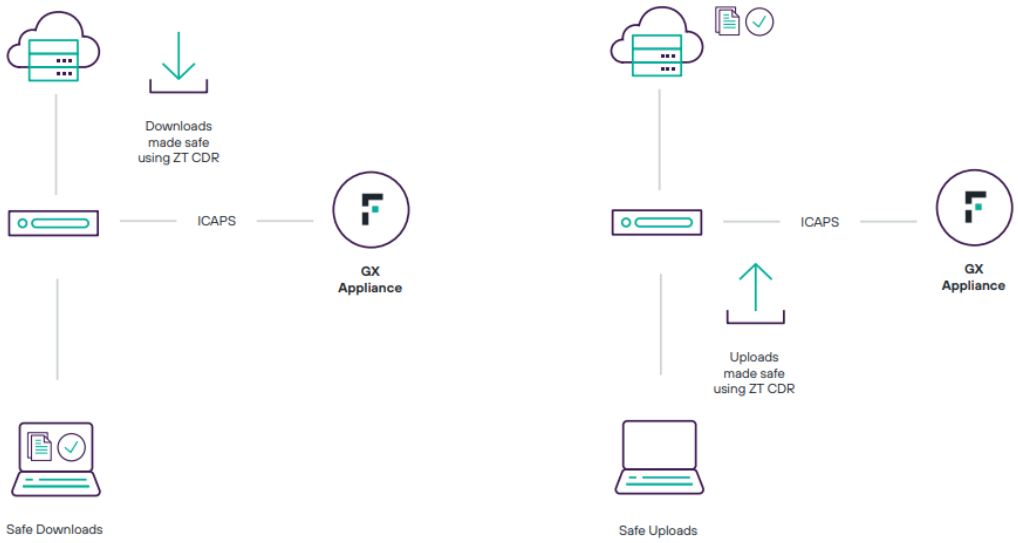

*Figura 13- Implementação do Zero Trust CDR em gateways (*ForcePoint, *2024)*

2.6 Resumo

Em jeito de conclusão e para término da pesquisa e estudo dos CDR existentes, tanto OSS como aplicações proprietárias, foi elaborada uma tabela para apresentar o nome dos CDR que estudámos, se é OSS ou aplicação proprietária, o link do repositório no caso dos CDR

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

OSS e o link do website no caso dos CDR proprietário, e algumas vantagens que cada uma delas oferece ao utilizador.

NOME	TIPO DE CDR	LINK	VANTAGENS
DOCBLEACH	OSS	https://github.com/docbleach/DocBleach-Web	Não tem custos para o utilizador. Tem uma api que disponibiliza uma interface na web Fácil instalação do projeto
CODEREDLIGHT	OSS	https://github.com/interprobe/CoDeRedlight	Não tem custos para o utilizador Fácil instalação do projeto
BLEACH	OSS	https://github.com/mozilla/bleach	Não tem custos para o utilizador Como é *plugin* no Mozilla não sobrecarrega o computador
CIRCLEAN	OSS	https://github.com/CIRCL/Circlean	Não tem custos para o utilizador Limpeza de ficheiros fora do sistema informático Difícil execução do projeto
ODIX	Proprietário	https://www.odi-x.com/	Quatro ferramentas bastante úteis para qualquer empresa Escalabilidade e eficiência
OPSWAT	Proprietário	https://www.opswat.com/	Disponibiliza um plano free limitado Escalabilidade e eficiência Adaptabilidade a diferentes casos de uso

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

FORCEPOINT	Proprietário	https://www.forcepoint.com/	Escalabilidade e eficiência Enorme quantidade de produtos que utilizam o CDR

Tabela 2 - Tabela resumo de aplicações CDR

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

3 IMPLEMENTAÇÃO DE UMA SOLUÇÃO CDR

Neste capítulo descrevemos as operações necessárias para a execução do projeto CDR proposto nesta dissertação. Neste capítulo procedemos à seleção de uma das tecnologias revistas no Capítulo 3. O objetivo desta seleção passa por pegar num projeto *open source* ou proprietário, de preferência num plano gratuito e trabalhar sobre esse projeto, apresentando melhorias à experiência do utilizador.

3.1 Seleção de Aplicações e Tecnologias

Esta secção consiste no estudo para a seleção da solução informática mais adequada para a realização do projeto. Dado os custos dos serviços mais complexos e completos, decidi realizar o estudo sobre um projeto *open source*. Estes projetos são vantajosos porque não carecem de investimento e têm acesso público ao código. Para o nosso caso específico, temos para escolha cinco aplicações, sendo que duas delas são do mesmo autor.

As ferramentas envolvidas na escolha são o DocBleach que é executado localmente em ambiente Linux e o DocBleach-Web que pode ser integrado na *cloud* e ser acedido automaticamente sem a necessidade de intervenção do utilizador, dado que é um *endpoint* que recebe ficheiros, devolvendo-os já tratados. Na sequência do estudo sobre os projetos, depressa nos deparámos com problemas no código, nomeadamente no facto de estar escrito em versões antigas do Java, dando o próprio Java o aviso de que aquele bloco de código estava obsoleto, e continha algumas bibliotecas que já não conseguia importar pois já não existem ou foram descontinuadas.

Estudámos também o CoDeRedlight que é executado localmente e apenas tem suporte para ficheiros Word e Excel. Este programa tem maior parte do código já obsoleto, condicionando assim a nossa escolha.

Depois não testámos o Bleach, que é mais direcionado para o HTML, mas que o próprio Mozilla tem fora de serviço desde janeiro de 2023.

Por fim temos o CIRCLean que efetua a limpeza de ficheiros que são oriundos de suportes amovíveis. Como o nosso foco era a limpeza de ficheiros que seriam descarregados da *web*, este programa não foi considerado para a avaliação.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Após os testes efetuados nos programas anteriormente descritos, efetuou-se uma pesquisa mais profunda em outros locais, sendo encontrado um CDR para email escrito em Python. Este programa correu e conseguiu-se iniciar os testes, mas a única coisa que fazia era apagar os emails se fossem com anexo de um tipo de ficheiro que pudesse conter vírus. Como isto não pode ser considerado um CDR, esta opção foi descartada após o início dos testes.

Após esta exaustiva pesquisa e teste de cada uma das soluções *open source*, foi efetuada uma pesquisa por aplicações que fossem gratuitas até determinados limites, e aqui encontrámos uma solução que pode servir de base para o que precisamos e que estamos dispostos a testar para o nosso projeto. Esta aplicação é o MetaDefender Cloud (*MetaDefender Cloud*, 2024), uma aplicação da OPSWAT (OPSWAT, 2024) que tem como suporte o OPSWAT Deep CDR para a limpeza de ficheiros. Esta aplicação disponibiliza um plano grátis para usar, com pequenos limites e que satisfaz a carga necessária de ficheiros para os testes da nossa implementação.

Esta aplicação fornece uma API key que nos permite criar uma ligação para efetuar a limpeza do ficheiro enviado. Também fornece vários endpoints que podem ser usados para enviar e receber os ficheiros, recolher informação sobre os ficheiros que foram carregados para serem tratados pela API, e informação sobre a API que estamos a utilizar.

Para a execução dos *endpoints* mais importantes fornecidos pela API, e com a perspetiva de não haver uma partilha de acessos à interface da API por várias pessoas, foi criada uma aplicação Blazor para efetuar a comunicação utilizador / API. Para esta comunicação acontecer, apenas é necessário o utilizador aceder à aplicação, podendo assim fazer o *upload* do seu ficheiro. Pode também ver os detalhes e os resultados da análise ao mesmo. Após a API efetuar o *scan* do ficheiro, esta retorna um *link* para o *download* do ficheiro limpo e pronto a ser utilizado para a finalidade que lhe é esperada.

Com o desenvolvimento desta aplicação, o responsável pela segurança não tem de estar preocupado com a partilha de algum tipo de informações sensíveis, como por exemplo os acessos de entrada na conta OPSWAT.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

3.2 Instalação e execução da Solução

3.2.1 API MetaDefender Cloud

A API que vai servir de apoio à realização do projeto não precisa de instalação, mas precisa que seja criada uma conta na OPSWAT (OPSWAT, 2024). Isto é exigido para se conseguir ter um plano grátis para uso muito pouco intensivo e bastante limitado. Caso seja necessário aumentar os limites do plano, estes podem ser subscritos na própria conta. Os limites desta API são bastante pequenos, sendo assim uma limitação para haver mais que uma pessoa a enviar os ficheiros para depurar, e para a implementação desta solução para mais que um ou dois utilizadores, tem de haver um upgrade para um plano que seja mais adequado para cada empresa.

Após o registo podemos entrar na plataforma e ver a informação da nossa conta. Aqui vamos ter presente vários detalhes sobre os limites do nosso plano, se o nosso plano é pago, e a nossa API Key para conseguirmos fazer a ligação entre a API e a nossa aplicação, como ilustrado na Figura 14.

Esta página também tem um espaço onde podemos fazer o *upload* de um ficheiro para análise, *dashboards* que permitem visualizar dados que são transmitidos após a análise do ficheiro. Também tem uma página com estatísticas sobre as nossas limpezas, outra sobre o nosso histórico de submissão de ficheiros, e a última sobre as vulnerabilidades das nossas submissões.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

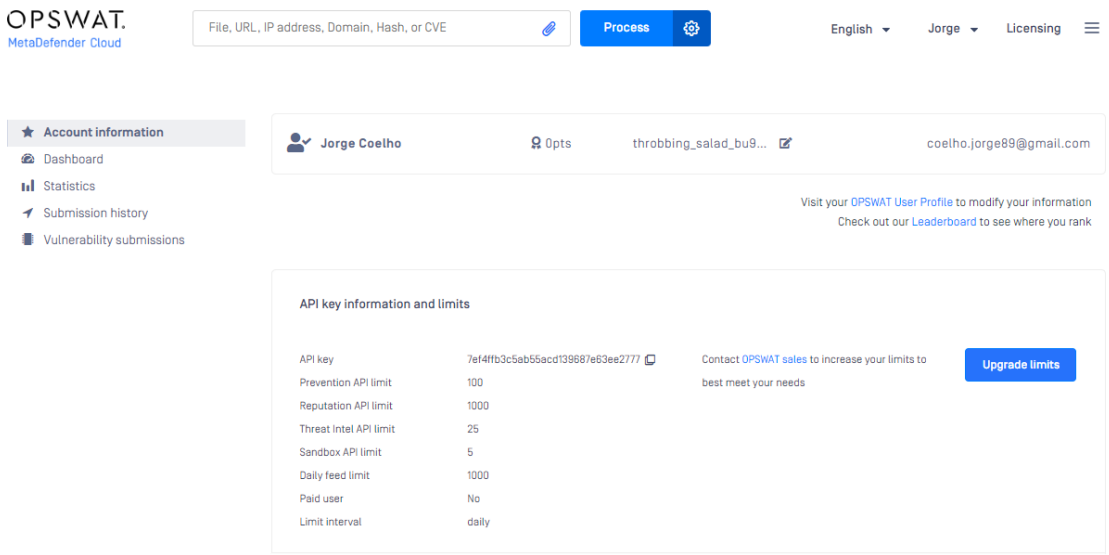

*Figura 14 - Layout página inicial OPSWAT MetaDefender Cloud (*MetaDefender Cloud, *2024)*

Após a visualização da interface *web* do MetaDefender Cloud, fizemos uma recolha dos *endpoints* que são disponibilizados pela API na sua documentação. Todos os *endpoints* têm como base o *path* onde a API está instalada `https://api.metadefender.com/v4`, assim como nos Headers do pedido, deve ser enviada a nossa API Key. Esta é a chave para entrar na nossa conta e o MetaDefender Cloud trabalhar a informação sobre ela.

Esta API fornece-nos *endpoints* que nos permite enviar o ficheiro para a API, assim como nos fornece *endpoints* que também ajudam a recolher informação sobre o nosso ficheiro, e dos quais destacamos:

Endpoint	**Path parameter**	**Método**	**Descrição**
Apikey info	/apikey/	GET	Devolve a informação sobre a nossa conta e os nossos limites no plano adquirido.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Apikey ramaining limits	/apikey/limits/status	GET	Devolve a informação sobre os limites restantes para a Apikey.
Apikey scan history	/apikey/scan-history	GET	Devolve uma lista que pode ser paginada, de ficheiros carregados pelo utilizador.
Analyze file	/file	POST	A análise é efetuada de forma assíncrona e cada pedido de análise é controlado pela identificação dos dados, que pode ser obtido através do Fetch Analysis Result
Fetch analysis result	/file/{dataId}	GET	Devolve os dados relativos ao scan de um ficheiro que é reconhecido pelo seu `dataId`. Este pedido deve ser feito várias vezes até a análise ser concluída.
False positives feed	/feed/false-positives	GET	Devolve uma lista de falsos positivos. Estes ficheiros são designados assim porque o resultado do *scan* pelos antivírus teve apenas dois ou menos motores a detetarem o ficheiro como infetado. Este *feed* é atualiazado diariamente.

Tabela 3 - Tabela descritiva de endpoints do MetaDefender Cloud

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Estes *endpoints* são os que mais informação nos devolvem na API, e os que mais contribuem para a recolha de dados dos nossos testes. Apenas os *endpoints* `Apikey info` e `Apikey ramaining limits` não são utilizados pela nossa aplicação para recolher dados dos ficheiros, mas sim da conta e dos seus limites.

Esta API também fornece um repositório onde mantém os ficheiros que foram limpos, após o seu envio para análise. Estes ficheiros têm o prazo de validade de dois dias, que após expirar o prazo, estes são removidos.

3.2.2 Aplicação CDRFileCleanerApp

Para a implementação na nossa aplicação utilizámos como base o Blazor na linguagem .Net Core 8. Nesta aplicação instalámos a biblioteca de apoio ao código do `Newtonsoft.Json`, que nos vai permitir ler os valores recebidos da nossa API com mais facilidade. Esta biblioteca cria um mapeamento mais simples entre os atributos das classes e os atributos que recebemos nas mensagens da API, que são devolvidas em Json.

A comunicação entre a aplicação e a API, como se pode ver na Figura 15, consiste no envio de um pedido para a API a partir da aplicação desenvolvida. Na API o pedido terá o devido tratamento e será gerada uma mensagem de retorno. Esta vai ser recebida pela nossa aplicação, será tratada e apresentada no *layout* desenhado.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

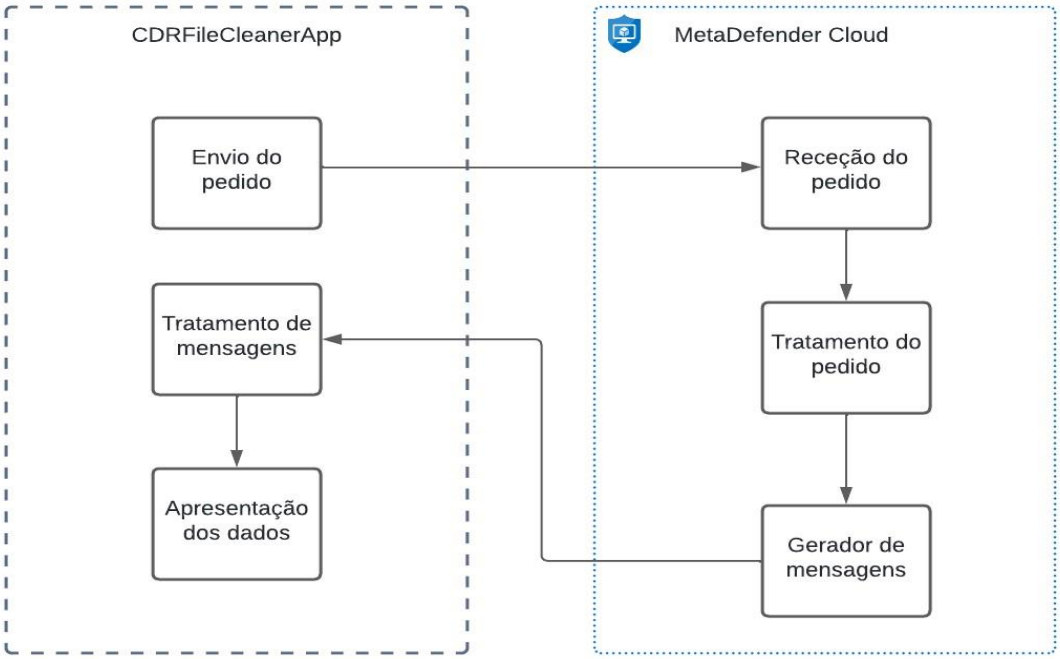

Figura 15 - Comunicação entre CDRFileCleanerApp e MetaDefender Cloud

Para apoio ao Blazor e para melhorar a interface para o utilizador, utilizámos o serviço MudBlazor. Este serviço, com os seus componentes mais trabalhados, permite-nos de uma forma mais simples e ágil aplicar componentes com melhor aspeto e mais práticos que os disponibilizados pelo Blazor e pelo Bootstrap.

Para os testes de ligação à API também foi utilizado a aplicação Postman, para garantir que a mensagem recebida seria a correta, e se os parâmetros que eram enviados através da *query string* do *path* de ligação estavam corretos. Os resultados das mensagens destes testes de ligação à API serão apresentados na secção Anexos. Para uma apresentação também da mensagem retornada da API, compactou-se as classes herdadas.

3.2.2.1 Layout página Home

Depois de os *endpoints* testados passámos ao desenvolvimento da nossa aplicação, o qual também estará apresentado neste capítulo através de prints do código que desenvolvemos. A aplicação foi desenvolvida com três páginas. A página de entrada que irá conter as informações sobre a nossa conta, ou seja, os limites e os limites remanescentes que temos diários, como podemos ver na Figura 16.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

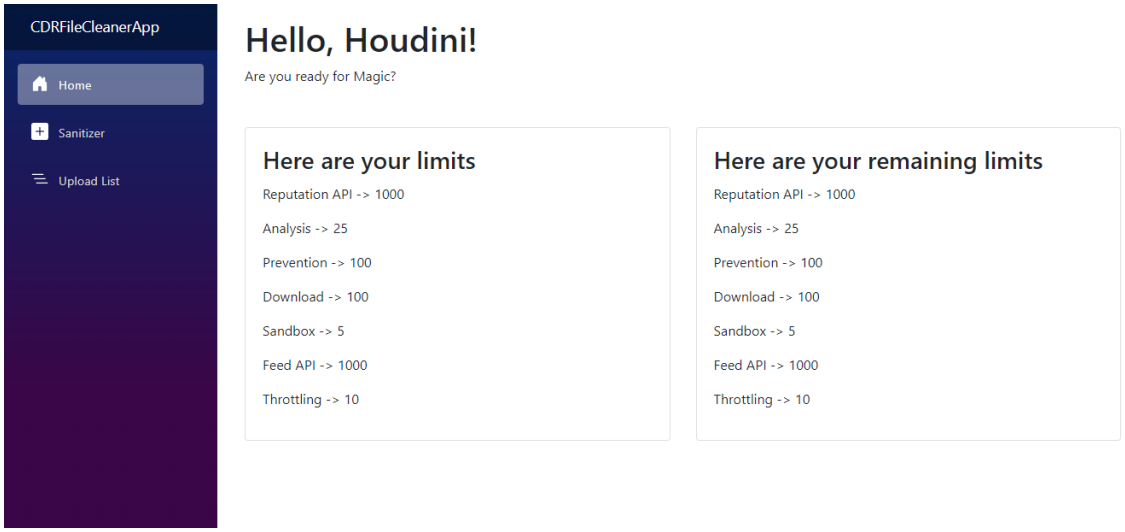

Figura 16 - Página inicial CDRFileCleanerApp

3.2.2.2 Layout página Sanitizer

Na página Sanitizer, disponível na Figura 17, temos o local onde podemos depositar o nosso ficheiro para seguidamente fazer o nosso *upload*.

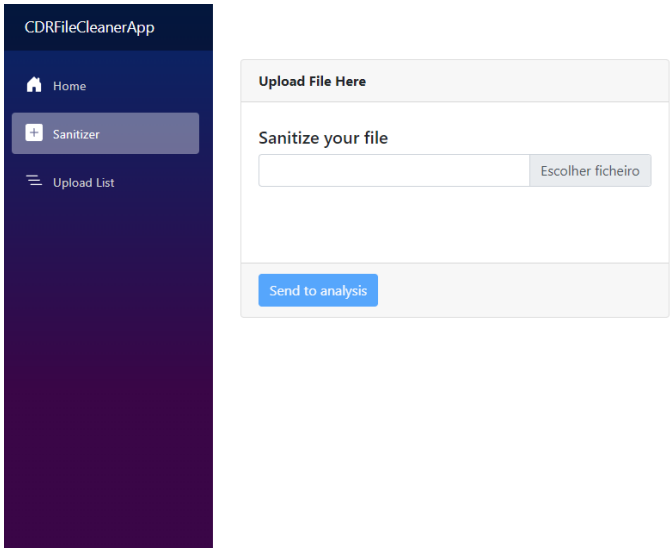

Figura 17 - Página Sanitizer sem ficheiro carregado

Após o *upload* feito irão aparecer vários dados sobre o ficheiro, como ilustra a Figura 18, principalmente dados que sobre a identificação do ficheiro na API, numa secção denominada "`File Data`" onde aparece o `DataId`, que é o identificador do ficheiro, o

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

`Status` do ficheiro, e as chaves hash `SHA1` e `SHA256`. Também é disponibilizada a secção dos resultados do scan do ficheiro e resultados da limpeza, mas devido ao tempo que dura a ação de scan e de remoção de componentes potencialmente perigosos, estes valores aparecem vazios, constando na secção de resultados de *scan* o estado "`In Progress`". Para a atualização da página foram inseridos dois botões para executar o *get* dos resultados novamente.

