PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA POLITÉCNICA

CURSO DE CIÊNCIAS AERONÁUTICAS

MATEUS FREITAS DA SILVA

*RANSOMWARE*: OS RISCOS DO SEQUESTRO DE DADOS NA AVIAÇÃO CIVIL

GOIÂNIA

2021

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA POLITÉCNICA

CURSO DE CIÊNCIAS AERONÁUTICAS

MATEUS FREITAS DA SILVA

*RANSOMWARE*: OS RISCOS DO SEQUESTRO DE DADOS NA AVIAÇÃO CIVIL

Artigo Científico apresentado à Pontifícia Universidade Católica de Goiás como exigência parcial para a obtenção do grau de bacharel em Ciências Aeronáuticas.

Professor Orientador: M. Sc. Raul Francé Monteiro.

GOIÂNIA

2021

MATEUS FREITAS DA SILVA

***RANSOMWARE*: OS RISCOS DO SEQUESTRO DE DADOS NA AVIAÇÃO CIVIL**

GOIÂNIA-GO, \_\_\_\_/\_\_\_\_\_/2021.

BANCA EXAMINADORA

M. Sc. Raul Francé Monteiro \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ CAER/PUC-GO \_\_\_\_\_\_\_

 Assinatura Nota

Me. Fabrício Schlag \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ CAER/PUC-GO \_\_\_\_\_\_\_

 Assinatura Nota

Esp. Salmen Chaquip Bukzem \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_CAER/PUC-GO \_\_\_\_\_\_\_

 Assinatura Nota

# *RANSOMWARE*: OS RISCOS DO SEQUESTRO DE DADOS NA AVIAÇÃO CIVIL

**RESUMO:**

Essa pesquisa tem como foco informar sobre o risco que os tipos de *ransomware* oferecem para a aviação civil. O *ransomware* é um software malicioso capaz de criptografar os arquivos da vítima e restringir o acesso ao sistema afetado exigindo um valor de resgate para que o mesmo seja reestabelecido. Considerando que o avião é um meio de transporte altamente tecnológico e dependente de sistemas computadorizados, tais como *software,* rede de computadores, internet das coisas (IoT), um elemento torna-se fundamental para o seu funcionamento: os dados. Eles estão presentes em praticamente todas as áreas da aviação, seja na hora de fazer *check-in* via internet ou na emissão de planos de voos, por exemplo. Assim, eles acabam se tornando ferramentas muito valiosas para empresas e entidades do setor, o que faz do modal aeronáutico um alvo atrativo para ações criminosas. De fato, a interdependência desses sistemas computadorizados trouxe novos desafios para a proteção contra atos de interferência ilícita uma vez que as ameaças passaram a ser não apenas físicas, mas também virtuais e o sequestro de dados é uma delas. Desse modo, o *ransomware* pode degradar ou mesmo suspender sistemas essenciais para a aviação, causando uma série de prejuízos, podendo comprometer até mesmo a segurança. Sendo assim, além de fazer uma análise histórica dos casos mais famosos de ataque e os respectivos impactos que eles causaram, o objetivo dessa pesquisa é conscientizar a comunidade aeronáutica, por meio de relatos e breves análises de estudos de caso, sobre os riscos relacionados a esse tipo de *software* malicioso bem como apresentar algumas práticas para evitá-los.

**Palavras-chave**: *Ransomware;* Dados; Aviação Civil; Prevenção.

***RANSOMWARE: THE RISKS OF DATA HIJACKING IN CIVIL AVIATION***

***ABSTRACT:***

*This research is focused on informing about the risk that types of ransomware pose to civil aviation. Ransomware is malicious software capable of encrypting a victim's files and restricting access to the affected system by requiring a ransom value to restore it. Considering that the plane is a highly technological means of transport and depends on computerized systems, such as software, computer networks, and the Internet of Things (IoT), one element is essential for its operation: data. They are present in practically all areas of aviation, whether when checking in via the internet or issuing flight plans, for example. Thus, they end up becoming very valuable tools for companies and entities in the sector, which makes the aeronautical modal an attractive target for criminal actions. In fact, the interdependence of these computerized systems has brought new challenges to the protection against acts of unlawful interference since the threats are now not only physical, but also virtual and data hijacking is one of them. In this way, ransomware can degrade or even suspend essential systems for aviation, causing a series of damages and even compromising security. Therefore, in addition to making a historical analysis of the most famous attack cases and the respective impacts they caused, the objective of this research is to raise awareness of the aeronautical community, through reports and brief analysis of case studies, about the risks related to this type of malicious software as well as present some practices to avoid them.*

***Keywords****: Ransomware; Data; Civil Aviation; Prevention*.

**INTRODUÇÃO**

Sabe-se que a aviação é uma atividade de transporte que lida atualmente com equipamentos altamente tecnológicos, digitais e cada vez mais dependentes de sistemas computadorizados, sendo altamente “hiperconectada”. Elementos como *software*, rede de computadores, tecnologia da informação e internet das coisas (IoT) são fundamentais no que se refere ao atendimento das necessidades de passageiros, controladores, pilotos, empresas aéreas etc.

Desse modo, um elemento essencial para o funcionamento desse modal são os dados. Seja em situações mais simples, como reservas de passagens, pagamentos com cartões e realização do *check-in*, ou mais complexas, como planejamento de voo, navegação aérea e emissão de planos de voo, os dados estão presentes. Sem eles não seria possível, por exemplo, obter informações meteorológicas precisas, realizar *check-in* via internet ou ainda utilizar serviços de navegação RNAV[[1]](#footnote-1). Sendo assim, eles acabam se tornando ferramentas muito valiosas para empresas e entidades do setor. Por essa razão, também transforma o modal aeronáutico em um alvo extremamente atrativo para ações criminosas.

Essa interdependência da aviação desses sistemas computadorizados trouxe novos desafios para a proteção contra atos de interferência ilícita. Dessa vez, as ameaças passaram a ser não apenas físicas, mas também virtuais, sendo o sequestro de dados uma delas. Significa dizer que os criminosos passaram a usar o ciberespaço[[2]](#footnote-2) para sequestrar dados por meio do *ransomware,* um software malicioso, ou, em outros termos, vírus sofisticados de computador. Esse sequestro permite gerar cobranças para pagamentos de resgates muito rápidos.