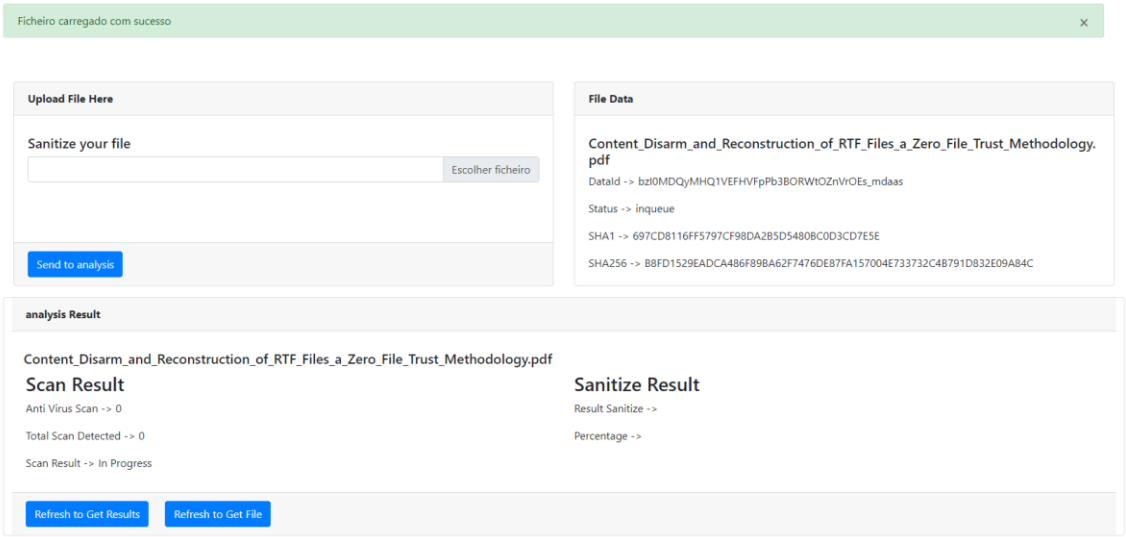

Figura 18 - Layout página Sanitizer após carregamento do ficheiro

Após carregar no botão "Refresh to get results", os resultados aparecerão e o botão desaparece, podendo-se dar o caso de a API ainda estar a limpar o ficheiro, e neste caso vão aparecer os resultados, mas não irá aparecer ainda o botão para download do ficheiro limpo. Caso isto aconteça, o botão "Refresh to get File" vai continuar visível. Caso contrário aparecerá imediatamente o botão "Download File" para o *download* do ficheiro limpo, como demonstrado na Figura 19.

Na secção dos resultados do *scan* vai aparecer a informação de quantos antivírus fizeram o scan do ficheiro, quantos dos antivírus detetaram código ou outra fonte maliciosa embutida no ficheiro e o resultado do scan.

Na secção dos resultados da limpeza do ficheiro, aparece o resultado da limpeza e a percentagem da ação para caso esta ainda não ter ocorrido na integra, o utilizador saber.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Irá aparecer também o botão para *download* do ficheiro quando o *path* para o repositório para onde foi enviado após limpeza, estiver disponível.

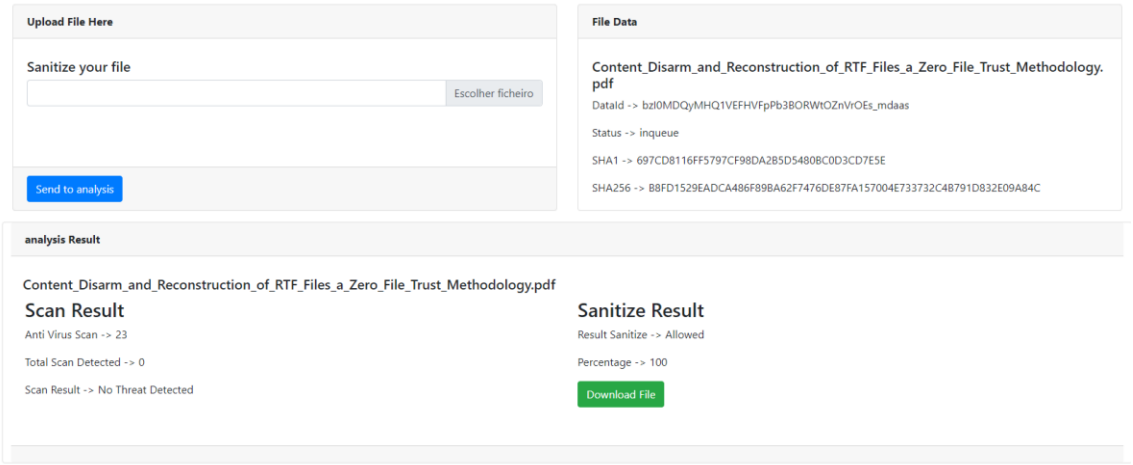

Figura 19 - Página Sanitizer após carregamento dos resultados da análise

Depois de carregar no botão de *download*, o ficheiro limpo será disponibilizado na pasta para o qual os downloads feitos no browser do computador são reencaminhados, aparecendo a notificação do download no canto superior direito do *browser*, consoante o *browser* utilizado.

3.2.2.3 Layout página Upload List

Após muitos *uploads*, achámos necessário desenvolver também uma lista para apresentar um histórico dos *uploads* efetuados para a API. Esta lista, presente na Figura 20, irá ter vários tipos de dados identificativos, tal como a data do *upload*, o `DataId` do ficheiro, o nome do ficheiro e o `SHA1`, Informação da limpeza do ficheiro, o resultado das máquinas que inspecionaram o ficheiro e em quantas delas é que foram identificados como ficheiro potencialmente infetado. Caso seja apenas 1 ou 2, o resultado é considerado como um falso positivo. Tem também o resultado do *scan* dos antivírus, podendo estar infetado ou não, e um botão para fazer o *download* do ficheiro caso seja necessário, dependendo se o ficheiro ainda está disponível. Caso não esteja, aparece a informação de que já não existe ficheiro disponível.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

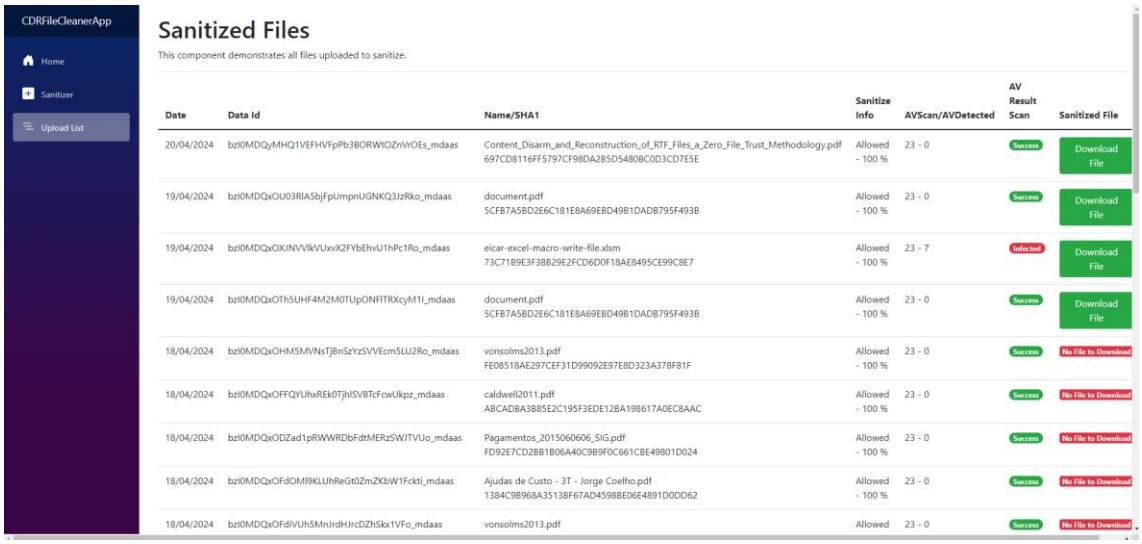

Figura 20 - Layout página List com tabela detalhada dos ficheiros

3.2.2.4 Código página Home

Para a construção desta aplicação foi necessário escrever código. Como a base do meu trabalho é a linguagem C#, onde executo muitas das vezes funções de *full stack developer*, queria desenvolver algo que contivesse essa base, mas também direcionado para *frontend*, então decidi escrever esta aplicação em Blazor, com base de .Net Core 8. Atualmente estas são as ferramentas mais desenvolvidas que os ambientes Microsoft nos oferecem. Ao mesmo tempo são ferramentas com que nunca trabalhei no mercado de trabalho, sendo que assim também seria um grande desafio para mim conseguir desenvolver algo que cumprisse com os problemas a que me propus de resolver.

O projeto da aplicação é desenvolvido em três páginas. A `Home.razor` que diz respeito à página principal da aplicação, a página `Sanitizer.razor` onde é desenvolvida a página Sanitizer do *layout*, e a `List.razor` que é referente à construção da página da lista dos ficheiros submetidos.

Para a realização da página `Home`, página *default* da aplicação, precisámos de realizar duas chamadas a *endpoints*, sendo essas chamadas efetuadas aquando da inicialização dos componentes. Para guardar o valor da resposta da chamada foram criadas as classes `Limits` e `RemainingLimits`, Figura 21.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
public class Limits
{
    [JsonProperty("limit_reputation")]
    public string ReputationApi { get; set; }
    [JsonProperty("limit_threat_intel_search")]
    public string ThreatSearchApi { get; set; }
    [JsonProperty("limit_prevention")]
    public string PreventionApi { get; set; }
    [JsonProperty("max_file_download")]
    public string DownloadFile { get; set; }
    [JsonProperty("limit_sandbox")]
    public string Sandbox { get; set; }
    [JsonProperty("limit_feed")]
    public string FeedApi { get; set; }
    [JsonProperty("throttling_limit")]
    public string ThrottlingLimit { get; set; }
}

public class RemainingLimits
{
    [JsonProperty("reputation_api")]
    public string ReputationApi { get; set; }
    [JsonProperty("threat_intel_search_api")]
    public string ThreatSearchApi { get; set; }
    [JsonProperty("prevention_api")]
    public string PreventionApi { get; set; }
    [JsonProperty("download_file")]
    public string DownloadFile { get; set; }
    [JsonProperty("sandbox_api")]
    public string Sandbox { get; set; }
    [JsonProperty("feed_api")]
    public string FeedApi { get; set; }
    [JsonProperty("throttling_limit")]
    public string ThrottlingLimit { get; set; }
}



private RemainingLimits remainingLimits = new RemainingLimits();
private Limits limits = new Limits();
```

Figura 21 - Classes Limits e RemainingLimits e variáveis locais do ficheiro Home.razor

Estas classes têm basicamente os mesmos atributos, mas os identificadores Json, que são usados para mapear a resposta Json recebida com os atributos da classe, são diferentes. Para as chamadas, vamos utilizar como base cada uma das classes, e para isso foram criadas as variáveis locais `limits` e `remainingLimits`, Figura 21. A primeira será para popular a variável `limits` do tipo `Limits`, a segunda chamada será para popular a variável `remainingLimits` do tipo `RemainingLimits`.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Para a população inicial dos dados da página `Home` através das variáveis `limits` e `remainingLimits` foi utilizado o método `OnInitializedAsync()`, descrito na Figura 22. Como é um método que por defeito é executado antes da renderização da página, permite a associação dos dados antes de estes serem distribuídos pelos campos a que estão assignados. Este método depois de receber os dados da API, vai ainda mandar executar o método `GetRemainingLimits()`.

O método `GetRemainingLimits()`, identificado na Figura 23, é o método que vai preencher a variável `remainigLimits`.

```
protected override async Task OnInitializedAsync()
{
    try
    {
        var client = new HttpClient();
        var request = new HttpRequestMessage
            {
                Method = HttpMethod.Get,
                RequestUri = new
Uri("https://api.metadefender.com/v4/apikey/"),
                Headers =
                {
                    { "apikey", "7ef4ffb3c5ab55acd139687e63ee2777" }
                }
            };
        using (var response = await client.SendAsync(request))
        {
            var jsonString = await response.Content.ReadAsStringAsync();
            limits = JsonConvert.DeserializeObject<Limits>(jsonString);

            await GetRemainingLimits();
        }
    }
    catch (Exception exc)
    {
        Console.WriteLine(exc.Message);
    }
}
```

Figura 22 - Método OnInitializedAsync() da página Home.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Estes *endpoints* vão servir para que sejam recolhidos os dados da nossa API, dando assim conhecimento ao utilizador da quantidade de pedidos de scan de ficheiros ainda pode efetuar no dia.

```
private async Task GetRemainingLimits()
{
    try
    {
        var client = new HttpClient();
        var request = new HttpRequestMessage
            {
                Method = HttpMethod.Get,
                RequestUri = new
Uri("https://api.metadefender.com/v4/apikey/limits/status"),
                Headers =
                {
                    { "apikey", "7ef4ffb3c5ab55acd139687e63ee2777" }
                }
            };
        using (var response = await client.SendAsync(request))
        {
            var jsonString = await response.Content.ReadAsStringAsync();
            remainingLimits =
JsonConvert.DeserializeObject<RemainingLimits>(jsonString);
        }
    }
    catch (Exception exc)
    {
        Console.WriteLine(exc.Message);
    }
}
```

Figura 23 - Método GetRemainingLimits() da página Home.razor

Estes dados vão ser fornecidos ao utilizador através do código de *frontend*, apresentado na Figura 24, que aplicámos com base no template de Blazor que integrámos no projeto, o Blazorise.

Cada *card* que criámos vai disponibilizar um tipo de informação. A Informação sobre os limites disponíveis por dia vai ser apresentada no primeiro *card*, e a informação sobre os limites remanescentes vai ser apresentada no segundo card.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
<PageTitle>Home</PageTitle>

<h1>Hello, Houdini!</h1>

Are you ready for Magic?

<CardDeck Margin="Margin.Is5.FromTop">
    <Card>
        <CardBody>
            <CardTitle Size="3">
                Here are your limits
            </CardTitle>
            <CardText>
                <p>Reputation API -> @limits.ReputationApi</p>
                <p>Analysis -> @limits.ThreatSearchApi</p>
                <p>Prevention -> @limits.PreventionApi</p>
                <p>Download -> @limits.DownloadFile</p>
                <p>Sandbox -> @limits.Sandbox</p>
                <p>Feed API -> @limits.FeedApi</p>
                <p>Throttling  -> @limits.ThrottlingLimit</p>
            </CardText>
        </CardBody>
    </Card>
    <Card>
        <CardBody>
            <CardTitle Size="3">
                Here are your remaining limits
            </CardTitle>
            <CardText>
                <p>Reputation API -> @remainingLimits.ReputationApi</p>
                <p>Analysis -> @remainingLimits.ThreatSearchApi</p>
                <p>Prevention -> @remainingLimits.PreventionApi</p>
                <p>Download -> @remainingLimits.DownloadFile</p>
                <p>Sandbox -> @remainingLimits.Sandbox</p>
                <p>Feed API -> @remainingLimits.FeedApi</p>
                <p>Throttling  -> @remainingLimits.ThrottlingLimit</p>
            </CardText>
        </CardBody>
    </Card>

</CardDeck>
```

Figura 24 - Código frontend da página Home.razor

3.2.2.5 Código página Sanitizer

Para a página `Sanitizer` foi preciso incorporar mais lógica, visto que tem várias ações para fazer aparecer a informação necessária a passar ao utilizador. Na Figura 25, estão representadas todas as classes e variáveis locais da página `Sanitizer.razor`. A classe

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
public class FileResponse
{
    [JsonProperty("data_id")]
    public string DataId { get; set; }
    [JsonProperty("status")]
    public string Status { get; set; }
    [JsonProperty("sha1")]
    public string SHA1 { get; set; }
    [JsonProperty("sha256")]
    public string SHA256 { get; set; }
}
public class AnalysisResult
{
    [JsonProperty("sanitized")]
    public Sanitize? Sanitize { get; set; }
    [JsonProperty("scan_results")]
    public ScanResult? ScanResult { get; set; }
    [JsonProperty("stored")]
    public bool Stored { get; set; }
}
public class ScanResult
{
    [JsonProperty("total_avs")]
    public int AntiVirusScan { get; set; }
    [JsonProperty("total_detected_avs")]
    public int TotalAVScanDetected { get; set; }
    [JsonProperty("current_av_result_a")]
    public string? AVResultScan { get; set; }
    [JsonProperty("scan_all_result_a")]
    public string? AllResultScan { get; set; }
}
public class Sanitize
{
    [JsonProperty("result")]
    public string? Result { get; set; }
    [JsonProperty("progress_percentage")]
    public int Percentage { get; set; }
    [JsonProperty("file_path")]
    public string? FileSanitized { get; set; }

}

private FileResponse? fileResponse = new FileResponse();
private FileEntry file = new FileEntry();
private AnalysisResult analysis = new AnalysisResult();
private bool alertVisible = false;
private bool HasNoDocument = true;

private bool analisedFile = false;
```

Figura 25 - Variáveis locais e Classes da página Sanitizer.razor

`FileResponse` é a responsável por receber toda a informação útil retornada, da resposta do envio do ficheiro para limpeza.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

A classe `AnalysisResult` é a classe que diz respeito ao retorno dos resultados obtidos da limpeza e *scan* do ficheiro enviado para a API. Esta classe é constituída por uma classe `Sanitize` e uma classe `ScanResult`. Também é composta por um `bollean Stored`, que é utilizado para saber se o ficheiro para download está disponível ou não.

A classe `ScanResult` é o resultado do *scan* efetuado pelos antivírus presentes na API, enquando que a classe `Sanitize` é o resultado da limpeza que foi efetuada ao ficheiro pelo CDR.

Estas são as classes fundamentais para apresentar a melhor informação sobre o ficheiro, e o seu estado, tanto no ato de *scan* do ficheiro, como no ato de limpeza.

Para efetuar a associação dos valores recebidos nas chamadas aos endpoints aos atributos das classes, foram criadas as variáveis `fileResponse`, `file` e `analysis`. A variável `file` é do tipo `FileEntry` que é uma classe incorporada na biblioteca Blazorise.

Foram também criadas variáveis para gravar alguns valores que vão definir que ação é que o *frontend* vai tomar, como por exemplo esconder ou mostrar botões, os *cards* ou o alerta.

```
private void OnChanged(FileChangedEventArgs e)
{
    try
    {
        analisedFile = false;
        HasNoDocument = false;
        file = (FileEntry)e.Files[0];
    }
    catch (Exception exc)
    {
        Console.WriteLine(exc.Message);
    }
}
```

Figura 26 - Método OnChange() da página Sanitizer.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
private async Task SubmitFile()
{
    try
    {
        file.Name = Regex.Replace(file.Name, @"[^\u0000-\u007F]+",
string.Empty);
        var fileContent = new
StreamContent(file.OpenReadStream(10000000));
        fileContent.Headers.ContentDisposition = new
ContentDispositionHeaderValue("form-data")
            {
                Name = "file",
                FileName = file.Name
            };
        var client = new HttpClient();
        var request = new HttpRequestMessage
            {
                Method = HttpMethod.Post,
                RequestUri = new
Uri("https://api.metadefender.com/v4/file"),
                Headers =
                      {
                        { "apikey", "7ef4ffb3c5ab55acd139687e63ee2777" },
                        { "filename", file.Name },
                        { "rule", "sanitize" },
                      },
                Content = new MultipartFormDataContent
                      {fileContent}
            };
        using (var response = await client.SendAsync(request))
        {
            if (response.StatusCode == System.Net.HttpStatusCode.OK)
            {
                alertVisible = analisedFile = true;
                var jsonString = await
response.Content.ReadAsStringAsync();
                var fileResponseFromApi =
JsonConvert.DeserializeObject<FileResponse>(jsonString);

                fileResponse = new FileResponse()
                    {
                        DataId = fileResponseFromApi.DataId,
                        Status = fileResponseFromApi.Status,
                        SHA1 = fileResponseFromApi.SHA1,
                        SHA256 = fileResponseFromApi.SHA256
                    };
                await RequestAnalysis();
            }
        }
    }
    catch (Exception exc){
        Console.WriteLine(exc.Message);}
}
```

Figura 27 - Método SubmitFile() da página Sanitizer.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Para o ficheiro do qual fazemos *upload* ser associado à variável `file`, foi preciso criar a regra no *change* do *input* do ficheiro, representado na Figura 26.

Após o a inserção do ficheiro no *input*, podemos submeter o ficheiro e para isso será preciso enviar este para a API através do método apresentado na Figura 27, o `SubmitFile()`. Neste caso vamos ter de utilizar um `Stream` para a leitura do ficheiro e limitar a 10MB para não serem enviados ficheiros de um tamanho exagerado para a API

```
private async Task RequestAnalysis()
{
    try
    {
        var client = new HttpClient();
        var request = new HttpRequestMessage
            {
                Method = HttpMethod.Get,
                RequestUri = new
Uri("https://api.metadefender.com/v4/file/" + fileResponse.DataId),
                Headers =
            {
                { "apikey", "7ef4ffb3c5ab55acd139687e63ee2777" },
                { "x-file-metadata", "1" }
            }
            };
        using (var response = await client.SendAsync(request))
        {
            if (response.StatusCode == System.Net.HttpStatusCode.OK)
            {
                var jsonString = await
response.Content.ReadAsStringAsync();
                var fileResponseFromApi =
JsonConvert.DeserializeObject<AnalysisResult>(jsonString);
                if (fileResponseFromApi != null)
                {
                    analysis = new AnalysisResult()
                        {
                            Sanitize = fileResponseFromApi?.Sanitize,
                            ScanResult = fileResponseFromApi?.ScanResult,
                            Stored = fileResponseFromApi.Stored
                        };
                }
            }
        }
    }
    catch (Exception exc)
    {
        Console.WriteLine(exc.Message);
    }
}
```

Figura 28 - Método RequestAnalysis() da página Sanitizer.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

nestes testes. Por defeito o `Stream` tem um tamanho máximo de 512KB, daí se ter dado um limite um pouco maior, mas noutro contexto, este limite pode ser aumentado, bastando alterar este no código.

Quando a resposta da API é recebida com sucesso, irá aparecer um alerta a avisar que o *upload* do ficheiro foi realizado com sucesso, e irão ser mapeados os valores da resposta para o `fileResponse`. Após isto, será efetuada a chamada representada na Figura 28,

```
<PageTitle>Sanitizer</PageTitle>
<div class="row w-100">
    <Alert Color="Color.Success" @bind-Visible="@alertVisible">
        <AlertDescription>
            Ficheiro carregado com sucesso
        </AlertDescription>
        <CloseButton />
    </Alert>
</div>
<div class="row mt-5">
    <div class="col-6">
        <div class="card w-100" style="height: 300px;">
            <div class="card-header fw-bold">Upload File Here</div>
            <div class="card-body">
                <h5 class="card-title mt-2 mb-2">Sanitize your file</h5>
                <Field class="mb-4">
                    <FileEdit Changed="@OnChanged" />
                </Field>

            </div>
            <div class="card-footer">
                <Button Type="ButtonType.Submit"
Disabled="@HasNoDocument" Clicked="@SubmitFile"
Color="Color.Primary">Send to analysis</Button>
            </div>
        </div>
    </div>
    @if (analisedFile)
    {
        <div class="col-6">
            <div class="card w-100" style="height: 300px;">
                <div class="card-header fw-bold">File Data</div>
                <div class="card-body">
                    <h5 class="card-title mt-2 mb-2">@file.Name</h5>
                    <p>DataId -> @fileResponse.DataId</p>
                    <p>Status -> @fileResponse.Status</p>
                    <p>SHA1 -> @fileResponse.SHA1</p>
                    <p>SHA256 -> @fileResponse.SHA256</p>
                </div>
            </div>
        </div>}
</div>
```

Figura 29 - Frontend - parte I da página Sanitizer.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

para ir buscar o *status* da análise. Maior parte dos dados virão vazios nesta altura, devido à demora que a análise leva a ser feita, mas o valor que interessa é o *status* do *Scan* dos antivírus.

Esta chamada pode ser feita depois nos dois botões onde se pode atualizar o *status* do *scan* ou no botão que permite ir buscar o *link* para o ficheiro.

Todos os dados serão apresentados nas variáveis que estão dispostas pelo *frontend*, como podemos ver na Figura 29 e Figura 30. Estas estão todas associadas aos atributos das classes. Existem também validações que vão sendo feitas para certos componentes aparecerem, ou não quando alguns valores são assumidos.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
@if (analisedFile)
{<div class="row mt-3">
        <div class="card w-100" style="height: 350px;">
            <div class="card-header fw-bold">analysis Result</div>
            <div class="card-body">
                <div class="row">
                    <h5 class="card-title mt-2 mb-2">@file.Name</h5>
                </div>
                <div class="row">
                    <div class="col-6">
                        <h3>Scan Result</h3>
                        <p>Anti Virus Scan ->
@analysis?.ScanResult?.AntiVirusScan</p>
                        <p>Total Scan Detected ->
@analysis?.ScanResult?.TotalAVScanDetected</p>
                        @if
(string.IsNullOrEmpty(analysis?.ScanResult?.AVResultScan))
                        {<p>Scan Result ->
@analysis?.ScanResult?.AllResultScan</p>}
                        else
                        {<p>Scan Result ->
@analysis?.ScanResult?.AVResultScan</p>}
                    </div>

                    <div class="col-6">
                        <h3>Sanitize Result</h3>
                        <p>Result Sanitize ->
@analysis?.Sanitize?.Result</p>
                        <p>Percentage ->
@analysis?.Sanitize?.Percentage</p>
                        @if
(!string.IsNullOrEmpty(analysis?.Sanitize?.FileSanitized))
                        {<Button Color="Color.Success"
Type="ButtonType.Link" To="@analysis?.Sanitize?.FileSanitized"
Target="Target.Blank">Download File</Button>}
                    </div>
                </div>
            </div>
            <div class="card-footer">
                @if (string.IsNullOrEmpty(@analysis?.Sanitize?.Result))
                {<Button Type="ButtonType.Submit"
Clicked="@RequestAnalysis" Color="Color.Primary"
Margin="Margin.Is4.FromEnd">Refresh to Get Results</Button>}
                @if
(string.IsNullOrEmpty(@analysis?.Sanitize?.FileSanitized))
                {
                    <Button Type="ButtonType.Submit"
Clicked="@RequestAnalysis" Color="Color.Primary">Refresh to Get
File</Button>
                }
            </div>
        </div>
    </div>}
```

Figura 30 - Frontend - parte II da página Sanitizer.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

3.2.2.6 Código página Upload List

Para o código da página `Upload List`, foram inseridas seis classes que são fundamentais para a página em questão, estando elas descritas na Figura 32. Uma delas é fundamental para a funcionalidade do botão de *download* do ficheiro limpo, na lista dos *uploads*. Este botão vai estar disponível no máximo dois dias, devido à validade do ficheiro no repositório da API.

A classe `DataObject` é fundamental para a chamada que retorna o histórico de *uploads*. O objeto retornado é um único objeto que contém dentro dele um *array* de múltiplos `FileScanned`. A classe `AnalysisResult` é a classe que é utilizada para ser feita a chamada g*et* do ficheiro em cada uma das linhas da tabela, porque o *endpoint* do histórico de *uploads* não devolve o URL do ficheiro no repositório.

Para as chamadas aos *endpoints* também precisamos de duas variáveis, uma das quais o *array* de `FileScanned files`, e a variável do tipo `AnalysisResult Analysiss`, representadas ambas na Figura 31.

Para popular a tabela, é preciso executar uma chamada ao *endpoint* assim que a página é carregada com o método `OnInitializedAsync()`, representado na Figura 33 que devolve a lista de ficheiros carregados para a API. Após a receção, para cada item `files` vamos fazer uma chamada ao *endpoint* através do método `RequestAnalysis()`, representado na Figura 34, que devolve todos os dados do ficheiro, conseguindo assim ir buscar o *link* para o *download* do ficheiro em questão. Caso este ficheiro não exista, o *link* vem vazio e já não pode ser feito o *download* do ficheiro.

```
private FileScanned[]? files = null;
private AnalysisResult analysis = new AnalysisResult();
```

Figura 31 - Variáveis locais da página List.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
public class AnalysisResult
 {
     [JsonProperty("sanitized")]
     public Sanitize? Sanitize { get; set; }
 }
 public class FileScanned
 {
     [JsonProperty("data_id")]
     public string DataId { get; set; }
     [JsonProperty("scan_results")]
     public ScanResult? ScanResult { get; set; }
     [JsonProperty("file_info")]
     public FileInformation? FileInformation { get; set; }
     [JsonProperty("sanitized")]
     public Sanitize? SanitizeInfo { get; set; }
     public string? FilePath { get; set; }
 }
 public class ScanResult
 {
     [JsonProperty("total_avs")]
     public int TotalAntiVirusScan { get; set; }
     [JsonProperty("start_time")]
     [DisplayFormat(ApplyFormatInEditMode = true, DataFormatString =
"{0:MM/dd/yyyy}")]
     public DateTime Date { get; set; }
     [JsonProperty("total_detected_avs")]
     public int TotalAVScanDetected { get; set; }
     [JsonProperty("current_av_result_i")]
     public int AVResultScan { get; set; }
 }
 public class FileInformation
 {
     [JsonProperty("sha1")]
     public string SHA1 { get; set; }
     [JsonProperty("display_name")]
     public string Name { get; set; }
 }
 public class Sanitize
 {
     [JsonProperty("result")]
     public string? Result { get; set; }
     [JsonProperty("progress_percentage")]
     public int Percentage { get; set; }
     [JsonProperty("file_path")]
     public string? FileSanitized { get; set; }
 }
 public class DataObject
 {
     [JsonProperty("data")]
     public FileScanned[]? Data { get; set; }

 }
```

Figura 32 - Classes da página List.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
protected override async Task OnInitializedAsync()
{
    try
    {
        var client = new HttpClient();
        var request = new HttpRequestMessage
            {
                Method = HttpMethod.Get,
                RequestUri = new
Uri("https://api.metadefender.com/v4/apikey/scan-history"),
                Headers =
              {
                { "apikey", "7ef4ffb3c5ab55acd139687e63ee2777" }
              }
            };
        using (var response = await client.SendAsync(request))
        {
            var jsonString = await response.Content.ReadAsStringAsync();
            DataObject? data =
JsonConvert.DeserializeObject<DataObject>(jsonString);
            files = data?.Data;
            foreach(FileScanned file in files)
            {
                await RequestAnalysis(file.DataId);
                file.FilePath = analysis?.Sanitize?.FileSanitized;
            }
        }
    }
    catch (Exception exc)
    {
        Console.WriteLine(exc.Message);
    }
}
```

Figura 33 - Método OnInitializedAsync() da página List.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

```
private async Task RequestAnalysis(string dataId)
{
    try
    {
        var client = new HttpClient();
        var request = new HttpRequestMessage
            {
                Method = HttpMethod.Get,
                RequestUri = new
Uri("https://api.metadefender.com/v4/file/" + dataId),
                Headers =
            {
                { "apikey", "7ef4ffb3c5ab55acd139687e63ee2777" },
                { "x-file-metadata", "1" }
            }
            };
        using (var response = await client.SendAsync(request))
        {
            if (response.StatusCode == System.Net.HttpStatusCode.OK)
            {
                var jsonString = await
response.Content.ReadAsStringAsync();
                var fileResponseFromApi =
JsonConvert.DeserializeObject<AnalysisResult>(jsonString);
                if (fileResponseFromApi != null)
                {
                    analysis = new AnalysisResult()
                        {
                            Sanitize = fileResponseFromApi?.Sanitize
                        };