Relatos de empresas privadas que atuam no ramo de segurança da informação indicam um nível cada vez maior de *hackers*[[3]](#footnote-3)direcionados à aviação. Além disso, o sequestro de dados por meio digital é considerado barato, fácil e muito eficaz para esses criminosos. Aliado a isso, o fato de as empresas desse setor movimentarem altas quantias cotidianamente, de possuírem informações preciosas, como dados pessoais de passageiros e funcionários, e dependerem de sistemas computacionais para o seu funcionamento torna esse tipo de crime virtual bastante visado e extremamente lucrativo.

Além disso, à medida que as organizações do setor aéreo digitalizam suas operações e funcionários passam, cada vez mais, a usar *e-mails*, armazenamento em nuvem[[4]](#footnote-4), aplicativos e dispositivos móveis para trabalhar, o número de pontos de entrada em potencial para invasores aumentam exponencialmente. Como efeito, depois que uma rede é violada, as infecções podem se espalhar mais rapidamente, afetando os sistemas críticos que estão a ela conectados. No caso da aviação, um ataque de *ransomware* pode interromper, negar, degradar ou destruir informações presentes em computadores e rede de computadores, resultando no mal funcionamento ou mesmo na suspensão de sistemas que lhe sejam vitais, como o sistema de navegação aérea.

Tendo em vista a importância dos dados para os sistemas computadorizados – essenciais não apenas à aviação, mas também a outras áreas com as quais ela interage direta e indiretamente –, o foco dessa pesquisa é avaliar os riscos que o *ransomware* podem oferecer à aviação. Importantes contribuições foram identificadas por meio das construções divulgadas pelos autores Calvin Nobles (2017); Lawrance Miller (2020) e Ronny Richardson; Max North (2017).

Para tanto, o método empregado neste estudo foi o dedutivo. No que tange ao procedimento técnico, buscou-se, por meio de pesquisas bibliográficas e de estudo de caso, identificar, constatar e pesquisar a respeito dos possíveis riscos que os ataques do tipo *ransomware* podem oferecer aos sistemas de aviação civil, como dito, assim como seus impactos na segurança.

Quanto à classificação científica, este estudo baseou-se em uma abordagem qualitativa de pesquisa, visto que se utilizou como fonte direta para coleta de dados o ambiente natural. Em relação aos objetivos, tem um caráter exploratório com a finalidade de obter mais informações a respeito dos efeitos que o sequestro de dados por vírus do tipo *ransomware* podem causar na aviação. Essa pesquisa é, ainda, de natureza básica, pois não apresenta finalidades imediatas, esperando-se, contudo, que possa produzir conhecimentos que possam ser utilizados em outros trabalhos.

# 1 CONCEITO DE *RANSOMWARE* E SEU CONTEXTO HISTÓRICO

*Ransomware* é um software malicioso (*malware*) usado para criptografar os dados da vítima por meio de uma chave de criptografia conhecida apenas pelo invasor, de modo a tornar os dados inutilizáveis até que um pagamento de resgate (geralmente criptomoeda, como Bitcoin) seja feito pela vítima. A criptomoeda é uma moeda digital alternativa que usa criptografia para regular a “impressão” de unidades monetárias (como Bit-moeda) e para verificar a transferência de fundos entre as partes, sem intermediário ou banco central.

Os valores de resgate são normalmente altos, mas geralmente não exorbitantes. No entanto, esses valores estão aumentando com o tempo, conforme os invasores começam a concentrar sua atenção em organizações com mais capacidades para pagar quantias maiores – e mais possibilidade de incorrer de prejuízos. Os valores de resgate também podem aumentar significativamente, quanto mais tempo uma vítima espera. Novamente, isso ocorre intencionalmente em um esforço para limitar as opções da vítima e fazer com que ela pague o resgate o mais rapidamente possível (MILLER, 2020).

A palavra “*ransomware”* é a junção de outras duas palavras: “*ransom*” (que significa resgate em inglês) e “malware” (que significa *software* malicioso). Ele pode ser dividido em dois tipos básicos. O mais comum é o *ransomware* de criptografia (*crypto ransomware*), que criptografa arquivos e dados, mas permite o uso do computador infectado; já o segundo tipo é o *ransomware* de bloqueio (*locker ransomware*). Esta versão bloqueia o computador ou outro dispositivo, evitando que as vítimas o utilizem até que o resgate seja pago.

Vale ressaltar que esse tipo de vírus é normalmente projetado apenas para impedir o acesso à interface do computador, deixando grande parte do sistema e os arquivos subjacentes intactos. Isso significa que se o *malware* for removido, as chances de ter acesso aos arquivos originais novamente é muito grande. Isso torna o *ransomware* de bloqueio menos eficaz na extorsão de pagamentos de resgate em comparação com os *ransomware* de criptografia, os quais podem ser mais destrutivos (SAVAGE; COOGAN; LAU, 2015).

Apesar de o *ransomware* estar em alta hoje em dia, ele não surgiu agora. O primeiro ataque registrado desse tipo ocorreu em 1989 e ficou conhecido como AIDS *trojan[[5]](#footnote-5)*. Esse programa de computador malicioso tinha a capacidade de criptografar arquivos e ocultar pastas necessárias para o funcionamento do sistema operacional *Windows*. O usuário por ele infectado tinha de pagar uma falsa renovação de licença no valor de 189 USD para novamente ter seus arquivos. O dinheiro tinha que ser enviado para uma conta de uma empresa chamada *PC Cyborg Corporation*, no Panamá. Curiosamente, esse ataque recebeu esse nome não pelo modo de infecção e disseminação, o qual ocorria via disquetes contaminados, mas porque o responsável por trás desse *malware* era o doutor Joseph L. Popp, um biólogo evolutivo que fazia pesquisas relacionadas ao vírus da AIDS. O dinheiro arrecadado dos usuários infectados pelo *malware* seria então destinado à sua pesquisa (PEREIRA; LIMA, 2017).