                }
            }
        }
    }
    catch (Exception exc)
    {
        Console.WriteLine(exc.Message);
    }
}
```

Figura 34 - Método RequestAnalysis() da página List.razor

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

4 TESTES E ANÁLISE DE RESULTADOS

Neste capítulo procedemos aos testes da aplicação desenvolvida no Capítulo 4, mas também aos testes da aplicação que escolhemos para efetuar a limpeza dos nossos ficheiros. Durante os testes vamos recolher os resultados que a aplicação MetaDefender Cloud nos vai retornar, mas para garantir que esta aplicação é eficaz, usar como apoio a plataforma VirusTotal (*VirusTotal*, 2024). Desta maneira conseguimos entender de uma forma mais séria se a aplicação remove fontes maliciosas na sua totalidade ou não.

Após a recolha dos resultados, dar-se-á lugar à análise dos resultados obtidos nos testes.

4.1 Testes da Solução

Após a conclusão do desenvolvimento de todo o código para a aplicação correr sem dar erros, e efetuar todos os processos que são pretendidos, foram iniciados os testes da nossa aplicação, com o envio de vários tipos de ficheiros, uns infetados e outros sem qualquer tipo de vírus. Para o nosso teste e para a verificação da limpeza, utilizámos a ferramenta web que a plataforma VirusTotal (*VirusTotal*, 2024) nos fornece para analisar se um ficheiro está infetado ou não com algum agente malicioso.

Assim, a sequência dos testes passará por efetuar um *scan* do ficheiro no VirusTotal para verificar se o ficheiro está realmente infetado ou não, como exemplo na Figura 35, fazer o *upload* do ficheiro na nossa aplicação para efetuarmos a sua limpeza, fazer o *download* do mesmo e depois voltar a passar o ficheiro no VirusTotal, como exemplificado também na Figura 36, para garantir que o ficheiro foi limpo.

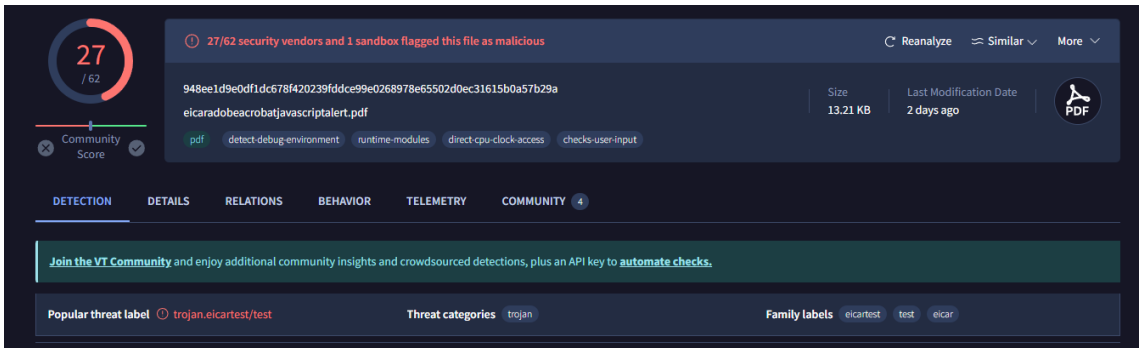

*Figura 35 - Teste antes de limpeza com CDR na plataforma VirusTotal (*VirusTotal, *2024)*

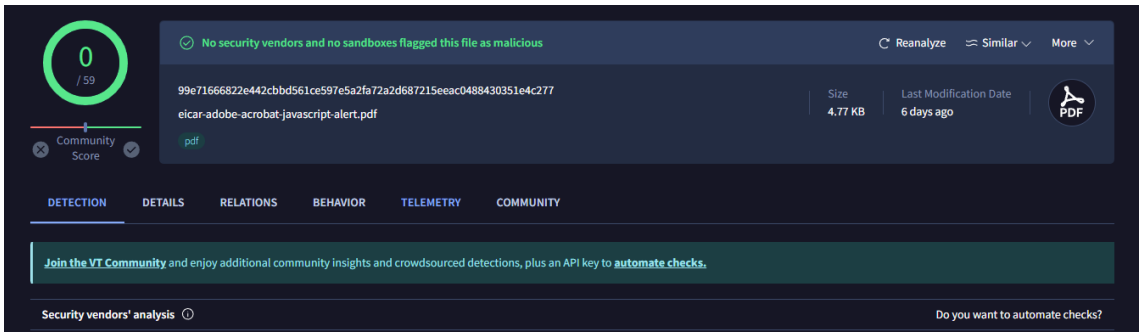

*Figura 36 - Teste após limpeza com CDR na Plataforma VirusTotal (*VirusTotal, *2024)*

Para efetuar estes testes, recorremos a um repositório no github que continha ficheiros infetados com vírus (fire1ce, 2020). Este repositório disponibiliza vários formatos de ficheiros para estes testes, desde PDFs, ficheiros Word, Excel e Powerpoints. Como nas empresas maior parte dos ficheiros transferidos são ficheiros do Office, estes ficheiros são ideais para testar a nossa aplicação e a eficácia da API.

Dos ficheiros recolhidos para os testes, foram utilizados catorze, sendo que dos vinte testes que foram realizados, seis deles foram efetuados com ficheiros PDF sem qualquer tipo componente malicioso neles. Estes testes com documentos sem vírus também foram efetuados para testar a análise dos antivírus da API e se o ficheiro era desmontado e limpo como era de esperar.

As imagens descritivas dos testes da aplicação estão presentes na secção Anexos – Testes Aplicação, para melhor visualização dos mesmos. Para melhor interpretação da sequência de imagens, estas estão divididas pelo número do teste. Por vezes, dentro do número do teste existe apenas duas imagens. Isto deve-se ao bloqueio do ficheiro por parte do MetaDefender Cloud, porque o tipo ou algo dentro dele é incompatível com a aplicação.

4.2 Resultados e Análise

Antes da realização dos testes, foi criada uma tabela para recolher os resultados relativos a cada ficheiro sobre os seguintes dados:

- Resultado recolhido do scan através do VirusTotal (*VirusTotal*, 2024), antes do envio para o MetaDefender Cloud.
- total de deteções através dos antivírus no MetaDefender Cloud.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

- Tempo total de scan.
- Resultado do scan: "Infected" ou "No Threat detected".
- Tamanho do ficheiro enviado
- Resultado recolhido do scan através do VirusTotal, após o download do ficheiro limpo.
- Se o ficheiro em questão pertence ao *dataset* de ficheiros infetados.

Para entender melhor os resultados obtidos sobre cada situação em cada fase, dividimos estes em duas tabelas distintas. A Tabela 4 representa os valores obtidos no primeiro scan efetuado no VirusTotal, antes do envio dos ficheiros para a API do MetaDefender Cloud. Para esta tabela, foram usadas três variáveis em que uma delas foi controlada, detalhando se o ficheiro que enviámos pertencia ao *dataset* do qual recolhemos a nossa amostra de ficheiros, e as outras duas, resultados obtidos a partir do VirusTotal.

Ficheiro	**Nº de Antivírus**	**Nº de deteções**	**Ficheiro malicioso**
eicar-adobe-acrobat-attachment.pdf	63	39	Sim
2307.14057.pdf	62	0	Não
eicar-adobe-acrobat-javascript-alert.pdf	62	27	Sim
eicar-com	65	62	Sim
paper 13.pdf	60	0	Não
eicar-excel-macro-msgbox.xlsm	63	28	Sim
eicar-word-macro-write-file.docm	65	35	Sim
sim2018.pdf	60	0	Não
eicar-excel-dde-cmd-powershell-echo.xls	61	34	Sim
eicar-powerpoint-action-macro-msgbox.ppt	62	28	Sim
vonsolms2013.pdf	59	0	Não
eicar-test.txt	67	64	Sim
eicar-word-macro-cmd-echo.docm	65	39	Sim

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Content_Disarm_and_Reconstruction _of_RTF_Files_a_Zero_File_Trust_ Methodology.pdf	60	0	Não
eicar-powerpoint-action-powershell-echo.ppt	62	27	Sim
eicar-excel-macro-write-file.xls	63	35	Sim
eicar-word-macro-powershell-echo.docm	66	43	Sim
CISA_Zero_Trust_Maturity_Model_ Version_2_508c.pdf	55	0	Não
eicar-excel-macro-powershell-echo.xlsm	63	41	Sim
eicar-powerpoint-action-powershell-echo.pptx	65	28	Sim

*Tabela 4 – Resultados dos testes no website VirusTotal (*VirusTotal, *2024)*

Depois de analisarmos estes dados podemos concluir que os ficheiros que pertenciam ao *dataset* de ficheiros infetados, e que foram enviados para análise, foram sempre identificados por algumas máquinas como potencial ficheiro infetado. Ao todo, em nove deles mais de 50% das máquinas detetaram alguma forma de vírus, enquanto em cinco dos ficheiros mais de metade das não detetaram que o ficheiro era malicioso. Nos restantes seis ficheiros nenhuma das máquinas detetou algo malicioso. Nota para os ficheiros eicar-com e o eicar-test.txt em que quase 100% das máquinas detetaram que os ficheiros continham vírus.

Com recurso à aplicação desenvolvida, estes ficheiros foram enviados, sem que tenha falhado nenhum envio, e os resultados das respostas da API sempre apresentados.

Quanto à análise após o envio destes ficheiros para a API, esta retornou os valores que são apresentados de seguida na tabela. Não serão apresentados o número de antivírus que efetuou o scan por o número ser fixo e não haver nenhuma variação dos vinte e três antivírus responsáveis por esta função.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Na Tabela 5 vamos utilizar os parâmetros recolhidos que se traduzem nos mais condizentes para o nosso estudo e relevantes para os nossos resultados, que são:

- Total de deteções Antivírus
- Tempo de scan
- Retorno do ficheiro
- Tamanho do ficheiro

Ficheiro	Total de deteções Antivírus	Tempo de scan	Retorno do ficheiro	Tamanho do ficheiro
eicar-adobe-acrobat-attachment.pdf	11	203	Blocked	7
2307.14057.pdf	0	623	Sim	658
eicar-adobe-acrobat-javascript-alert.pdf	7	209	Sim	13
eicar-com	19	204	Blocked	1
paper 13.pdf	0	239	Sim	781
eicar-excel-macro-msgbox.xlsm	5	207	Sim	11
eicar-word-macro-write-file.docm	7	207	Sim	16
sim2018.pdf	0	213	Sim	275
eicar-excel-dde-cmd-powershell-echo.xls	10	210	Sim	25
eicar-powerpoint-action-macro-msgbox.ppt	6	213	Sim	89
vonsolms2013.pdf	0	332	Sim	304
eicar-test.txt	19	206	Blocked	1
eicar-word-macro-cmd-echo.docm	9	204	Sim	16
Content_Disarm_and_Reconstruction_of_RTF_Files_a_Zero_File_Trust_Methodology.pdf	0	729	Sim	1788

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

eicar-powerpoint-action-powershell-echo.ppt	8	203	Sim	109
eicar-excel-macro-write-file.xls	8	340	Sim	31
eicar-word-macro-powershell-echo.docm	10	206	Sim	16
CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf	0	767	Sim	1430
eicar-excel-macro-powershell-echo.xlsm	9	211	Sim	11
eicar-powerpoint-action-powershell-echo.pptx	4	790	Sim	35

Tabela 5 - Resultados dos testes efetuados no CDRFileCleanApp, oriundos do MetaDefender Cloud

Com a avaliação destes dados recolhidos na análise pela API que utilizámos, verificamos que houve uma boa análise dos ficheiros. Desta análise retiramos que os antivírus não detetaram nenhum tipo de vírus nos ficheiros que não pertenciam ao *dataset*. Para além disso, notamos que houve dois ficheiros do *dataset* de ficheiros infetados que foram detetados por dezanove dos vinte e três antivírus, o eicar-com e o eicar-test.txt. Desta forma, o resultado da aplicação entrou em concordância com a tabela anterior, pois já tinham sido identificados como os ficheiros que mais reportes tinham sofrido no passo anterior.

Nesta tabela também podemos reparar que não foram devolvidos três dos vinte ficheiros, gerando assim um retorno de ficheiros de cerca de 85%. Estes ficheiros não retornados, tinham associado como tipo de ficheiro um .PDF, um executável, e um txt.

Quanto ao tempo de execução da análise, o tempo médio é de 325,8 milissegundos. Dado que o tamanho dos ficheiros varia um pouco, o *scan* pode ser considerado rápido, mas retirando o tempo dos três maiores ficheiros ficamos com uma média de *scan* de 239,05 milissegundos. Com esta exclusão podemos concluir que o tempo de *scan* varia bastante com o tamanho do ficheiro. Contrastando com o tamanho do ficheiro, os tempos de *scan*

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

poderão ser mais curtos ou mais longos consoante os componentes que o ficheiro contiver dentro.

No exemplo destes três maiores ficheiros, existem imensas imagens na sua composição, o que faz com que o seu tamanho seja maior que um documento que apresente apenas texto, e consequentemente, a sua análise seja também mais demorada.

Após a análise e o retorno dos ficheiros, deu-se lugar aos testes no VirusTotal para confirmar se a limpeza do ficheiro retornado estava bem feita, e o resultado foi excelente. De todos os ficheiros que foram retornados e analisados, em nenhum dos ficheiros foi detetado algum tipo de vírus, sendo o resultado deste último scan um resultado muito positivo para a análise e execução de um CDR.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

CONCLUSÃO

Com o término do nosso desenvolvimento, esperamos ter contribuído para uma implementação de baixo nível de uma metodologia que devia de estar acessível a todos. Apesar de o nosso desenvolvimento ser local, a implementação numa empresa seria bastante simples, pois até poderia ser implementada dentro da rede interna da empresa, desde que haja uma ligação para a aplicação desenvolvida se ligar à API MetaDefender Cloud.

O desenvolvimento desta aplicação não só serviu como contribuição para a implementação de uma consciencialização de maior segurança numa pequena empresa, como a nível pessoal serviu para crescer no âmbito do meu trabalho e aumentar a capacidade de adaptação, quer com o uso de tecnologias que uso algumas vezes, mas principalmente com o uso de tecnologias que nunca utilizei e que fiquei a conhecer melhor como elas funcionam.

Limitações

Algumas limitações apareceram logo no início do projeto, aquando da realização do Capítulo 2, muito por causa da escassez de artigos diretamente relacionados com o CDR, o que me levou a basear-me maioritariamente em *websites* e documentação de empresas que têm produtos seus com esta metodologia.

Conforme já descrito também no ponto 4.1, houve um desafio importante para escolher que tipo de projeto seria feito, pois a direção seria a tentativa de implementação de uma tecnologia CDR OSS, o que veio a não acontecer. Os projetos CDR OSS atualmente disponíveis são feitos em versões antigas, e muitos deles obsoletos, de linguagens que não têm a ver com a linguagem em que tenho experiência de trabalho, e o qual tinha de ser refeito. Como não tenho bases de Python nem de Java, que eram as linguagens que os OSS estudados e explorados tinham, ficou decidido prescindir deste tipo de software e avançar com a construção de uma interface para utilizadores enviarem o seu documento e verem os dados do resultado da análise a este. Assim, como trabalho em ASP .Net, e de maneira a desenvolver capacidades em outras Frameworks dentro dos serviços Microsoft, escolhi realizar a interface em Blazor. A falta de conhecimento desta aplicação também

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

levou a que tivesse algumas limitações tal como a implementação de alguns componentes, a sua conexão para com o código ser bastante diferente do ASP .Net também criou algum atraso para adaptação, o uso de um serviço de *templates* e a aprendizagem rápida deste, também foram limitações que foram aparecendo ao longo da realização do projeto.

Trabalho futuro

Para trabalho futuro pretende-se pegar na aplicação e tratar dela, alterando um pouco o seu *layout* para a tornar mais atrativa para os utilizadores. Esta aplicação também poderá sofrer uma alteração para se tornar mais eficaz para o utilizador ao enviar vários ficheiros ao mesmo tempo para o *endpoint* do MetaDefender Cloud. Assim tinha de receber uma intervenção para mostrar os dados de uma forma dinâmica, que permitisse ver os dados de cada ficheiro conforme a sua seleção.

Como esta aplicação foi elaborada para ter uma utilização limitada, poderíamos pensar também em inserir uma página de início de sessão para limitarmos a utilização da aplicação a quem a ela tivesse acesso.

Com perspetiva de aumento do número de utilizadores também teriam de ser feitos desenvolvimentos ao nível de uma base de dados local para guardar a informação dos utilizadores, e dados relativos a estes.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

REFERÊNCIAS BIBLIOGRÁFICAS

Akailvi, S., Gautam, U., Bhandari, P., Rashid, H., Huff, P. D., & Springer, J. P. (2023). HELOT-Hunting Evil Life in Operational Technology. *IEEE Transactions on Smart Grid*, *14*(4), 3058–3071. https://doi.org/10.1109/TSG.2022.3222261

Andrew Park. (2023, April 13). *Open Source vs. Proprietary: Development, Licensing, Business Models, Security, and More*. Https://Www.Heavybit.Com/Library/Article/Open-Source-vs-Proprietary.

Caldwell, T. (2011). Ethical hackers: Putting on the white hat. *Network Security*, *2011*(7), 10–13. https://doi.org/10.1016/S1353-4858(11)70075-7

CNCS. (2023). *CERT.PT*. Https://Www.Cncs.Gov.Pt/Pt/Certpt/.

What is Content Disarm and Reconstruction. (2024, October 10). Https://Www.Checkpoint.Com/Cyber-Hub/Threat-Prevention/What-Is-Content-Disarm-and-Reconstruction-Cdr/.

CheckPoint. (2024). Https://Www.Checkpoint.Com/.

CNCS. (2023). *CIBERSEGURANÇA*.

cps.gov.uk. (2019, September 26). Https://Www.Cps.Gov.Uk/Legal-Guidance/Cybercrime-Prosecution-Guidance.

David Tutin. (2023, September). *What is Content Disarm and Reconstruction (CDR)?* Https://Www.Glasswall.Com/Blog/What-Is-Content-Disarm-and-Reconstruction-Cdr.

Dubin, R. (2023a). Content Disarm and Reconstruction of PDF Files. *IEEE Access*, *11*, 38399–38416. https://doi.org/10.1109/ACCESS.2023.3267717

Dubin, R. (2023b). Content Disarm and Reconstruction of RTF Files a Zero File Trust Methodology. *IEEE Transactions on Information Forensics and Security*, *18*, 1461–1472. https://doi.org/10.1109/TIFS.2023.3241480

fire1ce. (2020). *eicar-standard-antivirus-test-files*. Https://Github.Com/Fire1ce/Eicar-Standard-Antivirus-Test-Files.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Fitzgerald, B. (2006). The Transformation of Open Source Software. In *Source: MIS Quarterly* (Vol. 30, Issue 3).

ForcePoint. (2024). Https://Www.Forcepoint.Com/.

Fortinet. (2024). Https://Www.Fortinet.Com/.

Gibert, D., Mateu, C., Planes, J., & Marques-Silva, J. (2021). Auditing static machine learning anti-Malware tools against metamorphic attacks. *Computers and Security*, *102*. https://doi.org/10.1016/j.cose.2020.102159

Global Content Disarm and Reconstruction (CDR) Market. (2023, June 1). Https://Www.Transparencymarketresearch.Com/Content-Disarm-and-Reconstruction-Cdr-Market.Html.

Goutam, R. K. (2015). Importance of Cyber Security. In *International Journal of Computer Applications* (Vol. 111, Issue 7).

Malware protection test March. (2023, May 30). Https://Www.Av-Comparatives.Org/Tests/Malware-Protection-Test-March-2021/.

Hussain, A., Mohamed, A., & Razali, S. (2020, March 31). A Review on Cybersecurity: Challenges & Emerging Threats. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3386723.3387847

InterProbe. (2022). *CoDeRedlight*. Https://Github.Com/Interprobe/CoDeRedlight.

Kemp, S. (2024, January 31). *DIGITAL 2024: GLOBAL OVERVIEW REPORT*. Https://Datareportal.Com/Reports/Digital-2024-Global-Overview-Report.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, *105*. https://doi.org/10.1016/j.cose.2021.102248

Lenarduzzi, V., Taibi, D., Tosi, D., Lavazza, L., & Morasca, S. (2020). Open Source Software Evaluation, Selection, and Adoption: A Systematic Literature Review. *Proceedings - 46th Euromicro Conference on Software Engineering and Advanced*

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Applications, SEAA 2020, 437–444. https://doi.org/10.1109/SEAA51224.2020.00076

Linux security Expert. (2021). *Linux security Expert*. Https://Linuxsecurity.Expert/.

Maalej, W., & Robillard, M. P. (2013). Patterns of knowledge in API reference documentation. *IEEE Transactions on Software Engineering*, *39*(9), 1264–1282. https://doi.org/10.1109/TSE.2013.12

Maxime Guerreiro. (2016, December). *DocBleach*. Https://Github.Com/Docbleach/DocBleach.

McDuffie, E. L., & Piotrowski, V. P. (2014). The Future of Cybersecurity Education. *Computer*, *47*(08), 67–69. https://doi.org/10.1109/MC.2014.224

Mee, P., Brandenburg, R., & Lin, W. (2021). *Oliver Wyman Forum Global Cyber Risk Literacy and Education Index*. https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html

MetaDefender Cloud. (2024). Https://Metadefender.Opswat.Com/.

Mozilla. (2023). *Mozilla Bleach*. Https://Github.Com/Mozilla/Bleach.

Odix. (2024). *Odix Technology*. Https://Www.Odi-x.Com/Odix-Technology/.

OPSWAT. (2024). *OPSWAT Deep CDR*. Https://Www.Opswat.Com/Technologies/Deep-Content-Disarm-and-Reconstruction.

Pahl, C., Brogi, A., Soldani, J., & Jamshidi, P. (2019). Cloud container technologies: A state-of-the-art review. *IEEE Transactions on Cloud Computing*, *7*(3), 677–692. https://doi.org/10.1109/TCC.2017.2702586

Petrosyan, A. (2023, February). *Most common malicious file types received globally via web and e-mail in 2022*. Https://Www.Statista.Com/Statistics/1238996/Top-Malware-by-File-Type/. https://www.statista.com/statistics/1238996/top-malware-by-file-type/

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Phạm, T. B., Nguyễn, N. H., V\~u, V. ông, & Trịnh, Q. K. (2021). *Content disarm and reconstruction for web application*.

OPSWAT. (2020). *Prevent Zero-day and Advanced Malware Threats with Content Disarm and Reconstruction (CDR) Technology*.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Raphaël Vinot. (2019). *CIRCLean*. Https://Github.Com/CIRCL/Circlean.

Sasa Software. (n.d.). *3rd. Party Applications*. www.sasa-software.com

Security Agency, I. (2023). *Zero Trust Maturity Model Version 2.0*. http://www.cisa.gov/tlp/.

Sim, G. (2018). Defending against the malware flood. *Network Security*, *2018*(5), 12–13. https://doi.org/10.1016/S1353-4858(18)30044-8

sunshine2021. (n.d.).

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*. https://doi.org/10.1016/j.irfa.2021.101795

VirusTotal. (2024, April). Https://Www.Virustotal.Com/Gui/Home/Upload.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Votiro. (2022, October 18). *Votiro*. Https://Votiro.Com/Resource-Center/What-Is-Cdr-Positive-Selection/.

Wetzig, C. (2022, November 10). *15 Alarming Cybersecurity Facts And Statistics*. Https://Thrivedx.Com/Resources/Article/Cyber-Security-Facts-Statistics?Referrer=cybint.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Wiseman, S. (2023, March 15). *Effective Content Disarm and Reconstruction*. Https://Www.Forcepoint.Com/Blog/x-Labs/Effective-Content-Disarm-Reconstruction.

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ANEXOS

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ANEXO POSTMAN - P

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

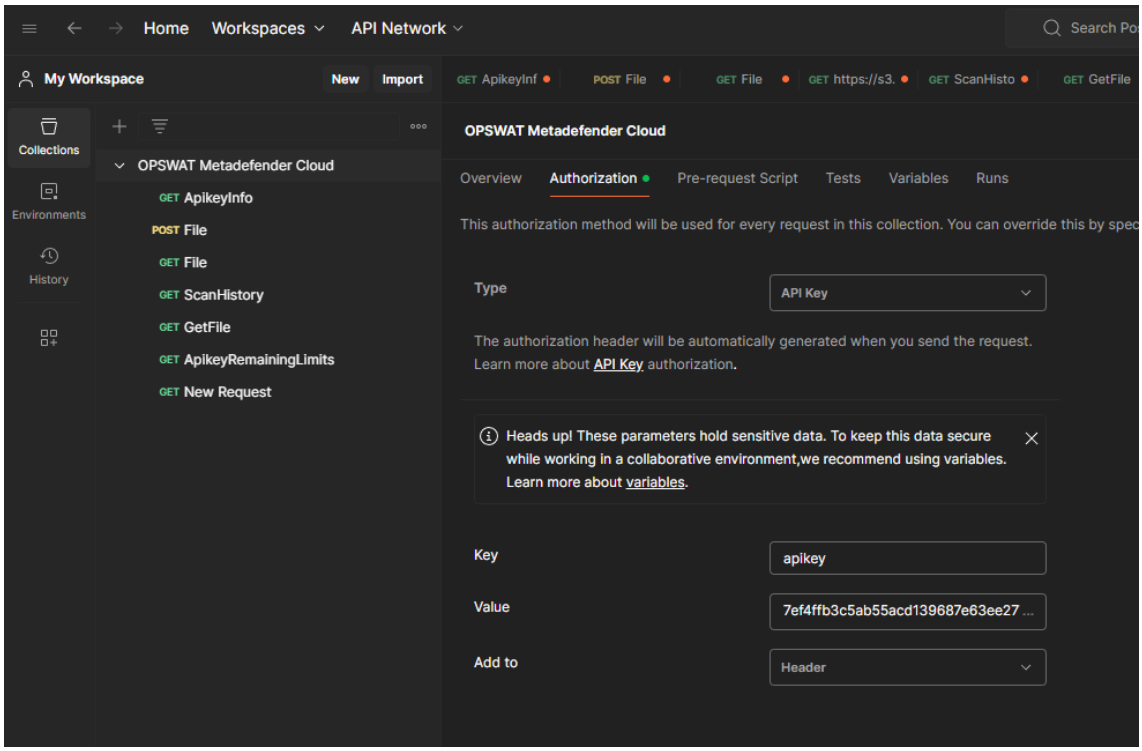

Figura 37 - P1 - Dados da ligação entre o Postman e a API MetaDefender Cloud

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

GET https://api.metadefender.com/v4/apikey/

Params Authorization Headers (7) Body Pre-request Script Tests Settings

Body Cookies Headers (13) Test Results

Pretty Raw Preview Visualize JSON


```
{
    "max_file_download": 100,
    "max_upload_file_size": 75,
    "max_archive_file_depth": 5,
    "max_archive_file_size": 75,
    "max_archive_file_number": 25,
    "limit_prevention": 100,
    "limit_reputation": 1000,
    "limit_threat_intel_search": 25,
    "limit_sandbox": 5,
    "limit_feed": 1000,
    "throttling_limit": 10,
    "workflow_rule": 0,
    "enforce_private_scan": false,
    "blocked_avs": [],
    "partner": 1,
    "time_interval": "daily",
    "qos_scan": "normal",
    "portal_api_key": "7ef4ffb3c5ab55acd139687e63ee2777",
    "created_at": "2024-04-15T00:03:37.656Z",
    "nickname": "throbbing_salad_bu9cvmmo",
    "sandbox_qos_scan": "normal",
    "expiration_date": "1970-01-01T00:00:00.000Z",
    "vulnerability_submissions": [],
    "is_enterprise": false,
    "mtls_only": false,
    "is_encrypt_enable": false,
    "source": "cognito",
    "sso_user_id": "b480be15-bef4-47b9-8afd-5e7e40941eff",
    "userid": "b480be15-bef4-47b9-8afd-5e7e40941eff",
    "license_change_note": "CreateNewUser",
    "mdc_license_type": "community",
    "updated_at": "2024-04-15T00:03:37.656Z",
    "paid_user": 0
}
```


Figura 38 - P2 - Resultado do pedido APIKeyInfo à API MetaDefender Cloud

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

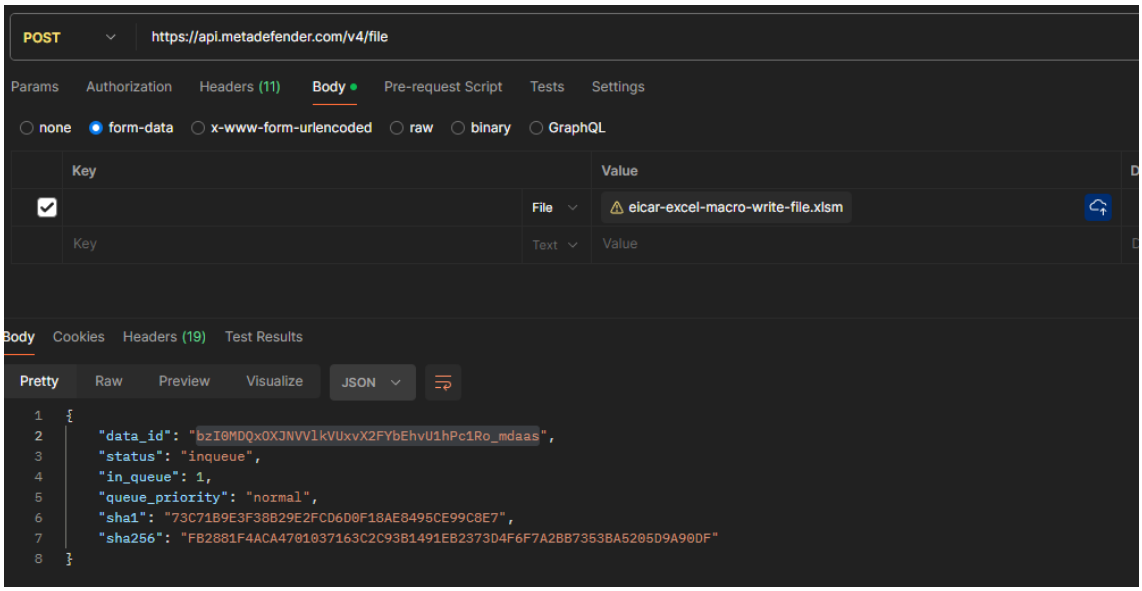

Figura 39 - P3 - Resultado do envio de um ficheiro para a API MetaDefender Cloud

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

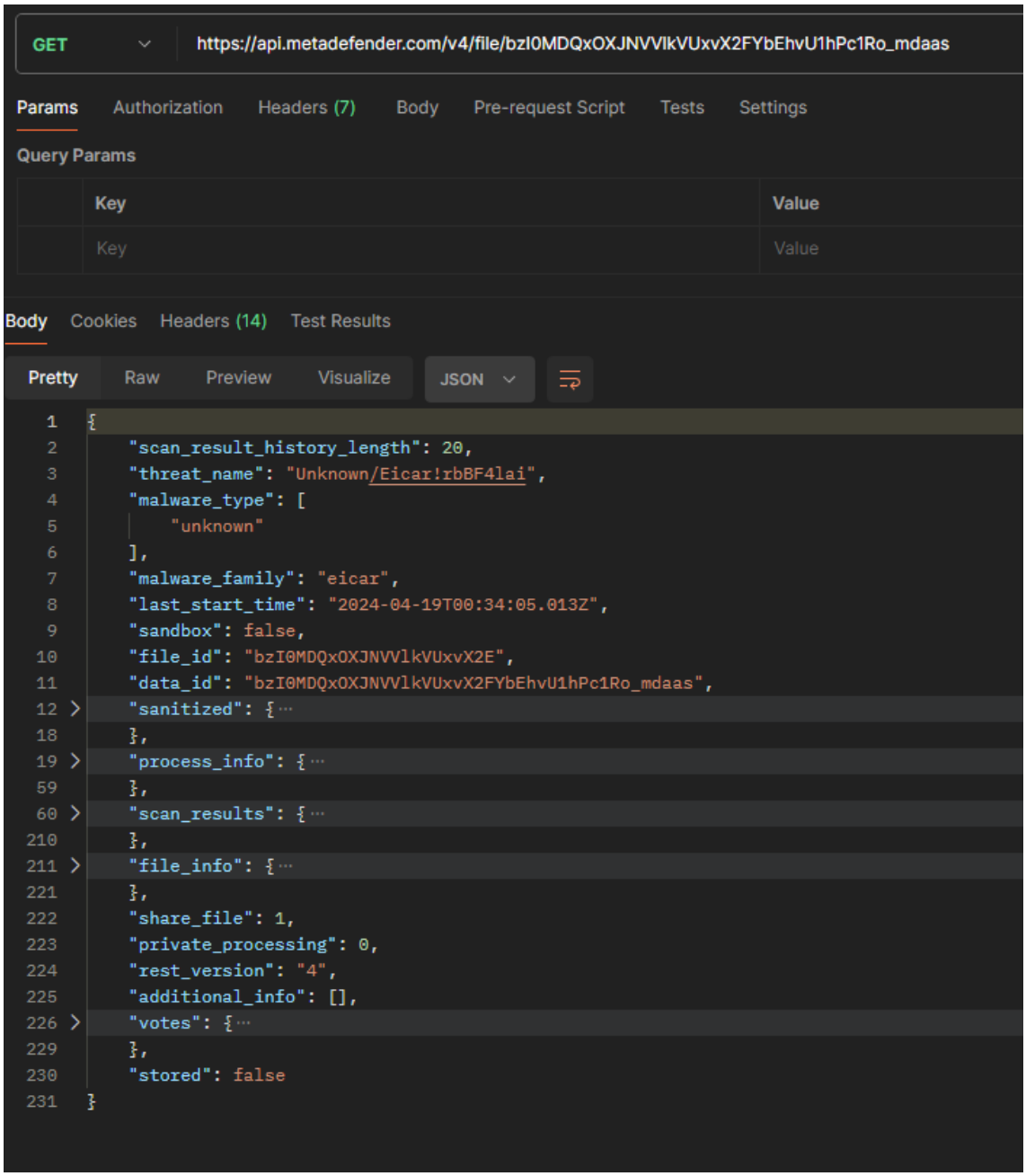

Figura 40 - P4 - Resultado do pedido de informação de um ficheiro da API MetaDefender Cloud

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

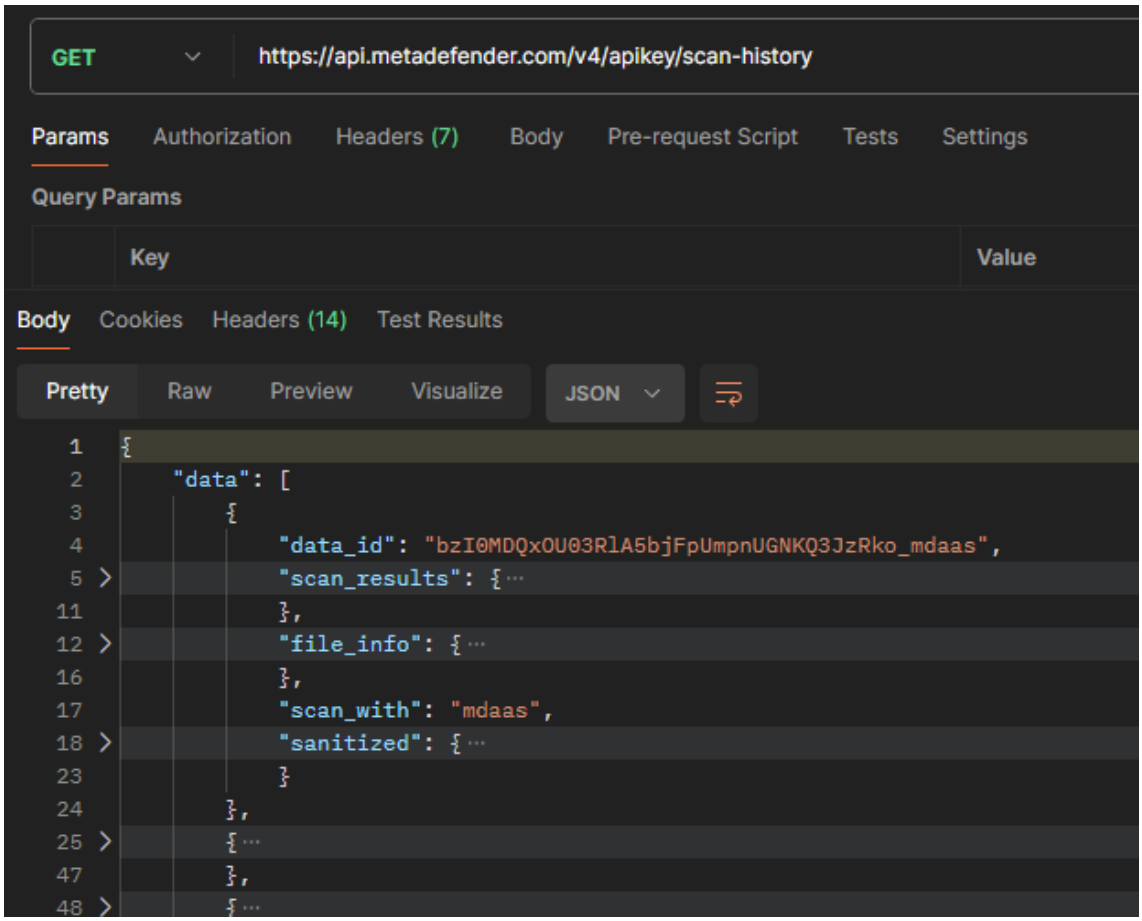

Figura 41 - P5 - Resultado do pedido de histórico de scan da API MetaDefender Cloud

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

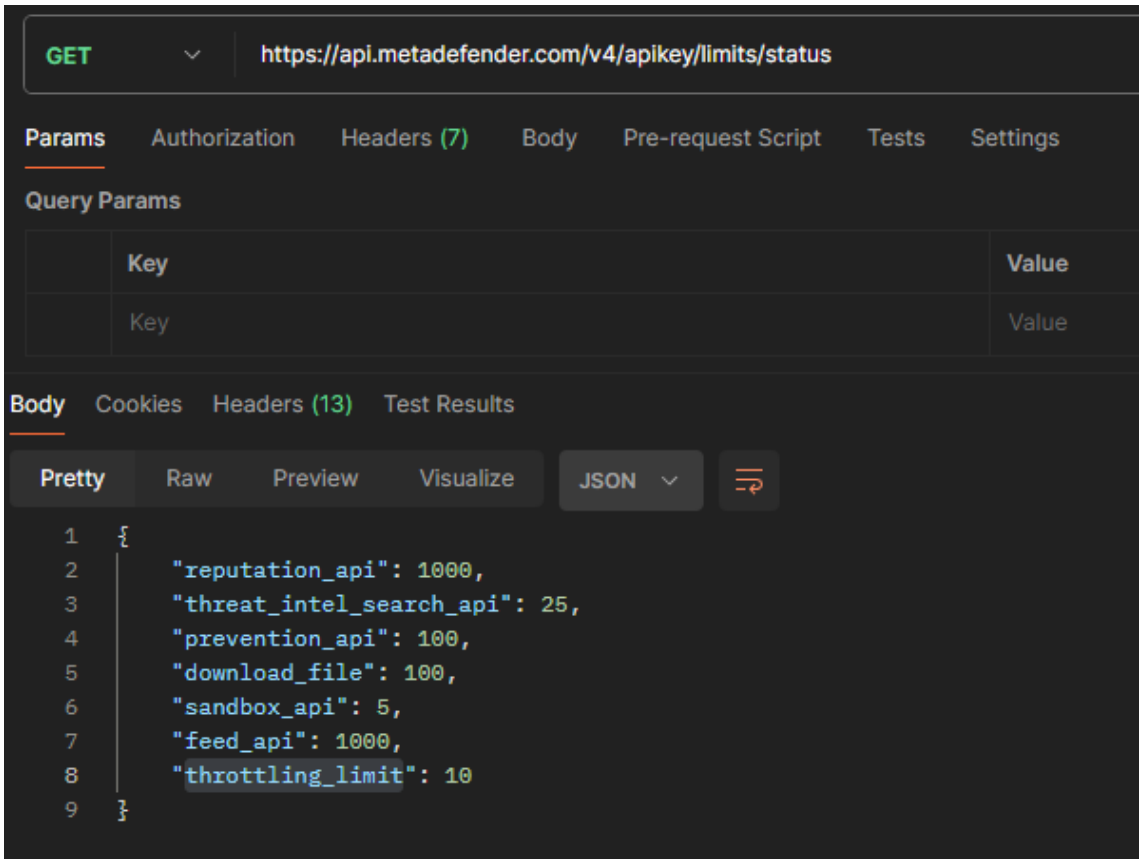

Figura 42 - P6 - Resultado do pedido de limites remanescentes da API MetaDefender Cloud

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

ANEXO TESTES - T

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 1 - eicar-adobe-acrobat-attachment.pdf

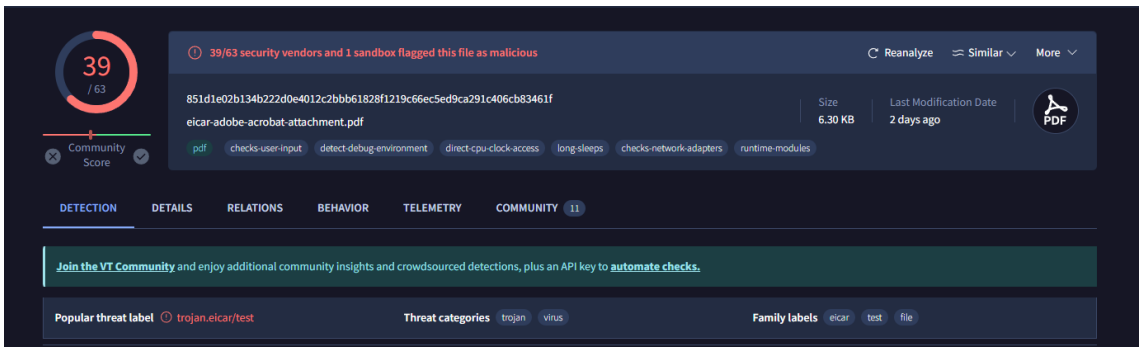

Figura 43 - T1 - Scan Test ficheiro1 no VirusTotal antes de limpeza no ficheiro

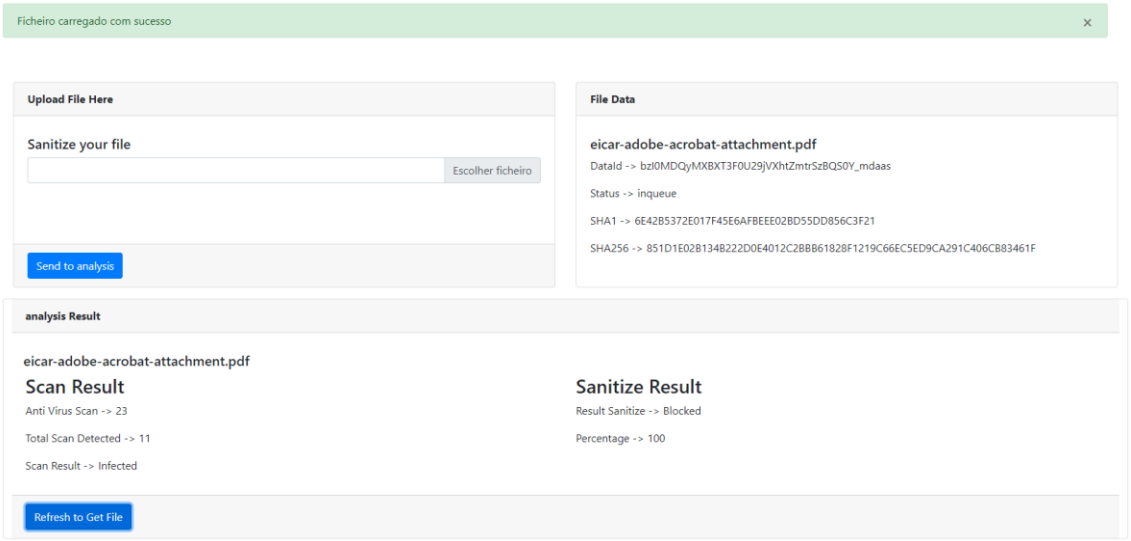

Figura 44 - T2 - Resultado do ficheiro 1 no CDRFileCleanerApp após envio do ficheiro para limpeza

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 2 -2307.14057.pdf

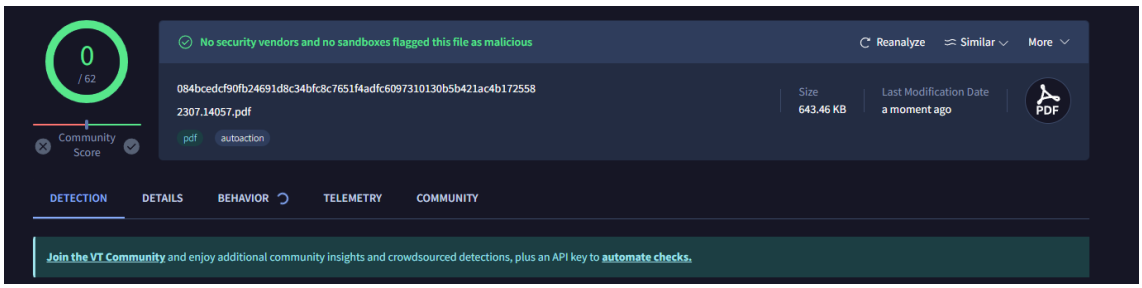

Figura 45 - T3 - Scan Test ficheiro2 no VirusTotal antes de limpeza no ficheiro

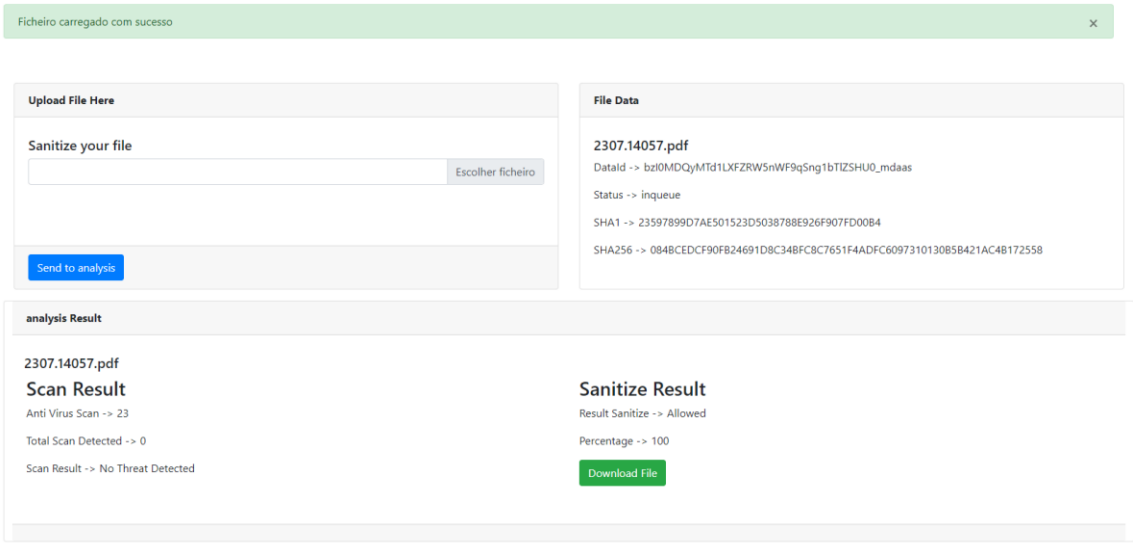

Figura 46 - T4 - Resultado do ficheiro 2 no CDRFileCleanerApp após envio do ficheiro para limpeza