Na década de 1980, a segurança computacional era pouco desenvolvida e a tecnologia apresentava diversas falhas. Em contrapartida, a internet era um recurso a que poucos tinham acesso e, por essa razão, os ataques não eram tão bem-sucedidos e difundidos como atualmente. Apesar disso, o AIDS *trojan* mostrou ao mundo a sua capacidade de inutilizar sistemas operacionais, bem como a possibilidade do uso de ferramentas digitais para atos criminosos, em especial, para o roubo e o sequestro de dados e informações potencialmente sigilosas (PEREIRA; LIMA, 2017).

A partir de então, surgiram várias versões desse tipo de *malware*, cada vez mais sofisticados e especializados para determinado tipo de sistema operacional; porém, todos tinham um objetivo comum: sequestrar dados, criptografar arquivos e extorquir dinheiro das vítimas.

No ano de 2005, com o início da popularização da internet e dos *e-mails*, surge o primeiro *ransomware* de criptografia moderno, o *Pgpcoder* ou *Gpcoder,* que atingiu os Estados Unidos e a Europa. Ele se espalhava por meio de um anexo de *spam*[[6]](#footnote-6) de *e-mail*, alegando ser uma vaga de emprego. Um aspecto importante sobre esse *trojan* é o fato de ele se propagar via internet, podendo infectar qualquer computador do mundo, bastando, para isso, estar conectado à rede, e, portanto, está a apenas alguns cliques do usuário. Em síntese, a partir de agora o *ransomware* atingiria proporções globais (RICHARDSON; NORTH, 2017).

Em 2011 surgiu um tipo mais evoluído de *ransomware*, o *Winlocker*. Ele foi o primeiro *malware* de escala global, pois afetou diversos usuários do sistema operacional *Windows* ao redor do mundo. Criado na Rússia, esse programa malicioso era capaz de bloquear o acesso do usuário ao sistema, exibindo uma falsa tela de renovação de licença do *Windows*. Acredita-se que o valor arrecadado com esse tipo de ataque foi estimado em 16 milhões de dólares. Além disso, com a introdução de novos meios de pagamentos digitais, tais como a criptomoeda *bitcoin*, tornou-se ainda mais difícil rastrear os criminosos (RICHARDSON; NORTH, 2017).

Durante esse mesmo período, surgiu também outra modalidade de *ransomware,* que se tornou popular principalmente nos EUA: o *scareware*. Eles funcionavam de modo similar ao *Winlocker*, bloqueando o acesso do usuário através de uma tela falsa, porém exibindo uma mensagem de um órgão governamental, como o *Federal Bureau of Investigation* (FBI), por exemplo. A ideia era transmitir ao usuário a sensação de que ele teria cometido um crime acessando documentos ilegais on-line (GALVÃO, 2016). Ele então deveria pagar uma falsa multa, se quisesse ter o acesso a seu computador restabelecido. De fato, esses ataques causaram prejuízo não apenas a usuários comuns, mas também a empresas que dependiam desse sistema operacional para suas operações diárias (PEREIRA; LIMA, 2017).

Entre os anos de 2013 e 2014, um *ransomware* mais sofisticado ficou bastante conhecido, tornando-se “a bola da vez” quando o assunto era sequestro de dados: o *CryptoLocker*. O modo de infecção geralmente ocorria mediante *downloads* automáticos feitos por meio de sites maliciosos ou anexos de *e-mails* contendo o *malware*. Ele destacou-se por uma caraterística importante usada para enganar as vítimas (em especial as organizações): a utilização de engenharia social (CAVALANCIA, 2018). Segundo a empresa Kaspersky, essa prática empregada por criminosos consiste em manipular psicologicamente e induzir as vítimas a enviarem informações sigilosas, acessar *links* contaminados ou ainda infectar seus computadores com o *malware* (PEREIRA; LIMA, 2017).

Em muitos dos casos os *hackers* aproveitam da falta de conhecimento de funcionários e clientes sobre a importância do cuidado com os dados pessoais para extrair informações valiosas. No geral, os invasores fazem uso de *e-mails* ou links falsos para conseguir tal feito, estratégia conhecida como *phishing*[[7]](#footnote-7). No caso do *CryptoLocker*, eram utilizados *e-mails* com falso conteúdo social. Eles eram projetados para parecerem cartas de reclamação de clientes, faturas ou alertas de contas o que encorajava o destinatário abrir um anexo e, consequentemente, ser infectado (CAVALANCIA, 2018).

Até maio de 2014, estima-se que pelo menos meio milhão de vítimas, entre eles usuários comuns e organizações ao redor do mundo, foi alvo do *CryptoLocker,* e os prejuízos causados por ele foram inestimáveis. A partir de então, o *ransomware* passou a chamar bastante atenção não apenas dos cibercriminosos, mas também de entidades governamentais e empresas de segurança da informação interessados na proteção de sistemas críticos.

Foi então que, em julho do mesmo ano, a Operação Tovar, composta por agências de aplicação de lei e fornecedores de segurança e acadêmicos, foi capaz de derrubar os servidores responsáveis por disseminar o *malware*. Além disso, duas empresas de segurança cibernética (*FireEye* e a *Fox-IT*) descobriram a chave que permitia a descriptografia dos arquivos e disponibilizaram esse serviço gratuitamente às vítimas do *CryptoLocker*. Ainda assim, de acordo com o FBI, este ataque rendeu aos criminosos cerca de 27 milhões de dólares apenas em resgates (RICHARDSON; NORTH, 2017).

Em meados de 2015, outros *malware* similares ao *CryptoLocker* surgiram. Entre eles, um bastante popular: o *CryptoWall* e suas versões posteriores. Em pouco tempo ele ultrapassou o *CryptoLocker*, tornando-se a versão líder em termos de infecção. Sem dúvida, a partir desse período, os *ransomware* começaram a crescer exponencialmente à medida que a internet se fazia mais presente no cotidiano de pessoas e organizações. De acordo com os estudos da Kaspersky, entre os anos de 2014 e 2015 os ataques desse tipo aumentaram 448%. De fato, tais *software* maliciosos tornaram-se tão lucrativos e eficazes para os criminosos que em maio daquele mesmo ano de 2015 surgiu o *Ransomware-As-A-Service* (RAAS) que literalmente significa “*ransomware* como um serviço”. Os invasores disponibilizavam em sites da *Deep-Web[[8]](#footnote-8)* a possibilidade de se criar tais vírus gratuitamente, oferecendo uma comissão pelo valor do resgate. A prática funcionava como um esquema de afiliados e o intuito principal era disseminar ainda mais esses *malware* (RICHARDSON; NORTH, 2017).

Em 2016 o *ransomware* tornou-se ainda mais sofisticado e crítico. Em abril desse mesmo ano, foi lançado o *Petya*. Ele era capaz não apenas de criptografar alguns arquivos comuns, mas um disco rígido inteiro, tornando-o inacessível. Em outras palavras, o computador que fosse infectado por ele ficaria indisponível até que o resgate fosse pago (RICHARDSON; NORTH,2017). O *Petya* foi a primeira ferramenta maliciosa registrada com capacidade para isso, demonstrando assim o potencial dos *ransomware* de interromper atividades que dependiam diretamente de computadores sem necessitar da intervenção do invasor (CAVALANCIA, 2018).

O ano de 2017 foi um dos mais bem-sucedidos para os *malware* de sequestro de dados. Com objetivo de extorquir mais dinheiro das vítimas, o foco dos cibercriminosos passou a ser grandes empresas e órgãos governamentais, em especial aqueles que fornecem estruturas críticas (SECURITY REPORT, 2018). Durante aquele ano, muitos hospitais, empresas, governos e pelo menos 150 universidades foram vítimas do *software* malicioso *WannaCry*, sendo um dos maiores ataques *ransomware* registrados em 2017. Multinacionais como a FedEx e a Nissan, empresas ferroviárias na Alemanha, ferrovias russas, empresas de telecomunicação na Espanha e pelo menos 16 organizações no Reino Unido foram afetadas e tiveram seus sistemas comprometidos (MOHURLE; PATIL, 2017).

Ainda em 2017, uma nova versão mais sofisticada de *ransomware* surgiu e atingiu países que vão dos EUA até a Ucrânia: o *NotPetya*. A princípio, acreditava-se tratar de uma versão diferente do *Petya*, mas não era – por essa razão o nome *NotPetya*, ou seja, “Não-Petya”. Ele foi projetado para se parecer com um *ransomware* comum, mas, na verdade, além de criptografar arquivos e dados importantes, ele os destruía e causava o maior dano possível no sistema que fosse infectado. Ele foi responsável por paralisar quase todas as agências governamentais ucranianas, incapacitando a infraestrutura nacional como aeroportos e ferrovias (COMPUGRAF, 2020).

 De acordo com a Agência Central de Inteligência dos Estados Unidos (CIA), os supostos agentes por trás desse vírus de computador é a Agência Russa de Espionagem Militar GRU. Pressupõe-se que ele tenha sido usado com objetivos políticos, com intuito de paralisar o sistema bancário do país em meio ao conflito relacionado à Crimeia, já que o *malware* apagou dados dos computadores de bancos. O ataque então foi uma estratégia para esconder a identidade do culpado. Sendo assim, o *ransomware* tornou-se muito mais do que uma simples ferramenta maliciosa para extorquir dinheiro. Tornaram-se verdadeiras armas cibernéticas que podem ser usadas tanto por Estados-Nações quanto por ciberterroristas (NAKASHIMA, 2018).

Em 2018, o *ransomware* *Samsam* ganhou notoriedade mundial após uma série de ataques em algumas cidades dos EUA. Ele infectou o departamento de transporte do Colorado, espalhando-se rapidamente por toda a rede de computadores, o que impediu os funcionários de cumprir suas funções e, consequentemente, interrompeu os serviços de transporte. Além disso, ele também infectou o Porto de San Diego, a Universidade de Calgary e a Cidade de Atlanta.

Alguns meses depois, *hackers* iranianos usaram o *Samsam* para sequestrar dados de empresas canadenses e norte-americanas. Como resultado, hospitais municipais e instituições públicas foram vítimas, paralisando serviços e gerando um prejuízo estimado em 30 milhões de dólares (GATEFY, 2021).

Em 2019 e 2020, o *ransomware* *Ryuk* também ficou famoso por infectar grandes organizações, hospitais, instituições governamentais e também por exigir um valor alto para o resgate dos dados, variando entre 100 e 500 mil dólares, em alguns casos podendo chegar a valores maiores, a depender da vítima. Os cibercriminosos envolvidos nesse tipo de ataque buscam empresas com dados essenciais em seus sistemas, sendo, por essa razão, mais propensas a realizar o pagamento.

Além disso, um dado interessante nesse caso é que a chave utilizada na descriptografia dos arquivos é única e diferente para cada vítima. Isso dificulta a utilização de engenharia reversa para criação de mecanismos de recuperação dos arquivos (CONSTANTIN, 2021). Para se ter noção do dano causado pelo *Ryuk*, a rede estadunidense de serviços médicos *United Health Services* teve seus sistemas de computadores e telefonia desabilitados após um ataque desse *malware*, o que interrompeu parcialmente a prestação de seus serviços. Para piorar, o acontecimento tornou-se ainda mais crítico quando foi somado aos efeitos da pandemia do COVID-19 (RIGUES, 2020b).

Em 2021, os *ransomware* tornaram-se praticamente uma epidemia virtual. De acordo com a empresa de cibersegurança *Cybersecurity Ventures*, a cada 11 segundos, uma nova empresa é vítima de um ataque (MILLER, 2020). Outro fator contribuinte para essa realidade é a migração das empresas para o regime de trabalho remoto em função da pandemia de COVID-19, o que facilitou ainda mais a incidência desse tipo de vírus (RIGUES, 2020a).