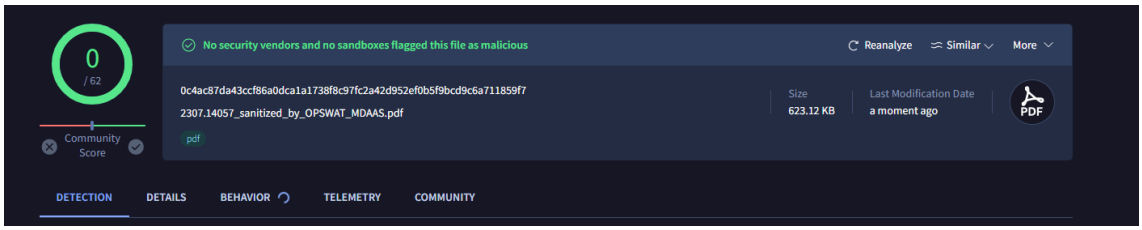

Figura 47 - T5 - Scan Test ficheiro 2 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 3 - eicar-adobe-acrobat-javascript-alert.pdf

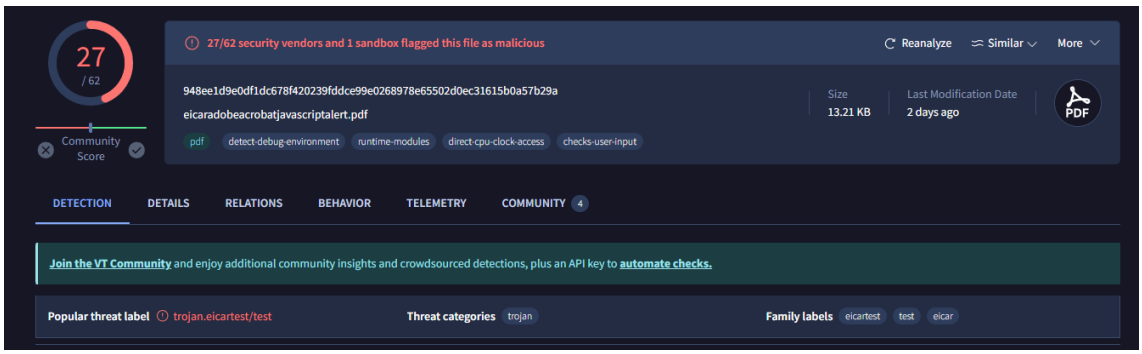

Figura 48 - T6 - Scan Test ficheiro3 no VirusTotal antes de limpeza no ficheiro

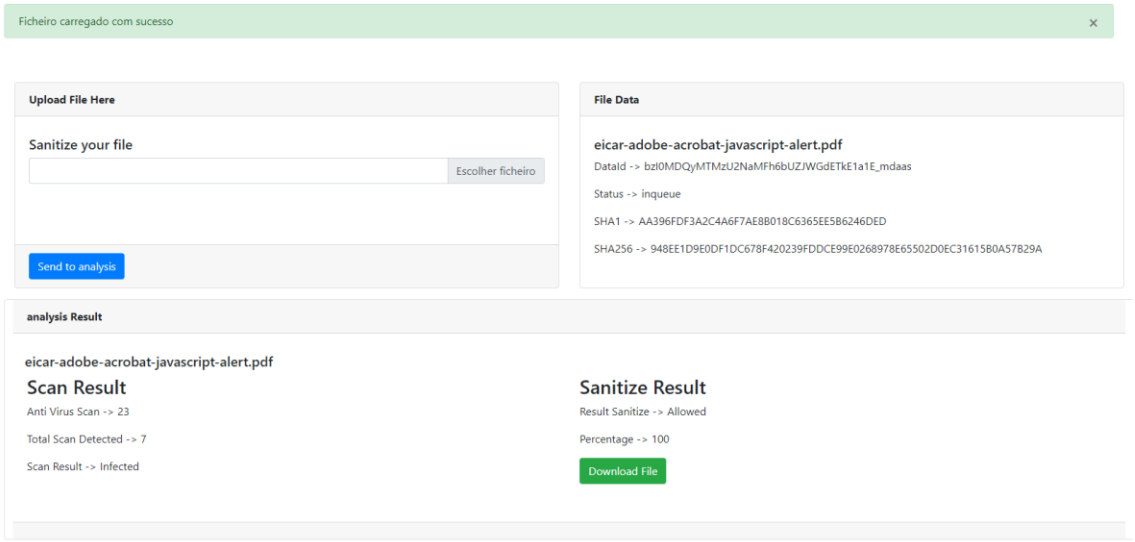

Figura 49 - T7 - Resultado do ficheiro 3 no CDRFileCleanerApp após envio do ficheiro para limpeza

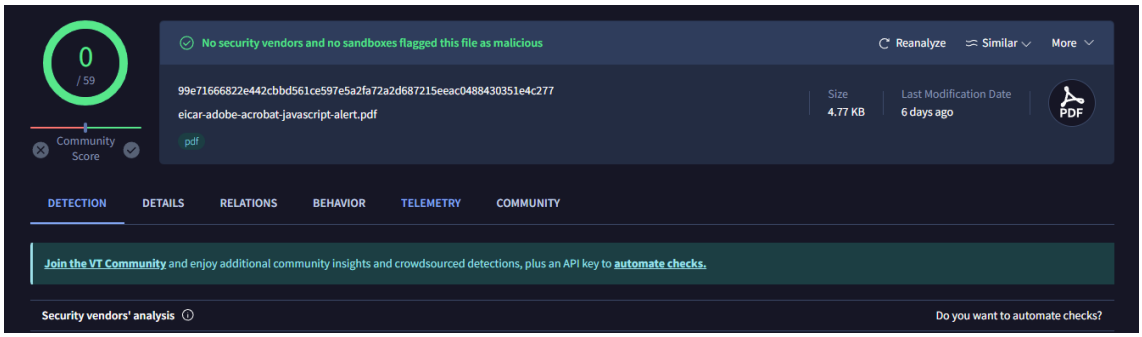

Figura 50 - T8 - Scan Test ficheiro 3 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 4 - eicar-com

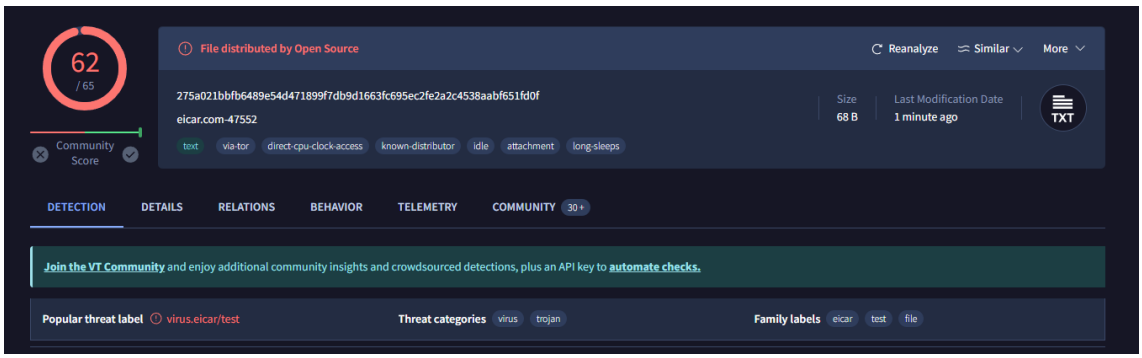

Figura 51 - T9 - Scan Test ficheiro 4 no VirusTotal antes de limpeza no ficheiro

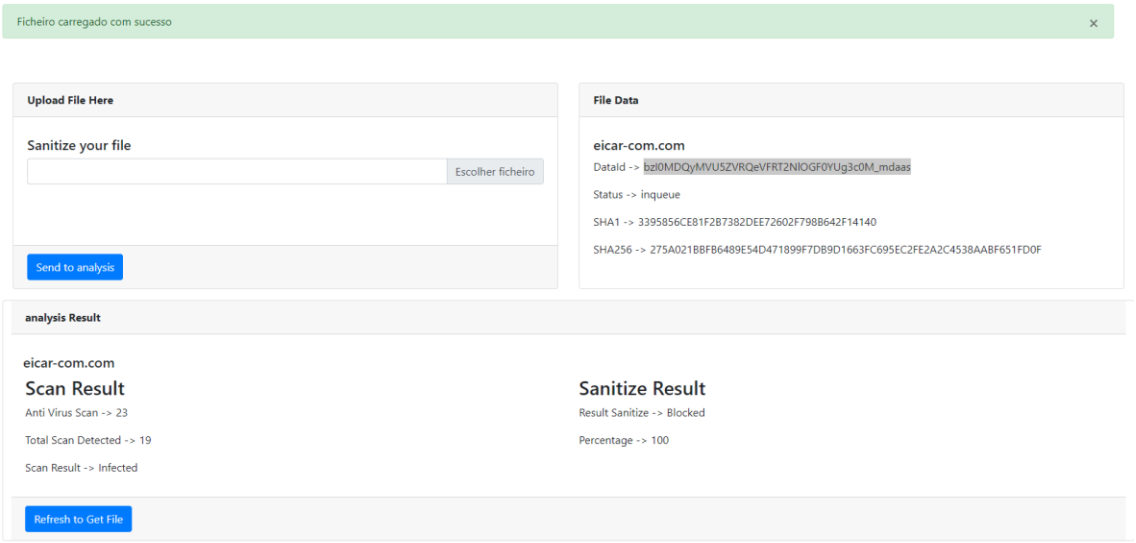

Figura 52 - T10 - Resultado do ficheiro 4 no CDRFileCleanerApp após envio do ficheiro para limpeza

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 5 – paper 13.pdf

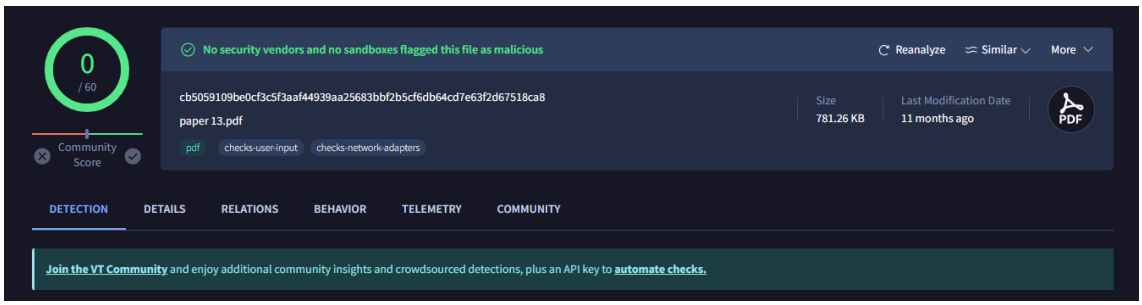

Figura 53 - T11 - Scan Test ficheiro 5 no VirusTotal antes de limpeza no ficheiro

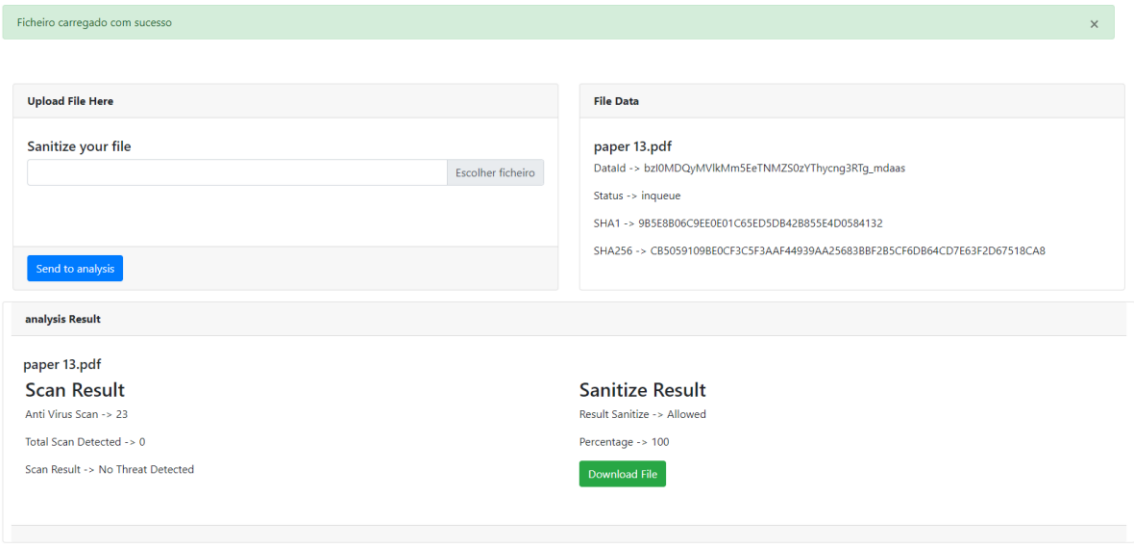

Figura 54 - T12 - Resultado do ficheiro 5 no CDRFileCleanerApp após envio do ficheiro para limpeza

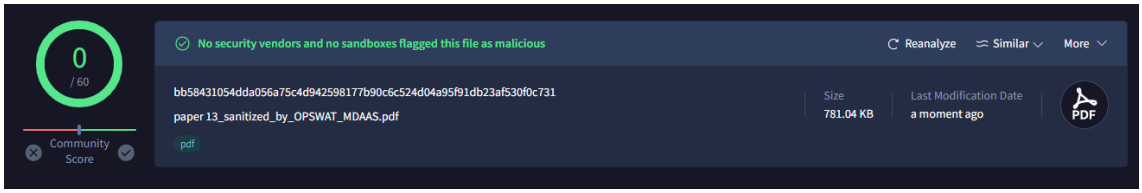

Figura 55 - T13 - Scan Test ficheiro 5 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 6 – eicar-excel-macro-msgbox.xlsm

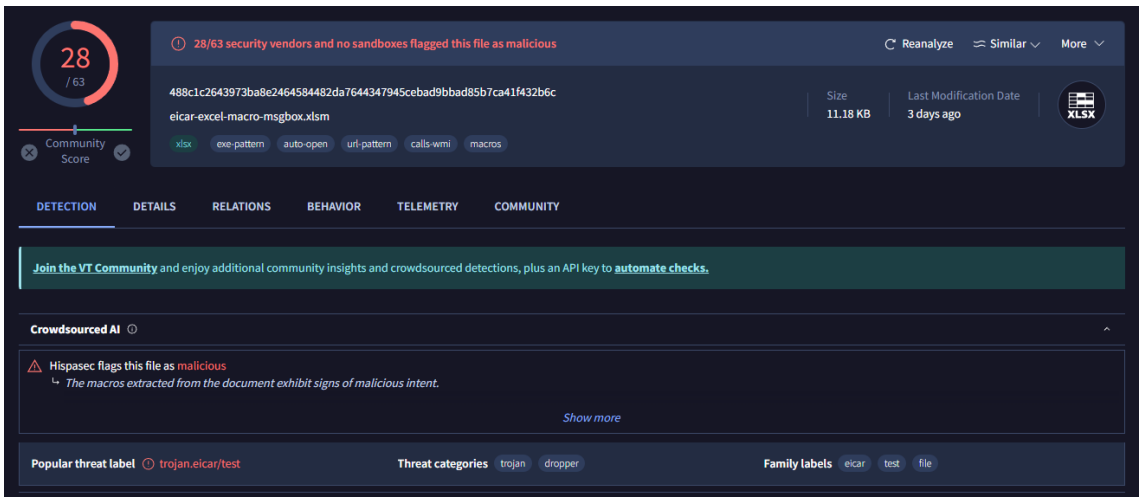

Figura 56 - T14 - Scan Test do ficheiro 6 no VirusTotal antes de limpeza no ficheiro

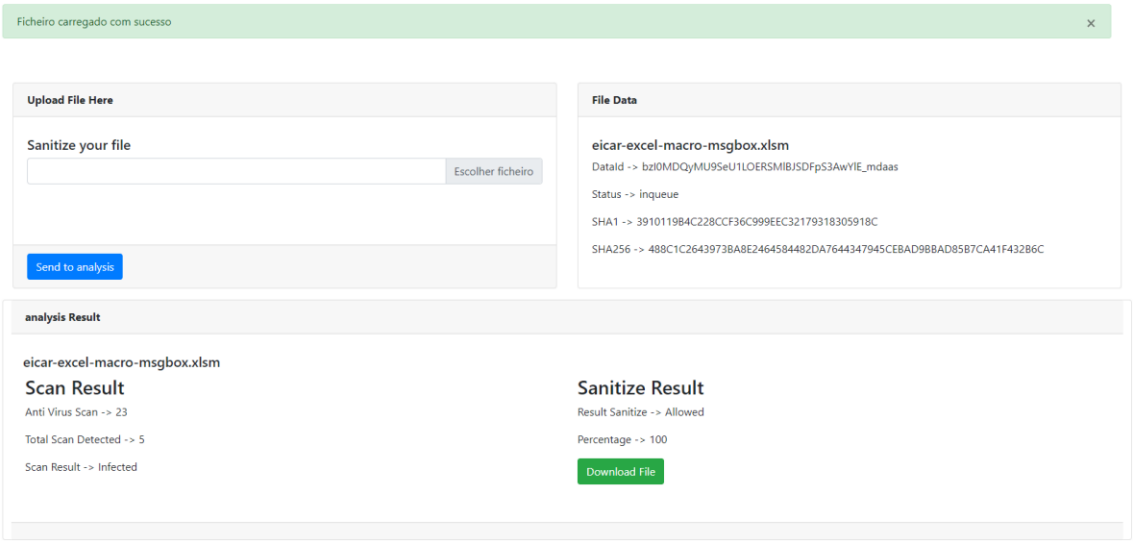

Figura 57 - T15 - Resultado do ficheiro 6 no CDRFileCleanerApp após envio do ficheiro para limpeza

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

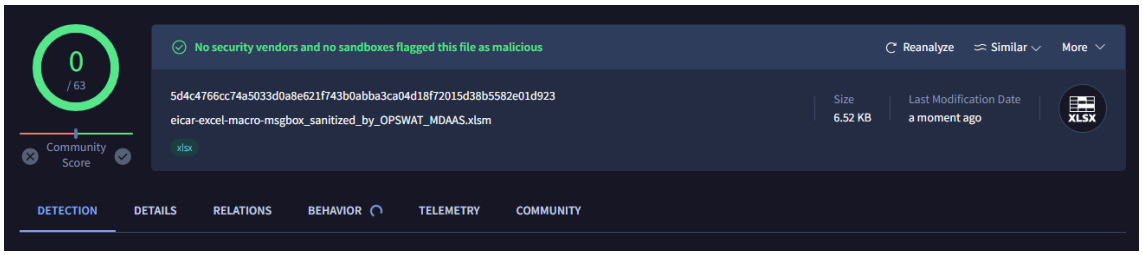

Figura 58 - T16 - Scan Test ficheiro 6 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 7 – eicar-word-macro-write-file.docm

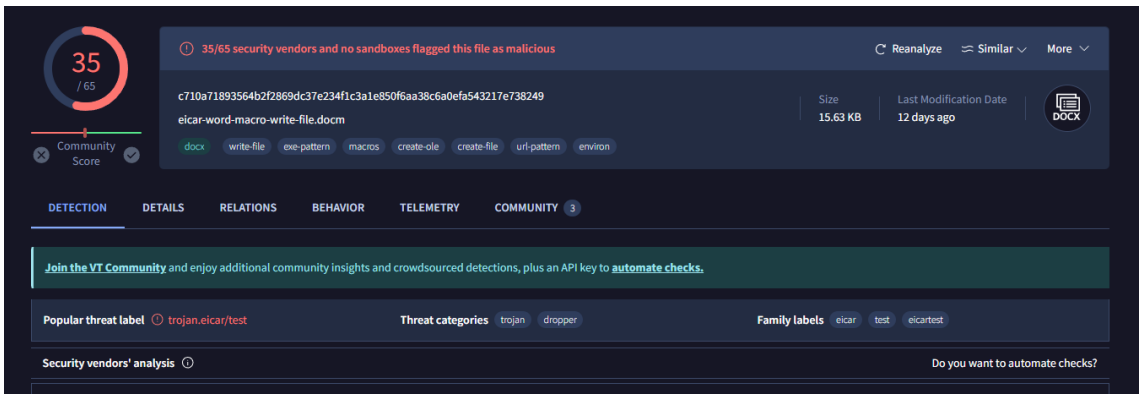

Figura 59 - T17 - Scan Test do ficheiro 7 no VirusTotal antes de limpeza no ficheiro

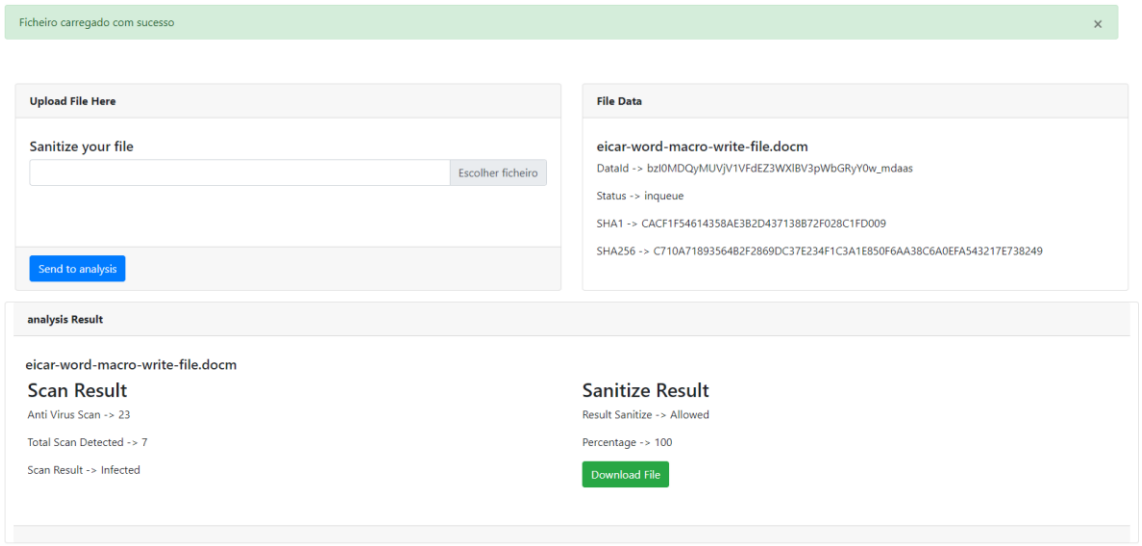

Figura 60 - T18 - Resultado do ficheiro 7 no CDRFileCleanerApp após envio do ficheiro para limpeza

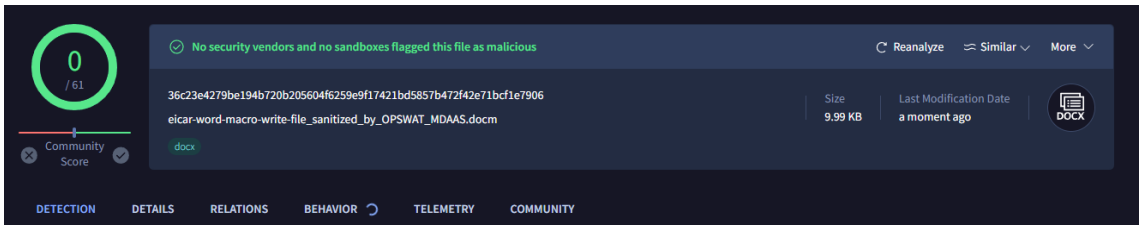

Figura 61 - T19 - Scan Test ficheiro 7 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 8 – sim2018.pdf

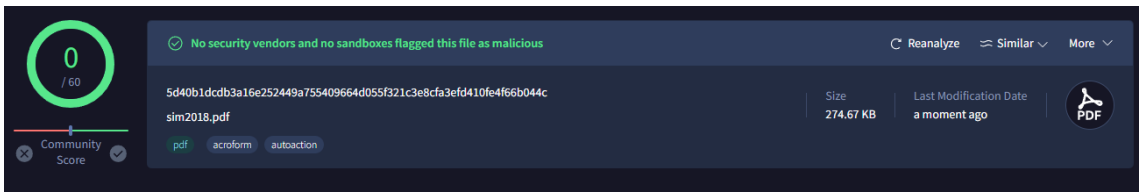

Figura 62 - T20 - Scan Test do ficheiro 8 no VirusTotal antes de limpeza no ficheiro

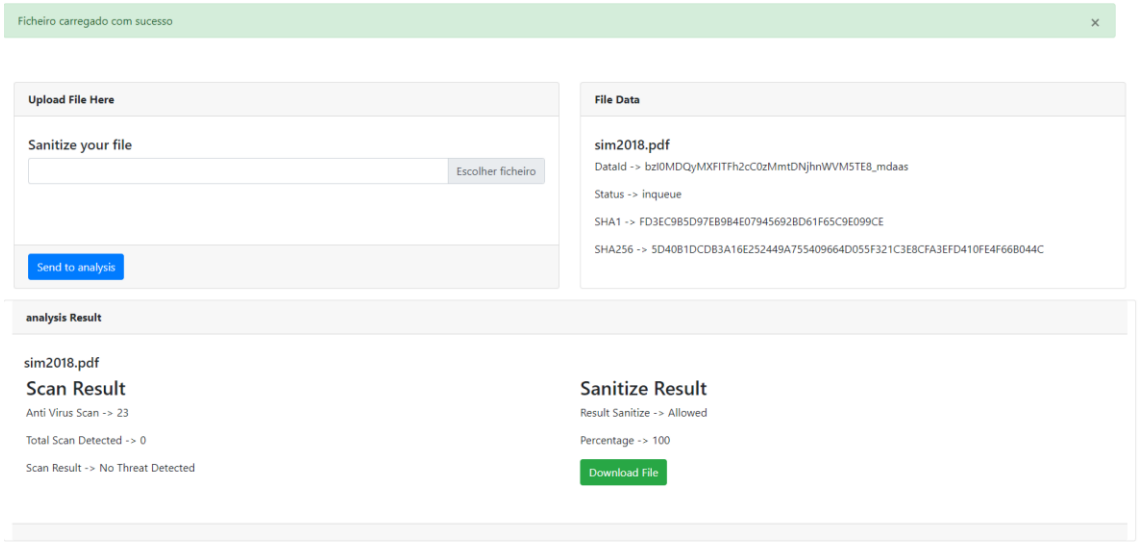

Figura 63 - T21 - Resultado do ficheiro 8 no CDRFileCleanerApp após envio do ficheiro para limpeza

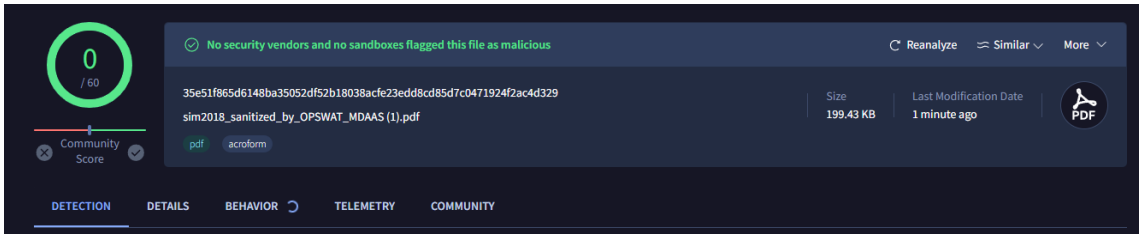

Figura 64 - T22 - Scan Test ficheiro 8 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 9 – eicar-excel-dde-cmd-powershell-echo.xls

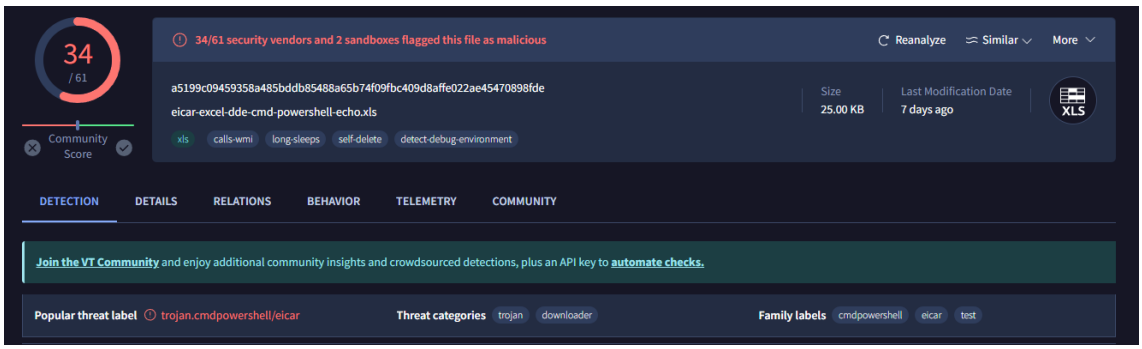