Indubitavelmente, os *ransomware* são uma preocupação para as empresas de todos os setores especialmente na área da aviação. Devido à sua importância para o transporte Internacional, globalização, segurança financeira, comércio internacional e negócios, ela é considerada uma infraestrutura crítica, além de constantemente movimentar grandes valores econômicos e daí tornar-se um alvo atrativo não apenas para ações maliciosas, mas também para o terrorismo cibernético (NOBLES, 2017).

Por acontecer em um ambiente virtual, o sequestro de dados parece não oferecer qualquer perigo para aviação. Porém, um ataque desse tipo pode ocasionar uma série de prejuízos na vida real. Cita-se como exemplo a empresa Garmin, que teve seu banco de dados criptografados pelo *ransomware WastedLocker* e, em consequência disso, os pilotos que dependiam da plataforma FlyGarminficaram incapazes de utilizar os serviços de navegação aérea fornecido pela empresa (AEROMAGAZINE, 2020). De efeito, os aviões que necessitavam exclusivamente dos sistemas Garmin para navegação se viram impossibilitados de realizá-la de maneira confiável e precisa.

A fabricante de aviões Embraer também sofreu um ataque similar e, como resultado, teve dados confidenciais vazados e seus sistemas de tecnologia da informação interrompidos (EMBRAER, 2021). Os dados incluíam detalhes sobre funcionários, contratos comerciais, fotos de simulação de voo e código-fonte, modelos 3D de aeronaves, entre outros. O vazamento ocorreu após a empresa se negar a pagar o valor do resgate. Esse incidente, além de paralisar as atividades da empresa que dependiam dos sistemas afetados e prejudicar sua reputação em âmbito internacional, evidenciou a importância do armazenamento seguro de informações sigilosas, como o código fonte de sistemas embarcados em aeronaves, por exemplo. De posse desse código, criminosos podem explorar brechas de segurança presentes nesses sistemas e utilizá-las para atos de interferência na aeronave. Além disso, os dados de funcionários e contratos comerciais podem ser usados como ferramenta de engenharia social para obtenção de outras informações sigilosas ou para realização de novos ataques. Vale ressaltar que no Brasil, a lei 13.709 de 14 de agosto de 2018 conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) exige medidas de segurança em relação ao tratamento desses dados por parte de empresas e indivíduos. Um vazamento, portanto, constitui uma violação dessa lei sujeitando a Embraer à análise e sansão por parte da Autoridade Nacional de Proteção de Dados (ANPD) (IAHN, 2021). Por fim, os modelos 3D de aeronaves e fotos de simulação podem ser comercializados ilegalmente para empresas concorrentes.

Em arremate, além de comprometer sistemas, o *ransomware* também pode ser utilizado para obtenção de informações sigilosas relacionadas à segurança as quais podem ser utilizadas por outros grupos criminosos para outras ações maliciosas, como ciberterroristas, por exemplo (ALECRIM, 2020).

# 2 PREVENÇÃO E MITIGAÇÃO DE ATAQUES *RANSOMWARE*

Dada a crescente “digitalização” da aviação, o sequestro de dados é algo cada vez mais provável e possível de acontecer. Ele representa um grande desafio para o setor, pois a complexidade dos ataques, bem como sua imprevisibilidade, torna os riscos difíceis de serem mensurados. Em outras palavras, é difícil estimar dano que um ataque *ransomware* pode causar antes que ele aconteça, já que o ataque pode atuar em diversas frentes da Aviação Civil – como na indústria aeronáutica, no controle de tráfego aéreo, em empresas aéreas e nas demais entidades do setor. Além disso, novas oportunidades de ataque surgem continuamente à medida que novos sistemas são desenvolvidos. Por essa razão, a implementação de práticas que visem à prevenção de ataquese à mitigação de riscos após uma infecção, bem como a constante busca por melhoria desses processos, são fundamentais para a segurança dos sistemas da aviação (HAASS, 2016).

2.1 DA PREVENÇÃO CONTRA *RANSOMWARE*

Sem dúvidas, um dos passos iniciais essenciais à prevenção desse tipo de ataque é a conscientização sobre os riscos envolvidos e o treinamento de pessoal para lidar com essa ameaça, da melhor maneira possível. Dito de outro modo, adotar medidas de proteção não é suficiente: é necessário também um esforço individual para que elas sejam cumpridas (MILLER, 2020). Embora tenha havido progresso significativo para fortalecer a segurança da aviação (*Safety* e *Security*), há claramente muito a ser feito em relação à prevenção de ataques cibernéticos na aviação, e a conscientização é uma importante ação, nesse sentido (SCHÓBER; KOBLEN; SZABO, 2012).

Conscientizar envolve, entre outras coisas, reforçar as políticas da organização quanto ao não compartilhamento de credenciais de usuário; o incentivo à implementação de senhas fortes e o uso da autenticação de dois fatores sempre que possível. Apesar de serem medidas simples, elas atuam como barreiras primárias de segurança, dificultando a entrada de invasores. Outro ponto importante, segundo Zaghetto et al. (2017), é instruir os usuários a utilizarem a internet e dispositivos digitais de maneira consciente e segura, bem como garantir que eles se sintam confortáveis para relatar incidentes de segurança. Isso evita que novas oportunidades de ataque ocorram (MILLER, 2020).

Considerando que um dos meios de infecção ocorre no acesso de anexos de *e-mail* contendo *ransomware,* uma boa medida de prevenção consiste em adotar um *software* ou plataforma própria específica para a comunicação dentro da empresa. Isso reduz (ou mesmo elimina) o risco de os usuários clicarem em *e-mails* contendo o vírus, diminuindo significativamente a incidência de *spam* e *phishing,* além de evitar que o *malware* se propague a partir do usuário infectado*.* Além disso, sites maliciosos também podem conter o vírus. Desse modo, uma maneira de garantir a segurança dos usuários, caso acessem sites infectados é, além do treinamento, o uso de um bom antivírus corporativo (MILLER, 2020). Somado a isso, o uso de equipamentos de Gerenciamento Unificado de Ameaças (*Unified Threat Management* ou UTM) asseguram ainda mais a proteção, pois reúnem uma série de recursos de segurança em um só aparelho. Eles atuam como filtros e impedem que o *ransomware* tenha acesso aos dados do sistema.

Vale ressaltar também a importância de manter os sistemas operacionais sempre atualizados, pois isso garante que as vulnerabilidades sejam corrigidas e evita brechas na segurança. O sistema operacional *Windows*,por exemplo, disponibiliza aos seus usuários atualizações periódicas que devem ser feitas para maior proteção. Além disso, são disponibilizadas ferramentas gratuitas para o gerenciamento de atualizações, como o *Windows Server Update Service* (WSUS), que visa atender às redes empresariais que podem ter uma grande quantidade de computadores conectados. Gerenciar atualizações ajuda a manter a eficiência operacional, a superar vulnerabilidades de segurança e a manter a estabilidade do ambiente de produção. Isso evita que o *ransomware* utilize essas deficiências como uma oportunidade de invasão (GEREND, 2021).

Outra prática utilizada tanto para a prevenção quanto para a diminuição do estrago nos ataques é a utilização de cópias de segurança dos arquivos, conhecidas como *backups*. Zaghetto e outros (2017) afirmam que os *backups* são a chave para se limitar o poder dos *ransomware,* pois, em caso de infecção, será necessário apenas formatar as máquinas atingidas, restaurar os arquivos, rever as políticas de segurança e alertar a equipe. Existem basicamente dois tipos de *backup: online* e *offline*. O primeiro tipo consiste em armazenar os dados em um servidor via internet, atividade esta, conhecida como armazenamento em nuvem. As vantagens neste casoé o armazenamento mais seguro dos dados e a possibilidade de acesso a partir de qualquer computador com internet. Porém, a desvantagem é justamente a dependência de conexão com a internet, pois, caso ela venha a ser interrompida, torna-se difícil o remanejamento dos arquivos e a restituição do sistema.

Por sua vez, os *backups offline* deverão serfeitos com o uso de unidades externas que permitirão o armazenamento de dados em unidades físicas, como HDs (*Hard Disks)*, SSDs (*Solid-State Drive*) e *pendrives*. Sua vantagem é que não necessitam de internet para que se tenha acesso aos dados; entretanto, as unidades físicas precisam ser guardadas em segurança, pois podem ser roubadas, danificadas ou extraviadas e, de efeito, os dados serão perdidos (ZAGHETTO et al., 2017).

2.2 DA MITIGAÇÃO CONTRA *RANSOMWARE*

Mesmo com todos os esforços de prevenção, ainda é possível ser alvo de ataques de um *ransomware,* pois sempre haverá ameaças que exploram vulnerabilidades anteriormente desconhecidas (MILLER, 2020). Sendo assim, medidas de mitigação são necessárias para reduzir os impactos de uma infecção. Do ponto de vista da segurança, formatar o computador e fazer a recuperação dos arquivos a partir dos *backups* é sempre a melhor opção. Caso não seja viável, pode-se usar *software* de descriptografia que geralmente são oferecidos por antivírus. Eles não garantem que os arquivos sejam recuperados, pois novos *ransomware* surgem constantemente e algumas criptografias utilizadas por eles são praticamente impossíveis de serem quebradas (ZAGHETTO et al., 2017).

Além disso é fundamental desconectar ou desligar imediatamente o computador infectado. Se ele estiver conectado a uma rede, os administradores devem desligá-la o mais rapidamente possível para minimizar a propagaçãodo vírus para outras máquinas*.* Após isolado, é importante ainda executar uma verificação completa no computador afetado para descobrir qual foi o vírusutilizado no ataque pois, a partir dessa informação, é possível saber se existe alguma ferramenta de descriptografia que lhe seja específica. Cabe ressaltar que grande parte dos *ransomware* não destrói os dados, apenas os criptografa. Desta feita, removê-lo não é suficiente para ter os dados de volta (RICHARDSON; NORTH, 2017).

A orientação de segurança é que nunca se deve pagar o resgate pois, além de não haver qualquer garantia de que os dados serão recuperados, o pagamento incentiva os criminosos a darem continuidade à prática delituosa. No entanto, em alguns casos, o pagamento do resgaste infelizmente pode ser a única alternativa, sendo necessário considerá-lo como a última das opções e somente no caso de todas as demais serem esgotadas (ZAGHETTO et al*.,* 2017).

**CONSIDERAÇÕES FINAIS**

Sem dúvidas, a constante evolução de tecnologias como *software,* internet das coisas (IoT) e tantos outros sistemas computadorizados na aviação trouxeram novos desafios à segurança, e o *ransomware* é um deles. Considerando a abrangência e a importância de tais elementos nas operações aéreas diárias, o sequestro de dados pode, entre outras coisas, comprometer ou indisponibilizar sistemas necessários à aviação de um modo geral e, com ainda mais força, à aviação civil, afetando empresas aéreas, aeroportos, pilotos, controladores, passageiros etc. Apesar de ter-se a sensação de que não há grandes riscos no ambiente virtual, os *ransomware* são capazes de ocasionar enormes prejuízos, podendo ser causa latente para um acidente ou ser usados para o terrorismo cibernético.

Além disso, segundo Miller (2020), eles se tornaram, atualmente, uma verdadeira epidemia cibernética e, portanto, as chances de ataque tornam-se cada vez mais acentuadas e possíveis. Assim, para garantir que os sistemas da aviação sejam mais seguros, são fundamentais a análise e o gerenciamento de risco deste ambiente virtual, considerando políticas e procedimentos de proteção que visem à manutenção da segurança cibernética. Tais elementos devem incluir a conscientização e o treinamento dos usuários voltados à importância de manter o ambiente virtual seguro, ao uso constante de *backups* e à implementação de um constante plano de contingência que identifique pistas prováveis de alguma invasão.