Figura 65 - T23 - Scan Test do ficheiro 9 no VirusTotal antes de limpeza no ficheiro

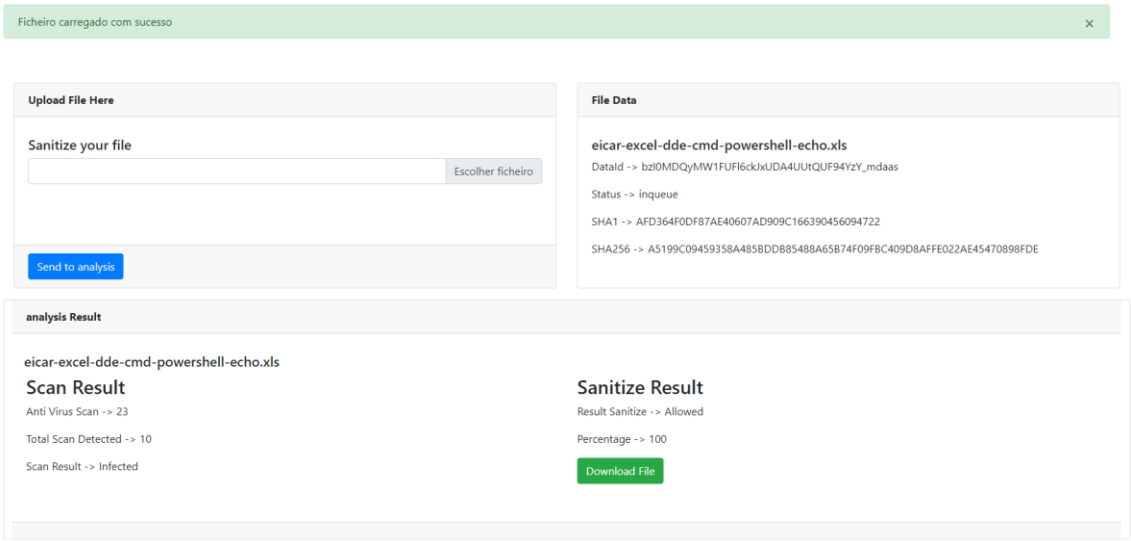

Figura 66 - T24 - Resultado do ficheiro 9 no CDRFileCleanerApp após envio do ficheiro para limpeza

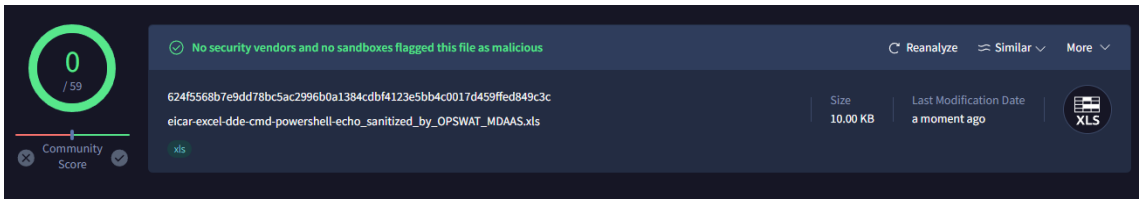

Figura 67 - T25 - Scan Test ficheiro 9 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 10 – eicar-powerpoint-action-macro-msgbox.ppt

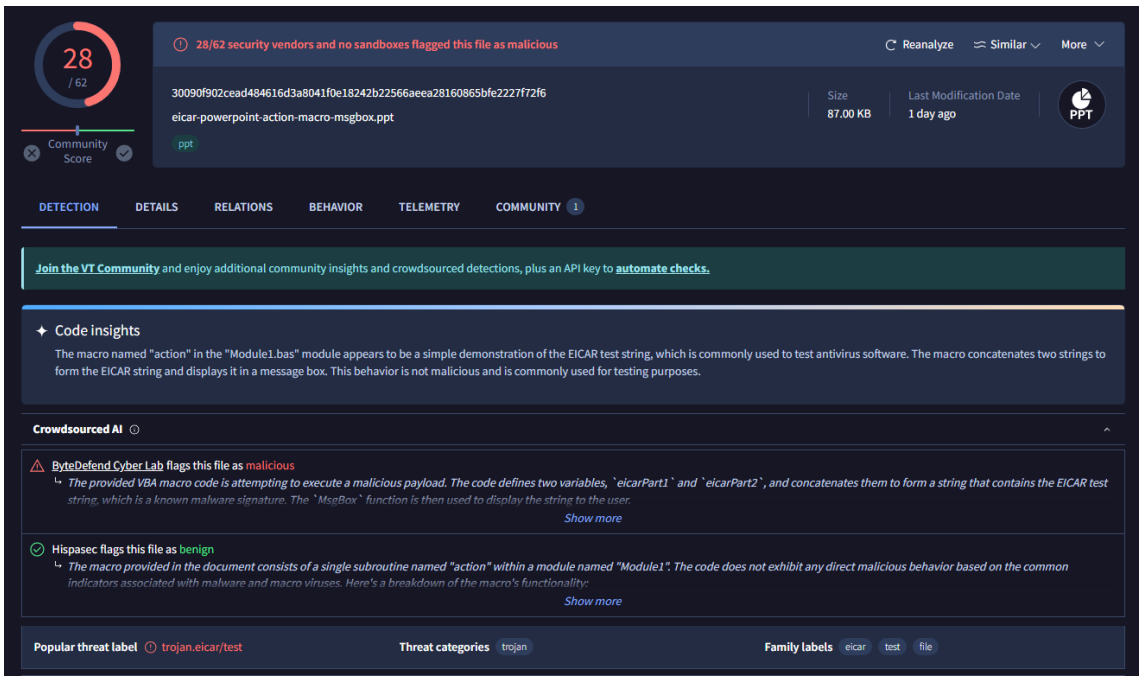

Figura 68 - T26 - Scan Test do ficheiro 10 no VirusTotal antes de limpeza no ficheiro

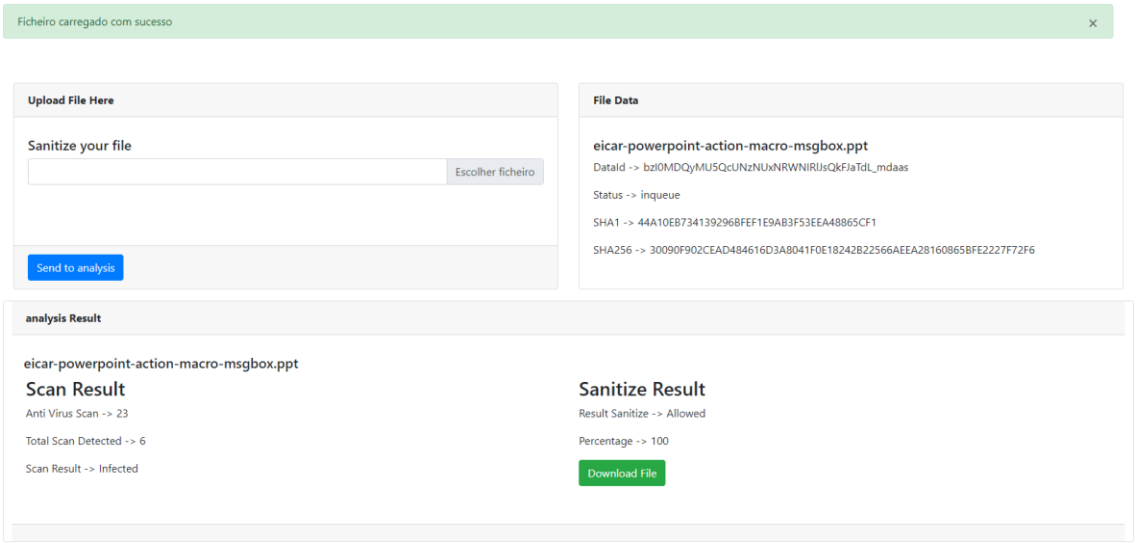

Figura 69 - T27 - Resultado do ficheiro 10 no CDRFileCleanerApp após envio do ficheiro para limpeza

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

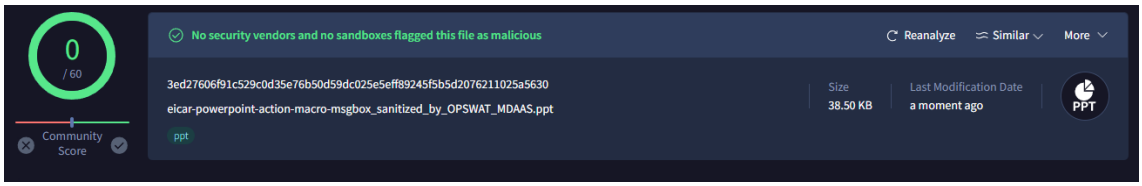

Figura 70 - T28 - Scan Test ficheiro 10 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 11 – vonsolms2013.pdf

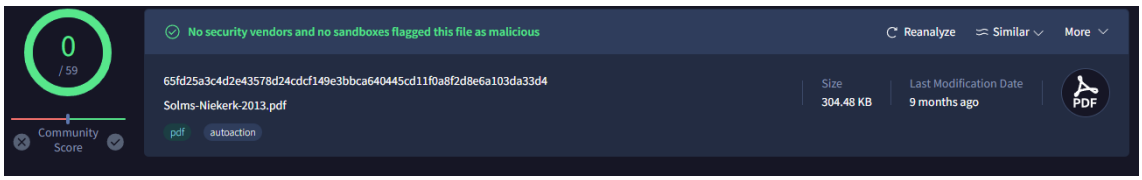

Figura 71 - T29 - Scan Test do ficheiro 11 no VirusTotal antes de limpeza no ficheiro

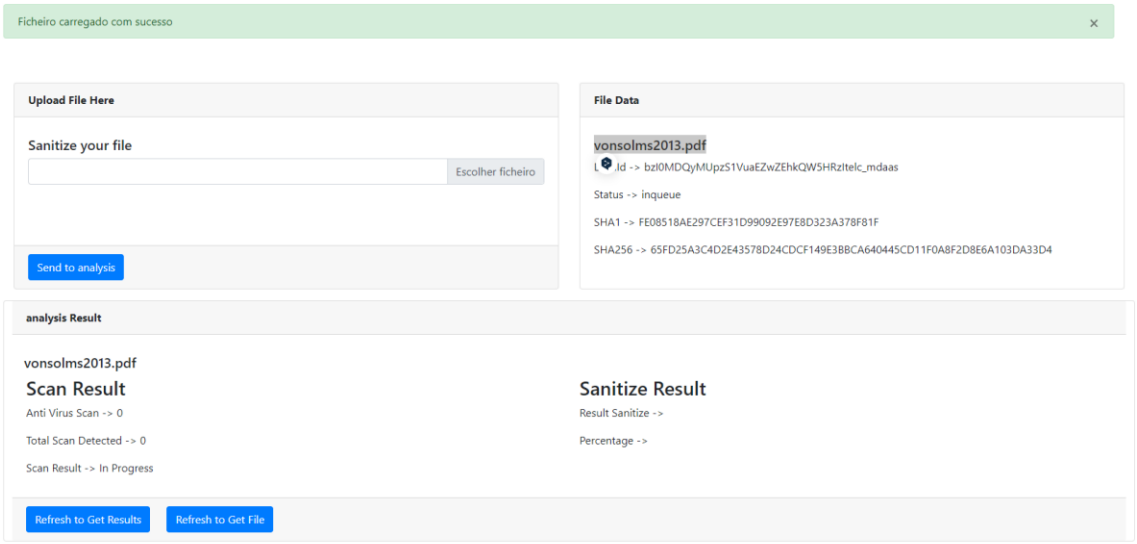

Figura 72 - T30 - Resultado do ficheiro 11 no CDRFileCleanerApp após envio do ficheiro para limpeza

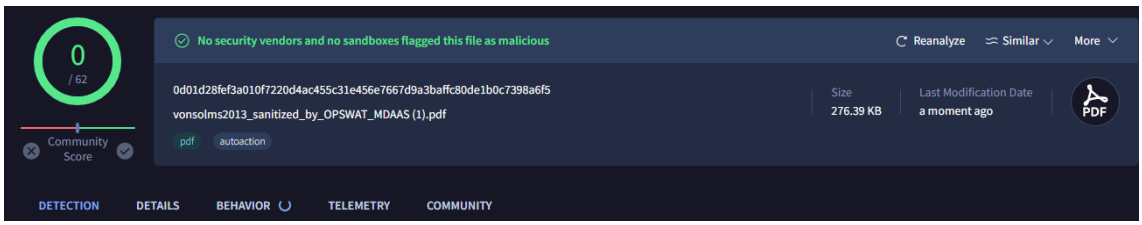

Figura 73 - T31 - Scan Test ficheiro 11 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 12 – eicar-test.txt

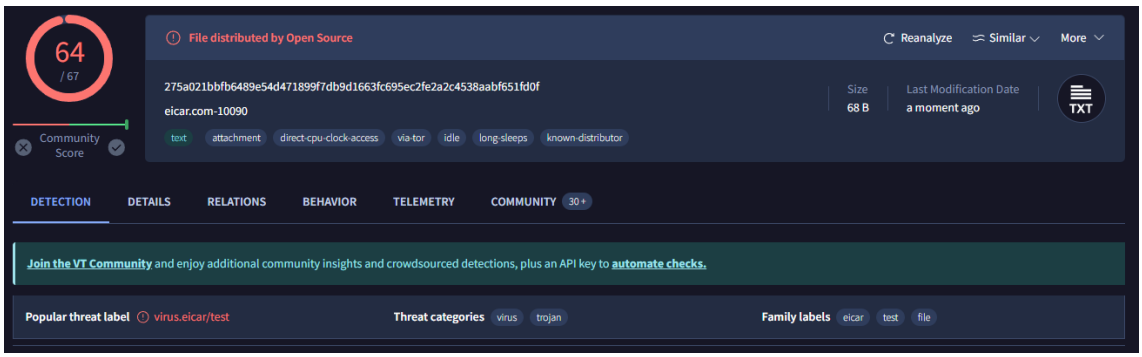

Figura 74 - T32 - Scan Test do ficheiro 12 no VirusTotal antes de limpeza no ficheiro

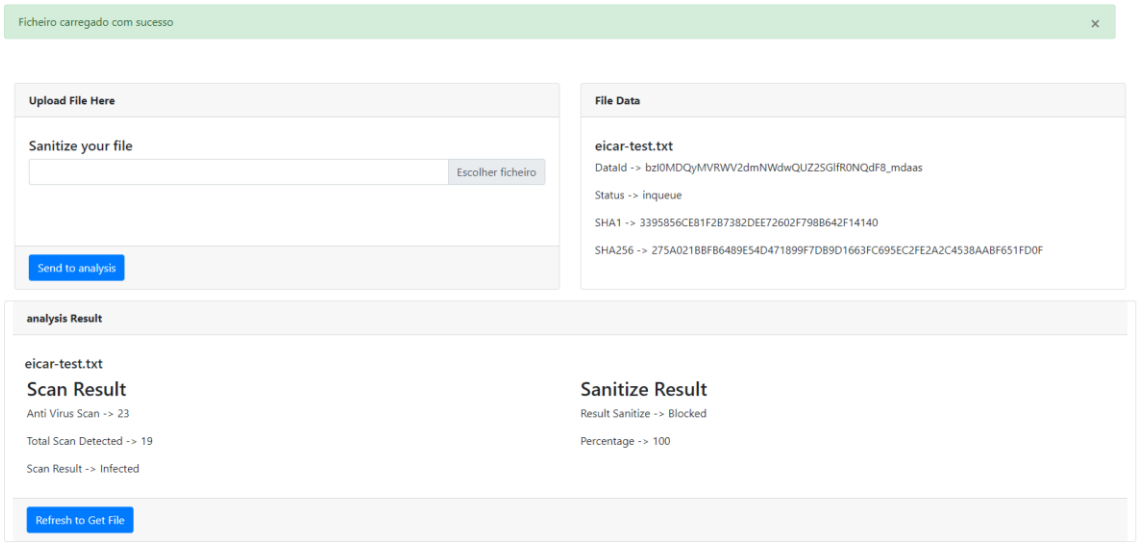

Figura 75 - T33 - Resultado do ficheiro 12 no CDRFileCleanerApp após envio do ficheiro para limpeza

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 13 – eicar-word-macro-cmd-echo.docm

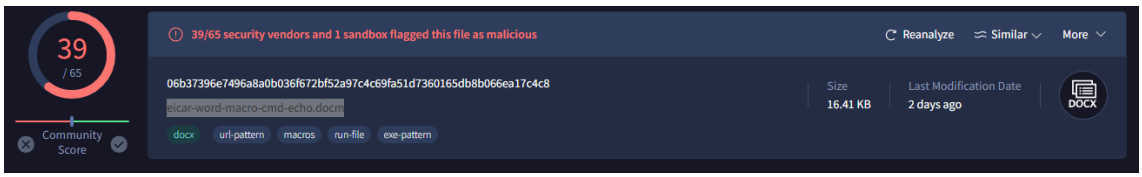

Figura 76 - T34 - Scan Test do ficheiro 13 no VirusTotal antes de limpeza no ficheiro

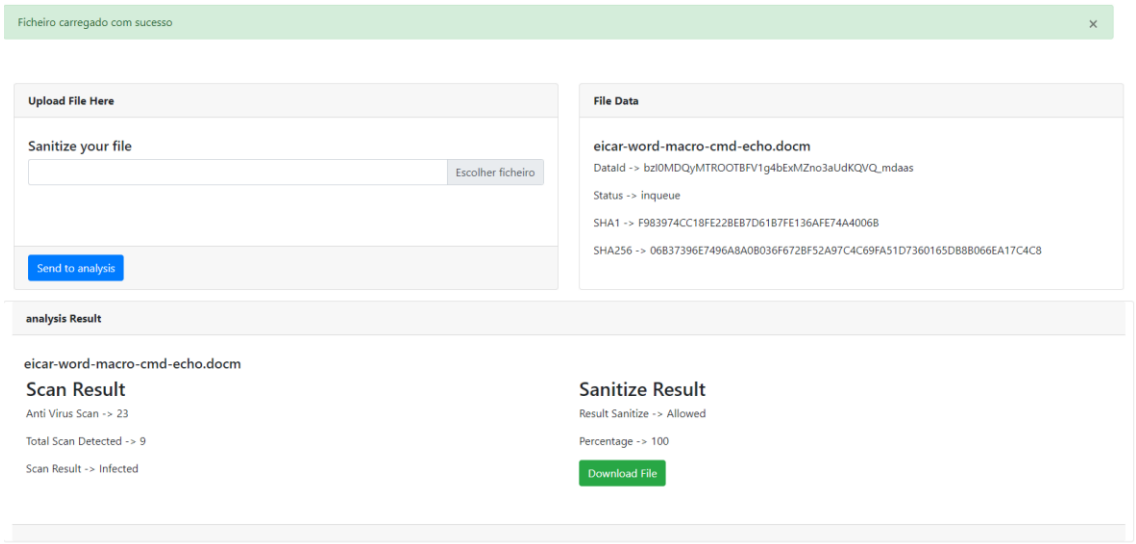

Figura 77 - T35 - Resultado do ficheiro 13 no CDRFileCleanerApp após envio do ficheiro para limpeza

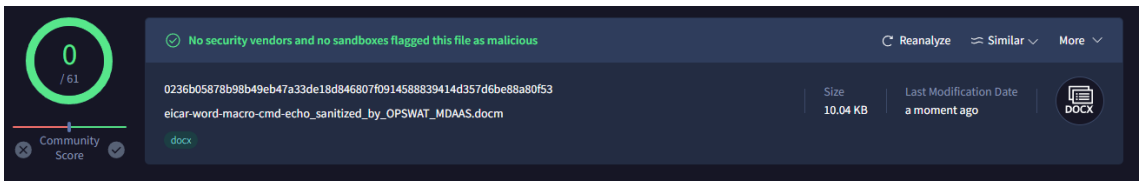

Figura 78 - T36 - Scan Test ficheiro 13 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 14 – Content_Disarm_and_Reconstruction_of_RTF_Files_a_Zero_File_Trust_Methodology.pdf

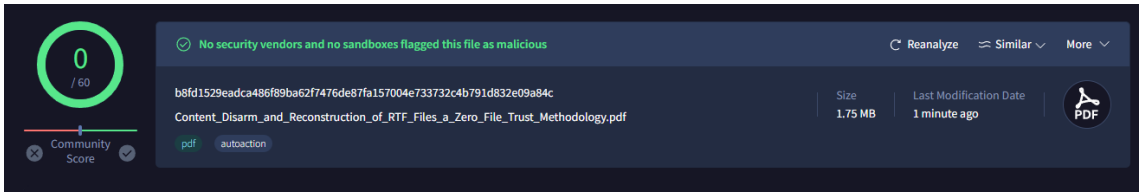

Figura 79 - T37 - Scan Test do ficheiro 14 no VirusTotal antes de limpeza no ficheiro

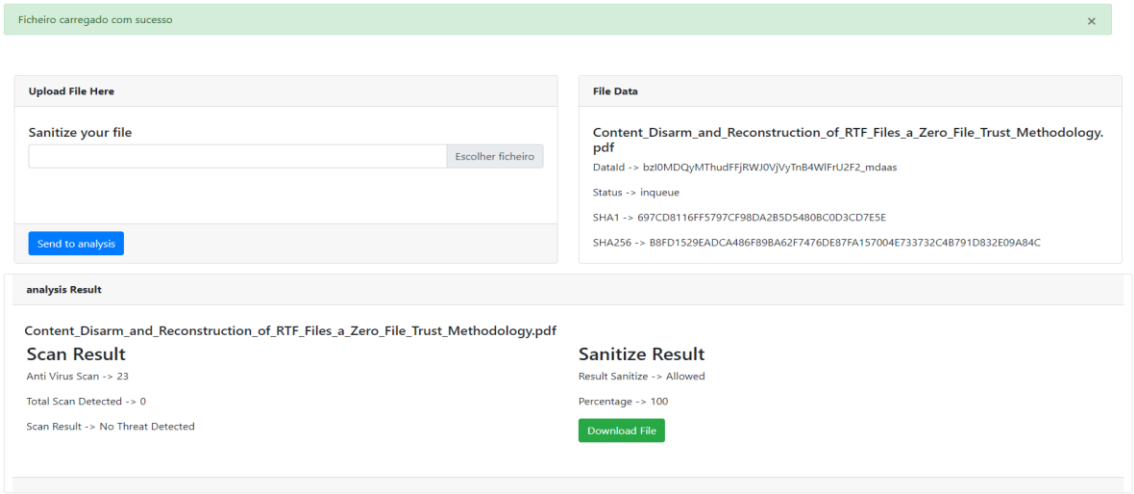

Figura 80 - T38 - Resultado do ficheiro 14 no CDRFileCleanerApp após envio do ficheiro para limpeza

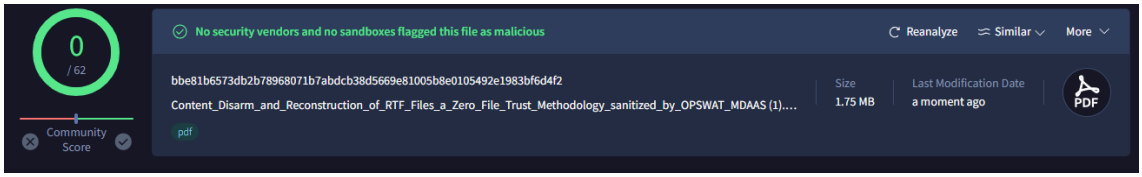

Figura 81 - T39 - Scan Test ficheiro 14 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 15 – eicar-powerpoint-action-powershell-echo.ppt

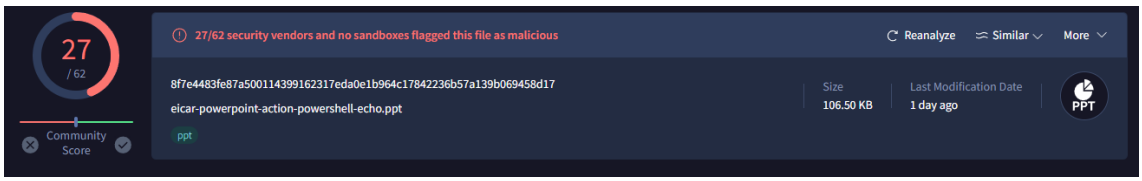

Figura 82 - T40 - Scan Test do ficheiro 15 no VirusTotal antes de limpeza no ficheiro

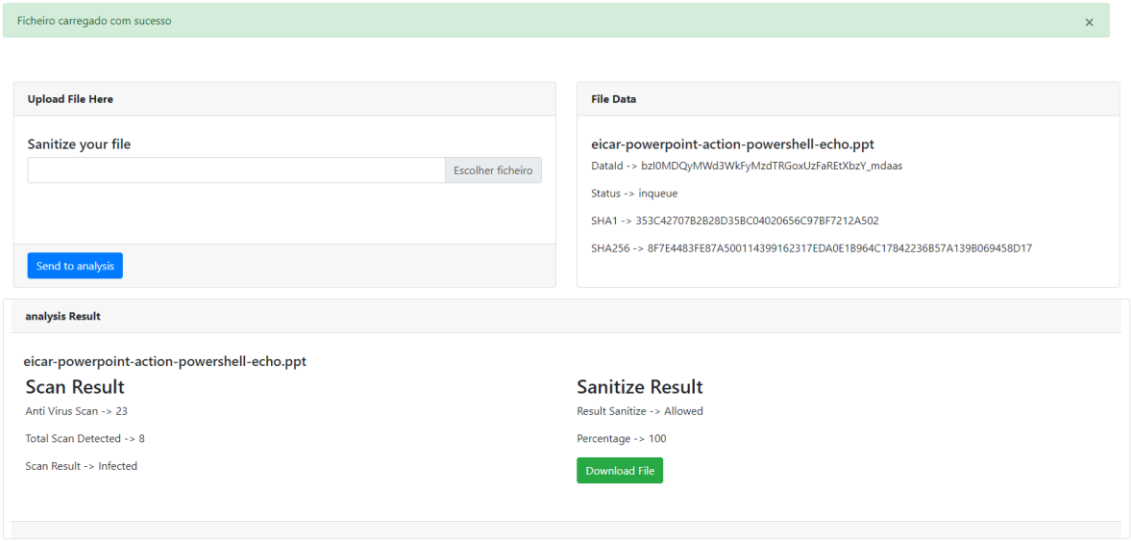

Figura 83 - T41 - Resultado do ficheiro 15 no CDRFileCleanerApp após envio do ficheiro para limpeza

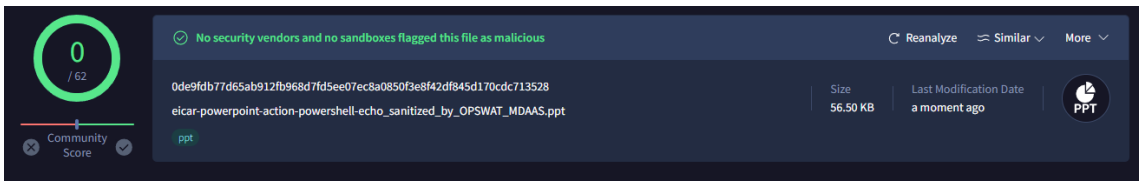

Figura 84 - T42 - Scan Test ficheiro 15 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 16 – eicar-excel-macro-write-file.xls

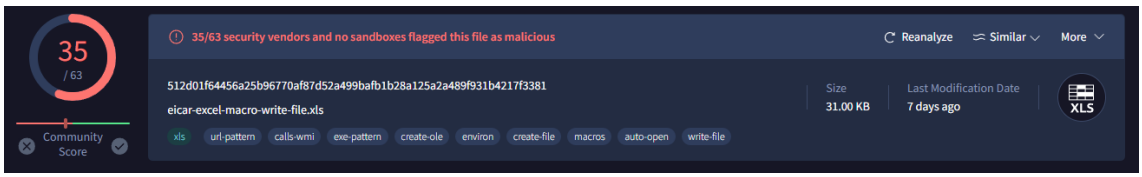

Figura 85 - T43 - Scan Test do ficheiro 16 no VirusTotal antes de limpeza no ficheiro

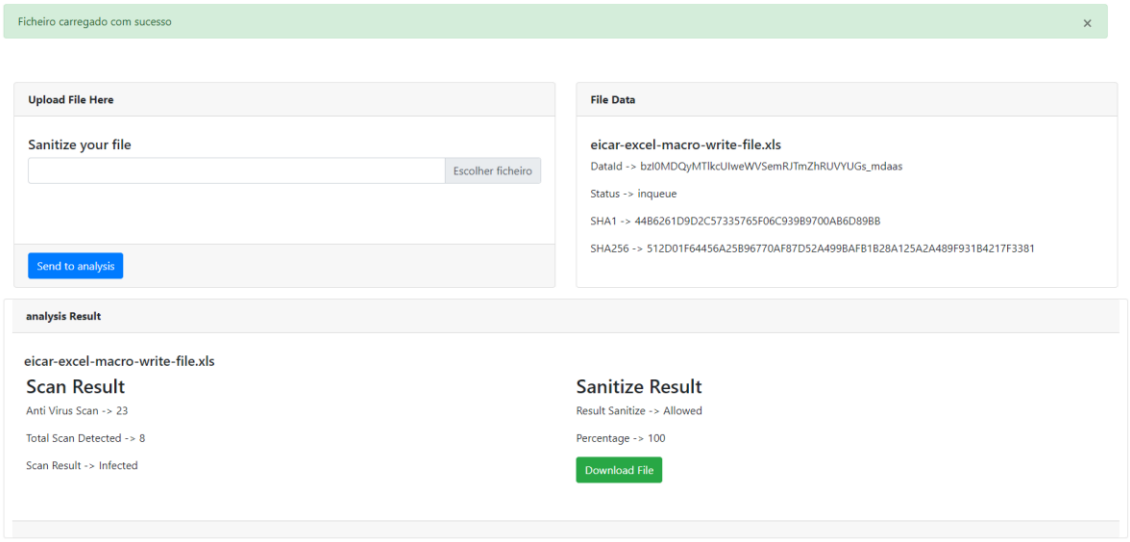

Figura 86 - T44 - Resultado do ficheiro 16 no CDRFileCleanerApp após envio do ficheiro para limpeza

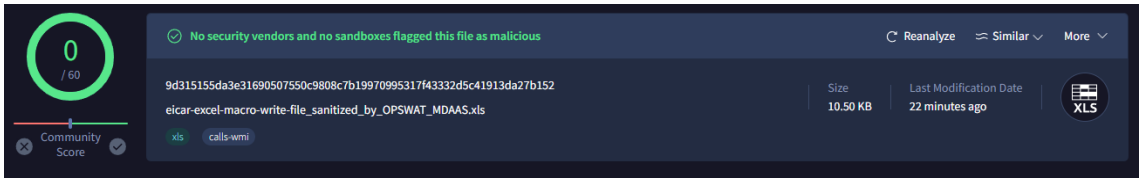

Figura 87 - T45 - Scan Test ficheiro 16 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 17 – eicar-word-macro-powershell-echo.docm

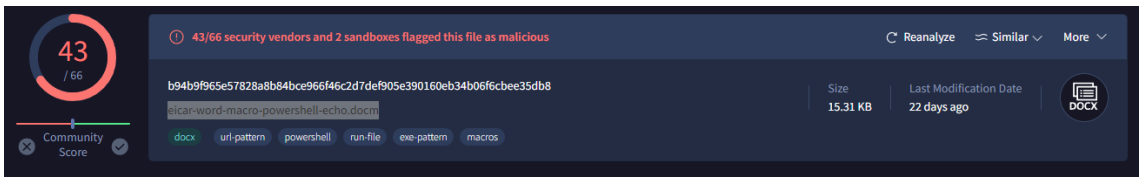

Figura 88 - T46 - Scan Test do ficheiro 17 no VirusTotal antes de limpeza no ficheiro

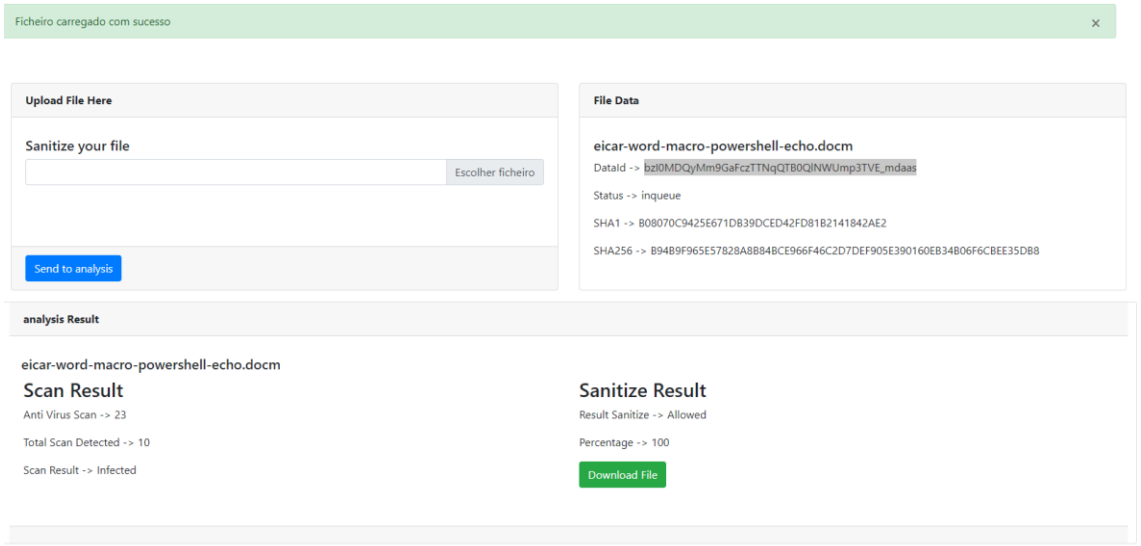

Figura 89 - T47 - Resultado do ficheiro 17 no CDRFileCleanerApp após envio do ficheiro para limpeza

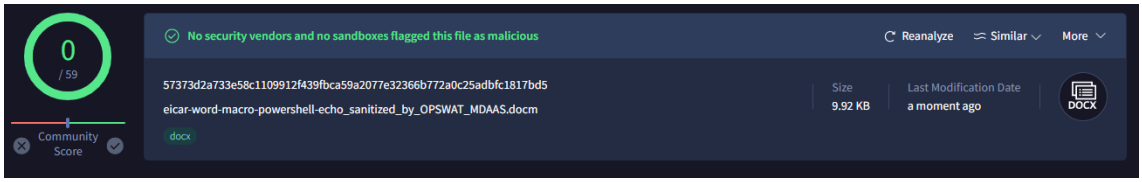

Figura 90 - T48 - Scan Test ficheiro 17 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 18 – CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf

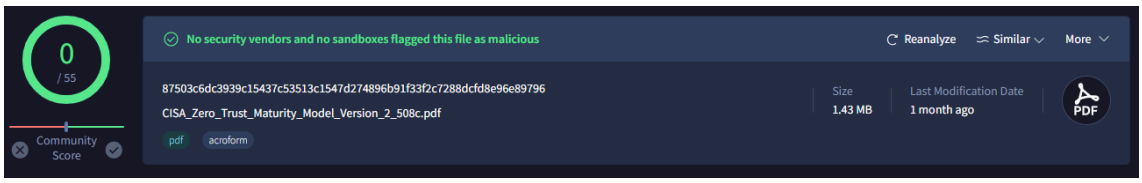

Figura 91 - T49 - Scan Test do ficheiro 18 no VirusTotal antes de limpeza no ficheiro

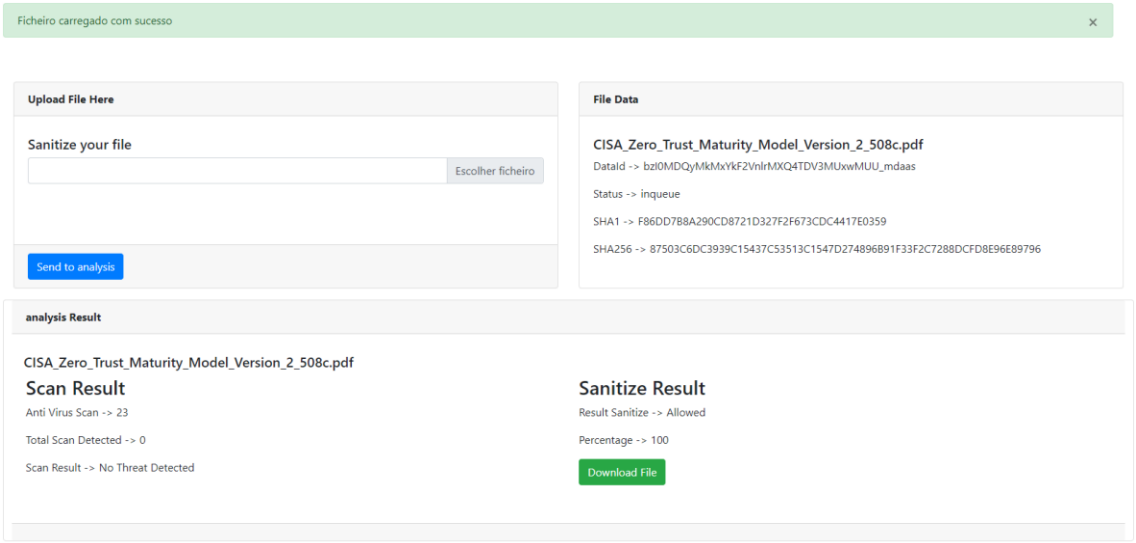

Figura 92 - T50 - Resultado do ficheiro 18 no CDRFileCleanerApp após envio do ficheiro para limpeza

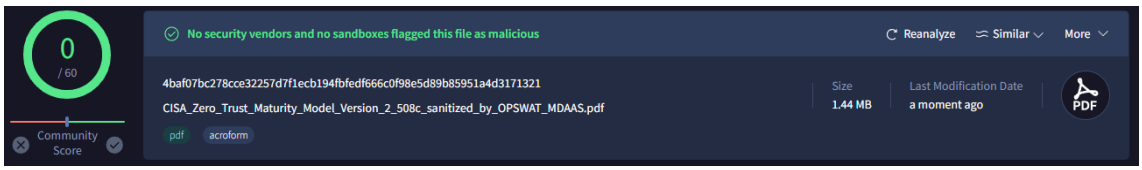

Figura 93 - T51 - Scan Test ficheiro 18 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 19 – eicar-excel-macro-powershell-echo.xlsm

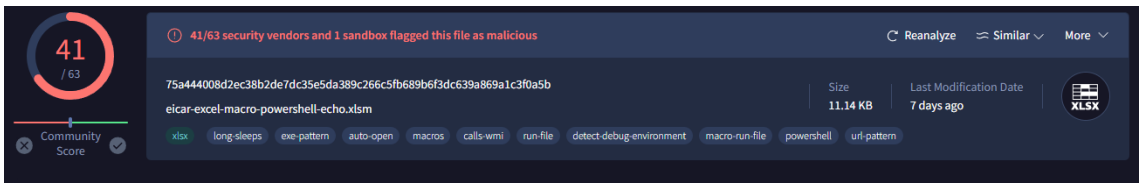

Figura 94 - T52 - Scan Test do ficheiro 19 no VirusTotal antes de limpeza no ficheiro

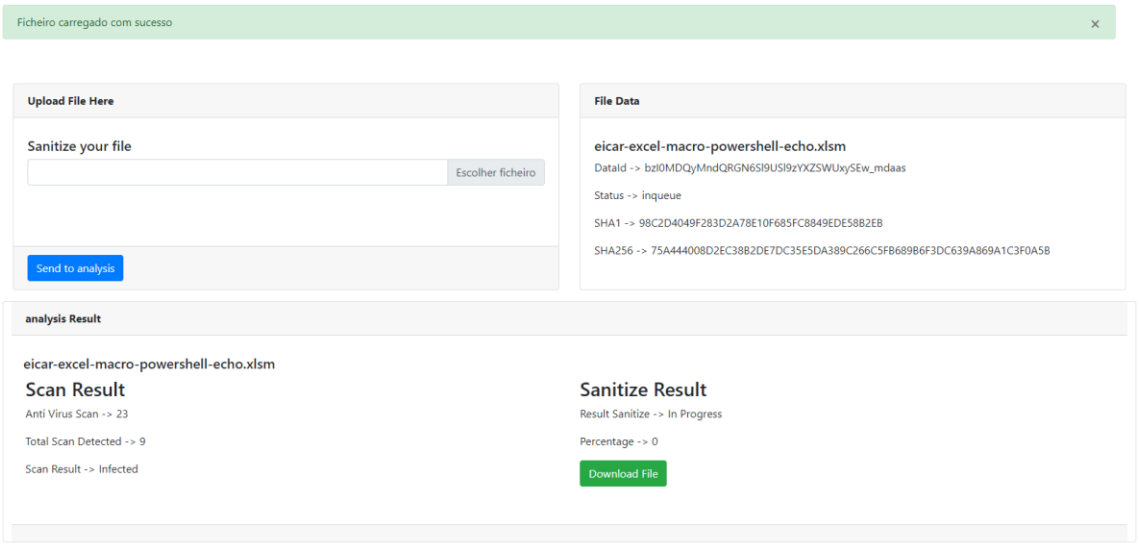

Figura 95 - T53 - Resultado do ficheiro 19 no CDRFileCleanerApp após envio do ficheiro para limpeza

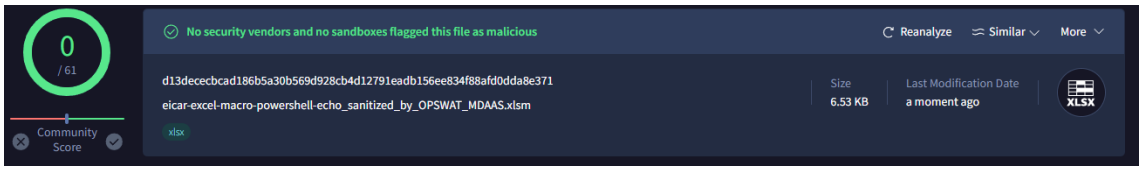

Figura 96 - T54 - Scan Test ficheiro 19 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt

Teste 20 – eicar-powerpoint-action-powershell-echo.pptx

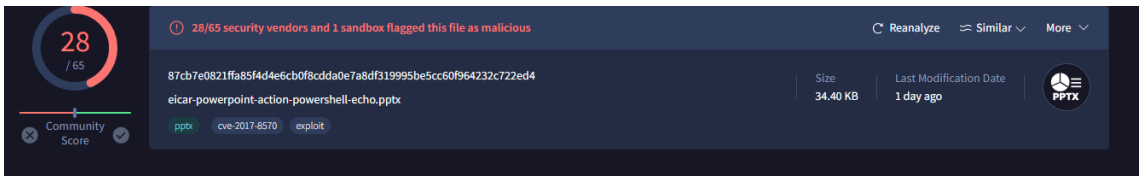

Figura 97 - T55 - Scan Test do ficheiro 20 no VirusTotal antes de limpeza no ficheiro

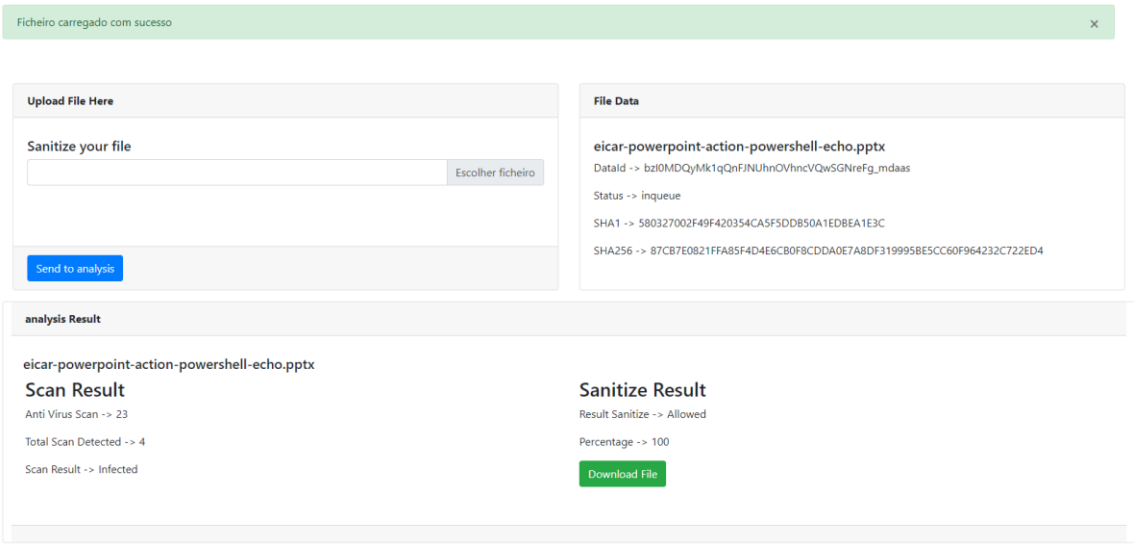

Figura 98 - T56 - Resultado do ficheiro 20 no CDRFileCleanerApp após envio do ficheiro para limpeza

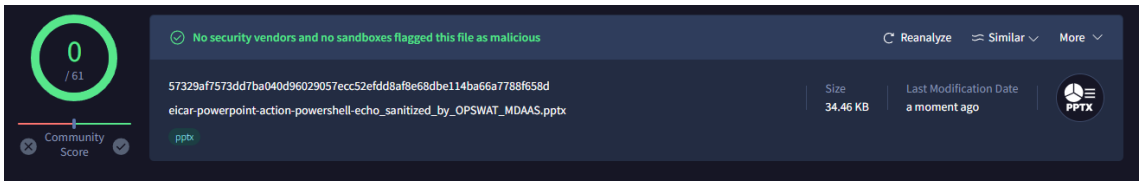

Figura 99 - T57 - Scan Test ficheiro 20 no VirusTotal após limpeza do ficheiro

Coimbra Business School | ISCAC
Quinta Agrícola – Bencanta, 3045-601 Coimbra
Tel +351 239 802 000; E-mail: secretariado@iscac.pt; www.iscac.pt