 Cabe ressaltar a observâncias de algumas leis que regem o âmbito da prevenção de ameaças cibernéticas e da proteção de dados pessoais, tais como a resolução A39-19 adotada pela Assembleia da Organização da Aviação Civil Internacional (OACI), a qual aborda a segurança cibernética na aviação civil bem como apresenta ações direcionadas aos Estados-Membros visando a proteção de sistemas críticos da aviação, e, no contexto nacional, a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual dispõe sobre o tratamento de dados pessoais.

Por fim, mas não menos importante, baseando-se nos estudos de Schober, Koblen e Szabo (2012) e também na resolução A39-19 da OACI (2016), torna-se necessária uma estreita cooperação intergovernamental com os *players* do segmento aeronáutico.De igual modo*,* considera-seindispensável uma política de segurança cibernética com a coordenação de todas as entidades ligadas à aviação, como os sistemas aeroportuários, as indústrias aeronáuticas, as companhias aéreas, as instituições de ensino superior e as autoridades governamentais correlatas, visando à implementação de medidas de prevenção e de combate às ameaças cibernéticas, especialmente os *ransomware*.

**REFERÊNCIAS**

AEROMAGAZINE (São Paulo**). Hackers sequestram dados da Garmin e exigem US$ 10 milhões de resgate:** Grupo criminoso criptografou milhares de documentos e dados do fabricante. 1.0. [S. l.], 27 jul. 2020. Disponível em: https://aeromagazine.uol.com.br/artigo/hackers-sequestram-dados-da-garmin-e-exigem-us-10-milhoes-de-resgate\_5579.html. Acesso em: 30 set. 2021

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL (ANAC). **Anacpédia**. [*S. l.*], RNAV 2010. Disponível em: https://www2.anac.gov.br/anacpedia/por\_esp/tr329.htm. Acesso em: 13 set. 2021.

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. (ANAC) **Manual de Conscientização em Segurança Cibernética na Aviação Civil** – Ciberespaço; Trojan; Spam; Phishing Brasília: [*s. n.*], 2021. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aerodromos/avsec/arquivos/Manual\_de\_conscientizacao\_sobre\_Ciberseguranca.pdf. Acesso em: 23 set. 2021.

ALECRIM, Emerson. **Embraer sofre vazamento de dados após ataque de ransomware**. [S. l.], 8 dez. 2020. Disponível em: https://tecnoblog.net/391594/embraer-sofre-vazamento-dados-apos-ataque-ransomware/#:~:text=A%20Embraer%20entrou%20para%20a%20lista%20de%20organiza%C3%A7%C3%B5es,internos%20vazados.%20Como%20recuperar%20arquivos%20encriptados%20por%20ransomware. Acesso em: 30 set. 2021.

CAVALANCIA, Nick. **Destaques da história do Ransomware:** do AIDS Trojan ao Locky. [*S. l.*], 8 mar. 2018. Disponível em: https://www.veeam.com/blog/pt-br/ransomware-history-study-cases.html. Acesso em: 12 set. 2021.

COMPUGRAF (SP). ***NotPetya*:** tudo sobre o Ciberataque mais devastador da História. [*S. l.*], 5 ago. 2020. Disponível em: https://www.compugraf.com.br/*NotPetya*-tudo-sobre-o-ciberataque-mais-devastador-da-historia/. Acesso em: 12 set. 2021.

CONSTANTIN, Lucian. **Ryuk ransomware explained:** a targeted, devastatingly effective attack. [*S. l.*], 19 mar. 2021. Disponível em: https://www.csoonline.com/article/3541810/ryuk-ransomware-explained-a-targeted-devastatingly-effective-attack.html. Acesso em: 14 set. 2021.

FREITAS, Ernani; PRODANOV, Cléber. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo - Rio Grande do Sul, Brasil: Editora Feevale, 2013. 227 p. v. 1b. ISBN 978-85-7717-158-3. *E-book*.

GALVÃO, Ricardo. **Ransomware**: Sequestro de Dados. Palestra proferida na VI Semana de Infraestrutura da Internet. [S. l.], 12 dez 2016. Disponível em: https://www.youtube.com/watch?v=RZIjBQ3ejUY. Acesso em: 15 set. 2021.

GARRETT, Filipe. **O que é Deep Web?**: Entenda o que é e como funciona a Deep Web, parte da Internet que não pode ser achada no Google. 2. ed. [S. l.]: Techtudo, 16 mar. 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/03/o-que-e-deep-web.ghtml. Acesso em: 21 set. 2021.

GATEFY. **7 casos reais e famosos de ataques de ransomware**. [*S. l.*], 23 mar. 2021. Disponível em: https://gatefy.com/pt-br/blog/casos-reais-famosos-ataques-ransomware/. Acesso em: 15 set. 2021.

GEREND, Jason. **Windows Server Update Services (WSUS).** [S. l.]: Microsoft, 12 ago. 2021. Disponível em: https://docs.microsoft.com/pt-br/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus. Acesso em: 11 set. 2021.

HAASS, John *et al*. Aviation and Cybersecurity: Opportunities for Applied Research. **Embry-Riddle Aeronautical University Scholarly Common,** [*s. l.*], 7 jul. 2016.

IAHN: Tiago. *In*: SERPO. **Você sabe o que é um ataque de ransomware?** [*S. l.*], 5 ago. 2021. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2021/ataque-de-ransomware. Acesso em: 7 dez. 2021.

LONGEN, Andrei. **O Que é Armazenamento em Nuvem?** [*S. l.*]: Weblink, 7 nov. 2018. Disponível em: https://www.weblink.com.br/blog/o-que-e-armazenamento-em-nuvem. Acesso em: 15 set. 2021.

MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa**. Hacker. [*S. l.*]: Melhoramentos, 2021. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/hacker/. Acesso em: 14 set. 2021.

MILLER, Lawrence. **Ransomware Defense For Dummies**. 2. ed. atual. Nova Jérsei: Cisco, 2020. 46 p. v. 1. ISBN 978-1-119-68282-0. *E-book*.

MOHURLE, Savita; PATIL, Manisha. A brief study of Wannacry Threat: Ransomware Attack 2017. **International Journal of Advanced Research in Computer Science**, Pune, Índia, v. 8, n. 5, p. 1938-1940, 1 jun. 2017. Disponível em: https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf. Acesso em: 14 set. 2021.

NAKASHIMA, Ellen. **Russian military was behind ‘*NotPetya*’ cyberattack in Ukraine, CIA concludes**. [*S. l.*], 2018. Disponível em: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef\_story.html. Acesso em: 15 set. 2021.

NOBLES, Calvin. Cyber Threats in Civil Aviation. **Security Solutions for Hyperconnectivity and the Internet of Things**, [*s. l.*], p. 272-301, 2017. DOI 10.4018/978-1-5225-0741-3.ch011. Disponível em: https://www.academia.edu/40191438/Cyber\_Threats\_in\_Civil\_Aviation. Acesso em: 9 set. 2021.

ORGANIZAÇÃO DA AVIAÇÃO CIVIL INTERNACIONAL. Resolução nº A39-19, de 27 de setembro de 2016. DELIBERAÇÕES APROVADAS NA 39ª SESSÃO DA ASSEMBLÉIA. **Addressing Cybersecurity in Civil Aviation**, [*S. l.*], 6 out. 2016. Disponível em: https://www.icao.int/Meetings/a39/Documents/Resolutions/a39\_res\_prov\_en.pdf. Acesso em: 7 dez. 2021.

PEREIRA, Danielle; LIMA, Isabela. **Ransomware e suas relações com a criptografia**. Orientador: Claiton Luís Soares. 2017. 13 p. Trabalho de conclusão de curso (Técnico em Informática) – Instituto Federal Triângulo Mineiro, Paracatu-MG, 2017. Disponível em: https://roitier.pro.br/wp-content/uploads/2017/02/Banca-02-RANSOMWARE-E-SUAS-RELA%C3%87%C3%95ES-COM-A-CRIPTOGRAFIA.pdf. Acesso em: 15 set. 2021.

RICHARDSON, Ronny; NORTH, Max M. Ransomware: Evolution, Mitigation and Prevention. **International Management Review**, Kennesaw State University, v. 13, ed. 1, p. 10-21, 1 jan. 2017. Disponível em: https://digitalcommons.kennesaw.edu/facpubs/4276/. Acesso em: 15 set. 2021.

RIGUES, Rafael. **Ransomware pode se tornar um problema ainda maior em 2021**. 1. ed. [*S. l.*], 17 set. 2020a. Disponível em: https://olhardigital.com.br/2020/12/31/noticias/ransomware-pode-se-tornar-um-problema-ainda-maior-em-2021/. Acesso em: 14 set. 2021.

RIGUES, Rafael. **Ataque de ransomware afeta rede de hospitais nos EUA**. [*S. l.*]: Olhar Digital, 29 set. 2020b. Disponível em: https://olhardigital.com.br/2020/09/29/seguranca/ataque-de-ransomware-afeta-rede-de-hospitais-nos-eua/. Acesso em: 15 set. 2021.

SCHÓBER, Tomáš; KOBLEN, Ivan; SZABO, Stanislav. Present and potential security threats posed to civil aviation. **Incas Bulletin,** Eslováquia, 2012, v. 4, n. 2, p. 169-175, 10 fev. 2012. DOI 10.13111/2066-8201.2012.4.2.17. Disponível em: https://bulletin.incas.ro/files/schober\_koblen\_szabo\_v4\_iss\_2\_full.pdf. Acesso em: 9 set. 2021

SECURITY REPORT. **Brechas relacionadas a infraestruturas de nuvem crescem mais de 400%**. 1. ed. [*S. l.*]: Redação, 16 abr. 2018. Disponível em: https://www.securityreport.com.br/destaques/brechas-relacionadas-a-infraestruturas-de-nuvem-crescem-mais-de-400/#.YUSdWbhKhPZ. Acesso em: 14 set. 2021.

ZAGHETTO, Cauê *et al*. Ransomware: este problema pode ser seu também. **Tecnologias em Projeção,** [*s. l.*], v. 8, n. 2, 10 nov. 2017. ISSN 2178-6267. Disponível em: http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/view/791. Acesso em: 11 set. 2021.



1. Método de navegação que permite a operação de uma aeronave em qualquer curso desejado dentro da área de abrangência dos sinais de um auxílio à navegação ou dentro das limitações da capacidade do sistema de navegação de bordo (ANAC, 2010). [↑](#footnote-ref-1)
2. Nos anos 90 surgiu o termo ciberespaço indicando um espaço virtual que se acredita existir atrás das atividades eletrônicas dos dispositivos computacionais (ANAC, 2021). [↑](#footnote-ref-2)
3. Indivíduo que se dedica a entender o funcionamento interno de dispositivos, programas e redes de informática com o fim, entre outras coisas, de encontrar falhas em sua segurança ou conseguir um atalho inteligente que possa vir a resultar em um novo recurso ou ferramenta (MICHAELIS, 2021). [↑](#footnote-ref-3)
4. É uma tecnologia que permite guardar dados na internet por meio de um servidor online sempre disponível. Nele, o usuário pode armazenar arquivos, documentos e outras informações sem precisar de um HD no seu computador (LONGEN, 2018). [↑](#footnote-ref-4)
5. Trojan ou Cavalo de Tróia é um *malware* que pode entrar em um computador disfarçado como um programa comum e legítimo. Ele serve para possibilitar a abertura de uma porta de forma que usuários mal-intencionados possam invadir um PC (ANAC (2021). [↑](#footnote-ref-5)
6. *Spam* é uma mensagem eletrônica (e-mail) recebida, mas não solicitada, que possui conteúdo publicitário (ANAC, 2021). [↑](#footnote-ref-6)
7. *Phishing* é o método usado por criminosos para obter informações de usuários de Internet, geralmente mediante envio de e-mail por organizações aparentemente legítimas, com o endereço de página eletrônica (URL) falso (ANAC, 2021). [↑](#footnote-ref-7)
8. A *Deep Web* (Internet Profunda, em tradução livre) é uma área da Internet que fica "escondida" e tem pouca regulamentação (GARRETT, 2020). [↑](#footnote-ref-8)